Dahmun Goudarzi

PhD Candidate

34 rue de la Montagne Sainte-Genevieve
75005 Paris
+33 (0)6 40 40 74 39
dahmun.goudarzi@gmail.com

Education

2015 – 2018 **PhD in Cryptography**,
under supervision of Matthieu Rivain and Damien Vergnaud,
École Normale Supérieure de Paris, Paris.

2014 – 2015 **Master 2 in Cryptography (SFPN)**,
Université Pierre et Marie Curie, Paris.

2013 – 2014 **Master 1 in Science and Technology of Software Languages (STL)**,
Université Pierre et Marie Curie, Paris.

2012 – 2013 **Master 1 in Artificial Intelligence and Decision (IAD)**,
Université Pierre et Marie Curie, Paris.

July 2011 **Exchange program at Brown University, Rhodes Island**,
Initiation to machine learning and research.

2010 – 2012 **Computer Science and Maths Science**,
Université Pierre et Marie Curie, Paris.

Professional Experiences

2015 – Today **CryptoExperts**, *PhD Candidate*, Paris (France).
Worked on design and implementations of efficient and secure cryptography for embedded systems.

- Studied efficient decomposition of s-boxes with minimal multiplicative complexity leading to 2 publications at CHES (2016 and 2017).
- Studied the theoretical security of Boolean circuit against side-channel attackers.
- Developed efficient implementations in ARM assembly of several secure multiplications techniques leading to a publication at COSADE 2018.
- Analysed the practical security of Boolean circuit against correlation power attacks.

Proposed a lattice attack against a countermeasure for elliptic curve signature (published at SAC 2016).

2015 **CryptoExperts**, *Internship*, Paris (France).
5 months Efficient polynomial evaluation over finite fields and application to secure software implementations protected against side-channel attacks. Implementations in ARM assembly of the state-of-the-art and speed records for a secure AES with high order Boolean masking and bitslice strategy.
Published at Eurocrypt 2017.

2014 **Philips**, *Internship*, Eindhoven (Netherlands).
3 months Study and implementation (Java, C and AtMega) of a variant of the HIMMO key generation cryptosystem. Evaluation of the efficiency and integration to a project on Smart Cities.

2014 **Laboratoire Informatique de Paris 6 (LIP6)**, *Internship*, Paris.
1 month Study and implementation (C, magma) of the Bleichenbacher attack on ECDSA (Paper of CHES 2013)

2013 **Médiathèque du Musée du Quai Branly**, *Assistant*, Paris.
1 month Design of their internal website with Drupal. Secretary work.

2013 **Master 1 Project** , *Laboratoire Informatique de Paris 6 (LIP6)*.
3 months Construction of a data set of French words for "feelings" classification with machine learning.

2012 **Neoxia**, *Internship*, Paris.
1 month Management of primary problems on data base accessibility. Analysis and interpretation of source code.

2010 **Bundestag**, *Internship*, Berlin (Germany).
1 month Summary and analysis of the French actuality.

2006 and 2008 **Carwash**, *Checkout Operator*, Oceanside (CA-USA).
1 month

Personnal Skills

Languages	French (native), English (fluent), German (intermediate)
Programming	C, Java, Python, Sage, ARM v7, LaTeX, HTML
Formations	Cryptography, Linear algebra, Side-channel analysis and countermeasures

Major Software Developments

ARM v7 Assembly	Implementations of the state-of-the-art secure schemes for high order Boolean masking (from secure multiplication to secure block-ciphers such as AES and PRESENT). Implementations in bitslice of generic s-boxes and specific ones (AES, PRESENT) that achieved new speed records with high order Boolean masking.
C	Implementation of SURF, a code-based post-quantum signature, that fits NIST API for the standardization competition.
HTML	Websites for three workshops organized by CryptoExperts (WhiBox 2016, AWACS 2016, wr0ng 2017)

Publications

2018 **COSADE**, with Anthony Journault, Matthieu Rivain, and Francois-Xavier Standaert.
Secure Multiplication for Bitslice Higher-Order Masking : Optimisation and Comparison.

2017 **CHES**, with Matthieu Rivain, Damien Vergnaud, and Srinivas Vivek.
Generalized Polynomial Decomposition for S-boxes with Application to Side-Channel Countermeasures.

2017 **Eurocrypt**, with Matthieu Rivain.
How Fast Can Higher-Order Masking Be in Software ?

2016 **CHES**, with Matthieu Rivain.
On the Multiplicative Complexity of Boolean Functions and Bitsliced Higher-Order Masking.

2016 **SAC**, with Matthieu Rivain, and Damien Vergnaud .
Lattice Attacks against Elliptic-Curve Signatures with Blinded Scalar Multiplication.

Presentations

2018 **COSADE**, with Anthony Journault, Matthieu Rivain, and Francois-Xavier Standaert.
Singapore Secure Multiplication for Bitslice Higher-Order Masking : Optimisation and Comparison.

2017 **CHES**, with Matthieu Rivain, Damien Vergnaud, and Srinivas Vivek.
Tapei (Taiwan) Generalized Polynomial Decomposition for S-boxes with Application to Side-Channel Countermeasures.

2017 **Eurocrypt**, with Matthieu Rivain.
Paris (France) How Fast Can Higher-Order Masking Be in Software ?

2017 **Journees Codes et Cryptographie**, with Matthieu Rivain.
La Bresse (France) How Fast Can Higher-Order Masking Be in Software ?

2016 **CHES**, with Matthieu Rivain.
Santa-Barbara (USA) On the Multiplicative Complexity of Boolean Functions and Bitsliced Higher-Order Masking.