

## Benoît Chevallier-Mames

Secrétariat Général de la Défense Nationale, DCSSI/SDS/LCR,  
51, boulevard de la Tour-Maubourg, 75700 Paris - 07 SP France  
benoit.chevalliermames@gmail.com  
31, Single, French  
<http://bcm.crypto.free.fr>

# Cryptographer

## Supélec Master of Science, Ph.D. in Cryptology

### EDUCATION

#### Engineering School:

- 1997–2000** • **Master of Science at the École supérieure d'Électricité (SUPELEC)**, which is one of the French *grandes écoles*: courses include notably electrical and computer engineering.
- 1995–1997** • **Classes préparatoires aux grandes écoles**: special French preparatory classes which dispense undergraduate university-level education.
- 1995** • **Baccalauréat in Sciences**: Final diploma of French high school, with high honors (*Mention Bien*).

#### Ph.D. in Cryptology:

- 2003–2006** • **Ph.D. in computer science at the Université de Paris VII** with a speciality in cryptology, within the École normale supérieure and within the Gemplus/Gemalto Security Labs.
  - **Title:** Public key cryptography: Design and security proofs.
  - **Domain:** Computer science (algorithmics).
  - **Supervisor:** David Pointcheval (École normale supérieure and CNRS).
  - **Jury members:** Arnaud Durand (Université de Paris VII), Marc Girault (France Télécom R&D), Marc Joye (Thomson R&D), David Naccache (Université de Paris II) Adi Shamir (Weizmann Institute of Science, Israël) and Jacques Stern (École normale supérieure).

### PROFESSIONAL EXPERIENCE

#### Cryptologist at the DCSSI:

- 2007–...** • **Inspector of the DCSSI (Central Information Systems Security Division)**, the State's focal center for Information Systems Security, within the SGDN (Secretariat-General for National Defence):
  - **Research:** Primitive study, conception and proof of security.
  - **Security audit:** Analysis, proofs and cryptanalysis of public and secret algorithms.
  - **Advising:** Assist public and governmental services about security issues.
  - **Teaching:** Provide training in the CFSSI (Information Systems Security Training Center).

#### Engineering Work:

- 2000–2007** • **Security engineer in the Gemplus/Gemalto Security Labs (smartcards dealer):**
  - **Development:** Embedded cryptographical libraries for smartcards. Code optimization, countermeasure conception.
  - **Security:** Library security study, design of protections against physical attacks, including notably faults and side-channel analysis.
  - **Patents:** Several patents (17 at this day) that present new protections against physical attacks or new cryptographical primitives.
  - **Training:** Training of internal and external clients: public key cryptography concepts and protections of embedded cryptographical libraries.

## COMPETENCES

### **Security and Cryptography:**

- **Symmetric cryptography:** Basic notions and background.
- **Asymmetric cryptography:** Concepts, Paradigms, Signature and encryption schemes. Identification protocols. Primitives design and provable security.
- **Physical security of cryptographical devices:** Physical attacks (SPA, DPA, FA, DFA) and efficient protections.

### **Computer Science and Skills:**

- **Languages:** Assembly codes (on numerous chips, including Infineon, Philips, Samsung and Renesas), crypto-assembly codes, C.
- **Scripting:** Large use of script tools, notably via Cygwin.
- **Experience:** Development on various environments, from smartcards to PCs or Unix systems.
- **Technicity:** Code size optimization, limited memory consumption, speed improvement. Inclusion of physical attack countermeasures (notably fault attacks and side-channel analysis).
- **French:** mother tongue.
- **English:** good level.

## TEACHING ACTIVITIES

### **Teaching:**

- 2007-... • **Lessons in the CFSSI (Information Systems Security Training Center):** Several themes about public key cryptography.
- 2007 • **Lectures in cryptography at the University of Luminy:** Signature schemes, physical attacks.
- 2006-2007 • **Lectures in cryptography at the École des Mines de Gardanne** to graduate students: Bases, signature schemes, encryption schemes, identification protocols, provable security notions.

### **Former trainees:**

- 2007 • **Davide Alessio (University of Bordeaux, 5 months):** Cryptanalysis of hash functions of the SHA family.
- 2006 • **Johann Urvoy (University of Limoges, 5 months):** Development of an elliptic-curve cryptographical library. Study and making of countermeasures. Analysis and optimization of performances.
- 2005 • **Amine Dogui (ENSIMAG, 5 months):** Development of an RSA library, including on-board key generation. Design and development of countermeasures .

## ACADEMICAL ACTIVITIES

### **Cryptographic community:**

- 2004-... • Participation to program committees: CHES'04, ISH'05, CT-RSA'06 and FDTC'08.
- 2000-... • Sub-reviewer for several conferences or journals, including Asiacrypt'05,'06,'08, CHES'03,'05,'06,'07,'08, Crypto'05,'07, CT-RSA'04,'07, Eurocrypt'05,'07, ICALP'06, IEEE Transactions on Computers and PKC'02,'06,'07.
- 2003-... • Participation to the excellence network ECRYPT and to the French funded-projects CRYPTO++ and SAPHIR.

### **Seminars:**

- 2008 • **Cryptographic seminar in Caen, invited presentation:** "Linear Bandwidth Naccache-Stern Encryption".
- 2008 • **Cryptographic seminar in Rennes, invited presentation:** "Linear Bandwidth Naccache-Stern Encryption".
- 2007 • **Cryptographic seminar in Limoges, invited presentation:** "A practical and tightly secure signature scheme without hash function".
- 2006 • **Cryptographic seminar of the École normale supérieure:** Thesis defense.

## ACADEMICAL ACTIVITIES (continued)

- 2005 • **Cryptographic seminar in Caen, invited presentation:** “Un schéma de signature efficace basé sur le CDH avec une réduction fine”.

### Conference talks:

- 2006 • **PKC:** “Encoding-free ElGamal encryption without random oracles”.
- 2005 • **ACNS:** “New signature schemes with coupons and tight reduction”.
- **ACNS:** “Optimal asymmetric encryption and signature paddings”.
- **Crypto:** “An efficient CDH-based signature scheme with a tight security reduction”.
- 2004 • **CT-RSA:** “Self-randomized exponentiation algorithms”.
- 2003 • **CHES:** “Faster double-size modular multiplication from euclidean multipliers”.

## LIST OF PUBLICATIONS

### Conference Proceedings

- 2008 • Benoît Chevallier-Mames and David Naccache and Jacques Stern. Linear Bandwidth Naccache-Stern Encryption. In *Security and Cryptography for Networks - SCN 2008*, to appear.
- 2007 • Benoît Chevallier-Mames and Marc Joye. A practical and tightly secure signature scheme without hash function. In *Topics in Cryptology - CT-RSA 2007*, pages 339-356.
- Guilhem Castagnos et Benoît Chevallier-Mames. Towards a DL-based additively homomorphic encryption scheme. In *Information Security Conference - ISC 2007*, pages 362-375.
- 2006 • Éric Brier, Benoît Chevallier-Mames, Mathieu Ciet and Christophe Clavier. Why one should secure its public elements. In *Cryptographic Hardware and Embedded Systems - CHES 2006*, pages 324-338.
- Benoît Chevallier-Mames, Pascal Paillier and David Pointcheval. Encoding-free ElGamal encryption without random oracles. In *Public Key Cryptography - PKC 2006*, pages 91-104.
- 2005 • Benoît Chevallier-Mames. An efficient CDH-based signature scheme with a tight security reduction. In *Advances in Cryptology - CRYPTO 2005*, pages 511-526.
- Benoît Chevallier-Mames. New signature schemes with coupons and tight reduction. In *Applied Cryptography and Network Security - ACNS 2005*, pages 513-528.
- Benoît Chevallier-Mames, Duong Hieu Phan and David Pointcheval. Optimal asymmetric encryption and signature paddings. In *Applied Cryptography and Network Security - ACNS 2005*, pages 254-268.
- 2004 • Benoît Chevallier-Mames. Self-randomized exponentiation algorithms. In *Topics in Cryptology - CT-RSA 2004*, pages 236-249.
- Benoît Chevallier-Mames, David Naccache, Pascal Paillier and David Pointcheval. How to disembed a program? In *Cryptographic Hardware and Embedded Systems - CHES 2004*, pages 441-454.
- 2003 • Benoît Chevallier-Mames, Marc Joye and Pascal Paillier. Faster double-size modular multiplication from euclidean multipliers. In *Cryptographic Hardware and Embedded Systems - CHES 2003*, pages 214-227.

### Journals

- 2004 • Benoît Chevallier-Mames, Mathieu Ciet and Marc Joye. Low-cost solutions for preventing simple side-channel analysis: Side-channel atomicity. *IEEE Trans. Computers*, 53(6):760-768.

### Thesis

- 2006 • Benoît Chevallier-Mames. *Cryptographie à clé publique: Constructions et preuves de sécurité* (Public key cryptography: Design and security proofs). Ph.D. thesis (in French), Université de Paris VII.

## PERSONAL INTERESTS

---

- 1992-... • **Table tennis:** Player and former trainer, at a regional level.
- 2001-... • **Viet Vo Dao** (Vietnamese martial art ): Practise and treasury of the club. Black belt (first dan).