

A Symbolic Intruder Model for Hash-Collision Attacks

Yannick Chevalier and Mounira Kourjeh
IRIT _ LILaC

Presented at CSTVA06

Outline

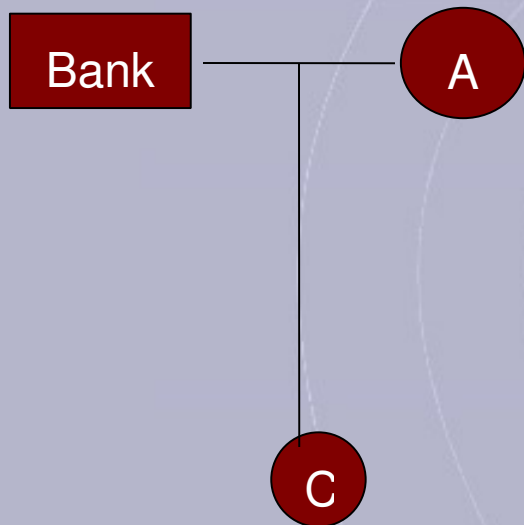
- Hash functions
- Insecurity Decidability procedure
- Application to I_h intruder system
- Conclusion

Hash function

- $h: M \rightarrow M'$, $|M| > |M'|$
 \Rightarrow unavoidable collision
- **Properties**
 - given x , compute $h(x)$ is easy.
 - given y , compute x such that $y=h(x)$ is infeasible (pre-image resistance) .
 - given x , compute x' such that $h(x)=h(x')$ is infeasible (2-pre-image resistance).
 - **compute x and x' such that $h(x)=h(x')$ is feasible (hash collision).**

Hash functions

- Exploitation of collision property



Protocol execution:

$A \longrightarrow \text{Bank}: m1, \{h(m1)\}_{K_a^{-1}}$

Execution of attack:

$A \longrightarrow \text{Bank}(C): m1, \{h(m1)\}_{K_a^{-1}}$

$C(A) \longrightarrow \text{Bank}: m2, \{h(m1)\}_{K_a^{-1}}$

C make A send m1

Insecurity Decidability procedure

- **Signature**

$G =$ set of function symbols.

$$A = \{u_i = v_i\}_{i \in \{1, \dots, n\}}$$

- **Intruder System**

$$I_G = \langle G, S, A \rangle$$

where S is used to create $R = \{l \rightarrow r\}$ as follows:

for each $t \in S$, $\text{Var}(t) \rightarrow t$, $L^t = \{l \rightarrow r; \exists \text{ bound } \theta, l = \text{Var}(t) \theta$
and $r =_{A} t \theta\}$.

Insecurity Decidability procedure

■ Definition1

For two set of terms E and F , we have $E \rightarrow F$ if and only if there exists $l \rightarrow r \in R$; $l \subseteq E$ and $F = E, r$.

■ Definition2

For a set of terms E , a variable v , a substitution θ , we have θ Satisfies $E \triangleright v$ if and only if there exists a derivation from $E \theta$ to $v \theta$ using the intruder deduction rules.

Insecurity Decidability procedure

- **Constraint System**

$$C = ((E_i \triangleright v_i)_{i \in \{1, \dots, n\}}, \{l_j = r_j\}_{j \in \{1, \dots, m\}})$$

E1: intruder initial knowledge

$$E_i \subseteq E_{i+1}$$

$$\text{Var}(E_i) \subseteq \{v_1, \dots, v_{i-1}\}$$

- **Reachability Problem : SAT(I_G)**

Input: C, < order over Var(C) and Cons(C)

Output: C is satisfiable if and only if there exists a substitution θ s.t. 1) θ satisfies $E_i \triangleright v_i$ for all $i \in \{1, \dots, n\}$,
 2) θ satisfies $l_j =_A r_j$ for all $j \in \{1, \dots, m\}$,
 3) θ satisfies <.

Application to I_h intruder system

- Collision from m_1 and m_2

$$m_1 = x_1 \cdot x_2 \quad \text{and} \quad m_2 = y_1 \cdot y_2$$

$$m'_1 = x_1 \cdot f(x_1, x_2, y_1, y_2) \cdot x_2$$

$$m'_2 = y_1 \cdot g(x_1, x_2, y_1, y_2) \cdot y_2$$

such that $h(m'_1) = h(m'_2)$

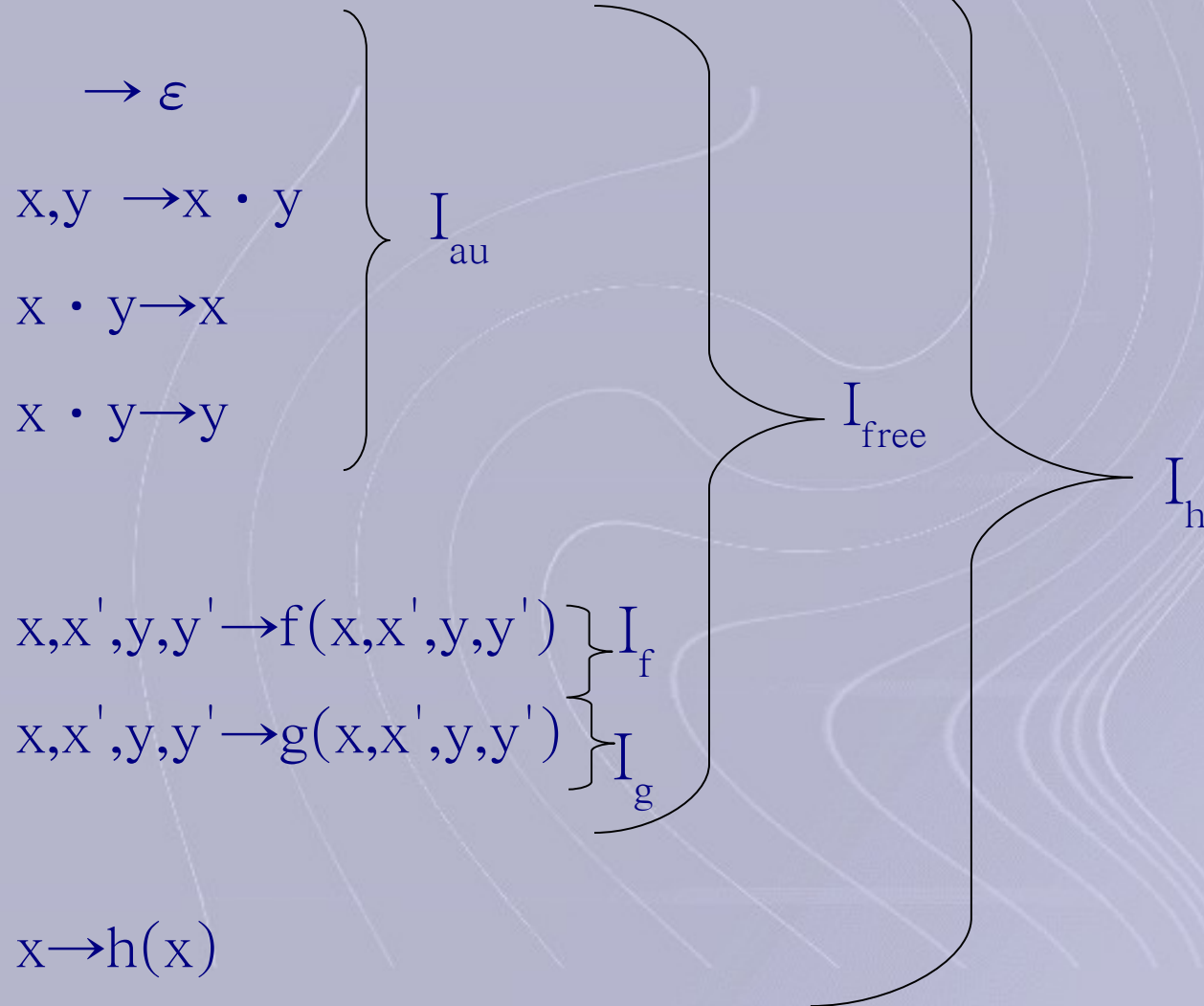
- Equational theory for I_h intruder

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

$$x \cdot \varepsilon = \varepsilon \cdot x = x$$

$$h(x \cdot f(x, x', y, y') \cdot x') = h(y \cdot g(x, x', y, y') \cdot y')$$

Application to I_h intruder system



Application to I_h intruder system

- **Theorem [Chevalier and Rusinowitch,05]**
 $SAT(I \cup I')$ is reducible to $SAT(I)$ and $SAT(I')$.
- **This paper:**
 - 1) construct a decision procedure for $SAT(I_h)$ by reducing $SAT(I_h)$ to $SAT(I_{free})$
 - 2) construct a decision procedure for $SAT(I_{free})$
 - 3) construct procedure for deciding insecurity of a class of cryptographic protocol with bounded number of sessions.

Future Works

- Implementation of the decision procedure in CL-Atse(Ofmc).
- Formalisation of the *AU intruder system*.
- Handling of other non-perfect primitives.

Questions?

ychevali@irit.fr

kourjieh@irit.fr