Matthieu Giraud *PhD Student in Cryptology*

Personal Data

Date of Birth	30 January 1987
Nationality	French
Address	1 rue de la Chebarde, 63 178 Aubière, France
Phone	+33 473 407 440
Email	matthieu.giraud@uca.fr
Website	http://sancy.clermont-universite.fr/~giraud/

Research Interests

I am interested in cryptology, 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.

Education

Oct'16 – Present PhD in Cryptology | Université Clermont Auvergne, France.
Laboratory: LIMOS (UMR 6158).
Thesis: *Security of Data Numerisation and Storage*.
Supervisor: Dr. Pascal Lafourcade.

Sep'14 – Sep'16 Master in Cryptology & Security | Université de Bordeaux, France.
Supervisors: Prof. Gillez Zémor, Assoc. Prof. Emmanuel Fleury.

Sep'11 – Sep'14 Bachelor's Degree in Mathematics | Université de Nantes, France.
Supervisor: Prof. Sylvain Gervais.

Work Experience

Apr'16 – Sep'16 Intership | Thales Communications & Security, Gennevilliers, France.
Laboratory: Chiffre LCH.
Description: Cryptanalysis of Symmetric Searchable Encryption.
Supervisors: Mr. Alexandre Anzala-Yamajako, Mr. Olivier Bernard.

Sep'15 – Dec'15 Tutorship | Université de Bordeaux, France.
Description: Tutorship in algebra for third year students of Computer Science.

Teaching Experience

Oct'16 – Present IUFE d'Auvergne | Université Clermont Auvergne, France.
Course: Certificat Informatique et Internet.
Responibilities: Teaching assistance for exercice sessions.
Group 1: 13 students | Group 2: 12 students
Level: Graduate | Language: French | Volume: 56h.

Student Supervision

Oct'16 – Mar'17 Mr. Alexandre Fabre, Mr. Thomas Glaziou, ISIMA | Level: Graduate
With Dr. Pascal Lafourcade.
Subject: Attacks on robust watermarking scheme.

Reviewing Service

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

Other Activity

- Co-organizer of the mensual seminar of the PhD students of the lab, since October 2016.

Conference Publications

4. *Verifiable Private Polynomial Evaluation*
   Xavier Bultel, Manik Lal Das, Hardik Gajera, David Gérault, Matthieu Giraud, and Pascal Lafourcade
   ProvSec (International Conference on Provable Security)
   Xi'an, China, October 23-25, 2017.

3. *Secure Matrix Multiplication with MapReduce.*
   Xavier Bultel, Radu Ciucanu, Matthieu Giraud, and Pascal Lafourcade.
   ARES (International Conference on Availability, Reliability and Security)
   Reggio Calabria, Italy, August 29 - September 01, 2017.

2. *Formal Analyze of a Private Access Control Protocol to a Cloud Storage.*
   Narjes Ben Rajeb, Mouhebeddine Berrima, Matthieu Giraud, and Pascal Lafourcade
   SECRYPT (International Conference on Security and Cryptography)
   Madrid, Spain, July 24-26, 2017.

1. *Practical Passive Leakage-Abuse Attacks Against Symmetric Searchable Encryption.*
   Alexandre Anzala-Yamajako, Olivier Bernard, Matthieu Giraud, and Pascal Lafourcade
   SECRYPT (International Conference on Security and Cryptography)
   Madrid, Spain, July 24-26, 2017.

Programming Skills

Languages	C, PARI/GP, PYTHON.
Software	OCTAVE, MATLAB, SAGEMATH.
Tools	LaTeX, EMACS, GIT.
Others	HTML, REDIS, SSDB.

Languages

French	Mother tongue.
English	Fluent.
Spanish	Notions.