

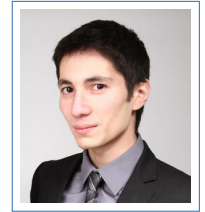
Luk Bettale

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**, *Oberthur Technologies*, 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. **Master 2 internship (5 months)**, *Laboratoire d'Informatique de Paris 6*, Paris, France.
2008 Implementation of algebraic attacks against hash functions.
- Jul.–Aug. **Master 1 internship (2 months)**, *Laboratoire d'Informatique de Paris 6*, Paris, France.
2007 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, L ^A T _E X, GIT...

Languages

French	Native		
English	Fluent		<i>papers and communications in international conferences</i>
Japanese	Intermediate		<i>JLPT N₄, frequent journeys in Japan</i>
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 ECC 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, E. Dottax, L. Genelle, and G. Piret, “Collision-correlation attack against a first-order masking scheme for MAC based on SHA-3,” in *Constructive Side-Channel Analysis and Secure Design - 5th International Workshop, COSADE 2014, Paris, France, April 13-15, 2014. Revised Selected Papers*, Springer, 2014.

S. Belaïd, L. Bettale, E. Dottax, L. Genelle, and F. Rondepierre, “Differential power analysis of HMAC SHA-2 in the hamming weight model,” in *SECURITY 2013 - Proceedings of the 10th International Conference on Security and Cryptography, Reykjavík, Iceland, 29-31 July, 2013*, SciTePress, 2013.

L. Bettale, “Secure simultaneous SBoxes implementation with arithmetically masked input,” in *Eleventh Smart Card Research and Advanced Application Conference – CARDIS 2012*, Springer, 2012.

L. Bettale, J.-C. Faugère, and L. Perret, “Solving polynomial systems over finite fields: Improved analysis of the hybrid approach,” in *International Symposium on Symbolic and Algebraic Computation – ISSAC 2012*, ACM, 2012.

L. Bettale, J.-C. Faugère, and L. Perret, “Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic,” *Design, Codes and Cryptography*, 2012.

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

L. Bettale, J.-C. Faugère, and L. Perret, “Hybrid approach: a tool for multivariate cryptography,” in *Proceedings of the ECRYPT Workshop on Tools for Cryptanalysis 2010*, pp. 15–23, ECRYPT II, 2010.

L. Bettale, J.-C. Faugère, and L. Perret, “Hybrid approach for solving multivariate systems over finite fields,” *Journal of Mathematical Cryptology*, vol. volume 3, no. issue 3, pp. 177–197, 2009.

L. Bettale, J.-C. Faugère, and L. Perret, “Security analysis of multivariate polynomials for hashing,” in *Information Security and Cryptology – INSCRYPT 2008*, vol. 5487 of *Lecture Notes in Computer Science*, Springer, 2008.

L. Bettale, J.-C. Faugère, and L. Perret, “Cryptanalysis of the TRMS signature scheme of PKC’05,” in *Progress in Cryptology – AFRICACRYPT 2008*, vol. 5023 of *Lecture Notes in Computer Science*, pp. 143–155, Springer, 2008.