Marc Stevens
Curriculum Vitae

Personal details

Titles, first name, surname:	dr.ir. Marc Stevens
Date of birth:	april 7, 1981
Nationality:	Netherlands
Telephone:	+31-6-38307119
E-mail:	marc.stevens@cwi.nl
Corresponding address:	CWI – Centrum Wiskunde & Informatica P.O. Box 94079 1090 GB Amsterdam The Netherlands

Research Highlights

- The first collision for full SHA-1:
  The cryptographic hash function SHA-1 was theoretically broken in 2005. Since then many cryptanalytic experts have attempted to practically break it by finding an example collision: two distinct files with the same SHA-1 hash. Based on new advances in the deep analysis of SHA-1 and a very efficient GPU CUDA framework for depth-first tree search, we succeeded in finding the first SHA-1 collision in 2017 using Google's AlphaGo GPU resources.
- Counter-cryptanalysis and the unknown MD5 attack in super malware Flame:
  We invented counter-cryptanalysis enabling real-time detection of MD5 and/or SHA-1 collision attacks given just a single file from a colliding pair. Our hardened SHA-1 implementation with integrated collision detection is currently deployed in Windows, Git, GitHub, Gmail, Google Drive, Microsoft OneDrive. It enabled us to expose the **unknown** variant MD5 attack in the super malware Flame that used it to forge signatures for malicious Windows Updates. We later reconstructed this unknown MD5 collision attack variant in detail.
- Rogue Certification Authority using MD5 collision attack on 200 PlayStation3s:
  The first collision for MD5 was announced in 2004 by a chinese team led by prof. Xiaoyun Wang. We developed significantly faster attacks, as well as a much more powerful attack that enables meaningful collisions for various file formats. We showed MD5 is insecure for digital signatures and immediately triggering its deprecation by responsibly forging a MD5-based signature from an internet certificate authority. We used a cluster of 200 PlayStation3s to satisfy computational power requirements due to particular constraints.

Work Experience

March 2017 – now	Permanent Research Staff, Cryptology Group, Centrum Wiskunde & Informatica (CWI)
June 2014 – February 2017	Tenure-Track Research Staff, Cryptology Group, Centrum Wiskunde & Informatica (CWI)
October 2014 – January 2015	Visiting Scholar, SYLLAB, Nanyang Technological University, Singapore
June 2012 – May 2014	Post-doctoral Researcher, Cryptology Group, Centrum Wiskunde & Informatica (CWI)
October 2007 – June 2012	PhD student, Cryptology Group, Centrum Wiskunde & Informatica (CWI) and Mathematical Institute, Leiden University
August 2007 – September 2007	Research intern, LACAL, École Polytechnique Fédérale de Lausanne (EPFL), Switzerland
September 2005 – May 2006	Research intern, NBV (Dutch national communications security agency), Voorburg
January 2004 – April 2004	Research intern, CITS, Ruhr-Universität Bochum, Germany

Grants, Honors and Awards

- *RealWorldCrypto 2020 Levchin Prize* for 'groundbreaking work on the security of collision resistant hash functions.' (The prize honors significant contributions to real-world cryptography and celebrates recent advances that have had a major impact on the practice of cryptography and its use in real-world systems. Two awards per year, each carries a cash prize of $10,000.)
- *NWO*[1] *Big Data: real time ICT for logistics Grant*, PI (Blockchain research consortium of ABN AMRO, CWI, KLM, ING, UvA, VU), awarded 685k€
- *Best Paper Award, 37th Annual IACR CRYPTO 2017, Santa Barbara, CA, USA*
- *BlackHat 2017 Pwnie Award for Best Cryptographic Attack, Las Vegas, Nevada, USA*
- *Google Junior Faculty Applied Research Award in Security, Privacy & Anti-abuse.* Awarded a $50k research gift to support my research in recognition of my work in Cryptanalysis, in particular related to SHA-1, 2016.
- *NWO Veni Grant 2014*, PI, awarded 248k€ (NWO: 'Veni is targeted at outstanding researchers who have recently obtained their PhD')
- *Best Young Researcher Paper Award, 33rd Annual IACR CRYPTO 2013, Santa Barbara, CA, USA* (best paper authored solely by young researcher(s) not having received their PhD before 2011)
- Winner of the *KHMW Martinus van Marum prize 2013* of The Royal Holland Society of Sciences and Humanities (KHMW) for my PhD thesis and other publications (awarded once every 5 years within Astronomy, Computer Science, Mathematics and Physics)
- *NWO Vrije Competitie Grant 2012*, Co-PI, awarded 216k€

[1] Netherlands Organization for Scientific Research

- *Best Paper Award, 29th Annual IACR CRYPTO 2009, Santa Barbara, CA, USA*
- *Eindhoven University of Technology – Afstudeerprijs 2008* (best master's thesis university-wide)
- Graduated Applied Mathematics *cum laude* (2007)

Publications [2]

- Esteban Landerreche, Marc Stevens, Christian Schaffner, *Non-interactive Cryptographic Timestamping based on Verifiable Delay Functions*, Financial Crypto 2020.
- Martin R. Albrecht, Léo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn W. Postlethwaite, Marc Stevens, *The General Sieve Kernel and New Records in Lattice Reduction*, EUROCRYPT 2019.
- Esteban Landerreche, Marc Stevens, *On Immutability of Blockchains*, ERCIM Blockchain Workshop 2018.
- Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini, Yarik Markov, *The first collision for full SHA-1*, CRYPTO 2017. **CRYPTO 2017 Best Paper Award** and **BlackHat 2017 Pwnie Award for Best Cryptographic Attack.**
- Marc Stevens, Dan Shumow, *Speeding up detection of SHA-1 collision attacks using unavoidable attack conditions*, USENIX Security 2017.
- Rusydi M. Makarim, Marc Stevens, *M4GB: An eficient Groebner-basis algorithm*, ISSAC 2017.
- Anne Canteaut, Eran Lambooij, Samuel Neves, Shahram Rasoolzadeh, Yu Sasaki, Marc Stevens, *Refined Probability of Differential Characteristics Including Dependency between Multiple Rounds*, FSE 2017.
- Muhammad Barham, Orr Dunkelman, Stefan Lucks and Marc Stevens, *New Second Preimage Attacks on Dithered Hash Functions with Low Memory Complexity*, Selected Areas in Cryptology 2016, Lecture Notes in Computer Science, Springer, 2016.
- Marc Stevens, Pierre Karpman, and Thomas Peyrin, *Freestart collision for full SHA-1*, 35th Annual IACR EUROCRYPT (Marc Fischlin and Jean-Sébastien Coron, eds.), Lecture Notes in Computer Science, vol. 9665, pp. 459–483, Springer, May 2016, Vienna, Austria.
- Max Fillinger, and Marc Stevens, *Reverse-engineering of the cryptanalytic attack used in the Flame super-malware*, 21st Annual IACR ASIACRYPT (Tetsu Iwata and Jung Hee Cheon, eds.), Lecture Notes in Computer Science, vol. 9453, pp. 586–611, Springer, December 2015, Auckland, New Zealand.
- Pierre Karpman, Thomas Peyrin, and Marc Stevens, *Practical free-start collision attacks on 76-step SHA-1*, 35th Annual IACR CRYPTO (Rosario Gennaro and Matthew Robshaw, eds.), Lecture Notes in Computer Science, vol. 9215, pp. 623–642, Springer, August 2015, Santa Barbara, CA, USA.
- Marc Stevens, *Counter-Cryptanalysis*, 33rd Annual IACR CRYPTO (Ran Canetti and Juan A. Garay, eds.), Lecture Notes in Computer Science, vol. 8042-I, pp. 129–146, Springer, August 2013, Santa Barbara, CA, USA. **Best young researcher paper award.**

[2] Please note that IACR's CRYPTO, EUROCRYPT and ASIACRYPT are generally considered the most important publication venues in the world for cryptographic academic research.

- Marc Stevens, *New Collision Attacks on SHA-1 Based on Optimal Joint Local-Collision Analysis*, 32nd Annual IACR EUROCRYPT (Thomas Johansson and Phong Q. Nguyen, eds.), Lecture Notes in Computer Science, vol. 7881, pp. 245–261, Springer, May 2013, Athens, Greece.
- Marc Stevens, Arjen K. Lenstra, and Benne de Weger, *Chosen-prefix collisions for MD5 and applications*, International Journal of Applied Cryptography, IJACT, vol. 2012-**2**, no. 4, Inderscience 2012, 322–359.
- Marc Stevens, *Advances in Hash Function Cryptanalysis*, Marc Stevens, ERCIM, Vol. 90, July, 2012.
- Marc Stevens, *Single-block collision attack on MD5*, Cryptology ePrint Archive, Report 2012/040. **Winner of Tao Xie and Dengguo Feng's $5,000 challenge:** `http://eprint.iacr.org/2010/643`.
- Marc Stevens, Alexander Sotirov, Jacob Appelbaum, Arjen K. Lenstra, David Molnar, Dag Arne Osvik, and Benne de Weger, *Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate*, 29th Annual IACR CRYPTO (Shai Halevi, ed.), Lecture Notes in Computer Science, vol. 5677, pp. 55–69, Springer, August 2009, Santa Barbara, CA, USA. **Best paper award.**
- Marc Stevens, *Breaking the Weakest Link: Becoming a Trusted Authority on the Internet*, ERCIM, Vol. 77 April, 2009.
- Marc Stevens, Arjen K. Lenstra, and Benne de Weger, *Chosen-Prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities*, 26th Annual IACR EUROCRYPT (Moni Naor, ed.), Lecture Notes in Computer Science, vol. 4515, pp. 1–22, Springer, May 2007, Barcelona, Spain.
- Marc Stevens, *Fast Collision Attack on MD5*, Cryptology ePrint Archive, Report 2006/104.
- Tanja Lange and Marc Stevens, *Efficient Doubling on Genus Two Curves over Binary Fields*, 11th Annual Workshop on Selected Areas in Cryptography (Helena Handschuh and M. Anwar Hasan, eds.), Lecture Notes in Computer Science, vol. 3357, pp. 170–181, Springer, August 2004, Waterloo, Ontario, Canada.

Invited Talks (selected)

- Keynote lecture, FSE 2018, Brugge, 2018, *On breaking SHA-1.*
- Keynote lecture, RCD 2017, Budapest, 2017, *On the construction of the first collision for SHA-1.*
- Keynote lecture, CRYPTODAY 2017, Technion, Haifa, 2017, *On the construction of the first collision for SHA-1.*
- Keynote lecture, SHARCS 2012, Washington D.C., USA, March 2012, *Cryptanalysis of MD5 and SHA-1.*
- Keynote lecture, 80th Anniversary of Breaking the Enigma Code - Return to the Roots, Warsaw, Poland, November 2012, *Cryptanalysis of MD5 and SHA-1.*
- Invited lecture, 20th Anniversary of the Founding of Institute of Advanced Study, Tsinghua University, 2017, *On the construction of the first collision for SHA-1.*

- Invited lecture, National Cyber Security Center, June 2017, Netherlands, *On the construction of the first collision for SHA-1.*
- Invited lecture, NLUUG Voorjaarsconferentie 2016, Utrecht, The Netherlands, *Bitcoin and the Security of the Blockchain.*
- Invited lecture, Security in Times of Surveillance 2015, Eindhoven, The Netherlands, *Need Security Against Digital Signature Forgeries.*
- Invited lecture, TCCM-CACR 2013, Tianjin, China, August 2013, *Analysis of Truncated Differential Paths and Local Collisions.*
- Invited lecture, ASK 2013, Wei Hai, China, August 2013, *Improving Counter-Cryptanalysis.*
- Invited lecture, Real World Crypto 2013, Stanford, January 2013, *Counter-cryptanalysis: analyzing Flame's new collision attack.*
- Invited lecture, Technion, Israel, November 2013, *Improving Counter-Cryptanalysis.*
- Invited lecture, Tsinghua University, China, September 2013, *Improving Counter-Cryptanalysis.*
- Invited lecture, National Cyber Security Center, March 2013, Netherlands, *Counter-cryptanalysis: analyzing Flame's new collision attack.*

Open-source Research Software

See `https://github.com/cr-marcstevens`.

- *HashClash*: a C++ framework for MD5 & SHA-1 cryptanalysis.
  See also file format exploitations: `https://github.com/corkami/collisions`.
- *SHA-1 collision detection*: a fast drop-in replacement SHA-1 library with detection of malicious files that were generated with cryptanalytic attacks. (Used by GIT, Google Drive, GMail, Microsoft One Drive, Microsoft SmartScreen)
- *M4GB*:An efficient Groebner Basis algorithm for multivariate cryptanalysis that holds some MQchallenge records.
- *G6K*: The General Sieve Kernel for lattice cryptanalysis that holds some Lattice Records.

Scientific Activities (selected)

- Board member Dutch National Mathematics Research Cluster DIAMANT since 2017
- Steering committee member of national Dutch Blockchain Consortium 2017–2019
- Guest Editor for Fall 2017 special edition on Cryptology of the "Nieuw Archief voor Wiskunde" of the Dutch Royal Mathematics Society
- Editorial Board member of IACR Transactions on Symmetric Cryptology
- Program Committee member of IACR CRYPTO 2014, 2020
- Program Committee member of IACR EUROCRYPT 2019
- Program Committee member of IACR ASIACRYPT 2014, 2018

- Program Committee member of CT-RSA 2017, 2016
- Program Committee member of IACR FSE 2020, 2019, 2018, 2017, 2016
- General Chair of IACR PKC 2017
- Scientific co-organizer of the CWI RISC Seminar

Supervision & Teaching

- MSc Course 'Selected Areas in Cryptology', MasterMath, 2017, 2019.
- MSc Course 'Cryptology', MasterMath, 2012, 2015.
- Esteban Landerreche, PhD student, CWI Amsterdam, The Netherlands, 2017–2021, *Immutability guarantees for Blockchains.*
- Rusydi Makarim, PhD student, Mathematical Institute Leiden & CWI Amsterdam, The Netherlands, 2014–2019, *Algebraic Cryptanalysis.*
- Esteban Landerreche, MSc Thesis, ILLC UvA, The Netherlands, 2017, *Leaning on Impossible-to-Parallelise Work for Immutability Guarantees on the Blockchain.*
- Maximillian Fillinger, MSc Thesis, University of Amsterdam, 2013, *Reconstructing the Cryptanalytic Attack behind the Flame Malware.*
- Huaifeng Chen, visiting PhD student (3 months), CWI Amsterdam, The Netherlands, 2015.
- Fatemeh Sefi Shahpar, visiting PhD student (5 months), Mathematical Institute Leiden, The Netherlands, 2015.

Outreach

- CWI Open Day Cryptographic educational activities (every year in october)
- Pre-University lectures on cryptography for high school students in Leiden (every 2 years)
- English and Dutch version of Cryptris (`https://cryptris.nl`): an online game on lattice-based cryptography

Media (selected)

Media Articles on the first SHA-1 collision (selection)

- Wall Street Journal, *Google & CWI Team Cracks Longtime Pillar of Internet Security*, Robert McMillan, February 23, 2017.
- Ars Technica, *At death's door for years, widely used SHA1 function is now dead*, Dan Goodin, February 23, 2017.
- Forbes, *Google & CWI Just 'Shattered' An Old Crypto Algorithm – Here's Why That's Big For Web Security*, Thomas Fox-Brewster, February 23, 2017.

Media Articles on the "SHAppening" (selection)

- Ars Technica, *SHA1 algorithm securing e-commerce and software could break by year's end*, Dan Goodin, October 8, 2015.
- SC Magazine, *Researchers say SHA-1 will soon be broken, urge migration to SHA-2*, Teri Robinson, October 10, 2015.
- The Register, *Crypto cadre cloud-cracks SHA-1 with just $75k of compute cost*, Darren Pauli, October 9, 2015.

Media Articles on the Flame discovery (selection)

- BBC News Technology, *Flame malware makers send 'suicide' code*, June 8, 2012.
- EuroTech, *Years of Secret Cryptographic Research Uncovered In 0.02 Seconds*, Max Huijgen, June 20, 2012.
- PC World, *"Flame's Windows Update Hack Required World-class Cryptanalysis, Researchers Say"*, Lucian Constantin, June 8, 2012.
- CWI News, *CWI cryptanalyst discovers new cryptographic attack variant in Flame spy malware*, Marc Stevens, June 2012.
- Techweek Europe, *"Microsoft 'Oversight' Helped Flame Spread"*, Tom Brewster, June 8, 2012.

Media Articles on the Rogue Certification Authority construction (selection)

- Le Monde, *L'algorithme MD5 utilisé par de nombreux sites n'est pas fiable*, Catherine Vincent, January 2, 2009.
- NRC, *De sleutel van de bank ligt voor het grijpen*, Margriet van der Heijden, December 30, 2008.
- The New York Times, *Outdated Security Threatens Web Commerce*, John Markoff, December 30, 2008.
- The Washington Post, *One Weak Link to Rule Them All*, Brian Krebs, December 30, 2008.

Media Articles Other (selection)

- NRC weekblad, *Tien beloftes voor de jaren 10* (ten talents of the tenties), Carola Houtekamer and Jannetje Koelewijn, December 19–23, 2009.
- Science Magazine, *Cryptologists Cook Up Some Hash for New 'Bake-Off'*, Dana Mackenzie, vol. 319, no. 5869, pp. 1480–1481, March, 2008.
- The Economist, Technology Quarterly, *Making a total hash of it*, Bas den Hond, March 6, 2008.

References

- prof. dr. Ronald Cramer, Cryptology Group, Centrum Wiskunde & Informatica (CWI) and Mathematical Institute, Leiden University, e-mail: `ronald.cramer @ cwi.nl`