# 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/

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

2018 *Proof of Location*, Dr Rei Safavi-Naini, University of Calgary, Calgary, Canada (4 months)
2017 *Security of IoT Devices*, Pr Manik Lal Das, DI-IICT, Gandhinagar, India (1 month)
2016 *Cryptanalysis of Symmetric Searchable Encryption (SSE) schemes*, Alexandre Anzala-Yamajako and Olivier Bernard, Thales Communications and Security, Gennevilliers, France (6 months)

## 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

2018b *"Secure Grouping and Aggregation with MapReduce"* by Radu Ciucanu, Matthieu Giraud, Pascal Lafourcade, and Lihua Ye. The 15th International Conference on Security and Cryptography (SECRYPT).

2018a *"Security Analysis and Psychological Study of Authentication Methods with PIN Codes"* by Xavier Bultel, Jannik Dreier, Pascal Lafourcade, Marie Izaute, Matthieu Giraud, Dounia Lakhzoum, Ladislav Motak, Timothée Kheyrkhah, and Vincent Marlin. The 12th International Conference on Research Challenges in Information Science (RCIS).

2017d *"Verifiable Private Polynomial Evaluation"* by Xavier Bultel, Manik Lal Das, Hardik Gajera, David Gérault, Matthieu Giraud, and Pascal Lafourcade. The 11th International Conference on Provable Security (ProvSec).

2017c *"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).

2017b *"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).

2017a *"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

Jun. 2018 *Verifiable Private Polynomial Evaluation.* iCIS Group Talk, University of Calgary, Calgary (Canada), June 15, 2018.

Mar. 2018 *"How to search in an Encrypted Database?"*. Clermont'ech API Hour #34, Clermont-Ferrand (France), March 15, 2018.

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

# Events

Aug. 2018 *SAC Summer School and Conference.* Calgary, Canada, August 13-17, 2018.

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

2018-2019 Introduction to Computer Security
IUT Réseaux et Télécoms, Université Clermont Auvergne, France

Level: L3 | Language: French | Volume: 10h

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: FPS'18 | AlgoTel'18 | C&SS'18 | PST 2018 | 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: LaTeX, EMACS, GIT
Others: HTML, REDIS, SSDB

## Languages

French: Mother tongue
English: Fluent
Spanish: Notions