

# Marten van Dijk

Resume

16 Curtis Street #2, Somerville, MA 02144  
Phone: 857-241-0549, Email: marten@mit.edu

## Summary

Skilled applied mathematician with 13 years research experience in coding and information theory, and security and cryptography. Excellent team player. Able to multi-task efficiently. Exceptional inventor and scientist with 60+ publications, 10+ issued patents, and 10+ pending patents.

## Professional Experience

*Massachusetts Institute of Technology* 2001 - present

Research scientist 2005 - present  
(MIT Computer Science and Artificial Intelligence Laboratory / CSAIL)

- Secured government (NSF) funding of \$500,000 for MIT CSAIL. Received industry funding of approximately \$100,000 per year from Quanta Computer Inc.
- Taught Course 6 classes at the MIT Electrical Engineering and Computer Science Department (Design and Analysis of Algorithms, Computer System Engineering, etc.).
- Contribute to research on various security related topics. Introduced a new secure device model called the trusted execution module (TEM) for commodity general-purpose trusted computing. Improved memory integrity checking mechanisms by applying trusted platform module (TPM) technology. Introduced virtual monotonic counters leading to new TPM applications; count-limited certificates for managing access rights and mobile agents. Invited expert TPM Work Group.
- Co-authored a paper on protein folding, studied bio-informatics, co-authored a paper on oblivious routing.

Philips Research Visiting scientist 2001 - 2005  
(MIT Computer Science and Artificial Intelligence Laboratory / CSAIL)

- Facilitated a productive collaboration between Philips and MIT in the area of security. Contributed to system security research which involves both practical and theoretical aspects. Started and managed a team at Philips Research focused on security research.
- Introduced physical random functions (PUFs); the startup company Verayo (2005, <http://www.verayo.com/>) offers a commercialized version of physical random functions as a solution for radio frequency identification (RFID), the startup company Intrinsic-ID (2008, <http://www.intrinsic-id.com/>) uses physical random functions to generate device-unique IDs and keys.
- Introduced single chip secure processors, memory integrity checking, visual crypto displays and practical torus based cryptography. Researched information embedding, biometrics, and the modeling and verification of system security properties.

*Philips Research Laboratories, the Netherlands*

1996 - 2005

Research scientist

1996 - 2001

(Digital Signal Processing group)

- Improved wireless communications and storage applications by applying the theory of error correcting codes.
- Invented the error correcting codes which have been accepted in the digital video recording standard for Blu-ray disc (<http://www.blu-raydisc.com/> and <http://www.blu-ray.com/>, see also US patents 6,367,049 and 7,103,829). Co-authored the paper “Optical Disc System for Digital Video Recording”, Jpn. J. Appl. Phys. Vol.39, 2000, on Philips’ contributions to Blu-ray disc technology, which got reprinted in the book *Origins and Successors of the Compact Disc Contributions of Philips to Optical Storage*, <http://www.ieee.be/milestone.html>, published as a result of the IEEE Milestone in Electrical Engineering and Computing dedicated to Philips for the development of the compact disc audio player.
- Developed error correcting codes for magnetic and optical storage and flash memory. Researched modulation codes for optical storage, convolutional codes and turbo decoding for broadcast satellite communication and wireless communications, and watermarking and copyright protection schemes for optical storage. Visited and contributed to Philips Consumer Electronics, Vienna, during September-December 1998.

*Chinese University of Hong Kong*

1996

Cryptology Research Associate

## Education

*Eindhoven University of Technology*, PhD in Mathematics, the Netherlands

1997

*Eindhoven University of Technology*, M.S. in Mathematics, Cum Laude, the Netherlands

1993

*Eindhoven University of Technology*, M.S. in Computer Science, Cum Laude, the Netherlands

1991

## Awards

- NSF Grant (Applications and Evolution of TPM Technology) for \$500,000 2007
- ACSAC’02 outstanding student paper award, <http://www.acsac.org/> 2002

## Languages

Fluent in Dutch and English. Intermediate in German.