

University of Grenoble

Pascal Lafourcade¹

¹Université Joseph Fourier, Verimag
pascal.lafourcade@imag.fr

Vancouver: December 6th 2007

Where is Grenoble?



- 3 hours by TGV to Paris, 1h30 to Turin
- 150 kms from Geneva and less than 1 hour to Alps
- 1 hour to Lyon International Airport
- One of the best Hockey Team “Les Brûleurs de Loups”



Studies and Research in Grenoble

Research

- International Pole of competitiveness:
“ *Nanotechnology and embedded systems*”
- 2nd Research center in France after Paris

Studies

- International Master: “Security, Cryptology and Coding of Information Systems”
 - Taught in English (tutoring French and English)
 - Open to foreign students (10/26)

<https://intranet.ensimag.fr/KIOSK/MasterCSCI/2A/index.html>

Security, Cryptology and Coding of Information Systems

- **Common Core: Security and Cryptology**
 - Security models: proofs, protocols and politics
 - Symmetric and asymmetric cryptology; PKI infrastructures
 - System administration and network security
- **Specialization 1: System security**
 - Advanced system and network security
 - Secured hardware architectures
 - Distributed algorithms and fault tolerance
 - Project: secured grid infrastructure
- **Specialization 2: Cryptology, coding and multimedia applications**
 - Advanced cryptology: elliptic curves, cryptanalysis and practical
 - Multimedia applications
 - Coding and fault-tolerance

Outline

- 1 Number theory and cryptographic applications
- 2 Computational Arithmetic and Algebra
- 3 Fault Tolerance and security for Grid Computation
- 4 Computational Aided Provable Security
- 5 Conclusion
- 6 Introduction & Motivation
- 7 Security Problem (Active Attacker)
 - New Extended Dolev-Yao Model
 - Modelisation of Protocols with Constraint System
 - Well-defined Constraints System
 - From Well-defined Constraints System to System of Equations
- 8 Conclusion

Outline

- 1 Number theory and cryptographic applications
- 2 Computational Arithmetic and Algebra
- 3 Fault Tolerance and security for Grid Computation
- 4 Computational Aided Provable Security
- 5 Conclusion
- 6 Introduction & Motivation
- 7 Security Problem (Active Attacker)
 - New Extended Dolev-Yao Model
 - Modelisation of Protocols with Constraint System
 - Well-defined Constraints System
 - From Well-defined Constraints System to System of Equations
- 8 Conclusion

Main research interests

- Applications of algebraic structures and number theory to symmetric ciphers (e.g., building S-boxes from elliptic or hyper-elliptic curves).
- (Hyper)Elliptic Curve Cryptography and design / cryptanalysis of cryptosystem and protocols using arithmetic geometry techniques.
- Lattice reduction over number rings, design and cryptanalysis of cryptosystems and protocols based on lattices over number rings.
- Number Field Sieves.

Present works

- Efficient implementation of ECC and cryptanalysis of ECMQV.
- Lattices reduction over number rings and generalization of NTRU.
- Algebraic sieving techniques.
- Design and cryptanalysis of a new cryptosystem based on Hecke algebra and arithmetic geometry of finite fields; this is part of the PhD thesis of K. Vankov.
- Algebraic aspects of codes and cryptography.
- Construction of S-boxes using hyper-elliptic curves.
- Cryptology of symmetric ciphers.
- Morpho-Cryptography; it is a new method for securing both information and storage media.

Members cryptographic team of Institute Fourier

- **Faculty members of the team:**
 - Philippe Elbaz-Vincent (joined the team in September 2007)
 - Roland Gillard
 - Alexei Pantchichkine.
- **Current PhD students:**
 - J. Lancrenon (R. Gillard / X.F. Roblot)
 - Th. Roche (R. Gillard / J.L. Roch)
 - A. Sarr (J.C. Bajard / Ph. Elbaz-Vincent)
 - K. Vankov (A. Pantchichkine).
- **Former members:**
 - F. Leprévost (currently at University of Luxembourg)
 - V. Despiegel (former PhD student of R. Gillard, currently at Sagem)
 - A. Gewirtz (former PhD student of F. Leprévost and A. Pantchichkine).

Outline

- 1 Number theory and cryptographic applications
- 2 Computational Arithmetic and Algebra**
- 3 Fault Tolerance and security for Grid Computation
- 4 Computational Aided Provable Security
- 5 Conclusion
- 6 Introduction & Motivation
- 7 Security Problem (Active Attacker)
 - New Extended Dolev-Yao Model
 - Modelisation of Protocols with Constraint System
 - Well-defined Constraints System
 - From Well-defined Constraints System to System of Equations
- 8 Conclusion

Computational Arithmetic and Algebra

- Givaro: C++ library for arithmetic and algebraic computations, fully compatible with LinBox.
- GMP-Elliptic Curve Method for prime number factorization.
- Linear algebra of crible algorithms for factorization or discrete logarithm.
- Efficient generation of primitive roots, application to key exchange and primality probabilistic tests.

Team CASYS-LJK

(Calculs Algébriques et Systèmes Dynamiques)

- Members:
 - Laurent Fousse
 - Rodney Coleman
 - Jean-Guillaume Dumas
- PhD: Anna Urbanska

"Théorie des Codes : compression, cryptage, correction" by

- Jean-Guillaume Dumas : Maître de conférences at University Grenoble 1. Responsable of Master 1 of applied math.
- Jean-Louis Roch : Maître de conférences l'ENSIMAG. Responsable of Master 2 "Cryptologie, sécurité et codage de l'information"
- Eric Tannier : Searcher at INRIA Rhne-Alpes.
- Sébastien Varrette : PhD at university of Luxembourg.

Outline

- 1 Number theory and cryptographic applications
- 2 Computational Arithmetic and Algebra
- 3 Fault Tolerance and security for Grid Computation**
- 4 Computational Aided Provable Security
- 5 Conclusion
- 6 Introduction & Motivation
- 7 Security Problem (Active Attacker)
 - New Extended Dolev-Yao Model
 - Modelisation of Protocols with Constraint System
 - Well-defined Constraints System
 - From Well-defined Constraints System to System of Equations
- 8 Conclusion

Fault Tolerance and security for Grid Computation

- **Certification and fault-tolerance**
 - Probabilistic certification against massive attacks
 - Algorithm-based fault-tolerance (eg use of ECC coding)
- **Design and development of the French Grid'5000 authentication system**
- **Parallel encryption/decryption and hashing**
 - Processor-oblivious algorithms (multi-core, embedded systems)
 - Parallel mode of operations,
 - FPGA integration of symmetric cipher
- **Evaluation/improvement of cryptography using grids:**
 - Computation intensive SBox robustness analysis
 - Integrity of distributed data

Outline

- 1 Number theory and cryptographic applications
- 2 Computational Arithmetic and Algebra
- 3 Fault Tolerance and security for Grid Computation
- 4 Computational Aided Provable Security**
- 5 Conclusion
- 6 Introduction & Motivation
- 7 Security Problem (Active Attacker)
 - New Extended Dolev-Yao Model
 - Modelisation of Protocols with Constraint System
 - Well-defined Constraints System
 - From Well-defined Constraints System to System of Equations
- 8 Conclusion

Members of the DCS Verimag team: Axe Security



Yassine Lahknech



Laurent Mounier



Jean-francois Monin



Cristian Ene



Michael Périn



Judicael Courant



Pascal Lafourcade

PhD : Manuel.S.M Garnacho

Topics

- CAPS: Computer-Aided provable Security
 - Verification of security protocols within Dolev-Yao model
 - Justification of the Dolev-Yao model with respect to the complexity-theoretic framework (computational security).
- Language-based security:
 - Computational Non-interference.
 - Security by typing: type system for ciphers, type system for hash and one-way functions (OAEP, etc...) (ongoing work).
 - Testing of security policies for networked information systems.
- Software engineering for security:
 - Computer-aided certification methodology for the EAL7 of the Common Criteria.
 - Security by construction using the B-method.
- Foundations of cryptography:
 - A general study of Diffie-Hellman problems (CRYPTO'07).
 - The selective decryption problem.
- E-voting

Project: AVOTE

Partners: LSV, LORIA, VERIMAG, France Telecom

Properties:

- correctness, which attest the accuracy of the results,
- privacy, which keep the voter's identity unknown,
- receipt-freeness, in order to prevent vote-selling,
- robustness, so to resist to attack,
- verifiability, so that the protocol can be trusted,
- democracy and fairness, which enable that the election is fair.

- Blind signature
- Mix-Net
- Homomorphic encryption

$$\prod \{m_i\}_k = \{\sum m_i\}_k$$



Project: SCALP

EVEREST INRIA, ProVal LRI, Plume-LIP and DCS-VERIMAG

Security of Cryptographic Algorithms with Probabilities

- Probabilistic language and semantics for cryptographic proofs.
- Formalization of random generators
- Proof theory
 - High-level reasoning about distributions defined by probabilistic programs.
 - Semantic preserving program transformations.
 - Cryptography-based program transformations.
 - Asymptotic reasoning.

We expect to have a Coq-based tool for proving correctness of cryptosystems, for key-exchange protocols, computationally sound type systems for non-interference and data integrity, and watermarking.

Outline

- 1 Number theory and cryptographic applications
- 2 Computational Arithmetic and Algebra
- 3 Fault Tolerance and security for Grid Computation
- 4 Computational Aided Provable Security
- 5 Conclusion**
- 6 Introduction & Motivation
- 7 Security Problem (Active Attacker)
 - New Extended Dolev-Yao Model
 - Modelisation of Protocols with Constraint System
 - Well-defined Constraints System
 - From Well-defined Constraints System to System of Equations
- 8 Conclusion

Summary

Grenoble Resources

- Covering security through number theory to software development
- Using symbolic and cryptographic approach
- Working on security and cryptography
- 24 persons in different teams
- High national and international visibility through more than 20 projects
- A real tradition in International Collaborations
- Possibility to accept students in International MASTER, in PhD and Postdocs.

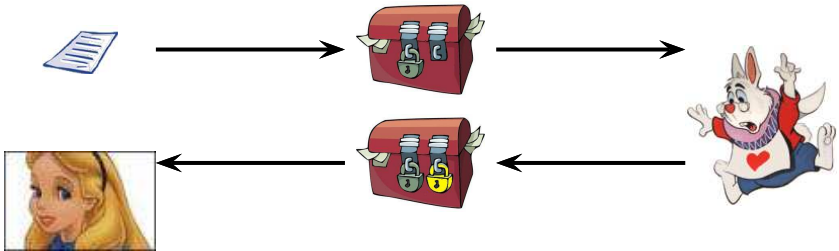
Outline

- 1 Number theory and cryptographic applications
- 2 Computational Arithmetic and Algebra
- 3 Fault Tolerance and security for Grid Computation
- 4 Computational Aided Provable Security
- 5 Conclusion
- 6 Introduction & Motivation**
- 7 Security Problem (Active Attacker)
 - New Extended Dolev-Yao Model
 - Modelisation of Protocols with Constraint System
 - Well-defined Constraints System
 - From Well-defined Constraints System to System of Equations
- 8 Conclusion

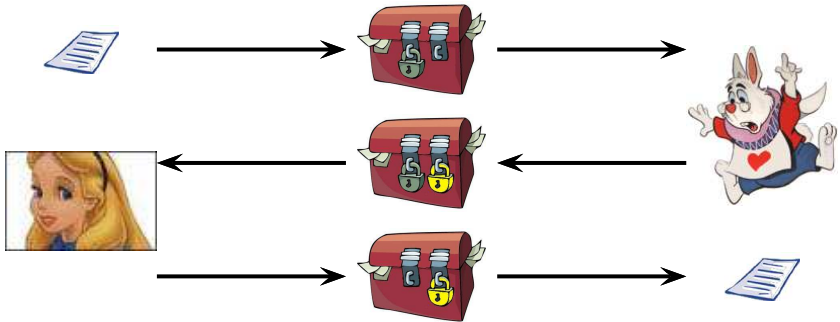
Example :



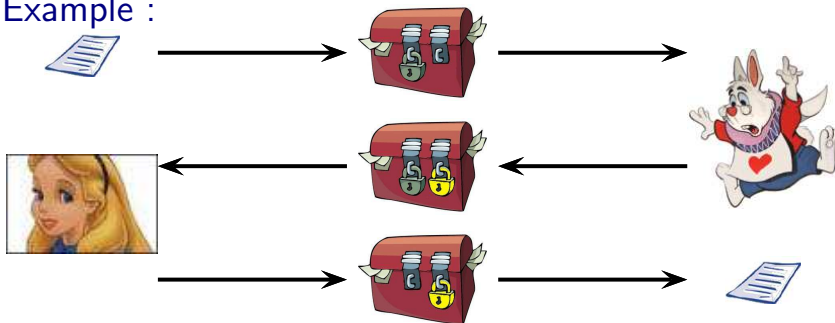
Example :



Example :



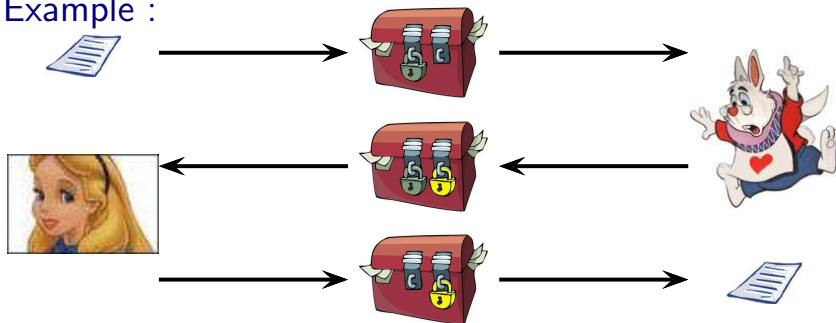
Example :



Shamir 3-Pass Protocol

1 $A \rightarrow B : \{m\}_{K_A}$

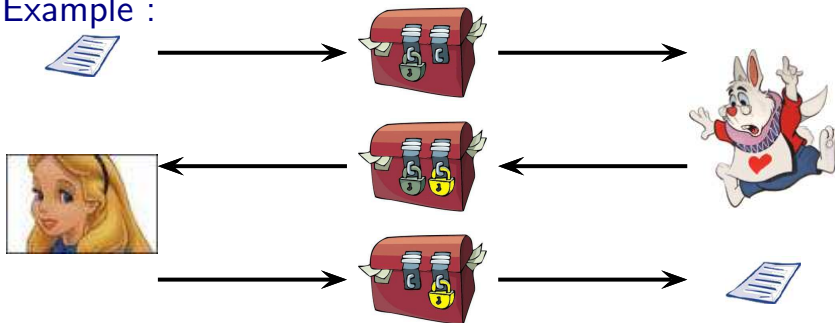
Example :



Shamir 3-Pass Protocol

- 1 $A \rightarrow B : \{m\}_{K_A}$
- 2 $B \rightarrow A : \{\{m\}_{K_A}\}_{K_B}$

Example :

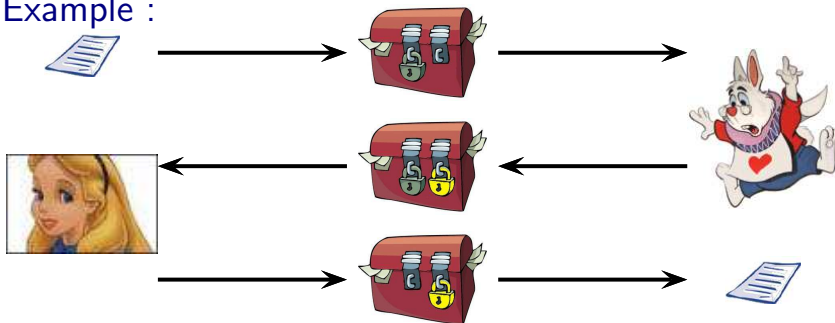


Shamir 3-Pass Protocol

$$\begin{aligned}
 1 \quad A &\rightarrow B : \{m\}_{K_A} \\
 2 \quad B &\rightarrow A : \{\{m\}_{K_A}\}_{K_B} = \{\{m\}_{K_B}\}_{K_A}
 \end{aligned}$$

Commutative
Encryption

Example :



Shamir 3-Pass Protocol

- 1 $A \rightarrow B : \{m\}_{K_A}$
- 2 $B \rightarrow A : \{\{m\}_{K_A}\}_{K_B} = \{\{m\}_{K_B}\}_{K_A}$
- 3 $A \rightarrow B : \{m\}_{K_B}$

Commutative
Encryption

Attacks

Computational Model Cryptanalysis



Attacks

Computational Model Cryptanalysis



Attacks

Computational Model
Cryptanalysis



Symbolic Model
Logical Attack

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]

Logical Attack on Shamir 3-Pass Protocol (I)

Perfect encryption one-time pad (Vernam Encryption)

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

XOR Properties (ACUN)

- $(x \oplus y) \oplus z = x \oplus (y \oplus z)$
- $x \oplus y = y \oplus x$
- $x \oplus 0 = x$
- $x \oplus x = 0$

Associativity

Commutativity

Unity

Nilpotency

Logical Attack on Shamir 3-Pass Protocol (I)

Perfect encryption one-time pad (Vernam Encryption)

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

XOR Properties (ACUN)

- $(x \oplus y) \oplus z = x \oplus (y \oplus z)$
- $x \oplus y = y \oplus x$
- $x \oplus 0 = x$
- $x \oplus x = 0$

Associativity

Commutativity

Unity

Nilpotency

Vernam encryption is a **commutative encryption** :

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

Logical Attack on Shamir 3-Pass Protocol (II)

Perfect encryption one-time pad (Vernam Encryption)

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

Shamir 3-Pass Protocol



- 1 $A \rightarrow B : m \oplus K_A$
- 2 $B \rightarrow A : (m \oplus K_A) \oplus K_B$
- 3 $A \rightarrow B : m \oplus K_B$



Passive attacker :

$$m \oplus K_A \quad m \oplus K_B \oplus K_A \quad m \oplus K_B$$



Logical Attack on Shamir 3-Pass Protocol (II)

Perfect encryption one-time pad (Vernam Encryption)

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

Shamir 3-Pass Protocol



- 1 $A \rightarrow B : m \oplus K_A$
- 2 $B \rightarrow A : (m \oplus K_A) \oplus K_B$
- 3 $A \rightarrow B : m \oplus K_B$



Passive attacker :

$$m \oplus K_A \oplus m \oplus K_B \oplus K_A \oplus m \oplus K_B = m$$



TMN Protocol: Distribution of a fresh symmetric key

[Tatebayashi, Matsuzuki, Newmann 89]:

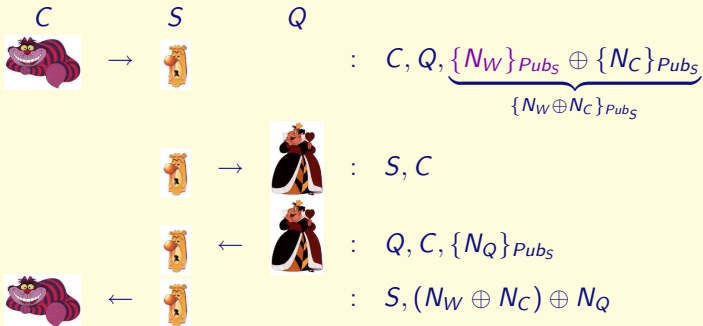


Alice retrieves N_W :

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

Attack on TMN Protocol [Simmons 89]

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

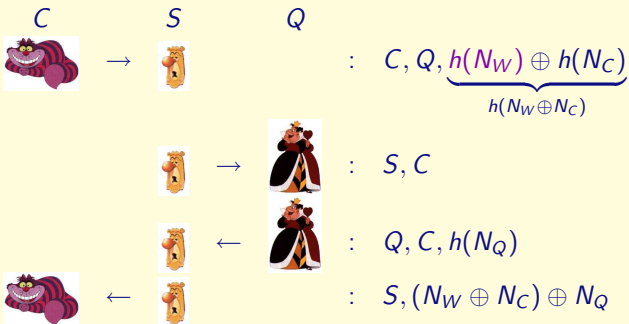


Cheshire Learns: N_W

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



Cheshire Learns: N_W

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

Relaxing the perfect encryption hypothesis.

[Journal of Computer Security'06]

	Examples of Protocols	Intruder Deduction Problem	Security Problem
Commutative encryption	Shamir	<i>P-TIME</i> [CKRT'04]	<i>NP-Complete</i> [CKRT'04]
ACUN	Bull, Gong	<i>P-TIME</i> [CS'03,CKRT'03]	<i>NP-Complete</i> [CS03,CKRT'03]
AG + Exp	IKA.1	<i>P-TIME</i> [CKRTV'03]	<i>Decidable</i> [MS'03]
ACUNh	WEP	<i>P-Time</i> [Delaune'06]	<i>Exp-Time</i> [DLLT'07]
AGh	TMN	<i>P-Time</i> [Delaune'06]	<i>Exp-Time</i> [DLLT'07]

Outline

- 1 Number theory and cryptographic applications
- 2 Computational Arithmetic and Algebra
- 3 Fault Tolerance and security for Grid Computation
- 4 Computational Aided Provable Security
- 5 Conclusion
- 6 Introduction & Motivation
- 7 Security Problem (Active Attacker)**
 - New Extended Dolev-Yao Model
 - Modelisation of Protocols with Constraint System
 - Well-defined Constraints System
 - From Well-defined Constraints System to System of Equations
- 8 Conclusion

New Extended Dolev-Yao Deduction System

Deduction System : $T_0 \vdash^? s$

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

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

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

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

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

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

$$(ME) \quad \frac{T_0 \vdash u_1 \quad \dots \quad T_0 \vdash u_n}{T_0 \vdash C[u_1, \dots, u_n]} \quad C \text{ is a context made with } \{h, \oplus\}$$

Modeling a protocol as a system of constraints

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

$$\mathcal{P} := \left\{ \begin{array}{l} \text{recv}(u_1); \text{send}(v_1) \\ \text{recv}(u_2); \text{send}(v_2) \\ \vdots \\ \text{recv}(u_n); \text{send}(v_n) \end{array} \right.$$

T_0 initial Intruder knowledge.

$$\mathcal{C} := \left\{ \begin{array}{ll} T_0 & \Vdash u_1 \\ T_0, v_1 & \Vdash u_2 \\ T_0, v_1, v_2 & \Vdash u_3 \\ \vdots & \\ T_0, v_1, \dots, v_n & \Vdash s \end{array} \right.$$

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

System of Constraints Well-formed [MS'03]

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

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

$$T_1 \subseteq T_2 \subseteq \dots \subseteq T_k$$

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

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

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.

$$T_1 \subseteq T_2 \subseteq \dots \subseteq T_k$$

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

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

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

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

Well-Definedness: Example

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

Monotonicity OK !

Well-Definedness: Example

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

Monotonicity OK !

Origination OK !

Well-Definedness: Example

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

Monotonicity OK !

Origination OK !

Well-formed OK !

Well-Definedness: Example

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

Monotonicity OK !

Origination OK !

Well-formed OK !

But **NOT** well-defined !

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

$$\mathcal{C}\theta := \begin{cases} T_0 & \Vdash 0 \\ T_0, X & \Vdash c \end{cases}$$

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

Example

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

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

Example

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

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

$$\mathcal{C}' := \left\{ \begin{array}{ll} T & \Vdash_1 X \\ T, X & \Vdash_1 h(Y) \\ T, X, h(Y) & \Vdash_1 \langle X, h(Y) \rangle \end{array} \right.$$

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

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

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

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

From W-D \Vdash_{ME} to W-D Equations System (I)

Idea

Abstraction ρ to get a constraint system on signature: \oplus , h , and constant symbols.

Example:

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

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

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

From W-D \Vdash_{M_E} to W-D Equations System (II)

Lemma

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

Example:

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

\mathcal{C} and \mathcal{C}_ρ are well-defined.

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

Constraint M_E to Quadratic Equations System

System \mathcal{C} of Constraints M_E

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

System of equations \mathcal{E}

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

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

Solving quadratic systems of equations is in general **undecidable**.

Constraint M_E to Quadratic Equations System

System \mathcal{C} of Constraints M_E

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

System of equations \mathcal{E}

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

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

Solving quadratic systems of equations is in general **undecidable**.

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

Outline

- 1 Number theory and cryptographic applications
- 2 Computational Arithmetic and Algebra
- 3 Fault Tolerance and security for Grid Computation
- 4 Computational Aided Provable Security
- 5 Conclusion
- 6 Introduction & Motivation
- 7 Security Problem (Active Attacker)
 - New Extended Dolev-Yao Model
 - Modelisation of Protocols with Constraint System
 - Well-defined Constraints System
 - From Well-defined Constraints System to System of Equations
- 8 Conclusion

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.

Future Works

Applications

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

Thank you for your attention



Questions ?