Theme 2
A Computationally sound logic

FormaCrypt meeting

March 6, ENS

Summary

Take an existing (successful) **logic** from the **symbolic world (PCL)**

- No protocol restriction (hand-made proofs, checkable in Isabelle)
- Datas *abstracted* by symbols (no collision, etc...)

Equip it with a **probabilistic polynomial-time semantic**

- Messages = *bitstrings* ; Intruder = *polynomial-time algorithm*.
- Sec. proofs that by reasoning about *probability*

Summary

Take an existing (successful) **logic** from the **symbolic world (PCL)**

- No protocol restriction (hand-made proofs, checkable in Isabelle)
- Datas *abstracted* by symbols (no collision, etc...)

Equip it with a **probabilistic polynomial-time semantic**

- Messages = *bitstrings* ; Intruder = *polynomial-time algorithm*.
- Sec. proofs that by reasoning about *probability*

We get a **Computationally Sound Logic**

- **No probabilistic computations** required for a proof with this logic.
- Instead use a set of **axioms** and **rules**
- **Easy to extend** the set of axioms & rules to model new properties
- **Modularity** : each axiom or rule describe on one cryptographic propert

Protocol Syntax

Atoms & Terms :

$$\begin{aligned} Atom &= Name \,|\, Nonce \,|\, Thread \,|\, Key \,|\, Var \\ Term &= Atom \,|\, \langle Term, Term \rangle \,|\, \{Term\}_{Key}^{Nonce} \end{aligned}$$

Actions :

$$\begin{aligned} Action ::= & \ \mathrm{New}(Thread,\ NVar) \\ & |\, Var := \mathrm{enc}(Thread,\ Term,\ Key) \quad |\, \mathrm{Send}(Thread,\ Term) \\ & |\, Var := \mathrm{dec}(Thread,\ Term,\ Key) \quad |\, \mathrm{Receive}(Thread,\ Term) \\ & |\, Var = Var \quad |\, \mathrm{Match}(Thread,\ Var/Term) \end{aligned}$$

Protocol specification :

- Based on the cord calculus
- A role is a sequence of actions (+ init. knowledge)

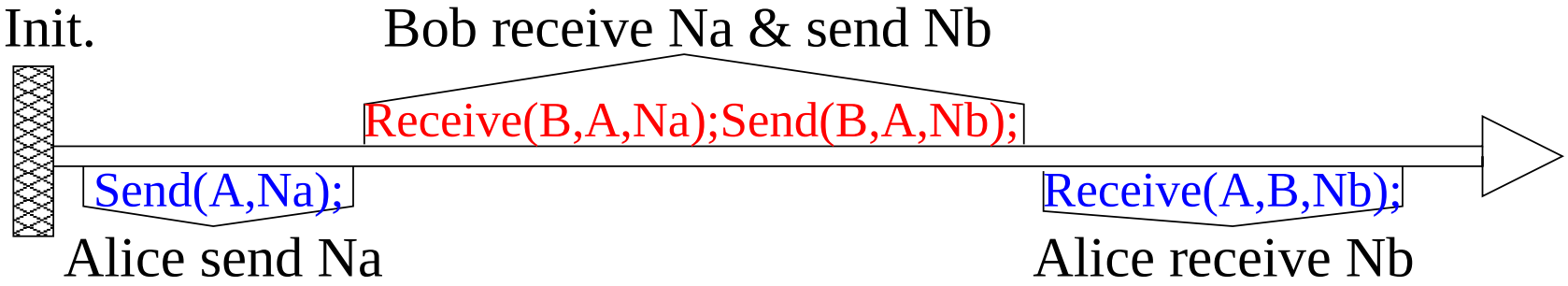
Computational Traces

Given :

Protocol Q ; Security parameter η ; Polynomial-time Adversary $\mathcal{A}$;

Some (trace) randomness R ; Sessions and honesty/dishonesty ;

Trace :



plus all the **bitstring values** of all atoms and variables (Na, Nb, ...)

and **Init** : use R to assign names, generate keys, etc ...

Logic Syntax (elements of..)

Property ϕ :

Trace-based predicates :

- $Fresh(Thread, Nonce)$, $Honest(Name)$, $Start(Thread)$,
- $Term = Term$, $Contains(Term, Term)$, $Send(...)$, etc...
- $DecryptsHonest(Thread, Term)$, $Source(Thread, Term, Term)$

First order elements : $\exists Var.\, \phi$ $\forall Var.\, \phi$

$\neg\phi$ $\phi \vee \psi$ $\phi \wedge \psi$ $\phi \supset \psi$

Logic Syntax (elements of..)

Property ϕ :

Trace-based predicates :

- $Fresh(Thread, Nonce)$, $Honest(Name)$, $Start(Thread)$,
- $Term = Term$, $Contains(Term, Term)$, $Send(...)$, etc...
- $DecryptsHonest(Thread, Term)$, $Source(Thread, Term, Term)$

First order elements : $\exists Var.\ \phi$ $\forall Var.\ \phi$

$\neg\phi$ $\phi \vee \psi$ $\phi \wedge \psi$ $\phi \supset \psi$

Actions ordering predicate : $Action \leq Action$

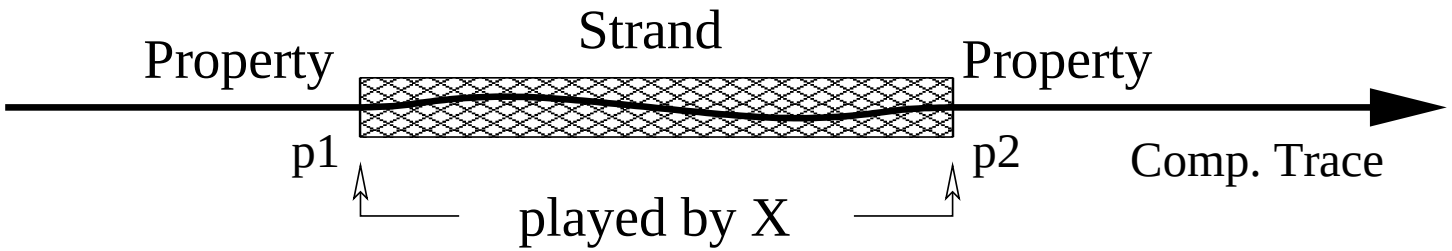
Tests : $Possess(Thread, Term)$, $Indist(Thread, Term)$, ...

Logic Syntax (elements of..)

Modal formulas :

$$Formula \quad ::= \quad Property\ [Strand]_{Thread}\ Property \quad | \quad Property$$

Meaning of $\psi\,[P]_{\tilde{X}}\,\phi$:



If ψ is true at position p_1 and $\tilde{X}$ plays P between p_1 and p_2,

then ϕ is true at position p_2.

Security Proofs in PCL

Security proof = Combination of axioms & rules

Examples of axioms & rules

– **AN3** : $\top\ [\mathrm{New}(x)]_X\ \mathrm{Has}(\tilde{Y}, x) \Rightarrow \tilde{Y} = \tilde{X}$

i.e. if agent X generates a nonce x, then no other agent Y knows

– **G2** : $$\frac{\theta\ [P]_X\ \varphi, \qquad \theta' \supset \theta, \qquad \varphi \supset \varphi'}{\theta'\ [P]_X\ \varphi'}$$

Example of proof

(Hyp.)	$\mathrm{Has}(A, x) \Rightarrow \mathrm{Has}(A, msg_1(\hat{A}, \hat{B}, x))$	(
ORIG, **G2**	$\mathrm{Start}(A)\ [\mathrm{New}(x)]_A\ \mathrm{Has}(A, x)$	(
(1), **(2)**, **G2**	$\mathrm{Start}(A)\ [\mathrm{New}(x)]_A\ \mathrm{Has}(A, msg_1(\hat{A}, \hat{B}, x))$	(

Main Theorem

Definition : $Q \models \varphi$ iff $\forall \mathcal{D}$ distinguisher, $\forall \nu$ neg. function,

$$\exists N, \forall \eta \geq N, \qquad [\![\varphi]\!]^{\mathcal{D}}_{\mathcal{T},\emptyset} \geq 1 - \nu(\eta)$$

Main Theorem

Definition : $Q \models \varphi$ iff $\forall \mathcal{D}$ distinguisher, $\forall \nu$ neg. function,

$$\exists N, \forall \eta \geq N, \qquad [\![\varphi]\!]^{\mathcal{D}}_{\mathcal{T},\emptyset} \geq 1 - \nu(\eta)$$

Theorem :

$$\forall Q \text{ protocol}, \forall \varphi \text{ formula}, \quad \text{if} \quad Q \vdash \varphi \quad \text{then} \quad Q \models \varphi$$

Remarks :

Main axioms comes from particular cryptographic property :

- Information-theory for **AN2** or **AN3,**
- CCA2 assumption for **Source** axiom, etc...