1 Introduction

This manual describes the input syntax and output of our cryptographic protocol verifier. It does not describe the internal algorithms used in the system. These algorithms have been described in research papers [3, 2, 4, 5] that can be downloaded at https://bblanche.gitlabpages.inria.fr/publications/index.html.

The goal of our protocol verifier is to prove security properties of protocols in the computational model. The input file describes the considered security protocol, the hypotheses on the cryptographic primitives used in the protocol, and security properties to prove.
2 Command Line

The syntax of the command line is as follows:

```
./cryptoverif [options] (filename)
```

where (filename) is the name of the input file. The options can be:

- `-in (frontend)`: Chooses the frontend to use by CryptoVerif. (frontend) can be either channels (the default) or oracles. The channels frontend uses a calculus inspired by the pi calculus, described in Section 3 and in [3, 2]. The oracles frontend uses a calculus closer to cryptographic games, described in Section 4 and in [4, 5]. By default, CryptoVerif uses the oracles frontend when the input (filename) ends with `.ocv`, and otherwise it uses the channels frontend.

- `-lib (filename)`: Specifies a library file to be loaded by the system before reading the input file. In the channels frontend, the loaded file is (filename).cwl; in the oracles frontend, it is (filename).ocwl. (The extension .cwl or .ocwl may also be included in (filename).) Library files typically contain default declarations useful for several protocols.

  When no `-lib` option appears, CryptoVerif loads the default library, default.cwl in the channels front-end, default.ocwl in the oracles front-end. The default library is searched in the current directory, then in the directory that contains the executable cryptoverif.

  Multiple libraries can be specified by using `-lib` for each library. The libraries are loaded in the same order as they appear on the command line.

- `-oproof (filename)`: Output the proof in the given file name, instead of displaying it on the standard output.

- `-ocommands (filename)`: Output the interactive commands in the given file name. By default, this file is in the current directory. If command-line option `-o` is present, it is in the directory specified by that option.

- `-tex (filename)`: Activates TeX output, and sets the output file name. In this mode, CryptoVerif outputs a TeX version of the proof, in the given file.

- `-oequiv (filename)`: Append the generated special equivalences to the given file. (See equiv ... special.)

- `-impl (language)`: Instead of proving the protocol, generate an implementation in the chosen language corresponding to the modules defined in the input file. The language can be OCaml or FStar.

- `-o (directory)`: Outputs the files generated by `out_game`, `out_state`, `out_facts`, `out_equiv`, and `out_commands` in the given directory. If the `-impl` option is given, outputs the implementation files in the given directory.

Input files with a name that ends in `.pcv` are meant to be analyzed by both CryptoVerif and ProVerif. When CryptoVerif analyzes such a file, it first preprocesses it with `m4` with CryptoVerif defined. Similarly, when ProVerif analyzes such a file, it first preprocesses it with `m4` with ProVerif defined. That allows you to conditionally include parts of the file depending on whether CryptoVerif or ProVerif analyzes it.

3 channels Front-end

Comments can be included in input files. Comments are surrounded by (`*` and `*`). Nested comments are supported.

Identifiers (`ident`) begin with a letter (uppercase or lowercase) and contain any number of letters, digits, the underscore character (`_`), the quote character (`'`), as well as accented letters of the ISO Latin 1 character set. Case is significant. Keywords cannot be used as ordinary identifiers.
• \([M]\) means that \(M\) is optional; \((M)^*\) means that \(M\) occurs 0 or any number of times.

• \(\text{seq}(X)\) is a sequence of \(X\): \(\text{seq}(X) = [(\langle X \rangle)^* (\langle X \rangle)] = (X), \ldots, (X).\) (The sequence can be empty, it can be one element \((X)\), or it can be several elements \((X)\) separated by commas.)

• \(\text{seq}^+(X)\) is a non-empty sequence of \(X\): \(\text{seq}^+(X) = (\langle X \rangle)^+ (\langle X \rangle) = (X), \ldots, (X).\) (It can be one or several elements of \((X)\) separated by commas.)

Figure 1: Grammar notations

The keywords are: \texttt{builtin}, \texttt{channel}, \texttt{collision}, \texttt{const}, \texttt{def}, \texttt{defined}, \texttt{diff}, \texttt{do}, \texttt{else}, \texttt{eps_find}, \texttt{eps_rand}, \texttt{equation}, \texttt{equiv}, \texttt{equivalence}, \texttt{event}, \texttt{event_abort}, \texttt{find}, \texttt{forall}, \texttt{foreach}, \texttt{fun}, \texttt{get}, \texttt{if}, \texttt{implementation}, \texttt{in}, \texttt{inf}, \texttt{inj-event}, \texttt{insert}, \texttt{is-cat}, \texttt{length}, \texttt{let}, \texttt{letfun}, \texttt{letprob}, \texttt{max}, \texttt{maxlength}, \texttt{min}, \texttt{new}, \texttt{newChannel}, \texttt{number}, \texttt{optim-if}, \texttt{orfind}, \texttt{out}, \texttt{param}, \texttt{Pcoll1rand}, \texttt{Pcoll2rand}, \texttt{proba}, \texttt{process}, \texttt{proof}, \texttt{public_vars}, \texttt{query}, \texttt{query_equiv}, \texttt{return}, \texttt{secret}, \texttt{set}, \texttt{special}, \texttt{suchthat}, \texttt{table}, \texttt{then}, \texttt{time}, \texttt{type}, \texttt{yield}.

Strings (⟨string⟩) start and end with "", inside the string, \(\backslash\) stands for ", \(\backslash\) stands for \(\), \(\backslash\) for linefeed, \(\backslash\) for tab, \(\backslash\) for backspace, \(\backslash\) for carriage return, and \(\backslash\) for \(\). Other combinations with \(\backslash\) are not allowed. Characters other than "" and \(\) stand for themselves.

In case of syntax error, the system indicates the character position of the error (line and column numbers). Please use your text editor to find the position of the error. (The error messages can be interpreted by \texttt{emacs}.)

The input file may consist of a list of declarations followed by a process:

\[
\text{<declaration>}^* \text{ process } \langle \text{iprocess} \rangle
\]

The process describes the considered security protocol; the declarations specify in particular hypotheses on the cryptographic primitives and the security properties to prove.

Alternatively, the input may also consist of a list of declarations followed by an equivalence query:

\[
\text{<declaration>}^* \text{ equivalence } \langle \text{iprocess} \rangle \langle \text{iprocess} \rangle \text{[public_vars seq]}\text{[ident]}\]
\]

The query \texttt{equivalence} \(Q_1 Q_2\) tells CryptoVerif to show that the processes (games) \(Q_1\) and \(Q_2\) are computationally indistinguishable. When it is present, the indication \texttt{public_vars} \(x_1, \ldots, x_n\) means that the adversary has read access to the variables \(x_1, \ldots, x_n\).

Finally, the input may also be:

\[
\text{<declaration>}^* \text{query_equiv}([\text{[ident]}][\text{[(ident)]}]) \hspace{1cm} \text{[omode]} [1 \ldots 1] \text{[omode]} \text{[n]} \text{[\langle n \rangle]} \text{[\langle seq \langle option \rangle \rangle 1]} \text{[\langle group \rangle]} [1 \ldots 1] \text{[\langle group \rangle]}
\]

The keyword \texttt{query_equiv} is followed by an indistinguishability property specified in the same syntax as assumptions on security primitives (see the declaration \texttt{equiv}), except that the probability of distinguishing the two sides is replaced with \(?\). CryptoVerif is going to bound this probability, so we do not need to give it.

• When the option \texttt{[computational]} is absent, CryptoVerif then converts this assumption into an equivalence between two processes and tries to prove it.

• When the option \texttt{[computational]} is present, CryptoVerif then converts this assumption into the unreachability of an event triggered when the oracles on the two sides return different results. The unreachability of this event implies that both sides are indistinguishable. In this case, the random values marked \texttt{[unchanged]} are shared between both sides, while the others are considered independent. In principle, any mapping from the random values of the left-hand side to the random values of the right-hand side could allow us to prove the desired indistinguishability property, as long as it preserves the probability distributions; however, CryptoVerif only supports the case in which some random values are equal on both sides and others are independent.
(identbound) ::= [ident] = (ident) <= (ident)  
(simpleterm) ::= (ident)  

(vartype) ::= seq^+(ident): (ident)  
| (ident)(seq(simpleterm))  
| (seq(simpleterm))  
| (ident)[seq(simpleterm)]  

(vartypeb) ::= seq^+(ident): (ident)  
| seq^+(ident) <= (ident)  
| (ident)(seq(simpleterm))  
| (seq(simpleterm))  
| (ident)[seq(simpleterm)]  

(ident_underscore) ::= (ident)  
| (ident)(seq(simpleterm))  
| (seq(simpleterm))  
| (ident)[seq(simpleterm)]  

(basicpat) ::= (ident_underscore)  
| (ident_underscore):(ident)  
| (ident_underscore) <= (ident)  

(letterm) ::= ... (as in (simpleterm) with (letterm) instead of (simpleterm))  
| (basicpat) <= (letterm);(letterm)  
| let (basicpat) = (letterm) in (letterm)  

(term) ::= ... (as in (simpleterm) with (term) instead of (simpleterm))  
| new (ident);(ident);(term)  
| (ident) <=R (ident);(term)  
| (basicpat) <= (term);(term)  
| let (pattern) = (term) in (term) [else (term)]  
| if (cond) then (term) else (term)  
| find[unique] (findbranch) (orfind (findbranch))^* else (term)  
| event (ident)[seq(term)]; (term)  
| event_abort (ident)  
| insert (ident)(seq(term)); (term)  
| get[unique] (ident)(seq(pattern)) [suchthat (term)] in (term) else (term)  

(varref) ::= (ident)[seq(simpleterm)]  
| (ident)  

(cond) ::= defined(seq^+(varref)) & (term)  
| (term)  

(findbranch) ::= seq(identbound) suchthat (cond) then (term)  

(pattern) ::= (basicpat)  
| (ident)(seq(pattern))  
| (seq(pattern))  
| = (term)  

Figure 2: Grammar for terms and patterns
\begin{verbatim}
⟨event⟩ ::= event(⟨ident⟩[seq⟨letterm⟩])
| inj-event(⟨ident⟩[seq⟨letterm⟩])
⟨queryterm⟩ ::= (⟨queryterm⟩)
| ⟨queryterm⟩ && ⟨queryterm⟩
| ⟨queryterm⟩ || ⟨queryterm⟩
| ⟨queryterm⟩ => ⟨queryterm⟩
| ⟨queryterm⟩ <- (⟨letterm⟩); ⟨queryterm⟩
| ⟨letterm⟩
⟨query⟩ ::= secret ⟨ident⟩ [public_vars seq⟨ident⟩] [Seq+⟨ident⟩]
| forall seq+(⟨vartype⟩); ⟨queryterm⟩ [public_vartypseq ⟨ident⟩]
\end{verbatim}

Figure 3: Grammar for queries

The goal of this query is to build modular proofs: we can prove a property using this query, and then use it as assumption in a subsequent proof by just copy-pasting it.

A library file (specified on the command-line by the -lib option) consists of a list of declarations. Notations are summarized in Figure 1 and various syntactic elements are described in Figures 2, 3, 4, 5, and 7.

Processes are described in a process calculus. In this calculus, terms represent computations on bitstrings. Simple terms consist of the following constructs:

- A term between parentheses (M) allows to disambiguate syntactic expressions.
- An identifier can be either a constant symbol f (declared by const or fun without argument) or a variable identifier.
- The function application f(M₁,...,Mₙ) applies function f to the result of M₁,...,Mₙ.
- The tuple application (M₁,...,Mₙ) builds a tuple from M₁,...,Mₙ (corresponds to the concatenation of M₁,...,Mₙ with length and type indications so that M₁,...,Mₙ can be recovered without ambiguity). This is allowed only for n ≠ 1, so that it is distinguished from parenthesizing.
- The array access x[M₁,...,Mₙ] returns the cell of indices M₁,...,Mₙ of array x.
- =, <>, ||, && are function symbols that represent equality and inequality tests, disjunction and conjunction. They use the infix notation, but are otherwise considered as ordinary function symbols.

Terms contain further constructs <-R, <-, event, event_abort, if, find, let, new, insert, get, and diff which are similar to the corresponding constructs of output processes but return a bitstring instead of executing a process. They are not allowed to occur in defined conditions of find. The constructs event and insert are not allowed to occur in conditions of find or get. We refer the reader to the description of processes below for a fully detailed explanation.

- new x:T;M chooses a new random number in type T, stores it in x, and returns the result of M. x <-R T;M is equivalent to new x:T;M.
- let p = M in M' else M'' tries to decompose the term M according to pattern p. In case of success, returns the result of M', otherwise the result of M''.

The pattern p can be:
Figure 4: Grammar for probabilities
(repl) ::= !='{$ident} <= {$ident}'
| foreach {$ident} <= {$ident} do
(res) ::= new {$ident}:{$ident};
| {$ident} <-R {$ident};
(obody_equiv) ::= ((obody_equiv))
| event_abort {$ident}
| (res) (obody_equiv)
| {basicpat} <- {$term}; (obody_equiv)
| let (pattern) = {$term} in (obody_equiv) [else (obody_equiv)]
| if (cond) then (obody_equiv) else (obody_equiv)
| find[uniquel] (findbranch) (orfind (findbranch))' else (obody_equiv)
| insert ($ident) (seq($term)); (obody_equiv)
| get[uniquel] ($ident)(seq(pattern)) [suchthat ($term)] in (obody_equiv) else (obody_equiv)
| return((term))

(findbranch) ::= seq($ident) suchthat (cond) then (obody_equiv)

(ogroup) ::= {$ident}(seq(vartype)) [Dx] [useful change] := (obody_equiv)
| [[repl]] (res)* (ogroup)
| [[repl]] (res)' (ogroup) | ... | (ogroup))

(omode) ::= (ogroup) [exist]
| (ogroup) [all]

(specialarg) ::= {$ident}
| ($string)
| (seq(specialarg))

Figure 5: Grammar for equivalences

(dim) ::= time[*{$int}]
| length[*{$int}]
| number
| (dim) * (dim)
| (dim) / (dim)

(vardim) ::= seq+ {$ident}: (dim)

Figure 6: Grammar for dimensions

7
(channel) ::= ⟨ident⟩[seq(⟨ident⟩)]
(oprocess) ::= ⟨ident⟩[(seq(term))]  
| ⟨(oprocess)⟩
| yield
| event ⟨ident⟩[(seq(term))] [; ⟨oprocess⟩]
| event_abort ⟨ident⟩
| ⟨ident⟩<= ⟨ident⟩[; ⟨oprocess⟩]
| ⟨basicpat⟩<= ⟨term⟩[; ⟨oprocess⟩]
| let ⟨pattern⟩= ⟨term⟩[in ⟨oprocess⟩] [else ⟨oprocess⟩]]
| if ⟨cond⟩ then ⟨oprocess⟩ [else ⟨oprocess⟩]
| find[unique] ⟨findbranch⟩ (orfind ⟨findbranch⟩)* [else ⟨oprocess⟩]
| insert ⟨ident⟩(seq(term)) [; ⟨oprocess⟩]
| get[unique] ⟨ident⟩(seq(pattern)) [suchthat ⟨term⟩] in ⟨oprocess⟩ [else ⟨oprocess⟩]
| out((channel), ⟨term⟩)[; ⟨iprocess⟩]

(findbranch) ::= seq(⟨identbound⟩) suchthat ⟨cond⟩ then ⟨oprocess⟩

(iprocess) ::= ⟨ident⟩[(seq(term))]  
| ⟨(iprocess)⟩
| 0
| ⟨(iprocess)⟩ | ⟨(iprocess)⟩
| !⟨ident⟩ <= ⟨ident⟩ ⟨iprocess⟩
| foreach ⟨ident⟩ <= ⟨ident⟩ do ⟨iprocess⟩
| in((channel), ⟨pattern⟩))[; ⟨oprocess⟩]

Figure 7: Grammar for processes (channels front-end)
- \(x[T]\) variable, possibly with its type. Matches any bitstring (in type \(T\)), and stores it in \(x\).
- \(_[T]\) underscore, possibly with a type. Matches any bitstring (in type \(T\)), and ignores its value.
- \(f(p_1, \ldots, p_n)\) where the function symbol \(f\) is declared [data]. Matches bitstrings \(M\) equal to \(f(M_1, \ldots, M_n)\) for some \(M_1, \ldots, M_n\) that match \(p_1, \ldots, p_n\). (The poly-injectivity of \(f\) allows us to compute possible values \(M_1, \ldots, M_n\) of its arguments from the value of \(M\), and to check whether \(M\) is equal to the resulting value of \(f(M_1, \ldots, M_n)\).)
- \((p_1, \ldots, p_n)\) tuples, which are particular [data] functions encoding unambiguously the values of \(p_1, \ldots, p_n\) and their type.
- \(\neq M'\) matches a bitstring equal to \(M'\).

When \(p\) is a variable, the else branch can be omitted (it cannot be executed).

- \(x[T]\) \(\leftarrow M; M'\) stores the result of \(M\) in \(x\) and returns the result of \(M'\). This is equivalent to the construct let \(x[T] = M\) in \(M'\). _ is allowed instead of \(x\), and in this case the value of \(x\) is simply ignored.
- if \(\text{cond}\) then \(M\) else \(M'\) is syntactic sugar for find suchthat \(\text{cond}\) then \(M\) else \(M'\). It returns the result of \(M\) if the condition \(\text{cond}\) evaluates to true and of \(M'\) if \(\text{cond}\) evaluates to false.
- find \(FB_1\) or find \(\ldots\) or find \(FB_m\) else \(M\) where \(FB_j = u_{j1} = i_{j1}, \ldots, u_{jm_j} = i_{jm_j}\) suchthat \(\text{cond}_j\) then \(M_j\) evaluates the conditions \(\text{cond}_j\) for each \(j\) and each value of \(i_{j1}, \ldots, i_{jm_j}\) in \([1, n_{j1}] \times \ldots \times [1, n_{jm_j}]\). If none of these conditions is true, it returns the result of \(M\). Otherwise, it chooses randomly with (almost) uniform probability one \(j\) and one value of \(i_{j1}, \ldots, i_{jm_j}\) such that the corresponding condition is true, stores it in \(u_{j1}, \ldots, u_{jm_j}\), and returns the result of \(M_j\). See the explanation of the find process below for more details.

- \(\text{event } e(M_1, \ldots, M_n); P\) executes the event \(e(M_1, \ldots, M_n)\), then executes \(P\). Events serve in recording the execution of certain parts of the program for using them in queries. The symbol \(e\) must have been declared by an event declaration.

- \(\text{event } \text{abort } e\) executes event \(e\) and aborts the game. It is intended to be used in the right-hand side of the definitions of some cryptographic primitives. (See also the equiv declaration: events in the right-hand side can be used when the simulation of left-hand side by the right-hand side fails. CryptoVerif is going to find a bound for the probability that the event is executed and include it in the probability of success of an attack.)

- \(\text{insert } tbl(M_1, \ldots, M_n); M\) inserts the tuples \((M_1, \ldots, M_n)\) in the table \(tbl\), then returns the result of \(M\). The table \(tbl\) must have been declared with the appropriate types using the table declaration.

- \(\text{get } tbl(p_1, \ldots, p_n)\) suchthat \(M\) in \(M'\) else \(M''\) tries to find an element of the table \(tbl\) that matches the patterns \(p_1, \ldots, p_n\) and such that \(M\) is true. If it succeeds, it returns the result of \(M'\) with the variables of \(p_1, \ldots, p_n\) bound to that element of the table. If several elements match, one of them is chosen randomly with (almost) uniform probability. If no element matches, it returns the result of \(M''\).

When suchthat \(M\) is omitted, it is equivalent to suchthat true.

A variant of get is get [unique], which guarantees that at most one element of the table satisfies the condition, except in cases of negligible probability.

Internally, get is converted into find by CryptoVerif.

- \(\text{diff } [M_1, M_2]\) allows the user to define two processes: in the first process, the first argument of diff is always used, while in the second process, the second argument of diff is always used. CryptoVerif shows indistinguishability between the obtained two processes.
The calculus distinguishes two kinds of processes: input processes (i-process) are ready to receive a message on a channel; output processes (o-process) output a message on a channel after executing some internal computations. When an input or output process is an identifier, it is substituted with its value defined by a let declaration. Processes allow parenthesizing for disambiguation.

Let us first describe input processes:

- **proc**\(M_1, \ldots, M_n\) is replaced with \(\text{let} \ x_1 = M_1 \text{ in } \ldots \text{let } x_n = M_n \text{ in } P\) when **proc** is declared by \(\text{let } \text{proc}(x_1 : T_1, \ldots, x_n : T_n) = P\), where \(P\) is an input process. The terms \(M_1, \ldots, M_n\) must contain only variables, replication indices, and function applications.

- **0** does nothing.

- \(Q ! Q'\) is the parallel composition of \(Q\) and \(Q'\).

- \(! : i \leftarrow N \ Q\) represents \(N\) copies of \(Q\) in parallel each with a different value of \(i \in [1, N]\). The identifier \(N\) must have been declared by \text{param} \(N\). The identifier \(i\) cannot be referred to explicitly in the process; it is used only implicitly as array index of variables defined under the replication \(! : i \leftarrow N\). The replication \(! : i \leftarrow N\) can be abbreviated \(! N\).

When a program point is under replications \(! : i \leftarrow N\), \(\ldots\), \(! : i_n \leftarrow N_n\), the current replication indices at that point are \(i_1, \ldots, i_n\).

- For each \(i \leftarrow N\) do \(Q\) is equivalent to \(! : i \leftarrow N \ Q\).

- The semantics of the input \(\text{in}((\text{channel}), (\text{pattern})); (\text{o-process})\) will be explained below together with the semantics of the output.

Note that the construct **newChannel** \(c:Q\) used in research papers is absent from the implementation: this construct is useful in the proof of soundness of CryptoVerif, but not essential for encoding games that CryptoVerif manipulates.

Let us now describe output processes:

- **proc**\(M_1, \ldots, M_n\) is replaced with \(\text{let } x_1 = M_1 \text{ in } \ldots \text{let } x_n = M_n \text{ in } P\) when **proc** is declared by \(\text{let } \text{proc}(x_1 : T_1, \ldots, x_n : T_n) = P\), where \(P\) is an output process.

- **yield** yields control to another process, by outputting an empty message on channel **yield**. It can be understood as an abbreviation for **out**(**yield**(),());0:

- **event** \(e(M_1, \ldots, M_n); P\) executes the event \(e(M_1, \ldots, M_n)\), then executes \(P\). Events serve in recording the execution of certain parts of the program for using them in queries. The symbol \(e\) must have been declared by an **event** declaration.

- **event**\_\_\_\_\_\_\_\_\_\_\_\_\_**event** \(e\) executes event \(e\) and terminates the game. (Nothing can be executed after this instruction, neither by the protocol nor by the adversary.) The symbol \(e\) must have been declared by an **event** declaration, without any argument.

- **new** \(x:T; P\) or \(x \leftarrow \text{R} \ T; P\) chooses a new random number in type \(T\), stores it in \(x\), and executes \(P\). \(T\) must be declared with option **fixed**, **bounded**, or **nonuniform**. Each such type \(T\) comes with an associated default probability distribution \(D_T\): the random number is chosen according to that distribution. The time for generated random numbers in that distribution is bounded by **time**(\(\text{new } T\)) or equivalently **time**(\(\leftarrow \text{R} \ T\)).

  - When the type \(T\) is **nonuniform**, the default probability distribution \(D_T\) for type \(T\) may be non-uniform. It is left unspecified. (Notice that random bitstrings with non-uniform distributions can also be obtained by applying a function to a random bitstring chosen uniformly among a finite set of bitstrings, chosen in another type.)

  - When the type \(T\) is **fixed**, it consists of the set of all bitstrings of a certain length \(n\). Probabilistic Turing machines can return uniformly distributed random numbers in such types, in bounded time. If \(T\) is not marked **nonuniform**, the default probability distribution \(D_T\) for \(T\) is the uniform distribution.
For other bounded types $T$, probabilistic bounded-time Turing machines can choose random numbers with a distribution as close as we wish to uniform, but may not be able to produce exactly a uniform distribution. If $T$ is not marked nonuniform, the default probability distribution $D_T$ is such that its distance to the uniform distribution is at most $\epsilon_{\text{rand}}(T)$. The distance between two probability distributions $D_1$ and $D_2$ for type $T$ is

$$d(D_1, D_2) = \sum_{a \in T} |\Pr[X_1 = a] - \Pr[X_2 = a]|$$

where $X_i$ ($i = 1, 2$) is a random variable of distribution $D_i$.

For example, a possible algorithm to obtain a random integer in $[0, m-1]$ is to choose a random integer $x'$ uniformly among $[0, 2^k - 1]$ for a certain $k$ large enough and return $x' \mod m$. By euclidean division, we have $2^k = qm + r$ with $r \in [0, m-1]$. With this algorithm

$$\Pr[x = a] = \begin{cases} \frac{q+1}{2^k} & \text{if } a \in [0, r-1] \\ \frac{1}{m} & \text{if } a \in [r, m-1] \end{cases}$$

so

$$|\Pr[x = a] - \frac{1}{m}| = \begin{cases} \frac{q+1}{2^k} - \frac{1}{m} & \text{if } a \in [0, r-1] \\ \frac{1}{m} - \frac{q}{2^k} & \text{if } a \in [r, m-1] \end{cases}$$

Therefore

$$d(D_T, \text{uniform}) = \sum_{a \in T} |\Pr[x = a] - \frac{1}{m}| = r \left( \frac{q+1}{2^k} - \frac{1}{m} \right) - (m-r) \left( \frac{1}{m} - \frac{q}{2^k} \right)$$

$$= 2r(m-r) \frac{m}{m.2^k} \leq \frac{m}{2^k}$$

so we can take $\epsilon_{\text{rand}}(T) = \frac{m}{2^k}$. A given precision of $\epsilon_{\text{rand}}(T) = \frac{1}{2^k}$ can be obtained by choosing $k = k' + \text{number of bits of } m \text{ random bits}$.

When IgnoreSmallTimes is set to a value greater than 0 (which is the default), the time for random number generations and the probability $\epsilon_{\text{rand}}(T)$ are ignored, to make probability formulas more readable.

- let $p = M$ in $P$ else $P'$ tries to decompose the term $M$ according to pattern $p$. In case of success, executes $P$, otherwise executes $P'$.

The pattern $p$ can be:

- $x[:T]$ variable, possibly with its type. Matches any bitstring (in type $T$), and stores it in $x$.
- $\_[:T]$ underscore, possibly with a type. Matches any bitstring (in type $T$), and ignores its value.
- $f(p_1, \ldots, p_n)$ where the function symbol $f$ is declared [data]. Matches bitstrings $M$ equal to $f(M_1, \ldots, M_n)$ for some $M_1, \ldots, M_n$ that match $p_1, \ldots, p_n$. (The poly-injectivity of $f$ allows us to compute possible values $M_1, \ldots, M_n$ of its arguments from the value of $M$, and to check whether $M$ is equal to the resulting value of $f(M_1, \ldots, M_n)$.)
- $(p_1, \ldots, p_n)$ tuples, which are particular [data] functions encoding unambiguously the values of $p_1, \ldots, p_n$ and their type.
- $=M'$ matches a bitstring equal to $M'$.

The else clause is never executed when the pattern is simply a variable. When else $P'$ is omitted, it is equivalent to else yield. Similarly, when in $P$ is omitted, it is equivalent to in yield.

- $= M; P$ stores the result of term $M$ in $x$ and executes $P$. $M$ must be of type $T$ when $T$ is mentioned. This is equivalent to the construct let $x[:T] = M$ in $P$. _ is allowed instead of $x$, and in this case the value of $M$ is simply ignored.
• if cond then P else P' is syntactic sugar for find such that cond then P else P'. It executes P if the condition cond evaluates to true and P' if cond evaluates to false. When the else clause is omitted, it is implicitly else yield. (else 0 would not be syntactically correct.)

• Next, we explain the process find FB1 or find ... or find FBm else P where each branch FBj is FBj = uj1 = i1j, . . . , ujm = jmj such that defined(M1, . . . , Mj) & & Mj then Pj.

A simple example is the following: find u = i <= u such that defined(x[i]) & & x[i] = a then P'
else P tries to find an index i such that x[i] is defined and x[i] = a, and when such an i is found, it stores that i in u and executes P'; otherwise, it executes P. In other words, this find construct looks for the value a in the array x, and when a is found, it stores in u an index such that x[u] = a.

Therefore, the find construct allows us to access arrays, which is key for our purpose.

More generally, find u1 = i1 <= u1, . . . , um = im such that defined(M1, . . . , M) & & M then P' else P tries to find values of i, . . . , im for which M1, . . . , M are defined and M is true. In case of success, it stores the values of i, . . . , im in u1, . . . , um executes P'. In case of failure, it executes P.

This is further generalized to m branches: find FB1 or find ... or find FBm else P where FBj = uj1 = i1j, . . . , ujm = jmj such that defined(M1, . . . , Mj) & & Mj then Pj tries to find a branch j in [1, m] such that there are values of i1j, . . . , jmj for which M1, . . . , Mj are defined and Mj is true. In case of success, it stores the value of i1j, . . . , jmj in u1j, . . . , umj and executes Pj. In case of failure for all branches, it executes P. More formally, it evaluates the conditions condj = defined(M1, . . . , Mj) & & Mj for each j and each value of i1j, . . . , jmj in [1, nj1] × . . . × [1, njm]. If none of these conditions is true, it executes P. Otherwise, it chooses randomly with almost uniform probability one j and one value of i1j, . . . , jmj such that the corresponding condition is true, stores that value in u1j, . . . , umj and executes Pj.

In the general case, the conditions condj are of the form defined(M1, . . . , M) & & M or simply M. The condition defined(M1, . . . , M) means that M1, . . . , M are defined. At least one of the two conditions defined or M must be present. Omitted defined conditions are considered empty; when M is omitted, it is considered true.

The variables i1j, . . . , jmj, are considered as replication indices, and are used in the defined condition and in Mj; they are temporary variables that are used as loop indices to look for indices that satisfy the desired conditions. Once suitable indices are found, their value is stored in u1j, . . . , umj, and the then branch is executed using these variables. It is possible to make array accesses to u1j, . . . , umj (such as u1j[M1, . . . , Mk]) elsewhere in the game, which is not possible for i1j, . . . , jmj.

As an abbreviation, one may write FBj = uj1 = i1j, . . . , umj = jmj such that defined(M1, . . . , Mj) & & Mj then Pj. In this case, the same identifier ujk is used for both the variable and the associated replication index ijk.

A variant of find is find[unique]. Consider the process find[unique] FB1 or find ... or find FBm else P where FB1 = uj1 = i1j, . . . , umj = jmj such that defined(M1, . . . , Mj) & & Mj then Pj. When there are several values of j, i1j, . . . , jmj, for which M1, . . . , Mj are defined and Mj is true, this process executes an event NonUnique and aborts the game. In all other cases, it behaves as find. Intuitively, find[unique] should be used when there is a negligible probability of finding several suitable values of j, i1j, . . . , jmj. The construct find[unique] is typically not used in the initial game. (One would have to prove manually that there is indeed a negligible probability of finding several suitable values of j, i1j, . . . , jmj. CryptoVerif displays a warning if find[unique] occurs in the initial game.) However, find[unique] is used in the specification of cryptographic primitives, in the right-hand of equivalences specified by equiv.

• insert tbl(M1, . . . , M) ; P inserts the tuples (M1, . . . , M) in the table tbl, then executes P. The table tbl must have been declared with the appropriate types using the table declaration.

1 Precisely, the distance between the distribution actually used for choosing j, i1j, . . . , jmj, and the uniform distribution is at most eps, find/2. See the explanation of new x : T for details on how to achieve this.
• get tbl(p₁, . . . , pₙ) such that M in P else P′ tries to find an element of the table tbl that matches the patterns p₁, . . . , pₙ and such that M is true. If it succeeds, it executes P with the variables of p₁, . . . , pₙ bound to that element of the table. If several elements match, one of them is chosen randomly with (almost) uniform probability. If no element matches, it executes P′.

When else P′ is omitted, it is equivalent to else yield. When suchthat M is omitted, it is equivalent to suchthat true.

A variant of get is get[unique], which guarantees that at most one element of the table satisfies the condition, except in cases of negligible probability.

Internally, get is converted into find by CryptoVerif.

• Let us now explain the output out(c[M₁, . . . , Mₙ], N); Q. A channel c[M₁, . . . , Mₙ] consists of both a channel name c (declared by channel c) and a tuple of terms M₁, . . . , Mₙ. Terms M₁, . . . , Mₙ are intuitively analogous to IP addresses and ports which are numbers that the adversary may guess. Two channels are equal when they have the same channel name and terms that evaluate to the same bitstrings. A semantic configuration always consists of a single output process (the process currently being executed) and several input processes. When the output process executes out(c[M₁, . . . , Mₙ], N); Q, one looks for an input on the same channel in the available input processes. If no such input process is found, the process blocks. Otherwise, one such input process in(c[M₁, . . . , Mₙ], p); P is chosen randomly with (almost) uniform probability. The communication is then executed: the output message N is evaluated, its result is truncated to the maximum length of bitstrings on channel c, the obtained bitstring is matched against pattern p. Finally, the output process P that follows the input is executed. The input process Q that follows the output is stored in the available input processes for future execution.

Patterns p are as in the 1st process, except that variables in p that are not under a function symbol f(...) must be declared with their type.

In the game as given to CryptoVerif, the channel can be either c[i₁, . . . , iₙ] where i₁, . . . , iₙ are the current replication indices at the considered input or output, or just a channel name c, as an abbreviation for c[i₁, . . . , iₙ]. It is recommended to use as channel a different channel name for each input and output. Then the adversary has full control over the network: it can decide precisely from which copy of which input it receives a message and to which copy of which output it sends a message, by using the appropriate channel name and value of the replication indices.

Note that the syntax requires an output to be followed by an input process, as in [S]. If one needs to output several messages consecutively, one can simply insert fictitious inputs between the outputs. The adversary can then schedule the outputs by sending messages to these inputs.

• diff[P₁, P₂] allows the user to define two processes: in the first process, the first argument of diff is always used, while in the second process, the second argument of diff is always used. CryptoVerif shows indistinguishability between the obtained two processes. Internally, this is encoded by choosing a random bit diff_bit, running the first argument of diff when diff_bit is true and the second one when when diff_bit is false, and showing the secrecy of diff_bit. The variables that are public due to other queries (variables included in public_vars in queries as well as variables on which there is a query secret) are considered public when proving the secrecy of diff_bit.

In this calculus, all variables are implicitly arrays. When a variable x is defined (by new, <-R, <-, let, find, in) under replications !i₁ ≜ N₁, . . . , !iₙ ≜ Nₙ, x has implicitly indices i₁, . . . , iₙ: x stands for x[i₁, . . . , iₙ]. Arrays allow us to have full access to the state of the process. Arrays can be read using find. Similarly, when x is used with k < n indices the missing n − k indices are implicit: x[i₁, . . . , uₖ] stands for x[i₁, . . . , iₙ−k, u₁, . . . , uₖ] where i₁, . . . , iₙ−k must be the n − k first replication indices both at the creation of x and at the usage x[u₁, . . . , uₖ]. (So the usage and creation of x must be under the same n − k top-most replications.)

In the initial game, several variables may be defined with the same name, but they are immediately renamed to different names, so that after renaming, each variable is defined once. When several variables are defined with the same name, they can be referenced only under their definition without explicit array indices, because for other references, we would not know which variable to reference after renaming.
In subsequent games created by CryptoVerif, a variable may be defined at several occurrences, but these occurrences must be in different branches of \texttt{if}, \texttt{find}, or \texttt{let}, so that they cannot be executed with the same value of the array indices. This constraint guarantees that each array cell is defined at most once.

Each usage of $x$ must be either:

- $x$ without array index syntactically under its definition. (Then $x$ is implicitly considered to have as indices the current replication indices at its definition.)

- $x$ possibly with array indices inside the \texttt{defined} condition of a \texttt{find}.

- $x[M_1, \ldots, M_n]$ in $M$ in a \texttt{find} branch ... such that \texttt{defined}(M'_1, \ldots, M'_j) \&\& M$ then ..., such that $x[M_1, \ldots, M_n]$ is a subterm of $M'_1, \ldots, M'_j$.

- $x[M_1, \ldots, M_n]$ in $P$ in a \texttt{find} branch $u_1 = i_1 \leftarrow n_1, \ldots, u_m = i_m \leftarrow n_m$ such that \texttt{defined}(M'_1, \ldots, M'_j) \&\& \ldots \&\& then $P$, such that $x[M_1, \ldots, M_n] = M[u_1/i_1, \ldots, u_m/i_m]$ and $M$ is a subterm of $M'_1, \ldots, M'_j$.

- $x[M_1, \ldots, M_n]$ in $M''$ in a \texttt{find} branch $u_1 = i_1 \leftarrow n_1, \ldots, u_m = i_m \leftarrow n_m$ such that \texttt{defined}(M'_1, \ldots, M'_j) \&\& \ldots \&\& then $M''$, such that $x[M_1, \ldots, M_n] = M[u_1/i_1, \ldots, u_m/i_m]$ and $M$ is a subterm of $M'_1, \ldots, M'_j$.

These syntactic constraints guarantee that a variable is accessed only when it is defined. Moreover, the variables defined in conditions of \texttt{find} or in patterns or conditions of \texttt{get} must not have array accesses (that is, accesses corresponding to the last four cases above).

Finally, the calculus is equipped with a type system. To be able to use variables outside their scope (by \texttt{find}), the type checking algorithm works in two passes.

In the first pass, it collects the type of each variable: when a variable $x$ is defined with type $T$ under replications $!N_1, \ldots, !N_n$, $x$ has type $[1, N_1] \times \ldots \times [1, N_n] \rightarrow T$. When the type of $x$ is not explicitly given in its declaration (in $\leftarrow$ or in patterns in \texttt{let} or \texttt{in}), its type is left undefined in this pass, and $x$ cannot be used outside its scope.

In the second pass, the type system checks the following requirements: In $x[M_1, \ldots, M_n]$, $M_1, \ldots, M_m$ must be of the suitable interval type, that is, a suffix of the types of replication indices at the definition of $x$. In $f(M_1, \ldots, M_m)$, if $f$ has been declared by \texttt{fun} $f(T_1, \ldots, T_m) : T$, $M_j$ must be of type $T_j$, and $f(M_1, \ldots, M_m)$ is then of type $T$. In $(M_1, \ldots, M_m)$, $M_j$ can be of any bitstring type (that is, not an index type $[1, N]$), and the result is of type bitstring. In $M_1 = M_2$ and $M_1 \leftarrow M_2$, $M_1$ and $M_2$ must be of the same type, and the result is of type bool. In $M_1 | M_2$ and $M_1 \&\& M_2$, $M_1$ and $M_2$ must be of type bool and the result is of type bool. The type system requires each subterm to be well-typed. Furthermore, in \texttt{event} $e(M_1, \ldots, M_n)$, if $e$ has been declared by \texttt{event} $e(T_1, \ldots, T_n)$, $M_j$ must be of type $T_j$. In \texttt{new} $x : T$ or $x \leftarrow \mathbb{R}$, $T$ must be declared with option \texttt{bounded} (or \texttt{fixed}). In \texttt{if} $M$ then ... else ..., $M$ must be of type bool. Similarly, for

\begin{verbatim}
find ... or \texttt{find} ... such that \texttt{defined}(...) \&\& M then ...
\end{verbatim}

$M$ must be of type bool. In \texttt{let} $p = M$ in ..., $M$ and $p$ must be of the same type. For function application and tuple patterns, the typing rule is the same as for the corresponding terms. The pattern $x : T$ is of type $T$; the pattern $x$ can be of any bitstring type, determined by the usage of $x$ (when the pattern $x$ is used as argument of a tuple pattern, its type is \texttt{bitstring}); the pattern $=M$ is of the type of $M$. In \texttt{out} $(e[M_1, \ldots, M_n], M)$, $M$ must be of a bitstring type.

A declaration can be:

- \texttt{set} \{parameter\} = \{value\}.

This declaration sets the value of configuration parameters. The following parameters and values are supported:

- \texttt{set allowUndefinedVar} = \texttt{false}.
- \texttt{set allowUndefinedVar} = \texttt{true}.

By default (allowUndefinedVar = false), variables in defined conditions must be defined somewhere in the game. The setting allowUndefinedVar = true allows defined conditions with variables that are defined nowhere. The corresponding branch of find is then removed immediately, since the defined condition does not hold. This setting is useful to parse intermediate games generated by CryptoVerif, because such impossible defined conditions may occur in these games.

- set diffConstants = true.
  set diffConstants = false.
  When true, different constant symbols are assumed to have a different value. When false, CryptoVerif does not make this assumption.

- set constantsNotTuple = true.
  set constantsNotTuple = false.
  When true, constant symbols are assumed to be different from the result of applying a tuple function to any argument. When false, CryptoVerif does not make this assumption.

- set expandAssignXY = true.
  set expandAssignXY = false.
  When true, CryptoVerif automatically removes assignments let x = y or x <- y where x and y are variables by substituting y for x (in the transformation remove_assign_useless) When false, this transformation is not performed as part of remove_assign_useless.

- set minimalSimplifications = true.
  set minimalSimplifications = false.
  When true, simplification replaces a term with a rewritten term only when the rewriting has used at least one rewriting rule given by the user, not when only equalities that come from let definitions and other instructions in the game have been used. When false, a term is replaced with its rewritten form in all cases. The latter configuration often leads to replacing a term with a more complex one, in particular expanding let definitions, thus duplicating their contents.

- set autoMergeBranches = true.
  set autoMergeBranches = false.
  When true, the transformation merge_branches is applied after simplification, to merge branches of if, let, and find when all branches execute the same code. This is useful in order to remove the test, which can remove a use of a secret. When false, this transformation is not performed. This is useful in particular when the test has been manually introduced in order to force CryptoVerif to distinguish cases.

- set autoMergeArrays = true.
  set autoMergeArrays = false.
  When true, merge_branches advises merge_arrays commands to make the merging of branches of if, find, let succeed more often. When false, this advice is not automatically given and the user should use the manual command merge_arrays (defined in Section 7) to perform the merging.

- set uniqueBranch = true.
  set uniqueBranch = false.
  When uniqueBranch = true, the following transformation is enabled as part of simplify: if a branch of a find[unique] is proved to succeed, then simplification removes all other branches of that find. When uniqueBranch = false, this transformation is not performed.

- set uniqueBranchReorganize = true.
  set uniqueBranchReorganize = false.
  When uniqueBranchReorganize = true, the following transformations are enabled as part of simplify:
  * If a find[unique] occurs in the then branch of a find[unique], we reorganize them.
  * If a find[unique] occurs in the condition of a find, we reorganize them.
When uniqueBranchReorganize = false, these transformations are not performed.

- set inferUnique = false.
  set inferUnique = true.
  When inferUnique = true, CryptoVerif tries to infer that a find that is not explicitly tagged \[unique\] is in fact unique, by showing that having several solutions for this find leads to a contradiction. When this proof succeeds, the find becomes find[unique].
  When inferUnique = false, CryptoVerif does not try to make such proofs and just exploits explicit \[unique\] tags.

- set guessRemoveUnique = false.
  set guessRemoveUnique = true.
  When we use a guess transformation (guess or guess_branch) and a (one-session) secrecy query is present, we must reprove that all find[unique] in the game are really unique. When guessRemoveUnique = false (the default), we reprove them. When guessRemoveUnique = true, we instead remove the \[unique\] annotations to avoid having to reprove them.

- set autoSARename = true.
  set autoSARename = false.
  When true, and a variable is defined several times and used only in the scope of its definition with the current replication indices at that definition, each definition of this variable is renamed to a different name, and the uses are renamed accordingly, by the transformation all_simplify and by the simplification after the crypto and SARename transformations.
  When false, such a renaming is not done automatically, but in manual proofs, it can be requested specifically for each variable by SARename x, where x is the name of the variable.

- set autoRemoveAssignFindCond = true.
  set autoRemoveAssignFindCond = false.
  When true, the default removal of assignments performed by CryptoVerif removes assignments on variables x defined by let x = M in ... inside a condition of find. When false, the removal of this assignments is not performed automatically, but in manual proofs, it can be requested by the command remove_assign findcond.

- set autoRemoveIfFindCond = true.
  set autoRemoveIfFindCond = false.
  When true, simplification removes if in defined conditions of find by transforming them into logical formulae. When false, this removal is not performed.

- set autoMove = true.
  set autoMove = false.
  When true, the transformation move all is automatically executed after each cryptographic transformation. This transformation moves random number generations (new or \(<\)-R) downwards as much as possible, duplicating them when crossing a if, let, or find. (A future SARename transformation may then enable us to distinguish cases depending on which of the duplicated random number generations a variable comes from.) It also moves assignments down in the syntax tree but without duplicating them, when the assignment can be moved under a if, let, or find, in which the assigned variable is used only in one branch. (In this case, the assigned term is computed in fewer cases thanks to this transformation.)
  When false, the transformation move all is never automatically executed.

- set autoExpand = true.
  set autoExpand = false.
  When true, the transformation expand is automatically executed after transformations that result in a game containing if, let, find, event, event_abort, or new terms. The transformation expand expands these terms into processes. That leads to distinguishing the branches until the end of the process, which may help the proof by distinguishing more cases, but may lead to very large games. This is also needed because some game transformations of CryptoVerif do not support non-expanded games (global_dep_anal, insert, merge_arrays, merge_branches, move; furthermore, simplify is weaker when it is applied to a non-expanded
game, and success fails to prove equivalence queries in non-expanded games and correspondence queries when the arguments of the considered events contain if, let, find, event, event_abort, or new.

When false, the transformation expand is never automatically executed.

- set interactiveMode = false.
  set interactiveMode = true.

When false, CryptoVerif runs automatically. When true, CryptoVerif waits for instructions of the user on how to perform the proof. (See Section 7 for details on these instructions.) This setting is ignored when proof instructions are included in the input file using the proof command. In this case, the instructions given in the proof command are executed, without user interaction.

- set autoAdvice = true.
  set autoAdvice = false.

In interactive mode, when autoAdvice = true, execute the advised transformations automatically. When autoAdvice = false, display the advised transformations, but do not execute them. The user may then give them as instructions if he wishes.

- set noAdviceCrypto = false.
  set noAdviceCrypto = true.

When noAdviceCrypto = true, prevents the cryptographic transformations from generating advice. Useful mainly for debugging the proof strategy.

- set noAdviceGlobalDepAnal = false.
  set noAdviceGlobalDepAnal = true.

When noAdviceGlobalDepAnal = true, prevents the global dependency analysis from generating advice. Useful when the global dependency analysis generates bad advice.

- set simplifyAfterSARename = true.
  set simplifyAfterSARename = false.

When simplifyAfterSARename = true, apply simplification (remove_assign useless if autoRemoveAssignUseless = false, remove_assign findcond if autoRemoveAssignFindCond = true, SARename new if autoSARename = true, simplify) after each execution of the SARename transformation. This slows down the system, but enables it to succeed more often.

- set backtrackOnCrypto = false.
  set backtrackOnCrypto = true.

When backtrackOnCrypto = true, use backtracking when the proof fails, to try other cryptographic transformations. This slows down the system considerably (so it is false by default), but enables it to succeed more often, in particular for public-key protocols that mix several primitives. One usage is to try first with the default setting and, if the proof fails although the property is believed to hold, try again with backtracking.

- set useKnownEqualitiesInCryptoTransform = true.
  set useKnownEqualitiesInCryptoTransform = false.

When useKnownEqualitiesInCryptoTransform = true, CryptoVerif relies on known equalities between terms to replace variables with their values in the cryptographic transformations. When it is false, CryptoVerif just uses the variables as they appear in the game, and relies only on advice to replace variables with their values.

- set priorityEventUnchangedRand = n. (default: 5)

During the cryptographic transformation, variables that occur in event and are mapped to random variables marked [unchanged] in the equivalence can be left unchanged. Sometimes, it is also possible to transform the term that contains them using one of the oracles of the equivalence.

This setting determines which option is chosen: CryptoVerif prefers leaving the variable unchanged rather than using an oracle with priority at least n. It prefers using an oracle with priority less than n rather than leaving the variable unchanged.
- set casesInCorresp = true.
  set casesInCorresp = false.

  When casesInCorresp = true, CryptoVerif distinguishes cases depending on the definition point of variables, to infer more facts in order to prove correspondence properties. However, this can be slow in complex cases. Using set casesInCorresp = false disables this case distinction and speeds up the proof of correspondences.

- set elsefindFactsInReplace = true.
  set elsefindFactsInReplace = false.

  When elsefindFactsInReplace = true, CryptoVerif will try to infer more facts when doing a replace operation: when it encounters a find in the process, it considers a variable $x[M_1, \ldots, M_l]$, which is guaranteed to be defined by this find. If $x$ is defined in the else part of another find construct, then at the definition of $x$, we know that the conditions of the then branches of this find are not satisfied:

  $$\forall u_1, \ldots, u_k. \neg \text{defined}(y_1[M_1, \ldots, M_{l_1}], \ldots, y_k[M_{k_1}, \ldots, M_{k_1}]) \land t$$

  We try to infer not($t$) from this fact.

  $\ast$ if each variable $y_j[M_{j_1}, \ldots, M_{j_l}]$ is defined before $x[M_1, \ldots, M_l]$, then not($t$) indeed holds by the fact above;

  $\ast$ for each $y_j[M_{j_1}, \ldots, M_{j_l}]$, we assume that $y_j[M_{j_1}, \ldots, M_{j_l}]$ is defined after or at the same time as $x[M_1, \ldots, M_l]$ and try to prove not($t$).

  If this proof succeeds, we can infer that not($t$) holds at the current program point.

- set elsefindFactsInSimplify = true.
  set elsefindFactsInSimplify = false.

  Similar to elsefindFactsInReplace, but applies in simplify operations.

- set elsefindFactsInSuccess = true.
  set elsefindFactsInSuccess = false.

  Similar to elsefindFactsInReplace, but applies in success operations.

- set elsefindFactsInSuccessSimplify = true.
  set elsefindFactsInSuccessSimplify = false.

  Similar to elsefindFactsInReplace, but applies in the elimination of useless code in success simplify operations.

- set elsefindAdditionalDisjunct = true.
  set elsefindAdditionalDisjunct = false.

  When elsefindAdditionalDisjunct = true, the procedure that infers facts from false conditions of find (see set elsefindFactsInReplace) is enriched: in case $y_j[M_{j_1}, \ldots, M_{j_l}]$ may be defined at the same time as $x[M_1, \ldots, M_l]$, we additionally assume that they have different indices, that is, $(M_{j_1}, \ldots, M_{j_l}) \neq (M_1, \ldots, M_l)$ to eliminate this case. Therefore, we infer $(M_{j_1}, \ldots, M_{j_l}) \neq (M_1, \ldots, M_l) \Rightarrow \neg t(t)$ or equivalently $(M_{j_1}, \ldots, M_{j_l}) = (M_1, \ldots, M_l) \Rightarrow \neg t(t)$. This is typically more costly and more precise than the basic procedure that just infers not($t$) when possible.

- set improvedFactCollection = false.
  set improvedFactCollection = true.

  When improvedFactCollection = true, and CryptoVerif collects the facts that hold at each program point, it also takes into account variables that cannot be defined at a certain program point, variables that cannot be simultaneously defined, and elsefind facts, in order to prove more facts.

  It is a bit costly, so it is disabled by default (improvedFactCollection = false).

- set useEqualitiesInSimplifyingFacts = false.
  set useEqualitiesInSimplifyingFacts = true.

  When useEqualitiesInSimplifyingFacts = true, CryptoVerif uses known equalities between terms to determine whether a fact is equal to another fact.

  It is a bit costly, so it is disabled by default (useEqualitiesInSimplifyingFacts = false).
- set useKnownEqualitiesWithFunctionsInMatching = false.
  set useKnownEqualitiesWithFunctionsInMatching = true.
  When useKnownEqualitiesWithFunctionsInMatching = true, CryptoVerif uses known equalities $M_1 = M_2$ where the root of $M_1$ is a function application to normalize terms before testing whether they match an equation or collision statement or an oracle in a cryptographic transformation. That can allow to apply these statements or transformations more often. It is a bit costly, so it is disabled by default (useKnownEqualitiesWithFunctionsInMatching = false).

- set ignoreSmallTimes = $\langle n \rangle$. (default 3)
  When 0, the evaluation of the runtime is very precise, but the formulas are often too complicated to read.
  When 1, the system ignores many small values when computing the runtime of the games. It considers only function applications and pattern matching.
  When 2, the system ignores even more details, including application of boolean operations ($\&$, $\|$, not), constants generated by the system, () and matching on (). It ignores the creation and decomposition of tuples in inputs and outputs.
  When 3, the system additionally ignores the time of equality tests between values of bounded length, as well as the time of all constants.

- set maxIterSimplif = $\langle n \rangle$. (default 2)
  Sets the maximum number of repetitions of the simplification transformation for each simplify instruction. A greater value slows down the system but may enable it to obtain simpler games, and therefore increase its chances of success. When $n \leq 0$, repeats simplification until a fixpoint is reached.

- set maxAddFactDepth = $\langle n \rangle$. (default 1000)
  Sets the maximum depth of recursion in the addition and simplification of known facts. When $n \leq 0$, puts no limit on this depth of recursion. Putting a limit avoids an infinite loop in some rare cases.

- set maxTryNoVarDepth = $\langle n \rangle$. (default 20)
  Sets the maximum depth of recursion in the replacement of variables with their values. When $n \leq 0$, puts no limit on this depth of recursion. Putting a limit avoids an infinite loop in some rare cases.

- set maxReplaceDepth = $n$. (default 20)
  Sets the maximum number of rewriting steps that are allowed to prove that the new term is equal to the old one in a replace transformation.

- set maxIterRemoveUselessAssign = $\langle n \rangle$. (default 10)
  Sets the maximum number of repetitions of the removal of useless assignments for each remove_assign useless instruction. A greater value slows down the system but may enable it to obtain simpler games, and therefore increase its chances of success. When $n \leq 0$, repeats removal of useless assignments until a fixpoint is reached.

- set maxAdvicePossibilitiesBeginning = $n_1$. (default 50)
  set maxAdvicePossibilitiesEnd = $n_2$. (default 10)
  In cryptographic transformations, when CryptoVerif can transform many terms in several ways of different priority, these various ways combine, yielding a very large number of advice possibilities. These two options allow to limit the number of considered advice possibilities by keeping the $n_1$ first possibilities (with highest priority) and the $n_2$ last possibilities (with lowest priority but fewer advised transformations). When $n_1$ or $n_2$ are not positive, all advice possibilities are kept, but that may yield a very slow execution.

- set maxElsefind = $n$. (default 50)
  Maximum of facts guaranteed in else branches of find collected from a single term.
- set minAutoCollElim = (s). (default pest80)

  Sets the maximum probability for which elimination of collisions is possible automatically
  (which corresponds to a minimum cardinal for the type, when the probability distribution is
  uniform). The argument (s) can be large (probability $2^{-160}$), password (probability $2^{-20}$),
  or pestn (probability $2^{-n}$; see also the type declaration).

- set maxGuess = (s). (default size40)

  Sets the maximum size for which we can guess the value of a certain type. The argument (s) can
  be default or passive (size $2^{30}$), small (size $2^2$), or sizeen (size $2^n$).

- set forgetOldGames = false.

  When forgetOldGames = true, old games are removed from memory after each crypto-
  graphic transformation or each interactive command. That allows to save some memory,
  but prevents undo. The display of the games is saved into a temporary file to allow displaying
  the games at the end of the proof.

The default value is the first mentioned, except when explicitly specified. In most cases, the default
values should be left as they are, except for interactiveMode, which allows to perform interactive
proofs.

- param \textbf{seq}[^{+}] (ident) \{[noninteractive] | [passive] | [default] | [small] | [size]\}.

  \textbf{param} $n_1, \ldots, n_m$, declares parameters $n_1, \ldots, n_m$. Parameters are used to represent the number of
  copies of replicated processes (that is, the maximum number of calls to each query). In asymptotic
  analyses, they are polynomial in the security parameter. In exact security analyses, they appear in
  the formulas that express the probability of an attack.

  The options [noninteractive], [passive], [default], [small], or [size] indicate to CryptoVerif an order of magnitude of the parameter. The option [size] (where $n$ is a constant integer)
  indicates the parameter is at most $2^n$. CryptoVerif uses this information to optimize the computed
  probability bounds: when several bounds are correct, it chooses the smallest one. It also uses it to
  estimate the probability of collisions, and decide whether to eliminate the collision or not.

  The option [noninteractive] means that the queries bounded by the considered parameters can be
  made by the adversary without interacting with the tested protocol, so the number of such
  queries is likely to be large. Parameters with option [noninteractive] are typically used for
  bounding the number of calls to random oracles. [noninteractive] is equivalent to [size80].

  The absence of option, the option [default], and the option [passive] correspond to adversary
  interacting with the tested protocol without any limitation on the number of sessions. This can
  correspond to two situations:

  - The protocol can start new sessions without limit even if it could detect that an active attack
    happened in previous sessions.

  - The adversary listens passively to sessions of the protocol that run as expected (hence the word [passive]). Therefore, for such runs, the adversary is undetected.

  No option, [default], and [passive] are equivalent to [size30].

  The option [small] should be used for sessions in which the adversary actively interacts with the
  honest participants and mounts detectable attacks, when these participants stop after a certain
  number of failed attempts (e.g. credit cards are blocked after 3 incorrect PINs). [small] is
  equivalent to [size2].

- proba \{ident\} [(\textbf{seq}(\textbf{dim}))] \{[\textbf{est}]\}.

  \textbf{proba} $p(d_1, \ldots, d_n)$, declares a probability function $p$ taking $n$ arguments of dimensions $d_1, \ldots, d_n$
  respectively. The syntax of dimensions is given in Figure 1 where *, /, and ^ are the usual product,
  division, and exponentiation. After reduction, dimensions are of the form time$^t \times$ length$^l$, where
  $t$ and $l$ are integers. The dimension number corresponds to time$^0 \times$ length$^0$. 

20
proba \( p \), declares a probability function \( p \) taking any arguments. In this case, CryptoVerif checks that the number and dimensions of the arguments of \( p \) are compatible across calls to \( p \).

When \([\langle \text{pest} \rangle]\) (probability estimate) is present, it gives an estimate of the value of the probability: \( \text{pest} n \), where \( n \) is an integer, means that the probability is at most \( 2^{-n} \); \text{password} is equivalent to \( \text{pest} 20 \), i.e. probability at most \( 2^{-20} \); \text{large} is equivalent to \( \text{pest} 160 \), i.e. probability at most \( 2^{-160} \). When \([\langle \text{pest} \rangle]\) is absent, large is the default. When the probability \( p \) appears in a collision statement and the command allowed_collisions \( \text{pest} n \) has been issued, CryptoVerif applies the collision statement only when the probability of collision (taking into account how many times it is applied) is less than \( 2^{-n} \). The estimate is only used to decide whether to eliminate collisions or not. The probability formula output by CryptoVerif at the end of the proof remains correct even if the estimates are incorrect. However, incorrect estimates may have the consequence that, when evaluating this probability, its value is larger than desired.

- **letproba** \((\text{ident})\)[\(\langle\text{seq} \ldots (\text{vardim})\rangle\)] = \((\text{proba})\).

- **letproba** \( p(x_1 : d_1, \ldots, x_n : d_n) = \text{proba} \), declares a probability function \( p \) with \( n \) arguments \( x_i \) of dimension \( d_i \), equal to the probability formula \( \text{proba} \). See proba above for an explanation of dimensions. The formula \( \text{proba} \) must represent a probability. It may refer to \( x_1, \ldots, x_n \). It is instantiated with the appropriate values of \( x_1, \ldots, x_n \) every time the probability function \( p \) is applied.

- **type** \((\text{ident})\)[\(\langle\text{seq} \ldots (\text{option})\rangle\)],

  declares a type \( T \). Types correspond to sets of bitstrings or a special symbol \( \bot \) (used for failed decryptions, for instance). Optionally, the declaration of a type may be followed by options between brackets. These options can be:
  
  - **bounded** means that the type is a set of bitstrings of bounded length or perhaps \( \bot \). In other words, the type is a finite subset of bitstrings plus \( \bot \).
  
  - **fixed** means that the type is the set of all bitstrings of a certain length \( n \). In particular, the type is a finite set, so **fixed** implies **bounded**.
  
  - **nonuniform** means that random numbers may be chosen in the type with a non-uniform distribution. (When **nonuniform** is absent, random numbers are chosen using a uniform distribution for **fixed** types, an almost uniform distribution for bounded types, and random values cannot be chosen among other types. Note that **fixed**, **nonuniform** and **bounded**, **nonuniform** are also allowed to have a non-uniform distribution on a **fixed** or **bounded** type.)
  
  - **sizen** indicates the order of magnitude of the cardinal of the type: **sizen** means that its cardinal is \(|T| = 2^n\), where \( n \) is an integer (like the set of bitstrings of length \( n \)).
  
  - **sizemin, max** means that \( 2^\text{min} \leq |T| \leq 2^\text{max} \), where \( \text{min} \) and \( \text{max} \) are integers.
  
  - **pcolln** (probability of collision) means that \( \text{PcollRand}(T) \leq 2^{-n} \), where \( n \) is an integer. \( \text{PcollRand}(T) \) is the probability of collision between a random element chosen according to the default probability distribution \( D_T \) for the considered type \( T \), and an independent element of type \( T \).

When the default distribution is uniform or almost uniform (fixed and bounded types), \( \text{PcollRand}(T) = \frac{1}{|T|} \), so CryptoVerif estimates the probability of collision from the cardinal of the type and conversely, so mentioning one of **sizen** or **pcolln** is sufficient.

CryptoVerif uses this information to determine whether collisions with random elements of the considered type \( T \) should be eliminated. For collisions to be eliminated, two conditions must be satisfied:

1. \( \text{PcollRand}(T) \leq 2^{-n'} \), that is, \( T \) has option **pcolln** with \( n \geq n' \), where \( n' \) is set by \( \text{set} \ \text{minAutoCollElim} = \text{pest} n' \) (the default is \( n' = 80 \)), or elimination of collisions on this data has been manually requested by the command \( \text{simp}lify \ \text{coll_elim}() \ldots \) or \( \text{global_dep} \ \text{x coll_elim}() \ldots \).

2. The probability of collision satisfies the conditions specified by the command allowed_collisions (used inside a proof environment). By default, collisions are eliminated when
* either \( \text{Pcoll1rand}(T) \leq 2^{-160} \) (\( T \) has option `pcolln` with \( n \geq 160 \) or option `large`)
* or \( \text{Pcoll1rand}(T) \leq 2^{-20} \) (\( T \) has option `pcolln` with \( n \geq 20 \) or option `password`), the collision is repeated at most \( N \) times, and \( N \) is a parameter of size at most 2.

See the command `allow_collisions` for more details.

- `large` is equivalent to `size160_10000000000`. `pcoll160`, that is, \( |T| \geq 2^{160} \) and \( \text{Pcoll1rand}(T) \leq 2^{-160} \). By default, `large` means that the type \( T \) is large enough so that all collisions with random elements of \( T \) can be eliminated. (In asymptotic analyses, \( \text{Pcoll1rand}(T) \) is negligible. In exact security analyses, the probability of a collision is correctly expressed by the system.)
- `password` is equivalent to `size20_40`. `pcoll20`, that is, \( 2^{20} \leq |T| \leq 2^{40} \) and \( \text{Pcoll1rand}(T) \leq 2^{-20} \). `password` is intended for passwords in password-based security protocols. These passwords are taken in a dictionary whose size is much smaller than the size of a nonce for instance, so the probability of collisions among passwords is larger than among data of large types. `CryptoVerif` assumes that passwords are taken in a dictionary of between about one million \( (2^{20}) \) and about one trillion \( (2^{40}) \) elements.
- `small` is equivalent to `size0_2`, that is, \( |T| \leq 2^2 \). By default, such a type is small enough so that its value can be guessed by the `guess` command.

- `fun` `(ident)(seq(ident)): (ident) [seq^+ (option)]`.

  `fun f(T_1, . . . , T_n): T`, declares a function that takes \( n \) arguments, of types \( T_1, . . . , T_n \), and returns a result of type \( T \). Optionally, the declaration of a function may be followed by options between brackets. These options can be:

  - `[data]` means that \( f \) is injective and that its inverse can be computed in polynomial time: \( f(x_1, . . . , x_m) = y \) implies for \( i \in \{1, . . . , m\} \), \( x_i = f_i^{-1}(y) \) for some functions \( f_i^{-1} \). (In the vocabulary of `[2]`, \( f \) is poly-injective.) \( f \) can then be used for pattern matching.
  - `[projection]` means that \( f \) is an inverse of a poly-injective function. \( f \) must be unary. (Thanks to the pattern matching construct, one can in general avoid completely the declaration of projection functions, by just declaring the corresponding poly-injective function data.)
  - `[uniform]` means that \( f \) maps the default distribution of its argument into the default distribution of its result. \( f \) must be unary: the argument and the result of \( f \) must be of types marked `fixed`, `bounded`, or `nonuniform`.
  - `[autoSwapIf]` tells `CryptoVerif` to rewrite terms of the form \( f(\ldots, \text{if}_\text{fun}(M_1, M_2, M_3, \ldots)) \) into \( \text{if}_\text{fun}(f(\ldots, M_2, \ldots), f(\ldots, M_3, \ldots)) \), where `if_fun` is a predefined test function that satisfies `if_fun(true, x, y) = x` and `if_fun(false, x, y) = y`.

- `letfun` `(ident) [(seq (var type))]: (term)`.

  `letfun f(x_1:T_1, . . . , x_n:T_n)=M`, declares a function \( f \) that takes \( n \) arguments named \( x_1, . . . , x_n \) of types \( T_1, . . . , T_n \), respectively. The subsequent calls to this function are replaced by the term \( M \) in which we replace \( x_1, . . . , x_n \) with the arguments given by the caller. (We use \( x_i \leftarrow N_i \) instead of \( x_i:T_i \) when \( x_i \) is of type \( [1, N_i] \), where \( N_i \) is a parameter, declared by `param` \( N_i \).

Variables defined inside `letfun` can be used in array references and in queries, provided the process after expansion of `letfun` satisfies the required conditions for that.

- `const` `seq^+ (ident): (ident)`.

  `const c_1, . . . , c_n: T`, declares constants \( c_1, . . . , c_n \) of type \( T \). Different constants are assumed to correspond to different bitstrings (except when the instruction set `diffConstants = false` is given).

- `table` `(ident)(seq^+ (ident))`.

  `table tbl(T_1, . . . , T_n)`, declares the table \( tbl \), whose elements are tuples of type \( T_1, . . . , T_n \). Types \( T_i \) may be replaced with parameters \( N_i \), to declare a table that contains a replication index of type \( [1, N_i] \). Elements can be inserted in the table by `insert tbl(M_1, . . . , M_n)` and the table can be read using `get`.

22
• channel seq^{+}(\text{id})
channel c_{1}, \ldots, c_{n}, declares communication channels c_{1}, \ldots, c_{n}.

• event [\text{id}]\langle \text{seq}(\text{id})\rangle.
event e(T_{1}, \ldots, T_{n}), declares an event e that takes arguments of types T_{1}, \ldots, T_{n}. When there are no arguments, we can simply declare event e. Types T_i may be replaced with parameters N_i, to declare an event that takes as argument a replication index of type [1, N_i].

• let [\text{id}]\langle \text{seq}(\text{vartyp})\rangle = \{\text{oprocess}\}.
let proc(x_{1} : T_{1}, \ldots, x_{n} : T_{n}) = P, says that proc takes n arguments, x_{1} of type T_{1}, \ldots, x_{n} of type T_{n}, and is equal to the process P. (We use x_{i} = N_{i} instead of x_{i} : T_{i} when x_{i} is of type [1, N_{i}], where N_{i} is a parameter, declared by \text{param} N_{i}.) When passing a process, proc\langle M_{1}, \ldots, M_{n}\rangle will be replaced with \text{proj}(M_{1}/x_{1}, \ldots, M_{n}/x_{n}) when P is an input process. In this case, the terms M_{1}, \ldots, M_{n} must contain only variables, replication indices, and function applications and the variables x_{1}, \ldots, x_{n} cannot have array accesses. The process proc\langle M_{1}, \ldots, M_{n}\rangle will be replaced with let x_{1} = M_{1} in \ldots let x_{n} = M_{n} in P when P is an output process.

• equation \forall seq(\text{vartyp})\langle \text{letterm} \mid \text{if} (\text{letterm}) \rangle.
equation \forall x_{1} : T_{1}, \ldots, x_{n} : T_{n}; M, says that for all values of x_{1}, \ldots, x_{n} in types T_{1}, \ldots, T_{n} respectively, M is true. The term M must be a simple term without array accesses. All bound variables x_{1}, \ldots, x_{n} must occur in M. When M is an equality M_{1} = M_{2}, CryptoVerif uses this information for rewriting M_{1} into M_{2}, so one must be careful of the orientation of the equality, in particular for termination. In this case, all bound variables x_{1}, \ldots, x_{n} must occur in M_{1}, so that the target term M_{2} is entirely determined knowing the instance of M_{1}. When M is an inequality, M_{1} \not= M_{2}, CryptoVerif rewrites M_{1} = M_{2} to false and M_{1} \not< M_{2} to true. Otherwise, it rewrites M to true.

Variables bound by assignments inside M are replaced by their value.

• equation buildin \langle \text{eq} _{name}\rangle(seq^{+}(\text{id}))\rangle.
This declaration declares the equational theories satisfied by function symbols. The following equational theories are supported:

– equation buildin \text{commut}(f), indicates that the function f is commutative, that is, f(x, y) = f(y, x) for all x, y. In this case, the function f must be a binary function with both arguments of the same type. (The equation f(x, y) = f(y, x) cannot be given by the \forall x\langle f\rangle declaration because CryptoVerif interprets such declarations as rewrite rules, and the rewrite rule f(x, y) \rightarrow f(y, x) does not terminate.)

– equation buildin \text{assoc}(f), indicates that the function f is associative, that is, f(x, f(y, z)) = f(f(x, y), z) for all x, y, z. In this case, the function f must be a binary function with both arguments and the result of the same type.

– equation buildin \text{AC}(f), indicates that the function f is associative and commutative. In this case, the function f must be a binary function with both arguments and the result of the same type.

– equation buildin \text{assoc0}(f, n), indicates that the function f is associative, and that n is a neutral element for f, that f(x, n) = f(n, x) = x for all x. In this case, the function f must be a binary function with both arguments and the result of the same type as the type of the constant n.

23
- equation builtin $ACU(f, n)$, indicates that the function $f$ is associative and commutative, and that $n$ is a neutral element for $f$. In this case, the function $f$ must be a binary function with both arguments and the result of the same type as the type of the constant $n$.

- equation builtin $ACUN(f, n)$, indicates that the function $f$ is associative and commutative, that $n$ is a neutral element for $f$, and that $f$ satisfies the cancellation equation $f(x, x) = n$. In this case, the function $f$ must be a binary function with both arguments and the result of the same type as the type of the constant $n$.

- equation builtin $group(f, inv, n)$, indicates that $f$ forms group with inverse $inv$ and neutral element $n$, that is, the function $f$ is associative, $n$ is a neutral element for $f$, and $inv(x)$ is the inverse of $x$, that is, $f(inv(x), x) = f(x, inv(x)) = n$. In this case, the function $f$ must be a binary function with both arguments and the result of the same type $T$, $inv$ must be a unary function that takes and returns a value of type $T$, and $n$ must be a constant of type $T$.

- equation builtin $commut_group(f, inv, n)$, indicates that $f$ forms commutative group with inverse $inv$ and neutral element $n$, that is, the function $f$ is associative and commutative, $n$ is a neutral element for $f$, and $inv(x)$ is the inverse of $x$. In this case, the function $f$ must be a binary function with both arguments and the result of the same type $T$, $inv$ must be a unary function that takes and returns a value of type $T$, and $n$ must be a constant of type $T$.

- equation builtin $[\text{random_choices_may_be_equal}]|forall \, seq\,(\forall \text{vartyp})|$,
  \[
  \text{return}((\text{letterm}) \iff (\text{proba}) \Rightarrow \text{return}((\text{letterm}) | \text{if} \, \langle \text{cond} \rangle)) .
  \]
  \[
  \langle \text{cond} \rangle ::= (\langle \text{cond} \rangle) \\
  \mid (\text{letterm}) \\
  \mid (\text{ident}) \text{ independent-of } (\text{ident}) \\
  \mid (\text{cond}) \land (\text{cond}) \\
  \mid (\text{cond}) \lor (\text{cond}) \\
  \mid (\text{basicpat}) \, <- \, (\text{letterm}) ; (\text{cond}) \\
  \mid \text{let} \, (\text{basicpat}) = \, (\text{letterm}) \, \text{in} \, \langle \text{cond} \rangle
  \]

where

\[
\text{collision new} \, x_1:T_1; \ldots \, \text{new} \, x_n:T_n; \text{forall} \, y_1:T'_1, \ldots, y_m:T'_m; \\
\text{return}(M_1) \iff (o) \Rightarrow \text{return}(M_2).
\]

means that when $x_1, \ldots, x_n$ are chosen randomly and independently in $T_1, \ldots, T_n$ respectively (with the default probability distributions for these types), a Turing machine running in time $t$ has probability at most $p$ of finding $y_1, \ldots, y_m$ in $T'_1, \ldots, T'_m$ such that $M_1 \neq M_2$. The terms $M_1$ and $M_2$ must be simple terms without array accesses. See below for the syntax of probability formulas. This allows CryptoVerif to rewrite $M_1$ into $M_2$ with probability loss $p$, when $x_1, \ldots, x_n$ are created by independent random number generations of types $T_1, \ldots, T_n$ respectively. One should be careful of the orientation of the equivalence, in particular for termination.

\[
\text{collision new} \, x_1:T_1; \ldots \, \text{new} \, x_n:T_n; \text{forall} \, y_1:T'_1, \ldots, y_m:T'_m; \\
\text{return}(M_1) \iff (o) \Rightarrow \text{return}(M_2) \, \text{if} \, c.
\]

means that the previous property holds when the condition $c$ is true, where $c$ is built by conjunctions or disjunctions of simple terms and independence conditions “$y_i \text{ independent-of } x_j$”, where $y_i$ is bound by forall and $x_j$ is bound by new. (However, disjunctions cannot mix terms and independence conditions.)

The option $[\text{random_choices_may_be_equal}]$, when it is present, allows several random number generations among $x_1, \ldots, x_n$ to be the same, instead of being independent. One can then group, in a single collision statement, situations in which $x_1, \ldots, x_n$ are the same or they are independent. The indices of the variables corresponding to $x_1, \ldots, x_n$ in the game are still made independent of $x_1, \ldots, x_n$. Hence, there are two cases: either $x_i$ is the same as $x_j$, or $x_i$ and $x_j$ are independent of each other. With the option $[\text{random_choices_may_be_equal}]$, the independence conditions can
also be “$x_i \text{ independent-of } x_j$”, where $x_i$ and $x_j$ are both bound by $\text{new}$. This condition then means $x_i$ and $x_j$ are different random choices, so $x_j$ is also independent of $x_i$.

Variables bound by assignments inside $M_1$, $M_2$, $c$ are replaced by their value.

- **equiv**(\text{ident} \{\text{ident}\})
  
  \text{(omode)} \{[1 \ldots 1 \text{ (omode)}] \Rightarrow (\text{proba}) \Rightarrow \{[n]\} \{\text{seq}^+ (\text{option})\}\} \{\text{ogroup}\} \{[1 \ldots 1] \{\text{ogroup}\}\}.

  \text{equiv(name)} L \Leftarrow(p)\Rightarrow R$, means that the probability that a probabilistic Turing machine that runs in time $t$ time distinguishes $L$ from $R$ is at most $p$. The name $\text{name}$ is used to designate the equivalence in the crypto command used in manual proofs (see Section 7). This name can be either an identifier $id$, or $id(f)$, where $id$ is an identifier and $f$ a second identifier. Names of the form $id(f)$ are most useful when the equivalence is defined inside a macro definition (def). In this case, the identifier $id$ is kept unchanged and the identifier $f$ is renamed during macro expansion; if $f$ is a parameter of the macro, it is then replaced with its value at macro expansion, so that one can always designate precisely the desired equivalence even when a macro is expanded several times. The name may be omitted.

$L$ and $R$ define sets of oracles. (They can be translated into processes as explained in [3].)

- $O(x_1 : T_1, \ldots , x_n : T_n) := \text{FP}$ represents an oracle $O$ that takes arguments $x_1, \ldots , x_n$ of types $T_1, \ldots , T_n$ respectively, and returns the result computed by $\text{FP}$. The oracle body $\text{FP}$ is similar to term, but terminates with a return as shown in the grammar of \text{(body} _\text{equiv}) (Figure 5).

- Optionally, in the left-hand side, an integer between brackets $[n] \ (n \geq 0)$ can be added in the definition of an oracle, which becomes $O(x_1 : T_1, \ldots , x_n : T_n) \ [n] := \text{FP}$. This integer does not change the semantics of the oracle, but is used for the proof strategy: CryptoVerif uses preferably the oracles with the smallest integers $n$ when several oracles can be used for representing the same expression. When no integer is mentioned, $n = 0$ is assumed, so the oracle has the highest priority.

- Optionally, in the left-hand side, the indication $\text{[useful change]}$ can also be added in the definition of an oracle, which becomes $O(x_1 : T_1, \ldots , x_n : T_n) \ [\text{useful change}] := \text{FP}$. This indication is also used for the proof strategy: if at least one $\text{[useful change]}$ indication is present, CryptoVerif applies the transformation defined by the equivalence only when at least one $\text{[useful change]}$ function is called in the game.

- $\text{[new]} \Leftarrow N \text{ new } y_1 : T_1' ; \ldots \text{ new } y_m : T_m' ; (\text{FG} \ldots \text{FG} n)$ represents $N$ copies of a process that picks fresh random numbers $y_1, \ldots , y_n$ of types $T_1', \ldots , T_m'$ respectively, and makes available the functions described in $\text{FG} \ldots \text{FG} n$. Each copy has a different value of $i \in [1, N]$. The identifier $i$ cannot be referred to explicitly in the process; it is used only implicitly as array index of variables defined under $\text{[new]} \Leftarrow N$. The replication $\text{[new]} \Leftarrow N$ can be abbreviated $\text{!N}$.

The replication $\text{[new]} \Leftarrow N$ can be omitted only at the root of the equivalence, when it contains a single \text{(omode)} on the left-hand side, and a single \text{(ogroup)} on the right-hand side. CryptoVerif then automatically adds a replication internally, and adjusts the probability accordingly.

CryptoVerif uses such equivalences to transform processes that call oracles of $L$ into processes that call oracles of $R$.

$L$ may contain mode indications to guide the rewriting: the mode $\text{[all]}$ means that all occurrences of the root function symbol of oracles in the considered group must be transformed; the mode $\text{[exist]}$ means that at least one occurrence of an oracle in this group must be transformed. ([exist] is the default; there must be at most one oracle group with mode [exist]; when an oracle group contains no random number generation, it must be in mode [all]).

Optionally, an integer between brackets $[n] \ (n \geq 0)$ can be added in an equivalence. This integer does not change the semantics of the equivalence, but is used for the proof strategy: CryptoVerif uses preferably the equivalences with the smallest integers $n$ when several equivalences can be used. When no integer is mentioned, $n = 0$ is assumed, so the equivalence has the highest priority.

Two options can be specified for an equivalence, in \text{[seq}^+ (\text{option})]}:
- The **manual** option, when it is present in the equivalence, prevents the automatic application of the transformation. The transformation is then applied only using the manual `crypto` command.

- The **computational** option, when it is present in the equivalence, means that the transformation relies on a computational assumption (by opposition to decisional assumptions). This indication allows one to mark some random number generations of the right-hand side of the equivalence with [unchanged], which means that the random value is preserved by the transformation. The transformation is then allowed even if the random value occurs as argument of events. (This argument will be unchanged.) The mark [unchanged] is forbidden when the equivalence is not marked [computational]. Indeed, decisional assumptions may alter any random values.

$L$ and $R$ must satisfy certain syntactic constraints:

- $L$ and $R$ must be well-typed, satisfy the constraints on array accesses (see the description of processes above), and the type of the results of corresponding oracles in $L$ and $R$ must be the same.

- All oracle definitions in $L$ are of the form $O(.) := \text{return}(M)$ where $M$ is a simple term. Oracle definitions in $R$ are of the form $O(.) := \text{obody}_\equiv$.

- $L$ and $R$ must have the same structure: same replications, same number of oracles, same oracle names in the same order, same number of arguments with the same types for each oracle.

- Under a replication with no random number generation in $L$, one can have only a single oracle.

- Replications in $L$ (resp. $R$) must have pairwise distinct bounds. Oracles in $L$ (resp. $R$) must have pairwise distinct names.

- Finds in $R$ are of the form

  \[
  \text{find[unique]} \ldots
  \]

  or

  \[
  \text{orfind } u_1 \Leftarrow N_1, \ldots, u_m \Leftarrow N_m \text{ suchthat defined}(z_1[u_1], \ldots, z_l[u_l]) \&\& M \text{ then } FP' \ldots \text{ else } FP''
  \]

  where $\tilde{u}_k$ is a non-empty suffix of $u_1, \ldots, u_m$, at least one $\tilde{u}_k$ for $1 \leq k \leq l$ is the whole sequence $u_1, \ldots, u_m$ optionally followed by a sequence of indices $\tilde{u}_0$, and the implicit suffix of the current array indices is the same for all $z_1, \ldots, z_l$. (When $z$ is defined under replications $!N_1, \ldots, !N_n$, $z$ is always an array with $n$ dimensions, so it expects $n$ indices, but the first $n' < n$ indices are left implicit when they are equal to the current indices of the top-most $n'$ replications above the usage of $z$—which also must also be the top-most $n'$ replications above the definition of $z$. We require the implicit indices to be the same for all variables $z_1, \ldots, z_l$.) Furthermore, there must exist $k \in \{1, \ldots, l\}$ such that for all $k' \neq k$, $z_{k'}$ is defined syntactically above all definitions of $z_k$ and $\tilde{u}_{k'}$ is a suffix of $\tilde{u}_k$.

  When $\tilde{u}_0$ is not empty, the find is automatically transformed into

  \[
  \text{find[unique]} \ldots
  \]

  or

  \[
  \text{orfind } u_1 \Leftarrow N_1, \ldots, u_m \Leftarrow N_m, \tilde{u}_0' \Leftarrow \tilde{N}_0' \text{ suchthat defined}(z_1[\tilde{u}_1'], \ldots, z_l[\tilde{u}_l']) \&\& M' \text{ then } FP'''
  \]

  where $\tilde{u}_k'$ are fresh variables of the same type as $\tilde{u}_0$ and $\tilde{N}_0'$ are their bounds ($\tilde{u}_0' \Leftarrow \tilde{N}_0'$ abbreviates a sequence of possibly several inequalities), $u_k' = u_k(\tilde{u}_0'/\tilde{u}_0)$, $M' = M(\tilde{u}_0'/\tilde{u}_0)$, $FP''' = FP'(\tilde{u}_0'/\tilde{u}_0)$, and $i$ is the implicit suffix of the current array indices. After this transformation, we are in the situation above with an empty $\tilde{u}_0$.

  In case a variable $z_k$ is defined by a `find` in $R$, $z_k$ is automatically renamed into a fresh variable $z_k'$ at its definition, and $z_k$ is defined by let $z_k = z_k'$ in the then branch of the find that defines $z_k'$. The array accesses to $z_k$ are left unchanged. After this transformation, the variables $z_k$ on which array accesses are performed are never defined by a `find` in $R$.  

26
- In addition to making array accesses, a limited usage of indices is allowed in $R$. Precisely, the following sequences of indices are allowed:

1. the current array indices, and any suffix thereof;
2. the sequence of indices $u_1, \ldots, u_m$ defined by a `find` followed by the associated implicit suffix of the current array indices (see above), and any suffix thereof;
3. indices received as argument by the oracle, when a variable in $L$ has these indices.

When such a sequence of indices contains a single element, it is represented by the index itself. When it contains several elements, it is represented as a tuple (...) containing the indices. Such sequences of indices can be stored in variables (using `let`), and the sequences or variables containing them can be compared using equality = or disequality <>.

- However, instead of using games given explicitly, CryptoVerif generates the games from special functions (see above), or copying declarations from examples.

This is the key declaration for defining the security properties of cryptographic primitives. Since such declarations are delicate to design, we recommend using predefined primitives listed in Section 5 or copy-pasting declarations from examples.

- `equiv[(ident)](ident(seq(specialarg))] [manual] | [vd],
  `equiv(name) special specialname(a_1, \ldots, a_n)` declares an equivalence (that is, indistinguishability) between two games, like the previous version of `equiv`. However, instead of using games given explicitly, CryptoVerif generates the games from `specialname(a_1, \ldots, a_n)`.

The following values of `specialname` are supported: `rom` and `rom_partial` for random oracles, `prf` and `prf_partial` for pseudo-random functions, `prp` and `prp_partial` for pseudo-random permutations, `sprp` and `sprp_partial` for super pseudo-random permutations (pseudo-random permutations whose inverse is also a pseudo-random permutations), `icm` and `icm_partial` for the ideal cipher model.

Let us first explain the cases `rom`, `rom_partial`, `prf`, `prf_partial`, `prp`, and `prp_partial`. They take the following arguments `seq(specialarg) = a_1, \ldots, a_n`:

1. A string `key_pos`, which can be "key_first" when the key is the first argument of the considered function, "key_last" when it is the last argument, or "key n" when it is its n-th argument. ($n$ is an integer between 1 and the number of arguments of $f$.)

2. An identifier $f$, the considered function. The function $f$ must be declared before the `equiv` declaration. For `prp` and `prp_partial`, the function $f$ must take one argument in addition to the key, the type $T$ of this argument must be the same as the type of the result of $f$, and it must be large enough so that collisions between a random element of the domain and an independent value can be eliminated (because we model a PRF and apply the PRF/PRP switching lemma), that is, $\text{PcollRand}(T) \leq 2^{-n}$, that is, $T$ has option $\text{pcolln}$ with $n \geq n'$ where $n'$ is set by `set minAutoCollElim = pext n'`; the default is $n' = 80$. For other values of `specialname`, the function $f$ must take at least one argument in addition to the key. In all cases, we must be able to choose an element randomly in the type of the key and in the type of the result of $f$, that is, these types must be declared fixed, bounded, or nonuniform.

3. When `specialname` is not `rom` nor `rom_partial`, an identifier $p$ such that $p(t, N, l_1, \ldots, l_m)$ is the probability that an adversary breaks the PRF (resp. PRP) assumption in time $t$, with at most $N$ queries to the function $f$, with arguments of lengths at most $l_1, \ldots, l_m$. The length is omitted when the corresponding type is bounded. The identifier $p$ must be declared with `proba` $p$. This argument is omitted for random oracles because the probability is always 0.

4. A tuple of identifiers $(k, r, x, y, z, u)$ for ROM and PRF, $(k, r, x, u)$ for PRP, which are used to determine identifiers of variables in the generated equivalence:
   - $k$ is the identifier of the key;
   - $r$ is the identifier of the random result of $f$ after game transformation;
   - $x$ is the identifier used for arguments of $f$ in most oracles;
\[-y \text{ and } z \text{ are the identifiers used for arguments of the two calls to } f \text{ in oracles generated by the collision LHS } "Ocoll : new \ r_1:T; new \ r_2:T;forall \ a_1 : T_1; \ldots; a_n : T_n; M" \text{ (see the next argument);}\]

\[-u \text{ is the identifier used for indices of } \text{find.}\]

The identifiers \(x, y, z, u\) are suffixed by \(\_\) and the name of the oracle in which they are used. The identifier \(r\) is suffixed by \(\_\) and the suffix of the name of the oracle in which it is used. Moreover, if needed to avoid name clashes or to generate several variables, a suffix \(\_n\) may be added to these identifiers or modified if they already have one. Using identifiers not used elsewhere allows the user to have stable identifiers in the generated equivalence.

5. A tuple of strings \texttt{collisions LHS}, which can be either ("large") or a tuple of strings of the following forms:

\[-"Ocoll : forall \ a_1 : T_1; \ldots; a_n : T_n; new \ r_1:T; M" \text{ where } T \text{ is the type of the result of } f \text{ and the simple term } M \text{ uses the variables } a_1; \ldots; a_n, r_1. \text{ In this case, CryptoVerif tries to simplify } M \text{ assuming } r_1 \text{ is a random value and } a_1; \ldots; a_n \text{ do not depend on } r_1. \text{ If it rewrites } M \text{ into a term } N \text{ that does not contain } r_1, \text{ then it uses this information to transform terms } M\{f(...)/r_1\} \text{ into } N \text{ when the result of } f(...) \text{ is a fresh random value, in the generated cryptographic transformation. (See files examples/obasic/undeniable-sig1.ocv and examples/obasic/undeniable-sig2.ocv for examples.)}\]

\[-"Ocoll : new \ r_1:T; forall \ a_1 : T_1; \ldots; a_n : T_n; M" \text{ where } T \text{ is the type of the result of } f \text{ and the simple term } M \text{ uses the variables } a_1; \ldots; a_n, r_1. \text{ In this case, CryptoVerif tries to simplify } M \text{ assuming } r_1 \text{ is a random value } (a_1; \ldots; a_n \text{ may depend on } r_1). \text{ If it rewrites } M \text{ into a term } N \text{ that does not contain } r_1, \text{ then it uses this information to transform terms } M\{f(...)/r_1\} \text{ into } N, \text{ in the generated cryptographic transformation.}\]

\[-"Ocoll : new \ r_1:T; new \ r_2:T;forall \ a_1 : T_1; \ldots; a_n : T_n; M" \text{ where } T \text{ is the type of the result of } f \text{ and the simple term } M \text{ uses the variables } a_1; \ldots; a_n, r_1, r_2. \text{ In this case, CryptoVerif tries to rewrite } M \text{ assuming } r_1 \text{ and } r_2 \text{ are independent random values into a term } N_2 \text{ that does not contain } r_1 \text{ nor } r_2, \text{ and to rewrite } M \text{ assuming } r_1 = r_2 \text{ is a random value into a term } N_1 \text{ that does not contain } r_1 \text{ nor } r_2. \text{ If it succeeds, then it uses this information to transform terms } M\{f(\text{args}_1)/r_1, f(\text{args}_2)/r_2\} \text{ into } \text{if } \text{args}_1 = \text{args}_2 \text{ then } N_1 \text{ else } N_2, \text{ in the generated cryptographic transformation.}\]

Obviously, when \(n = 0\), \texttt{forall } \texttt{a_1 : T_1; \ldots; a_n : T_n; } \text{is omitted. The identifiers } Ocoll \text{ are used to form the oracle names in the generated equivalence (see below); they must not contain } \_\text{ and must be different from } 0 \text{ and pairwise distinct. Only the first form is allowed for prp and prp\_partial. Even when a single string is present, the argument must be a tuple of strings, so this string must be between parentheses.}\]

When \texttt{collisions LHS} is ("large"), the type \(T\) of the result of \(f\) must be large enough so that collisions between a random element of the domain and an independent value can be eliminated, that is, \texttt{PCollIrand(T) \leq 2^{n'}} \text{, that is, } T \text{ has option pcollI with } n \geq n' \text{ where } n' \text{ is set by set } \texttt{minAutoCollElim = pevn'}; \text{ the default is } n' = 80. \text{ In this case, this is equivalent to } \texttt{collisions LHS} \text{ containing:}\]

\[-"\text{Def: forall } a_1 : T; new \ r_1:T; r_1 = a_1\". \text{ Assuming } a_1 \text{ does not depend on } r_1, r_1 = a_1 \text{ simplifies into false, so } f(...) = a_1 \text{ is transformed into false in the generated cryptographic transformation, when the result of } f(...) \text{ is a fresh random value.}\]

\[-\text{When specialname is not prp nor prp\_partial, } "Ocoll : new \ r_1:T; new \ r_2:T; r_1 = r_2\". \text{ The term } r_1 = r_2 \text{ simplifies into false when } r_1 \text{ and } r_2 \text{ are independent random values and into true when } r_1 = r_2, \text{ so } f(\text{args}_1) = f(\text{args}_2) \text{ is transformed into } \text{args}_1 = \text{args}_2 \text{ in the generated cryptographic transformation.}\]

The argument \texttt{collisions LHS} can be overridden when the equivalence is used in a crypto command, by passing the desired \texttt{collisions LHS} as special argument to the crypto command.

The last or the last two arguments may be omitted.

When \texttt{specialname} is \texttt{rom}, \texttt{prf}, or \texttt{prp}, the generated equivalence provides the following oracles:
- Oracle $\emptyset$ evaluates $f$ on its arguments in the left-hand side, and performs a lookup into previous arguments of $\emptyset$ in the right-hand side: it returns the previous result when the current arguments are equal to previous arguments and otherwise it returns a fresh random value.

- For each element of $\text{collisions}_\text{LHS}$, oracle $\text{Ocoll}$ evaluates $M$ with $r_i$ replaced with a call to $f$ in left-hand side and uses the simplified form of $M$ in the right-hand side.

When $\text{specialname}$ is $\text{rom}_\text{partial}$, $\text{prf}_\text{partial}$, or $\text{prp}_\text{partial}$, the generated equivalence provides oracles named $\text{Ocoll}$ for each element "$\text{Ocoll} : \text{new } r_1: T; \text{forall } a_1 : T_1, \ldots, a_n : T_n; M"$ or "$\text{Ocoll} : \text{new } r_1: T; \text{new } r_2: T; \text{forall } a_1 : T_1, \ldots, a_n : T_n; M"$ of $\text{collisions}_\text{LHS}$. These oracles act like the oracle of the same name when $\text{specialname}$ is $\text{rom}$ (resp. $\text{prf}$—there are no such oracles for $\text{prp}_\text{partial}$).

It also provides oracles named $\text{prefix}_{\text{suffix}}$ where $\text{prefix}$ is $\emptyset$ or an iden tier $\text{Ocoll}$ from a collision "$\text{Ocoll} : \text{forall } a_1 : T_1, \ldots, a_n : T_n; \text{new } r_1: T; M"$ in $\text{collisions}_\text{LHS}$ and $\text{suffix}$ is arbitrary. These oracles act like the oracle of $\text{prefix}$ when $\text{specialname}$ is $\text{rom}$ (resp. $\text{prf}$ or $\text{prp}$), except that:

- When $\text{suffix}$ starts with $\text{leave}$, the right-hand side still uses calls to $f$; it does not replace them with fresh random values. However, it still performs look ups as needed to make sure that the returned result is coherent with results previously returned by other oracles.

- It uses a collision matrix to determine whether arguments of oracles with various suffixes are allowed to collide with non-negligible probability. By default, this collision matrix says that the arguments of two oracles are allowed to collide when they have the same suffix or when one of the suffixes starts with $\text{leave}$. A different collision matrix can be specified by passing a string as a special argument to the crypto command, which can be either "$\text{no collisions}$" or statements $\text{seq}"(\text{suffix})$ may collide with previous $\text{seq}"(\text{suffix})$ separated by semi-colons ($;$). "$\text{no collisions}$" says that the arguments of two oracle calls are never allowed to collide. $\text{suffix}_1\ldots, \text{suffix}_n$ may collide with previous $\text{suffix}_1'\ldots, \text{suffix}_n'$ says that the arguments of oracles with suffix $\text{suffix}_i (i \in \{1, \ldots, n\})$ are allowed to collide with arguments of previous calls to oracles with suffix $\text{suffix}_j (j \in \{1, \ldots, n'\})$. In the right-hand side, the oracles execute $\text{event}_\text{abort}$ $\text{ev}_\text{coll}$ when a disallowed collision happens. That avoids generating further code in this case, and thus may considerably reduce the size of the generated game after applying the cryptographic transformation. However, in case a disallowed collision actually happens with non-negligible probability, CryptoVerif will be unable to prove that event $\text{ev}_\text{coll}$ does not happen, so the proof will fail.

The oracles $\text{prefix}_{\text{leave}}$ are generated by default. The other oracles are generated on demand when they are present in the terms: information of the crypto command. Therefore, you must explicitly mention in the terms: information all occurrences of terms that should be transformed by an oracle different from $\text{prefix}_{\text{leave}}$. (See file examples/arinc823/sharedkey/lemmaEnc_equiv_v2_optim.occ for an example with $\text{prf}_\text{partial}$.)

Let us now explain the cases $\text{sprp}$, $\text{sprp}_\text{partial}$, $\text{icm}$, and $\text{icm}_\text{partial}$. They take the following arguments $\text{seq}(\text{specialarg}) = a_1, \ldots, a_n$:

1. A tuple of strings $\text{arg}_\text{order}$, which contains the strings "$\text{msg}$", "$\text{key}$", and for $\text{icm}$ and $\text{icm}_\text{partial}$, "$\text{local_key}$", in the order in which the encryption and decryption functions take their arguments. (For the ideal cipher model, the "$\text{key}$" is the key that models the choice of the encryption scheme, and the "$\text{local_key}$" is the key passed to each encryption and decryption.)

2. A identifier $\text{enc}$ and an identifier $\text{dec}$, which are respectively the encryption and decryption functions. These functions must have the same type, and take arguments as specified by $\text{arg}_\text{order}$. We must be able to choose an element randomly in the type of the argument "$\text{key}$" and in the type of the result of $\text{enc}$ and $\text{dec}$, that is, these types must be declared fixed, bounded, or nonuniform. The type of the argument "$\text{msg}$" must be the same as the type of the result of $\text{enc}$ and $\text{dec}$. ($\text{enc}$ and $\text{dec}$ are permutations of this type.) This type $T$ must be large enough so that collisions between a random element of this type and an independent value can be eliminated (because we model a PRF and apply the PRF/PRP
switching lemma), that is, \(P_{\text{coll}}(T) \leq 2^{-n'}\), that is, \(T\) has option \(p_{\text{coll}} n\) with \(n \geq n'\) where \(n'\) is set by \(\text{set minAutoCollElim} = \text{pestn}'\); the default is \(n' = 80\).

3. When \(\text{specialname}\) is \(\text{sprp}\) or \(\text{sprp\_partial}\), an identifier \(p\) such that \(p(t, N, N', l, l', l)\) is the probability that an adversary breaks the \(\text{SPRP}\) assumption in time \(t\), with at most \(N\) queries to the function \(\text{enc}\), with messages of length at most \(l\), and at most \(N'\) queries to the function \(\text{dec}\), with ciphertexts of length at most \(l'\). The length is omitted when the type is bounded. The identifier \(p\) must be declared with \(\text{prob}\). This argument is omitted for the ideal cipher model because the probability is always 0.

4. A tuple of identifiers \((k, lk, m, c, \_u)\) for \(\text{ICM}\), \((k, m, c, \_u)\) for \(\text{SPRP}\), which are used to determine identifiers of variables in the generated equivalence:

   - \(k\) is the identifier of the key;
   - \(lk\) is the identifier of the local key;
   - \(m\) is the identifier of cleartext messages;
   - \(c\) is the identifier of ciphertexts;
   - \(u\) is the identifier used for indices of \(\text{find}\).

   The identifiers \(lk, m, c, \_u\) are suffixed by \(\_\) and the name of the oracle in which they are used. Moreover, if needed to avoid name clashes or to generate several variables, a suffix \(\_n\) may be added to these identifiers or modified if they already have one. Using identifiers not used elsewhere allows the user to have stable identifiers in the generated equivalence.

5. A tuple of strings \(\text{collisions\_LHS}\), which can be either ("large") or a tuple of strings of the following form:

   "\(O_{\text{coll}}: \forall a_1: T_1, \ldots, a_n: T_n; \text{new } r_1: T; M\)"

   where \(T\) is the type of the result of \(\text{enc}\) and the simple term \(M\) uses the variables \(a_1, \ldots, a_n, r_1\). In this case, CryptoVerif tries to simplify \(M\) assuming \(r_1\) is a random value and \(a_1, \ldots, a_n\) do not depend on \(r_1\). If it rewrites \(M\) into a term \(N\) that does not contain \(r_1\), then it uses this information to transform terms \(M\{f(\ldots)/r_1\}\) into \(N\) when the result of \(f(\ldots)\) is a fresh random value, in the generated cryptographic transformation. Obviously, when \(n = 0\), \(\forall a_1: T_1, \ldots, a_n: T_n; M\) is omitted. The identifiers \(O_{\text{coll}}\) are used to form the oracle names in the generated equivalence (see below); they must not contain \(\_\) and must be different from 0 and pairwise distinct. Even when a single string is present, the argument must be a tuple of strings, so this string must be between parentheses.

   When \(\text{collisions\_LHS}\) is ("large"), this is equivalent to \(\text{collisions\_LHS}\) containing:

   "\(O_{\text{eq}}: \forall a_1: T; \text{new } r_1: T; r_1 = a_1\)"

   Assuming \(a_1\) does not depend on \(r_1\), \(r_1 = a_1\) simplifies into \(\mathsf{false}\), so \(f(\ldots) = a_1\) is transformed into \(\mathsf{false}\) in the generated cryptographic transformation, when the result of \(f(\ldots)\) is a fresh random value.

   The argument \(\text{collisions\_LHS}\) can be overriden when the equivalence is used in a \(\text{crypto}\) command, by passing the desired \(\text{collisions\_LHS}\) as special argument to the \(\text{crypto}\) command.

   The last or the last two arguments may be omitted.

When \(\text{specialname}\) is \(\text{icm}\) or \(\text{sprp}\), the generated equivalence provides the following oracles:

- Oracle \(0_{\text{enc}}\) evaluates \(\text{enc}\) on its arguments in the left-hand side, and performs a lookup into previous cleartexts (and local keys for \(\text{icm}\)) of calls to \(0_{\text{enc}}\) and \(0_{\text{dec}}\) in the right-hand side: it returns the previous ciphertext when the current arguments are equal to previous cleartexts (and local keys for \(\text{icm}\)) and otherwise it returns a fresh random value.

- Oracle \(0_{\text{dec}}\) evaluates \(\text{dec}\) on its arguments in the left-hand side, and performs a lookup into previous ciphertexts (and local keys for \(\text{icm}\)) of calls to \(0_{\text{enc}}\) and \(0_{\text{dec}}\) in the right-hand side: it returns the previous cleartext when the current arguments are equal to previous ciphertexts (and local keys for \(\text{icm}\)) and otherwise it returns a fresh random value.
- For each element of collisions\_LHS, oracles Ocoll\_enc and Ocoll\_dec evaluate M with \(v_i\) replaced with a call to \(\text{enc}\) (resp. \(\text{dec}\)) in left-hand side and uses the simplified form of M in the right-hand side.

When specialname is \(\text{icm\_partial}\) or \(\text{sprp\_partial}\), the generated equivalence provides oracles named \(\text{prefix}\_\text{middle}\_\text{suffix}\) where \(\text{prefix}\) is for an identifier \(\text{Ocoll}\) from a collision in collisions\_LHS, \(\text{middle}\) is \(\text{enc}\) or \(\text{dec}\), and \(\text{suffix}\) is arbitrary. These oracles act like the oracle \(\text{prefix}\_\text{middle}\) when specialname is \(\text{icm}\) (resp. \(\text{sprp}\)), except that it uses a collision matrix to determine whether arguments of oracles with various suffixes are allowed to collide with non-negligible probability. By default, this collision matrix says that the arguments of two oracles are allowed to collide when they have the same suffix or when one of the suffixes is \default. A different collision matrix can be specified by passing a string as a special argument to the \text{crypto} command, which can be either "no collisions" or statements \seq\(1\) (suffix) may collide with previous \seq\(1\) (suffix) separated by semi-colons (\;). "no collisions" says that the arguments of two oracle calls are never allowed to collide. \seq\(1, \ldots, \seq\(n\) may collide with previous \seq\(1, \ldots, \seq\(n\) says that the arguments of oracles with suffix \seq\(1, \ldots, \seq\(n\) are allowed to collide with arguments of previous calls to oracles with suffix \seq\(1, \ldots, \seq\(n\) in the right-hand side, the oracles execute \text{event\_abort ev\_coll} when a disallowed collision happens. That avoids generating further code in this case, and thus may considerably reduce the size of the generated game after applying the cryptographic transformation. However, in case a disallowed collision actually happens with non-negligible probability, CryptoVerif will be unable to prove that \text{event ev\_coll} does not happen, so the proof will fail.

The oracles with suffix \default are generated by default. The other oracles are generated on demand when they are present in the terms: information of the \text{crypto} command. Therefore, you must explicitly mention in the terms: information all occurrences of terms that should be transformed by an oracle with a suffix different from \default.

The \[\text{manual}\] option, when it is present in the declaration, prevents the automatic application of the transformation. The transformation is then applied only using the manual \text{crypto} command. Alternatively, an integer between brackets \([\, n\,] (n \geq 0)\) can also be added to the declaration. This integer does not change the semantics of the equivalence, but is used for the proof strategy: CryptoVerif uses preferably the equivalences with the smallest integers \(n\) when several equivalences can be used. When no integer is mentioned, \(n = 0\) is assumed, so the equivalence has the highest priority.

- **query** \[\text{seq}\(1\) (\text{vartype});\}]\(\langle\,\text{query}\rangle\langle\,\text{query}\rangle\rfloor\*

The query declaration indicates which security properties we would like to prove. CryptoVerif allows two variants of the syntax for queries:

- In the recommended syntax, the part \[\text{seq}\(1\) (\text{vartype});\}] is omitted, and the query declaration is of the form query \(Q_1; \ldots; Q_n\). The variables in correspondence queries are explicitly quantified inside each query \(Q_i\), as explained below.

- In the other syntax, the query declaration is of the form query \(x_1:T_1, \ldots, x_n:T_n; Q_1; \ldots; Q_n\). First, we declare the types of all variables \(x_1, \ldots, x_n\) that occur in correspondence queries that follow. (We use \(x_i \in N_i\) instead of \(x_i:T_i\) when \(x_i\) is of type \([1, N_i]\), where \(N_i\) is a parameter, declared by \text{param} \(N_i\).) Second, we give the queries \(Q_1, \ldots, Q_n\) themselves, without any \text{forall} \(x_1:T_1, \ldots, x_j:T_j\); and \text{exists} \(y_1:T_1, \ldots, y_k:T_k\). This form is not recommended because the quantifiers applied to the variables are less obvious to the user: variables that occur before \[\Rightarrow\] are universally quantified and variables that occur after \[\Rightarrow\] but not before \[\Rightarrow\] are existentially quantified just after \[\Rightarrow\].

The available queries \(Q_i\) are as follows:

- secret \(x\) \[\text{public\_vars} l\] or
- secret \(x\) \[\text{public\_vars} l\] \[\text{real\_or\_random}\]: show that the array \(x\) is indistinguishable from an array of independent random numbers (by several test queries), even when the variables
in \( l \) are public. The list \( l \) is considered empty when it is omitted. In the vocabulary of [2],
this is secrecy.

- **secret** \( x \) \([public\_vars \ l \)[onesession] or \[real\_or\_random,onesession] show that any element of the array \( x \) cannot be distinguished from a random number (by a single test query), even when the variables in \( l \) are public. The list \( l \) is considered empty when it is omitted. In the vocabulary of [2], this is one-session secrecy.

- **secret** \( x \) \([public\_vars \ l \)[reachability] shows that the adversary cannot compute any element of the array \( x \), even when it has access to the other elements of \( x \) and to the variables in \( l \). This query is allowed only when \( x \) is of a large type (or type declared with \( pcoll \)) for \( n \geq n' \) with set \( \text{minAutoCollElim} = \text{pest} n' \), that is, collisions can be eliminated between random values of that type. Otherwise, the adversary would have a non-negligible probability of finding the value of \( x \) just by guessing.

- **secret** \( x \) \([public\_vars \ l \)[reachability,onesession] shows that the adversary cannot compute any element of the array \( x \), even when it has access to the variables in \( l \). This query is allowed only when \( x \) is of a large type (or type declared with \( pcoll \)) for \( n \geq n' \) with set \( \text{minAutoCollElim} = \text{pest} n' \), that is, collisions can be eliminated between random values of that type. Otherwise, the adversary would have a non-negligible probability of finding the value of \( x \) just by guessing.

This notion of secrecy as the adversary cannot compute is less common in the computational model than “the adversary cannot distinguish from random”, but it is still used (e.g. in the property of one-wayness or in the computational Diffie-Hellman assumption).

- **secret** \( x \) \([public\_vars \ l \)[cv_bit] shows that the adversary cannot guess the value of the boolean variable \( x \) significantly better than at random. It applies only when \( x \) is a boolean variable defined under no replication. When the process chooses \( x \) randomly and executes different code depending on whether \( x \) is true or false, this property also shows that the process with \( x \) true is indistinguishable from the process with \( x \) false.

The options \( \text{cv\_onesession}, \text{cv\_real\_or\_random}, \text{cv\_reachability} \) are also allowed, and synonym of the similar options without \( \text{cv\_} \) prefix. The only difference is that options that start with \( \text{cv\_} \) apply to CryptoVerif only, while options that start neither with \( \text{cv\_} \) nor with \( \text{pv\_} \) apply to both CryptoVerif and ProVerif. All options starting with \( \text{pv\_} \) are also allowed, but ignored: they are for ProVerif.

- \( \text{forall} \ x_1; T_1, \ldots, x_j; T_j; M_0 \) \([public\_vars \ l \), where in \( M_0 \) \( \Rightarrow \) is not allowed under \&\&, ||, or \( \exists \) and \( \exists \) and \( \exists \) are allowed only after \( \Rightarrow \), so that after replacing variables bound by assignments by their value and moving existential quantifiers just after \( \Rightarrow \), \( M_0 \) is of form \( M \Rightarrow \) \([\exists y_1; T_1, \ldots, y_k; T_k; M' \) or \( M, \) where \( M \) and \( M' \) do not contain \( \Rightarrow \). The query \( M \) is an abbreviation for \( M \Rightarrow \text{false} \), so we only need to consider \( M \Rightarrow \) \([\exists y_1; T_1, \ldots, y_k; T_k; M' \ (W \ use \ x_i < N_i \) instead of \( x_i; T_i \ when \ x_i \) is of type \([1, N_i] \), where \( N_i \) is a parameter, declared by \( \text{param} \ N \). We use the same notation for \( y_k \).

The variables \( x_1, \ldots, x_j \) are the variables that occur in \( M \), and the variables \( y_1, \ldots, y_k \) are the variables of \( M' \) that do not occur in \( M \). (In particular, a universally quantified variable \( x_i \) is not allowed to occur in \( M' \) and not in \( M \).) CryptoVerif shows that, for all values of \( x_1, \ldots, x_j \) if \( M \) is true then there exist values of \( y_1, \ldots, y_k \) such that \( M' \) is true, even when the variables in \( l \) are public.

\( M \) must be a conjunction of terms \( \text{event}(e), \text{inj-event}(e), \text{event}(e(M_1, \ldots, M_n)) ), or \( \text{inj-event}(e(M_1, \ldots, M_n)) \) where \( e \) is an event declared by \( \text{event} \) and the \( M \) are simple terms without array accesses (not containing events).

\( M' \) must be formed by conjunctions and disjunctions of terms \( \text{event}(e), \text{inj-event}(e), \text{event}(e(M_1, \ldots, M_n)), \text{inj-event}(e(M_1, \ldots, M_n)) \), or simple terms without array accesses (not containing events).

When \( \text{inj-event} \) is present, the system proves an injective correspondence, that is, it shows that several different events marked \( \text{inj-event} \) before \( \Rightarrow \) imply the execution of several different events marked \( \text{inj-event} \) after \( \Rightarrow \). More precisely, \( \text{inj-event}(e_1(M_1, \ldots, M_{1m_1})) \)
& & ... & & inj-event(\epsilon_n(M_{n1}, . . . , M_{nm})) & & ... \Rightarrow M' \text{ means that for each tuple of executed events } \epsilon(M_{M1}, . . . , M_{Mm}) \text{ (executed } N \text{ times)}, \ M' \text{ holds, considering that an event } inj-event(\epsilon'(M_{M1}, . . . , M_{Mm})) \text{ in } M' \text{ holds when it has been executed at least } N \times \ldots \times N \text{ times. The } inj-event \text{ marker must occur either before and after } \Rightarrow \text{ or not at all. (Otherwise, the query would be equivalent to a non-injective correspondence.)}

- **proof** \{⟨(command); . . . ; (command)⟩⟩

  Allows the user to include in the CryptoVerif input file the commands that must be executed by CryptoVerif in order to prove the protocol. The allowed commands are those described in Section 7 except that help and ? are not allowed and that the crypto command must be fully specified (so that no user interaction is required). If the command contains a string that is not a valid identifier, *, or ., then this string must be put between quotes "". This is useful in particular for variable names introduced internally by CryptoVerif and that contain \$ (so that they cannot be confused with variables introduced by the user), for example "@2_r1".

- **def** ⟨ident⟩(seq⟨ident⟩) {seq⟨decl⟩}

  The function ⟨ident⟩(seq⟨ident⟩) {seq⟨decl⟩} defines a macro named ⟨ident⟩, with arguments seq⟨ident⟩. This macro expands to the declarations seq⟨decl⟩, which can be any of the declarations listed in this manual, except def itself. The macro is expanded by the expand declaration described below. When the expand declaration appears inside a def declaration, the expanded macro must have been defined before the def declaration (which prevents recursive macros, whose expansion would loop). Macros are used in particular to define a library of standard cryptographic primitives that can be reused by the user without entering their full definition. These primitives are presented in Section 6.

- **expand** ⟨ident⟩(seq⟨ident⟩)

  The command expand ⟨ident⟩(seq⟨ident⟩) expands the macro ⟨ident⟩ by applying it to the arguments seq⟨ident⟩. If the definition of the macro ⟨ident⟩ is def ⟨ident⟩(seq⟨ident⟩) {seq⟨decl⟩}, then it generates seq⟨decl⟩ in which seq⟨ident⟩ are substituted for seq⟨ident⟩ and the other identifiers that were not already defined at the def declaration are renamed to fresh identifiers.

The following identifiers are predefined:

- The type bitstring is the type of all bitstrings.

- The type bitstringbot is the type that contains all bitstrings and ⊥.

- The type bool is the type of boolean values, which consists of two constant bitstrings true and false. It is declared fixed.

- The function not is the boolean negation, from bool to bool.

- The constant bottom represents ⊥. (The special element of bitstringbot that is not a bitstring.)

- The function if_fun takes three arguments, one of type bool and two arguments of the same type. It satisfies if_fun(true, x, y) = x and if_fun(false, x, y) = y.

  The syntax of probability formulas allows parenthesizing and the usual algebraic operations +, -, *, /, \^\#. \(\^\#\) is the exponentiation, its second argument must be an integer; \(^\#\) has higher priority than \(*\) and /, which have higher priority than + and -, as usual, as well as the maximum, denoted max(p1, . . . , pn), and minimum, denoted min(p1, . . . , pn). They may also contain

- \(P\) or \(P(p1, . . . , pn)\) where \(P\) has been declared by proba \(P\) and \(p1, . . . , pn\) are probability formulas; this formula represents an unspecified probability depending on \(p1, . . . , pn\).

- \(N\), where \(N\) has been declared by param \(N\), designates the number of copies of a replication.

- \#O, where \(O\) is an oracle, designates the number of different calls to the oracle \(O\).
• $(O \text{ foreach } x)$, where $O$ is an oracle and $x$ is a random variable, designates the maximum number of different calls to the oracle $O$ for each choice of the random variable $x$. The variable $x$ must be chosen in a sequence of random variables at least one replication above the definition of oracle $O$. 

• $(O \text{ foreach } i_1, \ldots, i_n)$, where $O$ is an oracle and $i_1, \ldots, i_n$ are replication indices, designates the maximum number of different calls to the oracle $O$ for each value of the replication indices $i_1, \ldots, i_n$. These replication indices must be a strict suffix of the current replication indices at the definition of $O$. ($i_n$ must be the index of the replication at the top of equiv statement, $i_{n-1}$ must be a replication index of replication just under the one with index $i_n$, and so on.)

• $[T]$, where $T$ has been declared by type $T$ and is fixed or bounded, designates the cardinal of $T$.

• $\text{maxlength}(M)$ is the maximum length of term $M$ ($M$ must be a simple term without array access, and must be of a non-bounded type).

• $\text{length}(f, p_1, \ldots, p_n)$ designates the maximal length of the result of a call to $f$, where $p_1, \ldots, p_n$ represent the maximum length of the non-bounded arguments of $f$ ($p_i$ must be built from $\text{max}$, $\text{maxlength}(M)$, and $\text{length}(f', \ldots)$, where $M$ is a term of the type of the corresponding argument of $f$ and the result of $f'$ is of the type of the corresponding argument of $f$).

• $\text{length}(T)$ designates the maximal length of a bitstring of type $T$, where $T$ is a bounded type.

• $\text{length}((T_1, \ldots, T_n), p_1, \ldots, p_n)$ designates the maximal length of the result of the tuple function from $T_1 \times \ldots \times T_n$ to $\text{bitstring}$, where $p_1, \ldots, p_n$ represent the maximum length of the non-bounded arguments of this function.

• $n$ is an integer constant.

• $\text{eps\_find}$ is 2 times the maximum distance between the uniform probability distribution and the probability distribution used for choosing elements in find.

• $\text{eps\_rand}(T)$ is the maximum distance between the uniform probability distribution and the default probability distribution $D_T$ for type $T$ (when $T$ is bounded).

• $P_{\text{coll1rand}}(T)$ is the maximum probability of collision between a random value $X$ of type $T$ chosen according to the default distribution $D_T$ for type $T$ and an element of type $T$ that does not depend on it (when $T$ is nonuniform). This is also the maximum probability of choosing any given element of $T$ in the default distribution for that type:

$$P_{\text{coll1rand}}(T) = \max_{a \in T} \Pr[X = a]$$

where $X$ is chosen according to distribution $D_T$.

• $P_{\text{coll2rand}}(T)$ is the maximum probability of collision between two independent random values of type $T$ chosen according to the default distribution $D_T$ for type $T$ (when $T$ is nonuniform). We have

$$\frac{1}{|T|} \leq P_{\text{coll2rand}}(T) = \sum_{a \in T} \Pr[X = a]^2 \leq P_{\text{coll1rand}}(T)$$

where $X$ is chosen according to the default distribution $D_T$.

• **optim-if** *condition* then $p_1$ else $p_2$ evaluates to $p_1$ when the condition *condition* is proved to be true and to $p_2$ otherwise. Hence, the formula $p_2$ must always be a sound estimate, whether the condition is true or not (because it may happen that the condition is true and CryptoVerif does not manage to prove it). The formula $p_1$ is typically a better estimate valid when the condition holds. The grammar for the condition *condition* is defined in Figure 4. The condition *is-int(p)* is true when $p$ is a constant. The other conditions have their usual meaning.

• $\text{time}$ designates the runtime of the environment (attacker).

Finally, $\text{time}(\ldots)$ designates the runtime time of each elementary action of a game:
\( \text{time}(f, p_1, \ldots, p_n) \) designates the maximal runtime of one call to function symbol \( f \), where \( p_1, \ldots, p_n \) represent the maximum length of the non-bounded arguments of \( f \).

\( \text{time(let } f, p_1, \ldots, p_n) \) designates the maximal runtime of one pattern matching operation with function symbol \( f \), where \( p_1, \ldots, p_n \) represent the maximum length of the non-bounded arguments of \( f \).

\( \text{time((T_1, \ldots, T_m), p_1, \ldots, p_n)} \) designates the maximal runtime of one call to the tuple function from \( T_1 \times \ldots \times T_m \) to bitstring, where \( p_1, \ldots, p_n \) represent the maximum length of the non-bounded arguments of this function.

\( \text{time(let((T_1, \ldots, T_m), p_1, \ldots, p_n)} \) designates the maximal runtime of one pattern matching with the tuple function from \( T_1 \times \ldots \times T_m \) to bitstring, where \( p_1, \ldots, p_n \) represent the maximum length of the non-bounded arguments of this function.

\( \text{time(=} T_1[, p_1, p_2]) \) designates the maximal runtime of one call to bitstring comparison function for bitstrings of type \( T \), where \( p_1, p_2 \) represent the maximum length of the arguments of this function when \( T \) is non-bounded.

\( \text{time(!) or time(foreach)} \) is the maximum time of an access to a replication index.

\( \text{time([n])} \) is the maximum time of an array access with \( n \) indices.

\( \text{time(&&)} \) is the maximum time of a boolean and.

\( \text{time(||)} \) is the maximum time of a boolean or.

\( \text{time(new } T \) or \( \text{time(<-R } T) \) is the maximum time needed to choose a random number of type \( T \) according to the default distribution for type \( T \).

\( \text{time(newChannel)} \) is the maximum time to create a new private channel.

\( \text{time(if)} \) is the maximum time to perform a boolean test.

\( \text{time(find } n \) is the maximum time to perform one condition test of a find with \( n \) indices to choose. (Essentially, the time to store the values of the indices in a list and part of the time needed to randomly choose an element of that list.)

\( \text{time(out } [T_1, \ldots, T_m] T, p_1, \ldots, p_n) \) represents the time of an output in which the channel indices are of types \( T_1, \ldots, T_m \), the output bitstring is of type \( T \), and the maximum length of the channel indices and the output bitstring is represented by \( p_1, \ldots, p_n \) when they are non-bounded.

\( \text{time(in } n \) is the maximum time to store an input in which the channel has \( n \) indices in the list of available inputs.

CryptoVerif checks the dimension of probability formulas.

4 oracles Front-end

The oracles front-end is similar to the channels with the following differences. The keyword newChannel is replaced with newOracle, run is a keyword, and channel and out are not keywords.

The input file consists of a list of declarations followed by an oracle definition or an equivalence query:

\[
\text{⟨declaration⟩}* \text{ process (odef)}
\text{⟨declaration⟩}* \text{ equivalence (odef) ⟨odef⟩ [public_vars seq ⟨ident⟩]}
\text{⟨declaration⟩} \text{ query equiv[⟨ident⟩[⟨ident⟩]]}
\text{⟨omode⟩} \text{ [1 ... 1⟨omode⟩] <=(?)=> [1n] [Seq+⟨option⟩]1 ⟨ogroup⟩ [1 ... 1⟨ogroup⟩]}
\]

35
\[
\langle \text{obody} \rangle ::= \text{run} \langle \text{id} \rangle[(\text{seq} \langle \text{term} \rangle)]
\]

\[
| \langle \text{obody} \rangle
| \text{yield}
| \text{event} \langle \text{id} \rangle[(\text{seq} \langle \text{term} \rangle)] [; \langle \text{obody} \rangle]
| \text{event_abort} \langle \text{id} \rangle
| \text{new} \langle \text{id} \rangle; \langle \text{id} \rangle[(\langle \text{term} \rangle)]; \langle \text{obody} \rangle]
| \langle \text{id} \rangle[\langle \text{id} \rangle] <= \langle \text{term} \rangle[; \langle \text{obody} \rangle]
| \text{let} \langle \text{pattern} \rangle = \langle \text{term} \rangle [\text{in} \langle \text{obody} \rangle [\text{else} \langle \text{obody} \rangle]]
| \text{if} \langle \text{cond} \rangle \text{then} \langle \text{obody} \rangle [\text{else} \langle \text{obody} \rangle]
| \text{find}[\langle \text{unique} \rangle] (\text{findbranch}) (\text{orfind} (\text{findbranch}))^* [\text{else} \langle \text{obody} \rangle]
| \text{insert} \langle \text{id} \rangle[\text{seq} \langle \text{term} \rangle]; \langle \text{obody} \rangle]
| \text{get} \langle \text{id} \rangle[\text{seq} \langle \text{pattern} \rangle] [\text{suchthat} \langle \text{term} \rangle] \text{in} \langle \text{obody} \rangle [\text{else} \langle \text{obody} \rangle]
| \text{return} \langle \text{seq} \langle \text{term} \rangle \rangle; \langle \text{odef} \rangle]
\]

\[
\langle \text{findbranch} \rangle ::= \text{seq} \langle \text{id} \rangle[\text{bound}] \text{suchthat} \langle \text{cond} \rangle \text{then} \langle \text{obody} \rangle
\]

\[
\langle \text{odef} \rangle ::= \text{run} \langle \text{id} \rangle[(\text{seq} \langle \text{term} \rangle)]
\]

\[
| \langle \text{odef} \rangle
| 0
| \langle \text{odef} \rangle | \langle \text{odef} \rangle
| ![\langle \text{id} \rangle <= \langle \text{id} \rangle](\langle \text{id} \rangle \langle \text{odef} \rangle
| \text{foreach} \langle \text{id} \rangle <= \langle \text{id} \rangle \text{do} \langle \text{odef} \rangle
| \langle \text{id} \rangle[\text{seq} \langle \text{pattern} \rangle] := \langle \text{obody} \rangle
\]

Figure 8: Grammar for processes (oracles front-end)
The syntax of processes is given in Figure 8. The calculus distinguishes two kinds of processes: oracle definitions (odef) define new oracles; oracle bodies (obody) return a result after executing some internal computations. When a process (oracle definition or oracle body) is an identifier, it is substituted with its value defined by a let declaration.

The oracle definition run proc$(M_1, \ldots, M_n)$ is replaced with $P\{M_1/x_1, \ldots, M_n/x_n\}$ when proc is declared by let proc$(x_1 : T_1, \ldots, x_n : T_n) = P$, where $P$ is an oracle definition. The terms $M_1, \ldots, M_n$ must contain only variables, replication indices, and function applications.

The oracle definition $O(p_1, \ldots, p_n) := P$ defines an oracle $O$ taking arguments $p_1, \ldots, p_n$, and returning the result of the oracle body $P$. The patterns $p_1, \ldots, p_n$ are as in the let construct above, except that variables in $p$ that are not under a function symbol $f(\ldots)$ must be declared with their type. The other oracle definitions are similar to input processes in the channels front-end.

When an oracle $O$ is defined under foreach $i_1 \Leftarrow N_1, \ldots, \text{foreach } i_n \Leftarrow N_n$, it also implicitly defines $O[i_1, \ldots, i_n]$. Note that the construct newOracle $c; Q$ used in research papers is absent from the implementation: this construct is useful in the proof of soundness of CryptoVerif, but not essential for encoding games that CryptoVerif manipulates.

Let us now describe oracle bodies:

- run proc$(M_1, \ldots, M_n)$ is replaced with let $x_1 = M_1$ in ... let $x_n = M_n$ in $P$ when proc is declared by let proc$(x_1 : T_1, \ldots, x_n : T_n) = P$, where $P$ is an oracle body.
- yield terminates the oracle, returning control to the caller.
- return $(N_1, \ldots, N_l); Q$ terminates the oracle, returning the result of the terms $N_1, \ldots, N_l$. Then, it makes available the oracles defined in $Q$.
- The other oracle bodies are similar to output processes in the channels front-end.

In return $(M_1, \ldots, M_n)$. $M_j$ must be of a bitstring type $T_j$ for all $j \leq n$ and that return instruction is said to be of type $T_1 \times \ldots \times T_n$. All return instructions in an oracle body $P$ (excluding return instructions that occur in oracle definitions $Q$) in processes of the form return$(M_1, \ldots, M_n); Q$ must be of the same type, and that type is said to be the type of the oracle body $P$. For each oracle definition $O(p_1, \ldots, p_n) := P$ under foreach $i_1 \Leftarrow N_1, \ldots, \text{foreach } i_n \Leftarrow N_n$, the oracle $O$ is said to be of type $[1, N_1] \times \ldots \times [1, N_n] \rightarrow T_1' \times \ldots \times T_m' \rightarrow T_1 \times \ldots \times T_n$ where $p_j$ is of type $T_j'$ for all $j \leq m$ and $P$ is of type $T_1 \times \ldots \times T_n$. When an oracle has several definitions, it must be of the same type for all its definitions. Furthermore, definitions of the same oracle $O$ must not occur on both sides of a parallel composition $Q \parallel Q'$ (so that several definitions of the same oracle cannot be simultaneously available). An oracle $O$ must not occur under a definition of the same oracle $O$ in the syntax tree, and oracles defined in different branches of if, find, let, get must have compatible structures (oracles with the same name must occur at the same place in the sequence of possible oracle calls). The other constructs are typed as in the channels front-end.

The channel seq+ (ident), declaration is removed, since channels do not exist in the oracles front-end.

In probability formulas (Figure 4), time(out ...) and time(in $n$) are removed and time(newChannel) is replaced with time(newOracle). time(newOracle) is the maximum time to create a new private oracle.

5 Summary of the Main Differences between the two Front-ends

The main difference between the two front-ends is that the oracles front-end uses oracles while the channels front-end uses channels. So we have essentially the following correspondence:

<table>
<thead>
<tr>
<th>channels</th>
<th>oracles</th>
</tr>
</thead>
<tbody>
<tr>
<td>input process</td>
<td>oracle definition</td>
</tr>
<tr>
<td>output process</td>
<td>oracle body</td>
</tr>
<tr>
<td>newChannel $c$</td>
<td>newOracle $O$</td>
</tr>
<tr>
<td>in($c$, $(x_1 : T_1, \ldots, x_l : T_l)$); $P$</td>
<td>$O(x_1 : T_1, \ldots, x_l : T_l) := P$</td>
</tr>
<tr>
<td>out($c$, $(M_1, \ldots, M_l)$); $Q$</td>
<td>return$(M_1, \ldots, M_l); Q$</td>
</tr>
</tbody>
</table>
The `newChannel` or `newOracle` instruction does not appear in processes, but appears in the evaluation time of contexts. In the `channels` front-end, channels must be declared by a `channel` declaration. There is no such declaration in the `oracles` front-end.

Finally, both front-ends accept two syntaxes for replication, generation of random numbers, and assignments. However, the default syntax for the display differs:

<table>
<thead>
<tr>
<th>display in channels</th>
<th>display in oracles</th>
</tr>
</thead>
<tbody>
<tr>
<td>$!i:N Q$</td>
<td>$\text{foreach } i:N \text{ do } Q$</td>
</tr>
<tr>
<td><code>new x:T; P</code></td>
<td>$x \leftarrow R T; P$</td>
</tr>
<tr>
<td><code>let x:T = M in P</code></td>
<td>$x:T \leftarrow M; P$</td>
</tr>
</tbody>
</table>

The assignment $x:T \leftarrow M$ can be used only for assigning a variable; when a pattern occurs instead of the variable $x$, one has to use the `let` instruction.

## 6 Predefined cryptographic primitives

A number of standard cryptographic primitives are predefined in CryptoVerif. The definitions of these primitives are given as macros in the library file `default.csvl` (or `default.ocvl` for the `oracles` front-end) that is automatically loaded at startup. The user does not need to redefine these primitives, he can just expand the corresponding macro. The examples contained in the library can be used as a basis in order to build definitions of new primitives, by copying and modifying them as desired. Here is a list of the predefined primitives.

- **`expand IND_CPA_sym_enc(key, cleartext, ciphertext, enc, dec, injbot, Z, Penc)`**, defines a IND-CPA (indistinguishable under chosen plaintext attacks) probabilistic symmetric encryption scheme.  
  `key` is the type of keys, must be bounded (to be able to generate random numbers from it, and to talk about the runtime of `enc` without mentioning the length of the key), typically fixed and large.  
  `cleartext` is the type of cleartexts.  
  `ciphertext` is the type of ciphertexts.  
  `enc(cleartext, key) : ciphertext` is the encryption function. Internally, it generates random coins, so that it is probabilistic.  
  `dec(ciphertext, key) : bitstringbot` is the decryption function; it returns `bottom` when decryption fails.  
  `injbot(cleartext) : bitstringbot` is the natural injection from `cleartext` to `bitstringbot`.  
  `Z(cleartext) : cleartext` is the function that returns for each cleartext a cleartext of the same length consisting only of zeros.  
  `Penc(t, N, l)` is the probability of breaking the IND-CPA property in time $t$ for one key and $N$ encryption queries with cleartexts of length at most $l$.

The types `key`, `cleartext`, `ciphertext` and the probability `Penc` must be declared before this macro is expanded. The functions `enc`, `dec`, `injbot`, and `Z` are declared by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

This macro defines the equivalence named `ind_cpa(enc)` for use in the `crypto` command in interactive proofs (see Section 7).

- **`expand IND_CPA_sym_enc_all_args(key, cleartext, ciphertext, enc_seed, enc, enc_r, enc_r', dec, injbot, Z, Penc)`**, is similar to the above, with three additional arguments.  
  `enc_seed` is the type of random coins for encryption, must be bounded.  
  `enc_r(cleartext, key, enc_seed) : ciphertext` is the encryption function that takes coins as argument (instead of generating them internally).  
  `enc_r'$ is the symbol that replaces `enc_r` after game transformation.
• expand IND_CPA_sym_enc_nonce(key, cleartext, ciphertext, nonce, enc, dec, injbot, Z, Penc). defines a IND-CPA (indistinguishable under chosen plaintext attacks) probabilistic symmetric encryption scheme using a nonce (which must have a different value in each call to encryption) instead of random coins generated by encryption.

key is the type of keys, must be bounded (to be able to generate random numbers from it, and to talk about the runtime of enc without mentioning the length of the key), typically fixed and large.

cleartext is the type of cleartexts.
ciphertext is the type of ciphertexts.
nonce is the type of nonces.

enc(cleartext, key, nonce): ciphertext is the encryption function.

dec(ciphertext, key) : bitstringbot is the decryption function; it returns bottom when decryption fails.
injbot(cleartext): bitstringbot is the natural injection from cleartext to bitstringbot.

Z(cleartext): cleartext is the function that returns for each cleartext a cleartext of the same length consisting only of zeroes.

Penc(t, N, l) is the probability of breaking the IND-CPA property in time t for one key and N encryption queries with cleartexts of length at most l.

The types key, cleartext, ciphertext, nonce and the probability Penc must be declared before this macro is expanded. The functions enc, dec, injbot, and Z are declared by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

This macro defines the equivalence named ind_cpa(enc) for use in the crypto command in interactive proofs (see Section 7).

• expand IND_CPA_sym_enc_nonce_all_args(key, cleartext, ciphertext, nonce, enc, enc’, dec, injbot, Z, Penc). is similar to the above, with one additional argument: enc’ is the symbol that replaces enc after game transformation.

• expand IND_CPA_INT_CTX_sym_enc(key, cleartext, ciphertext, enc, dec, injbot, Z, Penc, Pencctxt). defines a IND-CPA (indistinguishable under chosen plaintext attacks) and INT-CTXT (ciphertext integrity) probabilistic symmetric encryption scheme.

key is the type of keys, must be bounded (to be able to generate random numbers from it, and to talk about the runtime of enc without mentioning the length of the key), typically fixed and large.

cleartext is the type of cleartexts.
ciphertext is the type of ciphertexts.

enc(cleartext, key): ciphertext is the encryption function. Internally, it generates random coins, so that it is probabilistic.

dec(ciphertext, key) : bitstringbot is the decryption function; it returns bottom when decryption fails.
injbot(cleartext): bitstringbot is the natural injection from cleartext to bitstringbot.

Z(cleartext): cleartext is the function that returns for each cleartext a cleartext of the same length consisting only of zeroes.

Penc(t, N, l) is the probability of breaking the IND-CPA property in time t for one key and N encryption queries with cleartexts of length at most l.

Pencctxt(t, N, N’, l, l’) is the probability of breaking the INT-CTXT property in time t for one key, N encryption queries, N’ decryption queries with cleartexts of length at most l and ciphertexts of length at most l’.
The types key, cleartext, ciphertext and the probabilities Penc and Pencctxt must be declared before this macro is expanded. The functions enc, dec, injbot, and Z are declared by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

This macro defines the equivalences named ind_cpa(enc), int_ctxt(enc), and int_ctxt_corrupt(enc) for use in the crypto command (see Section 7). The first equivalence corresponds to the IND-CPA property, the last two to the INT-CTXT property. The equivalence int_ctxt_corrupt(enc) is used when the key may be corrupted. It is applied only manually. The equivalence int_ctxt(enc) should generally be applied before ind_cpa(enc), because int_ctxt(enc) eliminates the decryption oracle.

- **expand IND_CPA_INT_CTXT_sym_enc_all_args(key, cleartext, ciphertext, enc_seed, enc, enc_r, enc_r′, dec, injbot, Z, Penc, Pencctxt),** is similar to the above, with three additional arguments.
  
  enc_seed is the type of random coins for encryption, must be bounded.
  
  enc_r(cleartext, key, enc_seed) : ciphertext is the encryption function that takes coins as argument (instead of generating them internally).
  
  enc_r′ is the symbol that replaces enc_r after game transformation.

- **expand IND_CPA_INT_CTXT_sym_enc_nonce(key, cleartext, ciphertext, nonce, enc, dec, injbot, Z, Penc, Pencctxt),** defines an IND-CPA (indistinguishable under chosen plaintext attacks) and INT-CTXT (ciphertext integrity) probabilistic symmetric encryption scheme using a nonce (which must have a different value in each call to encryption) instead of random coins generated by encryption.
  
  key is the type of keys, must be bounded (to be able to generate random numbers from it, and to talk about the runtime of enc without mentioning the length of the key), typically fixed and large.
  
  cleartext is the type of cleartexts.
  
  ciphertext is the type of ciphertexts.
  
  nonce is the type of nonces.
  
  enc(cleartext, key, nonce) : ciphertext is the encryption function.
  
  dec(ciphertext, key, nonce) : bitstringbot is the decryption function; it returns bottom when decryption fails.
  
  injbot(cleartext) : bitstringbot is the natural injection from cleartext to bitstringbot.
  
  Z(cleartext) : cleartext is the function that returns for each cleartext a cleartext of the same length consisting only of zeroes.
  
  Penc(t, N, l) is the probability of breaking the IND-CPA property in time t for one key and N encryption queries with cleartexts of length at most l.
  
  Pencctxt(t, N, N′, l, l′) is the probability of breaking the INT-CTXT property in time t for one key, N encryption queries, N′ decryption queries with cleartexts of length at most l and ciphertexts of length at most l′.

The types key, cleartext, ciphertext, nonce and the probabilities Penc and Pencctxt must be declared before this macro is expanded. The functions enc, dec, injbot, and Z are declared by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

This macro defines the equivalences named ind_cpa(enc), int_ctxt(enc), and int_ctxt_corrupt(enc) for use in the crypto command (see Section 7). The first equivalence corresponds to the IND-CPA property, the last two to the INT-CTXT property. The equivalence int_ctxt_corrupt(enc) is used when the key may be corrupted. It is applied only manually. The equivalence int_ctxt(enc) should generally be applied before ind_cpa(enc), because int_ctxt(enc) eliminates the decryption oracle.

- **expand IND_CPA_INT_CTXT_sym_enc_nonce_all_args(key, cleartext, ciphertext, nonce, enc, enc′, dec, injbot, Z, Penc, Pencctxt),** is similar to the above, with one additional argument: enc′ is the symbol that replaces enc after game transformation.

40
expand Aead\((key, cleartext, ciphertext, add\_data, enc, dec, injbot, Z, Penc, Pencctxt)\). defines an authenticated encryption scheme with additional data.

\(key\) is the type of keys, must be bounded (to be able to generate random numbers from it, and to talk about the runtime of \(enc\) without mentioning the length of the key), typically fixed and large.

cleartext is the type of cleartexts.

ciphertext is the type of ciphertexts.

add\_data is the type of additional data.

\(enc\)(cleartext, add\_data, key) : ciphertext is the encryption function. Internally, it generates random coins, so that it is probabilistic.

\(dec\)(ciphertext, add\_data, key) : bitstringbot is the decryption function; it returns bottom when decryption fails.

\(inj\)(cleartext) : bitstringbot is the natural injection from cleartext to bitstringbot.

\(Z\)(cleartext) : cleartext is the function that returns for each cleartext a cleartext of the same length consisting only of zeros.

\(Penc\)(t, \(N\), \(l\)) is the probability of breaking the IND-CPA property in time \(t\) for one key and \(N\) encryption queries with cleartexts of length at most \(l\).

\(Penctxt\)(t, \(N\), \(l\)', \(l\)', \(ld\)', \(ld\)') is the probability of breaking the INT-CTXT property in time \(t\) for one key, \(N\) encryption queries, \(N\)' decryption queries with cleartexts of length at most \(l\) and ciphertexts of length at most \(l\)', additional data for encryption of length at most \(ld\)', and additional data for decryption of length at most \(ld\)'.

The types \(key\), cleartext, ciphertext, add\_data and the probabilities \(Penc\) and \(Penctxt\) must be declared before this macro is expanded. The functions \(enc\), \(dec\), \(inj\), and \(Z\) are declared by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

This macro defines the equivalences named \(\text{ind\_cpa}(enc)\), \(\text{int\_ctxt}(enc)\), and \(\text{int\_ctxt\_corrupt}(enc)\) for use in the crypto command (see Section [7]). The first equivalence corresponds to the IND-CPA property, the last two to the INT-CTXT property. The equivalence \(\text{int\_ctxt\_corrupt}(enc)\) is used when the key may be corrupted. It is applied only manually. The equivalence \(\text{int\_ctxt}(enc)\) should generally be applied before \(\text{ind\_cpa}(enc)\), because \(\text{int\_ctxt}(enc)\) eliminates the decryption oracle.

\(\text{expand\ AEAD\ all\ args}(key, cleartext, ciphertext, add\_data, enc\_seed, enc, enc\_r, enc\_r', dec, injbot, Z, Penc, Penctxt)\), is similar to the above, with three additional arguments.

\(enc\_seed\) is the type of random coins for encryption, must be bounded.

\(enc\_r\)(cleartext, add\_data, key, enc\_seed) : ciphertext is the encryption function that takes coins as argument (instead of generating them internally).

\(enc\_r'\) is the symbol that replaces \(enc\_r\) after game transformation.

\(\text{expand\ AEAD\ nonce}(key, cleartext, ciphertext, add\_data, nonce, enc, dec, injbot, Z, Penc, Penctxt)\), defines an authenticated encryption scheme with additional data, using a nonce that must have a different value in each call to encryption. A typical example is AES-GCM.

\(key\) is the type of keys, must be bounded (to be able to generate random numbers from it, and to talk about the runtime of \(enc\) without mentioning the length of the key), typically fixed and large.

cleartext is the type of cleartexts.

ciphertext is the type of ciphertexts.

add\_data is the type of additional data.

\(nonce\) is the type of nonces.
enc(cleartext, add_data, key, nonce) : ciphertext is the encryption function.
dec(ciphertext, add_data, key, nonce) : bitstringbot is the decryption function; it returns bottom when decryption fails.
injbot(cleartext) : bitstringbot is the natural injection from cleartext to bitstringbot.
Z(cleartext) : cleartext is the function that returns for each cleartext a cleartext of the same length consisting only of zeroes.
Penc(t, N, l) is the probability of breaking the IND-CPA property in time t for one key and N encryption queries with cleartexts of length at most l.
Pencctxt(t, N, N', l', ld, ld') is the probability of breaking the INT-CTXT property in time t for one key. N encryption queries, N' decryption queries with cleartexts of length at most l and ciphertexts of length at most l', additional data for encryption of length at most ld, and additional data for decryption of length at most ld'.

The types key, cleartext, ciphertext, add_data, nonce and the probabilities Penc and Pencctxt must be declared before this macro is expanded. The functions enc, dec, injbot, and Z are declared by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

This macro defines the equivalences named ind$\_cpa$($\text{enc}$), int\_ctxt($\text{enc}$), and int\_ctxt\_corrupt($\text{enc}$) for use in the crypto command (see Section 7). The first equivalence corresponds to the IND-CPA property, the last two to the INT-CTXT property. The equivalence int\_ctxt\_corrupt($\text{enc}$) is used when the key may be corrupted. It is applied only manually. The equivalence int\_ctxt($\text{enc}$) should generally be applied before ind$\_cpa$($\text{enc}$), because int\_ctxt($\text{enc}$) eliminates the decryption oracle.

- expand AEAD\_nonce\_all\_args(key, cleartext, ciphertext, add_data, nonce, enc, enc', dec, injbot, Z, Penc, Pencctxt), is similar to the above with one additional argument.

enc' is the symbol that replaces enc after game transformation.

- expand IND\_dollar\_CPA\_sys\_enc(key, cleartext, ciphertext, cipher\_stream, enc, dec, injbot, Z, enc\_len, truncate, Penc).
- expand IND\_dollar\_CPA\_sys\_enc\_all\_args(key, cleartext, ciphertext, enc\_seed, cipher\_stream, enc, enc\_r, dec, injbot, Z, enc\_len, truncate, Penc).
- expand IND\_dollar\_CPA\_sys\_enc\_nonce(key, cleartext, ciphertext, nonce, cipher\_stream, enc, dec, injbot, Z, enc\_len, truncate, Penc).
- expand IND\_dollar\_CPA\_INT\_CTXT\_sys\_enc(key, cleartext, ciphertext, cipher\_stream, enc, dec, injbot, Z, enc\_len, truncate, Penc, Pencctxt).
- expand IND\_dollar\_CPA\_INT\_CTXT\_sys\_enc\_all\_args(key, cleartext, ciphertext, enc\_seed, cipher\_stream, enc, enc\_r, dec, injbot, Z, enc\_len, truncate, Penc, Pencctxt).
- expand IND\_dollar\_CPA\_INT\_CTXT\_sys\_enc\_nonce(key, cleartext, ciphertext, nonce, cipher\_stream, enc, dec, injbot, Z, enc\_len, truncate, Penc, Pencctxt).
- expand AEAD\_IND\_dollar\_CPA\_key(key, cleartext, ciphertext, add_data, cipher\_stream, enc, dec, injbot, Z, enc\_len, truncate, Penc, Pencctxt).
- expand AEAD\_IND\_dollar\_CPA\_all\_args(key, cleartext, ciphertext, add_data, enc\_seed, cipher\_stream, enc, enc\_r, dec, injbot, Z, enc\_len, truncate, Penc, Pencctxt).
- expand AEAD\_IND\_dollar\_CPA\_nonce(key, cleartext, ciphertext, add_data, nonce, cipher\_stream, enc, dec, injbot, Z, enc\_len, truncate, Penc, Pencctxt).

define macros similar to the ones above, but with the IND$\_dollar$-CPA property instead of IND-CPA. IND$\_dollar$-CPA means that the length of the ciphertext only depends on the length of the cleartext, and that the ciphertext is indistinguishable from a random bitstring of the same length. In comparison with the previous macros, they do not have the primed encryption argument (enc\_r' or enc'), so the all\_args variant disappears for encryptions with a nonce since enc' was the only additional argument. They additionally have the following arguments:
cipher\_stream is the type of unbounded streams (must be nonuniform).
\textit{enc\_len(cleartext)} : ciphertext is a function that returns, for each bitstring \(x\), a bitstring of the same length as the encryption of \(x\), consisting only of zeroes.

\textit{truncate(cipher\_stream, ciphertext)} : ciphertext is the function such that \(\text{truncate}(s, x)\) is the truncation of \(s\) to the length of \(x\), where \(s\) is a stream of unbounded length.

The type \textit{cipher\_stream} must be declared before these macros are expanded. The functions \textit{enc\_len} and \textit{truncate} are declared by these macros. They must not be declared elsewhere, and they can be used only after expanding one of the macros.

These macros define the equivalence \texttt{imdollar\_cpa(enc)} instead of \texttt{ind\_cpa(enc)}.

- \texttt{expand IND\_CCA2\_sym\_enc(key, cleartext, ciphertext, enc, dec, injbot, Z, Penc)} defines a IND-CCA2 (indistinguishable under adaptive chosen ciphertext attacks) probabilistic symmetric encryption scheme.

  \textit{key} is the type of keys, must be \texttt{bounded} (to be able to generate random numbers from it, and to talk about the runtime of \texttt{enc} without mentioning the length of the key), typically \texttt{fixed} and \texttt{large}.

  \textit{cleartext} is the type of cleartexts.

  \textit{ciphertext} is the type of ciphertexts.

  \textit{enc(cleartext, key)} : ciphertext is the encryption function. Internally, it generates random coins, so that it is probabilistic.

  \textit{dec(ciphertext, key)} : \texttt{bitstringbot} is the decryption function; it returns \texttt{bottom} when decryption fails.

  \textit{injbot(cleartext)} : \texttt{bitstringbot} is the natural injection from \textit{cleartext} to \texttt{bitstringbot}.

  \textit{Z(cleartext)} : \textit{cleartext} is the function that returns for each cleartext a cleartext of the same length consisting only of zeroes.

  \textit{Penc(t, N, Nu, N', l, l')} is the probability of breaking the IND-CCA2 property in time \(t\) for one key, \(N\) encryption queries that are different in both sides of the IND-CCA2 equivalence, \(Nu\) encryption queries that are the same in both sides of the IND-CCA2 equivalence, \(N'\) decryption queries with cleartexts of length at most \(l\) and ciphertexts of length at most \(l'\).

  The types \textit{key}, \textit{cleartext}, \textit{ciphertext} and the probability \textit{Penc} must be declared before this macro is expanded. The functions \textit{enc}, \textit{dec}, \textit{injbot}, and \textit{Z} are declared by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

  This macro defines the equivalences named \texttt{ind\_cca2(enc)} and \texttt{ind\_cca2\_partial(enc)}, for use in the \texttt{crypto} command (see Section 7). While the equivalence \texttt{ind\_cca2(enc)} replaces all cleartexts with zeroes, the equivalence \texttt{ind\_cca2\_partial(enc)} replaces only some of them with zeroes. The latter equivalence can be applied only manually. The user should map the occurrences of encryption that he wants to transform to oracle \texttt{Oenc}, the ones he wants to leave unchanged to oracle \texttt{Oenc\_unchanged}, and the ones that have already been transformed by a previous application of this equivalence to oracle \texttt{Oenc\_unchanged}'.

- \texttt{expand IND\_CCA2\_sym\_enc\_all\_args(key, cleartext, ciphertext, enc\_seed, enc, enc\_r, enc\_r', dec, dec', injbot, Z, Penc)} is similar to the above, with four additional arguments.

  \textit{enc\_seed} is the type of random coins for encryption, must be \texttt{bounded}.

  \textit{enc\_r(cleartext, key, enc\_seed)} : ciphertext is the encryption function that takes coins as argument (instead of generating them internally).

  \textit{enc\_r'} and \textit{dec'} are the symbols that replace \textit{enc\_r} and \textit{dec} respectively after game transformation.

- \texttt{expand INT\_PTXT\_sym\_enc(key, cleartext, ciphertext, enc, dec, injbot, Penc\_ptxt)} defines an INT-PTXT (plaintext integrity) probabilistic symmetric encryption scheme.

  \textit{key} is the type of keys, must be \texttt{bounded} (to be able to generate random numbers from it, and to talk about the runtime of \texttt{enc} without mentioning the length of the key), typically \texttt{fixed} and \texttt{large}.

43
\textit{cleartext} is the type of cleartexts.
\textit{ciphertext} is the type of ciphertexts.

\texttt{enc(cleartext, key)} : \textit{ciphertext} is the encryption function. Internally, it generates random coins, so that it is probabilistic.

\texttt{dec(ciphertext, key)} : \texttt{bitstringbot} is the decryption function; it returns bottom when decryption fails.

\texttt{injbot(cleartext)} : \texttt{bitstringbot} is the natural injection from \textit{cleartext} to \texttt{bitstringbot}.

\texttt{Penc}(t, N, N', N' \prime, l, l') is the probability of breaking the INT-PTXT property in time \( t \) for one key, \( N \) encryption queries, \( N' \) decryption queries that are modified by the transformation, and \( N' \prime \) decryption queries that are left unchanged by the transformation, with cleartexts of length at most \( l \) and ciphertexts of length at most \( l' \).

The types \texttt{key}, \texttt{cleartext}, \texttt{ciphertext} and the probability \texttt{Penc} must be declared before this macro is expanded. The functions \texttt{enc}, \texttt{dec}, and \texttt{injbot} are declared by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

This macro defines the equivalences named \texttt{int\_ptxt(enc)} and \texttt{int\_ptxt\_corrupt\_partial(enc)}, for use in the crypto command (see Section 7). While the equivalence \texttt{ind\_ptxt(enc)} replaces all decryption with lookups in encryption queries, the equivalence \texttt{ind\_ptxt\_corrupt\_partial(enc)} may replace only some of them and supports corruption of the key. The latter equivalence can be applied only manually. To transform only some occurrences of decryption, the user should map the occurrences of decryption that he wants to transform to oracle \texttt{Odec}, the ones he wants to leave unchanged to oracle \texttt{Odec\_unchanged}, and the ones that have already been transformed by a previous application of this equivalence to oracle \texttt{Odec\_unchanged}.

- \texttt{expand INT\_PTXT\_sym\_enc\_all\_args(key, cleartext, ciphertext, enc\_seed, enc, enc\_r, dec, dec', injbot, Penc)} is similar to the above, with three additional arguments.

\texttt{enc\_seed} is the type of random coins for encryption, must be bounded.

\texttt{enc\_r(cleartext, key, enc\_seed)} : \textit{ciphertext} is the encryption function that takes coins as argument (instead of generating them internally).

\texttt{dec'} is the symbol that replaces \texttt{dec} after game transformation.

- \texttt{expand IND\_CCA2\_INT\_PTXT\_sym\_enc(key, cleartext, ciphertext, enc, dec, injbot, Z, Penc, Pencptxt)} defines a IND-CCA2 (indistinguishable under adaptive chosen ciphertext attacks) and INT-PTXT (plaintext integrity) probabilistic symmetric encryption scheme.

\texttt{key} is the type of keys, must be bounded (to be able to generate random numbers from it, and to talk about the runtime of \texttt{enc} without mentioning the length of the key), typically \texttt{fixed} and \texttt{large}.

\textit{cleartext} is the type of cleartexts.
\textit{ciphertext} is the type of ciphertexts.

\texttt{enc(cleartext, key)} : \textit{ciphertext} is the encryption function. Internally, it generates random coins, so that it is probabilistic.

\texttt{dec(ciphertext, key)} : \texttt{bitstringbot} is the decryption function; it returns bottom when decryption fails.

\texttt{injbot(cleartext)} : \texttt{bitstringbot} is the natural injection from \textit{cleartext} to \texttt{bitstringbot}.

\texttt{Z(cleartext)} : \textit{cleartext} is the function that returns for each cleartext a cleartext of the same length consisting only of zeros.

\texttt{Penc}(t, N, N', N' \prime, l, l') is the probability of breaking the IND-CCA2 property in time \( t \) for one key, \( N \) encryption queries that are different in both sides of the IND-CCA2 equivalence, \( N' \) encryption queries that are the same in both side of the IND-CCA2 equivalence, \( N' \prime \) decryption queries with cleartexts of length at most \( l \) and ciphertexts of length at most \( l' \).
Penctxt(t, N, N', Nu', l, l') is the probability of breaking the INT-PTXT property in time t for one key, N encryption queries, N' decryption queries that are modified by the transformation, and Nu' decryption queries that are left unchanged by the transformation, with cleartexts of length at most l and ciphertexts of length at most l'.

The types \textit{key}, \textit{cleartext}, \textit{ciphertext} and the probabilities \textit{Penc} and \textit{Penctxt} must be declared before this macro is expanded. The functions \textit{enc}, \textit{dec}, \textit{injbot}, and \textit{Z} are declared by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

This macro defines the equivalences named \texttt{ind\_cca2(enc)}, \texttt{ind\_cca2\_after\_int\_ptxt(enc)}, \texttt{ind\_cca2\_partial(enc)}, \texttt{int\_ptxt(enc)}, \texttt{int\_ptxt\_after\_ind\_cca2(enc)}, and \texttt{int\_ptxt\_corrupt\_partial(enc)}, for use in the crypt command (see Section 7). The first three correspond to the IND-CCA2 property, the last three to the INT-PTXT property. The equivalence \texttt{ind\_cca2(enc)} can be applied before applying the INT-PTXT property, while \texttt{ind\_cca2\_after\_int\_ptxt(enc)} can be applied after applying the INT-PTXT property. Similarly, the equivalence \texttt{int\_ptxt(enc)} can be applied before applying the IND-CCA2 property, while \texttt{int\_ptxt\_after\_ind\_cca2(enc)} can be applied after applying the IND-CCA2 property.

The equivalences \texttt{ind\_cca2\_partial(enc)} and \texttt{int\_ptxt\_corrupt\_partial(enc)} may transform only some occurrences of encryption and/or decryption, and \texttt{int\_ptxt\_corrupt\_partial(enc)} supports corruption of the key. They can be applied only manually, in any order. For \texttt{ind\_cca2\_partial(enc)}, the user should map the occurrences of encryption that he wants to transform to oracle \texttt{Oenc} the ones he wants to leave unchanged to oracle \texttt{Oenc\_unchanged}. For \texttt{int\_ptxt\_partial(enc)}, the user should map the occurrences of decryption that he wants to transform to oracle \texttt{Odec} the ones he wants to leave unchanged to oracle \texttt{Odec\_unchanged}.

CryptoVerif often needs manual guidance with this property, because it does not know which property (IND-CCA2 or INT-PTXT) to apply first. Moreover, when empty plaintexts are not allowed, IND-CCA2 and INT-PTXT is equivalent to IND-CPA and INT-CTXT, which is much easier to use for CryptoVerif, so we recommend using the latter property when possible.

- \texttt{expand \texttt{IND\_CCA2\_INT\_PTXT\_sym\_enc\_all\_args(key, cleartext, ciphertext, enc\_seed, enc, enc\_r, enc\_r', dec, dec', injbot, Z, Penc, Penctxt)}} is similar to the above, with four additional arguments.
  - \texttt{enc\_seed} is the type of random coins for encryption, must be bounded.
  - \texttt{enc\_r(cleartext, key, enc\_seed)}: \texttt{ciphertext} is the encryption function that takes coins as argument (instead of generating them internally).
  - \texttt{enc\_r'} and \texttt{dec'} are the symbols that replace \texttt{enc\_r} and \texttt{dec} respectively after game transformation.

- \texttt{expand \texttt{SPRP\_cipher(key, blocksize, enc, dec, Penc)}} defines a SPRP (super-pseudo-random permutation) deterministic symmetric encryption scheme.
  - \texttt{key} is the type of keys, must be bounded (to be able to generate random numbers from it), and to talk about the runtime of \texttt{enc} without mentioning the length of the key), typically fixed and large.
  - \texttt{blocksize} is the type of cleartexts and ciphertexts, must be fixed and large. (The modeling of SPRP block ciphers is not perfect in that, in order to encrypt a new message, one chooses a fresh random number, not necessarily different from previously generated random numbers. Then CryptoVerif needs to eliminate collisions between those random numbers, so \texttt{blocksize} must really be large.)
  - \texttt{enc(blocksize, key)}: \texttt{blocksize} is the encryption function.
  - \texttt{dec(blocksize, key)}: \texttt{blocksize} is the decryption function.

\texttt{Penc(t, N, N')} is the probability of breaking the SPRP property in time t for one key, N encryption queries, and N' decryption queries.

The types \textit{key}, \textit{blocksize} and the probability \textit{Penc} must be declared before this macro is expanded. The functions \textit{enc} and \textit{dec} are declared by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.
This macro defines equivalences named sprp(enc) and sprp_partial(enc) for use in the crypto command (see Section 7). These equivalences are generated via equiv ... special: the crypto command therefore supports special arguments collisions_LHS and, for sprp_partial(enc), collision matrix. See the explanation of the collisions_LHS argument, the collision matrix, and the oracles present in these equivalences in the documentation of equiv ... special.

- expand PRP_cipher(key, blocksize, enc, dec, Penc). defines a PRP (pseudo-random permutation) deterministic symmetric encryption scheme.

  key is the type of keys, must be bounded (to be able to generate random numbers from it, and to talk about the runtime of enc without mentioning the length of the key), typically fixed and large.

  blocksize is the type of cleartexts and ciphertexts, must be fixed and large. (The modeling of PRP block ciphers is not perfect in that, in order to encrypt a new message, one chooses a fresh random number, not necessarily different from previously generated random numbers. In other words, we model a PRF rather than a PRP, and apply the PRF/PRP switching lemma to make sure that this is sound. Then CryptoVerif needs to eliminate collisions between those random numbers, so blocksize must really be large.)

  enc(blocksize, key) : blocksize is the encryption function.

  dec(blocksize, key) : blocksize is the decryption function.

  Penc(t, N) is the probability of breaking the PRP property in time t for one key and N encryption queries.

  The types key, blocksize and the probability Penc must be declared before this macro is expanded. The functions enc and dec are declared by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

  This macro defines equivalences named prp(enc) and prp_partial(enc) for use in the crypto command (see Section 7). These equivalences are generated via equiv ... special: the crypto command therefore supports special arguments collisions_LHS and, for prp_partial(enc), collision matrix. See the explanation of the collisions_LHS argument, the collision matrix, and the oracles present in these equivalences in the documentation of equiv ... special.

- expand ICM_cipher(cipherkey, key, blocksize, enc, dec, enc_dec_oracle, qE, qD). defines a block cipher in the ideal cipher model.

  cipherkey is the type of keys that correspond to the choice of the scheme, must be bounded or nonuniform, typically fixed.

  key is the type of keys (typically large).

  blocksize is type of the input and output of the cipher, must be bounded or nonuniform (to be able to generate random numbers from it), typically fixed, and large. (The modeling of the ideal cipher model is not perfect in that, in order to encrypt a new message, one chooses a fresh random number, not necessarily different from previously generated random numbers. Then CryptoVerif needs to eliminate collisions between those random numbers, so blocksize must really be large.)

  enc(cipherkey, blocksize, key) : blocksize is the encryption function.

  dec(cipherkey, blocksize, key) : blocksize is the decryption function.

  enc_dec_oracle is a parametric process that allows the adversary to call the encryption and decryption functions. WARNING: the encryption and decryption functions take 2 keys as input: the key of type cipherkey that corresponds to the choice of the scheme, and the normal encryption/decryption key. The cipherkey must be chosen once and for all at the beginning of the game and the encryption and decryption oracles must be made available to the adversary, by including the process enc_dec_oracle(ck) where ck is the cipherkey.

  qE is the number of queries to the encryption oracle.

  qD is the number of queries to the decryption oracle.
The types cipherkey, key, blocksize must be declared before this macro is expanded. The functions enc, dec, the process enc_dec_oracle, and the parameters qE and qD are declared by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

This macro defines equivalences named icm(enc) and icm_partial(enc) for use in the crypto command (see Section 7). These equivalences are generated via equiv ... special; the crypto command therefore supports special arguments collisions_LHS and, for icm_partial(enc), collision matrix. See the explanation of the collisions_LHS argument, the collision matrix, and the oracles present in these equivalences in the documentation of equiv ... special.

- **expand SUF_CMA_det_mac**(mkey, macinput, macres, mac, check, Pmac), defines an SUF-CMA (strongly unforgeable under chosen message attacks) deterministic MAC (message authentication code).

  The difference between a UF-CMA (unforgeable under chosen message attacks) MAC and a SUF-CMA MAC is that, for a UF-CMA MAC, the adversary may easily forge a new MAC for a message for which he has already seen a MAC. Such a forgery is guaranteed to be hard for a SUF-CMA MAC. For deterministic MACs, the verification can be done by recomputing the MAC, and in this case, an UF-CMA MAC is always SUF-CMA, so we model only SUF-CMA deterministic MACs. This macro transforms tests $mac(k, m) = m'$ into $check(k, m, m')$, so that the MAC verification can also be written $mac(k, m) = m'$.

  mkey is the type of keys, must be bounded (to be able to generate random numbers from it, and to talk about the runtime of mac without mentioning the length of the key), typically fixed and large.

  macinput is the type of inputs of MACs

  macres is the type of MACs.

  $mac$(macinput, mkey) : macres is the MAC function.

  $check$(macinput, mkey, macres) : bool is the verification function.

  $Pmac(t, N, N', N', l)$ is the probability of breaking the SUF-CMA property in time $t$ for one key, $N$ MAC queries, $N'$ verification queries modified by the transformation and $N'$ verification queries left unchanged by the transformation for messages of length at most $l$.

  The types mkey, macinput, macres and the probability Pmac must be declared before this macro is expanded. The functions mac, check are declared by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

  This macro defines the equivalences named suf_cma(mac), suf_cma_corrupt(mac), and suf_cma_corrupt_partial(mac), for use in the crypto command (see Section 7). All equivalences correspond to the SUF-CMA property, but the first one does not allow corruption of the secret keys while last two allow it. The last two equivalences are applied only manually, in particular because their automatic application can sometimes be done too early, when other transformations should first be done in order to eliminate uses of the secret keys. The equivalence suf_cma_corrupt_partial(mac) allows the user to transform only some occurrences of the MAC verification into a lookup in the MACed messages. The user should map the occurrences he wants to transform to the oracle Ocheck and the ones he does not want to transform to the oracle Ocheck_unchanged.

  - **expand SUF_CMA_det_mac_all_args**(mkey, macinput, macres, mac, mac', check, Pmac). is similar to the above, with one additional argument.

    mac' is the symbol that replaces mac after game transformation.

  - **expand UF_CMA_proba_mac**(mkey, macinput, macres, mac, check, Pmac). defines a UF-CMA (unforgeable under chosen message attacks) probabilistic MAC (message authentication code).

    The arguments are the same as for SUF_CMA_det_mac, but the mac function chooses random coins internally so that it is probabilistic, and the verification is not done by recomputing the MAC. This macro defines the equivalences named uf_cma(mac), uf_cma_corrupt(mac), and uf_cma_corrupt_partial(mac) for use in the crypto command (see Section 7), similarly to SUF_CMA_det_mac.
• expand UF_CMA_proba_mac_all_args(mkey, macinput, macres, mac_seed, mac, mac_r, mac_r', check, check', Pmac). is similar to the above, with four additional arguments.

  mac_seed is the type of random coins for MAC, must be bounded.

  mac_r(macinput, mkey, mac_seed) : macres is the MAC function that takes coins as argument (instead of generating them internally).

  mac_r' and check' are the symbols that replace mac_r and check respectively after game transformation.

• expand SUF_CMA_proba_mac(mkey, macinput, macres, mac, check, Pmac). defines a SUF-CMA (strongly unforgeable under chosen message attacks) probabilistic MAC (message authentication code). The arguments are the same as for SUF_CMA_det_mac, but the mac function chooses random coins internally so that it is probabilistic, and the verification is not done by recomputing the MAC. This macro defines the equivalences named suf_cma_corrupt(mac), suf_cma_corrupt_partial(mac), for use in the crypto command (see Section 7), similarly to SUF_CMA_det_mac.

• expand SUF_CMA_proba_mac_all_args(mkey, macinput, macres, mac_seed, mac, mac_r, mac_r', check, Pmac). is similar to the above, with three additional arguments.

  mac_seed is the type of random coins for MAC, must be bounded.

  mac_r(macinput, mkey, mac_seed) : macres is the MAC function that takes coins as argument (instead of generating them internally).

  mac_r' is the symbol that replaces mac_r after game transformation.

• expand IND_CCA2_public_key_enc(keyseed, pkey, skey, cleartext, ciphertext, skgen, pkgen, enc, dec, injbot, Z, Penc, Penccoll). defines a IND-CCA2 (indistinguishable under adaptive chosen ciphertext attacks) probabilistic public-key encryption scheme.

  keyseed is the type of key seeds, must be bounded (to be able to generate random numbers from it, and to talk about the runtime of pkgen without mentioning the length of the key), typically fixed and large.

  pkey is the type of public keys, must be bounded.

  skey is the type of secret keys, must be bounded.

  cleartext is the type of cleartexts.

  ciphertext is the type of ciphertexts.

  skgen(keyseed) : skey is the secret key generation function.

  pkgen(keyseed) : pkey is the public key generation function.

  enc(cleartext, pkey) : ciphertext is the encryption function. Internally, it generates random coins, so that it is probabilistic.

  dec(ciphertext, skey) : bitstringbot is the decryption function; it returns bottom when decryption fails.

  injbot(cleartext) : bitstringbot is the natural injection from cleartext to bitstringbot.

  Z(cleartext) : cleartext is the function that returns for each cleartext a cleartext of the same length consisting only of zeros.

  Penc(t, N) is the probability of breaking the IND-CCA2 property in time t for one key and N decryption queries.

  Penccoll is the probability of collision between independently generated keys.

The types keyseed, pkey, skey, cleartext, ciphertext, and the probabilities Penc, Penccoll must be declared before this macro is expanded. The functions skgen, pkgen, enc, dec, injbot, and Z are declared by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.
This macro defines the equivalences named \texttt{ind\_cca2(\text{enc})} and \texttt{ind\_cca2\_partial(\text{enc})} for use in the \texttt{crypto} command (see Section 7). The equivalence \texttt{ind\_cca2\_partial(\text{enc})} can be applied only manually and allows the user to replace the encryption of a message with the encryption of zeroes for only some occurrences of encryption under the considered key, the ones in which the public key appears explicitly.

- \texttt{expand \text{IND\_CCA2\_public\_key\_enc\_all\_args}(keyseed, pkey, skey, cleartext, ciphertext, enc\_seed, skgen, skgen', pkeygen, pkeygen', enc, enc\_r, enc\_r', dec, dec', injbot, Z, Penc, Penccoll)} is similar to the above, with six additional arguments.

  - \texttt{enc\_seed} is the type of random coins for encryption, must be bounded.
  - \texttt{enc\_r(cleartext, pkey, enc\_seed)} is the encryption function that takes coins as argument (instead of generating them internally).
  - \texttt{pkgen', skgen', enc\_r', and dec'} are the symbols that replace \texttt{pkgen}, \texttt{skgen}, \texttt{enc\_r} and \texttt{dec} respectively after game transformation.

- \texttt{expand \text{UF\_CMA\_det\_signature}(keyseed, pkey, skey, signinput, signature, skgen, pkeygen, sign, check, Psig, Psig\_coll)} defines a UF-CMA (unforgeable under chosen message attacks) deterministic signature scheme.

  - \texttt{keyseed} is the type of key seeds, must be bounded (to be able to generate random numbers from it, and to talk about the runtime of \texttt{pkgen} without mentioning the length of the key), typically fixed and large.
  - \texttt{pkey} is the type of public keys, must be bounded.
  - \texttt{skey} is the type of secret keys, must be bounded.
  - \texttt{signinput} is the type of signature inputs.
  - \texttt{signature} is the type of signatures.
  - \texttt{skgen(keyseed)} is the secret key generation function.
  - \texttt{pkgen(keyseed)} is the public key generation function.
  - \texttt{sign(signinput, skey)} is the signature function.
  - \texttt{check(signinput, pkey, signature)} is the verification function.

  - \texttt{Psig(t, N, l)} is the probability of breaking the UF-CMA property in time \( t \), for one key, \( N \) signature queries with messages of length at most \( l \).
  - \texttt{Psigcoll} is the probability of collision between independently generated keys.

  The types \texttt{keyseed}, \texttt{pkey}, \texttt{skey}, \texttt{signinput}, \texttt{signature} and the probabilities \texttt{Psig}, \texttt{Psigcoll} must be declared before this macro is expanded. The functions \texttt{skgen}, \texttt{pkgen}, \texttt{sign}, and \texttt{check} are declared by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

  This macro defines the equivalences named \texttt{uf\_cma(sign)}, \texttt{uf\_cma\_corrupt(sign)}, and \texttt{uf\_cma\_corrupt\_partial(sign)}, for use in the \texttt{crypto} command (see Section 7). All three equivalences correspond to the UF-CMA property, but the first one does not allow corruption of the secret keys while last two allow it. The last two equivalences are applied only manually, in particular because their automatic application can sometimes be done too early, when other transformations should first be done in order to eliminate uses of the secret keys. The equivalence \texttt{uf\_cma\_corrupt\_partial(sign)} allows the user to transform only some occurrences of the signature verification into a lookup in the signed messages, the ones in which the public key appears explicitly.

- \texttt{expand \text{UF\_CMA\_det\_signature\_all\_args}(keyseed, pkey, skey, signinput, signature, skgen, skgen', pkeygen, pkeygen', sign, sign', check, check', Psig, Psig\_coll)} is similar to the above with four additional arguments.

  - \texttt{pkgen', skgen', sign', and check'} are the symbols that replace \texttt{pkgen}, \texttt{skgen}, \texttt{sign} and \texttt{check} respectively after game transformation.
• \texttt{expand \texttt{SUF\textunderscore CMA\textunderscore det\textunderscore signature}}(keyseed, pkey, skkey, signinput, signature, skgen, pkgen, sign, check, Psign, Psigncoll), defines a SUF-CMA (strongly unforgeable under chosen message attacks) deterministic signature scheme. The difference between a UF-CMA signature and a SUF-CMA MAsignature is that, for a UF-CMA signature, the adversary may easily forge a new signature for a message for which he has already seen a signature. Such a forgery is guaranteed to be hard for a SUF-CMA signature. The arguments are the same as for \texttt{UF\textunderscore CMA\textunderscore det\textunderscore signature}. This macro defines the equivalences named \texttt{uf\textunderscore cma\textunderscore Signature} and \texttt{uf\textunderscore cma\textunderscore corrupt\textunderscore partial} for use in the \texttt{crypto} command (see Section 7).

• \texttt{expand \texttt{SUF\textunderscore CMA\textunderscore det\textunderscore signature\textunderscore all\textunderscore args}}(keyseed, pkey, skkey, signinput, signature, skgen, pkgen, pkgen', sign, sign', check, check', Psign, Psigncoll), is similar to the above with four additional arguments.

• \texttt{expand \texttt{UF\textunderscore CMA\textunderscore proba\textunderscore signature}}(keyseed, pkey, skkey, signinput, signature, skgen, pkgen, sign, check, Psign, Psigncoll), defines a UF-CMA (strongly unforgeable under chosen message attacks) probabilistic signature scheme. The arguments are the same as for \texttt{UF\textunderscore CMA\textunderscore det\textunderscore signature}, but the signature function internally generated random coins, so that it is probabilistic. This macro defines the equivalences named \texttt{uf\textunderscore cma\textunderscore Signature}, \texttt{uf\textunderscore cma\textunderscore corrupt\textunderscore partial} for use in the \texttt{crypto} command (see Section 7).

• \texttt{expand \texttt{UF\textunderscore CMA\textunderscore proba\textunderscore signature\textunderscore all\textunderscore args}}(keyseed, pkey, skkey, signinput, signature, sign_seed, skgen, skgen', pkgen, pkgen', sign, sign_r, sign_r', check, check', Psign, Psigncoll), is similar to the above, with six additional arguments.

• \texttt{expand \texttt{SUF\textunderscore CMA\textunderscore proba\textunderscore signature}}(keyseed, pkey, skkey, signinput, signature, skgen, pkgen, sign, check, Psign, Psigncoll), defines a SUF-CMA (strongly unforgeable under chosen message attacks) probabilistic signature scheme. The arguments are the same as for \texttt{UF\textunderscore CMA\textunderscore det\textunderscore signature}, but the signature function internally generated random coins, so that it is probabilistic. This macro defines the equivalences named \texttt{uf\textunderscore cma\textunderscore Signature}, \texttt{uf\textunderscore cma\textunderscore corrupt\textunderscore partial} for use in the \texttt{crypto} command (see Section 7).

• \texttt{expand \texttt{SUF\textunderscore CMA\textunderscore proba\textunderscore signature\textunderscore all\textunderscore args}}(keyseed, pkey, skkey, signinput, signature, sign_seed, skgen, pkgen, sign, sign_r, check, Psign, Psigncoll), is similar to the above, with six additional arguments.

• \texttt{expand \texttt{ROM\textunderscore hash}}(key, hashinput, hashoutput, hash, hashoracle, qH), defines a hash function in the random oracle model \cite{1}. 

key is the type of the key of the hash function, which models the choice of the hash function, must be \texttt{bounded}, typically \texttt{fixed}.

hashinput is the type of the input of the hash function.

hashoutput is the type of the output of the hash function, must be \texttt{bounded} or \texttt{nonuniform} (typically \texttt{fixed}).
hash(key, hashinput) : hashoutput is the hash function.

hashoracle is a process that allows the adversary to call the hash function. WARNING: The key must be generated once and for all at the beginning of the game and the hash oracle must be made available to the adversary, by including hashoracle(hk) in the executed process, where hk is the key.

qH is the number of queries to the hash oracle.

The types key, hashinput, and hashoutput must be declared before this macro. The function hash, the process hashoracle, and the parameter qH are defined by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

This macro defines equivalences named rom(hash) and rom_partial(hash) for use in the crypto command (see Section 7). These equivalences are generated via equiv special; the crypto command therefore supports special arguments collisions_LHS and, for rom_partial(hash), collision matrix. See the explanation of the collisions_LHS argument, the collision matrix, and the oracles present in these equivalences in the documentation of equiv special.

- expand ROM_hash_large(key, hashinput, hashoutput, hash, hashoracle, qH). defines a random oracle with a large output, that is, it optimizes the definition by eliminating collisions between random output elements. Its interface is the same as the one of ROM_hash above.

- expand CollisionResistant_hash(key, hashinput, hashoutput, hash, hashoracle, Phash). defines a collision-resistant hash function [11], [7, Section 8.2].
  - key is the type of the key of the hash function, must be bounded or nonuniform, typically fixed.
  - hashinput is the type of the input of the hash function.
  - hashoutput is the type of the output of the hash function.
  - hash(key, hashinput) : hashoutput is the hash function.
  - hashoracle is a process that leaks the key that it receives as argument. WARNING: A collision resistant hash function is a keyed hash function. The key must be generated once and for all at the beginning of the game, and immediately made available to the adversary, for instance by including the process hashoracle(hk), where hk is the key.

    Phash(t) is the probability of breaking collision resistance, for an adversary that runs in time at most t. (t is the time since the choice of the hash function, that is, of the key hk.)

    The types key, hashinput, and hashoutput and the probability Phash must be declared before this macro. The function hash and the process hashoracle are defined by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

- expand HiddenKeyCollisionResistant_hash(key, hashinput, hashoutput, hash, hashoracle, qH, Phash). defines a hidden-key collision-resistant hash function [11] Section 8.6. It differs from collision-resistance in that the adversary is not allowed to access the key that defines the hash function; it is just allowed to query the hash oracle. The interface is similar to collision-resistant hash functions above.

    hashoracle is a process that provides a hash oracle to the adversary. WARNING: A hidden-key collision resistant hash function is a keyed hash function. The key must be generated once and for all at the beginning of the game, and the hash oracle for that key must be provided to the adversary by including the process hashoracle(hk), where hk is the key.

    qH is the number of calls to the hash oracle provided by hashoracle.

    Phash(t, N) is the probability of breaking collision resistance, for an adversary that runs in time at most t and calls the hash oracle at most N times.

This macro defines the equivalence named collision_res(hash) for use in the crypto command (see Section 7).
• expand SecondPreimageResistant_hash(key, hashinput, hashoutput, hash, hashoracle, Phash), defines a second-preimage-resistant hash function \([11]\). The interface is the same as for collision-resistant hash functions above. However, note that the argument type hashinput must be bounded or nonuniform so that one can generate random values in it. It is typically fixed and large.

• expand HiddenKeySecondPreimageResistant_hash(key, hashinput, hashoutput, hash, hashoracle, qH, Phash), defines a hidden-key second-preimage-resistant hash function. The interface is the same as for hidden-key collision-resistant hash functions above. However, note that the argument type hashinput must be bounded or nonuniform so that one can generate random values in it. It is typically fixed and large.

This macro defines the equivalence named second_pre_res(hash) for use in the crypto command (see Section 7).

• expand FixedSecondPreimageResistant_hash(hashinput, hashoutput, hash, Phash), defines a second-preimage-resistant hash function, for a hash function without key. (It can also be interpreted as a hash function with a fixed key as in \([11]\), which we omit in our model.) hashinput is the type of the input of the hash function. It must be bounded or nonuniform so that one can generate random values in it. It is typically fixed and large.

hashoutput is the type of the output of the hash function.

Phash(t) is the probability of breaking second-preimage resistance, for an adversary that runs in time at most \(t\).

The types hashinput, and hashoutput and the probability Phash must be declared before this macro. The function hash is defined by this macro. It must not be declared elsewhere, and it can be used only after expanding the macro.

• expand PreimageResistant_hash(key, hashinput, hashoutput, hash, hashoracle, Phash), defines a preimage-resistant hash function \([11]\). The interface is the same as for collision-resistant hash functions above. However, note that the argument type hashinput must be bounded or nonuniform so that one can generate random values in it. It is typically fixed and large.

This macro defines the equivalence named preimage_res(hash) for use in the crypto command (see Section 7).

• expand PreimageResistant_hash_all_args(key, hashinput, hashoutput, hash, hash', hashoracle, Phash), is similar, with an additional argument hash', which is a symbol that replaces hash after game transformation.

• expand HiddenKeyPreimageResistant_hash(key, hashinput, hashoutput, hash, hashoracle, qH, Phash), defines a hidden-key preimage-resistant hash function. The interface is the same as for hidden-key collision-resistant hash functions above. However, note that the argument type hashinput must be bounded or nonuniform so that one can generate random values in it. It is typically fixed and large.

This macro defines the equivalence named preimage_res(hash) for use in the crypto command (see Section 7).

• expand HiddenKeyPreimageResistant_hash_all_args(key, hashinput, hashoutput, hash, hash', hashoracle, qH, Phash), is similar, with an additional argument hash', which is a symbol that replaces hash after game transformation.

• expand FixedPreimageResistant_hash(hashinput, hashoutput, hash, Phash), defines a preimage-resistant hash function, for a hash function without key. (It can also be interpreted as a hash function with a fixed key as in \([11]\), which we omit in our model.) The interface is the same as for fixed second-preimage-resistant hash functions above.

This macro defines the equivalence named preimage_res(hash) for use in the crypto command (see Section 7).
expand FixedPreimageResistant_hash_all_args(hashinput, hashoutput, hash, hash', Phash).

is similar, with an additional argument hash', which is a symbol that replaces hash after game transformation.

• expand UniversalOneWay_hash(key, hashinput, hashoutput, hash, hashoracle, Phash). defines a
universally one-way hash function [10].

key is the type of the key of the hash function, must be bounded or nonuniform, typically fixed.
hashinput is the type of the input of the hash function.
hashoutput is the type of the output of the hash function.
hash(key, hashinput) : hashoutput is the hash function.

hashoracle is a process that leaks the key that it receives as argument. WARNING: A (family of)
universal one-way hash function(s) is a keyed hash function. The key must be made available to
the adversary, for instance by including the process hashoracle(hk), where hk is the key. The key
is often generated once and for all at the beginning of the game, and immediately made available
to the adversary.

Phash(t) is the probability of breaking collision resistance, for an adversary that runs in time at
most t. (t is the time since the choice of the hash function, that is, of the key hk.)
The types key, hashinput, and hashoutput and the probability Phash must be declared before this
macro. The function hash and the process hashoracle are defined by this macro. They must not
be declared elsewhere, and they can be used only after expanding the macro.

• Similarly to the macros above, for N from 1 to 10, the macros
expand ROM_hash_N(key, hashinput1, . . . , hashinputN, hashoutput, hash, hashoracle, qH).
expand ROM_hash_large_N(key, hashinput1, . . . , hashinputN, hashoutput, hash, hashoracle, qH).
expand CollisionResistant_hash_N(key, hashinput1, . . . , hashinputN, hashoutput, hash, hashoracle, Phash).
expand HiddenKeyCollisionResistant_hash_N(key, hashinput1, . . . , hashinputN, hashoutput, hash, hashoracle, qH, Phash).
expand SecondPreimageResistant_hash_N(key, hashinput1, . . . , hashinputN, hashoutput, hash, hashoracle, Phash).
expand HiddenKeySecondPreimageResistant_hash_N(key, hashinput1, . . . , hashinputN, hashoutput, hash, hashoracle, Phash).
expand FixedSecondPreimageResistant_hash_N(hashinput1, . . . , hashinputN, hashoutput, hash, Phash).
expand FixedPreimageResistant_hash_N(key, hashinput1, . . . , hashinputN, hashoutput, hash, hashoracle, Phash).
expand PreimageResistant_hash_N(key, hashinput1, . . . , hashinputN, hashoutput, hash, hashoracle, Phash).
expand PreimageResistant_hash_all_args_N(key, hashinput1, . . . , hashinputN, hashoutput, hash, hash', hashoracle, Phash).
expand HiddenKeyPreimageResistant_hash_N(key, hashinput1, . . . , hashinputN, hashoutput, hash, hashoracle, qH, Phash).
expand HiddenKeyPreimageResistant_hash_all_args_N(key, hashinput1, . . . , hashinputN, hashoutput, hash, hash', hashoracle, qH, Phash).
expand FixedPreimageResistant_hash_N(hashinput1, . . . , hashinputN, hashoutput, hash, Phash).
expand FixedPreimageResistant_hash_all_args_N(hashinput1, . . . , hashinputN, hashoutput, hash, hash', Phash).
expand UniversalOneWay_hash_N(key, hashinput1, . . . , hashinputN, hashoutput, hash, hashoracle, Phash).

define hash functions with N arguments, with the same properties as above.

hashinput1, . . . , hashinputN are the types of the inputs of the hash function and
hash(key, hashinput1, . . . , hashinputN) : hashoutput is the hash function, except for
FixedSecondPreimageResistant_hash_N and FixedPreimageResistant_hash_N, where
hash(hashinput1, . . . , hashinputN) : hashoutput is the hash function.
• \texttt{expand OW\textunderscore trapdoor\textunderscore perm}(\texttt{seed}, \texttt{pkey}, \texttt{skey}, \texttt{D}, \texttt{pkgen}, \texttt{skgen}, \texttt{f}, \texttt{invf}, \texttt{POW}) . defines a one-way trapdoor permutation.

\texttt{seed} is the type of key seeds, must be bounded (to be able to generate random numbers from it, and to talk about the runtime of \texttt{pkgen} without mentioning the length of the key), typically fixed and large.
\texttt{pkey} is the type of public keys, must be bounded.
\texttt{skey} is the type of secret keys, must be bounded.
\texttt{D} is the type of the input and output of the permutation, must be bounded, typically fixed.
\texttt{pkgen(\texttt{seed}) : pkey} is the public key generation function.
\texttt{skgen(\texttt{seed}) : skey} is the secret key generation function.
\texttt{f(\texttt{pkey}, \texttt{D}) : D} is the permutation (taking as argument the public key)
\texttt{invf(\texttt{skey}, \texttt{D}) : D} is the inverse permutation of \( f \) (taking as argument the secret key, i.e. the trapdoor)
\texttt{POW(t)} is the probability of breaking the one-wayness property in time \( t \), for one key and one permuted value.
The types \texttt{seed}, \texttt{pkey}, \texttt{skey}, \texttt{D}, and the probability \texttt{POW} must be declared before this macro. The functions \texttt{pkgen}, \texttt{skgen}, \texttt{f}, \texttt{invf} are defined by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.
This macro defines the equivalences \texttt{remove invf(f)}, which expresses that, for \( y \) chosen randomly in \( D \), \( y \) and \texttt{invf(skey, y)} are distributed like for \( x \) chosen randomly in \( D \), \( f(pkey, x) \) and \( x \), and \texttt{ow(f)}, which corresponds to one-wayness, for use in the \texttt{crypto} command (see Section 7).

• \texttt{expand OW\textunderscore trapdoor\textunderscore perm\textunderscore RSR}(\texttt{seed}, \texttt{pkey}, \texttt{skey}, \texttt{D}, \texttt{pkgen}, \texttt{skgen}, \texttt{f}, \texttt{invf}, \texttt{POW}) . defines a one-way trapdoor permutation, with random self-reducibility. The arguments are the same as for \texttt{OW\textunderscore trapdoor\textunderscore perm}, but the probability of breaking one-wayness is bounded more precisely. This macro defines the equivalences \texttt{remove invf(f)} as above and \texttt{ow\textunderscore rsr(f)}.

• \texttt{expand set\textunderscore PD\textunderscore OW\textunderscore trapdoor\textunderscore perm}(\texttt{seed}, \texttt{pkey}, \texttt{skey}, \texttt{D}, \texttt{Dow}, \texttt{Dr}, \texttt{pkgen}, \texttt{skgen}, \texttt{f}, \texttt{invf}, \texttt{concat}, \texttt{P\textunderscore PD\textunderscore OW}) . defines a set partial-domain one-way trapdoor permutation.

\texttt{seed} is the type of key seeds, must be bounded (to be able to generate random numbers from it, and to talk about the runtime of \texttt{pkgen} without mentioning the length of the key), typically fixed and large.
\texttt{pkey} is the type of public keys, must be bounded.
\texttt{skey} is the type of secret keys, must be bounded.
\texttt{D} is the type of the input and output of the permutation, must be bounded, typically fixed.
The domain \( D \) consists of the concatenation of bitstrings in \( Dow \) and \( Dr \). \( Dow \) is the set of sub-bitstrings of \( D \) on which one-wayness holds (it is difficult to compute the random element \( x \) of \( Dow \) knowing \( f(pk, concat(x, y)) \) where \( y \) is a random element of \( Dr \)). \( Dow \) and \( Dr \) must be bounded, typically fixed.
\texttt{pkgen(\texttt{seed}) : pkey} is the public key generation function.
\texttt{skgen(\texttt{seed}) : skey} is the secret key generation function.
\texttt{f(\texttt{pkey}, \texttt{D}) : D} is the permutation (taking as argument the public key)
\texttt{invf(\texttt{skey}, \texttt{D}) : D} is the inverse permutation of \( f \) (taking as argument the secret key, i.e. the trapdoor)
\texttt{concat(\texttt{Dow}, \texttt{Dr}) : D} is bitstring concatenation.
\texttt{P\textunderscore PD\textunderscore OW(t, l)} is the probability of breaking the set partial-domain one-wayness property in time \( t \), for one key, one permuted value, and \( l \) tries.
The types \texttt{seed}, \texttt{pkey}, \texttt{skey}, \texttt{D}, \texttt{Dow}, \texttt{Dr} and the probability \texttt{P\textunderscore PD\textunderscore OW} must be declared before this macro. The functions \texttt{pkgen}, \texttt{skgen}, \texttt{f}, \texttt{invf}, \texttt{concat} are defined by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.
This macro defines the equivalences remove_invf(f), which expresses that, for y chosen randomly in D, y and invf(sk, y) are distributed like for x chosen randomly in D, f(pkey, x) and x, and pd-ow(f), which corresponds to set partial-domain one-wayness, for use in the crypto command (see Section 7).

- expand OW_trapdoor_perm_all_args(seed, pkey, skkey, D, pkgen, pkgen', skgen, f, f', invf, POW).
- expand OW_trapdoor_perm_RSR_all_args(seed, pkey, skkey, D, pkgen, pkgen', skgen, f, f', invf, POW).
- expand set_PD_OW_trapdoor_perm_all_args(seed, pkey, skkey, D, pkgen, pkgen', skgen, f, f', invf, concat, P_PD_OW).

These equivalences are generated via equiv...special; the crypto command supports special arguments collisions_LHS and, for prf_partial(f), collision matrix. See the explanation of the collisions_LHS argument, the collision matrix, and the oracles present in these equivalences in the documentation of equiv...special.

- expand PRF_large(key, input, output, f, Pprf), defines a pseudo-random function with a large output, that is, it optimizes the definition by eliminating collisions between random output elements. Its interface is the same as the one of PRF above.

Similarly, for N from 1 to 10, the macros expand PRF_N(key, input1, ..., inputN, output, f, Pprf), expand PRF_large_N(key, input1, ..., inputN, output, f, Pprf), define pseudo-random functions with N arguments, similarly to PRF and PRF_large above. input1, ..., inputN are the types of the inputs of the PRF and f(key, input1, ..., inputN) : output is the PRF.

The specification of Diffie-Hellman key agreements is typically composed of two or three macro expansions:

- One from the following set of macros, which defines properties of the group:
  - expand DH_basic(G, Z, g, exp, exp', mult). defines a Diffie-Hellman structure G.
    - G: type of group elements (must be bounded and large).
    - Z: type of exponents (must be bounded and large).
    - g: an element of the group G.
    - exp'(G, Z): G: symbol used to replace exp after game transformations.
    - The equation exp(exp(a, x), y) = exp(a, mult(x, y)) must be satisfied.
The private Diffie-Hellman keys are generated by choosing an element randomly in \( Z \), according to its default distribution (which is not necessarily uniform). The public Diffie-Hellman keys are generated as \( X = \text{exp}(g, x) \), where \( x \) is a private Diffie-Hellman key, and similarly \( Y = \text{exp}(g, y) \). The Diffie-Hellman shared secret is \( \text{exp}(X, y) = \text{exp}(Y, x) = \text{exp}(g, \text{mult}(x, y)) \). This macro makes no other assumption. In particular, it allows \( G \) to contain elements other than those generated by \( g \).

The types \( G \) and \( Z \) must be declared before this macro. The functions \( g \), \( \text{exp} \), and \( \text{mult} \) are defined by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

* \textbf{expand DH\textunderscore basic\textunderscore with\textunderscore is\textunderscore neutral}(G, Z, g, \text{exp}, \text{exp}', \text{mult}, \text{is\textunderscore neutral}) \textbf{.} defines a Diffie-Hellman structure like \textbf{expand DH\textunderscore basic}(G, Z, g, \text{exp}', \text{mult}) \textbf{.} with additionally \text{is\textunderscore neutral}(g) is false and for \( X \) in \( G \), \text{is\textunderscore neutral}(\text{exp}(X, y)) if and only if \text{is\textunderscore neutral}(X).

\text{is\textunderscore neutral}(G) : bool is defined by this macro. It must not be declared elsewhere, and can be used only after expanding the macro.

Prime-order groups with the neutral element included satisfy this assumption, for instance, where \text{is\textunderscore neutral}(X) is true if and only if \( X \) is the neutral element. Prime-order groups without the neutral element also satisfy this assumption, with \text{is\textunderscore neutral}(X) = \text{false}.

* \textbf{expand DH\textunderscore subgroup}(G, Z, g, \text{exp}, \text{mult}, \text{sub}G, g\_k, \text{exp\_div\_k}, \text{exp\_div\_k}', \text{pow\_k}, \text{sub}G\text{to}G) \textbf{.} defines a Diffie-Hellman structure that satisfies the following properties:

\( G \): type of elements (must be bounded and large).

\( Z \): type of exponents, a set of integers multiple of \( k \); prime to \( n \) (possibly modulo \( kn \)); \( k \) is prime to \( n \); \( Z \) must be bounded and large.

\( g \): an element of \( G \).

There is an exponentiation function such that for \( X \) in \( G \) and \( y \) integer, we have \( X^y \) in \( G \) with the following properties:

1. \((X^x)^y = X^{xy})\);
2. \(\text{sub}G = \{X^k \mid X \in G\}\) is a subset of \( G \);
3. for \( X, X' \) in \( \text{sub}G \), for any \( x \) prime to \( n \), \( X^x = X'^x \Rightarrow X = X'\);
4. exponentiation yields the same results for exponents equal modulo \( kn \).

\text{exp}(G, Z) : G \) is defined by \text{exp}(X, y) = X^y.

\text{mult}(Z, Z) : Z \) is the product of integers (possibly modulo \( kn \)), commutative.

\text{sub}G = \{X^k \mid X \in G\} \) is a subset of \( G \) as mentioned above. The type \( \text{sub}G \) must be bounded and large.

\( g\_k = g^k \in \text{sub}G \).

\text{exp\_div\_k}(\text{sub}G, Z) : \text{sub}G \) is defined by \text{exp\_div\_k}(X, y) = X^{y/k}.

\text{exp\_div\_k}' \) is defined like \text{exp\_div\_k} \textbf{,} it replaces \text{exp\_div\_k} after games transformations.

\text{pow\_k}(G) : \text{sub}G \) is defined by \text{pow\_k}(X) = X^k.

\text{sub}G\text{to}G : G \) is the injection from \text{sub}G to \( G \).

The types \( G \), \( Z \), and \( \text{sub}G \) must be declared before expanding this macro. The constants \( g \) and \( g\_k \), and the functions \( \text{exp}, \text{mult}, \text{exp\_div\_k}, \text{exp\_div\_k}', \text{pow\_k}, \text{sub}G\text{to}G \) are defined by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

When this macro is used, the other Diffie-Hellman macros (detailed below) except \textbf{DH\textunderscore exclude\textunderscore weak\textunderscore keys} should be applied to the subgroup, that is, \textbf{expand assumption(sub}G, Z, g\_k, \text{exp\_div\_k}, \text{exp\_div\_k}', \text{mult}, \ldots\).

Curve25519 satisfies these properties with \( k = 8 \), \( n = pp' \) where the curve has order \( kp \) and the quadratic twist has order \( k'p' \) (\( k' = 4 \), \( p \) and \( p' \) are large primes). See \texttt{https://hal.inria.fr/hal-02100345}.

Curve448 satisfies these properties with \( k = 4 \), \( n = pp' \) after removing the weak private key \( kp \) which is not prime to \( n = pp' \), where the curve has order \( kp \) and the quadratic twist has order \( k'p' \) (\( k' = 4 \), \( p \) and \( p' \) are large primes). This can be done as follows
Groups of prime order \( q \) also satisfy these properties, with \( k = 1 \), \( n = q \), \( \text{sub}G = G \), \( g_k = g \), \( \text{pow}_k \) and \( \text{sub}GtoG \) are the identity (assuming private keys are chosen in \( \{1, \ldots, q-1\} \)).

8 expand DH_subgroup_with_is_neutral\((G, Znw, g, \text{expnw}, \text{mult}, \text{sub}G, g_k, \text{exp}_\text{div}_k, \text{exp}_\text{div}_k', \text{pow}_k, \text{sub}GtoG)\).

letproba \( P\text{weak}_\text{key} = 2^n - 445 \).

expand DH_exclude_weak_keys\((G, Z, Znw, \text{ZnwtoZ}, \text{exp}, \text{expnw}, P\text{weak}_\text{key})\).

Prime order groups (without the neutral element) satisfy these properties with \( \text{is}_\text{neutral}(X) = (X = 0) \). Curve448 also satisfies these properties with \( \text{is}_\text{neutral}(X) = (X = 0) \), after removing the weak private key as follows:

8 expand DH_subgroup_with_is_neutral\((G, Znw, g, \text{expnw}, \text{mult}, \text{sub}G, g_k, \text{exp}_\text{div}_k, \text{exp}_\text{div}_k', \text{pow}_k, \text{sub}GtoG, \text{is}_\text{neutral}_G, \text{is}_\text{neutral}_\text{sub}G)\).

letproba \( P\text{weak}_\text{key} = 2^n - 445 \).

expand DH_exclude_weak_keys\((G, Z, Znw, \text{ZnwtoZ}, \text{exp}, \text{expnw}, P\text{weak}_\text{key})\).

This macro defines the following equivalences for use in the crypto command (see Section 7):

- \( \text{group}_t\text{o}_\text{exp}_\text{strict}(\text{exp}) \) which allows to replace a random \( X \in G \) with \( \text{exp}(g, x) \) for a random \( x \in Z \), provided \( \text{exp}(X, _) \) occurs in the game.
- \( \text{group}_t\text{o}_\text{exp}(\text{exp}) \) which allows to replace a random \( X \in G \) with \( \text{exp}(g, x) \) for a random \( x \in Z \) in any case. (This transformation is applied only manually.)
- \( \text{exp}_\text{t}_\text{o}_\text{group}(\text{exp}) \) which allows to replace \( \text{exp}(g, x) \) for a random \( x \in Z \) with a random \( X \in G \).
- \( \text{exp}_\text{t}_\text{o}_\text{group}(\text{exp}) \) which allows to replace \( \text{exp}(g, x) \) for a random \( x \in Z \) with a random \( X \in G \).

8 expand DH_single_coord_ladder\((G, Z, g, \text{exp}, \text{mult}, \text{sub}G, Znw, \text{ZnwtoZ}, g_k, \text{exp}_\text{div}_k, \text{exp}_\text{div}_k', \text{pow}_k, \text{sub}GtoG, \text{is}_\text{zero}_G, \text{is}_\text{zero}_\text{sub}G) \), models an elliptic curve defined by the equation \( Y^2 = X^3 + AX^2 + X \) in the field \( \mathbb{F}_p \) of non-zero integers modulo the large prime \( p \), where \( A^2 - 4 \) is not a square modulo \( p \). This curve must form a commutative group of order \( kq \) where \( k \) is a small integer and \( q \) is a large prime. Its quadratic twist must form a commutative group of order \( k'q' \) where \( k' \) is a small integer.
and $q'$ is a large prime. $k$ must be a multiple of $k'$. We must use a single coordinate ladder defined as follows: we consider the elliptic curve $E(\mathbb{F}_{p^2})$ defined by the equation $Y^2 = X^3 + AX^2 + X$ in a quadratic extension $\mathbb{F}_{p^2}$ of $\mathbb{F}_p$, we define $X_0: E(\mathbb{F}_{p^2}) \to \mathbb{F}_{p^2}$ by $X_0(x) = 0$ and $X_0(X, Y) = X$, and for $X \in \mathbb{F}_p$ and $y$ an integer, we define $y \cdot X \in \mathbb{F}_p$ as $y \cdot X = X_0(yQ)$ for all $Q \in E(\mathbb{F}_{p^2})$ such that $X_0(Q) = X$. The value $g = X_0(g_0)$ represents the base point $g_0$ which must have order $q$. The public keys (bitstrings) are mapped to elements of $\mathbb{F}_p$ by the function red and conversely, elements of $\mathbb{F}_p$ are mapped to public keys by the function repr, such that $\text{red(} \text{repr(} X \text{)} \text{)} = X$. The secret keys are chosen uniformly in $\{kn \mid n \in [n_{\min}, n_{\max}]\}$ where $n_{\min} < n_{\max}$. $n_{\max} - n_{\min} < q$ and $n_{\max} - n_{\min} < q'$. Therefore the set of secret keys may contain a multiple of $q$ (resp. $q'$). Such keys are weak, in the sense that they yield $0$ for all public keys on the curve (resp. on the twist). We exclude them as a first step in the proof, by applying the equivalence \texttt{exclude_weak_keys}(Z) defined by this macro, automatically or with the \texttt{crypto} command (see Section 7).

This model is justified in [9].

$G$: type of public keys (must be \texttt{bounded} and \texttt{large}).

$\text{subG}$: type of $\{k \cdot X \mid X \in \mathbb{F}_p\}$ (must be \texttt{bounded}, \texttt{nonuniform}, and \texttt{large}). Random choices in $\text{subG}$ are done by choosing uniformly in $\{x \cdot g \mid x \in \{1, \ldots, q - 1\}\}$. (This set is not the whole $\text{subG}$, since $\text{subG}$ also contains elements of the twist.) This is important when the DDH assumption or the square DDH assumption is used.

$Z$, $\text{znw}$: type of exponents (must be \texttt{bounded}, \texttt{nonuniform}, and \texttt{large}). $\text{znw}$ is the set of integers multiple of $k$, prime to $qq'$ modulo $qq'$. This is, exponents without weak keys. Random choices in $\text{znw}$ are done by choosing uniformly in $\{kn \mid n \in [n_{\min}, n_{\max}], n \text{ prime to } qq'\}$. $Z$ is the set of integers multiple of $k$ modulo $qq'$, that is, exponents with weak keys. Random choices in $Z$ are done by choosing uniformly in $\{kn \mid n \in [n_{\min}, n_{\max}]\}$, hence $\text{Fcol11rand}(Z) = 1/(n_{\max} - n_{\min} + 1)$.

$\text{znwtoZ}(\text{znw}) : Z$: injection from $\text{znw}$ to $Z$.

$g : G$: represents the base point.

$\text{exp}(G, Z) : G$: the exponentiation function.

$\text{mult}(\text{znw}, \text{znw}) : Z$: multiplication function for exponents, defined as $\text{mult}(x, y) = xy \mod qq'$. (It remains in $\text{znw}$.)

$g \cdot k = k \cdot \text{red}(g)$. It is an element of $\text{subG}$.

$\text{exp}_{\text{div}}(k, \text{znw}) : \text{subG}$ is defined by $\text{exp}_{\text{div}}(k, X, y) = (y/k) \cdot X$.

$\text{exp}_{\text{div}}(k)$: symbol that replaces $\text{exp}_{\text{div}}(k)$ after game transformation, with the same definition as $\text{exp}_{\text{div}}(k)$.

$\text{pow}_{\text{k}}(G) : \text{subG}$, defined by $\text{pow}_{\text{k}}(x) = k \cdot \text{red}(x)$.

$\text{subGtoG}(\text{subG}) : G$ is \texttt{repr} restricted to $\text{subG}$.

$\text{is}_\text{zero}_{\text{G}}(G) : \text{bool}$ is defined by: $\text{is}_\text{zero}_{\text{G}}(X)$ is true when $X$ is the public key 0.

$\text{is}_\text{zero}_{\text{subG}}(\text{subG}) : \text{bool}$ is defined by: $\text{is}_\text{zero}_{\text{subG}}(X)$ is true when $X$ is the public key 0.

The types $G$, $\text{subG}$, $Z$, and $\text{znw}$ must be declared before this macro. The functions $g$, $\text{exp}$, $\text{mult}$, $\text{znwtoZ}$, $g \cdot k$, $\text{exp}_{\text{div}}(k)$, $\text{exp}_{\text{div}}(k')$, $\text{pow}_{\text{k}}$, $\text{subGtoG}$, $\text{is}_\text{zero}_{\text{G}}$, $\text{is}_\text{zero}_{\text{subG}}$ are defined by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

When this macro is used, the other Diffie-Hellman macros (detailed below) should be applied to the subgroup, that is, $\text{expand assumption}(\text{subG}, \text{znw}, g \cdot k, \text{exp}_{\text{div}}(k), \text{exp}_{\text{div}}(k'), \text{mult}, \ldots)$.

8 expand DH_X25519(G, Z, g, $\text{exp}$, $\text{mult}$, $\text{znwtoZ}$, $g \cdot k$, $\text{exp}_{\text{div}}(k)$, $\text{exp}_{\text{div}}(k')$, $\text{pow}_{\text{k}}$, $\text{subGtoG}$, $\text{is}_\text{zero}_{\text{G}}$, $\text{is}_\text{zero}_{\text{subG}}$). models Curve25519 as defined in RFC 7748 [https://tools.ietf.org/html/rfc7748]. It is justified in detail in [9]. More generally, it supports the same curves as DH_single_coord_ladder with the additional assumption that all secret keys are prime to $qq'$. Therefore, we do not need to exclude weak secret
Optionally, one or more of the following macros:

- expand DH_proba_collision\((G, Z, g, x, y, \text{exp}, \text{mult}, \text{PCollKey1}, \text{PCollKey2})\), adds the following properties: the probability that \(\text{exp}(g, x) = Y\) where \(x\) is random and \(Y\) is independent of \(x\) is at most \(\text{PCollKey1}\), and the probability that \(\text{exp}(g, \text{mult}(x, y)) = Y\) where \(x\) and \(y\) are independent random private keys and \(Y\) is independent of \(x\) or \(y\) is at most \(\text{PCollKey2}\). These probabilities are negligible in most Diffie-Hellman groups, but need to be evaluated more precisely for using this property.

- The types \(G\) and \(Z\) and the probabilities \(\text{PCollKey1}\) and \(\text{PCollKey2}\) must be declared before this macro. The functions \(g, \text{exp}, \text{mult}\) are defined by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

- DH_proba_collision should be used with DH_basic, DH_basic_with_is_neutral, DH_subgroup, or DH_subgroup_with_is_neutral; with the latter two, it should be

\[\exp(G, Z, g, x, y, \text{exp}, \text{mult}, \text{PCollKey1}, \text{PCollKey2})\]
applied to the subgroup. (The macros DH_good_group, DH_single_coord_ladder, DH_X25519, DH_X448 already include such collision information.) It should not be used with square_DH_proba_collision or is_neutral_DH_proba_collision: they include information provided by DH_proba_collision.

* expand square_DH_proba_collision(G, Z, g, exp, exp', mult, PCollKey1, PCollKey2, PCollKey3). is similar to DH_proba_collision, but additionally says that the probability that exp(g, mult(x,x)) = Y where x is random and Y is independent of x is at most PCollKey3, with PCollKey3 ≥ PCollKey2. The types G and Z and the probabilities PCollKey1, PCollKey2, and PCollKey3 must be declared before this macro. The functions g, exp, and mult are defined by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

square_DH_proba_collision should be used with DH_basic, DH_basic_with_is_neutral, DH_subgroup, or DH_subgroup_with_is_neutral; with the latter two, it should be applied to the subgroup. (The macros DH_good_group, DH_single_coord_ladder, DH_X25519, DH_X448 already include such collision information.) It should not be used with DH_proba_collision or is_neutral_DH_proba_collision: it includes information provided by DH_proba_collision and is_neutral_DH_proba_collision includes information provided by square_DH_proba_collision.

* expand is_neutral_DH_proba_collision(G, Z, g, exp, exp', mult, is_neutral, PCollKey2, PCollKey3, PCollKey4). should be used with either DH_basic_with_is_neutral or DH_subgroup_with_is_neutral; with the latter, it should be applied to the subgroup, as follows:

expand DH_subgroup_with_is_neutral(G, Z, g, exp, mult, subG, g_k, exp_div_k, exp_div_k', pow_k, subGtoG, is_neutral_G, is_neutral_subG).

expand is_neutral_DH_proba_collision(subG, Z, g_k, exp_div_k, exp_div_k', mult, is_neutral_subG, PCollKey2, PCollKey3, PCollKey4).

In addition to the information provided by DH_basic_with_is_neutral or DH_subgroup_with_is_neutral, it assumes that
- if is_neutral(X) and is_neutral(Y) then X = Y (in other words, there is 0 or 1 neutral element in G);
- the probability that exp(X,x) = Y where x is random and X and Y are independent of x and not neutral is at most PCollKey2;
- the probability that exp(g, mult(x,x)) = Y with random x and Y independent of x is at most PCollKey3, with PCollKey3 ≥ PCollKey2;
- the probability that exp(X,y) = exp(X,z) with y, z random independent of each other and X is not neutral is at most PCollKey4.

It states these collisions and others that can be inferred from them. It should not be used with DH_proba_collision or square_DH_proba_collision: it includes the information provided by these two macros.

* expand DH_dist_random_group_element_vs_exponent(G, Z, g, exp, exp', mult, PDist). This macro says that the probability of distinguishing a random group element from an exponentiation exp(g,x) with a random exponent x is at most PDist. The other arguments are as in DH_basic and all arguments must be defined before expanding the macro. This macro defines the following equivalences for use in the crypto command (see Section 7):
- group_to_exp_strict(exp) which allows to replace a random X ∈ G with exp(g,x) for a random x ∈ Z, provided exp(X,_) occurs in the game.
- group_to_exp(exp) which allows to replace a random X ∈ G with exp(g,x) for a random x ∈ Z in any case. (This transformation is applied only manually.)
One from the following set of macros, which defines the Die-Hellman assumption itself:

- \( \text{exp}_\text{to}_\text{group}(exp) \) which allows to replace \( exp(g, x) \) for a random \( x \in Z \) with a random \( X \in G \).
- \( \text{exp}_\text{to}_\text{group}'(exp) \) which allows to replace \( exp'(g, x) \) for a random \( x \in Z \) with a random \( X \in G \).

This macro can be used with any of the previous macros, except that it is useless with the macro \( \text{DH}_{\text{good}} \text{group} \), because this macro already includes these properties with \( PDist = 0 \). When the macro \( \text{DH}_{\text{subgroup}} \), \( \text{DH}_{\text{subgroup with is neutral}} \), \( \text{DH}_{\text{single coord ladder}} \), \( \text{DH}_{\text{X25519}} \), or \( \text{DH}_{\text{X448}} \) is used, this macro should be applied to the subgroup. For instance, with \( \text{expand DH}_{\text{single coord ladder}}(G, Z, g, \exp, \mult, \subG, Znw, ZnutoZ, g_k, \exp_{\div k}, \exp_{\div k'}, \pow_k, \subGtoG, \zero, \subzero) \), it should be \( \text{expand DH}_{\text{dist random group element vs exponent}}(\subG, Znw, g_k, \exp_{\div k}, \exp_{\div k'}, \mult, \Pdist) \).

- One from the following set of macros, which defines the Diffie-Hellman assumption itself:

  - \( \text{expand CDH}(G, Z, g, exp, exp', \mult, p) \) says that the group \( G \) satisfies the computational Diffie-Hellman assumption; \( p(t) \) is the probability of breaking the \( \text{CDH} \) assumption, for one pair of exponents, in time \( t \). This macro defines the equivalence \( \text{cdh}(exp) \), which corresponds to the \( \text{CDH} \) property, for use in the \( \text{crypto} \) command (see Section 7).
  - \( \text{expand CDH}_{\text{RSR}}(G, Z, g, exp, exp', \mult, p, p_d) \) is similar to \( \text{CDH} \), but uses random self reducibility. \( p_d \) is the probability of distinguishing a key that comes from rerandomization from an honestly chosen key. We have \( p_d = 0 \) when the exponents are chosen uniformly in \( (Z/qZ)^* \) in a group of prime order \( q \) (as assumed by the macro \( \text{DH}_{\text{good group}} \), \( p_d = 2^{-126} \) for Curve25519, and \( p_d = 2^{-221} \) for Curve448.
  - \( \text{expand DDH}(G, Z, g, exp, exp', \mult, p) \) says that the group \( G \) satisfies the decisional Diffie-Hellman assumption; \( p(t) \) is the probability of breaking the \( \text{DDH} \) assumption, for one pair of exponents, in time \( t \). This macro defines the equivalence \( \text{ddh}(exp) \), which corresponds to the \( \text{DDH} \) property, for use in the \( \text{crypto} \) command (see Section 7). 
  - \( \text{expand DDH}_{\text{RSR}}(G, Z, g, exp, exp', \mult, p, p_d) \) is similar to \( \text{DDH} \), but uses random self reducibility. \( p_d \) is the probability of distinguishing a key that comes from rerandomization from an honestly chosen key (see \( \text{CDH}_{\text{RSR}} \)). This macro is much more limited than the macro \( \text{DDH} \). It does not support corruption; corrupted keys must be in variables different from the ones containing honest keys. It supports only a single Diffie-Hellman query for each exponent \( a_i \), associated with an arbitrary \( b_i \) and no Diffie-Hellman queries for \( b_j \). The default distribution on \( G \) must be as follows: There is an underlying prime-order group (the Diffie-Hellman group itself when it has prime order; the prime-order subgroup of the curve generated by the base point for Curve25519/Curve448). The default distribution on \( G \) is obtained by choosing uniformly an element in that group minus its neutral element and taking the associated public key in \( G \) (the group element itself for prime-order Diffie-Hellman groups; the encoding of its X coordinate for Curve25519/Curve448). \( \text{CDH} \) and \( \text{GDH} \) with random self reducibility do not have such limitations.
  - \( \text{expand GDH}(G, Z, g, exp, exp', \mult, p, p_d) \) says that the group \( G \) satisfies the gap Diffie-Hellman assumption (GDH). The probability \( p(t, n) \) is the probability of breaking the \( \text{GDH} \) assumption for one pair of exponents in time \( t \) with at most \( n \) calls to the decisional Diffie-Hellman oracle. \( p_d \) is the probability of distinguishing a key that comes from rerandomization from an honestly chosen key (see \( \text{CDH}_{\text{RSR}} \)). It is needed because, for Curve25519/Curve448, to make the Diffie-Hellman decision oracle unambiguous, we generate secret keys in \( ((p + 1)/2, p - 1) \) instead of the set used for generating secret keys in the Curve25519/Curve448 implementation. (The latter set yields equivalent secret keys with small probability.) We make the same change of distribution for rerandomization. This macro defines the equivalence \( \text{gdh}(exp) \), which corresponds to the \( \text{GDH} \) property, for use in the \( \text{crypto} \) command (see Section 7).
  - \( \text{expand GDH}_{\text{RSR}}(G, Z, g, exp, exp', \mult, p, p_d) \) is similar to \( \text{GDH} \), but uses random self reducibility.
  - \( \text{expand square CDH}(G, Z, g, exp, exp', \mult, p, sqp) \) says that the group \( G \) satisfies the computational Diffie-Hellman assumption and the square computational Diffie-Hellman
assumption: \( p(t) \) is the probability of breaking the CDH assumption, for one pair of exponents, in time \( t \) and \( sqp(t) \) is the probability of breaking the square CDH assumption, for one pair of exponents, in time \( t \). This macro defines the equivalence \( cdh(exp) \), which corresponds to the (square) CDH property, for use in the \texttt{crypto} command (see Section 7). When the group has prime order, the computational Diffie-Hellman assumption is equivalent to the square variant, but CryptoVerif can do more proofs using the square variant. (It allows transforming \( exp(g, mult(x, x)) \).)

\begin{verbatim}
8 expand square_CDH_RSR(G, Z, g, exp, exp', mult, sqp). says that the group G satisfies the square computational Diffie-Hellman assumption; \( sqp(t) \) is the probability of breaking the square CDH assumption, for one pair of exponents, in time \( t \); this macro uses random self reducibility, and \( p_d \) is the probability of distinguishing a key that comes from rerandomization from an honestly chosen key (see \texttt{CDH_RSR}). This macro defines the equivalence \( cdh(exp) \), which corresponds to the square CDH property, for use in the \texttt{crypto} command (see Section 7).

8 expand square_GDH(G, Z, g, exp, exp', mult, p, sqp). says that the group G satisfies the decisional Diffie-Hellman assumption and the square decisional Diffie-Hellman assumption; \( p(t) \) is the probability of breaking the DDH assumption, for one pair of exponents, in time \( t \) and \( sqp(t) \) is the probability of breaking the square DDH assumption, for one pair of exponents, in time \( t \). This macro defines the equivalence \( gdh(exp) \), which corresponds to the (square) DDH property, for use in the \texttt{crypto} command (see Section 7).

8 expand square_GDH_RSR(G, Z, g, exp, exp', mult, p, sqp, p_d). says that the group G satisfies the gap Diffie-Hellman (GDH) assumption and the square gap Diffie-Hellman assumption; \( p(t, n) \) is the probability of breaking the GDH assumption, for one pair of exponents, in time \( t \) with at most \( n \) calls to the decisional Diffie-Hellman oracle and \( sqp(t, n) \) is the probability of breaking the square GDH assumption, for one pair of exponents, in time \( t \) with at most \( n \) calls to the decisional Diffie-Hellman oracle. \( p_d \) is the probability of distinguishing a key that comes from rerandomization from an honestly chosen key (see \texttt{CDH_RSR}). It is needed because, for Curve25519/448, to make the Die-Hellman decision oracle unambiguous, we generate secret keys in \( [(p + 1)/2, p - 1] \) instead of the set used for generating secret keys in the Curve25519/448 implementation. (The latter set yields equivalent secret keys with small probability.) We make the same change of distribution for rerandomization. This macro defines the equivalence \( gdh(exp) \), which corresponds to the (square) GDH property, for use in the \texttt{crypto} command (see Section 7).

8 expand square_GDH_RSR(G, Z, g, exp, exp', mult, sqp, p_d). says that the group G satisfies the square gap Diffie-Hellman assumption; \( sqp(t, n) \) is the probability of breaking the square GDH assumption, for one pair of exponents, in time \( t \) with at most \( n \) calls to the decisional Diffie-Hellman oracle; this macro uses random self reducibility, and \( p_d \) is the probability of distinguishing a key that comes from rerandomization from an honestly chosen key (see \texttt{CDH_RSR}). This macro defines the equivalence \( gdh(exp) \), which corresponds to the square GDH property, for use in the \texttt{crypto} command (see Section 7).

8 expand PRF_ODH1(G, Z, prf_in, prf_out, g, exp, exp', mult, prf, p). says that the group G satisfies the PRF-ODH1 (pseudo-random function oracle Diffie-Hellman) assumption, which corresponds to PRF-ODHnn in [6]. The pseudo-random function \( prf(G, prf\_in) : prf\_out \) takes as argument a group element in \( G \) and an element in \( prf\_in \), and produces a result in \( prf\_out \). The type \( prf\_out \) must be bounded or nonuniform. This assumption means that an adversary that has 2 public Diffie-Hellman keys \( exp(g, a) \) and \( exp(g, b) \) for random \( a, b \) cannot distinguish \( x \mapsto prf(exp(g, mult(a, b)), x) \) from a random function. A random function returns a fresh random value when it is called with a new argument and the previous result when it is called with the same argument as a previous call. The probability \( p(t, n) \) is the probability of breaking the PRF-ODH1 assumption in time \( t \) with \( n \) queries to \( prf(exp(g, mult(a, b)), x) \). This macro defines the equivalence \( prf\_odh(prf) \), which corresponds to the PRF-ODH1 property, for use in the \texttt{crypto} command (see Section 7).

When this assumption is used with \texttt{DH\_subgroup}, \texttt{DH\_subgroup\_with\_is\_neutral}, \texttt{DH\_X25519}, \texttt{DH\_X448}, or \texttt{DH\_single\_coord\_ladder}, it must be applied to the subgroup,
which can be done as follows:

\[ \text{expand } \text{DH\_single\_coord\_ladder}(G, Z, g, \exp, \mult, \subG, \Znw, \ZnwtoZ, g_k, \exp_{\text{div}} k, \exp_{\text{div}} k', \text{pow} k, \subGtoG, \text{zero}, \subzero). \]
\[ \text{expand } \text{PRF\_ODH1}(\subG, \Znw, \text{prf\_in}, \text{prf\_out}, g_k, \exp_{\text{div}} k, \exp_{\text{div}} k', \mult, \text{prf}_{\subG}(p). \]
\[ \text{fun } \text{prf}(G, \text{prf\_in}) : \text{prf\_out}. \]
\[ \text{equation for all } x : \subG, y : \text{prf\_in}; \text{prf}(\subGtoG(x), y) = \text{prf\_subG}(x, y). \]

\[ \text{expand } \text{PRF\_ODH2}(G, Z, \text{prf\_in}, \text{prf\_out}, g, \exp, \exp', \mult, \text{prf}, \text{p}, \text{PCollKey1}). \]

says that the group \( G \) satisfies the PRF-ODH2 assumption, which corresponds to PRF-ODHNN in \([6]\). The types \text{prf\_in} and \text{prf\_out} and the pseudo-random function \text{prf} are defined as for PRF-ODH1. This assumption means that an adversary that has access to the oracles \((Y, x) \mapsto \text{prf}(\exp(Y, a), x)\) and \((X, x) \mapsto \text{prf}(\exp(X, b), x)\) cannot distinguish \( x \mapsto \text{prf}(\exp(g, \mult(a, b)), x) \) from a random function. The probability \( p(t, n, n') \) is the probability of breaking the PRF-ODH2 assumption in time \( t \) with \( n \) queries to \( \text{prf}(\exp(g, \mult(a, b)), x) \) and \( n' \) queries to \( (Y, x) \mapsto \text{prf}(\exp(Y, a), x) \) and \((X, x) \mapsto \text{prf}(\exp(X, b), x)\) in total. This macro defines the equivalence \text{prf\_odh}(\text{prf})\), which corresponds to the PRF-ODH2 property, for use in the \text{crypto} command (see Section \([7]\)).

When this assumption is used with \text{DH\_subgroup}, \text{DH\_subgroup\_with\_is\_neutral}, \text{DH\_X25519}, \text{DH\_X448}, or \text{DH\_single\_coord\_ladder}, it must be applied to the subgroup, which can be done as for PRF-ODH1.

If \( G \) is Curve448, the weak private key \( kp \) must be excluded, which can be done using \text{DH\_exclude\_weak\_keys}, \text{DH\_X448}, or \text{DH\_single\_coord\_ladder}.

Additionally, this assumption requires that it is possible to test efficiently whether \( \exp(Y, a) = \exp(g, ab) \) knowing just \( Y \) and \( B = \exp(g, b) \) (so the result does not depend on \( a \)). This is possible for prime-order groups as well as Curve25519 and Curve448 when the weak private key is excluded. When this is true, we say that the keys \( Y \) and \( B \) are equivalent. The probability that two honestly generated random keys are equivalent is bounded by \text{PCollKey1}.

\[ \text{expand } \text{square\_PRF\_ODH1}(G, Z, \text{prf\_in}, \text{prf\_out}, g, \exp, \exp', \mult, \text{prf}, \text{p}, \text{sqp}). \]

says that the group \( G \) satisfies the square PRF-ODH1 assumption and the PRF-ODH1 assumption. The types \text{prf\_in} and \text{prf\_out} and the pseudo-random function \text{prf} are defined as for PRF-ODH1. The square PRF-ODH1 assumption means that an adversary that has a public Diffie-Hellman key \( \exp(g, a) \) for random \( a \) cannot distinguish \( x \mapsto \text{prf}(\exp(g, \mult(a, a)), x) \) from a random function. The probability \( \text{sqp}(t, n) \) is the probability of breaking the square PRF-ODH1 assumption in time \( t \) with \( n \) queries to \( \text{prf}(\exp(g, \mult(a, a)), x) \) and \( \text{prf}(\exp(X, a), x) \) and \((X, x) \mapsto \text{prf}(\exp(X, b), x)\) in total. This macro defines the equivalence \text{prf\_odh}(\text{prf})\), which corresponds to the square PRF-ODH1 and PRF-ODH1 properties, for use in the \text{crypto} command (see Section \([7]\)).

When this assumption is used with \text{DH\_subgroup}, \text{DH\_subgroup\_with\_is\_neutral}, \text{DH\_X25519}, \text{DH\_X448}, or \text{DH\_single\_coord\_ladder}, it must be applied to the subgroup, which can be done as for PRF-ODH1.

\[ \text{expand } \text{square\_PRF\_ODH2}(G, Z, \text{prf\_in}, \text{prf\_out}, g, \exp, \exp', \mult, \text{prf}, \text{p}, \text{sqp}). \]

says that the group \( G \) satisfies the square PRF-ODH2 assumption and the PRF-ODH2 assumption. The types \text{prf\_in} and \text{prf\_out} and the pseudo-random function \text{prf} are defined as for PRF-ODH1. The square PRF-ODH2 assumption means that an adversary that has a public Diffie-Hellman key \( \exp(g, a) \) for random \( a \) and has access to the oracle \((Y, x) \mapsto \text{prf}(\exp(Y, a), x)\) cannot distinguish \( x \mapsto \text{prf}(\exp(g, \mult(a, a)), x) \) from a random function. The probability \( \text{sqp}(t, n, n') \) is the probability of breaking the square PRF-ODH2 assumption in time \( t \) with \( n \) queries to \( \text{prf}(\exp(g, \mult(a, a)), x) \) and \( n' \)
queries to \((Y, x) \rightarrow prf(exp(Y, a), x)\). The probability \(p(t, n, n')\) is the probability of breaking the PRF-ODH2 assumption in time \(t\) with \(n\) queries to \(prf(exp(g, mult(a, b)), x)\) and \(n'\) queries to \((Y, x) \rightarrow prf(exp(Y, a), x)\) and \((X, x) \rightarrow prf(exp(X, b), x)\) in total. This macro defines the equivalence \(prf_odh(prf)\), which corresponds to the square PRF-ODH2 and PRF-ODH2 properties, for use in the crypto command (see Section 7). When this assumption is used with \(DH\_subgroup\), \(DH\_subgroup\_with\_is\_neutral\), \(DH\_X25519\), \(DH\_X448\), or \(DH\_single\_coord\_ladder\), it must be applied to the subgroup, which can be done as for PRF-ODH.

If \(G\) is Curve448, the weak private key \(kp\) must be excluded, which can be done using \(DH\_exclude\_weak\_keys\), \(DH\_X448\), or \(DH\_single\_coord\_ladder\).

Additionally, this assumption requires that it is possible to test efficiently whether \(exp(Y, a) = exp(g, ab)\) knowing just \(Y\) and \(B = exp(g, b)\) (so the result does not depend on \(a\)). This is possible for prime-order groups as well as Curve25519 and Curve448 when the weak private key is excluded.

The argument \(prf\) of the PRF-ODH macros is defined by these macros. It must not be declared elsewhere, and it can be used only after expanding the macro. All other arguments of these macros must be defined before expanding the macro.

- expand \(CDH\_single(G, Z, g, exp, exp', mult, p)\).
- expand \(CDH\_RSR\_single(G, Z, g, exp, exp', mult, p, p_0)\).
- expand \(DDH\_single(G, Z, g, exp, exp', mult, p)\).
- expand \(DDH\_RSR\_single(G, Z, g, exp, exp', mult, p, p_0)\).
- expand \(PRF\_ODH\_single(G, Z, prf\_in, prf\_out, g, exp, exp', mult, prf, p)\).
- expand \(PRF\_ODH2\_single(G, Z, prf\_in, prf\_out, g, exp, exp', mult, prf, p, PCollKey1)\).

are similar to macros with the same name without \_single\, except that they use a single family of exponents, \(a_i\), instead of two, \(a_i\) and \(b_j\). Obviously, they make no security claims on Diffie-Hellman between \(a_i\) and itself (because that is the square Diffie-Hellman property), but they guarantee security for Diffie-Hellman between \(a_i\) and \(a_j\) for any \(i \neq j\). That is more powerful than the properties without \_single\, because it allows proving protocols that rely on Diffie-Hellman computations between exponents in a single family, but may lead to larger probability bounds.

- \textit{expand Xor}(D, xor, zero). defines the function symbol xor to be exclusive or on the set of bitstrings \(D\), where zero is the bitstring consisting only of zeroes in \(D\). \(D\) should be fixed.

The type \(D\) must be declared before this macro is expanded. The function \(xor\) and the constant \(zero\) are declared by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

This macro defines the equivalence named \textit{remove_xor}(xor) for use in the crypto command (see Section 7).

- \textit{expand keygen}(keyseed, key, kgen). defines a key generation function \(kgen\). It can be used to add a key generation function to symmetric cryptographic primitives, if needed.

\(keyseed\) is the type of key seeds, must be bounded or nonuniform (to be able to generate random numbers from it), typically fixed, and large.

\(key\) type of keys, must be bounded.

\(kgen(keyseed): key\) is the key generation function.

The types \(keyseed\) and \(key\) must be declared before this macro is expanded. The function \(kgen\) is declared by this macro. It must not be declared elsewhere, and it can be used only after expanding the macro.

This macro defines the equivalence named \textit{keygen}(kgen) for use in the crypto command (see Section 7).
- **expand Auth_Enc_from_Enc_then_MAC**(key, cleartext, ciphertext, enc, dec, injbot, Z, Penc, Pmac), defines an authenticated encryption scheme, built by encrypt-then-MAC from an IND-CPA encryption scheme and an SUF-CMA deterministic MAC.

The arguments are the same as for IND_CP A_INT_CTX T_sym_enc except that Penc(t, N, l) is the probability of breaking the IND-CPA property of the underlying encryption scheme in time t for one key and N encryption queries with cleartexts of length at most l, and Pmac(t, N, N', Nu', l) is the probability of breaking the SUF-CMA property of the underlying MAC scheme in time t for one key, N MAC queries, N' verification queries modified by the transformation and Nu verification queries left unchanged by the transformation for messages of length at most l.

- **expand Auth_Enc_from_AEAD**(key, cleartext, ciphertext, enc, dec, injbot, Z, Penc, Pencctxt), defines an authenticated encryption scheme, built from an AEAD scheme using empty additional data.

The arguments are the same as for IND_CP A_INT_CTX T_sym_enc except that Penc(t, N, l) is the probability of breaking the IND-CPA property of the underlying AEAD scheme in time t for one key and N encryption queries with cleartexts of length at most l, and Pencctxt(t, N, N', l', ld, ld') is the probability of breaking the INT-CTX T property of the underlying AEAD scheme in time t for one key, N encryption queries, N' decryption queries with cleartexts of length at most l and ciphertexts of length at most l', additional data for encryption of length at most ld, and additional data for decryption of length at most ld'.

- **expand Auth_Enc_from_AEAD_nonce**(key, cleartext, ciphertext, enc, dec, injbot, Z, Penc, Pencctxt), defines an authenticated encryption scheme, built from an AEAD scheme with a nonce by choosing the nonce randomly at each encryption and using empty additional data.

The arguments are the same as for IND_CP A_INT_CTX T_sym_enc except that Penc(t, N, l) is the probability of breaking the IND-CPA property of the underlying AEAD scheme in time t for one key and N encryption queries with cleartexts of length at most l, and Pencctxt(t, N, N', l', ld, ld') is the probability of breaking the INT-CTX T property of the underlying AEAD scheme in time t for one key, N encryption queries, N' decryption queries with cleartexts of length at most l and ciphertexts of length at most l', additional data for encryption of length at most ld, and additional data for decryption of length at most ld'.

- **expand AEAD_from_Enc_then_MAC**(key, cleartext, ciphertext, add_data, enc, dec, injbot, Z, Penc, Pmac), defines an authenticated encryption scheme with additional data built by encrypt-then-MAC from an IND-CPA encryption scheme and an SUF-CMA deterministic MAC.

The arguments are the same as for AEAD except that Penc(t, N, l) is the probability of breaking the IND-CPA property of the underlying encryption scheme in time t for one key and N encryption queries with cleartexts of length at most l, and Pmac(t, N, N', Nu', l) is the probability of breaking the SUF-CMA property of the underlying MAC scheme in time t for one key, N MAC queries, N' verification queries modified by the transformation and Nu verification queries left unchanged by the transformation for messages of length at most l.

- **expand AEAD_from_AEAD_nonce**(key, cleartext, ciphertext, add_data, enc, dec, injbot, Z, Penc, Pencctxt), defines an authenticated encryption scheme with additional data, built from an AEAD scheme with a nonce by choosing the nonce randomly at each encryption.

The arguments are the same as for AEAD except that Penc(t, N, l) is the probability of breaking the IND-CPA property of the underlying AEAD scheme in time t for one key and N encryption queries with cleartexts of length at most l, and Pencctxt(t, N, N', l', ld, ld') is the probability of breaking the INT-CTX T property of the underlying AEAD scheme in time t for one key, N encryption queries, N' decryption queries with cleartexts of length at most l and ciphertexts of length at most l', additional data for encryption of length at most ld, and additional data for decryption of length at most ld'.

- **expand random_split**_N**(input_t, part1_t, ..., partN_t, tuple_t, tuple, split), defines allows to split a random value into N values, for N ≤ 10.
7 Interactive Mode

In interactive mode, the user specifies transformations to perform. Some of the instructions take a program point (or occurrence) in the current game as argument. One should use the command

```
In interactive mode, the user specifies transformations to perform. Some of the instructions take a program point (or occurrence) in the current game as argument. One should use the command
```

Before expanding the definition of \texttt{split}, this macro defines the equivalence named \texttt{splitter(split)} which replaces the splitting of a random number generation in \texttt{input\_t} with \texttt{N} independent random number generations in \texttt{part1\_t}, \ldots, \texttt{partN\_t}.

\texttt{input\_t, part1\_t, \ldots, partN\_t, tuple\_t} must be defined before expanding this macro. \texttt{tuple} and \texttt{split} are defined by this macro. They must not be declared elsewhere, and they can be used only after expanding the macro.

\begin{itemize}
\item an integer designates the program point labeled by that integer in the displayed game.
\item \texttt{before "regexp"} designates the program point at the beginning of the line that matches the regular expression \texttt{regexp}. Regular expressions follow the syntax of regular expressions in the OCaml \texttt{Str} module, see \url{https://ocaml.org/releases/4.14/api/Str.html}. In regular expressions, backslash (\texttt{\}) must be escaped as \texttt{\\}, as in OCaml string literals. There must be a single line that matches this regular expression, otherwise CryptoVerif shows an error message.
\item \texttt{after "regexp"} designates the program point at the beginning of the first line that has an occurrence number after the line that matches the regular expression \texttt{regexp}. There must be a single line that matches this regular expression, otherwise CryptoVerif shows an error message.
\item \texttt{before\_nth \texttt{n} "regexp"} designates the program point at the beginning of the \texttt{n}-th line that matches the regular expression \texttt{regexp}.
\item \texttt{after\_nth \texttt{n} "regexp"} designates the program point at the beginning of the first line that has an occurrence number after the \texttt{n}-th line that matches the regular expression \texttt{regexp}.
\item \texttt{at \texttt{n} \texttt{'}"regexp"} designates the program point at the \texttt{n\textquotesingle}'-th occurrence number that occurs inside the string that matches the regular expression \texttt{regexp} in the displayed game. There must be a single match for this regular expression, otherwise CryptoVerif shows an error message. (With \texttt{at}, if the same line matches the regular expression several times, it counts as several matches.)
\item \texttt{at\_nth \texttt{n} \texttt{'}"regexp"} designates the program point at the \texttt{n\textquotesingle}'-th occurrence number that occurs inside the string corresponding to the \texttt{n}-th match of the regular expression \texttt{regexp} in the displayed game. (With \texttt{at\_nth}, if the same line matches the regular expression several times, it counts as several matches.)
\end{itemize}
With before, after, before_nth, and after_nth, the match is performed on a game in which only occurrences of processes are displayed, at the beginning of lines. Therefore, the occurrence numbers typically do not appear in the regular expression given by the user, provided the regular expression does not require explicitly matching at the beginning of the line (i.e., the regular expression should not use ``). In contrast, with at and at_nth, the match is performed on a game in which all occurrence numbers are displayed. The regular expression needs to match at least one occurrence number. Any occurrence number can be matched by the regular expression `{0-9}+`.

Using an explicit integer to designate a program point is very unstable: it changes if the verified protocol is slightly modified, or if a new version of CryptoVerif itself is used, which may transform games in a slightly different way. The other ways of designating program points are therefore preferable when protocol is slightly modified, or if a new version of CryptoVerif itself is used, which may transform games.

In a slightly different way. The other ways of designating program points are therefore preferable when possible.

When an identifier is expected in an instruction, it is possible to put it between quotes. This is useful in particular for identifiers that clash with proof keywords.

Here is a list of available instructions:

- `help` or `?`: display a list of available commands.
- `remove_assign useless`: remove useless assignments, that is, assignments to \( x \) when \( x \) is unused and assignments between variables.
- `remove_assign find cond`: removes useless assignments, as above, as well as assignments let \( x = M \) in inside conditions of \( \text{find} \).
- `remove_assign binder \( x_1 \ldots x_n \)`: remove assignments to \( x_1,\ldots,x_n \) by replacing \( x_i \) with its value. When \( x_i \) becomes unused, its definition is removed. When \( x_i \) is used only in defined tests after transformation, its definition is replaced with a constant. The variables \( x_i \) may also be regular expressions, following the syntax of regular expressions in the OCaml Str module, see [https://ocaml.org/releases/4.14/api/Str.html](https://ocaml.org/releases/4.14/api/Str.html). In this case, they designate all variables that match the regular expression. This is particularly helpful to designate all variables that come from the same initial name but have different numbers: "\( \text{name}_1-[0-9]+ \)". Regular expressions need to be put between quotes because they use characters that do not belong to ordinary identifiers.

Blackslash (`\`) must then be escaped as `\\`, as in OCaml string literals.

- `use_variable \( x_1 \ldots x_n \)`: when \( x_i \) is defined by an assignment let \( x_i = M_i \), replace all occurrences of term \( M_i \) at which \( x_i \) is guaranteed to be defined by \( x_i \). The replacement is also performed with array accesses, that is, \( M_i[M/\bar{i}] \) is replaced with \( x_i[M] \), when \( x_i[M] \) is guaranteed to be defined, where \( \bar{i} \) are the current replication indices at the definition of \( x_i \). As in the command `remove_assign binder \( x_1 \ldots x_n \)`, the variables \( x_i \) may also be regular expressions, designating all variables that match the regular expression.

- `move \( m \)`: Try to move random number generations and assignments. It supports two versions.

  `move up \( x_1 \ldots x_n \) to occ` moves the random number generations or assignments of \( x_1,\ldots,x_n \) up in the syntax tree, to the program point \( occ \). This program point must correspond to an output process resp. oracle body. After the game transformation, a variable \( x \) (which may be among \( x_1,\ldots,x_n \)) is defined at program point \( occ \), and all other variables \( x_i \) are defined by let \( x_i = \text{in} \) in. All variables \( x_1,\ldots,x_n \) must have the same type. They must not be defined syntactically above the program point \( occ \). Either all variables \( x_1,\ldots,x_n \) must be defined by random number generations or all of them must be defined by assignments.

  - If \( x_1,\ldots,x_n \) are defined by random number generations, this transformation performs eager sampling of \( x_i \). The random number generation of \( x_1,\ldots,x_n \) must be executed at most once for each execution of program point \( occ \).

  - If \( x_1,\ldots,x_n \) are defined by assignments of terms \( M_i \), then all \( M_i \) must consist of variables, function applications, and tests; there must be one \( M_i \) defined at program point \( occ \) (which will be used as the definition of \( x_i \)); and all terms \( M_i \) must be equal.

For all other values of \( m \), `move \( m \)` moves random number generations and assignments down in the syntax tree.
- It moves random number generations down in the syntax tree as much as possible, in order to delay the choice of random numbers (lazy sampling). This is especially useful when the random number generations can be moved under a test \( \text{if, let, or find} \), so that we can distinguish in which branch of the test the random number is created by a subsequent \text{SArename} instruction.

- It moves assignments down in the syntax tree but without duplicating them. This is especially useful when the assignment can be moved under a test, in which the assigned variable is used only in one branch. In this case, the assigned term is computed in fewer cases thanks to this transformation. (Note that only assignments without array accesses can be moved, because in the presence of array accesses, the computation would have to be kept in all branches of the test, yielding a duplication that we want to avoid.)

Only the random number generations and assignment at the process level can be moved. (Those that are terms will be left unchanged.) The argument \( m \) specifies which instructions should be moved:

- all: move random number generations and assignments, when this is beneficial, that is, when they can be moved under a test.
- noarrayref: move random number generations and assignments without array accesses, when this is beneficial.
- random: move random number generations, when this is beneficial.
- random_noarrayref: move random number generations without array accesses, when this is beneficial.
- assign: move assignments, when this is beneficial.
- binder \( x_1 \ldots x_n \): move random number generations and assignments that define \( x_1, \ldots, x_n \) (even when this is not beneficial). The variables \( x_i \) may also be regular expressions.
- array \( x ["exp", \ldots, "exp"] \): move random number generations that define \( x \) when \( x \) is of a bounded or nonuniform type and \( x \) is not used in the process that defines it, until the next output after the definition of \( x \). \( x \) is then chosen at the point where it is really first used. (Since this point may depend on the trace, the uses of \( x \) are often transformed into \text{find} instructions that test whether \( x \) has been chosen before, and reuse the previously chosen value if this is true.) This transformation provides a stronger form of lazy sampling than other variants of \text{move}.

The expressions "exp" allow the user to specify expressions that do not require the generation of \( x \) when it has not been generated before, because the expression always yields the same result when \( x \) is a fresh random value, up to negligible probability. More precisely, these expressions must be of the form

\[
\text{forall seq(vartype);} \text{ new (ident):(ident); } \text{ (simpler term)}
\]

The expression can be forall \( y_1 : T_1, \ldots, y_n : T_n; \text{ new } x' : T; M \), where \( T \) is the type of \( x \) and \( y_1, \ldots, y_n, x' \) are the variables of \( M \). CryptoVerif tries to simplify \( M \) into a term \( M' \) that does not contain \( x' \), assuming that \( x' \) is random and \( y_1, \ldots, y_n \) are independent of \( x' \). If it fails, the move array transformation fails. If it succeeds, the transformation can be performed, replacing \( M\{x/x'\} \) with \( M' \) instead of generating a fresh \( x \).

When no expression "exp" is mentioned, the expressions that do not require the generation of \( x \) are equality tests with \( x \), and the type \( T \) of \( x \) must be large enough, so that collisions between \( x \) and a value independent of \( x \) can be eliminated (\( \text{PcollRand}(T) \leq 2^{-n'} \)), that is, \( T \) has option \text{pcolln} with \( n \geq n' \) where \( n' \) is set by \( \text{set minAutoCollElim} = \text{pest } n' \); the default is \( n' = 80 \).

The variables \( x \) may also be a regular expression. In this case, it designates all variables that match the regular expression; all these variables must have the same type.

- simplify: simplify the game.
• \texttt{simplify\ coll\_elim}(variables: x_1, \ldots, x_n; types: t_1, \ldots, t_n'; terms: occ_1, \ldots, occ_n'')\): simplify the game, additionally allowing elimination of collisions on data at all occurrences of variables x_1, \ldots, x_n, at all data of types t_1, \ldots, t_n', and at the program points occ_1, \ldots, occ_n''. See above for how to specify the program points occ_i. Some of the lists of variables, types, or terms may be omitted. In this case, the separating semi-colon \ was obviously omitted as well. It is also possible to reorder or repeat these lists; the lists add up. (The probability of the collision must still satisfy the condition given by \texttt{allowed\_collisions}.)

• \texttt{global\_dep\_anal \ x} performs global dependency analysis on \ x: it computes all variables that depend on \ x, and when possible, shows that all output messages are independent of \ x and that all tests are independent of \ x after eliminating collisions. The tests are then simplified by eliminating these collisions, so that all dependencies on \ x can be removed.

\texttt{global\_dep\_anal \ x\ coll\_elim}(variables: x_1, \ldots, x_n; types: t_1, \ldots, t_n'; terms: occ_1, \ldots, occ_n'') performs global dependency analysis on \ x, additionally allowing elimination of collisions on data at all occurrences of variables x_1, \ldots, x_n, at all data of types t_1, \ldots, t_n', and at the program points occ_1, \ldots, occ_n''\). See above for how to specify the program points occ_i. Some of the lists of variables, types, or terms may be omitted. In this case, the separating semi-colon \ was obviously omitted as well. It is also possible to reorder or repeat these lists; the lists add up. (The probability of the collision must still satisfy the condition given by \texttt{allowed\_collisions}.)

One must allow elimination on \ x independently of the program point, so if \ x is not large, \ x must be mentioned in x_1, \ldots, x_n or its type must be mentioned in t_1, \ldots, t_n; mentioning the occurrences of \ x in occ_1, \ldots, occ_n' is not sufficient.

The variable \ x may also be a regular expression. In this case, it designates all variables that match the regular expression, and the command \texttt{global\_dep\_anal} is executed for each of these variables in turn.

• \texttt{S\_rename \ x}: When \ x is defined at several places, rename \ x to a different name for each definition. This is useful for distinguishing cases depending on which definition of \ x is used. The variable \ x may also be a regular expression. In this case, it designates all variables that match the regular expression, and the command \texttt{S\_rename} is executed for each of these variables in turn.

• \texttt{S\_rename\ random}: Renames all variables defined by \texttt{new} or \texttt{<-R} that have several definitions and no array accesses to distinct names.

• \texttt{all\_simplify}: perform several simplifications on the game, as if
  
  - simplify,
  - \texttt{move\ all} if \texttt{auto\_Move} = true,
  - \texttt{remove\_assign\ useless} if \texttt{auto\_Remove\_Assign\_Find\_Cond} = false,
  - \texttt{remove\_assign\ find\_cond} if \texttt{auto\_Remove\_Assign\_Find\_Cond} = true,
  - \texttt{S\_rename\ random} if \texttt{auto\_S\_Rename} = true,
  - \texttt{and\ merge\_branches} if \texttt{auto\_Merge\_Branches} = true

  had been called.

• \texttt{expand}: expand if, let, find, event, event\_abort, new terms into processes. That leads to distinguishing the branches until the end of the process, which may help the proof by distinguishing more cases, but may lead to very large games. This is also needed because some game transformations of CryptoVerif do not support non-expanded games. When \texttt{auto\_Expand} = true (the default), this expansion is performed automatically in case a game transformation results in a non-expanded game.

• \texttt{crypto (crypto\_args)}: applies a cryptographic transformation that comes from a statement \texttt{equiv}. This command can have two forms:
crypto: list all available equiv statements, and ask the user to choose which one should be applied, with which special arguments when the chosen equivalence is generated by equiv...special, and with which (info) as described below.

crypto (name) [special(seq(spclargs))] (info): apply a cryptographic transformation determined by the name (name), where:

- (name) can be either an identifier id or id(f), and corresponds to the name given at the declaration of the cryptographic transformation by equiv. In case the name is not found, CryptoVerif reverts to the old way of designating cryptographic transformations, in which (name) can be either a function symbol that occurs in the terms in the left-hand side of the equiv statement, or a probability function that occurs in the probability formula of the equiv statement. When several equivalences correspond, the user is prompted for choice.

- special(seq(spclargs)), when present, passes the given special arguments to the generation of the chosen equivalence, which must be defined by equiv...special. The exact meaning of the arguments depend on the considered special equivalence.

1. For the special equivalences *rom, prf, prp, sprp, and icm there must be at most one special argument, and when one argument is present, it overrides the collisions_LHS argument of the special equivalence.

2. For the special equivalences *rom_partial, prf_partial, prp_partial, sprp_partial, and icm_partial there must be at most two special arguments, and when such arguments are present, one of them overrides the collisions_LHS argument of the special equivalence, and the other one determines the collision matrix between oracles. CryptoVerif determines which argument is which based on their type (tuple of strings for collisions_LHS, one string for the collision matrix).

See equiv...special for more information.

- (info) can be

1. *: The transformation is applied as many times as possible. (In this case, the advised transformations are applied automatically even when set autoAdvice = false.)

2. **: Similar to *, but the game is simplified only after the last cryptographic transformation instead of simplifying it after each transformation, for faster execution. This is recommended only for very simple cryptographic transformations.

3. x1 ... xn: apply the cryptographic transformation, where x1, ..., xn are variable names of the game corresponding to random number generations in the left-hand side of the equivalence. (CryptoVerif may automatically add variables to the list x1, ..., xn if needed, except when a dot is added at the end of the list x1, ..., xn. The transformation is applied only once. If several disjoint lists x1, ..., xn are possible and no variable name is mentioned, CryptoVerif makes a choice. It is better to mention at least one variable name when the left-hand side of the equivalence contains a random number generation, to make explicit which transformation should be applied.)

In case the command ends with a dot (.), CryptoVerif never adds other variable names to those already listed. If the dot is absent, CryptoVerif may add other variable names if that seems necessary to perform the transformation.

The variables xi may also be regular expressions. In this case, they designate all variables that match the regular expression.

4. [variables: x1->y1, ..., xn->yn; terms: occ1->O1, ..., occm->On]: apply the cryptographic transformation, where

(a) x1, ..., xn are variable names of the game which correspond to random number generations y1, ..., yn respectively in the left-hand side of the equivalence. (CryptoVerif may automatically add variables to the list x1->y1, ..., xn->yn if needed, except when a dot is added at the end of this list.)

The variables xi may also be regular expressions. In this case, they designate all variables that match the regular expression, and they are mapped to the same variable yi in the equivalence.
(b) \( occ_1, \ldots, occ_m \) are program points at which terms will be transformed using oracles \( O_1, \ldots, O_m \) respectively of the equivalence. See above for how to specify the program points \( occ \). (CryptoVerif may automatically add elements to the list \( occ_1 \rightarrow O_1, \ldots, occ_m \rightarrow O_m \) if needed, except when a dot is added at the end of this list.) When the considered equivalence is defined inside a macro, macro expansion may add an integer suffix \( k \) to the variable and oracle names of the equivalence (or may modify that suffix if they already have one). This suffix must be included in the variable and oracle names used in this command. This happens in particular for primitives defined in the library of primitives of CryptoVerif. The right value of \( k \) in the suffix can be determined by issuing a command \( \text{crypto} \) without further indication. This command will display the equivalences as they are stored by CryptoVerif after macro expansion. It can also be determined using the commands \( \text{show_equiv} \) and \( \text{out_equiv} \).

One of the lists of variables or terms may be omitted. In this case, the separating semicolon ; is obviously omitted as well. It is also possible to reorder or repeat the variables and/or terms lists; the lists add up.

- \text{insert\_event} \( e \ occ \) replaces the subprocess or term at program point \( occ \) with the event \( \text{event\_abort} \ e \). The games may be distinguished if and only if the event \( e \) is executed, and CryptoVerif then tries to find a bound for the probability of executing that event. See above for how to specify the program point \( occ \). The program point \( occ \) must correspond to an input process (resp. oracle body in the oracles front-end) or to a term not in a condition of \( \text{find} \) nor in the channel of an input.

When the setting \( \text{autoExpand} \) is true and the occurrence \( occ \) corresponds to a term, the game is automatically expanded after inserting the event, so that after expansion the event occurs in a process, not in a term.

- \text{insert} \( \text{"(ins)"} \) inserts instruction \( \langle \text{ins} \rangle \) at program point \( occ \). The instruction \( \langle \text{ins} \rangle \) can be

\[
\begin{align*}
\text{new} \ &\langle \text{id} \rangle: \langle \text{id} \rangle; \langle \text{ins} \rangle \\
\langle \text{id} \rangle &\leftarrow R \langle \text{id} \rangle; \langle \text{ins} \rangle \\
\text{event\_abort} \ &\langle \text{id} \rangle \\
\text{if} \ &\langle \text{cond} \rangle \ \text{then} \ \langle \text{ins} \rangle \ [\text{else} \ \langle \text{ins} \rangle] \\
\text{let} \ &\langle \text{pattern} \rangle = \langle \text{term} \rangle \ \text{in} \ \langle \text{ins} \rangle \ [\text{else} \ \langle \text{ins} \rangle] \\
\langle \text{basicpat} \rangle &\leftarrow \langle \text{term} \rangle; \langle \text{ins} \rangle \\
\text{find}[\text{unique}] \ &\text{findbranch} \ [\text{orfind} \ \text{findbranch} \]^* \ [\text{else} \ \langle \text{ins} \rangle] \\
\langle \text{ins} \rangle &\quad \langle \text{empty} \rangle
\end{align*}
\]

where \( \langle \text{findbranch} \rangle := \langle \text{seq} \langle \text{id} \rangle \text{bound} \rangle \) such that \( \langle \text{cond} \rangle \ \text{then} \ \langle \text{ins} \rangle \). The empty instruction is replaced by the code that follows the insertion point. In all cases except \( \text{event\_abort} \ e \), the code that follows the insertion point is executed after the inserted instruction. The probability of distinguishing the game before insertion from the game after insertion is then at most of the probability of the events \( \text{event\_abort} \ e \) in the inserted instruction. CryptoVerif then tries to bound this probability. This is similar to \text{insert\_event} \( e \ occ \). However, the \text{insert} command does not subsume \text{insert\_event}, because \text{insert} allows inserting only at process points while \text{insert\_event} allows inserting events at term points as well.

The instruction \( \langle \text{ins} \rangle \) is equivalent to \( \langle \text{ins} \rangle \). The parentheses just help resolving ambiguities of the grammar, for instance to specify to which process \( \text{else} \) branches are attached.

The main practical usage of this command is to introduce case distinctions (if, find, or let with a pattern that is not a variable). In this situation, the process that follows the insertion point is duplicated in each branch of if, find, or let, and can subsequently be transformed in different ways in each branch. It may be useful to disable the merging of branches in simplification by \text{set autoMergeBranches = false} when a case distinction is inserted, so that the operation is not immediately undone at the next simplification.
In contrast to the initial game, the terms event, event_abort, get, insert, new, if, find, or let are not expanded, so terms if, find, let and its synonym <- can occur only in conditions of find; event, event_abort, get, insert, new and its synonym <-R must not occur as a term. The variables of the inserted instruction are not renamed, so one must be careful when redefining variables with the same name. In particular, one is not allowed to add a new definition for a variable on which array accesses are done (because it could change the result of these array accesses). The obtained game must satisfy the required invariants (each variable is defined at most once in each branch of if, find, or let; each usage of a variable x must be either x without array index syntactically under its definition, inside a defined condition of a find, or x[M1, . . . , Mn] under a defined condition that contains x[M1, . . . , Mn] as a subterm). In case the inserted instruction is not appropriate, an error message explaining the problem is displayed.

See above for how to specify the program point occ. The program point occ must correspond to an output process (resp. oracle body in the oracles front-end).

• replace occ "term" replaces the term at program point occ with the term term. Obviously, CryptoVerif must be able to prove that these two terms are equal. These terms must not contain if, let, find, new, event, event_abort, insert, get. See above for how to specify the program point occ. The program point occ must correspond to a term not containing if, let, find, new, event, event_abort, insert, get.

• assume replace occ "term" does the same thing as replace occ "term", but does not check that the term at program point occ is equal the term term, hence the replacement may not be correct. This command is present only to allow testing whether a proof would succeed if some replacement could be done. If you make a proof by relying on this command, CryptoVerif still considers that the query is not proved.

• merge_branches merges the branches of if, find, and let when they execute equivalent code. Such a merging is already done in simplification, but merge_branches goes further. It performs several merges simultaneously and takes into account that merges may remove array accesses in conditions of find and thus allow further merges. Moreover, it advises merge_arrays when variables with different names and with array accesses are used in the branches that we may want to merge.

• merge_arrays x_1 1 . . . x_1 n , . . . , x_k 1 . . . x_k n takes as argument k lists of n variables separated by commas. It merges the variables x_1 1 , . . . , x_1 n into x_1 1 . This is useful when these variables play the same role in different branches of if, find, let: merging them into a single variable may allow to merge the branches of if, find, let by merge_branches.

The k lists to merge must contain the same number of variables n (at least 2). Variables x_ij and x_i j' for i ̸= i' must never be simultaneously defined for the same value of their array indices. Variables x_ij must have the same type and the same array indices for all j. Each variable x_ij must have a single definition, and must not be used in queries.

In general, the variables x_ij should preferably belong to the else branch of the if, find, let that we want to merge later. Indeed, the code of the else branch is often more general than the code of the other branches (which may exploit the conditions that are tested), so merging towards the code of the else branch works more often.

The variables x_ij should preferably be defined above the variables x_ij for any i > 1. If this is true, we can introduce special variables y_j at the definition site of x_ij which are used only for testing that branch j has been executed. This allows the merge to succeed more often.

• guess (guessspec) guesses the value of (guessspec), where (guessspec) can be one of the following:

1. i, where i is a replication index: one guesses the value of the replication index i in the tested session. (The other sessions still exist, but one does not try to prove queries for them.) There must be a single replication with index i in the game.

2. occ, where occ is the occurrence of a replication; then one guesses the value of the replication index i of that replication in the tested session.
3. If $i \&\&$ above, where $i$ is a replication index; then, just under the replication with index $i$, one guesses the value of the whole sequence of replication indices above the replication with index $i$ in the tested session. There must be a single replication with index $i$ in the game.

4. If $\text{occ} \&\&$ above, where $\text{occ}$ is the occurrence of a replication; then, just under that replication, one guesses the value of the whole sequence of replication indices above that replication in the tested session.

5. "$x[i_1, \ldots, i_n]"$, where $x[i_1, \ldots, i_n]$ is the variable to be guessed, defined under $n$ replications, and $i_1, \ldots, i_n$ are constant replication indices (typically produced by a previous guess of the replication indices). CryptoVerif must be able to determine, at each definition of $x$, whether its indices will be equal to $i_1, \ldots, i_n$ or not. Otherwise, the transformation fails. When $x$ is defined under no replication, one writes $x$ instead of "$x[i_1, \ldots, i_n]"$.

CryptoVerif distinguishes whether the element specified by $\langle \text{guessspec} \rangle$ is equal to a constant value $v_{\text{tested}}$ by introducing a test under the definition of that element, and tries to prove the security properties for $\langle \text{guessspec} \rangle = v_{\text{tested}}$. The queries are adjusted accordingly. The probability of breaking the initial query is typically the size of the guessed element $\langle \text{guessspec} \rangle$ (e.g. $N$ when we guess a replication index $i$ in $[1, N]$; $\#O$ when we guess the whole sequence of indices above a replication just above oracle $O$; $|T|$ when we guess a variable $x$ of type $T$) times the probability of breaking the query for $\langle \text{guessspec} \rangle = v_{\text{tested}}$. The size of the guessed element must be estimated less than $\text{maxGuess}$ (see the command set $\text{maxGuess}$).

Guessing the value of replication indices cannot apply to injective correspondences. When we guess replication indices and injective correspondences are present, CryptoVerif tries to prove injectivity, so that only a non-injective correspondence remains to prove. It that fails, injective correspondences are left unchanged and proved on all sessions. If all queries are injective correspondences for which that fails, the transformation fails. This transformation does not apply to equivalence and query_equiv proofs. The transformation fails if such a proof is still required.

- **guess "$x[i_1, \ldots, i_n]"$** no_test guesses the value of $x[i_1, \ldots, i_n]$, where $x[i_1, \ldots, i_n]$ is defined under $n$ replications, and $i_1, \ldots, i_n$ are constant replication indices (typically produced by a previous guess of the replication indices). CryptoVerif must be able to determine, at each definition of $x$, whether its indices will be equal to $i_1, \ldots, i_n$ or not. Otherwise, the transformation fails. When $x$ is defined under no replication, one writes $x$ instead of "$x[i_1, \ldots, i_n]"$. The variable $x$ must be defined by let $x = \ldots$

CryptoVerif replaces the definition of $x$ with a constant value $v_{\text{tested}}$. When the definition of $x$ is not a simple term (a term built from replication indices, variables, and function applications), the old definition is still evaluated but ignored.

Assuming $x$ is a variable of type $T$, the probability of breaking the initial query is $|T|$ times the probability of breaking the query for $x[i_1, \ldots, i_n] = v_{\text{tested}}$. $|T|$ must be estimated less than $\text{maxGuess}$ (see the command set $\text{maxGuess}$).

This transformation does not apply to secrecy queries, equivalence, and query_equiv proofs. The transformation fails if such a proof is still required.

- **guess_branch occ** guesses which branch is taken at program point $\text{occ}$. The instruction at program point $\text{occ}$ must be a test (if, let, or find) with at least two branches. This instruction must be executed at most once (either because it is not under replication, and because it is under replication and the replication indices are fixed, for instance because they have previously been guessed by the guess instruction above). If this instruction has $n$ branches, CryptoVerif generates $n$ games $G_i$ ($0 \leq i < n$) in which branch $i$ is kept and all other branches are replaced with an event bad_guess. (Branch 0 is the else branch.) The desired queries must then be proved in all games $G_i$ and the probability of breaking the queries in the initial game is bounded by the sum of the probabilities of breaking them in all games $G_i$. That allows the user to split cases depending on which branch is taken at program point $\text{occ}$.
The user first needs to prove the queries in game $G_0$. Once all queries are proved in this game, CryptoV erif automatically goes back and asks the user to prove the queries in next game, until they are proved in all games $G_i$.

In case the user is unable to prove some queries in a game $G_i$, it is blocked: it cannot consider the following games. In that case, the best is probably to remove the queries that cannot be proved and restart the proof. One can also undo the transformations until before guess_branch, use focus to limit oneself to the queries that can be proved and redo the proof from guess_branch.

This transformation does not apply to equivalence and query_equiv proofs. The transformation fails if such a proof is still required.

- **guess_branch occ no_test** guesses which branch is taken at program point occ. The instruction at program point occ must be a test if. This instruction must be executed at most once (either because it is not under replication, and because it is under replication and the replication indices are fixed, for instance because they have previously been guessed by the guess instruction above). CryptoV erif generates 2 games $G_0$ and $G_1$, keeping respectively only the else branch and the then branch. The test is removed. If the condition of the test is not a simple term (a term built from replication indices, variables, and function applications), it is still evaluated but ignored. The desired queries must then be proved in both games $G_i$ and the probability of breaking the queries in the initial game is bounded by the sum of the probabilities of breaking them in both games $G_i$. That allows the user to split cases depending on which branch is taken at program point occ.

The user first needs to prove the queries in game $G_0$. Once all queries are proved in this game, CryptoV erif automatically goes back and asks the user to prove the queries in game $G_1$.

In case the user is unable to prove some queries in a game $G_i$, it is blocked: it cannot consider the following games. In that case, the best is probably to remove the queries that cannot be proved and restart the proof. One can also undo the transformations until before guess_branch, use focus to limit oneself to the queries that can be proved and redo the proof from guess_branch.

This transformation does not apply to secrecy queries, equivalence, and query_equiv proofs. The transformation fails if such a proof is still required.

- **move_if_fun arg** moves the predefined function if_fun or transforms it into a term if ... then ... else ... It supports the following variants:
  - **move_if_fun loc1 ... locn** where each locj is either a program point or a function symbol. When locj is a program point, moves occurrences of if_fun from inside the term at that program point to the root of that term. When locj is a function symbol, moves occurrences of if_fun from under that function symbol to just above it.
  - **move_if_fun level n**, where n is a positive integer. Moves occurrences of if_fun n function symbols up in the syntax tree (provided those if_fun occur under at least n function symbols).
  - **move_if_fun to_term occ1 ... occn** transforms the function symbols if_fun that occur at program points occ1, ..., occn into terms if ... then ... else ... When no program point is given, performs that transformation everywhere in the game. When autoExpand = true (the default), a call to expand is automatically performed after move_if_fun, which transforms the terms if ... then ... else ... into processes.

- **start_from_other_end**: for proofs of indistinguishability only (equivalence), instruct CryptoV erif to start transforming from the other game. When your input file contains equivalence $Q_1 Q_2$, CryptoV erif initially works on the first process $Q_1$. When you issue the command start_from_other_end, CryptoV erif stores your current state, and starts working from $Q_2$. If you issue start_from_other_end again, it will store what you did from $Q_2$, and will restart working from the end of the sequence that you built from $Q_1$. This command allows you to alternate between the sequence that starts from $Q_1$ and the one that starts from $Q_2$. The property is proved when both sequences end with the same game (which you can check with the command success, as usual).

- **quit**: terminate execution.
success: test whether the desired properties are proved in the current game. If yes, display the proof and stop. Otherwise, wait for further instructions.

success simplify: run success then simplify, with the following addition. The command success collects information that is known to be true when the adversary manages to break at least one of the desired properties. The first iteration of simplify removes parts of the game that contradict this information and replaces them with event_abort adv_loses.

show_game: display the current game.

show_game occ: display the current game with occurrence numbers. Useful for some commands that require specifying a program point; see above for how program point are specified.

show_state: display the whole sequence of games until the current game.

show_facts occ: show the facts that are proved by CryptoVerif in the current game, at the program point occ. See above for how to specify the program point occ. This command is mainly helpful for debugging.

show_equiv (crypto_args): display the game equivalence corresponding to the cryptographic transformation specified by (crypto_args). These arguments are the same as for the crypto command. This command is useful to determine the exact variable and oracle names of an equivalence and to examine and possibly modify equivalences generated by equiv ... special.

show_commands: display the interactive commands executed so far (or from the last change of output file by out_commands).

out_game f: output the current game to file f. By default, f is output in the current directory. If the command-line option -o directory was given, f is output in the given directory. Only the digits, ascii letters, and %+-.=@_~ are allowed in the filename f. The dot (.) is not allowed as first character. (Be careful: file f will be overwritten if it already exists.)

out_game f occ: output the current game with occurrence numbers to file f. Useful for some commands that require specifying a program point; see above for how occurrences are specified. (See command out_game for details on the filename f. Be careful: file f will be overwritten if it already exists.)

out_state f: output the whole sequence of games until the current game to file f. (See command out_game for details on the filename f. Be careful: file f will be overwritten if it already exists.)

out_facts f occ: output the facts that are proved by CryptoVerif in the current game, at the program point occ, to file f. See above for how to specify the program point occ. This command is mainly helpful for debugging. (See command out_game for details on the filename f. Be careful: file f will be overwritten if it already exists.)

out_equiv f (crypto_args): output the game equivalence corresponding to the cryptographic transformation specified by (crypto_args) to the file f. The arguments (crypto_args) are the same as for the crypto command. This command is useful to determine the exact variable and oracle names of an equivalence and to examine and possibly modify equivalences generated by equiv ... special. (See command out_game for details on the filename f. Be careful: file f will be overwritten if it already exists.)

out_commands f: output the executed interactive commands to file f. If no output file was specified before, outputs both the previous and future interactive commands to f. If an output file was specified before (by the command-line setting -o commands or by a previous command out_commands), the previous commands are output to the previously specified file, and the future commands are output to f. If f is the empty string "", stops outputting interactive commands. (See command out_game for details on the filename f. Be careful: file f will be overwritten if it already exists.)
• auto: switch to automatic mode; try to terminate the proof automatically from the current game.

• set (parameter) = (value): sets parameters, as the set instruction in input files.

• allowed_collisions determines when to eliminate collisions. This command has two variants:
  
  - allowed_collisions (formulas): (formulas) is a comma-separated list of formulas of the form 
    \((\text{psize})_1^{n_1} \cdots \cdot (\text{psize})_k^{n_k}/\text{(pest)}\), where the exponents \(n_i\) can be omitted when equal to
    \(1\), writing \((\text{psize})\), instead of \((\text{psize})_1\), and the whole factor \((\text{psize})_1^{n_1} \cdots \cdot (\text{psize})_k^{n_k}\) is
    replaced with \(1\) when there is no \((\text{psize})_i\), factor at all; \((\text{psize})\), is an identifier that determines
    the size of a parameter: \(\text{size}\) for parameters of size \(n\), meaning that the parameter is at
    most \(2^n\); \(\text{small}\) for size 2; \(\text{passive}\) or \(\text{default}\) for size 30; \(\text{noninteractive}\) for size 80; \((\text{pest})\)
    (probability estimate) is an identifier such that \(1/(\text{pest})\) estimates a probability. It can take the following values: \(\text{psize}\) means that the probability \(1/(\text{pest})\) is at most \(2^{-n}\); \(\text{password}\) is equivalent to \(\text{pest}20\), i.e. the probability \(1/(\text{pest})\) is at most \(2^{-20}\); \(\text{large}\) is equivalent to
    \(\text{pest}160\), i.e. the probability \(1/(\text{pest})\) is at most \(2^{-160}\). (See also the declarations \(\text{param}\),
    \(\text{proba}\), and \(\text{type}\) for type explanations of these estimates.)

  Collisions are eliminated when, for some formula \((\text{psize})_1^{n_1} \cdots \cdot (\text{psize})_k^{n_k}/\text{(pest)}\) in the
  list (formulas), their probability is at most of the form \(\text{constant} \times p_1^{n_1} \cdots \cdot p_k^{n_k} \times \text{proba}\),
  where \(p_i\) is a parameter of size at most \((\text{psize})_i\), and the estimate of the probability \(\text{proba}\) is
  at most \(1/(\text{pest})\). This condition is applied both for collisions between elements of a type \(T\),
  in which case \(\text{proba} = \text{Pcoll1rand}(T)\), and for collision statements, in which case \(\text{proba}\) is
  the probability given in the collision statement. When the list of formulas (formulas) is
  empty, elimination of collisions is entirely disabled.

  By default, collisions are eliminated for \(\text{anything} \times \text{proba}\) when \(\text{proba} \leq 2^{-155}\) (where \(\text{large}\)
  would mean \(2^{-160}\), to allow collisions that have probability a small factor times collisions
  between elements of a \(\text{large}\) type), and for \(\text{p} \times \text{proba}\) when \(p \leq 2^{20}\) (\(\text{small}\) and \(\text{proba} \leq 2^{-20}\)
  (\(\text{password}\)). The default behavior is inspired by what happens in asymptotic security: \(\text{large}\)
  means that the probability of collision is asymptotically negligible, while the parameters are
  always polynomial, so \(\text{constant}\times p_1^{n_1} \cdots \cdot p_k^{n_k} \times \text{Pcoll1rand}(T)\) is negligible when \(T\) is large.

  Similarly, probabilities given in collision statements are always negligible (probabilities are
  declared \(\text{large}\) by default), while the parameters are always polynomial, so the probability
  obtained by applying \(\text{constant}\times p_1^{n_1} \cdots \cdot p_k^{n_k}\) times a collision statement remains negligible.

  - allowed_collisions (pest), where \((\text{pest})\) estimates a probability: \(\text{psize}\) means that the probability
    is at most \(2^{-n}\); \(\text{password}\) is equivalent to \(\text{pest}20\), i.e. probability at most \(2^{-20}\); \(\text{large}\)
    is equivalent to \(\text{pest}160\), i.e. probability at most \(2^{-160}\). Collisions are eliminated when
    their probability, taking into account how many times they are applied, is at most the
    probability specified by \((\text{pest})\). This behavior fits the exact security framework nicely: we
    eliminate collisions when they have a small enough probability.

• focus "(querydecl)", . . . , "(querydecl)" where (querydecl) := query seq(varypeb); | (query); | (query)" follows the syntax of query declarations given in Section 3 without the final dot: tell
  CryptoVerif to try to prove only the mentioned queries, ignoring all other queries. That sometimes
  allows to simplify the game further (e.g. remove events that are not used in the queries on which
  we focus), and may allow to prove the mentioned queries. The queries are considered equal modulo
  renaming of variables declared in seq(varypeb). When there is no ambiguity, the public variables
  of the queries can be omitted. When the queries on which we focus are all proved, CryptoVerif goes
  back to the state before the last focus command, to try to prove the other queries. undo focus
  also goes back to the state before the last focus command, to try to prove remaining queries.

• tag t: tag the current state with tag t (which can be an identifier or a string). This is useful to
  mark the current state and be able to go back to that state with the command undo t.

• undo: undo the last transformation.

• undo n: undo the last n transformations.

• undo focus: go back to the state before the last focus command.
- undo $t$: undo the transformations until the last state tagged $t$.
- restart: restart the proof from the beginning. (Still simplify automatically the first game.)
- interactive: starts interactive mode. Allowed in proof environments, but not when one is already in interactive mode. Useful to start interactive mode after some proof steps.
- forget_old_games: removes games before the current one from memory. That allows to save some memory, but prevents undo and undo n. However, tagged states are not removed from memory, so that the command undo $t$ where $t$ is a tag still works. Similarly, states before focus commands are not removed from memory, so that the command undo focus still works. The display of the games is saved into a temporary file to allow displaying the games at the end of the proof. You can save more memory by applying this command systematically with the setting set forgetOldGames = true.

Ctrl-C allows to interrupt a command in interactive mode, and go back to the state before the beginning of this command. This feature can be helpful when a command is very slow, to be able to try another command without waiting for the current command to terminate. It may not work under Windows.

The following indications can help finding a proof:

- When a message contains several nested cryptographic primitives, it is in general better to apply first the security definition of the outermost primitive.
- In order to distinguish more cases, one can start by applying the security of primitives used in the first messages, before applying the security of primitives used in later messages.

Using a text editor such as emacs to look at games output by out_game can be helpful, in order to use the search function to look for definitions or usages of variables in large games. For example, when trying to prove secrecy of $x$, one may look for usages of $x$, for definitions of $x$, and for usages of other variables used in those definitions.

8 Output of the system

The system outputs the executed transformations when it performs them. At the end, it outputs the sequence of games that leads to the proof of the desired properties. Between consecutive games, it prints the name of the performed transformation and details of what it actually did, and the formula giving the difference of probability between these games (if it is not 0). The description of the transformation between game may refer to program points in the previous game. These program points may not be completely accurate for the following reasons:

- When a step of the transformations transforms the same part of the game as a previous step, the program point in the second step actually refers to the code generated by the previous step, so it is not found in the previously displayed game.
- When a step transforms part of the game that was duplicated by a previous step of the transformation, the displayed program point is in fact ambiguous: one does not know which of the copies is actually transformed.

One can usually clarify the ambiguities by looking at the previous and next games.

Lines that begin with RESULT give the proved results. They may indicate that a property is proved and give an upper bound of the probability that the adversary breaks the property. These probabilities use the same notations are probabilities given as input for CryptoVerif, with the following addition: in the channel front-end, #c designates the total number of inputs performed on channel c. This notation mimics the notation #O for the number of oracles calls in the oracle front-end. The notation #c is used only when the channel names satisfy the same constraints as those required for oracle names: inputs on the same channel c must not occur on both sides of a parallel composition $Q | Q'$; an input on channel c must not occur under an input on the same channel c in the syntax tree; and inputs in different branches of if, find, let, get must have compatible structures (inputs on the same channel must occur at the
same place in the sequence of possible inputs). These constraints make sure that the usage of \#c does not mix unrelated inputs. When they are not satisfied, a warning is displayed and CryptoVerif uses only replication bounds for counting inputs.

In the end, they may also list the properties that could not be proved, if any.

When the `-tex` command-line option is specified, CryptoVerif also outputs a \(\text{\LaTeX}\) file containing the sequence of games and the proved properties.

Correspondence between ASCII and \(\text{\LaTeX}\) outputs To use nicer and more conventional notations, the \(\text{\LaTeX}\) output sometimes differs from the ASCII output. Here is a table of correspondence:

<table>
<thead>
<tr>
<th>ASCII</th>
<th>(\text{\LaTeX})</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\leq(p)\Rightarrow)</td>
<td>(\leq)</td>
</tr>
<tr>
<td>&amp;&amp;</td>
<td>&amp;</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>(\neq)</td>
</tr>
<tr>
<td>&lt;=</td>
<td>(\leq)</td>
</tr>
<tr>
<td>orfind</td>
<td>(\oplus)</td>
</tr>
<tr>
<td>=&gt;</td>
<td>(\Rightarrow)</td>
</tr>
</tbody>
</table>

For the channels front-end

<table>
<thead>
<tr>
<th>ASCII</th>
<th>(\text{\LaTeX})</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\text{in}(c,p))</td>
<td>(c(p))</td>
</tr>
<tr>
<td>(\text{in}(c,(p_1,\ldots,p_n)))</td>
<td>(c(p_1,\ldots,p_n))</td>
</tr>
<tr>
<td>(\text{out}(c,M))</td>
<td>(\pi(M))</td>
</tr>
<tr>
<td>(\text{out}(c,(M_1,\ldots,M_n)))</td>
<td>(\pi(M_1,\ldots,M_n))</td>
</tr>
<tr>
<td>(!N)</td>
<td>(\cancel{\text{!}})</td>
</tr>
<tr>
<td>yield</td>
<td>(\text{yield})</td>
</tr>
<tr>
<td>-&gt;</td>
<td>(\rightarrow)</td>
</tr>
</tbody>
</table>

For the oracles front-end

<table>
<thead>
<tr>
<th>ASCII</th>
<th>(\text{\LaTeX})</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;=</td>
<td>(\Leftarrow)</td>
</tr>
<tr>
<td>&lt;-R</td>
<td>(\Rightarrow)</td>
</tr>
</tbody>
</table>

9 Generation of OCaml implementations

CryptoVerif can generate an OCaml implementation of the protocol from the CryptoVerif specification, using the command-line option `-impl OCaml`.

CryptoVerif generates the code for the protocol itself, but the code for the cryptographic primitives and for interacting with the network and the application has to be manually written in OCaml.

- For the cryptographic primitives, one can specify which OCaml function corresponds to which CryptoVerif function as explained in Section 9.3 below. For the security guarantees to hold, the OCaml implementation must satisfy the security assumptions mentioned in the CryptoVerif specification. The subdirectory `cv2OCaml` provides a basic implementation for some cryptographic primitives, in the module `Crypto`. This module has two implementations:

  - `crypto_real.ml` corresponds to real cryptographic primitives, implemented by relying on the OCaml cryptographic library Cryptokit [https://github.com/xavierleroy/cryptokit]. You need to install this library in order to run the protocol implementations generated by CryptoVerif. (It is used at least for random number generation even if you implement the cryptographic primitives by other means.)
  - `crypto_dbg.ml` is a debugging implementation, which constructs terms instead of applying the real cryptographic primitives.

You can choose which implementation to use by linking `crypto.ml` to the desired implementation. If you implement your own protocol, you will probably need to define your own cryptographic primitives.

The module `Base` contains functions used by code generated by CryptoVerif. It should not be modified.
The network and application code calls the code generated by CryptoVerif. From the point of view of security, this code can be considered as part of the adversary. We require that this code does not use unsafe OCaml functions (such as Obj.magic or marshalling/unmarshalling with different types) to bypass the typesystem (in particular to access the environment of closures and send it on the network).

We also require that this code does not mutate the values received from or passed to functions generated by CryptoVerif. This can be guaranteed by using immutable types, with the previous requirement. However, OCaml typically uses string for cryptographic functions and for network input/output, and the type string is mutable in OCaml. For simplicity and efficiency, the generated code uses the type string, with the requirement mentioned above.

We also require that all data structures manipulated by the generated code are non-circular. This is necessary because we use OCaml structural equality to compare values, and this equality may not terminate in the presence of circular data structures. This can easily be guaranteed by requiring that all OCaml types declared in the CryptoVerif input file are non-recursive.

We also require that this code does not fork after obtaining but before calling an oracle that can be called only once (because it is not under a replication in the CryptoVerif specification). Indeed, forking at this point would allow the oracle to be called several times. In practice, forking generally occurs only at the very beginning of the protocol, when the server starts a new session, so this requirement should be easily fulfilled.

Finally, we require that the programs do not perform several simultaneous writes to the same file and do not simultaneously read and write in the same file. This requirement could be enforced using locks, but in practice, it is generally obtained for free if the programs are run as intended. More precisely, we have two categories of files:

- Files that are created to store variables defined in a program and used in another program, for example, long-term keys generated by a key generation program, then used by the protocol. These files are written in one program, and read at the beginning of another program. These two programs should not be run concurrently, and the program that writes the file should be run once on each machine, not several times.

- Files that store tables of keys. The programs that insert elements in the table should be run one at a time. The insertion in the table is actually appending the file, so the system should support reading the table while inserting elements in it. (Elements not yet completely inserted are ignored.)

The subdirectories \texttt{cv2OCaml/nspk} and \texttt{cv2OCaml/wlsk} provide two complete examples, with the CryptoVerif specification and the OCaml network and application code.

### 9.1 Restrictions on the processes for implementation

The following two constraints must be satisfied:

- **find** must not be used. You can obtain a similar result using **insert** and **get**, which are supported.

  - Let us name “oracles” the parts of the process that are between an \texttt{in/ident} (seq(pattern)) := ... and an \texttt{out/return} statement, because in the oracle frontend, they correspond exactly to that. Let us define the signature of an oracle as the pair containing

    - the type $T_1 \times \ldots \times T_k \rightarrow T'_1 \times \ldots \times T'_n$, where $T_1 \times \ldots \times T_k$ are the types of the arguments expected in the \texttt{in/ident} (seq(pattern)) := statement, and $T'_1 \times \ldots \times T'_n$ are the types of the result given in the \texttt{out/return} statements, and

    - the list containing for each of the following oracles, its name and whether it is under a replication or not.

    An oracle can have multiple \texttt{out/return} statements. To be able to implement it, we must be able to define the signature above for each oracle, that is, all \texttt{out/return} must return the same type of
\[
\begin{align*}
\langle \text{mod}_\text{opt} \rangle & ::= \langle \text{id} \rangle (\langle \text{ident} \rangle \langle \text{< | >} \rangle \langle \text{string} \rangle) \\
\langle \text{odef} \rangle & ::= + = \langle \text{id} \rangle [\text{seq}^+ \langle \text{mod}_\text{opt} \rangle] \{ \langle \text{odef} \rangle \\
\text{If channel frontend, } \langle \text{body} \rangle ::= + = \text{out}(\langle \text{channel} \rangle, \langle \text{term} \rangle) [\langle \text{odef} \rangle] \\
\text{If oracle frontend, } \langle \text{body} \rangle ::= + = \text{return}(\langle \text{term} \rangle) [\langle \text{odef} \rangle]
\end{align*}
\]

Figure 9: Extensions to the syntax elements, and the oracles present after each \text{out} / \text{return} statement must be the same. Moreover, if an oracle with the same name is defined at several places, all its definitions must have the same signature.

9.2 Defining modules

The syntax of the processes is extended to add annotations, described in Figure 9. The symbol ::= + = means that we add the rule at the right-hand side to the non-terminal symbol at the left-hand side.

The terminals \{ and \} are used to mark the boundary of a module. Different modules typically correspond to different programs, for instance, key generation, client, and server of a protocol. More precisely, the following two constructs define respectively the beginning and the end of a module:

- \(\mu[x_1>"\text{file}_x^1", \ldots, x_n>"\text{file}_x^n", y_1<"\text{file}_y^1", \ldots, y_m<"\text{file}_y^m"] \{ Q \} \): The module \(\mu\) will contain the oracles defined in \(Q\). The implementation of the module \(\mu\) will write the contents of the variables \(x_1, \ldots, x_n\) upon instantiation in the files \(\text{file}_x^1, \ldots, \text{file}_x^n\) respectively. The variables \(x_1, \ldots, x_n\) must be defined under no replication inside module \(\mu\). These variables can then be used in other modules defined after the end of \(\mu\); these modules will read them automatically from the files \(\text{file}_x^1, \ldots, \text{file}_x^n\) respectively. The module \(\mu\) will read at initialization the value of the variables \(y_1, \ldots, y_m\) from the files \(\text{file}_y^1, \ldots, \text{file}_y^m\) respectively. The variables \(y_1, \ldots, y_m\) must be free in \(\mu\). (They are defined before the beginning of \(\mu\).)

- In the channel frontend, \text{out}(c, t); Q, or in the oracle frontend \text{return}(t_1, \ldots, t_n); Q): The module being defined will not contain \(Q\).

We transform the oracles present in the module into functions taking the arguments given to the oracle, and returning a tuple containing the result of the oracle and closures corresponding to the oracles following the current oracle that are in the same module. A module implementation contains only one function: the function \text{init}, which returns closures corresponding to the oracles accessible at the beginning of the module.

9.3 Implementation options

The implementation options declares how the implementation should translate functions, tables and types, and one must declare them after the declaration of the element it modifies and before use. The syntax is described in Figure 10.

The available implementation options are described hereafter:

- \text{type }T=\"ty\": Sets the OCaml type \(\text{ty}\) to be the type corresponding to the type \(T\).

This also can be followed by options between brackets and separated by semicolons. These options are:

- \text{serial}=\"s\", \"d\": Sets the serialization/deserialization of the type. There is no default, and this is required when a variable of type \(T\) is written or read to a file/table, or when it is contained in a tuple. The serialization function \(s\) must be of type \(\text{ty} \rightarrow \text{string}\), the deserialization function \(d\) must be of type \(\text{string} \rightarrow \text{ty}\). When deserialization fails, it must raise exception \text{Match}_\text{fail}.
type fun const

if the constant is a string, one can write, for example, const

by letfun implementation generates the random choices inside the function, while the CryptoVerif
definition the protocol. This feature can be used, for instance, to define probabilistic functions: the OCaml
implementation allows one to define macros by letfun. When the OCaml implementation is not specified, CryptoVerif generates code
according to the letfun macro. When the OCaml implementation is specified, it is used when generating the OCaml code, while the CryptoVerif macro defined by letfun is used for proving the protocol. This feature can be used, for instance, to define probabilistic functions: the OCaml
implementation generates the random choices inside the function, while the CryptoVerif definition by letfun first makes the random choices, then calls a deterministic function.

const f="s": Sets the implementation of the function f that has no arguments to an OCaml
constant. If the constant is a string, one can write, for example, const f="\"constant\"".
10 Generation of F* implementations

CryptoVerif can also generate an F* implementation of the protocol from the CryptoVerif specification, using the command-line option `-impl FStar`. It works along similar principles to the OCaml generation of implementations, but additionally generates F* lemmas for equations used as assumptions in CryptoVerif, to be proved in F*. In the future, we plan to generate F* axioms for security properties proved by CryptoVerif.

The subdirectory cv2fstar contains files for CryptoVerif to F* as well as an example, the Needham-Schroeder-Lowe public-key protocol.

More documentation is going to be added here in the future.

11 Additional programs

11.1 test

Usage:

```
  test [-timeout ⟨n⟩] ⟨mode⟩ ⟨test_set⟩
```

where `-timeout ⟨n⟩` sets the timeout for each execution of the tested program to `n` seconds (by default, there is no timeout), ⟨mode⟩ can be:

- `test`: test the mentioned scripts
- `test_add`: test the mentioned scripts and add the expected result in the script when it is missing
- `add`: add the expected result in the script when it is missing, do not test scripts that already have an expected result
- `update`: test the mentioned scripts and update the expected result in the script

and ⟨test_set⟩ can be:

- `basic`: runs basic CryptoVerif tests
- `big`: runs bigger CryptoVerif examples
- `proverif`: runs ProVerif on tests suitable for it
- `converted`: runs CryptoVerif on examples converted from CryptoVerif 1.28
- `impl`: runs tests of the generation of OCaml implementations
- `all`: runs all tests included in `basic`, `proverif`, `converted`, `big`, and `impl`
- `dir ⟨prefix⟩ ⟨list_of_directories⟩` analyzes the mentioned directories using CryptoVerif, using ⟨prefix⟩ as prefix for the output files.

⟨test_set⟩ can be omitted when it is `basic`, and ⟨mode⟩ ⟨test_set⟩ can both be omitted when they are `test basic`.

The script `test` is a bash shell script, so you must have bash installed. On Windows, the best is to install Cygwin and run `test` from a Cygwin terminal.

The script `test` must be run in the CryptoVerif main directory; the programs `analyze` and `cryptoVerif` must be present in that directory.

For CryptoVerif tests, the programs first runs the script `prepare` in each directory when it is present. That allows for instance to generate the CryptoVerif scripts to run. Then it runs the program `analyze` described below.
11.2 analyze

The program analyze is mainly meant to be called from test, but it can also be called directly.

Usage:

```
analyze [(options)] (prog) (mode) (tmp_directory) (prefix_for_output_files) dirs (directories)
analyze [(options)] (prog) (mode) (tmp_directory) (prefix_for_output_files) file (directory) (filename)
```

where (options) can be

- `-timeout (n)` sets the timeout for each execution of the tested program to `n` seconds (by default, there is no timeout);
- `-progopt ⟨command-line options⟩ -endprogopt` passes the additional ⟨command-line options⟩ to the tested program (ProVerif or CryptoVerif);

(prog) is either CV for CryptoVerif or PV for ProVerif and (mode) is as for the test program above. Temporary files are stored in directory (tmp_directory), and the output files are:

- full output of the test: `tests/⟨prefix_for_output_files⟩⟨date⟩`.
- summary of the results: `tests/sum-⟨prefix_for_output_files⟩⟨date⟩`.
- comparison with expected results: `tests/res-⟨prefix_for_output_files⟩⟨date⟩`.

This program analyzes a series of scripts using the program specified by (prog).

- In the first command line, it analyzes scripts in the mentioned directories and in their subdirectories. The files whose name contains .m4, or .out, are excluded. (The first ones are supposed to be files to preprocess by m4 before actually analyzing them; the second ones are supposed to be output files.) When the program is CryptoVerif, the files whose name ends with .cv, .ocv, or .pcv are analyzed. When the program is ProVerif, the files whose name ends with .pcv, .pv, .pl, .horn, or .horntype are analyzed.

- In the second command line, the specified file in the specified directory is analyzed, provided it has one of the extensions above. (The directory and the file are mentioned separately because the directory may be used to locate the library mylib.*, see below.)

The executable for CryptoVerif is searched in the current directory, in `$HOME/CryptoVerif`, and in the PATH. The executable for ProVerif is searched in the current directory, in `$HOME/proverif/proverif`, and in the PATH.

When mylib.cvl is present in a directory, its files with extension .cv or .pcv are analyzed using that library of primitives for CryptoVerif. Otherwise, the default library is used.

When mylib.ocvl is present in a directory, its files with extension .ocv are analyzed using that library of primitives for CryptoVerif. Otherwise, the default library is used.

When mylib.pvl is present in a directory, its files with extension .pcv or .pv are analyzed using that library of primitives for ProVerif. Otherwise, the library cryptoverif.pvl is used for .pcv files and no library for .pv files. The file cryptoverif.pvl is searched in the current directory, in `$HOME/CryptoVerif` and `$HOME/proverif/proverif`. If it is not found and mylib.pvl is not present in the directory, .pcv files are not analyzed using ProVerif.

The result of running each script is compared to the expected result. The expected result is found in the script itself in a comment that starts with `EXPECTED` for CryptoVerif and `EXPECTPV` for ProVerif, and ends with `END`. (The entire lines that contain `EXPECTED`, resp. `EXPECTPV` and `END` do not belong to the expected result.) For CryptoVerif, the expected result consists of the line `RESULT Could not prove ...` or All queries proved in the output of CryptoVerif. For ProVerif, it consists of the lines that start with `RESULT` in the output of ProVerif. It also includes a runtime of the script or an error message `xtime: ...` if the execution terminates with an error.

In the modes update (resp. test_add or add), the expected result is updated (resp. added if it is absent or empty). To deal with generated files, the `EXPECTED`, resp. `EXPECTPV` line may contain the indications

```
FILENAME: name of the file TAG: distinct tag
```

83
In this case, the expected result is not updated in the script itself, but in the file whose name is mentioned after $\text{FILENAME}:$. And inside this file after an exact copy of the line that contains $\text{EXPECTED}$, resp. $\text{EXPECTPV}$. (This line is unique thanks to the tag.) The idea is that this file is the file from which the script was generated. Hence regenerating the script from this file with an updated expected result will update the expected result in the script.

11.3 addexpectedtags

Usage:

```
addexpectedtags (directories)
```

For each mentioned directory, for each file in that directory or its subdirectories that contains .m4, in its name and ends with .cv, .ocv, .pcv, .pv, .pi, .horn, .horn, this program adds at the end of each line that contains $\text{EXPECTED}$ or $\text{EXPECTPV}$ the indications

```
FILENAME: name of the file TAG: distinct integer
```

These files are supposed to be initial models used to generate CryptoVerif or ProVerif scripts by the m4 preprocessor. The additional indications will propagate to the generated scripts, and will allow the analyze program above to find from which m4 file the script was generated (indicated after $\text{FILENAME}:$) and inside this m4 file, which expected result indication ended up in the considered script (identified by the integer after $\text{TAG}:$). It can then update the expected results in the mode update, add, or test_add (the last two when the expected result was initially empty).

Acknowledgments

CryptoVerif was partly developed while the authors were at École Normale Supérieure, Paris.

We warmly thank David Pointcheval for his advice and explanations of the computational proofs of protocols. This project would not have been possible without him.

This project was partly supported by ARA SRIA Formacrypt, by the ANR projects ProSe (decision ANR-2010-VERS-004-01) and TECAP (decision ANR-17-CE39-0004-03), and benefited from funding managed by the French National Research Agency under the France 2030 programme with the reference ANR-22-PECY-0006 (PEPR Cybersecurity SVP).

References


