The ENS Crypto Team
CASCADE: Construction and Analysis of Systems for Confidentiality and Authenticity of Data and Entities

David Pointcheval

May 12th, 2011
Permanent Members

3 CNRS, 3 INRIA, 3 ENS, and 1 Univ. Paris 2

<table>
<thead>
<tr>
<th>Permanent Members (10)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Michel Abdalla, Junior Researcher, CNRS</td>
</tr>
<tr>
<td>Bruno Blanchet, Senior Researcher, INRIA</td>
</tr>
<tr>
<td>Pierre-Alain Fouque, Assistant Professor, ENS</td>
</tr>
<tr>
<td>Vadim Lyubashevsky, Junior Researcher, INRIA</td>
</tr>
<tr>
<td>David Naccache, Professor, Paris II</td>
</tr>
<tr>
<td>Phong Nguyen, Senior Researcher, INRIA</td>
</tr>
<tr>
<td>David Pointcheval, Senior Researcher, CNRS</td>
</tr>
<tr>
<td>Oded Regev, Senior Researcher, CNRS</td>
</tr>
<tr>
<td>Jacques Stern, Professor, ENS</td>
</tr>
<tr>
<td>Damien Vergnaud, Assistant Professor, ENS</td>
</tr>
</tbody>
</table>
# Ph. D. Students (14)

## Who Started in 2010 (8)
- David Cadé (ENS)
- Yuanmi Chen (ENS)
- Patrick Derbez (ENSC)
- Léo Ducas (ENS)
- Aurore Guillevic* (Thales)
- Jérémy Jean (ANR SAPHIR/DGA)
- Hassen Karray* (Gemalto)
- Miriam Paiola (INRIA)

## Who Started Before (6)
- Roch Lescuyer* (Orange)
- Mario Strefler (INRIA)
- Mehdi Tibouchi (ANR PACE)
- Olivier Blazy (Paris 7)
- Delphine Masgana* (DGA/CELAR)
- Charles Bouillaguet (EADS)
# Temporary Members

## Post-Docs (4)
- Dario Fiore (ANR PAMPA)
- Jiqiang Lu (ANR SAPHIR)
- Christian Rechberger (Chaire France Telecom)
- Siamak F Shahandashti (Univ. Paris 8)

## Delegation (1)
- Duong Hieu Phan (Paris 8, INRIA)

And a few internship students
Administrative and Technical Staff

Administrative Staff

- Nathalie Gaudechoux (INRIA Assistant)
- Joëlle Isnard (LIENS Administrative Head)
- Michelle Angely, Lise-Marie-Bivard, Isabelle Delais, and Valérie Mongiat

Technical Staff

- Jacques Beigbeder (System Administrator)
- Nasser Bacha, Jean-Claude Lovato, and Ludovic Ricardou
Teaching

L3/M1 Courses:
- Algorithms and Programming
  Jacques Stern, Damien Vergnaud, Pierre-Alain Fouque
- Algorithms and Hardness of Approximation
  Oded Regev
- Computer Science by Practice
  David Naccache
- Initiation to Cryptology
  Jacques Stern, Damien Vergnaud, David Naccache

M2 Courses:
- Cryptographic Protocols: Formal and Computational Proofs
  Bruno Blanchet, David Pointcheval
- Cryptanalysis
  Phong Nguyen, Pierre-Alain Fouque
### Visibility

- Thesis: 10 PhD and 2 HDR
- Edition of Proceedings: 5
- Chapters of Books: 4
- Journal Papers: 25
- Conference Papers: 113

#### Program Committees (2008–2010)
CASCADE is in all the PCs of the main crypto-conferences:
- 2008: 10 (incl. EC, AC, and PKC)
- 2009: 24 (incl. Crypto, EC, AC, FSE, and PKC)
- 2010: 25 (incl. Crypto, EC, AC, PKC, TCC, and CHES)

Chair of PCs: FSE ’09, ACNS ’09, PKC ’10, Latincrypt ’10

2 elected directors in the board of IACR (among 9)
## International Relations (2008–2010)

### International Visitors

- Mihir Bellare, UC San Diego, USA
- Xavier Boyen, Stanford Univ., USA
- Jonathan Katz, U. Maryland, USA
- Igor Shparlinski, U. Macquarie, AU
- Dennis Hofheinz, CWI, NL
- Vincent Rijmen, KU Leuven, BE
- Vadim Lyubashevsky, Tel-Aviv., IL
- Adi Shamir, Weizmann Institute, IL

### International Visits

- UC San Diego, USA
- Stanford Univ., USA
- Georgia Tech, Atlanta, USA
- UFF Univ., Rio de Janeiro, Brazil
- Tsinghua Univ., Beijing, China
- NTT, Tokyo, Japan
- Korea Univ., South Korea
- Wollongong, Australia
- Bangalore, India
- Dakar, Senegal
- Leuven, Belgium
- IMDEA, Madrid, Spain
- Univ. Bristol, Bristol, UK
- Imperial College London, UK
- Royal Holloway, Univ. London, UK
- Univ. Catania, Italy
- EPFL, Lausanne, Switzerland
- University of Bochum, Germany
Cryptography

3 Historical Goals

- **Confidentiality**: The content of a message is concealed
- **Authenticity**: The author of a message is well identified
- **Integrity**: Messages have not been altered between a sender and a recipient, against an adversary

New Goals

- **Privacy**: No (unnecessary) personal information released security within groups, with insider adversaries
First Encryption Mechanisms

The goal of encryption is to hide a message

Substitutions and permutations

Security relies on the secrecy of the mechanism

⇒ How to widely use them?

Scytale
Permutation

Alberti’s disk
Mono-alphabetical Substitution

Wheel – M 94 (CSP 488)
Poly-alphabetical Substitution
Use of a (Secret) Key

A shared information (secret key) between the sender and the receiver parameterizes the public mechanism:

- Vigenère: key letters tell the shift in the Caesar’s Code
- Enigma: connectors and rotors

Security looks better: but broken (Alan Turing et al.)

⇒ Security analysis is required
Modern Cryptography: DES and AES

Still substitutions and permutations, but considering various classes of attacks (statistic)

DES: Data Encryption Standard

“Broken” in 1998 by brute force: too short keys (56 bits)!

⇒ No better attack granted a safe design!

New standard since 2001: Advanced Encryption Standard

Longer keys: from 128 to 256 bits

Selection: Security arguments against many attacks
Modern Cryptography: Public-Key Encryption


- Bob’s public key $pk$ is used by Alice as a parameter to encrypt a message to Bob.
- Bob’s private key $sk$ is used by Bob as a parameter to decrypt ciphertexts.

The secrecy of the private key $sk$ guarantees the secrecy of communications $\Rightarrow$ to be proven!
### Conditional Security

#### Symmetric Cryptography

Quite a few constructions are at the information-theoretic level, and they are inefficient (one-time pad).

Security often relies on some internal primitives!

#### Asymmetric Cryptography

Security (at least) relies on the hardness of finding a private key associated to the public key.

This condition is often not enough!

- What does security mean?
  - Security notions have to be formally defined
- How to guarantee security claims for concrete schemes?
  - Provable security
Provable Security

Methodology

- If there exists an adversary able to efficiently break the cryptosystem
- Then there exists an algorithm (Simulator + Adversary) able to efficiently break the underlying problem
Provable Security

**Methodology**

- If there exists an adversary able to **efficiently** break the cryptosystem
- Then there exists an algorithm (Simulator + Adversary) able to **efficiently** break the underlying problem

If the underlying problem is hard to solve then the cryptosystem is secure
Security Proofs

Three Main Steps

- **Security Model**
  - Who is the adversary, and what do we want to prevent?
  - **Goals and means of the adversary**

- **Intractability Assumptions**
  - Admitted hard problems
    - Integer factoring, discrete log, short vector, etc.

- **Complexity Reduction**
  - Polynomial reduction (complexity theory)
  - **Efficient reduction**
    - proof for realistic parameters / key sizes
Goals

<table>
<thead>
<tr>
<th>Secure Schemes</th>
<th>For both symmetric and asymmetric cryptography, security proofs are nowadays a requirement, → strong security models → design of schemes with provable security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improvements</td>
<td>New features (anonymity, traceability, dynamic groups, etc) Better efficiency (time, size, power consumption, etc)</td>
</tr>
<tr>
<td>Actual Meaning of Provable Security</td>
<td><strong>Security Model:</strong> Is it well-suited? <strong>Intractability Assumptions:</strong> Are they still valid? <strong>Reduction:</strong> Is it efficient enough (key size)?</td>
</tr>
</tbody>
</table>
Cryptanalysis helps to answer these questions. Weaknesses can appear at various levels:

- **Mathematical level**
  - Study of the general intractability assumptions

- **Protocol level**
  - Study of the specific instances (not general class)

- **Modelling level**
  - Study of the security models

- **Implementation level**
  - Programming mistakes

- **Hardware level**
  - *side-channel / fault* attacks
Provable Security: Authenticated Key Exchange

A fundamental problem in cryptography:
Enable secure communication over insecure channels
⇒ encryption under a common secret key $K$ (symmetric crypto)

How to establish such a common secret $K$?
→ Key Exchange Protocols
Provable Security: Authenticated Key Exchange

- The secret $K$ should only be known to the involved parties
  - how to authenticate the players?
  - We addressed the password-based setting

- $K$ should be indistinguishable from a random string
  - how to extract a truly random string?
  - We worked on the randomness extractors

- AKE combined with other cryptographic protocols
  - we need **composable** security proofs:
  - Proofs in the UC framework, with adaptive adversaries

- We additionally considered AKE in (dynamic) groups
Besides AKE for groups, cryptographic protocols within groups face new threats, with *insider adversaries*

- **Group Key Exchange: Contributiveness**
  → insider adversaries cannot bias the common key

- **Dynamic Threshold Encryption**
  → enough recipients should agree to run decryption

- **Broadcast Encryption/Traitor Tracing**
  → only the legitimate users can decrypt
  a collusion of traitors should be traceable

Privacy also becomes an important issue

- **Group signatures**
- **Proxy Signatures**
- **Anonymous Encryption**
# Provable Security: Automatic Proofs

Development of two softwares:

**ProVerif: Dolev-Yao (Symbolic) Model**
- cryptographic primitives = black-boxes
- messages = terms on these primitives
- adversary is restricted to apply these primitives
  → secrecy, authentication, unbounded number of sessions

**CryptoVerif: Computational Model**
- cryptographic primitives = functions on bit-strings
- messages = bit-strings
- adversary = probabilistic polynomial time Turing machine
  → secrecy, proofs by sequences of games
Cryptanalysis

**Lattice-based Cryptanalysis**

- LLL and optimized variants
  - theoretical improvements
  - practical experiments with several successful attacks

  ⇒ Key-sizes in lattice-based schemes

**Multivariate Cryptography**

- New intractability assumption: system of multivariate quadratic equations

- Various attacks against cryptosystems using multivariate systems

  ⇒ No longer a real alternative
Symmetric Cryptography

Essentially on hash functions:

After the devastating attacks (in 2005)
- Improvement of the differential cryptanalysis
- Application to APOP, HMAC, etc
  → Key recovering

NIST SHA-3 Competition
- Analysis of the candidates
- Our candidate SIMD passed the 2nd round
Projects

ANR Projects
- RNRT/ANR SAPHIR and SAPHIR II (on Hash Functions)
- ANR PACE (on Pairing and E-cash)
- ANR PAMPA (on Password-based Authentication)
- ANR BEST (on Broadcast Encryption)
- ANR ProSe (on Automatic Proofs)
- ANR PRINCE (on Leakage Resilient Schemes)

European Projects
- ECRYPT I and II – AZTEC and MAYA virtual labs
- ERC Starting Grant LATTICE (Oded Regev)
Projects

Other
- with Joint MSR-INRIA laboratory (on Secure Computation)
- for DGA/CELAR (on Provably Secure Constructions)
- for DGA/CELAR (on ProVerif)
- for Hitachi (on a Hash Function)

PhD Fundings
- CIFRE with Orange Labs, Gemalto, and Thales
- Funding from EADS, the Fondation EADS
- Funding from DGA, INRIA, Ministry
Provable Security

- Granted the ANR BEST (2010–2013) with Nagra and Thales (Pay-TV)
  → **Broadcast Encryption and Traitor Tracing**
    - clean security models
    - new schemes with Trace & Revoke properties

- Granted the new ANR PRINCE (2011–2014) with Oberthur and Gemalto (smart-cards)
  → **Enhancement of the security models**
    - to consider leakage of information (side-channel attacks)
    - new models
    - generic countermeasures

- New tools and new primitives
  → **Pairing-based cryptography**
  → **Lattice-based cryptography**
Granted the ANR ProSe (2011–2014), with SECSI, CASSIS and VERIMAG

Automate proofs

- at the symbolic level (improving ProVerif)
- at the computational level (improving CryptoVerif)
- at the implementation level
  - generate implementations from specifications
  - From a specification proven with CryptoVerif
  - A proven compiler generates the implementation

→ application to Kerberos, TLS, etc
Cryptanalysis

Lattices

Further study of lattice algorithms
- from the theoretical point of view
- from the experimental point of view
- investigate the parallelization

Specific Instances

If new families (like multivariate cryptography proposed)
→ ready to study (break?) any new problem
## Symmetric Cryptography

### Hash Functions
From the SHA-3 competition: new interesting designs
- new proof techniques
- new classes of attacks

### Block Ciphers
Since the AES selection, many constructions use AES
- new automatic tool to derive attacks
- side-channel attacks
- algebraic attacks