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

Pascal Lafourcade
(with Stéphanie Delaune, Denis Lugiez & Ralf Treinen)

Venise Italy****

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

ICALP 10th July 2006

Symbolic approach

- Intruder controls the network
- Messages represented by terms
  - $\{m\}_k$
  - $\langle m_1, m_2 \rangle$
- Number of sessions bounded
- Perfect encryption hypothesis

Symbolic approach

- Intruder controls the network
- Messages represented by terms
  - $\{m\}_k$
  - $\langle m_1, m_2 \rangle$
- Number of sessions bounded
- Perfect encryption hypothesis

Advantages

- Automatic verification
- Useful abstraction

Symbolic approach

- Intruder controls the network
- Messages represented by terms
  - $\{m\}_k$
  - $\langle m_1, m_2 \rangle$
- Number of sessions bounded
- Perfect encryption hypothesis $+$ algebraic properties

Advantages

- Automatic verification
- Useful abstraction

TMN Protocol: Distribution of a fresh symmetric key

[Tatebayashi, Matsuzuki, Newmann 89]:

A		S		W		
	$\rightarrow$				:	$A, W, \{N_A\}_{Pub_S}$
			$\rightarrow$		:	S, A
			$\leftarrow$		:	$W, A, \{N_W\}_{Pub_S}$
	$\leftarrow$				:	$S, W, N_A \oplus N_W$

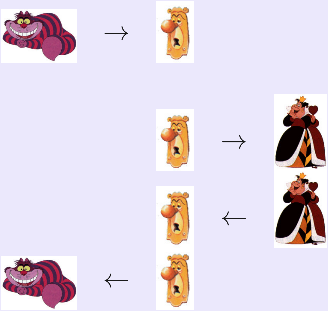
Alice retrieves N_W:

Using $x \oplus x = 0$ and $x \oplus 0 = x$, knowing N_A

Attack on TMN Protocol [Simmons 89]

With homomorphic encryption $\{a\}_k \oplus \{b\}_k = \{a \oplus b\}_k$

$C \quad S \quad Q$



$$C \rightarrow S \;:\; C, Q, \underbrace{\{N_W\}_{Pub_S} \oplus \{N_C\}_{Pub_S}}_{\{N_W \oplus N_C\}_{Pub_S}}$$

$$S \rightarrow Q \;:\; S, C$$

$$S \leftarrow Q \;:\; Q, C, \{N_Q\}_{Pub_S}$$

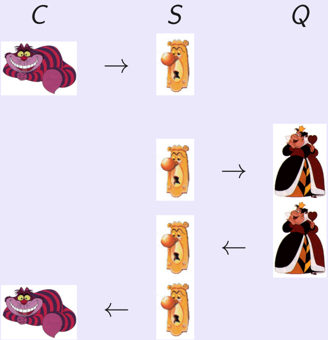
$$C \leftarrow S \;:\; S, (N_W \oplus N_C) \oplus N_Q$$

Cheshire Learns: N_W

Using $x \oplus x = 0$ and $x \oplus 0 = x$, knowing N_C and N_Q

Attack on TMN Protocol [Simmons 89]

With homomorphic function $h(a) \oplus h(b) = h(a \oplus b)$



$C \rightarrow S$: $C, Q, \underbrace{h(N_W) \oplus h(N_C)}_{h(N_W \oplus N_C)}$

$S \rightarrow Q$: S, C

$S \leftarrow Q$: $Q, C, h(N_Q)$

$C \leftarrow S$: $S, (N_W \oplus N_C) \oplus N_Q$

Cheshire Learns: N_W

Using $x \oplus x = 0$ and $x \oplus 0 = x$, knowing N_C and N_Q

Deduction System: Extended Dolev-Yao

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

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

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

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

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

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

(M_E) $\dfrac{T \vdash u_1 \quad \cdots \quad T \vdash u_n}{T \vdash C[u_1, \dots, u_n]\downarrow}$ C is an context made with $\{h, \oplus\}$

Example for M_E

T $\vdash a \oplus h(a)$ $\;T \vdash b T \vdash a \oplus h^2(a) \oplus h(b)$
$C[u_1, u_2] = u_1 \oplus h(u_1) \oplus h(u_2)$

Passive Intruder with homomorphisme and Xor

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

A minimal proof P of $T \vdash u$ contains only computable terms.

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 $\mathbb{Z}/2\mathbb{Z}[h]$

Some Results to Active Intruder

XOR : ACUN [Rusinowitch & al 03] [Comon-Shmatikov 03]

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

Abelian Group and Exponential : AG [Millen-Shmatikov 05]

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

Our contribution

Homomorphism over XOR : ACUNh

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

Theorem

The security problem with a bounded number of sessions is decidable with ACUNh.

Outline

Outline

Modelisation of a protocol in a system of constraint

The Intruder is the network, he can listen, built, send and replay messages.

$$\mathcal{P} \quad := \quad \begin{cases} recv(u_1); send(v_1) \\ recv(u_2); send(v_2) \\ \qquad \vdots \\ recv(u_n); send(v_n) \end{cases}$$

T_0 Intruder initial knowledge.

$$\mathcal{C} \quad := \quad \begin{cases} T_0 & \Vdash & u_1 \\ T_0, v_1 & \Vdash & u_2 \\ & \vdots & \\ T_0, v_1, \ldots, v_n & \Vdash & s \end{cases}$$

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

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:

$$x \in vars(T_i) \Rightarrow \exists j < i \text{ such that } : x \in vars(u_j)$$

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

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

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:

$$x \in vars(T_i) \Rightarrow \exists j < i \text{ such that } : x \in vars(u_j)$$

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

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

Well-Definedness: Example

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

Monotonicity OK !

Well-Definedness: Example

$$\mathcal{C} \quad := \quad \begin{cases} T_0 & \Vdash \quad X \oplus Y \\ T_0, X & \Vdash \quad c \end{cases}$$

Monotonicity OK !

Origination OK !

Well-Definedness: Example

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

Monotonicity OK !

Origination OK !

But NOT well-defined !

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

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

Outline

Outline of our Procedure

Let $\mathcal{C}$ a W-D constraints system

1. From W-D $\Vdash$ to W-D $\Vdash_1$
2. From W-D $\Vdash_1$ to W-D $\Vdash_{M_E}$
3. From W-D $\Vdash_{M_E}$ to W-D equations systems
4. Solve these W-D equations systems

From W-D $\Vdash$ to W-D $\Vdash_1$

Example

$$\mathcal{C} \quad := \quad \left\{ \begin{array}{lll} T & \Vdash & \langle X, h(Y) \rangle \\ T, X & \Vdash & \{Z\}_K \end{array} \right.$$

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

$S_0 = \{X, h(Y), \langle X, h(Y) \rangle\}$

$$\mathcal{C}' \quad := \quad \left\{ \begin{array}{lll} T & \Vdash_1 & X \\ T, X & \Vdash_1 & h(Y) \\ T, X, h(Y) & \Vdash_1 & \langle X, h(Y) \rangle \\ T, S_0 & \Vdash_1 & Z \\ T, S_0, Z & \Vdash_1 & K \\ T, S_0, Z, K & \Vdash_1 & \{Z\}_K \end{array} \right.$$

From W-D $\Vdash$ to W-D $\Vdash_1$

Example

$$\mathcal{C} \quad := \quad \left\{ \begin{array}{lll} T & \Vdash & \langle X, h(Y) \rangle \\ T, X & \Vdash & \{Z\}_K \end{array} \right.$$

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

$S_0 = \{X, h(Y), \langle X, h(Y) \rangle\}$

$$\mathcal{C}' \quad := \quad \left\{ \begin{array}{lll} T & \Vdash_1 & X \\ T, X & \Vdash_1 & h(Y) \\ T, X, h(Y) & \Vdash_1 & \langle X, h(Y) \rangle \\ T, S_0 & \Vdash_1 & Z \\ T, S_0, Z & \Vdash_1 & K \\ T, S_0, Z, K & \Vdash_1 & \{Z\}_K \end{array} \right.$$

From W-D $\Vdash_1$ to W-D $\Vdash_{M_E}$

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

Example

$$\mathcal{C} \quad := \quad \begin{cases} \langle a, b\rangle & \Vdash_1 \quad \langle X, b\rangle \\ \langle a, b\rangle, X \oplus b & \Vdash_1 \quad Y \oplus \langle a, b\rangle a \end{cases}$$

Guess $\{\langle X, b\rangle = \langle a, b\rangle\}$, compute ACUNh m.g.u. $\theta : \{X \mapsto a\}$ [UNIF'06]

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

From W-D $\Vdash_{M_E}$ to W-D equations system (I)

Idea

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

Example:

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

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

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

From W-D $\Vdash_{M_E}$ to W-D equations system (II)

Lemma

Restriction to systems where abstraction preserves Well-Definedness is sufficent for completeness.

Example:

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

$\mathcal{C}$ and $\mathcal{C}\rho$ are well-defined.

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

Constraint M_E to Quadratic Equations System

System $\mathcal{C}$ of Constraints M_E

$$\mathcal{C} \quad := \quad \left\{ \begin{array}{lll} t_1, t_2 & \Vdash_{\mathrm{M_E}} & h(X_1) \oplus X_2 \\ t_1, t_2, X_1 \oplus X_2 & \Vdash_{\mathrm{M_E}} & X_1 \oplus a \\ t_1, t_2, X_1 \oplus X_2, X_1 & \Vdash_{\mathrm{M_E}} & X_2 \oplus b \end{array} \right.$$

System of equations $\mathcal{E}$

$$\mathcal{E} \quad := \quad \left\{ \begin{array}{lll} z[1,1]t_1 \oplus z[1,2]t_2 & = & h(X_1) \oplus X_2 \\ z[2,1]t_1 \oplus z[2,2]t_2 \oplus z[2,3](X_1 \oplus X_2) & = & X_1 \oplus a \\ z[3,1]t_1 \oplus z[3,2]t_2 \oplus z[3,3](X_1 \oplus X_2) \oplus z[3,4]X_1 & = & X_2 \oplus b \end{array} \right.$$

Solve Quadratic system of equation is in general undecidable.

Constraint M_E to Quadratic Equations System

System $\mathcal{C}$ of Constraints M_E

$$\mathcal{C} \quad := \quad \left\{ \begin{array}{lll} t_1, t_2 & \Vdash_{\mathrm{M_E}} & h(X_1) \oplus X_2 \\ t_1, t_2, X_1 \oplus X_2 & \Vdash_{\mathrm{M_E}} & X_1 \oplus a \\ t_1, t_2, X_1 \oplus X_2, X_1 & \Vdash_{\mathrm{M_E}} & X_2 \oplus b \end{array} \right.$$

System of equations $\mathcal{E}$

$$\mathcal{E} \quad := \quad \left\{ \begin{array}{lll} z[1,1]t_1 \oplus z[1,2]t_2 & = & h(X_1) \oplus X_2 \\ z[2,1]t_1 \oplus z[2,2]t_2 \oplus z[2,3](X_1 \oplus X_2) & = & X_1 \oplus a \\ z[3,1]t_1 \oplus z[3,2]t_2 \oplus z[3,3](X_1 \oplus X_2) \oplus z[3,4]X_1 & = & X_2 \oplus b \end{array} \right.$$

Solve Quadratic system of equation is in general undecidable.

We propose a procedure to solve Well-defined Quadratic system of equation.

Outline

Our Procedure

Theorem

The security problem with a bounded number of sessions is decidable with ACUNh.

Given: Well-defined protocol.

1. From W-D $\Vdash$ to W-D $\Vdash_1$
2. From W-D $\Vdash_1$ to W-D $\Vdash_{M_E}$
3. From W-D $\Vdash_{M_E}$ to W-D equations systems
4. Solve these W-D equations systems

Results & Future Works

	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* [LLT'05]	*Undecidable*
ACUNh	*NP-complete [Guo,Narendran98]*	*P-TIME* [Del06]	*Decidable*
AGh	*Decidable [Baader93]*	*P-TIME* [Del06]	*Undecidable* [Del06]

Future works : $\{x \oplus y\}_k = \{x\}_k \oplus \{y\}_k$

Thank you for your attention

Questions ?