

Matthieu Giraud

LIMOS (UMR 6138)
Campus Universitaire des Cézeaux
1 rue de la Chebarde
63178 Aubière, France

Phone: +33 473 407 440

Fax: +33 473 405 356

email: matthieu.giraud@uca.fr

URL: <http://sancy.univ-bpclermont.fr/~giraud/>

Born: January 30, 1987 – Fontenay-le-Comte, France

Nationality: French

Current position

PhD student in cryptography since October 2016 under the supervision of [Dr Pascal Lafourcade](#).
The subject of my thesis is the *Security of Data Numerisation and Storage*.

Research interests

I am interested in cryptography, privacy and everything in between and around these topics. I am currently working on privacy for the Cloud and particularly on *Symmetric Searchable Encryption*, *Private Polynomial Evaluation*, *Secure Distributed Computing* and *Watermarking* schemes.

Internships

- 2017 *Security of IoT Devices*, Pr Manik Lal Das, DI-IICT, Gandhinagar, India
2016 *Cryptanalysis of Symmetric Searchable Encryption (SSE) schemes*, Alexandre Anzala-Yamajako and Olivier Bernard, Thales Communications and Security, Gennevilliers, France

Education

- 2016 Master in Cryptography and IT Security, Université de Bordeaux, France
2014 Bachelor's Degree in Mathematics, Université de Nantes, France

Publications

INTERNATIONAL CONFERENCES

- BD “*Verifiable Private Polynomial Evaluation*” by Xavier Bultel, Manik Lal Das, Hardik Gajera, David Gérard, Matthieu Giraud, and Pascal Lafourcade. The 11th International Conference on Provable Security (ProvSec).
BCGL17 “*Secure Matrix Multiplication with MapReduce*” by Xavier Bultel, Radu Ciucanu, Matthieu Giraud, and Pascal Lafourcade. The 12th International Conference on Availability, Reliability and Security (ARES).

BBGL17 “*Formal Analyze of a Private Access Control Protocol to a Cloud Storage*” by Narjes Ben Rajeb, Mouhebeddine Berrima, Matthieu Giraud, and Pascal Lafourcade. The 14th International Conference on Security and Cryptography (SECRYPT).

ABGL17 “*Practical Passive Leakage-Abuse Attacks Against Symmetric Searchable Encryption*” by Alexandre Anzala-Yamajako, Olivier Bernard, Matthieu Giraud, and Pascal Lafourcade. The 14th International Conference on Security and Cryptography (SECRYPT).

Talks

INTERNATIONAL CONFERENCES

Oct. 2017 “*Verifiable Private Polynomial Evaluation*”. ProvSec, Xi’an, China, October 23, 2017.

Aug. 2017 “*Secure Matrix Multiplication with MapReduce*”. ARES, Reggio Calabria, Italy, August 29, 2017.

Jul. 2017 “*Formal Analyze of a Private Access Control Protocol to a Cloud Storage*”. SECRYPT 2017, Madrid, Spain, July 26, 2017.

Jul. 2017 “*Practical Passive Leakage-Abuse Attacks Against Symmetric Searchable Encryption*”. SECRYPT 2017, Madrid, Spain, July 26, 2017.

SEMINARS

Jan. 2017 “*Practical Passive Leakage-Abuse Attacks Against Symmetric Searchable Encryption*”. PhD students’ seminar, LIMOS, Université Clermont Auvergne (France), January 13, 2017.

Events

Jan. 2018 *Real World Crypto*. Zurich, Switzerland, January 10-12, 2018.

Dec. 2017 *Black Hat Europe Conference*. London, United Kingdom, December 4-7, 2017.

Jul. 2017 *Summer school on real-world crypto and privacy*. Sibenik, Croatia, July 5-9, 2017.

Teaching

2017-2018 Introduction to Computer Security
IUT Réseaux et Télécoms, Université Clermont Auvergne, France
Level: L3 | Language: French | Volume: 10h

Security Models
ISIMA, Université Clermont Auvergne, France
Level: M2 | Language: English & French | Volume: 24h

Security of Information Systems
Université Clermont Auvergne, France
Level: M2 | Language: French | Volume: 12h

2016-2017 Certificat Informatique et Internet (C2i)
Institut Universitaire de Formation Ergothérapie d’Auvergne, Université Clermont Auvergne, France
Level: Graduate | Language: French | Volume: 56h

Service to the profession

REVIEWING SERVICE

Conferences: AlgoTel'17 | ATC 2017 | C&SS'17 | PST 2017.

Organiser

I am involved in the organisation of the PhD students' seminar of the LIMOS.

Contribution

Sharing of TikZ codes on *TikZ for Cryptographers*.

Programming skills

Languages: C, GO, PARI/GP, PYTHON

Software: OCTAVE, MATLAB, SAGEMATH

Tools: L^AT_EX, EMACS, GIT

Others: HTML, REDIS, SSDB

Languages

French: Mother tongue

English: Fluent

Spanish: Notions