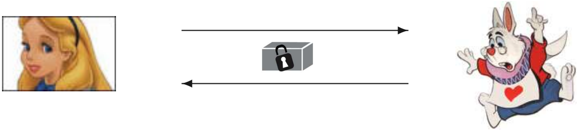
Intruder Deduction for *AC*-like Equational Theories with Homomorphism

Pascal Lafourcade
(joint work with Denis Lugiez & Ralf Treinen)

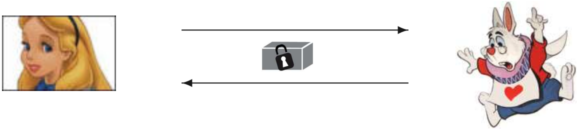
LSV E.N.S. Cachan & LIF University of Provence Marseille

RTA'05 : 20 April 2005

Alice communicates with The Whiterabbit via a network.



Alice communicates with The Whiterabbit via a network.



Intruder

- Active Intruder : Eaveasdrop, compose and play messages.
- Passive Intruder : Just eavesdrop messages.

Intruder deduction = Passive Intruder + Secrecy Property

Abelian Group (AG) [Comon-Shmatikov 03] PTIME

- $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ Associativity
- $x \oplus y = y \oplus x$ Commutativity
- $x \oplus 0 = x$ Unity
- $x \oplus I(x) = 0$ Inversion

XOR (ACUN) [Rusinowitch & al 03] [Comon-Shmatikov 03] PTIME

- $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ Associativity
- $x \oplus y = y \oplus x$ Commutativity
- $x \oplus 0 = x$ Unity
- $x \oplus x = 0$ Nilpotency

Homomorphism [Comon-Treinen 03] PTIME

- $\{\langle a, b \rangle\}_k = \langle \{a\}_k, \{b\}_k \rangle$

Our Goal Add Homomorphism over ⊕ for AC, ACUN and AG

- $f(a \oplus b) = f(a) \oplus f(b)$

(A) $\dfrac{u \in T}{T \vdash_E u}$

(P) $\dfrac{T \vdash_E u \qquad T \vdash_E v}{T \vdash_E \langle u, v \rangle}$

(UL) $\dfrac{T \vdash_E \langle u, v \rangle}{T \vdash_E u}$

(UR) $\dfrac{T \vdash_E \langle u, v \rangle}{T \vdash_E v}$

(C) $\dfrac{T \vdash_E u \qquad T \vdash_E v}{T \vdash_E \{u\}_v}$

(D) $\dfrac{T \vdash_E \{u\}_v \qquad T \vdash_E v}{T \vdash_E u}$

(F) $\dfrac{T \vdash_E u}{T \vdash_E f(u)}$

(Eq(E)) $\dfrac{T \vdash_E u \qquad u =_E v}{T \vdash_E v}$

(GX) $\dfrac{T \vdash_E u_1 \quad \cdots \quad T \vdash_E u_n}{T \vdash_E u_1 \oplus \ldots \oplus u_n}$

Equational Theory $E = (R, S)$
$R = \{x \oplus x \to 0, x \oplus 0 \to x, f(x \oplus y) \to f(x) \oplus f(y), f(0) \to 0\}$
$S = (AC)$
R is convergent and terminating modulo $S = (AC)$

(A) $$\frac{u \in T}{T \vdash u \downarrow}$$

(P) $$\frac{T \vdash u \qquad T \vdash v}{T \vdash \langle u, v \rangle \downarrow}$$

(UL) $$\frac{T \vdash r}{T \vdash u \downarrow} \quad \mathit{if}\, \langle u, v \rangle \rightarrow^! r$$

(UR) $$\frac{T \vdash r}{T \vdash v \downarrow} \quad \mathit{if}\, \langle u, v \rangle \rightarrow^! r$$

(C) $$\frac{T \vdash u \qquad T \vdash v}{T \vdash \{u\}_v \downarrow}$$

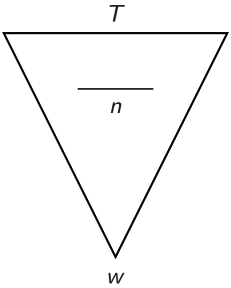
(D) $$\frac{T \vdash r \qquad T \vdash v}{T \vdash u \downarrow} \quad \mathit{if}\, \{u\}_v \rightarrow^! r$$

(F) $$\frac{T \vdash u}{T \vdash f(u) \downarrow}$$

(GX) $$\frac{T \vdash u_1 \quad \cdots \quad T \vdash u_n}{T \vdash (u_1 \oplus \ldots \oplus u_n) \downarrow}$$

Let $S : T \rightarrow T$

- A proof P of $T \vdash w$ is S-local :



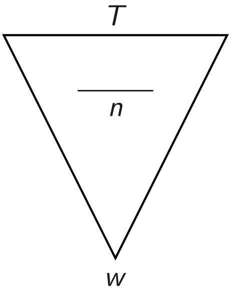
$$\forall n \in P, n \in S(T \cup \{w\})$$

- A Proof System is S-local

$$\mathrm{atoms}(a \oplus b \oplus \langle d, c\rangle) = \{a, b, \langle d, c\rangle\}$$
$$\mathrm{atoms}(\langle d \oplus a, c\rangle) = \{\langle d \oplus a, c\rangle\}$$

Definition

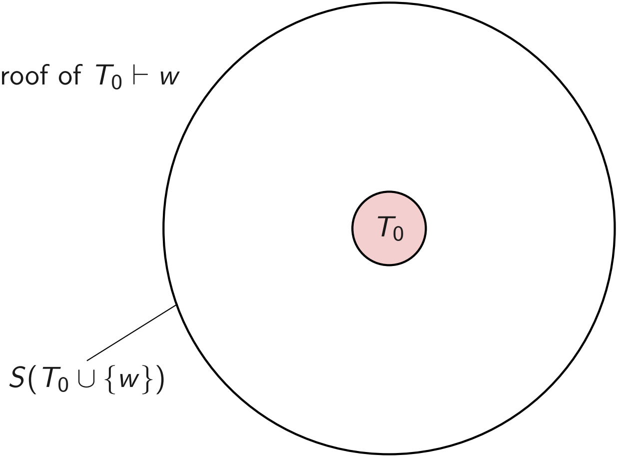
Binary proof: all nodes have at most two atoms.



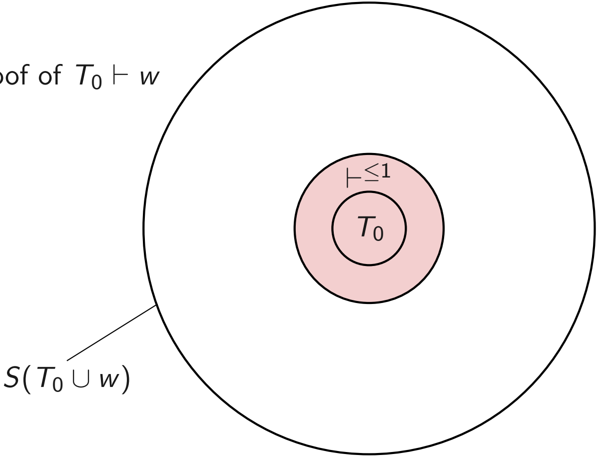
$\forall n \in P, n = *$ or $n = * \oplus *$

~~$n = * \oplus * \oplus \ldots \oplus *$~~

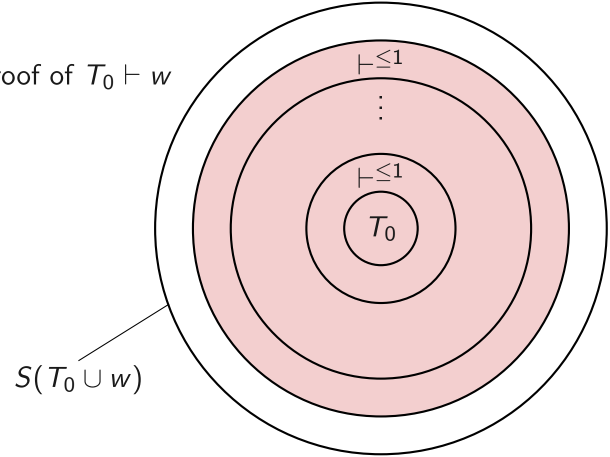
P a S-local proof of $T_0 \vdash w$



P a S-local proof of $T_0 \vdash w$



P a S-local proof of $T_0 \vdash w$



Extended McAllester's Theorem

Let P be a proof system, if:

- one-step deducibility is decidable with complexity K_1,
- the size of $S(T)$ is computable with complexity K_2,
- P is S-local,

then provability in the proof system P is decidable in $max(K_1, K_2)$.

Example

Let $T = \{a_1 \oplus a_2 \oplus a_3, a_1 \oplus a_4, a_2 \oplus a_4\}$ and $w = a_1 \oplus a_2$

$$\begin{array}{lcl} x_0 & : & a_1 \oplus a_2 \oplus a_3 \\ x_1 & : & a_1 \oplus a_4 \\ x_2 & : & a_2 \oplus a_4 \end{array}$$

We obtain the following system of equations :

$$\left\{ \begin{array}{lcl} a_1 & : & x_0 + x_1 = 1 \\ a_2 & : & x_0 + x_2 = 1 \\ a_3 & : & x_0 = 0 \\ a_4 & : & x_1 + x_2 = 0 \end{array} \right.$$

ACh Case:

- Binary case : One-step deductibility is PTIME (Directly).
- General case : Solvability of a system of linear equations over $\mathbb{N}$ is a NP-complete problem [Pap94].

ACUNh Case:

Solvability of a system of linear equations over $\mathbb{Z}/2\mathbb{Z}$ is PTIME[KKS87].

AGh Case:

Solvability of a system of linear equations over $\mathbb{Z}$ is PTIME[Sch86].

Definition of $S_T(t)$

$S_T(T)$ is the smallest set such that:

- $t \in S_T(t)$
- $\langle u, v \rangle \in S_T(t) \Rightarrow u, v \in S_T(t)$
- $\{u\}_v \in S_T(t) \Rightarrow u, v \in S_T(t)$
- $u = u_1 \oplus \ldots \oplus u_n \in S_T(t) \Rightarrow \mathrm{atoms}(u) \subseteq S_T(t)$
- $f(u)\downarrow \in S_T(t) \Rightarrow u \in S_T(t)$
- $f(u_1) \oplus \ldots \oplus f(u_n) \in S_T(t) \Rightarrow u_1 \oplus \ldots \oplus u_n \in S_T(t)$

Computing $S_T(T)$ is polynomial in size of T.

Lemma :

If $t \in S_T(u) \setminus \{u\}$ then $\forall v, t \in S_T(u \oplus v)$

Notice: False in ACUNh and AGh.

Example

This lemma is not satisfied in the ACUNh case:
$u = a \oplus b \oplus c$, $v = c \oplus b \Rightarrow u \oplus v = a$ and $b \notin S_T(u \oplus v)$

S_T-Locality for ACh

Counter-Example with S_T and ACUNh

Example

$T = \{u \oplus v, f(v)\}, w = f(u),\ S_T(T \cup \{w\}) = \{u, v, u \oplus v, f(v), f(u)\}$

$$\text{(GX)}\ \dfrac{\text{(F)}\ \dfrac{\text{(A)}\ \dfrac{u \oplus v \in T}{T \vdash u \oplus v}}{T \vdash f(u) \oplus f(v)} \qquad \text{(A)}\ \dfrac{f(v) \in T}{T \vdash f(v)}}{T \vdash f(u)}$$

Problem: $f(u) \oplus f(v) \notin S_T(T \cup \{w\})$.

Definitions of ⊕-lazy and ⊕-eager Proof

- ⊕-*lazy proof* : flat and no (GX) immediately above (F) in P.
- ⊕-*eager proof* : flat and at most one (F) immediately above (GX).

Transformation Rule

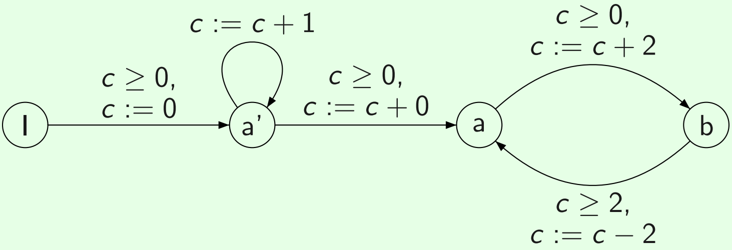
$$(F)\ \dfrac{(GX)\ \dfrac{T \vdash x_1 \ldots T \vdash x_n}{T \vdash x_1 \oplus \ldots \oplus x_n}}{T \vdash f(x_1) \oplus \ldots \oplus f(x_n)} \implies (GX)\ \dfrac{(F)\ \dfrac{T \vdash x_1}{T \vdash f(x_1)} \quad \ldots \quad (F)\ \dfrac{T \vdash x_n}{T \vdash f(x_n)}}{T \vdash f(x_1) \oplus \ldots \oplus f(x_n)}$$

Figure: Transformation of (GX)-(F) into (F)-(GX)

In the binary case one-counter automaton is used to bound the number of applications of f.

Example

The automaton A_T for $T = \{a \oplus f^2(b), a\}$:



Results in the ACUNh Case

- Binary case:
  - Define S_f in "PTIME" (bounding number of application of f using a one-counter automata representation)
  - Show S_f-locality in a minimal $\oplus$-lazy proof.
  - One-step deducibility is PTIME
- General case:
  - Define $S_{\oplus}$ in "EXPTIME" (partial sums)
  - Show $S_{\oplus}$-locality in a minimal $\oplus$-eager proof.
  - One-step deducibility is PTIME

The rule $x \oplus x = 0$ becomes $x \oplus I(x) = 0$.
A new rule (I) is used.

Results

- Binary case: show "PTIME locality".
- General case: show "EXP-TIME locality".

- $\{u \oplus v\}_k = \{u\}_k \oplus \{v\}_k$
- There are many different homomorphism symbols (H).
- $\Rightarrow$ ACH locality in PTIME.
- ACUNH and AGH
  - Binary case: locality in PTIME.
  - General case: locality in EXP-TIME.

	Intruder deduction problem	
	Binary case	**General case**
ACh	*PTIME*	*NP-Complete*
ACUNh	*PTIME*	*EXP-TIME*
AGh	*PTIME*	*EXP-TIME*

Same results are obtained if homomorphism = encryption.

- Active case

	Complexity		
	Unification Problem	**Intruder Deduction**	**Security Problem**
ACUN	*NP-complete [Guo,Narendran98]*	*P-TIME [CS03]*	*NP-Complete [CKTR03]*
ACh	*Undecidable [Narendran96]*	*NP-Complete*	*Undecidable*
ACUNh	*NP-complete [Guo,Narendran98]*	*EXP-TIME*	*?*
AGh	*Decidable [Baader93]*	*EXP-TIME*	*?*

Thank you for your attention