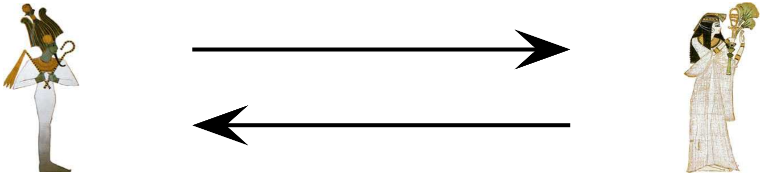
Vérification de protocoles cryptographiques en présence de théories équationnelles

Pascal Lafourcade

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

Cachan : September 25th 2006

Cryptographic Protocols



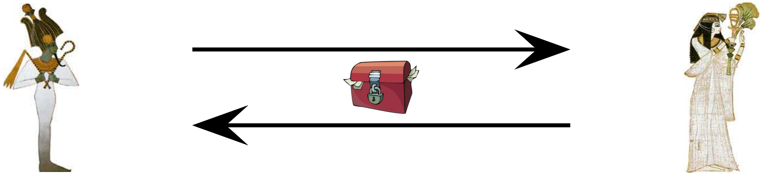
Osiris communicates with Isis via the net.

Cryptographic Protocols

Intruder

Osiris communicates with Isis via the net.

Cryptographic Protocols

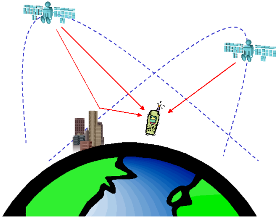


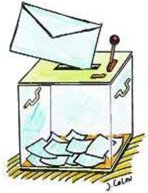
Intruder

Osiris communicates with Isis via the net.

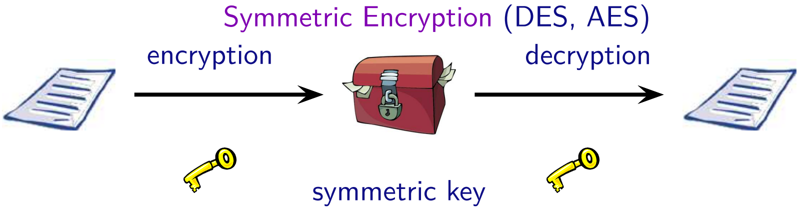
Secrecy Property: Intruder cannot learn a *secret data.*

Applications

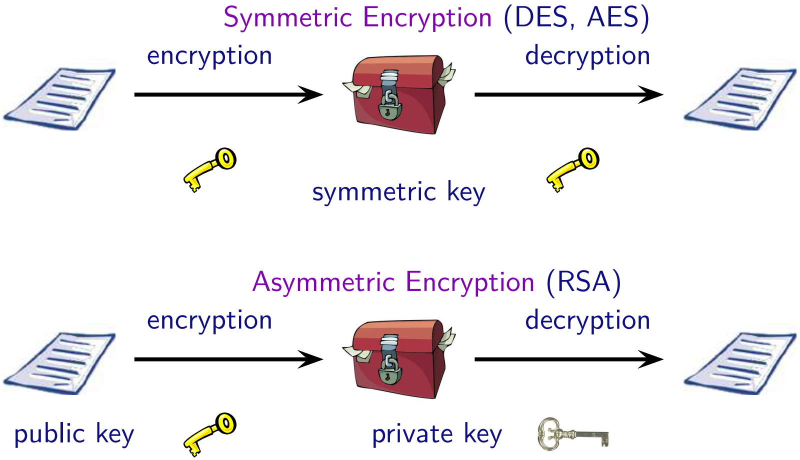




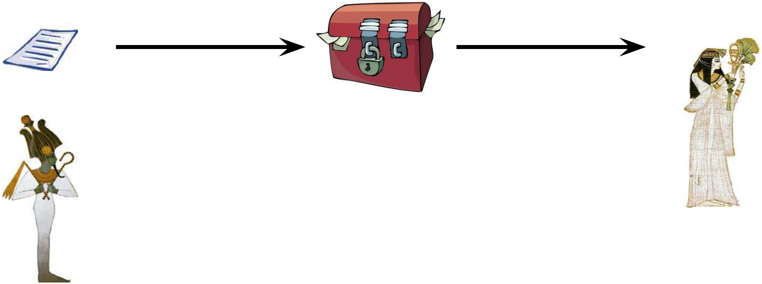
Cryptography



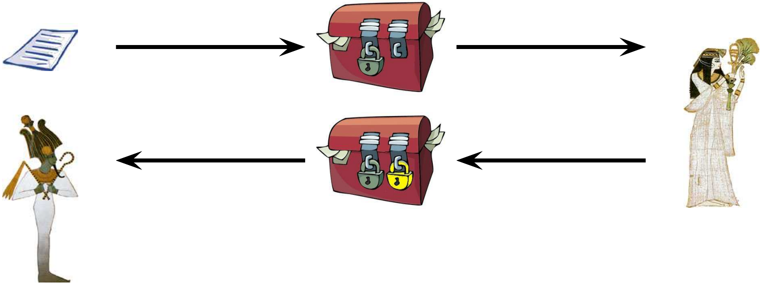
Cryptography



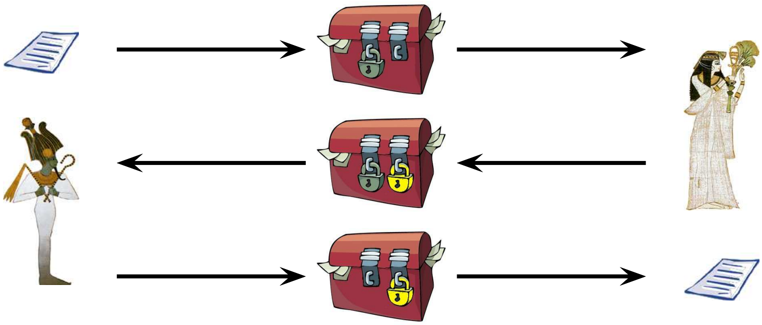
Example :



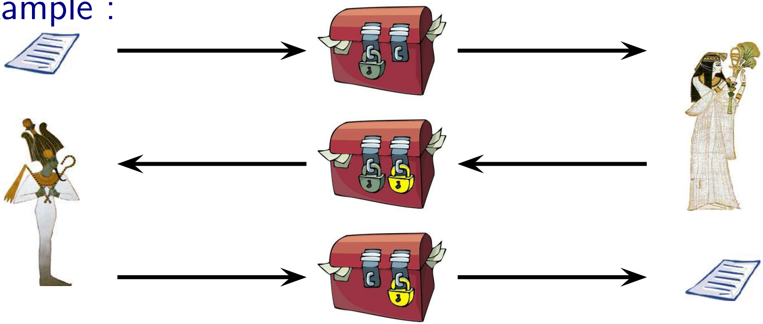
Example :



Example :



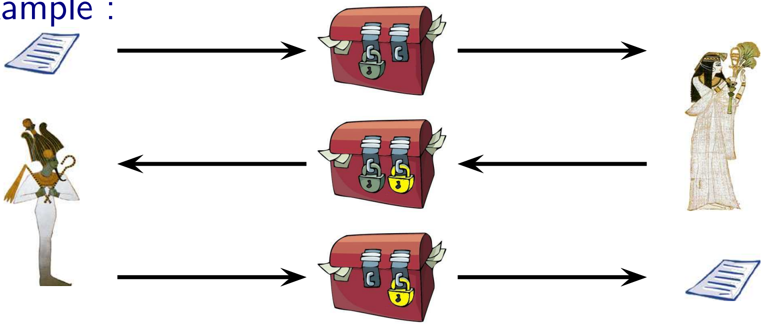
Example :



Shamir 3-Pass Protocol

$$1 \quad O \quad \rightarrow \quad I \quad : \quad \{m\}_{K_O}$$

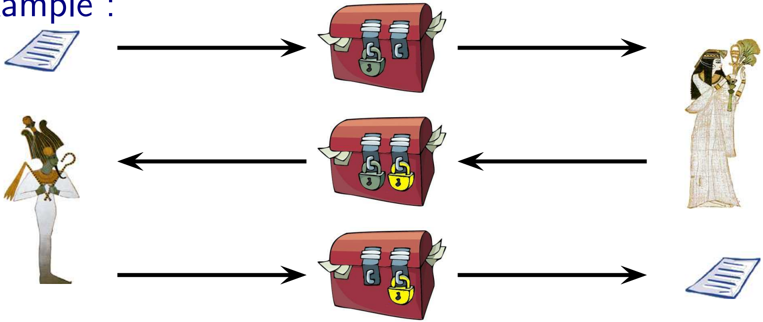
Example :



Shamir 3-Pass Protocol

$$\begin{array}{llcll} 1 & O & \to & I & : \{m\}_{K_O} \\ 2 & I & \to & O & : \{\{m\}_{K_O}\}_{K_I} \end{array}$$

Example :

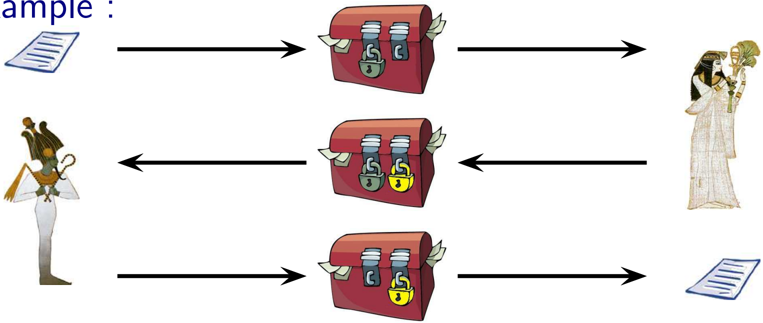


Shamir 3-Pass Protocol

$$\begin{array}{lllll} 1 & O & \rightarrow & I & : \{m\}_{K_O} \\ 2 & I & \rightarrow & O & : \{\{m\}_{K_O}\}_{K_I} = \{\{m\}_{K_I}\}_{K_O} \end{array}$$

Commutative Encryption

Example :



Shamir 3-Pass Protocol

$$\begin{array}{llcll} 1 & O & \rightarrow & I & : \{m\}_{K_O} \\ 2 & I & \rightarrow & O & : \{\{m\}_{K_O}\}_{K_I} = \{\{m\}_{K_I}\}_{K_O} \\ 3 & O & \rightarrow & I & : \{m\}_{K_I} \end{array}$$

Commutative Encryption

Attacks

Cryptanalysis

Attacks

Cryptanalysis





Attacks

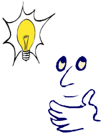
Cryptanalysis

Logical Attack

Perfect Encryption hypothesis

Needham-Schroeder Public Key Protocol (1978)

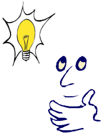
“Man in the middle attack” [Lowe’96]



Attacks

Cryptanalysis

Logical Attack + Algebraic properties



Perfect Encryption hypothesis

Needham-Schroeder Public Key Protocol (1978)

"Man in the middle attack" [Lowe'96]

Formal Approach

Symbolic abstraction

- Messages represented by terms
  - $\{m\}_k$
  - $\langle m_1, m_2 \rangle$
- Perfect encryption hypothesis

Formal Approach

Symbolic abstraction

- Messages represented by terms
  - $\{m\}_k$
  - $\langle m_1, m_2 \rangle$
- Perfect encryption hypothesis

Useful abstraction [Clark & Jacob'97]

Automatic verification with Tools:
AVISPA, Casper/FDR, Hermes, Murphi, NRL, Proverif, Scyther ...

Formal Approach

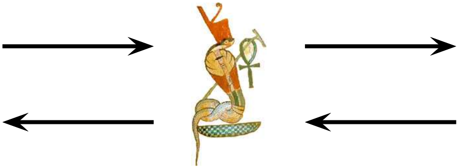
Symbolic abstraction

- Messages represented by terms
  - $\{m\}_k$
  - $\langle m_1, m_2 \rangle$
- Perfect encryption hypothesis $+$ algebraic properties

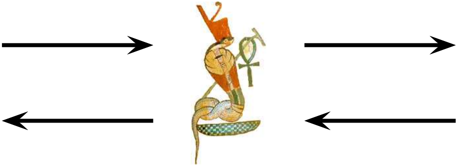
Useful abstraction [Clark & Jacob'97]

Automatic verification with Tools:
AVISPA, Casper/FDR, Hermes, Murphi, NRL, Proverif, Scyther ...

The Intruder is the Network (Worst Case)



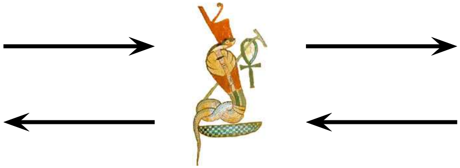
The Intruder is the Network (Worst Case)



Listen

Passive: Intruder deduction problem

The Intruder is the Network (Worst Case)



Listen

Intercept message

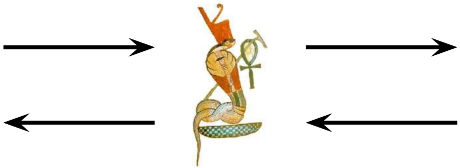
(Re)play message

Delete message

Passive: Intruder deduction problem

Active: Security problem

The Intruder is the Network (Worst Case)



Listen

Intercept message

(Re)play message

Delete message

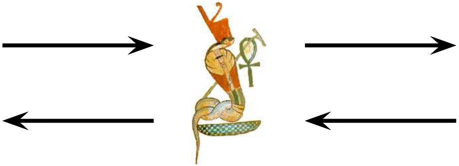
Passive: Intruder deduction problem

Active: Security problem

Intruder Capabilities (Dolev-Yao Model 80's)

- Encryption, Decryption with a key
- Pairing, Projection.

The Intruder is the Network (Worst Case)



Listen

Intercept message

(Re)play message

Delete message

Passive: Intruder deduction problem

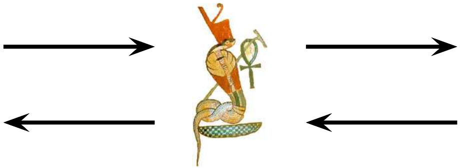
Active: Security problem

Intruder Capabilities (Dolev-Yao Model 80's)

- Encryption, Decryption with a key
- Pairing, Projection.

In general security problem undecidable [DLMS'99, AC'01]

The Intruder is the Network (Worst Case)



Listen

Intercept message

(Re)play message

Delete message

Passive: Intruder deduction problem

Active: Security problem

Intruder Capabilities (Dolev-Yao Model 80's)

- Encryption, Decryption with a key
- Pairing, Projection.

In general security problem undecidable [DLMS'99, AC'01]

Bounded number of session $\Rightarrow$ Decidability [AL'00, RT'01]

Logical Attack on Shamir 3-Pass Protocol (I)

Perfect encryption one-time pad (Vernam Encryption)

$\{m\}_k = m \oplus k$

XOR Properties (ACUN)

- $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ **A**ssociativity
- $x \oplus y = y \oplus x$ **C**ommutativity
- $x \oplus 0 = x$ **U**nity
- $x \oplus x = 0$ **N**ilpotency

Logical Attack on Shamir 3-Pass Protocol (I)

Perfect encryption one-time pad (Vernam Encryption)

$\{m\}_k = m \oplus k$

XOR Properties (ACUN)

- $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ — **A**ssociativity
- $x \oplus y = y \oplus x$ — **C**ommutativity
- $x \oplus 0 = x$ — **U**nity
- $x \oplus x = 0$ — **N**ilpotency

Vernam encryption is a commutative encryption :

$$\{\{m\}_{K_O}\}_{K_I} = (m \oplus K_O) \oplus K_I = (m \oplus K_I) \oplus K_O = \{\{m\}_{K_I}\}_{K_O}$$

Logical Attack on Shamir 3-Pass Protocol (II)

Perfect encryption one-time pad (Vernam Encryption)

$\{m\}_k = m \oplus k$

Shamir 3-Pass Protocol

$$\begin{array}{lllll} 1 & O & \rightarrow & I: & m \oplus K_O \\ 2 & I & \rightarrow & O: & (m \oplus K_O) \oplus K_I \\ 3 & O & \rightarrow & I: & m \oplus K_I \end{array}$$

Passive attacker :

$$m \oplus K_O \qquad m \oplus K_O \oplus K_I \qquad m \oplus K_I$$

Logical Attack on Shamir 3-Pass Protocol (II)

Perfect encryption one-time pad (Vernam Encryption)

$\{m\}_k = m \oplus k$

Shamir 3-Pass Protocol

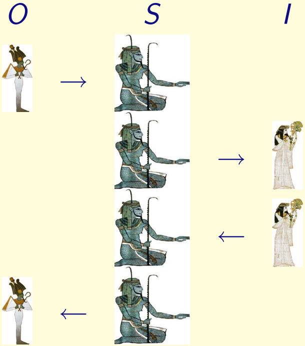
$$\begin{array}{llcll} 1 & O & \rightarrow & I: & m \oplus K_O \\ 2 & I & \rightarrow & O: & (m \oplus K_O) \oplus K_I \\ 3 & O & \rightarrow & I: & m \oplus K_I \end{array}$$

Passive attacker :

$$m \oplus K_O \oplus m \oplus K_O \oplus K_I \oplus m \oplus K_I = m$$

TMN Protocol: Distribution of a fresh symmetric key

[Tatebayashi, Matsuzuki, Newmann 89]:



$O \rightarrow S$: $O, I, \{N_O\}_{Pub_S}$

$S \rightarrow I$: S, O

$S \leftarrow I$: $I, O, \{N_I\}_{Pub_S}$

$O \leftarrow S$: $S, I, N_O \oplus N_I$

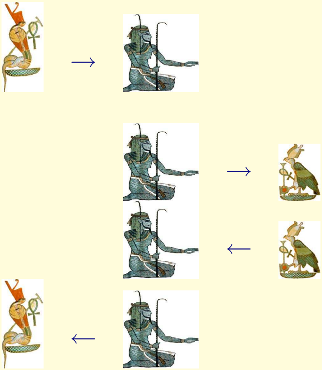
Osiris retrieves N_I:

Using $x \oplus x \oplus y = y$, knowing N_O

Attack on TMN Protocol [Simmons'94]

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

B $\quad$ S $\quad$ C



$B \rightarrow S$: $B, C, \underbrace{\{N_I\}_{Pub_S} \oplus \{N_B\}_{Pub_S}}_{\{N_I \oplus N_B\}_{Pub_S}}$

$S \rightarrow C$: S, B

$S \leftarrow C$: $C, B, \{N_C\}_{Pub_S}$

$B \leftarrow S$: $S, (N_I \oplus N_B) \oplus N_C$

Buto Learns:

Using $x \oplus x \oplus y = y$, knowing N_B and N_C, he deduces N_I.

Relaxing the perfect encryption hypothesis.

[Journal of Computer Security'06]

	Examples of Protocols	Intruder Deduction Problem	Security Problem
Commutative encryption	Shamir	*P-TIME [CKRT'04]*	*NP-Complete [CKRT'04]*
ACUN	Bull, Gong	*P-TIME [CS'03,CKRT'03]*	*NP-Complete [CS03,CKRT'03]*
AG + Exp	IKA.1	*P-TIME [CKRTV'03]*	*Decidable [MS'03]*
ACUNh	WEP	*?*	*?*
AGh	TMN	*?*	*?*

Combination Result [CR'06]

My contributions : Homomorphism property

Passive Intruder

- $h(x \oplus y) = h(x) \oplus h(y)$ [RTA'05]
  - ACh
  - ACUNh
  - AGh
- $\{x \oplus y\}_k = \{x\}_k \oplus \{y\}_k$
  - Distributive Encryption [I&C] Submitted (ACUN$\{.\}_.$, AG$\{.\}_.$)
  - Distributive and Commutative Encryption [Secret'06] $\{\{m\}_{k_1}\}_{k_2} = \{\{m\}_{k_2}\}_{k_1}$

Active Intruder [ICALP'05]

- ACUNh

Outline

Outline

Extended Dolev-Yao Deduction System

Deduction System : $T_0 \vdash^? s$

(A) $\dfrac{u \in T_0}{T_0 \vdash u}$

(UL) $\dfrac{T_0 \vdash \langle u, v\rangle}{T_0 \vdash u}$

(P) $\dfrac{T_0 \vdash u \qquad T_0 \vdash v}{T_0 \vdash \langle u, v\rangle}$

(UR) $\dfrac{T_0 \vdash \langle u, v\rangle}{T_0 \vdash v}$

(C) $\dfrac{T_0 \vdash u \qquad T_0 \vdash v}{T_0 \vdash \{u\}_v}$

(D) $\dfrac{T_0 \vdash \{u\}_v \qquad T_0 \vdash v}{T_0 \vdash u}$

(F) $\dfrac{T_0 \vdash u_1 \quad \cdots \quad T_0 \vdash u_n}{T_0 \vdash f(u_1, \ldots, u_n)}$

$$(Eq)\dfrac{T_0 \vdash u \qquad u =_E v}{T_0 \vdash v}$$

Extended Dolev-Yao Deduction System

Deduction System : $T_0 \vdash^? s$

(A) $\dfrac{u \in T_0}{T_0 \vdash u}$

(UL) $\dfrac{T_0 \vdash \langle u, v\rangle}{T_0 \vdash u}$

(P) $\dfrac{T_0 \vdash u \qquad T_0 \vdash v}{T_0 \vdash \langle u, v\rangle}$

(UR) $\dfrac{T_0 \vdash \langle u, v\rangle}{T_0 \vdash v}$

(C) $\dfrac{T_0 \vdash u \qquad T_0 \vdash v}{T_0 \vdash \{u\}_v}$

(D) $\dfrac{T_0 \vdash \{u\}_v \qquad T_0 \vdash v}{T_0 \vdash u}$

(F) $\dfrac{T_0 \vdash u_1 \quad \cdots \quad T_0 \vdash u_n}{T_0 \vdash f(u_1, \ldots, u_n)}$

$$(Eq)\frac{T_0 \vdash u \qquad u =_E v}{T_0 \vdash v}$$

E is represented by a confluent and terminating rewriting system modulo AC ↓

Extended Dolev-Yao Deduction System

Deduction System : $T_0 \vdash^? s$

(A) $\dfrac{u \in T_0}{T_0 \vdash u\downarrow}$

(UL) $\dfrac{T_0 \vdash \langle u, v\rangle}{T_0 \vdash u\downarrow}$

(P) $\dfrac{T_0 \vdash u \qquad T_0 \vdash v}{T_0 \vdash \langle u, v\rangle\downarrow}$

(UR) $\dfrac{T_0 \vdash \langle u, v\rangle}{T_0 \vdash v\downarrow}$

(C) $\dfrac{T_0 \vdash u \qquad T_0 \vdash v}{T_0 \vdash \{u\}_v\downarrow}$

(D) $\dfrac{T_0 \vdash \{u\}_v \qquad T_0 \vdash v}{T_0 \vdash u\downarrow}$

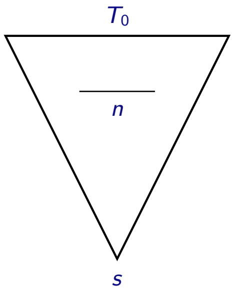
(F) $\dfrac{T_0 \vdash u_1 \quad \cdots \quad T_0 \vdash u_n}{T_0 \vdash f(u_1, \ldots, u_n)\downarrow}$

E is represented by a confluent and terminating rewriting system modulo AC $\downarrow$

Definition of S-Locality

- A proof P of $T_0 \vdash s$ is S-local :

$$\forall n \in P, n \in S(T_0 \cup \{s\})$$



Extended McAllester's Theorem

Let P be a proof system, if:

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

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

Intruder Deduction problem [RTA'05]

Dolev-Yao Model extended by:

$$(GX)\frac{T_0 \vdash_E u_1 \qquad \ldots \qquad T_0 \vdash_E u_n}{T_0 \vdash_E (u_1 \oplus \ldots \oplus u_n)\downarrow} \quad (h)\frac{T_0 \vdash_E u}{T_0 \vdash_E h(u)\downarrow}$$

NP-Complete ACh

- One-step deducibility ($\mathbb{N}$)
- Syntactic Subterms (P-TIME) and locality: easy

EXP-TIME ACUNh, AGh

- One-step deducibility: easy ($\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}$)
- Design S (EXP-TIME) and prove locality: difficult

Intruder Deduction problem [RTA'05]

Dolev-Yao Model extended by:

$$(GX)\frac{T_0 \vdash_E u_1 \qquad \ldots \qquad T_0 \vdash_E u_n}{T_0 \vdash_E (u_1 \oplus \ldots \oplus u_n)\downarrow} \quad (h)\frac{T_0 \vdash_E u}{T_0 \vdash_E h(u)\downarrow}$$

NP-Complete ACh

- One-step deducibility ($\mathbb{N}$)
- Syntactic Subterms (P-TIME) and locality: easy

EXP-TIME ACUNh, AGh

- One-step deducibility: easy ($\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}$)
- Design S (EXP-TIME) and prove locality: difficult

P-TIME Complete [Delaune'06] ACUNh, AGh

Distributive Encryption : ACUN$\{.\}_.$, AG$\{.\}_.$

$$\{x \oplus y\}_k = \{x\}_k \oplus \{y\}_k$$

Example

$T_0 = \{a \oplus \{b\}_k, \{b\}_k \oplus c, \{c\}_k \oplus d, k\}$ and $s = \{a\}_k \oplus d$
$S(T_0 \cup \{s\}) = T_0 \cup \{s, a, b, c, d, k, \{a\}_k, \{b\}_k, \{c\}_k\}$

Distributive Encryption : ACUN$\{.\}_.$, AG$\{.\}_.$

$$\{x \oplus y\}_k = \{x\}_k \oplus \{y\}_k$$

Example

$T_0 = \{a \oplus \{b\}_k, \{b\}_k \oplus c, \{c\}_k \oplus d, k\}$ and $s = \{a\}_k \oplus d$
$S(T_0 \cup \{s\}) = T_0 \cup \{s, a, b, c, d, k, \{a\}_k, \{b\}_k, \{c\}_k\}$

$$(GX)\dfrac{(C)\dfrac{a \oplus \{b\}_k \quad k}{\{a\}_k \oplus \{\{b\}_k\}_k} \qquad (C)\dfrac{\{b\}_k \oplus c \quad k}{\{\{b\}_k\}_k \oplus \{c\}_k} \qquad \{c\}_k \oplus d}{\{a\}_k \oplus d}$$

Distributive Encryption : ACUN$\{.\}_.$, AG$\{.\}_.$

$$\{x \oplus y\}_k = \{x\}_k \oplus \{y\}_k$$

Example

$T_0 = \{a \oplus \{b\}_k, \{b\}_k \oplus c, \{c\}_k \oplus d, k\}$ and $s = \{a\}_k \oplus d$
$S(T_0 \cup \{s\}) = T_0 \cup \{s, a, b, c, d, k, \{a\}_k, \{b\}_k, \{c\}_k\}$

$$(GX)\frac{(C)\dfrac{a \oplus \{b\}_k \quad k}{\{a\}_k \oplus \{\{b\}_k\}_k} \qquad (C)\dfrac{\{b\}_k \oplus c \quad k}{\{\{b\}_k\}_k \oplus \{c\}_k} \qquad \{c\}_k \oplus d}{\{a\}_k \oplus d}$$

Distributive Encryption : ACUN$\{.\}_.$, AG$\{.\}_.$

$$\{x \oplus y\}_k = \{x\}_k \oplus \{y\}_k$$

Example

$T_0 = \{a \oplus \{b\}_k, \{b\}_k \oplus c, \{c\}_k \oplus d, k\}$ and $s = \{a\}_k \oplus d$
$S(T_0 \cup \{s\}) = T_0 \cup \{s, a, b, c, d, k, \{a\}_k, \{b\}_k, \{c\}_k\}$

$$(GX)\frac{(C)\dfrac{a \oplus \{b\}_k \quad k}{\{a\}_k \oplus \{\{b\}_k\}_k} \qquad (C)\dfrac{\{b\}_k \oplus c \quad k}{\{\{b\}_k\}_k \oplus \{c\}_k} \qquad \{c\}_k \oplus d}{\{a\}_k \oplus d}$$

$$\Downarrow$$

$$(GX)\frac{(C)\dfrac{(GX)\dfrac{a \oplus \{b\}_k \qquad \{b\}_k \oplus c}{a \oplus c} \qquad k}{\{a\}_k \oplus \{c\}_k} \qquad \{c\}_k \oplus d}{\{a\}_k \oplus d}$$

Intruder Deduction Problem

ACUN$\{.\}_.$

- Atomic Locality Result
- EXP-TIME decision procedure

AG$\{.\}_.$

- Atomic Locality Result & $\mathbb{Z}$-module
- EXP-TIME decision procedure

Intruder Deduction Problem

ACUN$\{.\}_.$

- Atomic Locality Result
- EXP-TIME decision procedure

AG$\{.\}_.$

- Atomic Locality Result & $\mathbb{Z}$-module
- EXP-TIME decision procedure

Binary Case

$\forall n \in P, n = .$ or $n = . \oplus .$ but $\cancel{n = . \oplus . \oplus \ldots \oplus .}$

- AG$\{.\}_.$ P-TIME (prefix rewriting)

Intruder Deduction Problem

ACUN$\{.\}_.$ and Commutative Encryption

- Atomic Locality Result
- 2-EXP-TIME decision procedure

AG$\{.\}_.$ and Commutative Encryption

- Atomic Locality Result & $\mathbb{Z}$-module
- 2-EXP-TIME decision procedure

Binary Case

$\forall n \in P, n = .$ or $n = . \oplus .$ but $\cancel{n = . \oplus . \oplus \ldots \oplus .}$

- AG$\{.\}_.$ P-TIME (prefix rewriting)
- ACUN$\{.\}_.$ and Commutative Encryption EXP-SPACE hard

Outline

New Extended Dolev-Yao Deduction System

Deduction System : $T_0 \vdash^? s$

(A) $$\frac{u \in T_0}{T_0 \vdash u}$$

(UL) $$\frac{T_0 \vdash \langle u, v \rangle}{T_0 \vdash u}$$

(P) $$\frac{T_0 \vdash u \qquad T_0 \vdash v}{T_0 \vdash \langle u, v \rangle}$$

(UR) $$\frac{T_0 \vdash \langle u, v \rangle}{T_0 \vdash v}$$

(C) $$\frac{T_0 \vdash u \qquad T_0 \vdash v}{T_0 \vdash \{u\}_v}$$

(D) $$\frac{T_0 \vdash \{u\}_v \qquad T_0 \vdash v}{T_0 \vdash u}$$

(M_E) $$\frac{T_0 \vdash u_1 \quad \cdots \quad T_0 \vdash u_n}{T_0 \vdash C[u_1, \ldots, u_n]}$$ C is a context made with $\{h, \oplus\}$

New Extended Dolev-Yao Deduction System

Deduction System : $T_0 \vdash^? s$

(A) $\dfrac{u \in T_0}{T_0 \vdash u}$

(UL) $\dfrac{T_0 \vdash \langle u, v \rangle}{T_0 \vdash u}$

(P) $\dfrac{T_0 \vdash u \qquad T_0 \vdash v}{T_0 \vdash \langle u, v \rangle}$

(UR) $\dfrac{T_0 \vdash \langle u, v \rangle}{T_0 \vdash v}$

(C) $\dfrac{T_0 \vdash u \qquad T_0 \vdash v}{T_0 \vdash \{u\}_v}$

(D) $\dfrac{T_0 \vdash \{u\}_v \qquad T_0 \vdash v}{T_0 \vdash u}$

(M_E) $\dfrac{T_0 \vdash u_1 \quad \cdots \quad T_0 \vdash u_n}{T_0 \vdash C[u_1, \ldots, u_n]}$ C is a context made with $\{h, \oplus\}$

Example

$$\dfrac{T_0 \vdash a \oplus h(a) \quad T_0 \vdash b}{T_0 \vdash a \oplus h^2(a) \oplus h(b)}$$

$C[u_1, u_2] = (h \oplus 1)(u_1) \oplus h(u_2)$

$a \oplus h(a) \quad \oplus \quad h(a \oplus h(a)) \quad \oplus \quad h(b)$

Modeling a protocol as a system of constraints

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

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

T_0 initial Intruder knowledge.

$$\mathcal{C} \quad := \quad \begin{cases} T_0 & \Vdash & u_1 \\ T_0, v_1 & \Vdash & u_2 \\ T_0, v_1, v_2 & \Vdash & u_3 \\ & \vdots & \\ T_0, v_1, \ldots, v_n & \Vdash & s \end{cases}$$

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

System of Constraints Well-formed [MS'03]

$\mathcal{C} = \{T_i \Vdash u_i\}_{1 \le i \le k}$ 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 [MS'03]

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

System of Constraints Well-formed [MS'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 [MS'03]

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

Well-Definedness: Example

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

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 !

Well-Definedness: Example

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

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 !

Well-formed 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 !

Well-formed OK !

But NOT well-defined !

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

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

Our Procedure

Theorem [ICALP'06]

The security problem modulo ACUNh with a bounded number of sessions is decidable for deterministic protocols.

Idea of the proof:
Let $\mathcal{C}$ be 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

$$\mathcal{C} \quad := \quad T \quad \Vdash \quad \langle X, h(Y) \rangle$$

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

$$\mathcal{C}' \quad := \quad \begin{cases} T & \Vdash_1 \quad X \\ T, X & \Vdash_1 \quad h(Y) \\ T, X, h(Y) & \Vdash_1 \quad \langle X, h(Y) \rangle \end{cases}$$

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

Example

$$\mathcal{C} \quad := \quad T \quad \Vdash \quad \langle X, h(Y) \rangle$$

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

$$\mathcal{C}' \quad := \quad \begin{cases} T & \Vdash_1 \quad X \\ T, X & \Vdash_1 \quad h(Y) \\ T, X, h(Y) & \Vdash_1 \quad \langle X, h(Y) \rangle \end{cases}$$

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

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

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 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

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

System of equations $\mathcal{E}$

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

$z[i,j] \in \mathbb{Z}/2\mathbb{Z}[h]$

Solving quadratic systems of equations is in general undecidable.

Constraint M_E to Quadratic Equations System

System $\mathcal{C}$ of Constraints M_E

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

System of equations $\mathcal{E}$

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

$z[i,j] \in \mathbb{Z}/2\mathbb{Z}[h]$

Solving quadratic systems of equations is in general undecidable.

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

Outline

Theorem [ICALP'06]

The security problem modulo ACUNh with a bounded number of sessions is decidable for deterministic protocols.

Given: Well-defined protocol.

1. Guess partition of subterms $\Rightarrow$ WD one-step Constraints
2. Guess equality on subterms $\Rightarrow$ WD M_E Constraints
3. Abstraction $\Rightarrow$ System of equations WD
4. Solve system of equations $\Rightarrow$ Attack on Protocol.

Conclusions & Future Works

	Complexity	
	Intruder Deduction Problem	**Security Problem**
ACUNh	*EXP-TIME* [RTA'05]	*Decidable* [ICALP'06]
AGh	*EXP-TIME* [RTA'05]	*Undecidable*
ACUN$\{.\}_.$ **&** **AG**$\{.\}_.$	*EXP-TIME* Submitted	*?*
ACUN$\{.\}_.$ **&** **AG**$\{.\}_.$ **Commutative**	*2EXP-TIME* [Secret'06]	*?*

Future Works

Extensions

- Active case for distributive encryption.
- Complexity of our procedure (Active Case).
- General procedure for monoidal theories (AG,ACUN).

Applications

- Web Services.
- Elliptic curves.
- Others properties on new protocols: Authentification, Fairness, Timestamps...
  - E-auction
  - Wireless

Thank you for your attention.

Questions ?