Symbolic Protocol Analysis in Presence of a Homomorphism Operator and *Exclusive-Or*

Ralf Treinen
joint work with
Pascal Lafourcade, Stéphanie Delaune, Denis Lugiez

LSV, CNRS UMR 8643, ENS de Cachan & INRIA Futurs
LIF, Université Aix-Marseille 1 & CNRS UMR 6166

February 14, 2007

TMN Protocol: Distribution of a fresh session key

[Tatebayashi, Matsuzuki, Newmann 89]:

A	W	D		
	$\rightarrow$		:	$A, D, \{N_A\}_{Pub_W}$
		$\rightarrow$	:	W, A
		$\leftarrow$	:	$D, A, \{N_D\}_{Pub_W}$
	$\leftarrow$		:	$W, D, N_A \oplus N_D$

Alice retrieves N_D:

Using $x \oplus x \oplus y = y$, knowing N_A and N_D, she deduces N_D.

Attack on TMN Protocol

With homomorphic encryption

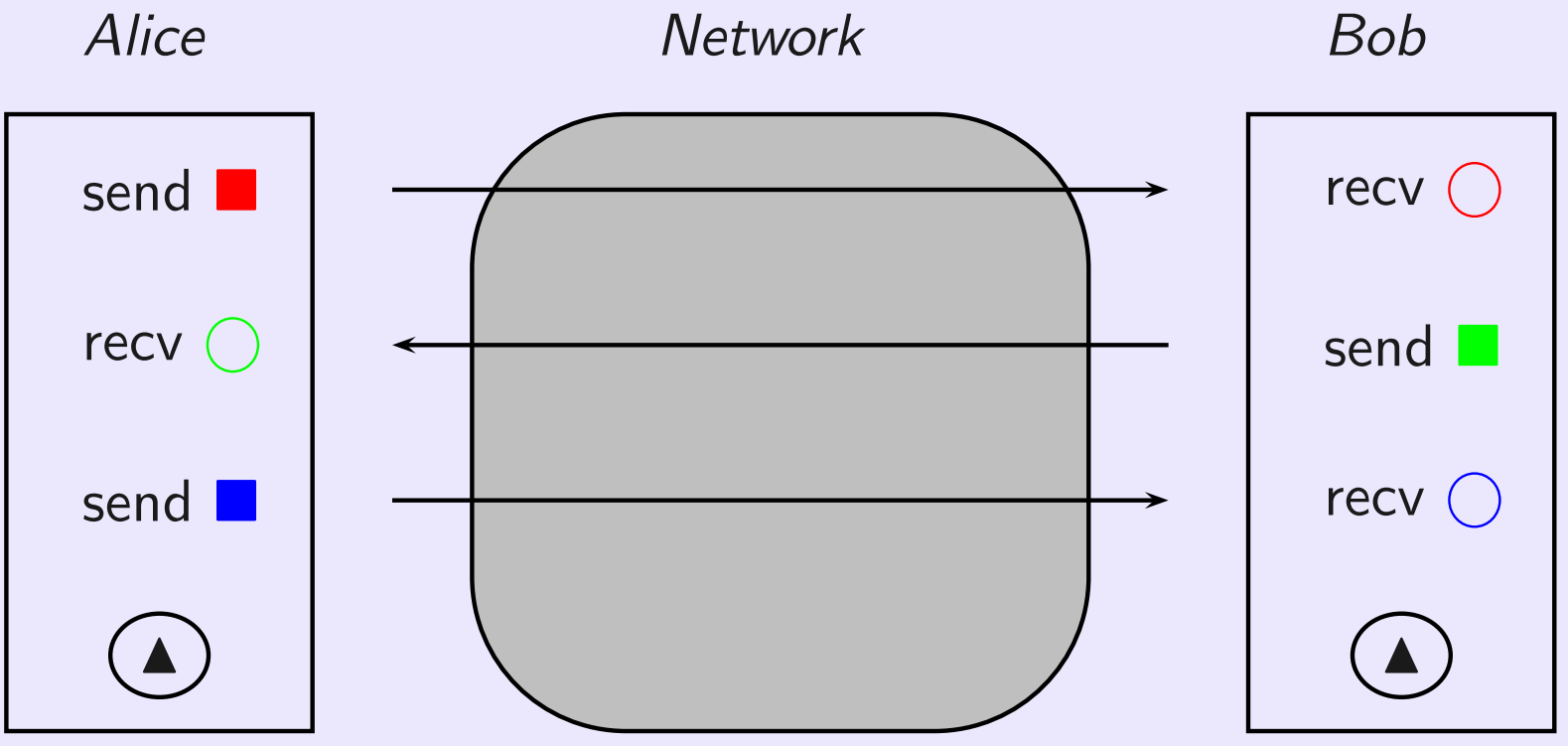
C		W		Dog	
	$\rightarrow$				: $C, Dog, \underbrace{\{N_A\}_{Pub_W} * \{N_C\}_{Pub_W}}_{\{N_A * N_C\}_{Pub_W}}$
			$\rightarrow$		: W, C
			$\leftarrow$		: $Dog, C, \{N_{Dog}\}_{Pub_W}$
	$\leftarrow$				: $W, N_A * N_C \oplus N_{Dog}$

Catbert Learns:

Using $x \oplus x \oplus y = y$, knowing N_C and N_{Dog}, he deduces N_A.

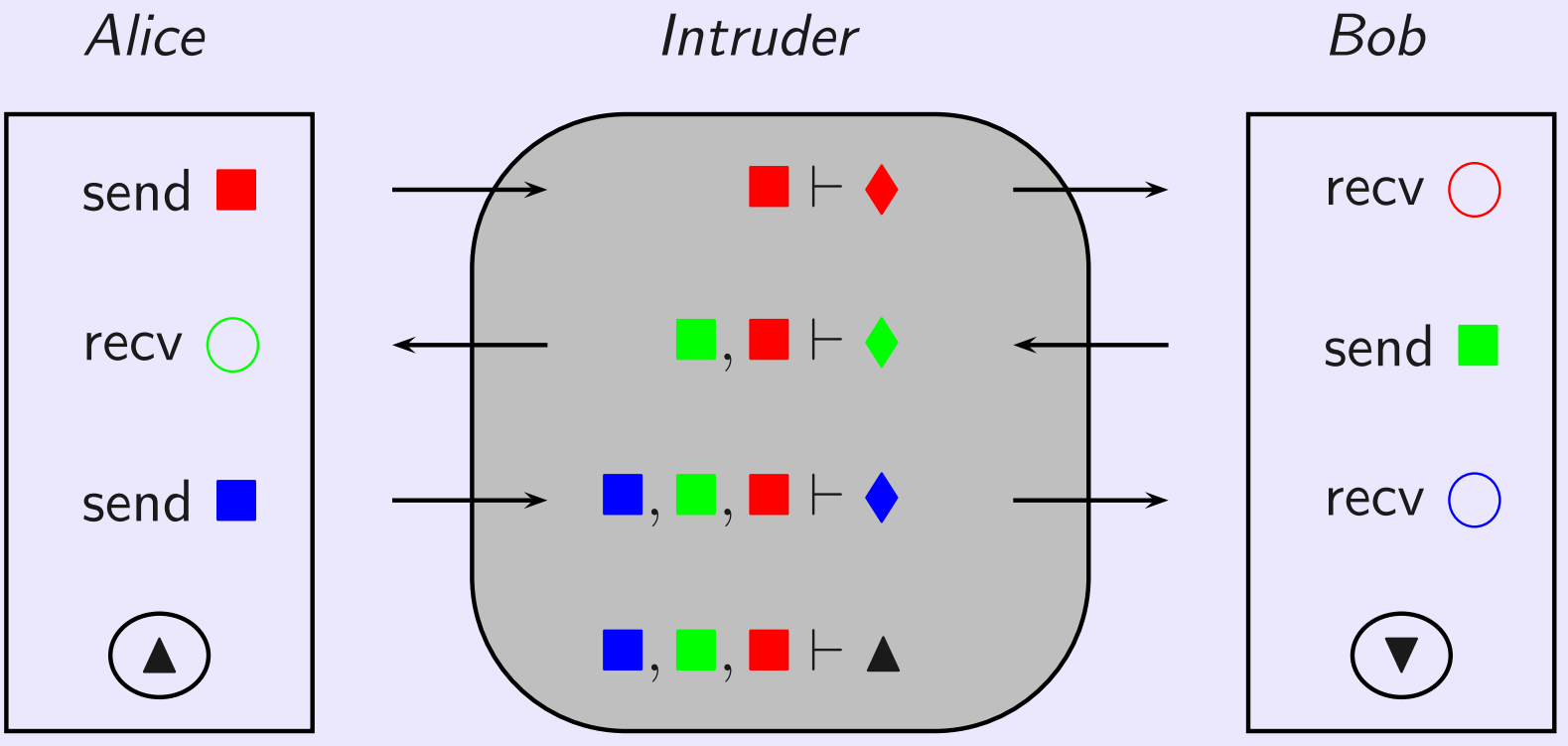
Intended Execution of Protocols

Execution of a Protocol between 2 Agents



The Intruder is the Network

Intruder can deduce messages by $\vdash$



Constraint System

- choose number of instances of the protocol
- guess a linearisation of the execution

$$\begin{array}{lcl} t_0, \ldots, t_n & \Vdash & u_1 \\ \vdots & \vdots & \vdots \\ t_0, \ldots, t_n, \ldots, t_k & \Vdash & u_{k+1} = \mathit{secret} \end{array}$$

Satisfiability is NP-complete [Rusinowitch, Turuani '03].

Example: TMN protocol

Protocol

$$
\begin{array}{lllll}
1. & A & \rightarrow & S: & A, B, h(K_a) \\
2. & S & \rightarrow & B: & S, A \\
3. & B & \rightarrow & S: & B, A, h(K_b) \\
4. & S & \rightarrow & A: & S, B, K_b \oplus K_a
\end{array}
$$

Constraint system (for one session)

$T_0 = \{A, B, S, I, C, h(K_b), h(K_a), K_i\}$

$$
\mathcal{C} \quad := \quad \left\{ \begin{array}{ll}
T_0 \Vdash X_a, X_b, h(Y_a) & S \text{ receives a request from } I \\
T_1 := T_0, S, X_a & S \text{ answers the request to } X_b \\
T_1 \Vdash X_b, X_a, h(Y_b) & S \text{ receives the answer of } X_b \\
T_2 := T_1, S, X_b, Y_a \oplus Y_b & S \text{ answers the request to } I \\
T_2 \Vdash K_b & \text{the secret } K_b \text{ is revealed}
\end{array} \right.
$$

If this system has a solution then the secret K_b can be obtain by the Intruder.

Perfect Cryptography Assumption

Knowledge about some encrypted message can only be obtained when encryption key is known.

Weakening of the Perfect Cryptography Assumption

Cryptographic primitives have properties which

- are necessary for the protocol
- can be exploited by an intruder

Algebraic properties: expressed by equational axioms

Abelian Group and Exponential [Millen-Shmatikov 05] NP

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

XOR [Rusinowitch & al 03] [Comon-Shmatikov 03] NP

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

Our contribution

Homomorphism over XOR

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

Outline

Outline

Inference System: Dolev-Yao with rewriting

$$(A)\quad \frac{u \in T}{T \vdash u} \qquad (UL)\quad \frac{T \vdash \langle u, v \rangle}{T \vdash u}$$

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

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

$$(M_E)\quad \frac{T \vdash u_1 \quad \cdots \quad T \vdash u_n}{T \vdash C[u_1, \ldots, u_n]\downarrow}$$

C is an context made with $\{h, \oplus\}$

Example for M_E

$$\frac{T \vdash a \oplus h(a) \quad T \vdash b}{T \vdash a \oplus h^2(a) \oplus h(b)}$$

$$C[u_1, u_2] = u_1 \oplus h(u_1) \oplus h(u_2)$$

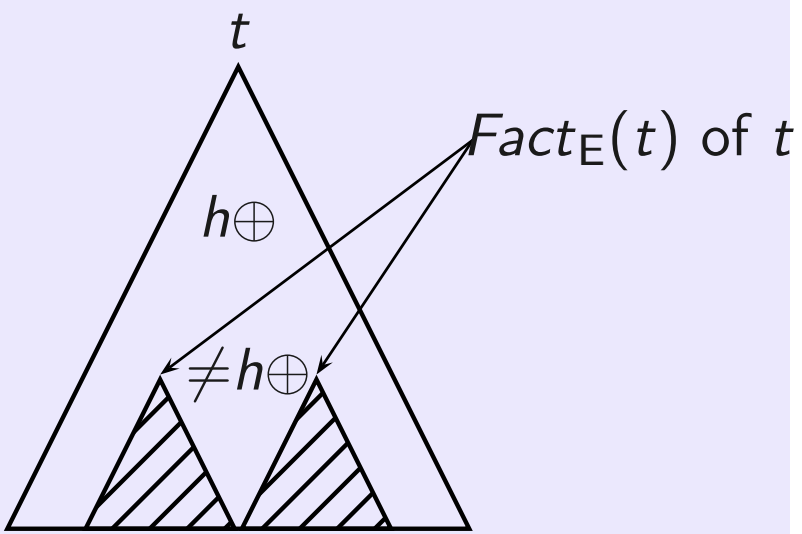
Standard Terms and Factors

t is *standard* if $t \neq f(u)$ where $f \in \{\oplus, h\}$

$Fact_{\mathsf{E}}(t)$: top-level standard subterms of t

Example:
$t_1 = h^2(a) \oplus b \oplus c$
$Fact_{\mathsf{E}}(t_1) = \{a, b, c\}$

$t_2 = h(\langle a, b \rangle) \oplus c$
$Fact_{\mathsf{E}}(t_2) = \{\langle a, b \rangle, c\}$



Subterms

The set of *subterms* :

- if $t = f(t_1, \ldots, t_n)$ standard:
  $St_{\mathsf{E}}(t) = \{t\} \cup St_{\mathsf{E}}(t_1) \cup \ldots \cup St_{\mathsf{E}}(t_n)$
- if $t = f(t_1, \ldots, t_n)$ non-standard:
  $St_{\mathsf{E}}(t) = \{t\} \cup St_{\mathsf{E}}(Fact_{\mathsf{E}}(t_1)) \cup \ldots \cup St_{\mathsf{E}}(Fact_{\mathsf{E}}(t_n))$

Example:
$t_1 = h^2(a) \oplus b \oplus c$
$St_{\mathsf{E}}(t_1) = \{t_1, a, b, c\}$.

$t_2 = h(\langle a, b \rangle) \oplus c$
$St_{\mathsf{E}}(t_2) = \{t_2, \langle a, b \rangle, a, b, c\}$.

Theorem of Locality [LLT'05,Del'05]

A minimal proof P of $T \vdash u$ contains only terms in $St_{\mathsf{E}}(T \cup \{u\})$.

Theorem of Locality [LLT'05,Del'05]

A minimal proof P of $T \vdash u$ contains only terms in $St_{\mathsf{E}}(T \cup \{u\})$.

Complexity of Intruder Deduction [Del'05]

$T \vdash u$ (for T, u ground) is decidable in PTIME

The proof uses

- McAllester's locality theorem
- linear equation solving over $\mathbb{Z}/2\mathbb{Z}[h]$

Outline

Deterministic Protocol

Definition

$$P \quad := \quad \begin{cases} u_1 \longrightarrow v_1 \\ u_2 \longrightarrow v_2 \\ \vdots \\ u_n \longrightarrow v_n \end{cases}$$

A protocol P is deterministic iff:
for all ground substitutions τ, σ and for all $i \in [1, \ldots n]$:
if $u_1\tau =_E u_1\sigma, \ldots, u_i\tau =_E u_i\sigma$ then $v_i\tau =_E v_i\sigma$.

Determinism is decidable (disunification problem modulo ACUNh)

Reminder: Constraint System

$$\mathcal{C} \quad := \quad \left\{ \begin{array}{lll} T_1 & \Vdash & u_1 \\ T_2 & \Vdash & u_2 \\ \vdots & \vdots & \vdots \\ T_k & \Vdash & u_k \end{array} \right.$$

where

- $T_1 \subseteq T(F)$
- $T_2, \ldots, T_k \subseteq T(F, X)$
- $u_1, \ldots, u_k \in T(F, X)$

System of Constraints Well-formed [Millen-Shmatikov 03]

$\mathcal{C} = \{T_i \Vdash u_i\}_{1 \leq i \leq k}$ is *well-formed* if:

- *monotonicity*: The knowledge of the intruder is increasing.

$$T_1 \subseteq T_2 \subseteq \ldots \subseteq T_k$$

- *origination*: Variables appear first on right side:

$$x \in vars(T_i) \Rightarrow \exists j < i : x \in vars(u_i)$$

System of Constraints Well-formed [Millen-Shmatikov 03]

$\mathcal{C} = \{T_i \Vdash u_i\}_{1 \leq i \leq k}$ is *well-formed* if:

- *monotonicity*: The knowledge of the intruder is increasing.

$$T_1 \subseteq T_2 \subseteq \ldots \subseteq T_k$$

- *origination*: Variables appear first on right side:

$$x \in vars(T_i) \Rightarrow \exists j < i : x \in vars(u_i)$$

System of Constraints Well-defined [Millen-Shmatikov 03]

$\mathcal{C}$ is *well-defined* if for every substitution θ, $\mathcal{C}\theta$ is well-formed.

Well-definedness: Example 1

The Constraint System from the TMN Example is Well-Defined

$T_0 = \{A, B, S, I, C, h(K_b), h(K_a), K_i\}$

$$\mathcal{C} := \left\{ \begin{array}{lll} T_0 & \Vdash & X_a, X_b, h(Y_a) \\ T_0, S, X_a & \Vdash & X_b, X_a, h(Y_b) \\ T_0, S, X_a, S, X_b, Y_a \oplus Y_b & \Vdash & K_b \end{array} \right.$$

Well-Definedness: Example 2

The Constraint System

$$\mathcal{C} := \left\{ \begin{array}{lll} T_0 & \Vdash & X \oplus Y \\ T_0, X & \Vdash & c \end{array} \right.$$

Well-Definedness: Example 2

The Constraint System

$$\mathcal{C} := \left\{ \begin{array}{lll} T_0 & \Vdash & X \oplus Y \\ T_0, X & \Vdash & c \end{array} \right.$$

Monotonicity OK !

Well-Definedness: Example 2

The Constraint System

$$\mathcal{C} \quad := \quad \left\{ \begin{array}{lll} T_0 & \Vdash & X \oplus Y \\ T_0, X & \Vdash & c \end{array} \right.$$

Monotonicity OK !

Origination OK !

Well-Definedness: Example 2

The Constraint System

$$\mathcal{C} := \left\{ \begin{array}{lll} T_0 & \Vdash & X \oplus Y \\ T_0, X & \Vdash & c \end{array} \right.$$

Monotonicity OK !

Origination OK !

But NOT well-defind !

$\theta = \{Y \rightarrow X\}$ and $\mathcal{C}\theta$ is not well-formed:

$$\mathcal{C}\theta := \left\{ \begin{array}{lll} T_0 & \Vdash & 0 \\ T_0, X & \Vdash & c \end{array} \right.$$

Lemma

Deterministic protocol $\Rightarrow$ well-defined constraint system.

Example: Non well-defined constraint system:

$$\mathcal{C} := \left\{ \begin{array}{lll} T_0 & \Vdash & X \oplus Y \\ T_0, X & \Vdash & c \end{array} \right.$$

Witness of non-definedness: $\theta = \{Y \rightarrow X\}$
Corresponding protocol: $P : X \oplus Y \rightarrow X$
is non-deterministic:
On reception of message 0, one can

- send out a since $a + a = 0$
- send out b since $b + b = 0$

Outline

Conservative Solution

Conservative solution σ

σ does not introduce structure not already in $\mathcal{C}$.

Example:

$$\begin{array}{lcl} 0, a, h(b) & \Vdash & h(x) \\ 0, a, h(b), x & \Vdash & \langle a, b \rangle \end{array}$$

$\sigma = \{x \mapsto \langle a, a \rangle \oplus b\}$ is a solution not conservative.
$\langle a, a \rangle$ is not a structure of $\mathcal{C}$.
However, $\rho = \{x \mapsto b\}$ is a conservative solution of $\mathcal{C}$.

Conservative Solution

Conservative solution σ

σ does not introduce structure not already in $\mathcal{C}$.

Example:

$$\begin{array}{lcl} 0, a, h(b) & \Vdash & h(x) \\ 0, a, h(b), x & \Vdash & \langle a, b \rangle \end{array}$$

$\sigma = \{x \mapsto \langle a, a \rangle \oplus b\}$ is a solution not conservative.
$\langle a, a \rangle$ is not a structure of $\mathcal{C}$.
However, $\rho = \{x \mapsto b\}$ is a conservative solution of $\mathcal{C}$.

Lemma

Let $\mathcal{C}$ be a well-defined constraint system. If there exists a solution σ of $\mathcal{C}$ then there exists a conservative one.

Lifting Locality Lemma and Effective Unification

Lifting Locality Lemma

σ a conservative solution of $\mathcal{C} = \{C_1, \ldots, C_k\}$. For each $i \leq k$, there exists a proof P_i of $C_i\sigma$ which involves only terms in $St_{\mathsf{E}}(\mathcal{C})\sigma$.

Effective Unification in ACUNh

Unification in ACUNh is finitary and there is an effective algorithm to compute all unifiers.

Outline

From Constraints to One-step Constraints

TMN Example

$T_0 = \{A, B, S, I, C, h(K_b), h(K_a), K_i\}$
$T_1 := T_0, S, X_a$
$T_2 := T_1, S, X_b, Y_a \oplus Y_b$

$$\mathcal{C} \quad := \quad \left\{ \begin{array}{lll} T_0 & \Vdash & X_a, X_b, h(Y_a) \\ T_1 & \Vdash & X_b, X_a, h(Y_b) \\ T_2 & \Vdash & K_b \end{array} \right.$$

We obtain a well-defined constraint system.

From Constraints to One-step Constraints

TMN Example

$T_0 = \{A, B, S, I, C, h(K_b), h(K_a), K_i\}$
$T_1 := T_0, S, X_a$
$T_2 := T_1, S, X_b, Y_a \oplus Y_b$

$$\mathcal{C} := \begin{cases} T_0 & \Vdash & X_a, X_b, h(Y_a) \\ T_1 & \Vdash & X_b, X_a, h(Y_b) \\ T_2 & \Vdash & K_b \end{cases}$$

We obtain a well-defined constraint system.

Guess set of subterms of $\mathcal{C}$ and an order on these subterms

$S_0 = \{X_a, X_b, h(Y_a)\}$ $S_1 = \{Y_b, h(Y_b)\}$ and $S_2 = \{K_b\}$.

$$\mathcal{C}' := \begin{cases} T_0 & \Vdash_1 & X_a \\ T_0, X_a & \Vdash_1 & X_b \\ T_0, X_a, X_b & \Vdash_1 & h(Y_a) \\ T_0, X_a, X_b, h(Y_a) & \Vdash_1 & X_a, X_b, h(Y_a) \\ T_1, S_0 & \Vdash_1 & Y_b \\ T_1, S_0, Y_b & \Vdash_1 & h(Y_b) \\ T_1, S_0, Y_b, h(Y_b) & \Vdash_1 & X_b, X_a, h(Y_b) \\ T_2, S_0, S_1 & \Vdash_1 & K_b \end{cases}$$

From One-step Constraints to M_E Constraints

Guess equalities between subterms of $\mathcal{C}$.
Consider all the possible applications of rules (C) (P) (D) (UR) (UL)

Example

$$\mathcal{C} \quad := \quad \left\{ \begin{array}{lll} \langle a, b\rangle & \Vdash_1 & \langle X, b\rangle \\ \langle a, b\rangle, X \oplus b & \Vdash_1 & Y \oplus \langle a, b\rangle a \end{array} \right.$$

Guess $\{\langle X, b\rangle = \langle a, b\rangle\}$, compute ACUNh m.g.u. $\theta : \{X \mapsto a\}$

$$\mathcal{C}\theta \quad := \quad \left\{ \begin{array}{lll} \langle a, b\rangle & \Vdash_{M_E} & \langle a, b\rangle \\ \langle a, b\rangle, a \oplus b & \Vdash_{M_E} & Y \oplus \langle a, b\rangle \end{array} \right.$$

Protocol is still well-defined, has a non-collapsing solution.

TMN Example

Substitution

We guess on $St_E(\mathcal{C}')$,
$R = \{X_a = I; X_b = C; Y_b = K_i; K_b = Y_a \oplus Y_b\}$.
Compute ACUNh m.g.u. from R:
$\theta = \{X_a \mapsto I; X_b \mapsto C; Y_b \mapsto K_i; Y_a \mapsto K_b \oplus K_i\}$.

$\mathcal{C}\theta$ is ground, every constraint is satisfied then there is an ATTACK.

Retrieve the real ATTACK

TMN Protocol

$T_0 = \{A, B, S, I, C, h(K_b), h(K_a), K_i\}$

$$\mathcal{C} \quad := \quad \begin{cases} T_0 \Vdash X_a, X_b, h(Y_a) & S \text{ receives a request from } I \\ T_1 := T_0, S, X_a & S \text{ answers the request to } X_b \\ T_1 \Vdash X_b, X_a, h(Y_b) & S \text{ receives the answer of } X_b \\ T_2 := T_1, S, X_b, Y_a \oplus Y_b & S \text{ answers the request to } I \\ T_2 \Vdash K_b & \text{the secret } K_b \text{ is revealed} \end{cases}$$

$\theta = \{X_a \mapsto I; X_b \mapsto C; Y_b \mapsto K_i; Y_a \mapsto K_b \oplus K_i\}$

$$\mathcal{C}\theta \quad := \quad \begin{cases} T_0 \Vdash I, C, h(K_b \oplus K_i) & S \text{ receives a request from } I \\ T_1 := T_0, S, I & S \text{ answers the request to } C \\ T_1 \Vdash C, I, h(K_i) & S \text{ receives the answer of } C \\ T_2 := T_1, S, C, K_b \oplus K_i \oplus K_i & S \text{ answers the request to } I \\ T_2 \Vdash K_b & \text{the secret } K_b \text{ is revealed} \end{cases}$$

Abstraction of Factors (I)

Idea

Abstraction ρ replaces all factors by new constant symbols to get a constraint system on signature:$\oplus$, h, and constant symbols.

Example:

$$\mathcal{C} \quad := \quad \left\{ \begin{array}{lll} a, b & \Vdash_{M_E} & \langle X, b \rangle \\ a, b, X & \Vdash_{M_E} & X \oplus b \end{array} \right.$$

$\mathcal{C}$ is well-defined, but not $\mathcal{C}\rho$

$$\mathcal{C}\rho \quad := \quad \left\{ \begin{array}{lll} a, b & \Vdash_{M_E} & c_1 \\ a, b, X & \Vdash_{M_E} & X \oplus b \end{array} \right.$$

Abstraction of Factors (II)

$\mathcal{C}$ is Factor-Preserving

Every non-variable factor appearing on the on right side of a constraint also appears on the left side of the same constraint.

Lemma

- Well-defined + non-collapsing solution $\Rightarrow$ Factor-Preserving.
- If $\mathcal{C}$ is W.D. and Factor-Preserving then $\mathcal{C}\rho$ is W.D.

Example:

$$\mathcal{C} := \begin{cases} a, b & \Vdash_{M_E} \quad X \oplus Y \\ a, b, \langle X \oplus Y, b \rangle & \Vdash_{M_E} \quad \langle X \oplus Y, b \rangle \oplus Z \end{cases}$$

$$\mathcal{C}\rho := \begin{cases} a, b & \Vdash_{M_E} \quad X \oplus Y \\ a, b, c_1 & \Vdash_{M_E} \quad c_1 \oplus Z \end{cases}$$

New Characterization of well-defined over $\{\oplus, h\}$

Example:

$$\begin{array}{lll} a, b & \Vdash_{\mathsf{M_E}} & u_1 = X_1 + X_2 + a \\ a, b, h(X_1) + h(X_2) & \Vdash_{\mathsf{M_E}} & u_2 = h(X_1) + h(b) \\ a, b, h(X_1) + h(X_2), h(X_2) & \Vdash_{\mathsf{M_E}} & u_3 = a + b \end{array}$$

We obtain

$$\begin{aligned} \vec{u_1} &= (1, 1) \\ \vec{u_2} &= (h, 0) \\ \vec{u_3} &= (0, 0) \end{aligned}$$

Basis $\mathcal{B} = \{\vec{u_1}, \vec{u_2}\}$

New Characterization of well-defined over $\{\oplus, h\}$

Example:

$$\begin{array}{lll} a, b & \Vdash_{\mathsf{M_E}} & u_1 = X_1 + X_2 + a \\ a, b, h(X_1) + h(X_2) & \Vdash_{\mathsf{M_E}} & u_2 = h(X_1) + h(b) \\ a, b, h(X_1) + h(X_2), h(X_2) & \Vdash_{\mathsf{M_E}} & u_3 = a + b \end{array}$$

We obtain

$$\begin{array}{rcl} \vec{u_1} & = & (1, 1) \\ \vec{u_2} & = & (h, 0) \\ \vec{u_3} & = & (0, 0) \end{array}$$

Basis $\mathcal{B} = \{\vec{u_1}, \vec{u_2}\}$

Characterization

Let $\mathcal{C} = \{t_1, \ldots, t_{n+i-1} \Vdash_{\mathsf{M_E}} u_i\}_{i=1,\ldots,k}$ on signature $\{\oplus, h\}$.
C is W.D. iff $\forall i \leq k, \{\vec{t}_{n+i-1}\} \cup \{\vec{u_j} \in \mathcal{B} \mid j < i\}$ are dependent.

New Characterization of well-defined over $\{\oplus, h\}$

Example:

$$\begin{array}{lll} a, b & \Vdash_{\mathsf{M_E}} & X_1 + X_2 + a \\ a, b, h(X_1) + h(X_2) & \Vdash_{\mathsf{M_E}} & h(X_1) + h(b) \\ a, b, h(X_1) + h(X_2), h(X_2) & \Vdash_{\mathsf{M_E}} & a + b \end{array}$$

$\vec{u_1} = (1, 1)$, $\vec{u_2} = (h, 0)$, $B = \{\vec{u_1}, \vec{u_2}\}$

Characterization

Let $\mathcal{C} = \{t_1, \ldots, t_{n+i-1} \Vdash_{\mathsf{M_E}} u_i\}_{i=1,\ldots,k}$ on signature $\{\oplus, h\}$.
C is W.D. iff $\forall i \leq k, \{\vec{t}_{n+i-1}\} \cup \{\vec{u_j} \in \mathcal{B} \mid j < i\}$ are dependent.

On the example:

$\{(h, h)\} \cup \{(1, 1)\}$ and $\{(0, h)\} \cup \{(1, 1), (h, 0)\}$ are dependent.

From M_E Constraints to Quadratic Equation Systems

Constraints M_E

$$
\begin{array}{lcl}
h(a) \oplus a, b \oplus h^2(a) & \vdash_{M_E} & h(X_1) \oplus h^2(X_2) \\
h(a) \oplus a, b \oplus h^2(a), X_1 \oplus h(X_2) & \vdash_{M_E} & X_1 \oplus a \\
h(a) \oplus a, b \oplus h^2(a), X_1 \oplus h(X_2), h(X_1) \oplus h(a) & \vdash_{M_E} & h(X_1) \oplus h^2(X_2) \oplus X_1 \oplus a
\end{array}
$$

NOTATION: $t_1 = h(a) \oplus a$ and $t_2 = b \oplus h^2(a)$.

System of equations

$$
\begin{array}{lcl}
z[1,1]t_1 \oplus z[1,2]t_2 & = & h(X_1) \oplus h^2(X_2) \\
z[2,1]t_1 \oplus z[2,2]t_2 \oplus z[2,3](X_1 \oplus h(X_2)) & = & X_1 \oplus a \\
z[3,1]t_1 \oplus z[3,2]t_2 \oplus z[3,3](X_1 \oplus h((X_2)) \oplus z[3,4](h(X_1) \oplus h(a)) & = & \\
 & & h(X_1) \oplus h^2(X_2) \oplus X_1 \oplus a
\end{array}
$$

Solvability of a quadratic system of equations is in general undecidable.

Solving Well-defined Quadratic Systems

Bound the Contexts of Well-defined Systems

If there exists a solution then there exists a solution where $z[i,j]$ are bounded by $Q_{max} = det(\vec{u_1}, \ldots, \vec{u_n})$ for Basis $\{\vec{u_1}, \ldots, \vec{u_n}\}$.

Example

$$Q_{max} = det(\vec{u}_1, \vec{u}_2) = det \begin{pmatrix} h & h^2 \\ 1 & 0 \end{pmatrix} = h^2.$$

$$\begin{aligned} z[1,1]t_1 \oplus z[1,2]t_2 &= h(X_1) \oplus h^2(X_2) \\ z[2,1]t_1 \oplus z[2,2]t_2 \oplus z[2,3](X_1 \oplus h(X_2)) &= X_1 \oplus a \end{aligned}$$

$\rho_1 = \{z[1,1] \mapsto 0; z[1,2] \mapsto h; z[2,1] \mapsto h \oplus 1; z[2,2] \mapsto 1; z[2,3] \mapsto 0\}.$

$$\begin{aligned} h \odot (b \oplus h^2(a)) &= h(X_1) \oplus h^2(X_2) \\ (h \oplus 1) \odot (h(a) \oplus a) \oplus 1 \odot (b \oplus h^2(a)) &= X_1 \oplus a \end{aligned}$$

$\theta = \{X_1 \mapsto b, X_2 \mapsto h(a)\}$.
Verify that θ satisfies the others constraints.

Outline

Our Procedure

Given: Deterministic protocol.

1. Guess order of execution $\Rightarrow$ constraint system (well-defined)
2. Guess partition of subterms $\Rightarrow$ one-step constraint system (well-defined)
3. Guess equality between subterms $\Rightarrow$ M_E constraint system (well-defined and factor-preserving)
4. Abstraction $\Rightarrow$ System of equations on $\mathbb{Z}/2\mathbb{Z}[h]$ (well-defined)
5. Solve system of equations $\Rightarrow$ Attack if solution

Overview

	Complexity		
	Unification Problem	**Intruder Deduction Problem**	**Security Problem**
ACUN	*NP-complete [Guo,Narendran98]*	*P-TIME [CS03]*	*NP-Complete [CKRT03]*
AG	*Decidable [Lankford84]*	*P-TIME [CS03]*	*Decidable [MS05]*
ACh	*Undecidable [Narendran96]*	*NP-Complete*	*Undecidable*
ACUNh	*NP-complete [Guo,Narendran98]*	*P-TIME*	*Decidable*
AGh	*Decidable [Baader93]*	*P-TIME*	*Undecidable*