Science Park 123
1098 XG Amsterdam Pays-Bas
+33 (0)6 71 12 04 46
pierre.karpman@protonmail.com
D.O.B.: 1989.01.29
Nationality: French

Pierre Karpman

Education

2013–2016 **PhD in Informatics**, *Université Paris-Saclay*, France.
Thesis entitled *Analyse de primitives symétriques*.
Advised by Daniel Augot, Pierre-Alain Fouque and Thomas Peyrin.
Prepared at the École polytechnique and the Nanyang Technological University.
Defended on November 18 2016 at Palaiseau in front of the jury made of:
Louis Goubin, president.
Anne Canteaut and Antoine Joux, reviewers.
Benoît Gérard and Hongjun Wu, examiners.
Daniel Augot, Pierre-Alain Fouque and Thomas Peyrin.

2010–2012 **Master's Degree in Informatics**, *ENS Cachan Bretagne*, Rennes, France, with *mention bien*.
Courses including: Software Verification, Real-time Systems, Computer Security, Cryptography.

2008–2011 **Master's Degree in Telecommunications**, *INSA Lyon*, France, with *félicitations du jury*.
Courses including: Algorithmics, Middleware; Signal Processing, Wireless Communications; Networking.
Exchange student at Chalmers Tekniska Högskola (Spring semester, 2010).

2006–2008 **Foundation courses in Engineering Science**, *INSA Lyon*, France.
Courses including: Mathematics, Physics, Mechanics, Chemistry.

2006 **Baccalauréat**, *Lycée Vaugelas*, Chambéry, France, with *mention très bien*.

Positions

Since October 2016 **Post-doc researcher**, *Centrum Wiskunde & Informatica*, Amsterdam, The Netherlands.
Researcher in the cryptology team.

2013-2014 **Teaching Assistant**, *École normale supérieure de Rennes*, France, (8 months).
Taught tutorial and lab sessions in Programming and Cryptography (64 hours).

2013 **Project Officer**, *Nanyang Technological University*, Singapore, Singapore, (6 months).
Worked in the CCRG lab of the Division of Mathematical Sciences, on Symmetric Cryptography.

2012-2013 **Research Intern**, *IRISA/Inria*, Rennes, France, (6 months).
Worked in the Celtique/CIDre team on Symmetric Cryptography.

Computer skills

Programming C, OCaml, x86 Assembly (basic knowledge).
System Unix/Linux.
Miscellaneous software LaTeX, CUDA, Sage, Frama-C.

Languages

French **Native speaker.**
English **Fluent.**
German **Intermediate level.**

Interests

Hobbies Music (Flute, Trumpet), reading
Sports Long-distance running, Hiking, Climbing.

Publications

ASIACRYPT 2016 *Efficient and Provable White-Box Primitives* with Pierre-Alain Fouque, Paul Kirchner and Brice Minaud

EUROCRYPT 2016 *Freestart collision for full SHA-1* with Marc Stevens and Thomas Peyrin

ASIACRYPT 2015 *Key-Recovery Attacks on ASASA* with Brice Minaud, Patrick Derbez and Pierre-Alain Fouque

ISC 2015 *From Distinguishers to Key Recovery: Improved Related-Key Attacks on Even-Mansour*

CRYPTO 2015 *Practical Free-Start Collision Attacks on 76-step SHA-1* with Thomas Peyrin and Marc Stevens

CRYPTO 2015 *Higher-Order Differential Meet-in-The-Middle Preimage Attacks on SHA-1 and BLAKE* with Thomas Espitau and Pierre-Alain Fouque

SAC 2014 *Diffusion Matrices from Algebraic-Geometry Codes with Efficient SIMD Implementation* with Daniel Augot and Pierre-Alain Fouque

CT-RSA 2014 *Analysis of BLAKE2* with Jian Guo, Ivica Nikolić, Lei Wang and Shuang Wu

IMA-CC 2013 *Security Amplification against Meet-in-the-Middle Attacks Using Whitening* with Pierre-Alain Fouque

Participation in program committees

FSE 2018

References

Daniel Augot : Daniel.Augot@inria.fr

Pierre-Alain Fouque : Pierre-Alain.Fouque@irisa.fr

Marc Stevens : Marc.Stevens@cwi.nl