Mechanizing Game-Based Proofs of Security Protocols: 
The Tool CryptoVerif

Bruno Blanchet

INRIA Paris
Bruno.Blanchet@inria.fr

Year 2023-24
Outline

1. Using CryptoVerif
2. Proof technique: game transformations, proof strategy
3. Two examples:
   - Encrypt-then-MAC
   - FDH
4. Conclusion, future directions
CryptoVerif is an **automatic prover** that:

- generates **proofs by sequences of games**.
- proves **secrecy, correspondence, and indistinguishability** properties.
- provides a **generic** method for specifying properties of **cryptographic primitives** which handles MACs (message authentication codes), symmetric encryption, public-key encryption, signatures, hash functions, Diffie-Hellman key agreements, …
- works for **$N$ sessions** (polynomial in the security parameter), with an **active adversary**.
- gives a bound on the **probability** of an attack (exact security).
Input and output of the tool

1. Prepare the input file containing
   - the specification of the protocol to study (initial game),
   - the security assumptions on the cryptographic primitives,
   - the security properties to prove.

2. Run CryptoVerif

3. CryptoVerif outputs
   - the sequence of games that leads to the proof,
   - a succinct explanation of the transformations performed between games,
   - an upper bound of the probability of success of an attack.
Process calculus for games

Games are formalized in a **process calculus**, a small specialized programming language:

- The processes define **oracles** that the adversary can call.
- The semantics is **purely probabilistic** (no non-determinism).
- The runtime of processes is **bounded**:
  - bounded number of copies of processes,
  - bounded length of messages.
- Extension to **arrays**.
Process calculus for games: terms

Terms represent computations on messages (bitstrings).

\[ M ::= \text{terms} \]
\[ x, y, z, x[M_1, \ldots, M_n] \text{ variable} \]
\[ f(M_1, \ldots, M_n) \text{ function application} \]

Function symbols \( f \) correspond to functions computable by deterministic Turing machines that always terminate.
Process calculus for games: processes

\[ Q ::= \]

- \(0\) \hspace{3cm} \text{oracle definitions}
- \([Q \mid Q']\) \hspace{3cm} \text{end}
- \textbf{foreach} \(i \leq N\) \textbf{do} \(Q\) \hspace{3cm} \text{parallel composition}
- \textbf{newOracle} \(O; Q\) \hspace{3cm} \text{replication} \(N\) \text{ times}
- \(O(x_1 : T_1, \ldots, x_m : T_m) := P\) \hspace{3cm} \text{restriction} \text{ for oracles}

\[ P ::= \]

- \textbf{yield} \hspace{3cm} \text{oracle} \text{ bodies}
- \textbf{return} \((M_1, \ldots, M_m); Q\) \hspace{3cm} \text{return}
- \textbf{event} \(e(M_1, \ldots, M_m); P\) \hspace{3cm} \text{event}
- \(x \leftarrow T; P\) \hspace{3cm} \text{random} \text{ number} \text{ generation} \text{ (uniform)}
- \textbf{let} \(x : T = M\) \textbf{in} \(P\) \hspace{3cm} \text{assignment}
- \textbf{if} \(M\) \textbf{then} \(P\) \textbf{else} \(P'\) \hspace{3cm} \text{conditional}
- \textbf{find} \(j \leq N\) \textbf{such} \textbf{that} \textbf{defined} \((x[j], \ldots) \land M\) \textbf{then} \(P\) \textbf{else} \(P'\) \hspace{3cm} \text{array} \text{ lookup}
Example: 1. symmetric encryption

We consider a probabilistic, length-revealing encryption scheme.

**Definition (Symmetric encryption scheme SE)**

- (Randomized) encryption function $\text{enc}(m, k, r')$ takes as input a message $m$, a key $k$, and random coins $r'$.
- Decryption function $\text{dec}(c, k)$ such that

$$\text{dec}(\text{enc}(m, k, r'), k) = i_{\bot}(m)$$

The decryption returns a bitstring or $\bot$:
- $\bot$ when decryption fails,
- the cleartext when decryption succeeds.

The injection $i_{\bot}$ maps a bitstring to the same bitstring in bitstring $\cup \{\bot\}$. 
Example: 2. MAC

**Definition (Message Authentication Code scheme MAC)**

- MAC function $mac(m, k)$ takes as input a message $m$ and a key $k$.
- Verification function $verify(m, k, t)$ such that

  $$verify(m, k, mac(m, k)) = true.$$ 

A MAC is essentially a keyed hash function.

A MAC guarantees the integrity and authenticity of the message because only someone who knows the secret key can build the MAC.
Example: 3. encrypt-then-MAC

We define an authenticated encryption scheme by the encrypt-then-MAC construction:

\[ enc'(m, (k, mk), r'') = e, mac(e, mk) \text{ where } e = enc(m, k, r''). \]

A basic example of protocol using encrypt-then-MAC:

- A and B initially share an encryption key \( k \) and a MAC key \( mk \).
- A sends to B a fresh key \( k' \) encrypted under authenticated encryption, implemented as encrypt-then-MAC.

\[ A \rightarrow B : e = enc(k', k, r''), \quad mac(e, mk) \quad k' \text{ fresh} \]

\( k' \) should remain secret.
Example: initialization

\[ A \rightarrow B : e = enc(k', k, r''), \text{mac}(e, mk) \quad \text{\(k'\) fresh} \]

\[ Q_0 = O_{\text{start}} := k \leftarrow \text{key}; mk \leftarrow \text{mkey}; \text{return}(); \]

\((\text{run } Q_A(k, mk) \mid \text{run } Q_B(k, mk))\)

Initialization of keys:

1. The process \(Q_0\) waits for a call to oracle \(O_{\text{start}}\) to start running. The adversary triggers this process.
2. \(Q_0\) generates encryption and MAC keys, \(k\) and \(mk\) respectively.
3. \(Q_0\) returns control to the adversary by \text{return}(). \(Q_A\) and \(Q_B\) represent the actions of \(A\) and \(B\) (see next slides).
Example: role of $A$

\[ A \rightarrow B : e = \text{enc}(k', k, r''), \text{mac}(e, mk) \quad k' \text{ fresh} \]

\[
Q_A(k, mk) = \text{foreach } i \leq n \text{ do}
\]

\[
O_A() := k' \xleftarrow{R} \text{key}; r'' \xleftarrow{R} \text{coins};
\]

\[
\text{let } e = \text{enc}(k2b(k'), k, r'') \text{ in}
\]

\[
\text{return}(e, \text{mac}(e, mk))
\]

Role of $A$:

1. **foreach $i \leq n$ do** represents $n$ copies, indexed by $i \in [1, n]$
   
   The protocol can be run $n$ times (polynomial in the security parameter).

2. The process is triggered by a call to oracle $O_A$ by the adversary.

3. The process **chooses a fresh key $k'$ and returns the message**.
Example: role of $B$

$$A \rightarrow B : e = enc(k', k, r''), \, mac(e, mk) \quad k' \text{ fresh}$$

$$Q_B(k, mk) = \text{foreach } i' \leq n \text{ do}$$

$$O_B(e' : \text{bitstring}, ma' : \text{macstring}) :=$$

$$\text{if verify(e', mk, ma') then}$$

$$\text{let } i_{\bot}(k2b(k'')) = \text{dec}(e', k) \text{ in return()}$$

Role of $B$:

1. $n$ copies, as for $Q_A$.
2. The process $Q_B$ waits for a call to oracle $O_B$, with the message as argument.
3. It verifies the MAC, decrypts, and stores the key in $k''$. 
Example: summary of the initial game

\[ A \rightarrow B : e = \text{enc}(k', k, r''), \text{mac}(e, mk) \quad k' \text{ fresh} \]

\[ Q_0 = O_{\text{start}} := k \leftarrow \text{key}; mk \leftarrow \text{mkey}; \text{return}(); \]

\( (\text{run } Q_A(k, mk) | \text{run } Q_B(k, mk)) \)

\( Q_A(k, mk) = \text{foreach } i \leq n \text{ do } O_A() := k' \leftarrow \text{key}; r'' \leftarrow \text{coins}; \)

\( \text{let } e = \text{enc}(k2b(k'), k, r'') \text{ in } \)

\( \text{return}(e, \text{mac}(e, mk)) \)

\( Q_B(k, mk) = \text{foreach } i' \leq n \text{ do } O_B(e' : \text{bitstring}, ma' : \text{macstring}) := \)

\( \text{if verify}(e', mk, ma') \text{ then } \)

\( \text{let } i_\bot(k2b(k'')) = \text{dec}(e', k) \text{ in return()} \)
Security assumptions on primitives

The most frequent cryptographic primitives are already specified in a library. The user can use them without redefining them.

In the example:

- The MAC is **SUF-CMA** (strongly unforgeable under chosen message attacks).

  An adversary that has access to the MAC and verification oracles has a negligible probability of forging a MAC (not produced by the MAC oracle).
Security assumptions on primitives

The most frequent cryptographic primitives are already specified in a library. The user can use them without redefining them.

In the example:

- The MAC is **SUF-CMA** (strongly unforgeable under chosen message attacks).
  An adversary that has access to the MAC and verification oracles has a negligible probability of forging a MAC (not produced by the MAC oracle).
- The encryption is **IND-CPA** (indistinguishable under chosen plaintext attacks).
  An adversary has a negligible probability of distinguishing the encryption of two messages of the same length.
Security assumptions on primitives

The most frequent cryptographic primitives are already specified in a library. The user can use them without redefining them.

In the example:

- The MAC is **SUF-CMA** (strongly unforgeable under chosen message attacks).
  An adversary that has access to the MAC and verification oracles has a negligible probability of forging a MAC (not produced by the MAC oracle).

- The encryption is **IND-CPA** (indistinguishable under chosen plaintext attacks).
  An adversary has a negligible probability of distinguishing the encryption of two messages of the same length.

- All keys have the same length: \( \text{forall } y : \text{key}; Z(k2b(y)) = Z_k \).
Security properties to prove

In the example:

- **One-session secrecy** of $k''$: each $k''$ is indistinguishable from a random number.
- **Secrecy** of $k''$: the $k''$ are indistinguishable from independent random numbers.
Demo

- CryptoVerif input file: enc-then-MAC.ocv
- library of primitives
- run CryptoVerif
- output
Arrays

A variable defined under a replication is implicitly an array:

\[ Q_A(k, mk) = \text{foreach } i \leq n \text{ do } O_A[i]() := k'[i] \xleftarrow{R} \text{key}; r''[i] \xleftarrow{R} \text{coins}; \]
\[
\quad \text{let } e[i] = \text{enc}(k2b(k'[i]), k, r''[i]) \text{ in } \\
\quad \text{return}(e[i], \text{mac}(e[i], mk))
\]

Requirements:

- Only variables with the current indices can be assigned.
- Variables may be defined at several places, but only one definition can be executed for the same indices. (if \ldots then let \texttt{x} = \texttt{M} in \texttt{P} else let \texttt{x} = \texttt{M'} in \texttt{P'} is ok)

So each array cell can be assigned at most once.

Arrays allow one to remember the values of all variables during the whole execution.
Arrays (continued)

**find** performs an array lookup:

```
foreach i ≤ N do ... let x = M in P
| foreach i' ≤ N' do O(y : T) :=
    find j ≤ N suchthat defined(x[j]) ∧ y = x[j] then ...
```

Note that **find** is here used outside the scope of x.

This is the only way of getting access to values of variables in other sessions.

When several array elements satisfy the condition of the **find**, the returned index is chosen randomly, with uniform probability.
Arrays versus lists

Arrays replace lists often used in cryptographic proofs.

foreach $i \leq N$ do 
  let $x = M$ in 
  let $y = M'$ in $P$
\mid \text{foreach } i' \leq N' \text{ do } O(x' : T) :=
  \text{find } j \leq N \text{ such that defined } (x[j], y[j]) \land x' = x[j] \text{ then } P'(y[j])

written by cryptographers

foreach $i \leq N$ do 
  let $x = M$ in 
  let $y = M'$ in insert $(x, y)$ in $L; P$
\mid \text{foreach } i' \leq N' \text{ do } O(x' : T) := \text{get } (x, y) \text{ in } L \text{ such that } x' = x; P'(y)

Arrays avoid the need for explicit list insertion instructions, which would be hard to guess for an automatic tool.
Indistinguishability

Two processes (games) $Q_1$, $Q_2$ are indistinguishable when the adversary has a negligible probability of distinguishing them: $Q_1 \approx Q_2$.

- The adversary is represented by an acceptable evaluation context
  $$C ::= [\ ] \ C \ | \ Q \ Q \ | \ C \ \text{newOracle} \ O; C.$$  
- $C[Q]$ may execute events, collected in a sequence $\mathcal{E}$.
- A distinguisher $D$ takes as input $\mathcal{E}$ and returns true or false.
  - Example: $D_e(\mathcal{E}) = \text{true}$ if and only if $e \in \mathcal{E}$.
  - $D_e$ abbreviated $e: e(\mathcal{E})$ is true if and only if $e \in \mathcal{E}$.
- $\Pr[C[Q] : D]$ is the probability that $C[Q]$ executes $\mathcal{E}$ such that $D(\mathcal{E}) = \text{true}$.

Definition (Indistinguishability)

We write $Q \approx_p^V Q'$ when, for all evaluation contexts $C$ acceptable for $Q$ and $Q'$ with public variables $V$ and all distinguishers $D$, 

$$\left| \Pr[C[Q] : D] - \Pr[C[Q'] : D] \right| \leq p(C, D).$$
Indistinguishability

Lemma

1. Reflexivity: $Q \approx^V Q$.
2. Symmetry: $\approx^V_p$ is symmetric.
3. Transitivity: if $Q \approx^V_p Q'$ and $Q' \approx^V_{p'} Q''$, then $Q \approx^V_{p+p'} Q''$.
4. Application of context: if $Q \approx^V_{p} Q'$ and $C$ is an evaluation context acceptable for $Q$ and $Q'$ with public variables $V$, then $C[Q] \approx^V_{p'} C[Q']$, where $p'(C', D) = p(C'[C[]], D)$ and $V' \subseteq V \cup \text{var}(C)$. 
Proof technique

We transform a game $G_0$ into an indistinguishable one using:

- **indistinguishability properties** $L \approx_p R$ given as axioms and that come from security assumptions on primitives. These equivalences are used inside a context:

$$G_1 \approx_0 C[L] \approx_{p'} C[R] \approx_0 G_2$$

- **syntactic transformations**: simplification, expansion of assignments, …

We obtain a sequence of games $G_0 \approx_{p_1} G_1 \approx \ldots \approx_{p_m} G_m$, which implies $G_0 \approx_{p_1+\ldots+p_m} G_m$.

If some trace property holds up to probability $p$ in $G_m$, then it holds up to probability $p + p_1 + \ldots + p_m$ in $G_0$. 

Bruno Blanchet (INRIA)
A MAC guarantees the integrity and authenticity of the message because only someone who knows the secret key can build the MAC. More formally, \( \text{Succ}^{\text{suf-cma}}_{\text{MAC}}(t, q_m, q_v, l) \) is negligible if \( t \) is polynomial in the security parameter:

\[
\text{Succ}^{\text{suf-cma}}_{\text{MAC}}(t, q_m, q_v, l) = \max_A \Pr[k \leftarrow \text{mkey}; (m, s) \leftarrow \mathcal{A}^{\text{mac}(\cdot, k), \text{verify}(\cdot, k, \cdot)} : \text{verify}(m, k, s) \wedge \text{no query to the oracle } \text{mac}(\cdot, k) \text{ with message } m \text{ returned } s]
\]

where \( A \) runs in time at most \( t \), calls \( \text{mac}(\cdot, k) \) at most \( q_m \) times with messages of length at most \( l \), calls \( \text{verify}(\cdot, k, \cdot) \) at most \( q_v \) times with messages of length at most \( l \).
MAC: intuition behind the CryptoVerif definition

By the previous definition, up to negligible probability,
- the adversary cannot forge a correct MAC
- so, assuming \( k \leftarrow mkey \) is used only for generating and verifying MACs, the verification of a MAC with \( \text{verify}(m, k, t) \) can succeed only if \( m \) is in the list (array) of messages whose \( \text{mac}(\cdot, k) \) has been computed, with result \( t \) by the protocol
- so we can replace a call to \( \text{verify} \) with an array lookup: if the call to \( \text{mac} \) is \( \text{mac}(x, k) \), we replace \( \text{verify}(m, k, t) \) with

\[
\text{find } j \leq N \text{ such that defined}(x[j]) \land (m = x[j]) \land t = \text{mac}(m, k) \text{ then true else false}
\]
MAC: CryptoVerif definition

\[
\text{verify}(m, k, \text{mac}(m, k)) = \text{true}
\]

\[
k \overset{R}{\leftarrow} mkey; (\text{foreach } i \leq N \text{ do } \text{Omac}(x : \text{bitstring}) := \text{return}(\text{mac}(x, k)) | \text{foreach } i' \leq N' \text{ do } \text{Overify}(m : \text{bitstring}, t : \text{macstring}) := \text{return}(\text{verify}(m, k, t)))
\]

\[
\approx
\]

\[
k \overset{R}{\leftarrow} mkey; (\text{foreach } i \leq N \text{ do } \text{Omac}(x : \text{bitstring}) := \text{let } ma = \text{mac}(x, k) \text{ in return}(ma) | \text{foreach } i' \leq N' \text{ do } \text{Overify}(m : \text{bitstring}, t : \text{macstring}) := \text{find } j \leq N \text{ such that defined}(x[j], ma[j]) \land (m = x[j]) \land (t = ma[j]) \text{ then true else false})
\]
MAC: CryptoVerif definition

\[
\text{verify}(m, k, \text{mac}(m, k)) = \text{true}
\]

\[
k \leftarrow^R \text{mkey}; ( \text{foreach } i \leq N \text{ do } \text{Omac}(x : \text{bitstring}) := \text{return}(\text{mac}(x, k)) | \text{foreach } i' \leq N' \text{ do } \text{Overify}(m : \text{bitstring}, t : \text{macstring}) := \text{return}(\text{verify}(m, k, t)))
\]

\[
\approx_{\text{Succ}_{\text{mac}}^{\text{cma}}} (\text{time}, N, N', \max(\maxl(x), \maxl(m)))
\]

\[
k \leftarrow^R \text{mkey}; ( \text{foreach } i \leq N \text{ do } \text{Omac}(x : \text{bitstring}) := \text{let } ma = \text{mac}'(x, k) \text{ in return}(ma) | \text{foreach } i' \leq N' \text{ do } \text{Overify}(m : \text{bitstring}, t : \text{macstring}) := \text{find } j \leq N \text{ such that } \text{defined}(x[j], ma[j]) \land (m = x[j]) \land (t = ma[j]) \text{ then true else false})
\]

CryptoVerif understands such specifications of primitives. They can be reused in the proof of many protocols.
MAC: using the CryptoVerif definition

CryptoVerif applies the previous rule automatically in any context, perhaps containing several occurrences of \( mac \) and of \( verify \):

- Each occurrence of \( mac(x_i, k) \) is replaced with
  \[
  \text{let } ma_i = mac'(x_i, k) \text{ in } ma_i.
  \]

- Each occurrence of \( verify \) is replaced with a \textbf{find} that looks in all arrays \( x_i, ma_i \) of computed MACs (one array for each occurrence of function \( mac \)).
Symmetric encryption: definition of security (IND-CPA)

An adversary has a negligible probability of distinguishing the encryption of two messages of the same length.

Definition (INDistinguishability under Chosen Plaintext Attacks, IND-CPA)

\[
\text{Succ}_{\text{SE}}^{\text{ind-cpa}}(t, q_e, l) =
\max_{A} 2 \Pr \left[ b \leftarrow \{0, 1\}; k \leftarrow \text{key}; b' \leftarrow A^{\text{enc}(LR(.,.,b),k)}: b' = b \right] - 1
\]

where \( A \) runs in time at most \( t \), calls \( \text{enc}(LR(.,.,b),k) \) at most \( q_e \) times on messages of length at most \( l \), \( LR(x, y, 0) = x \), \( LR(x, y, 1) = y \), and \( LR(x, y, b) \) is defined only when \( x \) and \( y \) have the same length.
Symmetric encryption: CryptoVerif definition

\[ \text{dec}(\text{enc}(m, k, r'), k) = i_\perp(m) \]

\[ \begin{align*}
    k & \leftarrow^R \text{key}; \textbf{foreach } i \leq N \textbf{ do } O_{\text{enc}}(x : \text{bitstring}) := \\
    & \quad r' \leftarrow^R \text{coins}; \textbf{return}(\text{enc}(x, k, r')) \\
    \text{\approx} & \\
    k & \leftarrow^R \text{key}; \textbf{foreach } i \leq N \textbf{ do } O_{\text{enc}}(x : \text{bitstring}) := \\
    & \quad r' \leftarrow^R \text{coins}; \textbf{return}(\text{enc}(Z(x), k, r'))
\end{align*} \]

\(Z(x)\) is the bitstring of the same length as \(x\) containing only zeroes (for all \(x : \text{nonce}, Z(x) = Z_{\text{nonce}}, \ldots\)).
Symmetric encryption: CryptoVerif definition

\[\text{dec}(\text{enc}(m, k, r'), k) = i_\perp(m)\]

\[k \xleftarrow{R} \text{key}; \textbf{foreach } i \leq N \textbf{ do } \text{Oenc}(x : \text{bitstring}) :=\]

\[r' \xleftarrow{R} \text{coins}; \textbf{return}(\text{enc}(x, k, r'))\]

\[\approx_{\text{Succ}_{\text{SE}}^{\text{ind-cpa}}(\text{time}, N, \maxl(x))}\]

\[k \xleftarrow{R} \text{key}; \textbf{foreach } i \leq N \textbf{ do } \text{Oenc}(x : \text{bitstring}) :=\]

\[r' \xleftarrow{R} \text{coins}; \textbf{return}(\text{enc}'(Z(x), k, r'))\]

\(Z(x)\) is the bitstring of the same length as \(x\) containing only zeroes (for all \(x : \text{nonce}, Z(x) = Z_{\text{nonce}}, \ldots\)).
Syntactic transformations (1)

Expansion of assignments: replacing a variable with its value. (Not completely trivial because of array references.)

Example

If \( pk \) is defined by

\[
\text{let } pk = pkgen(r)
\]

and there are no array references to \( pk \), then \( pk \) is replaced with \( pkgen(r) \) in the game and the definition of \( pk \) is removed.
Syntactic transformations (2)

Single assignment renaming: when a variable is assigned at several places, rename it with a distinct name for each assignment. (Not completely trivial because of array references.)

Example

\[
O_{\text{start}} := k_A \xleftarrow{R} T_k; k_B \xleftarrow{R} T_k; \text{return}(); (\text{run } Q_K \mid \text{run } Q_S)
\]

\[
Q_K = \text{foreach } i \leq n \text{ do } O(h : T_h, k : T_k) :=
\]

\[
\quad \text{if } h = A \text{ then let } k' = k_A \text{ else}
\]

\[
\quad \text{if } h = B \text{ then let } k' = k_B \text{ else let } k' = k
\]

\[
Q_S = \text{foreach } i' \leq n' \text{ do } O'(h' : T_h) :=
\]

\[
\quad \text{find } j \leq n \text{ suchthat defined}(h[j], k'[j]) \land h' = h[j] \text{ then } P_1(k'[j])
\]

\[
\quad \text{else } P_2
\]
Syntactic transformations (2)

Single assignment renaming: when a variable is assigned at several places, rename it with a distinct name for each assignment. (Not completely trivial because of array references.)

Example

\[ O_{\text{start}} := k_A \xrightarrow{R} T_k; k_B \xrightarrow{R} T_k; \text{return}(); (\text{run } Q_K \mid \text{run } Q_S) \]

\[ Q_K = \text{foreach } i \leq n \text{ do } O(h : T_h, k : T_k) := \]

\begin{align*}
\text{if } h = A \text{ then let } k_1' &= k_A \\
\text{if } h = B \text{ then let } k_2' &= k_B \text{ else let } k_3' &= k
\end{align*}

\[ Q_S = \text{foreach } i' \leq n' \text{ do } O'(h' : T_h) := \]

\begin{align*}
\text{find } j \leq n \text{ such that defined}(h[j], k_1'[j]) \land h' = h[j] \text{ then } P_1(k_1'[j]) \\
\text{or find } j \leq n \text{ such that defined}(h[j], k_2'[j]) \land h' = h[j] \text{ then } P_1(k_2'[j]) \\
\text{or find } j \leq n \text{ such that defined}(h[j], k_3'[j]) \land h' = h[j] \text{ then } P_1(k_3'[j]) \\
\text{else } P_2
\end{align*}
Syntactic transformations (3)

**Move new**: move random choices downwards in the game as much as possible, when there is no array reference to them.
(Moving $x \leftarrow R$ under a `if` or a `find` duplicates it.
A subsequent single assignment renaming will distinguish cases.)

**Example**


```plaintext
x \leftarrow nonce; \text{if } c \text{ then } P_1 \text{ else } P_2
```

becomes


```plaintext
\text{if } c \text{ then } x \leftarrow nonce; P_1 \text{ else } x \leftarrow nonce; P_2
```

Syntactic transformations (4)

- **Merge arrays**: merge several variables $x_1, \ldots, x_n$ into a single variable $x_1$ when they are used for different indices (defined in different branches of a test `if` or `find`).

- **Merge branches of `if` or `find** when they execute the same code, up to renaming of variables without array accesses.
Syntactic transformations (5): manual transformations

**Insert an instruction:** insert a test to distinguish cases; insert a variable definition; ...  
Preserves the semantics of the game (e.g., the rest of the code is copied in both branches of the inserted test).

**Example**

$P$ becomes

```
if cond then $P$ else $P$
```

Subsequent transformations can transform $P$ differently, depending on whether $cond$ holds.
Syntactic transformations (6): manual transformations

- **Insert an event**: to apply Shoup’s lemma.
  - A subprocess $P$ becomes **event** $e$.
  - The probability of distinguishing the two games is the probability of executing event $e$. It will be bound by a proof by sequences of games.

- **Replace a term with an equal term**: CryptoVerif verifies that the terms are really equal.
Simplification and elimination of collisions

- CryptoVerif collects equalities that come from:
  - Assignments: let $x = M$ in $P$ implies that $x = M$ in $P$
  - Tests: if $M = N$ then $P$ implies that $M = N$ in $P$
  - Definitions of cryptographic primitives
    - When a find guarantees that $x[j]$ is defined, equalities that hold at definition of $x$ also hold under the find (after substituting $j$ for the array indices at the definition of $x$)
    - Elimination of collisions: if $x$ is created by $x \leftarrow^R T$, $x[i] = x[j]$ implies $i = j$, up to negligible probability (when $T$ is large)
  - These equalities are combined to simplify terms.
  - When terms can be simplified, processes are simplified accordingly. For instance:
    - If $M$ simplifies to true, then if $M$ then $P_1$ else $P_2$ simplifies to $P_1$.
    - If a condition of find simplifies to false, then the corresponding branch is removed.
Proof of security properties: one-session secrecy

One-session secrecy: the adversary cannot distinguish any of the secrets from a random number with one test query.

Definition (One-session secrecy)
Assume that the variable $x$ of type $T$ is defined in $G$ under a single
foreach $i \leq n$ do.

$G$ preserves the one-session secrecy of $x$ up to probability $p$ when, for all evaluation contexts $C$ acceptable for $G \mid Q_x$ with no public variables that do not contain $S$ nor $\overline{S}$, $\Pr[C[G \mid Q_x] : S] - \Pr[C[G \mid Q_x] : \overline{S}] \leq p(C)$, where

$Q_x = O_0() := b \xleftarrow{R} \text{bool}; \text{return}();$

$(O(j : [1, n]) := \text{if defined}(x[j]) \text{ then}$

if $b$ then return($x[j]$) else $y \xleftarrow{R} T; \text{return}(y)$

| $O'(b' : \text{bool}) := \text{if } b = b' \text{ then event_abort } S \text{ else event_abort } \overline{S}$

$c_0, c, c', b, b', j, y, S, \overline{S}$ do not occur in $G$. 

Bruno Blanchet (INRIA)  CryptoVerif  Year 2023-24
Proof of security properties: one-session secrecy

**One-session secrecy**: the adversary cannot distinguish any of the secrets from a random number with one test query.

**Criterion for proving one-session secrecy of $x$**: $x$ is defined by $x[i] \leftarrow R_T$ and there is a set of variables $S$ such that only variables in $S$ depend on $x$. The output messages and the control-flow do not depend on $x$ nor on any variable in $S$. 
Proof of security properties: secrecy

Secrecy: the adversary cannot distinguish the secrets from independent random numbers with several test queries.

Criterion for proving secrecy of $x$: same as one-session secrecy, plus $x[i]$ and $x[i']$ do not come from the same copy of the same random choice when $i \neq i'$. 
Proof strategy: advice

- One tries to execute each transformation given by the definition of a cryptographic primitive.
- When it fails, CryptoVerif tries to analyze why the transformation failed, and suggests syntactic transformations that could make it work.
- One tries to execute these syntactic transformations. (If they fail, they may also suggest other syntactic transformations, which are then executed.)
- We retry the cryptographic transformation, and so on.
Proof of the example: initial game

\[ Q_0 = O_{\text{start}} := k \xleftarrow{R} \text{key}; mk \xleftarrow{R} \text{mkey}; \text{return}(); \]

\[ (\text{run } Q_A(k, mk) \mid \text{run } Q_B(k, mk)) \]

\[ Q_A(k, mk) = \text{foreach } i \leq n \text{ do } O_A() := k' \xleftarrow{R} \text{key}; r'' \xleftarrow{R} \text{coins}; \]

\[ \text{let } e = \text{enc}(k2b(k'), k, r'') \text{ in } \]

\[ \text{return}(e, \text{mac}(e, mk)) \]

\[ Q_B(k, mk) = \text{foreach } i' \leq n \text{ do } O_B(e' : \text{bitstring}, ma' : \text{macstring}) := \]

\[ \text{if } \text{verify}(e', mk, ma') \text{ then } \]

\[ \text{let } i_\perp(k2b(k'')) = \text{dec}(e', k) \text{ in return()} \]
Proof of the example: security of the MAC

\[ Q_0 = O_{\text{start}} := k \stackrel{R}{\leftarrow} \text{key}; mk \stackrel{R}{\leftarrow} \text{mkey}; \text{return}(); \]

\[ (\text{run } Q_A(k, mk) \mid \text{run } Q_B(k, mk)) \]

\[ Q_A(k, mk) = \text{foreach } i \leq n \text{ do } O_A() := k' \stackrel{R}{\leftarrow} \text{key}; r'' \stackrel{R}{\leftarrow} \text{coins}; \]
\[ \text{let } e = \text{enc}(k2b(k'), k, r'') \text{ in} \]
\[ \text{let } ma = \text{mac}'(e, mk) \text{ in return}(e, ma) \]

\[ Q_B(k, mk) = \text{foreach } i' \leq n \text{ do } O_B(e' : \text{bitstring}, ma' : \text{macstring}) := \]
\[ \text{find } j \leq n \text{ such that defined} (e[j], ma[j]) \land e' = e[j] \land \]
\[ ma' = ma[j] \text{ then} \]
\[ \text{let } i_\bot(k2b(k'')) = \text{dec}(e', k) \text{ in return}() \]

Probability: \( \text{Succ}_{\text{MAC}}^{\text{suf-cma}}(\text{time} + n \text{time(} \text{enc}, \text{length(} \text{key})\)) + \)
\( n \text{time(} \text{dec}, \text{maxl} (\text{e}')\)) ; n, n, \text{max(maxl} (\text{e}'), \text{maxl(e)))}. \)
Proof of the example: simplify

\[ Q_0 = O_{\text{start}} := k \leftarrow^R \text{key}; \ mk \leftarrow^R \text{mkey}; \text{return}(); \]

\[ (\text{run } Q_A(k, \ mk) \mid \text{run } Q_B(k, \ mk)) \]

\[ Q_A(k, \ mk) = \text{foreach } i \leq n \ do \ O_A() := k' \leftarrow^R \text{key}; \ r'' \leftarrow^R \text{coins}; \]

\[ \text{let } e : \text{bitstring} = \text{enc}(k2b(k'), k, r'') \text{ in} \]

\[ \text{let } ma = \text{mac}'(e, \ mk) \text{ in return}(e, \ ma) \]

\[ Q_B(k, \ mk) = \text{foreach } i' \leq n \ do \ O_B(e' : \text{bitstring}, \ ma' : \text{macstring}) := \]

\[ \text{find } j \leq n \text{ such that defined}(e[j], \ ma[j]) \land e' = e[j] \land \]

\[ ma' = ma[j] \text{ then} \]

\[ \text{let } k'' = k'[j] \text{ in return}() \]

\[ \text{dec}(e', k) = \text{dec}(\text{enc}(k2b(k'[j]), k, r''[j]), k) = i_\bot(k2b(k'[j])) \]
Proof of the example: security of the encryption

\[ Q_0 = O_{\text{start}} := k \leftarrow R \text{ key}; m k \leftarrow R \text{ mkey}; \text{return}(); \]
\[ (\text{run } Q_A(k, m k) \mid \text{run } Q_B(k, m k)) \]

\[ Q_A(k, m k) = \text{foreach } i \leq n \text{ do } O_A() := k' \leftarrow R \text{ key}; r'' \leftarrow R \text{ coins}; \]
\[ \text{let } e : \text{bitstring} = \text{enc}'(Z(k2b(k')), k, r'') \text{ in} \]
\[ \text{let } ma = \text{mac}'(e, m k) \text{ in } \text{return}(e, ma) \]

\[ Q_B(k, m k) = \text{foreach } i' \leq n \text{ do } O_B(e' : \text{bitstring}, ma' : \text{macstring}) := \]
\[ \text{find } j \leq n \text{ such that } \text{defined}(e[j], ma[j]) \land e' = e[j] \land \]
\[ ma' = ma[j] \text{ then} \]
\[ \text{let } k'' = k'[j] \text{ in } \text{return}() \]

Probability: \( \text{Succ}_{\text{ind-cpa}}^{\text{SE}}(\text{time} + n \text{ time}(\text{mac}, \maxl(e)) + n^2 \text{ time}(= \text{bitstring}, \maxl(e'), \maxl(e)), n, \text{length}(\text{key})) \)
Proof of the example: simplify

\[ Q_0 = O_{start} := k \leftarrow_R key; mk \leftarrow_R mkey; \text{return}(); \]
\[ \text{(run } Q_A(k, mk) \mid \text{run } Q_B(k, mk)) \]

\[ Q_A(k, mk) = \text{foreach } i \leq n \text{ do } O_A() := k' \leftarrow_R key; r'' \leftarrow_R \text{coins}; \]
\[ \text{let } e : \text{bitstring} = \text{enc}'(Z_k, k, r'') \text{ in} \]
\[ \text{let } ma = \text{mac}'(e, mk) \text{ in return}(e, ma) \]

\[ Q_B(k, mk) = \text{foreach } i' \leq n \text{ do } O_B(e' : \text{bitstring}, ma' : \text{macstring}) := \]
\[ \text{find } j \leq n \text{ suchthat defined}(e[j], ma[j]) \land e' = e[j] \land \]
\[ ma' = ma[j] \text{ then} \]
\[ \text{let } k'' = k'[j] \text{ in return}() \]

\[ Z(k2b(k')) = Z_k \]
Proof of the example: secrecy

\[ Q_0 = O_{\text{start}} := k \overset{R}{\leftarrow} \text{key}; mk \overset{R}{\leftarrow} m\text{key}; \text{return}(); \]
\[ \left( \text{run } Q_A(k, mk) \mid \text{run } Q_B(k, mk) \right) \]

\[ Q_A(k, mk) = \text{foreach } i \leq n \text{ do } O_A() := k' \overset{R}{\leftarrow} \text{key}; r'' \overset{R}{\leftarrow} \text{coins}; \]
\[ \text{let } e : \text{bitstring} = \text{enc}'(Z_k, k, r'') \text{ in} \]
\[ \text{let } ma = \text{mac}'(e, mk) \text{ in return}(e, ma) \]

\[ Q_B(k, mk) = \text{foreach } i' \leq n \text{ do } O_B(e' : \text{bitstring}, ma' : \text{macstring}) := \]
\[ \text{find } j \leq n \text{ suchthat defined}(e[j], ma[j]) \land e' = e[j] \land \]
\[ ma' = ma[j] \text{ then} \]
\[ \text{let } k'' = k'[j] \text{ in return}() \]

Preserves the one-session secrecy of \( k'' \) but not its secrecy.
Final result

Adding the probabilities, we obtain:

Result

The probability that an adversary that runs in time at most $t$, that executes $n$ sessions of $A$ and $B$ and sends messages of length at most $l_{mB}$ to $B$ breaks the one-session secrecy of $k''$ is

$$2\text{Succ}_{\text{MAC}}^{\text{suf-cma}}(t'_1, n, n, \max(l_{mB}, l_c)) + 2\text{Succ}_{\text{SE}}^{\text{ind-cpa}}(t'_2, n, l_k)$$

where $t'_1 = t + n \text{time}(\text{enc}, l_k) + n \text{time}(\text{dec}, l_{mB})$

$t'_2 = t + n \text{time}(\text{mac}, l_c) + n^2 \text{time}(\text{bitstring}, l_{mB}, l_c)$

$l_k$ is the length of keys, $l_c$ the length of encryptions of keys.

The factor 2 comes from the definition of secrecy.
Example of the FDH signature (joint work with D. Pointcheval)

hash hash function (in the random oracle model)
f(pk, m) one-way trapdoor permutation, with inverse invf(sk, m).

We define a signature scheme as follows:
- signature \( \text{sign}(m, sk) = \text{invf}(sk, \text{hash}(hk, m)) \)
- verification \( \text{verify}(m, pk, s) = (f(pk, s) = \text{hash}(hk, m)) \)

Our goal is to show that this signature scheme is UF-CMA (secure against existential forgery under chosen message attacks).
The advantage of the adversary:

$$\max_{\mathcal{A}} \Pr \left[ (pk, sk) \overset{R}{\leftarrow} kgen; (m, s) \leftarrow \mathcal{A}^{\text{sign}(\cdot, sk)}(pk) : \text{verify}(m, pk, s) \land m \text{ was never queried to the oracle } \text{sign}(\cdot, sk) \right]$$

is small.
Formalizing the security of a signature scheme (1)

Key generation:

\[ O_{\text{start}} := r \overset{\$}{\leftarrow} \text{keyseed}; \text{let } pk = \text{pkgen}(r) \text{ in let } sk = \text{skgen}(r) \text{ in return}(pk) \]

Chooses a random seed uniformly in the set of bit-strings \textit{keyseed} (consisting of all bit-strings of a certain length), generates a public key \textit{pk}, a secret key \textit{sk}, and returns the public key.
Signature:

\[ O_S(m : \text{bitstring}) := \text{return}(\text{sign}(sk, m)) \]
Formalizing the security of a signature scheme (2)

Signature:

\[ O_S(m : \text{bitstring}) := \text{return}(\text{sign}(sk, m)) \]

This process can be called at most \( q_S \) times:

\[
\text{foreach } i_S \leq q_S \text{ do } O_S(m : \text{bitstring}) := \text{return}(\text{sign}(sk, m))
\]
Formalizing the security of a signature scheme (2)

Signature:

\[ O_S(m : \text{bitstring}) := \text{return}(\text{sign}(sk, m)) \]

This process can be called at most \( q_S \) times:

\[
\text{foreach } i_S \leq q_S \text{ do } O_S(m : \text{bitstring}) := \text{return}(\text{sign}(sk, m))
\]

In fact, this is an abbreviation for:

\[
\text{foreach } i_S \leq q_S \text{ do } O_S[i_S](m[i_S] : \text{bitstring}) := \text{return}(\text{sign}(sk, m[i_S]))
\]

The variables in repeated oracles are arrays, with one cell for each call, to remember the values used in each oracle call. These arrays are indexed with the call number \( i_S \).
Test:

\[
O_T(m' : \text{bitstring}, s : D) := \text{if verify}(m', pk, s) \text{ then } \\
\text{find } j \leq q_S \text{ such that defined}(m[j]) \land (m' = m[j]) \text{ then yield else event bad}
\]

If \( s \) is a signature for \( m' \) and the signed message \( m' \) is not contained in the array \( m \) of messages passed to signing oracle, then the signature is a forgery, so we execute event bad.
Formalizing the security of a signature scheme (summary)

The signature and test oracles make sense only \textbf{after} the key generation oracle has been called, hence a \textit{sequential composition}.

The signature and test oracles are \textbf{simultaneously} available, hence a \textit{parallel composition}.

\begin{verbatim}
O_{start}() := r \leftarrow keyseed; let pk = pkgen(r) in let sk = skgen(r) in
return(pk);

(* signature oracle *)
foreach i_{\mathcal{S}} \leq q_{\mathcal{S}} do
O_{\mathcal{S}}(m : bitstring) := return(sign(sk, m))

(* forged signature? *)
O_{\mathcal{T}}(m' : bitstring, s : D) := if verify(m', pk, s) then
find j \leq q_{\mathcal{S}} suchthat defined(m[j]) \land (m' = m[j])
then yield else event bad)
\end{verbatim}

Probability of executing \textbf{event} bad = probability of forging a signature.
Application to the FDH signature scheme

We add a hash oracle because the adversary must be able to call the random oracle (even though it cannot be implemented).

\[ O_{\text{start}} := hk \leftarrow \text{hashkey}; \ r \leftarrow \text{keyseed}; \]

let \( sk = \text{skgen}(r) \) in let \( pk = \text{pkgen}(r) \) in return(\( pk \));

(* hash oracle *)

\[
\text{foreach } i_H \leq q_H \text{ do } O_H(x : \text{bitstring}) := \text{return}(\text{hash}(hk, x))
\]

(* signature oracle *)

\[
\text{foreach } i_S \leq q_S \text{ do } O_S(m : \text{bitstring}) := \text{return}(\text{invf}(sk, \text{hash}(hk, m)))
\]

(* forged signature? *)

\[
O_T(m' : \text{bitstring}, s : D) := \text{if } f(pk, s) = \text{hash}(hk, m') \text{ then find } j \leq q_S \text{ suchthat defined}(m[j]) \land (m' = m[j]) \text{ then yield else event bad)}
\]

Goal: bound the probability that event bad is executed in this game.
FDH: security of a random oracle

A random oracle is equivalent to a “random function”: a function that
- returns a new random number when it is called on a new argument,
- and returns the same result when it is called on the same argument.

\[ k \xleftarrow{\$} \text{hashkey}; \textbf{foreach} \ i \leq N \ \textbf{do} \ \text{Ohash}(x : \text{bitstring}) := \text{return}(\text{hash}(k, x)) \approx_0 \]

\textbf{foreach} \ i \leq N \ \textbf{do} \ \text{Ohash}(x : \text{bitstring}) :=
- find \ j \leq N \ suchthat \ defined(x[j], r[j]) \ \&\& \ (x = x[j])
- then return(\(r[j]\))
- else \(r \xleftarrow{\$} D; \ \text{return}(r)\)
For a test $r' = h(x')$, we can avoid computing $h(x')$ explicitly:

- if $x'$ has been passed to the hash function previously, compare $r'$ with the previous result;
- otherwise, return false.
For a test $r' = h(x')$, we can avoid computing $h(x')$ explicitly:

- if $x'$ has been passed to the hash function previously, compare $r'$ with the previous result;
- otherwise, return false.

In the latter case, test indeed false, except when the fresh random number $h(x')$ collides with $r'$ (probability $1/|D|$).
FDH: security of a random oracle (optimized)

\[ k \leftarrow \text{hashkey}; \]

\[ \begin{aligned}
& \text{(foreach } i \leq N \text{ do } Ohash(x : \text{bitstring}) := \text{return}(\text{hash}(k, x)) | \\
& \text{foreach } ieq \leq Neq \text{ do } Oeq(x' : \text{bitstring}; r' : D) := } \\
& \text{return}(r' = \text{hash}(k, x')) )
\end{aligned} \]

\[ \approx \frac{Neq}{|D|} \]

\[ \begin{aligned}
& \text{(foreach } i \leq N \text{ do } Ohash(x : \text{bitstring}) := } \\
& \quad \text{find } j \leq N \text{ suchthat defined}(x[j], r[j]) \&\& (x = x[j]) \\
& \quad \text{then return}(r[j]) \\
& \quad \text{else } r \leftarrow R; \text{return}(r) | \\
& \text{foreach } ieq \leq Neq \text{ do } Oeq(x' : \text{bitstring}; r' : D) := } \\
& \quad \text{find } j \leq N \text{ suchthat defined}(x[j], r[j]) \&\& (x' = x[j]) \\
& \quad \text{then return}(r' = r[j]) \\
& \quad \text{else return}(\text{false})
\end{aligned} \]
The adversary inverts $f$ when, given the public key $pk = pkgen(r)$ and the image of some random $x$ by $f(pk, \cdot)$, it manages to find $x$ (without having the trapdoor).

The function $f$ is **one-way** when the adversary has negligible probability of inverting $f$.

**Definition (One-wayness)**

$$
\text{Succ}_{\mathcal{P}}^{ow}(t) = \max_{\mathcal{A}} \Pr \left[ \begin{array}{l}
    r \xleftarrow{\$} \text{keyseed}, pk \xleftarrow{\$} pkgen(r), x \xleftarrow{\$} D, \\
    y \leftarrow f(pk, x), x' \leftarrow \mathcal{A}(pk, y) : x = x'
\end{array} \right]
$$

where $\mathcal{A}$ runs in time at most $t$. 
FDH: one-wayness (preliminary version)

\[ r \leftarrow^R \text{keyseed}; \]
\[ \text{Opk}() := \text{return}(\text{pkgen}(r)) | \]
\[ \text{foreach } i_1 \leq N_f \text{ do } x \leftarrow^R D; \]
\[ \text{Oy}() := \text{return}(f(\text{pkgen}(r), x)) | \]
\[ \text{foreach } i_2 \leq N_2 \text{ do } \text{Oeq}(x' : D) := \text{return}(x' = x)) \]

\[ \approx \]

\[ r \leftarrow^R \text{keyseed}; \]
\[ \text{Opk}() := \text{return}(\text{pkgen}(r)) | \]
\[ \text{foreach } i_1 \leq N_f \text{ do } x \leftarrow^R D; \]
\[ \text{Oy}() := \text{return}(f(\text{pkgen}(r), x)) | \]
\[ \text{foreach } i_2 \leq N_2 \text{ do } \text{Oeq}(x' : D) := \text{return}(\text{false})) \]
FDH: one-wayness

\[ r \stackrel{R}{\leftarrow} \text{keyseed}; \ (\]
\[ \text{Opk}() := \text{return}(\text{pkgen}(r)) \mid \]
\[ \text{foreach } i_1 \leq N_f \text{ do } x \stackrel{R}{\leftarrow} D; \ (\]
\[ \text{Oy}() := \text{return}(f(\text{pkgen}(r), x)) \mid \]
\[ \text{foreach } i_2 \leq N_2 \text{ do } \text{Oeq}(x' : D) := \text{return}(x' = x) \mid \]
\[ \text{Ox}() := \text{return}(x)) \]

\implies

\[ r \stackrel{R}{\leftarrow} \text{keyseed}; \ (\]
\[ \text{Opk}() := \text{return}(\text{pkgen}(r)) \mid \]
\[ \text{foreach } i_1 \leq N_f \text{ do } x \stackrel{R}{\leftarrow} D; \ (\]
\[ \text{Oy}() := \text{return}(f(\text{pkgen}(r), x)) \mid \]
\[ \text{foreach } i_2 \leq N_2 \text{ do } \text{Oeq}(x' : D) := \]
\[ \quad \text{if defined}(\text{leak}) \text{ then } \text{return}(x' = x) \text{ else } \text{return}(\text{false}) \mid \]
\[ \text{Ox}() := \text{let } \text{leak} : \text{bool} = \text{true in return}(x)) \]
Using CryptoVerif Proof technique Encrypt-then-MAC FDH Conclusion

**FDH: one-wayness**

\[ r \xleftarrow{R} \text{keyseed}; ( \]
\[ Opk() := \text{return}(pkgen(r)) | \]
\[ \text{foreach } i1 \leq Nf \text{ do } x \xleftarrow{R} D; ( \]
\[ Oy() := \text{return}(f(pkgen(r), x)) | \]
\[ \text{foreach } i2 \leq N2 \text{ do } Oeq(x' : D) := \text{return}(x' = x) | \]
\[ Ox() := \text{return}(x)) ) \]

\[ \approx Nf \times \text{Succ}^ow_P(\text{time} + (#Oy - 1) \times \text{time}(f)) \]

\[ r \xleftarrow{R} \text{keyseed}; ( \]
\[ Opk() := \text{return}(pkgen'(r)) | \]
\[ \text{foreach } i1 \leq Nf \text{ do } x \xleftarrow{R} D; ( \]
\[ Oy() := \text{return}(f'(pkgen'(r), x)) | \]
\[ \text{foreach } i2 \leq N2 \text{ do } Oeq(x' : D) := \]
\[ \text{if defined}(\text{leak}) \text{ then return}(x' = x) \text{ else return}(\text{false}) | \]
\[ Ox() := \text{let } \text{leak} : \text{bool} = \text{true in return}(x)) ) \]
FDH: other properties of one-way trapdoor permutations

(1)

invf is the inverse of f:

\[ \forall r : \text{keyseed}, x : D; \text{invf}(\text{skgen}(r), f(\text{pkgen}(r), x)) = x \]

f is injective:

\[ \forall k : \text{key}, x : D, x' : D; (f(k, x) = f(k, x')) = (x = x') \]
FDH: other properties of one-way trapdoor permutations (2)

We can replace a uniformly distributed random number $y$ with $f(pkgen(r), x)$ where $x$ is a uniformly distributed random number:

\[
y \leftarrow D; \ Oim() := \text{return}(y) \\
\approx_0 \\
x \leftarrow D; \ Oim() := \text{return}(f(pkgen(r), x))
\]
We can replace a uniformly distributed random number $y$ with $f(pkgen(r), x)$ where $x$ is a uniformly distributed random number:

$$
y \overset{R}{\leftarrow} D; \text{Oim}() := \text{return}(y)
$$

$$
\approx_0
$$

$$
x \overset{R}{\leftarrow} D; \text{Oim}() := \text{return}(f(pkgen(r), x))
$$

$\Rightarrow$ Can be applied too often!
FDH: other properties of one-way trapdoor permutations (2)

We can replace a uniformly distributed random number $y$ with $f(pkgen(r), x)$ where $x$ is a uniformly distributed random number:

$$r \overset{R}{\leftarrow} \text{keyseed}; (O_{pk}() := \text{return}(pkgen(r)) |$$

$$\text{foreach } i1 \leq Nf \text{ do } y \overset{R}{\leftarrow} D; (O_{\text{ant}}() := \text{return}(\text{invf}(\text{skgen}(r), y)) |$$

$$O_{\text{im}}() := \text{return}(y)))$$

$$\approx_0$$

$$r \overset{R}{\leftarrow} \text{keyseed}; (O_{pk}() := \text{return}(pkgen(r)) |$$

$$\text{foreach } i1 \leq Nf \text{ do } x \overset{R}{\leftarrow} D; (O_{\text{ant}}() := \text{return}(x) |$$

$$O_{\text{im}}() := \text{return}(f(pkgen(r), x))))$$
Demo

- CryptoVerif input file: fdh.ocv
- library of primitives
- run CryptoVerif
- output
FDH: initial game

\[ O_{start} := hk \overset{R}{\leftarrow} \text{hashkey}; r \overset{R}{\leftarrow} \text{keyseed}; \]

let \( sk : key = \text{skgen}(r) \) in
let \( pk : key = \text{pkgen}(r) \) in return(\( pk \));

( (* hash oracle *)
  foreach \( i_H \leq q_H \) do \( O_H(x : \text{bitstring}) := \text{return}(\text{hash}(hk, x)) \)
|
  (* signature oracle *)
  foreach \( i_S \leq q_S \) do \( O_S(m : \text{bitstring}) := \text{return}(\text{invf}(sk, \text{hash}(hk, m))) \)
|
  (* forged signature? *)
  \( O_T(m' : \text{bitstring}, s : D) := \)
if \( f(pk, s) = \text{hash}(hk, m') \) then
find \( j \leq q_S \) suchthat defined(\( m[j] \)) \&\& (\( m' = m[j] \)) then
  yield
else
  event bad
)
FDH step 1: apply the security of the random oracle

Replace each occurrence of hash($M$) with a lookup in the arguments of previous calls to hash.

- If $M$ is found, return the same result as the previous result.
- Otherwise, pick a new random number and return it.

For instance, return(hash($hk$, $x$)) is replaced with

\[
\text{find } i_1 \leq q_S \text{ such that defined}(m[i_1], r_1[i_1])
\]

\[
\text{&& (} x = m[i_1] \text{) then return}(r_1[i_1])
\]

or

\[
\text{find } i_2 \leq q_H \text{ such that defined}(x[i_2], r_2[i_2])
\]

\[
\text{&& (} x = x[i_2] \text{) then return}(r_2[i_2])
\]

else

\[
r_2 \leftarrow D; \text{ return}(r_2)
\]

The test $f(pk, s) = \text{hash}(hk, m')$ uses Oeq. Probability difference $1/|D|$. 
FDH step 2: simplify

(* forged signature? *)

\[ O_T(m': \text{bitstring}, s : D) := \]

\[
\text{find } i_5 \leq q_S \text{ such that defined}(m[i_5], r_1[i_5]) \land (m' = m[i_5]) \text{ then}
\]

\[
\quad \text{if } (f(pk, s) = r_1[i_5]) \text{ then}
\]

\[
\quad \text{find } j \leq q_S \text{ such that defined}(m[j]) \land (m' = m[j]) \text{ then yield else event bad}
\]

\[
\text{orfind } i_6 \leq q_H \text{ such that defined}(x[i_6], r_2[i_6]) \land (m' = x[i_6]) \text{ then}
\]

\[
\quad \text{if } (f(pk, s) = r_2[i_6]) \text{ then}
\]

\[
\quad \text{find } j \leq q_S \text{ such that defined}(m[j]) \land (m' = m[j]) \text{ then yield else event bad}
\]

\[
\text{else}
\]

\[
\quad \text{if false then}
\]

\[
\quad \text{find } j \leq q_S \text{ such that defined}(m[j]) \land (m' = m[j]) \text{ then yield else event bad}
\]

The red test always succeeds, so the blue part becomes yield.
The magenta part becomes yield.
FDH step 3: substitute $sk$ with its value

The variable $sk$ is replaced with $skgen(r)$, and the assignment

```
let $sk : key = skgen(r)$
```

is removed.

This transformation is advised in order to able to apply the
permutation property.
FDH step 4: permutation

(* signature oracle *)
foreach $i_S \leq q_S$ do
$O_S(m : \text{bitstring}) :=$
find $i_3 \leq q_S$ suchthat defined ($m[i_3], r_1[i_3]$) && ($m = m[i_3]$) then
   return (invf (skgen ($r$), $r_1[i_3]$))
orfind $i_4 \leq q_H$ suchthat defined ($x[i_4], r_2[i_4]$) && ($m = x[i_4]$) then
   return (invf (skgen ($r$), $r_2[i_4]$))
else
   $r_1 \leftarrow D$;
   return (invf (skgen ($r$), $r_1$))

$r_i \leftarrow D$ becomes $y_i \leftarrow D$,
invf (skgen ($r$), $r_i$) becomes $y_i$,
$r_i$ becomes f (pkgen ($r$), $y_i$)
FDH step 5: simplify

(* forged signature? *)

\[ O_T(m' : \text{bitstring}, s : D) := \]

\[ \begin{align*}
\text{find } i_5 \leq q_S \text{ such that } & \text{defined}(m[i_5], r_1[i_5]) \text{ and } (m' = m[i_5]) \text{ then yield} \\
\text{or find } i_6 \leq q_H \text{ such that } & \text{defined}(x[i_6], r_2[i_6]) \text{ and } (m' = x[i_6]) \text{ then} \\
& \text{if } (f(pk, s) = f(pkgen(r), y_2[i_6])) \text{ then} \\
& \text{find } j \leq q_S \text{ such that } \text{defined}(m[j]) \text{ and } (m' = m[j]) \text{ then yield} \text{ else event bad}
\end{align*} \]

\[ f(pk, s) = f(pkgen(r), y_i) \text{ becomes } s = y_i, \]

knowing \( pk = pkgen(r) \) and the injectivity of \( f \):

\[ \forall k : \text{key}, x : D, x' : D; (f(k, x) = f(k, x')) = (x = x') \]
FDH step 6: one-wayness

(* forged signature? *)

\[ O_T(m' : \text{bitstring}, s : D) := \]

\text{find } i_5 \leq q_S \text{ such that } \text{defined}(m[i_5], r_1[i_5]) \land (m' = m[i_5]) \text{ then }
\text{yield}

\text{or find } i_6 \leq q_H \text{ such that } \text{defined}(x[i_6], r_2[i_6]) \land (m' = x[i_6]) \text{ then }
\text{if } s = y_2[i_6] \text{ then}
\text{find } j \leq q_S \text{ such that } \text{defined}(m[j]) \land (m' = m[j]) \text{ then yield else event bad}

\[ s = y_i \text{ becomes } \text{find } j_i \leq q_H \text{ such that } \text{defined}(\text{leak}_i[j_i]) \]
\text{then } s = y_i \text{ else false,}

In hash oracle, \( f(pkgen(r), y_i) \) becomes \( f'(pkgen'(r), y_i) \),
In signature oracle, \( y_i \) becomes \text{let } \text{leak}_i : \text{bool} = \text{true in } y_i.

Difference of probability: \( (q_H + q_S)\text{Succ}^{ow}_{\mathcal{P}}(\text{time} + (q_H - 1)\text{time}(f)) \).
FDH step 7: simplify

(* forged signature? *)

\[ O_T(m' : \text{bitstring}, s : D) := \]

\textbf{find } i_5 \leq q_S \textbf{ suchthat defined}(m[i_5], r_1[i_5]) \land (m' = m[i_5]) \textbf{ then yield}

\textbf{or find } i_6 \leq q_H \textbf{ suchthat defined}(x[i_6], r_2[i_6]) \land (m' = x[i_6]) \textbf{ then}

\textbf{find } j_2 \leq q_S \textbf{ suchthat defined}(\text{leak}_2[j_2]) \land (i_4[j_2] = i_6) \textbf{ then}

\textbf{if } s = y_2[i_6] \textbf{ then}

\textbf{find } j \leq q_S \textbf{ suchthat defined}(m[j]) \land (m' = m[j]) \textbf{ then yield else event bad}

The test in \textcolor{red}{red} always succeeds, so \textcolor{event}{event} bad disappears, which proves the desired property.
FDH step 7: simplify (2)

(* forged signature? *)

\[ O_T(m' : \text{bitstring}, s : D) := \]

\[ \text{orfind } i_6 \leq q_H \text{ suchthat defined}(x[i_6], r_2[i_6]) \&\& (m' = x[i_6]) \text{ then } \]

\[ \text{find } j_2 \leq q_S \text{ suchthat defined}(\text{leak}_2[j_2]) \&\& (i_4[j_2] = i_6) \text{ then } \]

\[ \text{if } s = y_2[i_6] \text{ then } \]

\[ \text{find } j \leq q_S \text{ suchthat defined}(m[j]) \&\& (m' = m[j]) \text{ then yield else event bad } \]

Definition of \text{leak}_2:

\[ \text{foreach } i_S \leq q_S \text{ do } \]

\[ O_S(m : \text{bitstring}) := \]

\[ \text{orfind } i_4 \leq q_H \text{ suchthat defined}(x[i_4], y_2[i_4]) \&\& (m = x[i_4]) \text{ then } \]

\[ \text{let leak}_2 : \text{bool} = \text{true in} \ldots \]

When \text{leak}_2[j_2] is defined, \( m[j_2] \) is defined and \( m[j_2] = x[i_4[j_2]] = x[i_6] = m' \) so the red test succeeds with \( j = j_2 \).
Adding the probabilities, we obtain:

**Result**

The probability that an adversary that runs in time at most $t$ and makes $q_S$ signature queries and $q_H$ hash queries forges a FDH signature is at most

$$\frac{1}{|D|} + (q_S + q_H)\text{Succ}_P^\text{ow}(t + (q_H - 1)\text{time}(f))$$
Experiments

Tested on the following protocols (original and corrected versions):
- Otway-Rees (shared-key)
- Yahalom (shared-key)
- Denning-Sacco (public-key)
- Woo-Lam shared-key and public-key
- Needham-Schroeder shared-key and public-key

Shared-key encryption is assumed to be IND-CPA and INT-CTXT (authenticated encryption scheme).

Public-key encryption is assumed to be IND-CCA2.

We prove secrecy of session keys and correspondence properties.
Results

- In these examples, **CryptoVerif succeeds** in proving the desired properties when they hold, and obviously it always fails to prove them when they do not hold.

- Some public-key protocols need **manual proofs**. (Give the cryptographic proof steps and single assignment renaming instructions.)

- **Runtime**: 7 ms to 35 s, average: 5 s on a Pentium M 1.8 GHz.
Other case studies

- Full domain hash signature (with David Pointcheval)
- Encryption schemes of Bellare-Rogaway’93 (with David Pointcheval)
- Kerberos V, with and without PKINIT (with Aaron D. Jaggard, Andre Scedrov, and Joe-Kai Tsay)
- OEKE (variant of Encrypted Key Exchange)
- A part of an F# implementation of the TLS transport protocol (Microsoft Research and MSR-INRIA)
- SSH Transport Layer Protocol (with David Cadé)
- Avionic protocols (ARINC 823, ICAO9880 3rd edition)
- TextSecure v3 (with Nadim Kobeissi and Karthikeyan Bhargavan)
- TLS 1.3 draft 18 (with Karthikeyan Bhargavan and Nadim Kobeissi)
- WireGuard (with Benjamin Lipp and Karthikeyan Bhargavan)
- HPKE (with Joël Alwen, Eduard Hauck, Eike Kiltz, Benjamin Lipp, and Doreen Riepel)
Conclusion

CryptoVerif can automatically prove the security of primitives and protocols.

- The security assumptions are given as indistinguishability properties (proved manually once).
- The protocol or scheme to prove is specified in a process calculus.
- The prover provides a sequence of indistinguishable games that lead to the proof and a bound on the probability of an attack.
- The user is allowed (but does not have) to interact with the prover to make it follow a specific sequence of games.
Recent and future work: CryptoVerif extensions

- Support more **primitives**:
  - More equations, *e.g.* associativity for XOR [Done]
  - Primitives with internal state
- Combine CryptoVerif with EasyCrypt.
- Quantum adversaries.
- Improvements in the **proof strategy**.
  - More precise manual hints?
- More **case studies**.
  - Will suggest more extensions.
- **Certify** CryptoVerif.
Going further

- Proof of implementations of protocols in the computational model:
  - by analysis of implementations (e.g., FS2CV, F*, C to CryptoVerif),
  - by generation of implementations from specifications (e.g., CryptoVerif to OCaml, CryptoVerif to F*).
- Take into account side-channels.
I warmly thank David Pointcheval for his advice and explanations of the computational proofs of protocols. This project would not have been possible without him.

Work partly supported by the ANR projects FormaCrypt (ARA SSIA 2005), ProSe (VERSO 2010, decision number 2010-VERS-004), and TECAP (decision number ANR-17-CE39-0004-03) and by funding from the France 2030 program managed by the ANR under the reference ANR-22-PECY-0006 (PEPR Cybersecurity SVP).