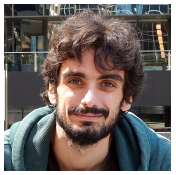
Matthieu Giraud

PhD student in cryptography



Address: 7 rue Barbançon, 63 000 Clermont-Ferrand, France
Phone: +33(0) 679.025.756
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. My research domain is the *cloud security*, in particular:

- Secure distributed computation
- Private verifiable delegation computation
- Searchable encryption

Internships

2018 *Verifiable Computation Delegation*, Pr Manik Lal Das, DI-IICT, Gandhinagar, India (3 weeks)
2018 *Proof of Location*, Pr 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 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

BCGL+18 *"Secure Joins with MapReduce"* by Xavier Bultel, Radu Ciucanu, Matthieu Giraud, Pascal Lafourcade, and Lihua Ye. The 11th International Symposium on Foundations & Practice of Security (FPS). Best Paper Award.

CGLY18 *"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).

BDLI+18 *"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).

BDGG+17 *"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).

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).

BGLR17 *"Formal Analyze of a Private Access Control Protocol to a Cloud Storage"* by Mouhebeddine Berrima, Matthieu Giraud, Pascal Lafourcade, and Narjes Ben Rajeb. 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).

Journal

ABGL18 *"No Such Thing As A Small Leak: Leakage-Abuse Attacks Against Symmetric Searchable Encryption"* by Alexandre Anzala-Yamajako, Olivier Bernard, Matthieu Giraud, and Pascal Lafourcade. Communications in Computer and Information Science series. [To appear]

BGLR18 *"Formal Analyze of a Private Access Control Protocol to a Cloud Storage"* by Mouhebeddine Berrima, Matthieu Giraud, Pascal Lafourcade, and Narjes Ben Rajeb. International Journal of Innovative Computing and Applications.

Popular science

G18 *"Protéger et utiliser ses données en ligne"* by Matthieu Giraud. Interstices.info.

Talks

International conferences

Nov. 2018 *"Secure Joins with MapReduce"*. FPS, Montréal, Canada, November 15, 2018.

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

Organizer

Oct. 2018 — *Fête de la science 2018.* Clermont-Ferrand, France, October 11, 2018.
Initiation to cryptography | High school students: 3 x 20 | Volume: 3 x 1 h 30

Apr. 2018 — *Clermont Innovation Week.* Clermont-Ferrand, France, April 23, 2018.
Workshop on GPG | Volume: 1 h

May 2018 — *Journée Informatique et Création Numérique.* Clermont-Ferrand, France, May 3, 2018.
Exploration teaching on cryptography with high school students | Volume: 3 x 1 h

Attender

Jan. 2019 — *Real World Crypto.* San Jose, USA, January 9-11, 2019.
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.

Administration collective

Reviewing service

Conferences: FPS'18 | AlgoTel'18 | C&SS'18 | PST 2018 | AlgoTel'17 | ATC 2017 | C&SS'17 | PST 2017.

Organizer

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

Contribution

Sharing of TikZ codes on *TikZ for Cryptographers*.

Teaching

2018-2019 — Introduction to Cryptography
IUT Réseaux et Télécoms, Université Clermont Auvergne, France
Students: 40 | Language: French | Volume: 10 h

Security Models
Master of Computer Science (M2), Université Clermont Auvergne, France
Students: 25 | Language: English | Volume: 12 h

Information Technology Security
Master of Computer Science (M2), UniversitĆlermont Auvergne, France
Students: 25 | Language: English | Volume: 12 h

2017-2018 — Introduction to Cryptography
IUT Réseaux et Télécoms, Université Clermont Auvergne, France
Students: 40 | Language: French | Volume: 10 h

Security Models
Master of Computer Science (M2), Université Clermont Auvergne, France
Students: 10 & 30 | Language: English & French | Volume: 2 x 12 h

Information Technology Security
Master of Computer Science (M2), Université Clermont Auvergne, France
Student: 30 | Language: English | Volume: 12 h

2016-2017 Certificat Informatique et Internet (C2i)
Institut Universitaire de Formation Ergothérapie d'Auvergne, Université Clermont Auvergne, France
Students: 2 x 10 | Language: French | Volume: 2 x 24 h

Programming skills

Languages: GO, C, PYTHON
Libraries: GMP, SEAL
Software: PARI/GP, SAGEMATH, MATLAB
Tools: GIT, EMACS, LaTeX
Others: REDIS, HTML

Languages

French: Mother tongue
English: Fluent
Spanish: Notions

Hobbies

Astronomy – Photography – Guitar – Go – Running – Trek – World cuisine