Science Park 123
1098 XG Amsterdam Pays-Bas
+33 (0)6 71 12 04 46
pierre.karpman@protonmail.com
Né le 29/01/1989 (28 ans)
Nationalité française

Pierre Karpman

Diplômes & études

2013–2016 **Doctorat en informatique**, *Université Paris-Saclay*, France.
Thèse intitulée *Analyse de primitives symétriques*.
Effectuée sous la direction de Daniel Augot, Pierre-Alain Fouque et Thomas Peyrin.
Préparée à l'École polytechnique et à la Nanyang Technological University, Singapour.
Soutenue le 18 novembre 2016 à Palaiseau devant le jury composé de :
Louis Goubin, président.
Anne Canteaut et Antoine Joux, rapporteurs.
Benoît Gérard et Hongjun Wu, examinateurs.
Daniel Augot, Pierre-Alain Fouque et Thomas Peyrin.

- Mission d'enseignement de 64 heures effectuée à l'ENS Rennes.

2010–2012 **Master d'informatique, spécialité recherche**, *ENS Cachan Bretagne*, France, avec mention bien.
Admis avec rang 1/45.
Mémoire intitulé *Building up on SIDAN : improved and new invariants for a software hardening Frama-C plugin*.
Encadré par Eric Totel et Frédéric Tronel.

- Reçu au concours d'entrée en troisième année de l'ENS Cachan, session 2011.

2006–2011 **Diplôme d'ingénieur en télécommunications**, *INSA Lyon*, France, avec les félicitations du jury.

2010 **Étudiant d'échange**, *Chalmers Tekniska Högskola*, Göteborg, Suède.

2006 **Baccalauréat général, série S**, *Lycée Vaugelas*, Chambéry, France, avec mention très bien.

Expérience professionnelle

Depuis Octobre 2016 **Chercheur Post-doctorant**, *Centrum Wiskunde & Informatica*, Amsterdam, Pays-Bas.
Chercheur dans l'équipe de cryptologie.

2013 **Stage de recherche**, *Nanyang Technological University*, Singapour, Singapour, (6 mois).
Stage dans l'équipe CCRG de la division de mathématiques. Cryptographie symétrique.

2012–2013 **Stage de recherche**, *IRISA/Inria*, Rennes, France, (6 mois).
Stage dans les équipes Celtique/CIDre. Cryptographie symétrique.

Compétences informatiques

Langages C, OCaml, Assembleur x86 (notions).
Système Unix/Linux.
Divers LaTeX, CUDA, Sage, Frama-C.

Langues

Anglais **Courant.**
Allemand **Intermédiaire.**
Néerlandais **Notions.**
Japonais **Notions.**

Divers

Loisirs Musique (flûte traversière, trompette), lecture.
Sports Escalade, randonnée, course de fond

Publications

CRYPTO 2017 *The first collision for full SHA-1* avec Marc Stevens, Elie Bursztein, Ange Albertini et Yarik Markov

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

EUROCRYPT 2016 *Freestart collision for full SHA-1* avec Marc Stevens et Thomas Peyrin

ASIACRYPT 2015 *Key-Recovery Attacks on ASASA* avec Brice Minaud, Patrick Derbez et 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* avec Thomas Peyrin et Marc Stevens

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

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

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

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

Participation à des comités de programme

FSE 2018

Références

Daniel Augot : Daniel.Augot@inria.fr

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

Marc Stevens : Marc.Stevens@cwi.nl