Acknowledgments

This PhD thesis would not be the same without the influence of many people whom I would like to thank here.

First of all, I would like to thank my supervisor Ronald Cramer for our many interactions and discussions that have improved my skills as a researcher and for letting me pursue a line of research different from his own that has led to this thesis.

Many thanks go to Arjen Lenstra and Benne de Weger for our many discussions, their many helpful suggestions and in writing our papers.

Also, I would like to thank the other members of my defense committee for taking the time to read this thesis and for their insightful comments: Eli Biham, Berry Schoenmakers, Peter Stevenhagen and Xiaoyun Wang. Special thanks go to Eli Biham and Xiaoyun Wang who have taken extra efforts to be able to attend the defense in Leiden and their contributions to the preceding RISC seminar.

Thanks to all the people of CWI who have helped with public relations and legal counseling concerning the publication of our rogue Certification Authority certificate.

I am very grateful to all my colleagues, family and friends for their continuing support and confidence in me during these years.

And finally Lisanne: thank you for all your support and understanding and enriching my life together with our future child.

Marc Stevens
Curriculum Vitae

Personal details

First name, surname:	Marc Stevens
Date and place of birth:	April 7, 1981, Hellevoetsluis
Nationality:	Netherlands
E-mail:	marc@marc-stevens.nl

Degrees

PhD

Title of thesis:	'Attacks on hash functions and applications'
University:	Mathematical Institute, Leiden University
Advisors:	prof. dr. Ronald Cramer, prof. dr. Arjen Lenstra (EPFL) *&* dr. Benne de Weger (TU/e)
Date of defense:	*expected June 19, 2012*

MSc

Title of thesis:	'On collisions for MD5'
University:	Faculty of Mathematics and Computer Science, Eindhoven University of Technology
Advisors:	prof. dr. Henk van Tilborg, dr. Benne de Weger *&* Gido Schmitz MSc (NBV, Dutch national communications security agency)
Date of defense:	August 28, 2007

Honors, awards and prizes

- Winner of the $10,000-challenge to construct a single-block collision for MD5 posted by Tao Xie and Dengguo Feng: `http://eprint.iacr.org/2010/643`
- Nominated for *Discoverer of the Year 2011*, Faculty of Science, Leiden University, January 2012
- *CRYPTO 2009 – Best Paper Award*

- *Eindhoven University of Technology – Afstudeerprijs 2008*
  (best master's thesis university-wide)
- Nominated for *Joop Bautz Information Security Award 2007* (best contribution to dutch information security branch, PvIB, ISACA, NOREA, `http://www.jbisa.nl`)
- Graduated Applied Mathematics *cum laude* (2007)

Publications

- Marc Stevens, *Exact joint local-collision analysis & new collision attacks for SHA-1*, submitted to CRYPTO 2012.
- Marc Stevens, *Single-block collision attack on MD5*, Cryptology ePrint Archive, Report 2012/040, 2012. Winner of the $10,000-challenge posted by Tao Xie and Dengguo Feng: `http://eprint.iacr.org/2010/643`.
- Marc Stevens, Arjen K. Lenstra and Benne de Weger, *Chosen-prefix Collisions for MD5 and Applications*, to appear in: International Journal of Applied Cryptology (IJACT).
- 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*, CRYPTO (Shai Halevi, ed.), Lecture Notes in Computer Science, vol. 5677, Springer, 2009, pp. 55–69.
- Marc Stevens, Arjen K. Lenstra, and Benne de Weger, *Chosen-Prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities*, EUROCRYPT (Moni Naor, ed.), Lecture Notes in Computer Science, vol. 4515, Springer, 2007, pp. 1–22.
- Marc Stevens, *Fast Collision Attack on MD5*, Cryptology ePrint Archive, 2006, Report 2006/104.
- Tanja Lange and Marc Stevens, *Efficient Doubling on Genus Two Curves over Binary Fields*, Selected Areas in Cryptography (Helena Handschuh and M. Anwar Hasan, eds.), Lecture Notes in Computer Science, vol. 3357, Springer, 2004, pp. 170–181.

Invited Talks (selected)

- Keynote address, SHARCS 2012, Washington DC, March 2012, *Cryptanalysis of MD5 and SHA-1*.

Software

- Marc Stevens, *HashClash project*, an open-source C++ framework for MD5 & SHA-1 differential path construction and chosen-prefix collisions for MD5, 2009–2011, `http://code.google.com/p/hashclash`.