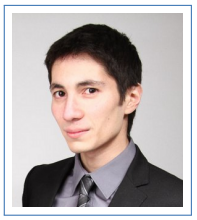
Luk Bettale

PhD in Computer Science

5 rue de la Vega
75012 Paris, France
+33 625 648 117
luk.bettale@protonmail.com



Cryptography, Security, Embedded Systems

Education

2008–2011 **PhD in Computer Science**, *Univ. Pierre et Marie Curie - EDITE*, Paris, France.
Cryptography and computer algebra. Funded by DGA/MRIS (french secretary of defense).
PhD defended October 3rd, 2011 *with honors*.

2006–2008 **Master in Computer Science**, *Univ. Pierre et Marie Curie - MPRI*, Paris, France.
Software Science and Technology.

2005–2006 **Bachelor in Computer Science**, *Univ. Pierre et Marie Curie*, Paris, France.

Experience

current position **R&D Senior Engineer**, *IDEMIA*, Colombes, France.
- Secure implementation of cryptographic algorithms for embedded systems (smart cards),
- Security analysis against Side-Channel Attacks,
- Lectures for graduate students.

2008–2011 **PhD candidate**, *Laboratoire d'Informatique de Paris 6*, Paris, France.
Algebraic cryptanalysis: tools and applications. Advisors: Jean-Charles Faugère and Ludovic Perret.
- Conception of algorithms for solving polynomial systems over finite fields,
- Algebraic modeling of hash functions (MD5, SHA-1, SHA-2...),
- Cryptanalysis of asymmetric multivariate cryptosystems (HFE, UOV...),
- Development of a software framework for algebraic cryptanalysis.

2008–2011 **Teaching Assistant**, *Université Pierre et Marie Curie*, Paris, France.
- Object oriented programming (Java) 42h
- Development Environment (Bash, Emacs, Make, gcc, gdb, cvs, svn...) 90h
- Machine and representation (MIPS assembly) 14h
- Scientific Computing (C, Maple) 49h

Apr.–Aug. 2008 **Master 2 internship (5 months)**, *Laboratoire d'Informatique de Paris 6*, Paris, France.
Implementation of algebraic attacks against hash functions.

Jul.–Aug. 2007 **Master 1 internship (2 months)**, *Laboratoire d'Informatique de Paris 6*, Paris, France.
Study and implementation of a multivariate cryptosystem (TRMS).

Computer skills

programming	C, Java, C++, Bash, Perl, Lisp...	system	GNU/Linux, POSIX systems
assembly	x86, 8051, ARM, MIPS...	embedded	JavaCard, ISO7816
comp. algebra	Magma, Maple, Sage	software	Emacs, Eclipse, LaTeX, GIT...

Languages

French	Native	
English	Fluent	*papers and communications in international conferences*
Japanese	Intermediate	*JLPT N4, frequent journeys in Japan*
Indonesian	Native	

Miscellaneous

Music electric/acoustic guitar

Sports savate french boxing, swimming, snowboarding.

Software

- Cryptography on smart cards (written in assembly, C)
- Smart card applets (written in JavaCard)
- Portable modular arithmetic and EC arithmetic library (written in C)
- 8051 assembler and virtual machine (written in C, lex+yacc)
- Framework for DPA simulation (written in C + Bash)
- Library for ANF to CNF conversion (written in C)
- Magma package for solving polynomial systems over finite fields (written in Magma)
- Framework for algebraic cryptanalysis (written in Bash + Magma)
- Emacs mode for editing Magma code (written in Emacs Lisp)
- Implementation of the NTRU cryptosystem (written in C)

Publications

L. Bettale, J. Coron, and R. Zeitoun, "Improved high-order conversion from boolean to arithmetic masking," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2018, no. 2, pp. 22–45, 2018.

L. Bettale, E. Dottax, and M. Ramphort, "Algebraic side-channel attacks on masked implementations of AES," in *ICETE (2)*, pp. 424–435, SciTePress, 2018.

L. Bettale, E. Dottax, L. Genelle, and G. Piret, "Collision-correlation attack against a first-order masking scheme for MAC based on SHA-3," in *COSADE*, vol. 8622 of *Lecture Notes in Computer Science*, pp. 129–143, Springer, 2014.

S. Belaïd, L. Bettale, E. Dottax, L. Genelle, and F. Rondepierre, "Differential power analysis of HMAC SHA-1 and HMAC SHA-2 in the hamming weight model," in *ICETE (Selected Papers)*, vol. 554 of *Communications in Computer and Information Science*, pp. 363–379, Springer, 2014.

L. Bettale, J. Faugère, and L. Perret, "Cryptanalysis of hfe, multi-hfe and variants for odd and even characteristic," *Des. Codes Cryptography*, vol. 69, no. 1, pp. 1–52, 2013.

S. Belaïd, L. Bettale, E. Dottax, L. Genelle, and F. Rondepierre, "Differential power analysis of HMAC SHA-2 in the hamming weight model," in *SECRYPT*, pp. 230–241, SciTePress, 2013.

L. Bettale, "Secure multiple sboxes implementation with arithmetically masked input," in *CARDIS*, vol. 7771 of *Lecture Notes in Computer Science*, pp. 91–105, Springer, 2012.

L. Bettale, J. Faugère, and L. Perret, "Solving polynomial systems over finite fields: improved analysis of the hybrid approach," in *ISSAC*, pp. 67–74, ACM, 2012.

L. Bettale, J. Faugère, and L. Perret, "Cryptanalysis of multivariate and odd-characteristic HFE variants," in *Public Key Cryptography*, vol. 6571 of *Lecture Notes in Computer Science*, pp. 441–458, Springer, 2011.

L. Bettale, J. Faugère, and L. Perret, "Hybrid approach for solving multivariate systems over finite fields," *J. Mathematical Cryptology*, vol. 3, no. 3, pp. 177–197, 2009.

L. Bettale, J. Faugère, and L. Perret, "Cryptanalysis of the TRMS signature scheme of pkc'05," in *AFRICACRYPT*, vol. 5023 of *Lecture Notes in Computer Science*, pp. 143–155, Springer, 2008.

L. Bettale, J. Faugère, and L. Perret, "Security analysis of multivariate polynomials for hashing," in *Inscrypt*, vol. 5487 of *Lecture Notes in Computer Science*, pp. 115–124, Springer, 2008.