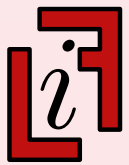
ACTION ROSSIGNOL

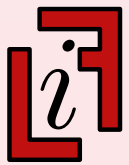
Denis Lugiez

LIF (Univ. de Provence) UMR 6166
LIX (E. Polytechnique) INRIA Futurs
LSV (ENS CACHAN) UMR 8643
VERIMAG (UJF-INPG) UMR 5104
http://www.cmi/ lugiez/rossignol.html

PaRISTIC: 22 Novembre 2005

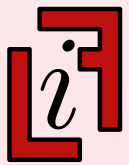


SEMANTIQUE DE LA VERIFICATION DES PROTOCOLES CRYPTOGRAPHIQUES



SEMANTIQUE DE LA VERIFICATION DES PROTOCOLES CRYPTOGRAPHIQUES

Models for Randomized Protocols



SEMANTIQUE DE LA VERIFICATION DES PROTOCOLES CRYPTOGRAPHIQUES

Models for Randomized Protocols

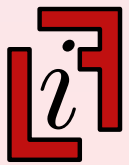
Formal Models and Computational Models

SEMANTIQUE DE LA VERIFICATION DES PROTOCOLES CRYPTOGRAPHIQUES

Models for Randomized Protocols

Formal Models and Computational Models

The Dolev-Yao Model and Extensions
(main part of this talk)



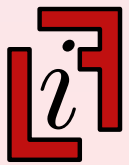
Cryptographic Protocols

- Small concurrent programs
- exchange confidential information over an unsecure network
- $\Rightarrow$ cryptographic primitives (RSA,DES,AES...)
  - ssh, kerberos,...
  - authentication, secrecy,...
  - e-commerce, e-voting,...

Cryptographic Protocols

Needham-Schroeder Protocol:

$$\begin{aligned} A &\rightarrow B : \{N_A\}_{K_B} \\ B &\rightarrow A : \{< N_A, N_B >\}_{K_A} \\ A &\rightarrow B : \{N_B\}_{K_B} \end{aligned}$$



Focus on the formal aspect of security protocols which use randomization to achieve the intended security properties

- An analysis of the protocol *Partial Secret Exchange*, which uses the randomized primitive *Oblivious Transfer*
  - Protocol expressed in a probabilistic π-calculus
  - Proof of correctness based on a probabilistic version of testing semantics

  (K. Chatzikokolakis and C. Palamidessi, *TCS* 2005)
- A new logic for Model Checking with Higher-Order Abstract Syntax
  - Application to the π-calculus
  - Planned probabilistic extension

  (D. Miller, A.Tiu, *TOCL* 2005)

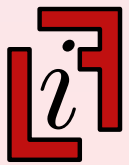
  (A.Tiu, G. Nadathur, D. Miller, *ESHOL* 2005)

- A formal study of the probabilistic aspects of Anonymity properties and protocols
  - Strong probabilistic anonymity, and the Dining Cryptographers M. Bhargava and C. Palamidessi, *CONCUR 2005*
  - Weak Anonymity, and the Dining Cryptographers with biased coins (K. Chatzikokolakis and C. Palamidessi, *FAST 2005*).
  - Probable innocence, and the Crowds protocol (Y. Deng, C. Palamidessi, J. Pang, *SecCo 2005*)
- A comparative survey of searchable, peer-to-peer file-sharing systems that offer the user some form of anonymity (T. Chothia and K. Chatzikokolakis, *NCUS* 2005)

The Computational World and the Formal World

Computational Model	Formal Semantics (Dolev-Yao)
Messages	
bit strings	Terms
Cyphering	
$\hat{m}' \xleftarrow{R} \mathcal{E}(\hat{m}, k)$ probabilistic	$\{m\}_k$ term
Nonce	
random values	names (distincts constants)
Intruder	
Probabilistic Polynomial TM	Inference Rules:$\vdash$
Verification	
Probability of attack negligible	Non existence of attack traces
Closer to reality	Simple Semantics

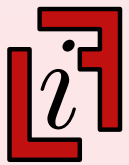
Automated verification



Relationship between the Models?

Attack in Computational Model $\Rightarrow$ Attack in DY Model?
Assumptions on cryptographic primitives: Non-Malleability, Indistinguishability,...

- A line of research initiated in: M. Abadi and P. Rogaway (Symmetric keys, passive intruder)
- Results by Rossignol participants:
  - Active Intruder, Asymmetric Keys, Symmetric Keys, Hashing and Signature all combined + some equational theories (L. Mazaré, Y. Lakhnech and R. Janvier'05)
  - + Diffie-Hellman key exchange modular exponentiation (L. Mazaré and Y. Lakhnech'05)
  - Opacity and e-voting/passive adversaries. (L. Mazaré and Y. Lakhnech'05)



How to Overcome the limitations of the Dolev-Yao Model

Goal: make the formal approach closer to the real world.

- Extend the DY Model to encompass Guessing Attacks. Enhance the Intruder deduction power to handle dictionary attacks. S.Delaune and F.Jacquemard (CSFW 04)

- Enrich the DY model by algebraic properties of operations used in protocols. Some known attacks on protocols use the algebraic properties of operators.
  $\Rightarrow$ this presentation from now on.

A zoo of algebraic properties

Properties of *exclusive or (ExOr)* (symmetric encryption)

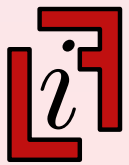
associativity	$(x \oplus y) \oplus z = x \oplus (y \oplus z)$
commutativity	$x \oplus y = y \oplus x$
unit	$0 \oplus x = x$
nilpotence	$x \oplus x = 0$

Homomorphism properties
(asymmetric encryption, block chaining modes)

homomorphic hash functions	$h(x \oplus y) = h(x) \oplus h(y)$
distributive encryption	$\{x \oplus y\}_k = \{x\}_k \oplus \{y\}_k$

Other properties...

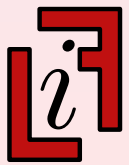
Survey in V. Cortier, S. Delaune, P. Lafourcade (J. of Comp.Sec. 04).



Combination of ExOr and Homomorphism

Pascal Lafourcade Ph.Thesis (Rossignol Grant)
Supervision of D. Lugiez (LIF) and R. Treinen (LSV)

- Occurs in existing protocols (TMN protocol).
- Doesn't fit any existing general approach (finite variant property, combination algorithm)
- Generalizes previous works on ExOr, homomorphism.



The Dolev-Yao Model of Intruder Capabilities

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

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

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

(F) $\dfrac{T \vdash u_1 \quad \cdots \quad T \vdash u_n}{T \vdash f(u_1, \ldots, u_n)} \quad f \in \Sigma^-$

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

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

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

Weakening the Perfect Cryptography Assumption

Extend the Dolev-Yao deduction system by

$$\text{(E)} \quad \frac{T \vdash u \qquad u =_E v}{T \vdash v}$$

$=_E$ defines a *canonical rewrite system* modulo some equational theory.

Here: ExOr $\oplus$ and homomorphism h (or distributive encryption)

Protocols as rewrite rules

Needham-Schroeder Protocol:

$$\begin{array}{lcl} A & \rightarrow & B : \{N_A\}_{K_B} \\ B & \rightarrow & A : \{< N_A, N_B >\}_{K_A} \\ A & \rightarrow & B : \{N_B\}_{K_B} \end{array}$$

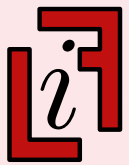
modelled as:

$$\begin{array}{lll} A & 0 & \rightarrow \{N_A\}_{K_B} \\ & \{\langle N_A, x\rangle\}_{K_A} & \rightarrow \{x\}_{K_B} \\ B & \{y\}_{K_B} & \rightarrow \{\langle y, N_B\rangle\}_{K_A} \\ & \{N_B\}_{K_B} & \rightarrow OK \end{array}$$

Execution

- Intruder knowledge contains
  - all public information,
  - all messages emitted.
- Agent a executes rule $u_i \longrightarrow v_i$:
  - wait for receiving an instance $\sigma(u_i)$ of u_i,
  - emit the instance $\sigma(v_i)$ of v_i.
- Compatibility conditions:
  - Check that $\sigma(u_i)$ can be deduced from the intruder knowledge
  - Add to I the term $\sigma(v_i)$
- Execution: an interleaving of the rules respecting protocol.

Express Protocol (un)Security by adding a final rules that reveals the secret.



Finding Attacks

- fix the number of session and identities of participants.
- guess a linearisation of the execution

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

- Solve the constraints: find instantiation σ of the variables s.t. $\sigma(u_i)$ is deducible from $\sigma(t_0), \ldots, \sigma(t_{n+i-1})$ for all i.

The Ground Case: Passive Intruder

- Listen, doesn't forge nor sends messages (eavesdropper).
- Variable can't be instantiated, i.e. decide validity of ground constraints $t_1, \ldots, t_n \vdash t$
- Prerequisite to resolution of non-ground constraints

Local proof of $T \vdash u$: contains only subterms (McAllester '93)

Theorem

(McAllester'93) Provability in local inference systems is decidable in PTIME.

Decidability Results for the Passive Intruder

Previous results:

- Empty theory (Rusinowitch, Turuani '03)
- Distributive encryption: PTIME (*locality*) (Comon&Treinen '03), Xor:PTIME (Comon, Shmatikov'03; Chevalier, Küsters, Rusinowitch, Turuani '03), AG (Millen, Shmatikov '05)

New results:

- ExOr + distributive encryption: EXPTIME (*locality*) PTIME in the binary case (*prefix rewrite system* (Lafourcade,Lugiez,Treinen '05)
- ExOr/AG + homomorphic hash function: PTIME (*locality + linear equations over polynomial rings*) Delaune'05

The Active Intruder Case for ExOr + homomorphism

Active: passive+ forge and send messages

Theorem (Delaune,Lafourcade, Lugiez,Treinen)

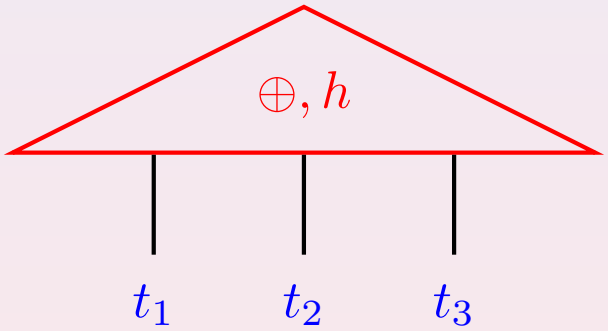
Protocol unsecurity is decidable in the active case (ExOr+homomorphism).

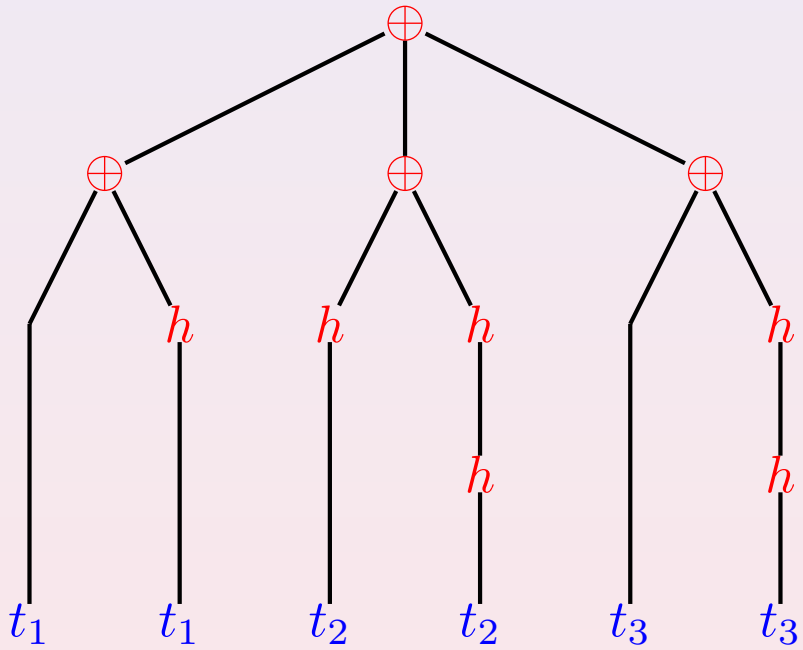
Ingredients of our proof:

- Decidability of ground constraints
- General unification modulo ExOr + homomorphism
- Equation systems over integral domains

Inspired by Millen-Schmatikov for AG/ExOr but cleaner concepts and presentation, many problems due to the homomorphism.

The structure of terms





Linear combination of t_1, t_2, t_3 with coefficients in $\mathbb{Z}/2\mathbb{Z}[h]$

$$(1 \oplus h) \odot t_1 \quad \oplus \quad (h \oplus h^2) \odot t_2 \quad \oplus \quad (1 \oplus h^2) \odot t_3$$

(In)Dependence of terms

Terms involving only $X_1, \ldots, X_n, \oplus, h$

$\equiv$

Linear combination of X_i's with coefficients in $\mathbb{Z}/2\mathbb{Z}[h]$

$u_1, \ldots, u_p$ independent

iff

$$\alpha_1 \odot u_1 + \ldots + \alpha_p \odot u_p = 0 \implies \alpha_1 = \ldots = \alpha_p = 0$$

Otherwise $u_1, \ldots, u_p$ dependent

$h \odot X_1 \oplus X_2, X_1 \oplus h \odot X_2$ independent, $X_1, X_2, X_1 \oplus X_2$ dependent.

Well-defined constraint systems

$$
\begin{array}{lcl}
t_0, \ldots, t_n & \vdash & u_1 \\
\ldots & \vdash & \ldots \\
\ldots & \vdash & u_i \\
t_0, \ldots, t_n, \ldots, t_{n+i} & \vdash & \ldots \\
\ldots & \vdash & \ldots \\
t_0, \ldots, t_n, \ldots\ldots, t_{n+k} & \vdash & u_{k+1} = \mathit{secret}
\end{array}
$$

A constraint system is *well-defined* (Millen, Shmatikov '03) iff

- The left-hand sides are monotonously increasing
- $\mathcal{V}(t_0, \ldots, t_{n+i}) \subseteq \mathcal{V}(u_1, \ldots, u_i)$
- the latter property is *stable under substitution*

Making use of well-definedness

Basis: subset of the r.h.s : $u_1, \ldots, u_l$ such that

- $\vec{u_1}, \ldots, \vec{u_l}$ independent
- $\vec{u}$ dependent on $\vec{u_1}, \ldots, \vec{u_l}$ if u not in the basis.

Consequence of well-definedness:
for every term t on the l.h.s : $\vec{t}$ dependent on $\vec{u_1}, \ldots, \vec{u_l}$.

How to solve $\vdash$ constraint systems for ExOr + homomorphism

1. from $\vdash$ constraints to $\vdash_1$ constraints
   generalisation of the locality of $\vdash$
2. from $\vdash_1$ constraints to $\vdash_{M_E}$ constraints
   general ExOr+h-unification is decidable and finitary
3. abstract subterms by constants
4. from $\vdash_{M_E}$ to ground $\vdash_{M_E}$ constraints
   determine value of variables from the contexts
5. check satisfiability of ground $\vdash_{M_E}$ constraint system

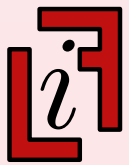
Conclusion

A difficult result for a theory which does not fall in general classes.

Further work:

- Extension to AG+homomorphism?
- Extension to Distributive encryption?
- Complexity Analysis?
- Does it cover a whole class of algebraic properties?

More generally Rossignol: Many works in progress randomized protocols, computational model, formal model.



Thank You

Questions?