Deciding the Security of Protocols with Commuting Public Key Encryption

Yannick Chevalier[1]
Ralf Küsters[2]
Michaël Rusinowitch[1]
Mathieu Turuani[1]

ARSPA 2004 Workshop

[1] Cassis Project, Loria

[2] Christian-Albrecht University, Kiel

Automated Validation of Internet Security Protocols and Applications

Shared cost RTD (FET open) project IST-2001-39252

Overview

- The general context of Protocol Security with the commuting public key encryption

  $\Rightarrow$ Definitions, Goals, and Hypothesis

- The Ground Case

  $\Rightarrow$ Bounds and Decidability (P-Complete)

- The General Case

  $\Rightarrow$ Bounds and Decidability (NP-Complete)

Motivation: Secured Electronic Transactions

Secured Transactions

- authentication
- exchange of confidential data

Motivation: Secured Electronic Transactions

Secured Transactions

– authentication
– exchange of confidential data

Hostile Environment

Internet, mobile phone networks:

– anonymous communications
– easy listening and/or interception of communications

Motivation: Secured Electronic Transactions

Secured Transactions

– authentication
– exchange of confidential data

Hostile Environment

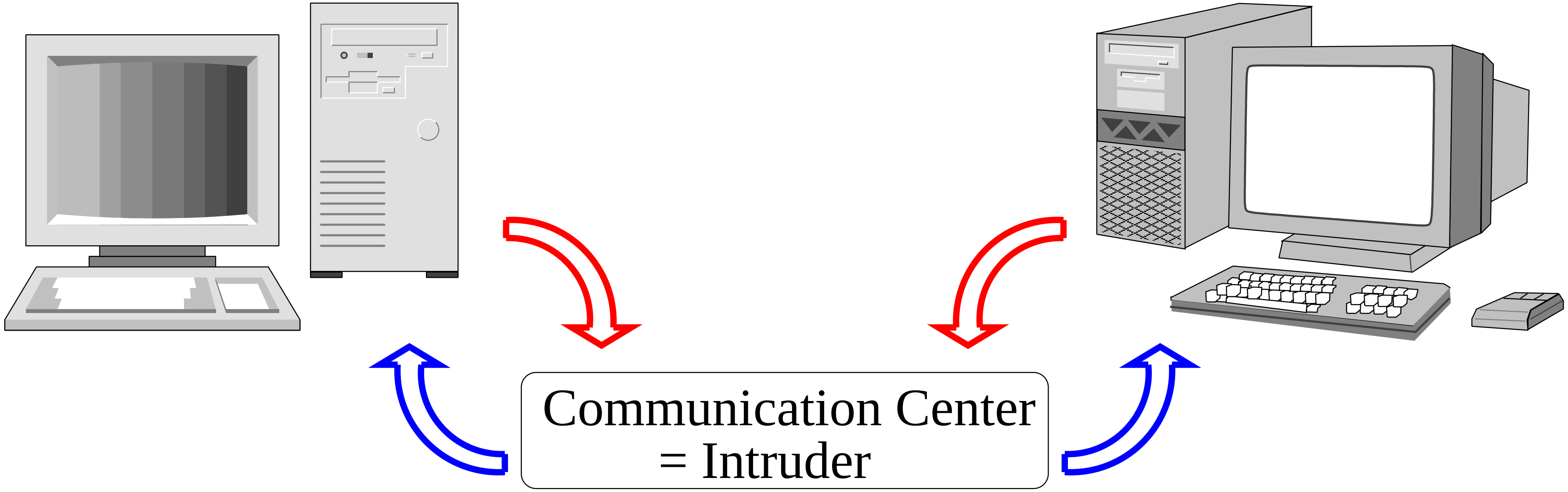
Internet, mobile phone networks:

– anonymous communications
– easy listening and/or interception of communications

Cryptographic Protocols

Goal : Provide secured transactions over an insecure network

Cryptographic Protocols



1. $A \rightarrow B: \quad \{Na, A\}_{Kb}$
2. $B \rightarrow A: \quad \{Na, Nb\}_{Ka}$
3. $A \rightarrow B: \quad \{Nb\}_{Kb}$

Unbounded message size but bounded number of sessions.

Commuting Public Key Encryption

Aim: Build asymmetric keys for a group

- One couple of keys for a group of agents
- Trusted user to build single public/private keys for all agents in the group

Permits to sign a message by several persons

Mean: RSA with same modulus

A wants to sign a contract M with B and C

1. $A \to B:\quad \{M\}^p_{Ka^{-1}}$
2. $B \to C:\quad \left\{\{M\}^p_{Ka^{-1}}\right\}^p_{Kb^{-1}}$
3. $C \to A:\quad \left\{\left\{\{M\}^p_{Ka^{-1}}\right\}^p_{Kb^{-1}}\right\}^p_{Kc^{-1}}$

Relies on the hardness of factorisation

The Goal

To check insecurity with an extended Dolev-Yao model of intruder

Standard rules:

	Composition	Decomposition
Pair	$a, b \rightarrow \langle a, b\rangle$	$\langle a, b\rangle \rightarrow a, b$
Cipher	$a, K \rightarrow \{a\}_K$	$\{a\}_K, K^{-1} \rightarrow a$

Add an Commuting Encryption rule:

RSA $\quad a,\ b,\ c,\ \ldots\ \rightarrow\ a^{b^{n_b} \times c^{n_c} \times \ldots}$

Theory for public key commuting encryption

Based on Meadows-Narendran article

Basics

RSA theory: • associative ciphering

- $\times$ group operator
- public and private key invert one of each other for $\times$

Theory for public key commuting encryption

Based on Meadows-Narendran article

Basics

RSA theory: • associative ciphering

- $\times$ group operator
- public and private key invert one of each other for $\times$

Restrictions

- never $\times$ operator outside encryption

Theory for public key commuting encryption

Based on Meadows-Narendran article

Basics

RSA theory: • associative ciphering

- $\times$ group operator
- public and private key invert one of each other for $\times$

Restrictions

- never $\times$ operator outside encryption
- no handling of multiplicative properties of exponential

Ground Reachability Problem

Deductions

- Deduce t from E in one step:

$$E \rightarrow E, t$$

If: $F \rightarrow t$ rule and $F \subseteq E$

Decision problem

Derive: Given t and E, does there exist F such that:

$$\begin{cases} E \rightarrow^* F \\ t \in F \end{cases}$$

Notation: If the answer is positive, $t \in \text{Forge}(E)$

Definition of Attacks

Setting

A Protocol is a set of steps $(A, n)\ :\ R_n \Rightarrow S_n$

An Attack is a substitution σ such that :

$$\boxed{\begin{array}{llll} \forall i, & R_i\sigma & \in & \text{Forge}\,(S_0\sigma, \ldots, S_{i-1}\sigma) \\ \text{and} & Secret & \in & \text{Forge}\,(S_0\sigma, \ldots, S_n\sigma) \end{array}}$$

modulo RSA

Hypothesis on protocol rules :

If $(t_1)^{t_2 \times \ldots \times t_n}$ subterm of R_i, then there exists at most one $k \in [2..n]$ with $Var(t_k) \not\subset Var(\{R_j \,|\, j < i\})$.

Example : $\{a^{x \times y}\}_K$ forbidden if x and y unknown, use $\{a^z\}_K$ instead

Deterministic protocols transformable to meet this restriction

Subterms

Formalism

- Deduction modulo
- Theory confluent modulo AC

Representation of classes by terms + normalisation function $\ulcorner \cdot \urcorner$

Subterms

- $|E|_{dag}$ number of distinct subterms in E
- products are not subterms

The Ground Case

Derivation starting from E of goal t

$$\boxed{D\ :\ \ E \rightarrow E, t_1 \rightarrow \ldots \rightarrow E, t_1, .., t_{n-1}, t}$$

with t and E ground and normalized modulo RSA.

Lemma. *If $t \in Forge(E)$, then there exists a derivation with all intermediate terms t_i subterms of E or t.*

The Ground Case (2)

Complexity

- $U \ \rightarrow_{RSA} \ v$ can be checked in polynomial time in $|U, v|_{dag}$.

- By closure, we can compute $Forge(E) \cap Sub(E, t)$ in polynomial time.

$\Rightarrow t \in Forge(E)$ can be checked in polynomial time w.r.t. $|E, t|_{dag}$

Theorem 1. $\mathrm{DERIVE} \in PTIME$.

Complexity of the General Case (1)

Decision problem

INSECURE: Given a protocol instance P presented by a set of rules, find an attack σ on $\mathcal{P}$

Idea: bounding the size of the representation of σ

- $|\sigma|_{dag}$: number of different substerms in σ
- $|\sigma|_{rsa}$: total size of representation of coefficients in σ

Main result

Theorem 2. Insecure $\in NPTIME$

Complexity of the General Case (2)

Results on subterms of a minimal attack

Lemma 1. Every insecure Protocol admits an attack σ, such that $\forall x \in Var$ with

$$\sigma(x) = (v_1)^{v_2^{n_2} \times \ldots \times v_n^{n_n}}$$

$n \geq 1$, for all i there exists a subterm t_i of the protocol such that $\ulcorner t_i \sigma \urcorner = v_i$.

Lemma 2. Any insecure Protocol P admits an attack σ with

$$\forall x \in Var, \ \ |\sigma(x)|_{dag} \leq 4 \cdot |P|_{dag}$$

More recently: $|Var\sigma|_{dag} \leq |P|_{dag}$

Complexity of the General Case (3)

Notation: $t \equiv_{coef} t'$ if $t = t'$ up to multiplicity of factors in products

Bounding the coefficient

- Let σ be an attack with $|\sigma|_{dag}$ minimal
- Abstract coefficients in σ by integer variables: σ^*
- $\mathcal{S}$ affine system on variables of σ^*
- Any solution β of $\mathcal{S}$ such that:

$$\forall t \in \mathrm{Sub}(P), \ulcorner \beta(t\sigma^*) \urcorner \equiv_{rsa} \ulcorner t\sigma \urcorner$$

and such that $\beta(\sigma^*)$ is also an attack

Theorem (Folklore). Polynomial bound on the size of a minimal solution of $\mathcal{S}$

Conclusion

Main result : Insecurity with commuting public key encryption is in NP

- NP-hard
- PTIME in the groud case.

A practical version of these rules is being implemented for the European Project AVISPA.