# Dahmun Goudarzi

*PhD Candidate*

*34 rue de la Montagne Sainte-Genevieve*
*75005 Paris*
*+33 (0)6 40 40 74 39*
*dahmun.goudarzi@gmail.com*
*31/01/1991*


## Educations

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 the University of Brown, Rhodes Island**,
Initiation to machine learning and research.

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

2009 – 2010 **Classe préparatoire, concentration in Mathematics and Physics (MPSI)**,
*Lycée Saint-Louis*, Paris.

2008 – 2009 **High school diploma**,
*Lycée Henri IV*, Paris.
European class (German)

## Professional Experiences

2015 – Today **CryptoExperts**, *PhD Candidate*, Paris (France).
Efficient and secure cryptographic implementations for embedded systems.

2015 **CryptoExperts**, *Internship*, Paris (France).
*5 months* Efficient polynomial evaluation over finite fields and application to secure software implementations protected against side-channel attacks.

2014 **Philips**, *Internship*, Eindhoven (Pays-Bas).
*3 months* Study and implementation (Java, C et 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* Rework of the intern website with Drupal. Secretary work.

2013 **Master 1 Project** , *Laboratoire Informatique de Paris 6 (LIP6)*.
*3 months* Construction of a data set based on the Internet for the classification of "feelings" in French language

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

2010 – 2014 **Mathematics Lesson for High School Students**, Paris.

2010 **Bundestag**, *Internship*, Berlin (Allemagne).
*1 month* Resume of the French actuality and article writing in german.

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

## Personnal Skills

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

## Publications

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

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.