

Équipe : Cryptographie
Responsable : David Pointcheval

Date de création : 1988

Établissements partenaires

- ENS – Ecole normale supérieure
- CNRS – Centre national de la recherche scientifique
- INRIA – Institut national de recherche en informatique et automatisme

1 Composition de l'équipe

Au 1er janvier 2008

Nom	Prénom	Fonction	Établissement	Date d'arrivée dans l'équipe
ABDALLA	Michel	Chercheur - CR1 Post-doctorant	CNRS CNRS puis ENS	01/10/05 01/08/03
BOUILLAGUET	Charles	Doctorant	ENS Cachan	01/10/07
CHEVALIER	Céline	Doctorant	ENS Cachan	01/10/06
DE CANNIÈRE	Christophe	Post-doctorant	ENS	01/10/07
FOUQUE	Pierre-Alain	Enseignant-chercheur – MdC	ENS	01/09/03
FUSCHBAUER	Georg	Doctorant	ENS	01/10/06
GAMA	Nicolas	Doctorant	Univ. Paris 7	01/10/05
HUFSCMITT	Emeline	Post-doctorant	ENS	01/12/07
IZABACHENE	Malika	Doctorant	Univ. Paris 7	01/10/06
LEURENT	Gaëtan	Doctorant	DGA	01/10/06
LEVIEIL	Eric	Doctorant	DGA	01/10/05
NACCACHE	David	Enseignant-chercheur – PU2	Univ. Paris 2	01/09/05
NGUYEN	Phong	Chercheur – CR1	CNRS	01/10/00
POINTCHEVAL	David	Chercheur – DR2	CNRS	01/10/98
VERGNAUD	Damien	Enseignant-chercheur – MdC	ENS	01/10/07
VUILLEMIN	Jean	Enseignant-chercheur – PU CE	ENS	01/01/08
ZIMMER	Sébastien	Doctorant	DGA	01/10/05

Autres permanents entre 2004 et 2008

Nom	Prénom	Fonction	Établissement	Date d'arrivée dans l'équipe	Date de départ de l'équipe
CATALANO	Dario	Chercheur – CR2	CNRS	01/10/03	30/09/06
GRANBOULAN	Louis	Enseignant-chercheur – MdC	ENS	01/09/98	30/08/06
STERN	Jacques	Enseignant-Chercheur - PU CE	ENS	01/09/93	31/08/07

2 Thématique scientifique de l'équipe

Cryptographic algorithms are the equivalent of locks, seals, security stamps and identification documents on the Internet. They are essential to protect our on-line bank transactions, credit cards, medical and personal information and to support e-commerce and e-government. They come in different flavors. Encryption algorithms are essential to

protect sensitive information such as medical data, financial information and Personal Identification Numbers (PINs) from prying eyes. Digital signature algorithms (in combination with hash functions) replace hand-written signatures in electronic transactions. A similar role can be played by MAC algorithms. Identification protocols allow to securely verify the identity of the party at the other end of the line. Therefore, cryptology is a research area with a high strategic impact for industries, individuals, and for the society as a whole.

Our research activity addresses the following topics, which cover almost all the domains that are currently active in the international cryptographic community :

1. Design and provable security, for
 - signature schemes
 - public-key encryption schemes
 - identity-based encryption schemes
 - key agreement protocols
 - group-oriented protocols
2. Attacks, using
 - side-channels
 - algebraic techniques
3. Design and analysis of symmetric schemes

3 Principaux résultats obtenus sur la période 2004-2008

Foundation

Finding Short Lattice Vectors Within Mordell's Inequality, STOC '08.

The shortest vector problem (SVP) in a lattice is a famous NP-hard problem of interest to both public-key cryptography and public-key cryptanalysis. Despite its importance, extremely few algorithms are known. This article presents the best polynomial-time algorithm known for approximating SVP. The algorithm, called slide reduction, has a natural interpretation : it can be viewed as an algorithmic version of a mathematical inequality proved by Mordell back in 1944.

The first polynomial-time algorithm for approximating SVP is the celebrated LLL algorithm, published by Lenstra, Lenstra and Lovász in 1982, and referenced by thousands of articles since : the historical applications of LLL were integer programming in fixed dimension, factoring polynomial with rational coefficients, and Diophantine approximation. The LLL algorithm is arguably best described as an algorithmic version of a mathematical inequality discovered by Hermite in 1850, which proved the existence of a constant related to lattice packings, now known as Hermite's constant. The principles and the worst-case output quality of the LLL algorithm are tightly related to Hermite's inequality.

In 1944, Mordell found a simple generalization of Hermite's inequality, which gave rise to better upper bounds on Hermite's constant. This article presents the first true algorithmic analogue of Mordell's inequality : the algorithm is to Mordell's inequality what LLL is to Hermite's inequality. As such, the new algorithm can be viewed as the "right" blockwise generalization of the LLL algorithm. Furthermore, it is simpler than previous blockwise generalizations of LLL, and a tight worst-case analysis is known.

Cryptanalysis

Learning a Parallelepiped : Cryptanalysis of GGH and NTRU Signatures, EUROCRYPT '06.

In 1997, Goldreich, Goldwasser and Halevi proposed a simple digital signature scheme based on lattice problems. This signature scheme was later optimized in 2001 for NTRU lattices, which gave rise to the efficient NTRU signature scheme, under consideration by the IEEE P1363 standardization body.

This article presents the first practical attack against the GGH signature scheme and the NTRU signature scheme. Besides being very efficient in practice (400 signatures are sufficient to disclose the signer's secret key within a few hours), the attack can be proved, which is not so frequent in cryptanalysis : there is a polynomial-time key-recovery

attack using only a polynomial number of random signatures. Interestingly, the attack introduces new techniques in public-key cryptanalysis. While the schemes attacked are based on lattices, the attack almost never uses lattices, except in the last stage : it is based on statistics and techniques from principal component analysis. More precisely, the attack transforms the key-recovery problem induced by the disclosure of random signatures into a multivariate optimization problem ; and because the multivariate function is here relatively simple, it is possible to provably solve this optimization problem by a well-chosen gradient descent.

Cryptanalysis of SFLASH with Slightly Modified Parameters, EUROCRYPT '07.

Practical Cryptanalysis of SFLASH, CRYPTO '07.

Key Recovery on Hidden Monomial Multivariate Schemes, EUROCRYPT '08.

Multivariate cryptography is a field of public-key cryptography which provides alternative schemes to RSA or Discrete-Log based schemes. The advantages of these schemes are two-folded : they are extremely fast, even on low power devices since no cryptographic coprocessor is needed ; and their security is related to a problem for which no quantum polynomial time algorithm is known. In 2003, the NESSIE project thus recommended the SFLASH signature scheme as a good scheme with high security level. This scheme has been proposed by Patarin, Goubin and Courtois in 2001. In multivariate cryptography, the public key is a system of multivariate polynomials over a small finite field. To sign a message with SFLASH, a trapdoor allows the legitimate user to invert the system, while the verification is very easy since it only requires to evaluate the system. The crypto team of the ENS proposed in 2007 two attacks against SFLASH. These attacks are very efficient in practice since they require 3 minutes to break the parameters. The attacks allow an adversary to find a signature for any message. They only use linear and bilinear algebra and are based on some properties of the differential functions associated to the system of the public key. Studying the differential functions has also been proposed by the crypto team in 2005 and allowed to cryptanalyze an encryption scheme whose security is related those of the SFLASH signature scheme. Finally, these attacks were recently extended and allow to recover equivalent secret keys on SFLASH and on other traitor tracing schemes based on other multivariate problems.

New Primitives

Unidirectional chosen-ciphertext secure proxy re-encryption, PKC '08.

Tracing malicious proxies in proxy re-encryption, Pairing '08.

Anonymous Proxy Signatures, SCN '08.

In 1998, Blaze, Bleumer and Strauss put forth a cryptographic primitive, termed *proxy re-encryption*, whose goal is to securely enable the translation of ciphertexts from one party to another. In such systems, a proxy transforms – without being able to infer any information on the corresponding plaintext – a ciphertext computed under Alice’s public key into one that can be opened using Bob’s secret key. Recently, the ENS Crypto Team has focused its research on delegation of rights : proxy re-encryption, as described above, and proxy signatures, which is the analogous delegation property for the signing rights. We furthermore studied anonymity and traceability. It thus shows some links with the group-oriented cryptography, such as group signature and broadcast encryption :

Dynamic Fully Anonymous Short Group Signatures, Vietcrypt '06.

Dynamic Threshold Public-Key Encryption, CRYPTO '08.

These two papers deal with efficient schemes which allow for some groups to sign or to decrypt documents. Dynamism is also an important property in practice : the users can dynamically join the system (by opposition to static systems), authorized people in the groups can evolve dynamically too.

Searchable Encryption Revisited : Consistency Properties, Relation to Anonymous IBE, and Extensions.

Journal of Cryptology, 2008.

There has recently been interest in various forms of “searchable encryption” in the literature. In this paper, we further explore one of the variants of this goal, namely public-key encryption with keyword search (PEKS) as introduced by Boneh, Di Crescenzo, Ostrovsky and Persiano in Eurocrypt 2004. A PEKS scheme allows the owner of a secret decryption key to give away pieces of trapdoor information based on this key that allows a third party to check whether a certain keyword is encrypted in a given ciphertext, without leaking any other information about the encrypted message however. The main application of PEKS schemes is to allow the intelligent routing of encrypted email containing

certain keywords over a low-bandwidth connection. The user sends the trapdoor corresponding to the keyword to the mail server, who can then independently check encrypted emails for presence of that keyword.

In this paper, we identify and fill some gaps with regard to consistency (the extent to which false positives are produced) for PEKS. We define computational and statistical relaxations of the existing notion of perfect consistency, show that the scheme of Boneh et al. in Eurocrypt 2004 is computationally consistent, and provide a new scheme that is statistically consistent. We also provide a transform of an anonymous identity-based encryption (IBE) scheme to a secure PEKS scheme that, unlike the previous one, guarantees consistency. Finally, we suggest three extensions of the basic notions, namely anonymous hierarchical identity-based encryption, public-key encryption with temporary keyword search, and identity-based encryption with keyword search.

Hardware

Alien vs. Quine, the Vanishing Circuit and Other Tales from the Industry's Crypt, 2006.

This work deals with the following question : is it possible, simply interacting with a hardware platform as a black-box, to determine exactly which software is under use ? This is not a trivial problem, since there are many ways to simulate the behavior of a software, such as a malware that does exactly the same thing, excepted in very specific cases. With an appropriate model of the machine, by measuring the execution time, one can make a correct decision.

4 Objectifs scientifiques 2009-2011

From the current state-of-the-art of cryptography, several issues are clearly identified as major problems to be tackled as soon as possible. We list some of them, and we will explain later which one we will address, why, and how.

Symmetric Primitives

- **Hash Functions.** Since the previous section just ended on this topic, we start with it for the major problems to address within the next 5 years. A NIST competition on hash functions has just started (the call has been sent November 2nd, 2007). In the first step, cryptographers will have to build and analyze their own candidate ; in a second step, cryptanalysts will be solicited, in order to analyze and break all the proposals. The conclusion is planned for 2012.

However, the main problem for hash functions is to identify the required security properties. Since they are used for many purposes, too many properties are often implicitly assumed, but not clearly stated, and clearly not satisfied. A lot of work has thus to be done on this topic of hash functions.

- **Stream Ciphers.** Right after the selection of AES, research on block ciphers decreased : a strong block cipher is now available, with various security levels. However, AES does not solve the whole symmetric encryption problem, since encrypting streams of data, audio, video, etc requires *stream ciphers*. Modes of operation can of course be used, but they are often too costly. The eStream project has thus been launched by ECRYPT, and closed mid-2008 with 8 selected schemes. However, it is not clear whether the problem is really closed too : as shown with the SFLASH recommendation, security analysis is still important. Stream ciphers remain a major issue in cryptography.

Confidentiality

- **Anonymity and Privacy.** Even if cryptography has been famous for addressing the problems of authenticity and confidentiality, by now, one of the main concerns of people is *privacy*. How can we live in this digital world, with bigger and bigger databases, really taking advantage of them, without the threat of “big brother”. Privacy and anonymity is thus one of the main challenges for the next years.
- **Copyright Protection.** Similarly to the privacy concern, the digital world makes easy the large-scale diffusion of information. But in some cases, this can be used in violation of some copyrights.

Cryptography should help at solving this problem, which is actually two-fold : one can either mark the original document in order to be able to follow the distribution (and possibly trace the traitor who illegally made it public) or one can publish information in an encrypted way, so that authorized people only can access it.

Password-based Cryptography

To be used in practice, cryptography must be efficient on both the machine and the user points of view. Computational cost has been a major concern for a long time, with various successes. This is still important to keep efficiency in mind. However, the security of the system is at most that of the weakest part. And this weakest part is quite often the human being : if intricate techniques have to be used, he will not use them.

Password-based cryptography can provide a good trade-off, if well specified. Of course, we cannot expect the same security as with a 128-bit secret key, but reasonable security levels can be reached, even with small passwords, easily memorable by users.

Cryptanalysis

As already explained, even with the *provable security* concept, cryptanalysis is still an important area, and attacks can be done at several levels. Algebraic tools (against integer factoring, discrete logarithm, polynomial multivariate systems, lattice reduction, etc) have thus to be studied and improved in order to further evaluation of the actual security level of cryptographic schemes.

At the hardware level, side-channel information has to be identified (time, power, radiation, noise, heat, etc) in order to securely protect embedded systems. But such an information may also be used in a positive way. . . .

5 Enseignement et Encadrement

Enseignements pour la période 2004-2008

Cours de niveau au moins égal à M1

Enseignant	Niveau	Titre court	Établissement	Volume Horaire	Nb années
Pierre-Alain Fouque	M1	Introduction à la cryptologie	ENS Ulm	16	4
Louis Granboulan	M2	Cryptographie symétrique	MPRI/ENS	12	4
David Naccache	M2	Sécurité informatique	Paris II	20	3
David Naccache	M2	Sécurité informatique	ENSMSE	20	3
Phong Nguyen	M1	Introduction à la cryptologie	EPITA	50	7
Phong Nguyen	M2	Réseaux euclidiens et applications en cryptographie	MPRI/ENS	6	4
David Pointcheval	M2	Cryptographie asymétrique	MPRI/ENS	12	4
David Pointcheval	M2	Cryptographie	Master SIS/ESIEA	12	4
Jacques Stern	M1	Introduction à la cryptologie	ENS Ulm	12	4

Thèses soutenues dans la période 2004-2008

Nom / Prénom	Date de Soutenance	Établissement	École Doctorale	Encadrant	Situation Actuelle
Martinet Gwenaëlle	03/11/2004	ENS	ED Paris Centre	Jacques Stern	Ministère Défense
Phan Duong Hieu	16/09/2005	ENS	ED Paris Centre	David Pointcheval	Univ. Paris 8
Chevallier-Mames Benoît	16/11/2006	ENS	ED Paris Centre	David Pointcheval	DCSSI
Duc Guillaume	17/09/2007	ENST Bretagne	ED Paris Centre	Jacques Stern	Orange Labs
Dubois Vivien	27/09/2007	ENS	EDX	Jacques Stern	DGA/CELAR
Kunz-Jacques Sébastien	27/09/2007	ENS DCSSI	ED Paris Centre	David Pointcheval	HSBC
Berbain Côme	26/10/2007	Orange Labs	ED Paris Centre	Jacques Stern	Orange Labs

HdR soutenues dans la période 2004-2008

Nom / Prénom	Date de Soutenance	Établissement	École Doctorale	Encadrant
Naccache David	13/12/2004	Gemplus	ED Paris Centre	Jacques Stern
Coron Jean-Sébastien	30/03/2006	Univ. Luxembourg	ED Paris Centre	Jacques Stern
Nguyen Phong	23/11/2007	ENS/CNRS	ED Paris Centre	Jacques Stern
Chabanne Hervé	27/03/2008	SAGEM	ED Paris Centre	Jacques Stern

Post-doctorants accueillis dans la période 2004-2008

Nom	Période	Établissement d'origine
Ivan Visconti	octobre 2003 – septembre 2004	Salerno Univ., Italie
Gilles Piret	juin 2005 – novembre 2007	UC Louvain, Belgique
Gregory Neven	octobre 2005 – octobre 2006	KULeuven, Belgique
Christopher Wolf	décembre 2005 – septembre 2006	KULeuven, Belgique
Krzysztof Pietrzak	janvier 2006 – décembre 2006	ETH Zurich, Suisse
Qiang Tang	octobre 2006 – septembre 2007	Royal Holloway, Londres, UK
De Cannière Christophe	octobre 2007 – septembre 2008	KULeuven
Hufschmitt Emeline	décembre 2007 – juin 2008	Univ. Caen
Dunkelman Orr	avril 2008 – mars 2009	KULeuven

6 Collaborations internationales avec publications conjointes

- M. Abdalla, J.-M. Bohli, M. I. Gonzalez Vasco and R. Steinwandt. *(Password) authenticated key establishment : From 2-party to group*. TCC '07, pages 499–514. Springer-Verlag, Berlin, 2007.
- M. Abdalla, E. Bresson, O. Chevassut, B. Moeller and D. Pointcheval. *Provably Secure Password-Based Authentication in TLS*. ASIACCS '06, pages 35–45. ACM Press, 2006.
- E. Andreeva, C. Bouillaguet, P.-A. Fouque, J. J. Hoch, J. Kelsey, A. Shamir and S. Zimmer. *Second Preimage Attacks on Dithered Hash Functions*. EUROCRYPT '08, pages 270–288. Springer-Verlag, Berlin, 2008.
- E. Biham, L. Granboulan and P. Q. Nguyen. *Impossible Fault Analysis of RC4 and Differential Fault Analysis of RC4*. FSE '05, pages 359–367. Springer-Verlag, Berlin, 2005.
- D. Coppersmith, N. Howgrave-Graham, P. Q. Nguyen and I. E. Shparlinski. *Testing set proportionality and the Ádám isomorphism of circulant graphs*. *J. Discrete Algorithms*, 4(2) :324–335, 2006.
- E. Fujisaki, T. Okamoto, D. Pointcheval and J. Stern. *RSA-OAEP is Secure under the RSA Assumption*. *Journal of Cryptology*, 17(2) :81–104, 2004.

- N. Gama, N. Howgrave-Graham, H. Koy and P. Q. Nguyen. *Rankin's Constant and Blockwise Lattice Reduction*. CRYPTO '06, pages 112–130. Springer-Verlag, Berlin, 2006.
- B. Libert and D. Vergnaud. *Unidirectional chosen-ciphertext secure proxy re-encryption*. PKC 2008, pages 360–379. Springer-Verlag, Berlin, 2008.
- D. Naccache, N. Smart and J. Stern. *Projective Coordinates Leak*. EUROCRYPT '04, pages 257–267. Springer-Verlag, Berlin, 2004.
- P. Q. Nguyen and O. Regev. *Learning a Parallelepiped : Cryptanalysis of GGH and NTRU Signatures*. EUROCRYPT '06, pages 215–233. Springer-Verlag, Berlin, 2006.

7 Logiciels et Brevets

Logiciels

Néant

Brevets

- Hervé Chabanne, Julien Bringer, David Pointcheval, and S. Zimmer. *Génération et utilisation d'une clé biométrique*, Patent in France FR0760311, December 2007.
- Emmanuel Bresson, Olivier Chevassut, and David Pointcheval, *Cryptography for secure dynamic group communications*, Patent in the USA, N° 0157874, July 2005.

8 Principaux Contrats

Avec partenaire industriel

- **ECRYPT : Network of Excellence in Cryptology.**
From February 2004 to July 2008.
The ECRYPT research roadmap is motivated by the changing environment (evolving toward ambient intelligence) and threat models in which cryptology is deployed, by the gradual erosion of the computational difficulty of the mathematical problems on which cryptology is based, by the need of strong foundations in the watermarking area and by the requirements of new applications and cryptographic implementations.
The main objective of ECRYPT is to ensure a durable integration of European research in both academia and industry and to maintain and strengthen the European excellence in these areas.
There are five virtual labs that focus on the following core research areas : symmetric key algorithms (STVL), public key algorithms (AZTEC), protocols (PROVILAB), secure and efficient implementations (VAMPIRE), and watermarking (WAVILA).
ENS leads the AZTEC virtual lab and the ECRYPT strategic committee.
- **BACH : Biometric Authentication with Cryptographic Handling.**
From November 2005 to October 2009.
Partners : Sagem, Cryptolog.
This project studies how to combine biometric data and cryptographic protocols, in order to preserve privacy.
- **SAPHIR (Sécurité et Analyse des Primitives de Hachage Innovantes et Récentes) : Security and analysis of innovating and recent hashing primitives.**
From November 2005 to October 2008.
Partners : France Telecom R&D, Gemalto, DCSSI, Cryptolog.
This project aims at improving recent attacks against hash functions, but also at designing new (provably secure) hash functions.
- **SAVE (Sécurité et Audit du Vote Electronique) : Security and audit for electronic voting.**
From December 2006 to June 2010.
Partners : France Telecom R&D, GET/ENST, GET/INT, Supélec, Cryptolog.

*This project extends an earlier **Crypto++** project, but for electronic voting only, and at a larger scale : not only the security at the cryptographic level will be considered (validity of the computations, correctness of the ballot, anonymity, etc) but also at the network level (infrastructure, etc).*

– **PACE : Pairings and Advances in Cryptology for E-cash.**

From December 2007 to November 2011.

Partners : France Telecom R&D, NXP, Gemalto, CNRS/LIX (TANC), Univ. Caen, Cryptolog.

This project aims at studying new properties of groups (similar to pairings, or variants), and then to exploit them in order to achieve more practical e-cash systems.

– **PAMPA : Password Authentication and Methods for Privacy and Anonymity.**

From December 2007 to November 2011.

Partners : EADS, Cryptolog.

One of the goals of this project is to improve existing password-based techniques, not only by using a stronger security model but also by integrating one-time passwords (OTP). This could avoid for example having to trust the client machine, which seems hard to guarantee in practice due the existence of numerous viruses, worms, and Trojan horses. Another extension of existing techniques is related to group applications, where we want to allow the establishment of secure multicast networks via password authentication. Several problems are specific to this scenario, such as dynamicity, robustness, and the random property of the session key, even in the presence of dishonest participants.

Finally, the need for authentication is often a concern of service providers and not of users, who are usually more interested in anonymity, in order to protect their privacy. Thus, the second goal of this project is to combine authentication methods with techniques for anonymity in order to address the different concerns of each party. However, anonymity is frequently associated with fraud, without any possible pursuit. Fortunately, cryptography makes it possible to provide conditional anonymity, which can be revoked by a judge whenever necessary. This is the type of anonymity that we will privilege.

Sans partenaire industriel

- For CELAR : Centre d'Electronique de l'Armement.

Provable security of cryptosystems.

From January 2007 to December 2008.

The goal of the contract is to make a survey on the methods and techniques used in provable security, for both cryptographic primitives and protocols.

- For France Telecom R&D.

CIDRE (Cryptographie Interactive et Dynamique des Réseaux) : Interactive cryptography and dynamic networks.

From June 2004 to May 2007.

In this project, we study interactive protocols which involve groups : group signatures, group key exchange, broadcast encryption.

- **ACI Cryptography – NFS : New functionalities for signature.**

From January 2002 to December 2004.

In this project, we worked on various kinds of signature schemes (group signatures, ring signatures, etc.).

- **ACI Security – CESAM (les Courbes Elliptiques pour la Sécurité des Appareils Mobiles) : Elliptic curves for the security of mobile devices.**

From September 2003 to September 2006.

Partners : INRIA/TANC.

In this project, we studied how elliptic curves could be used to improve efficiency in cryptographic protocols.

- **ARA FORMACRYPT : Formal security proofs for cryptographic protocols.**

From January 2006 to December 2008.

Partners : INRIA/ABSTRACTION, INRIA/SECSI, INRIA/CASSIS.

The verification of cryptographic protocols is a very active research area. Most works on this topic use either the computational approach, in which messages are bit strings, or the formal approach, in which messages are

terms. The computational approach is more realistic but more difficult to automate. The goal of our project is to bridge the gap between these two approaches.

- **ARA CrySCoE (Cryptographie pour la Sécurité des Codes Embarqués) : Cryptography for the security of embedded systems.**

From January 2006 to December 2008.

Partners : UVSQ/Prism, Univ. Bordeaux I/LaBRI.

The goal of this project is to provide security and confidence to embedded systems : privacy of the code (obfuscation), integrity and authenticity of the code, security proof of correctness of the code (formal methods).

9 Éléments de Visibilité

- Jacques Stern – 2005 : Silver Medal of CNRS
- Jacques Stern – 2006 : Gold Medal of CNRS
- Jacques Stern – 2007 : RSA Award for Excellence in the Field of Mathematics

- Jacques Stern – 2005 : Fellow of the *International Association for Cryptologic Research (IACR)*

- Phong Nguyen – 2006 : Best Paper Award à EUROCRYPT

- David Pointcheval – 2008–2010 : Director of the Board of the *International Association for Cryptologic Research (IACR)*
- Jean Vuillemin – 2008–2011 : on the International Scientific Advisory Board of National ICT Australia.
- Jean Vuillemin – 2008–2010 : Chair of the Scientific Advisory Board of the Institute for Infocomm Research I2R in Singapore

- Phong Nguyen – 2007 : Program Chair of *LLL+25* (France)
- Phong Nguyen – 2006 : Program Chair of *VietCrypt* (Vietnam)
- David Pointcheval – 2006 : Program Co-Chair of *The 5th International Workshop on Cryptology and Network Security (CANS '06)* (China)
- David Pointcheval – 2006 : Program Chair of *The Cryptographers' Track - RSA Conference 2006* (California, USA)

- David Pointcheval : Editor-in-chief of the *International Journal of Applied Cryptography (IJACT)* – Inderscience Publishers

- Phong Nguyen : Associate Editor of the *Journal of Cryptology*
- Phong Nguyen : Associate Editor of the *Journal of Mathematical Cryptology*
- David Naccache : Associate Editor of *IEE Proceedings - Information Security* – Publishing & Inspec
- David Naccache : Associate Editor of *IEEE Security and Privacy*
- David Naccache : Associate Editor of *ACM Transactions on Information and System Security*
- David Naccache : Associate Editor of *Computers & Security Elsevier Advanced Technology* – Elsevier
- David Pointcheval : Associate Editor of *Information Processing Letters* – Elsevier
- David Pointcheval : Associate Editor of *IEE Proceedings - Information Security* – Publishing & Inspec
- Jean Vuillemin : on the board of 8 international journals

10 Publications Majeures

- Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi, *Searchable Encryption Revisited : Consistency Properties, Relation to Anonymous IBE, and Extensions*, Journal of Cryptology, 2008.

- Bruno Blanchet and David Pointcheval, *Automated Security Proofs with Sequences of Games*, CRYPTO '06, 2006.
- Dario Catalano, David Pointcheval, and Thomas Pornin, *Trapdoor-Hard-to-Invert Isomorphism and their Application to Password-based Authentication*, Journal of Cryptology, 2007.
- Vivien Dubois, Pierre-Alain Fouque, Adi Shamir, and Jacques Stern, *Practical Cryptanalysis of SFLASH*, CRYPTO '07, 2007.
- Pierre-Alain Fouque, Gaëtan Leurent, and Phong Q. Nguyen, *Full Key-Recovery Attacks on HMAC/NMAC-MD4 and NMAC-MD5*, CRYPTO '07, 2007.
- Eiichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval, and Jacques Stern, *RSA–OAEP is Secure under the RSA Assumption*, Journal of Cryptology, 2004.
- Nicolas Gama and Phong Q. Nguyen, *Finding Short Lattice Vectors within Mordell's Inequality*, STOC '08, 2008.
- David Naccache, Nigel Smart, and Jacques Stern, *Projective Coordinates Leak*, EUROCRYPT '04, 2004.
- Phong Q. Nguyen and Oded Regev, *Learning a Parallelepiped : Cryptanalysis of GGH and NTRU Signatures*, EUROCRYPT '06, 2006.
- Phong Q. Nguyen and Damien Stehlé, *Floating-Point LLL Revisited*, EUROCRYPT '05, 2005.