Ferdinand SIBLEYRAS

CV

Education

2017–2020 **PhD in Computer Science**, *Sorbonne University / Inria*, Defended 23rd October 2020, Security of Modes of Operation and other provably secure cryptographic schemes.
https://tel.archives-ouvertes.fr/tel-03058306

2016–2017 **Parisian Master of Research in Computer Science (MPRI)**, *Université Paris Diderot*, GPA: 17.33/20 (Summa cum laude), Graduated September 2017.

2013–2015 **Master of Science MSc in Financial Engineering**, *École Polytechnique Fédérale de Lausanne (EPFL)*, Swiss Finance Institute, GPA: 5,33/6.

2012–2013 **Exchange in Computer Engineering**, *Nanyang Technological University (NTU)*, Singapore.

2010–2012 **Bachelor of Science BSc in Computer Science**, *École Polytechnique Fédérale de Lausanne (EPFL)*, Switzerland, GPA: 5,34/6.

2010 **Baccalauréat S spé maths**, *Lycée Louis Pasteur*, distinction "TB".

Experience

2020–today **Post-doctoral Researcher**, NTT Group, Social Informatics Laboratories.
Following up on my thesis research work with an additional focus on primitive cryptanalysis.

2017–2020 **PhD Student**, Inria, COSMIQ, under the direction of Anne Canteaut and supervised by Gaëtan Leurent on the "Security of modes of operation"..
Produced multiple publications to major international conferences with review committee and acts. Focus on cryptanalysis of various mode of operation as well as cryptographic primitives. Production of slides and presentation of results in conferences, enterprise, and university. Codes of various simulations as well as intricated MILP model for optimization.

2017–2020 **Teaching**, Université Paris Descartes, UFR maths-info, Chargé de TD.
Introduction to C programming, Numeration and boolean logic, 2nd year project supervisor (smartphone application and website).

2015 **Portfolio Manager**, Chorus Capital, Graduation Internship followed by a short contract.
Daily management of multiple CLOs with hundreds of underlying assets. Assisted in studying new deals. Study of various CLOs and redaction of a Master thesis: "Arbitrage vs. Balance Sheet CLOs: an Empirical Comparison" that focus on incentives and structural differences.

Publications

Gaëtan Leurent, Ferdinand Sibleyras, *The Missing Difference Problem, and its Applications to Counter Mode Encryption*, in EUROCRYPT 2018.
`https://doi.org/10.1007/978-3-319-78375-8_24`

Higashimurayama, Tokyo – JAPAN
(FR)+33 785 18 84 27 (JP)+81 80-7663-2699 • ferdinand@sibleyras.fr
LinkedIn

Gaëtan Leurent, Mridul Nandi, Ferdinand Sibleyras, *Generic Attacks against Beyond-Birthday-Bound MACs*, in CRYPTO 2018.
https://doi.org/10.1007/978-3-319-96884-1_11

Gaëtan Leurent, Ferdinand Sibleyras, *Low-Memory Attacks Against Two-Round Even-Mansour Using the 3-XOR Problem*, in CRYPTO 2019.
https://doi.org/10.1007/978-3-030-26951-7_8

Donghoon Chang, Nilanjan Datta, Avijit Dutta, Bart Mennink, MridulNandi, Somitra Sanadhya, Ferdinand Sibleyras, *Release of Unverified Plaintext: Tight Unified Model and Application to ANYDAE*, in ToSC 2019.
https://doi.org/10.13154/tosc.v2019.i4.119-146

Ferdinand Sibleyras, *Generic Attack on Iterated Tweakable FX Constructions*, in CT-RSA 2020.
https://doi.org/10.1007/978-3-030-40186-3_1

Antonio Flórez-Gutiérrez, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, André Schrottenloher, Ferdinand Sibleyras, *New Results on Gimli: Full-Permutation Distinguishers and Improved Collisions*, in ASIACRYPT 2020.
https://doi.org/10.1007/978-3-030-64837-4_2

Dhiman Saha, Yu Sasaki, Danping Shi, Ferdinand Sibleyras, Siwei Sun, Yingjie Zhang, *On the Security Margin of TinyJAMBU with Refined Differential and Linear Cryptanalysis*, in ToSC 2020(3).
https://doi.org/10.13154/tosc.v2020.i3.152-174

Languages

French **Mothertongue**
English **Fluent** *TOEFL 108/120*
Japanese **Conversational**

Higashimurayama, Tokyo – JAPAN
(FR)+33 785 18 84 27 (JP)+81 80-7663-2699 • ferdinand@sibleyras.fr
LinkedIn