David GERAULT

Phd Student

54, rue saint dominique
63000 Clermont-Ferrand
France
+33 6 99 48 64 42
david@gerault.net
www.gerault.net
07/20/1988

Research Interests

My main research topic is distance bounding authentication protocols, and I am particularly interested in designing provably secure privacy preserving protocols. In addition, I also work on automatic security evaluation of symmetric cryptography primitives using constraint programming.

Education

Since 2015 **Phd student: Security analysis of contactless communication protocols**, *Supervisor: Pascal Lafourcade*, Université Clermont Auvergne, LIMOS, Clermont Ferrand, France.
Funded by the FEDER program of 2014-2020 and the region council of Auvergne

2015 **Master's degree in Networks, Telecom and Services (with honours)**, *Université Lyon 1*, Lyon, France.

2013 **Licence (Bachelor) in computer sciences**, *Université Lyon 1*, Lyon, France.

2006 **Baccalauréat (A levels) Option literature and english**, *Lycée Blaise Pascal*, Clermont-Ferrand, France.

Internships

November 2017 **Security of distance bounding protocols**, *Ioana Boureanu*, University of Surrey, Surrey, UK.
Comparison of formal models for distance bounding

April-May 2017 **Cryptanalysis of symmetric primitives**, *Siwei Sun*, Chinese academy of sciences, Beijing, China.
Follow up work after the FSE'17 publication

December 2016 **Security of IoT devices**, *Manik Lal Das*, DI-IICT, Gandhinagar, India.
Collaboration on the design of new security primitives for the IoT. Led to a publication at ProvSec'17

2015 February to July **Using constraint programming to solve symmetric cryptography problems**, *Marine Minier, Christine Solnon*, Citi lab, Lyon, France.
Automatic security evaluation of the AES in the related key model with constraint programming. Led to a publication at CP'16

2014 January to February **Multi-agent approach to the generation of timetables**, *Nadia Kabachi, LIRIS*, Lyon, France, research initiation internship.
State of the art, partial implementation (JADE)

2013 June to August **Supervisor**, *AFD Technologies*, Bron.
Supervision of network equipment for a telecom operator and development of a monitoring tool (PHP, SQL, JavaScript, Json)

Publications

BDGGGL17 **Verifiable Private Polynomial Evaluation**, *Xavier Bultel, Manik Lal Das, Hardik Gajera, David Gérault, Matthieu Giraud, Pascal Lafourcade*, ProvSec'17.

GLMS17 **Using Constraint Programming to solve a Cryptanalytic Problem**, *David Gerault, Pascal Lafourcade, Marine Minier, Christine Solnon*, IJCAI'17.

BGLO17 **Breaking and Fixing the HB+DB protocol**, *Ioana Boureanu, David Gerault, Pascal Lafourcade, Cristina Onete*, Wisec'17.

GLMS17 **Revisiting AES Related-Key Differential Attacks with Constraint Programming**, *David Gerault, Pascal Lafourcade, Marine Minier, Christine Solnon*, eprint.

SGLYTQH17 **Analysis of AES, SKINNY and others with constraint programming**, *Siwei Sun, David Gerault, Pascal Lafourcade, Qianqian Yang, Yosuke Todo, Kexin Qiao, Lei Hu*, FSE'17.

ABGGLOR17 **A Terrorist-fraud Resistant and Extractor-free Anonymous Distance-bounding Protocol**, *Xavier Bultel, Sebastien Gambs, David Gerault, Pascal Lafourcade, Cristina Onete, Jean-Marc Robert*, AsiaCCS'17.

GL16 **Related-Key Cryptanalysis of Midori**, *David Gerault, Pascal Lafourcade*, Indocrypt'16.

GMS16 **Constraint Programming Models for Chosen Key Differential Cryptanalysis**, *David Gerault, Marine Minier, Christine Solnon*, CP'16.

BGGLOR16 **Prover-Anonymous and Terrorist-Fraud Resistant Distance Bounding Protocol**, *Xavier Bultel, Sebastien Gambs, David Gerault, Pascal Lafourcade, Cristina Onete, Jean-Marc Robert*, Wisec'16.

BGL15 **Survey of Distance Bounding Protocols and Threats**, *Agnes Brelurut, David Gerault, Pascal Lafourcade*, FPS'15.

Teaching

Classes

Since 2015 **Teaching at Université Clermont Auvergne**, IUT Réseaux et Télecom (Networks and Telecom).
System architecture, Telephony and System Administration, for first year students (64 hours/year)

Supervising

2015-2016 **Tutored project : Man in the middle, attack and defence strategies**, *Teddy Grzeskiewicz, Julien Cheminade et Anthony Huguet*, IUT Réseaux et Télecom.
Study of the means of intrusion and capabilities of an intruder on a company's network

2015-2016 **Project : Distance bounding protocols and attacks**, *Damien Teyssier*, Isima, with Pascal Lafourcade.
Implementation on a simulator of some distance bounding protocols and attacks against them

2015-2016 **Internship : Watermarking applications, techniques and attacks**, *Sumish Ahjmani*, IIT Kanpur, with Pascal Lafourcade.
Study of document watermatking techniques, and attacks using constraint programming

Others

Phd Seminar **Co organization of the bimensual seminar of the Phd students of the lab**, *Since 2015*.

Programming **Languages**, C/C++, Java/JEE, Awk, tcl, MiniZinc.

Tools, Choco, MiniZinc, ns2, WireShark, Vi, emacs, LaTeX, git.

Languages **French**, Mother language.

English, TOEIC score: 990/990 (2014).

German, Notions.