

## **Marten van Dijk**

Curriculum Vitae

MIT Computer Science and Artificial Intelligence Laboratory  
the Stata Center, 77 Massachusetts Ave, 32-G864 Cambridge, MA 02139, USA  
martens@mit.edu

### **Education**

- 1991-1997 Eindhoven University of Technology  
Doctor of Philosophy in Mathematics, December 1997  
Thesis: “Secret Key Sharing and Secret Key Generation”  
<http://alexandria.tue.nl/extra2/9704800.pdf>  
Henk van Tilborg, advisor
- 1987-1993 Eindhoven University of Technology  
Master of Science in Mathematics  
Thesis: “Wyner’s Wire-Tap Channel and its Cryptographic Application”  
Awarded cum laude in April 1993  
Henk van Tilborg, advisor
- 1987-1991 Eindhoven University of Technology  
Master of Science in Computer Science  
Thesis: “Graph Algorithms”  
Awarded cum laude in August 1991  
Anne Kaldewaij, advisor

### **Professional Experience**

- 2005- Research scientist at the MIT Computer Science and Artificial Intelligence Laboratory, member of the Computer Structures Group.
- 2001-2005 Visiting scientist from Philips Research (Information and System Security group) at the MIT Computer Science and Artificial Intelligence Laboratory.
- 1996-2001 Research scientist at Philips Research Laboratories (Digital Signal Processing group), the Netherlands. Visited Philips Consumer Electronics, Vienna, during September-December 1998.
- 1996 Research associate at the Chinese University of Hong Kong during January-August 1996.

### **Teaching Experience**

- Spring 2009 Lecturer for the course “Design and Analysis of Algorithms (6.046)” at MIT.
- Fall 2008 Lecturer for the course “Mathematics for Computer Science (6.042)” at MIT.

Spring 2008 Recitation instructor for the course “Computer System Engineering (6.033)” at MIT.

Spring 2007 Teaching assistant for the course “Introduction to Algorithms (6.046)” at MIT.

Fall 2005 Teaching assistant for the course “Introduction to Algorithms (6.046)” at MIT.

## Awards

2007 NSF Grant 0715680 (Applications and Evolution of Trusted Platform Module Technology) for \$500,000

2002 ACSAC’02 outstanding student paper award, <http://www.acsac.org/>

## Languages

Fluent in Dutch and English. Well developed passive understanding of German. Limited in speaking German.

## Citizenship

The Netherlands. Greencard in the category priority worker – alien with extraordinary ability (E16).

## Publications

### Journal Papers

- [1] M. van Dijk, On the Information Rate of Perfect Secret Sharing Schemes, Designs, Codes, and Cryptography 6(2), 143-169, 1995, preliminary versions appeared in the Proceedings of the 2nd International Winter Meeting on Coding and Information Theory, December 12 - 15, p. 27, 1993, and in the Proceedings of ISIT’94, June 27 - July 1, p. 489, 1994.
- [2] M. van Dijk, W.-A. Jackson, and K.M. Martin, A note on duality in linear secret sharing scheme, Bull. of the Institute of Combinatorics and its Applications 19, 93-101, 1997.
- [3] M. van Dijk, On a special class of broadcast channels with confidential messages, IEEE Trans. on Inform. Theory 43(2), 712-714, 1997.
- [4] M. van Dijk, More information theoretical inequalities to be used in secret sharing, Information Processing Letters 63(1), 41-44, 1997.
- [5] M. van Dijk, A linear construction of secret sharing schemes, Designs, Codes and Cryptography 12(2), 161-201, 1997.
- [6] M. van Dijk, W.-A. Jackson, and K. Martin, A general decomposition construction for incomplete secret sharing schemes, Designs, Codes and Cryptography 15(3), 301-321, 1998.

- [7] M. van Dijk, C. Gehrman, and B. Smeets, Unconditionally Secure Group Authentication, Designs, Codes and Cryptography 14(3), 281-296, 1998.
- [8] M. van Dijk and L. Tolhuizen, Efficient encoding for a class of subspace subcodes, IEEE Trans. on Inform. Theory 45, 2142-2146, 1999.
- [9] T. Narahara, S. Kobayashi, M. Hattori, Y. Shimpuku, G.J. van den Enden, J.A.H.M. Kahlman, M. van Dijk, and R. van Woudenberg, Optical Disc System for Digital Video Recording, Jpn. J. Appl. Phys. Vol.39 (2000), Part 1, No. 2B, 912-919, February 2000. An abstract has been published in the Proc. of ODS/ISOM, Hawaii, July, 1999.
- [10] W. Coene, H. Pozidis, M. van Dijk, J. Kahlman, R. van Woudenberg, and B. Stek, Channel coding and signal processing for optical recording systems beyond DVD, IEEE Trans. on Magn., Vol.37 (2001), Issue 2, Part 1, 682-688, March 2001.
- [11] S. Liu, H.C.A. van Tilborg, and M. van Dijk, A practical protocol for advantage distillation and information reconciliation, Designs, Codes and Cryptography 30(1), p. 39-62, 2003.
- [12] M. van Dijk, A.J.E.M. Janssen, and A. Koppelaar, Correcting systematic mismatches in computed log-likelihood ratios, European Transactions on Telecommunications 14, p. 227-244, 2003.
- [13] M. van Dijk, S. Egner, R. Motwani, and A. Koppelaar, Simultaneous zero-tailing of parallel concatenated codes, IEEE Trans. on Inform. Theory 49(9), p. 2236-2241, 2003. An abstract appeared in the Proceedings of ISIT 2000, June 25-30, p. 368, 2000.
- [14] B. Gassend, D. Lim, D. Clarke, M. van Dijk, and S. Devadas, Identification and authentication of integrated circuits, Concurrency and Computation: Practice and Experience 16(11), p. 1077-1098, 2004.
- [15] M. van Dijk, S. Egner, M. Greferath, and A. Wassermann, On two doubly even self-dual binary codes of length 160 and minimum weight 24, IEEE Trans. on Inform. Theory 51(1), p. 408-411, 2005. The abstract "On binary linear [160, 80, 24] codes" appeared in the Proceedings of ISIT 2003, p. 162, 2003.
- [16] F.M.J. Willems and M. van Dijk, Capacity and codes for embedding information in grayscale signals, IEEE Trans. on Inform. Theory 51(3), p. 1209-1214, 2005.
- [17] D. Lim, J.W. Lee, B. Gassend, G.E. Suh, M. van Dijk, and S. Devadas, Extracting secret keys from integrated circuits, IEEE Trans. VLSI Syst. 13(10), p. 1200-1205, 2005.
- [18] M. van Dijk, D. Clarke, B. Gassend, G.E. Suh, and S. Devadas, Speeding up exponentiation using an untrusted computational resource, Designs, Codes, and Cryptography 39(2), p. 253-273, 2006.
- [19] M. van Dijk, T. Kevenaar, G.J. Schrijen, and P. Tuyls, Improved constructions of secret sharing schemes by applying  $(\lambda, \omega)$ -decompositions, Information Processing Letters 99(4), p. 154-157, 2006. An abstract appeared in the Proceedings of ISIT 2003, p. 282, 2003.
- [20] B. Gassend, C.W. O'Donnell, G.E. Suh, W. Thies, A. Lee, M. van Dijk, and S. Devadas, Learning biophysically-motivated parameters for alpha helix prediction, BMC Bioinformatics 8(5), p. S3, 2007. Poster at 10th Annual International Conference on Research in Computational Molecular Biology (RECOMB 2006), 2006.

- [21] B. Gassend, M. van Dijk, D. Clarke, E. Torlak, S. Devadas, and P. Tuyls, Controlled physical random functions and applications, *ACM Transactions on Information and System Security (TISSEC)* 10(4), p. 15:1-15:22, 2008.

### Conference Contributions

- [22] M. van Dijk, A linear construction of perfect secret sharing schemes, *Advances in Cryptology - Eurocrypt'94, LNCS 950*, p. 23-34, 1995.
- [23] M. van Dijk, Coding Gain Strategies for the Binary Symmetric Broadcast Channel with Confidential Messages, *Proceedings of the 16th Symposium on Information Theory in the Benelux*, May 18 - 19, 53-60, 1995.
- [24] M. van Dijk, The binary symmetric broadcast channel with confidential messages, with tampering, *Proceedings of the EIDMA Winter Meeting on Coding Theory, Information Theory and Cryptology*, December 19-21, p. 42, 1994, and in the *Proceedings of ISIT'95*, September 17-22, p. 487, 1995.
- [25] M. van Dijk and A. Koppelaar, Quantum key agreement, *Proc. of the 18th Symposium on Information Theory in the Benelux*, May 15-16, 97-104, 1997, *Proc. of ISIT'98*, August 16-21, p. 350, 1998.
- [26] M. van Dijk and A. Koppelaar, High rate reconciliation, *Proc. of ISIT'97*, June 28 - July 4, p. 92, 1997.
- [27] M. van Dijk, "The optimal linear worst-case information rate", *Proc. of ISIT'97*, June 28 - July 4, p. 89, 1997.
- [28] J.P. Linnartz and M. van Dijk, Analysis of the sensitivity attack against electronic watermarks in images, *Proceeding of the Workshop on Information Hiding, Portland*, 15-17 April 1998, LNCS 1525, Springer-Verlag, 258-272, 1998.
- [29] T. Kalker, J.P. Linnartz, and M. van Dijk, Watermark estimation through detector analysis, *Proc. of the ICIP, Volume I, Chicago*, October 4-7, 425-429, 1998.
- [30] M. van Dijk and J. Keunig, A quaternary BCH-code based binary quasi-cyclic code construction, *Proc. of the 19th Symposium on Information Theory in the Benelux*, 83-90, 1998.
- [31] M. van Dijk and H. van Tilborg, The art of distilling [secret key generation], invited contribution, *Proc. of the ITW'98, Killarney*, June 22-26, 1998, 158-159, 1998.
- [32] A.G.C. Koppelaar and M. van Dijk, Symbol by symbol APP decoding with a generalized Viterbi decoder, *Proc. of the ITW'99, Kruger National Park, South Africa*, June 20-25, 1999, p. 95, 1999.
- [33] M. van Dijk and R. Motwani, Generalised Trellis Termination, *2<sup>nd</sup> International Symposium on Turbo Codes and Related Topics*, Brest, France, September 2000, 255-258, 2000.
- [34] M. van Dijk, S. Baggen, and L. Tolhuizen, Coding for Informed Decoders, *Proc. of ISIT 2001*, p. 202, 2001.
- [35] M. van Dijk and F.M.J. Willems, Embedding information in gray-scale images, *Proc. 22nd Symp. on Information Theory in the Benelux*, 147-154, 2001.

- [36] F.M.J. Willems and M. van Dijk, Codes for embedding information in gray-scale signals, cdrom Proceedings 39th Annual Allerton Conference on Communication, Control and Computing, Allerton House, Monticello, IL, USA, October 3-5, 2001, SPS-30 [06.11], 2001.
- [37] A. Gorokhov and M. van Dijk, Optimised labelings for bit-interleaved transmission with iterative demodulation, Proc. 22nd Symp. on Information Theory in the Benelux, 2001.
- [38] A. Gorokhov and M. van Dijk, Optimised labeling maps for bit-interleaved transmission with turbo demodulation, VTC 2001, IEEE VTS 53rd, Vol. 2, 2001, 1459-1463, 2001.
- [39] M. Kuijper, M. van Dijk, H. Hollmann, and J. Oostveen, A unifying system theoretic framework for errors-and erasures Reed-Solomon decoding, 14th International Symposium on Applied Algebra and Error-Correcting Codes (AAECC) 2001, 343-352, 2001.
- [40] D. Woodruff and M. van Dijk, Cryptography in an unbounded computational model, Advances in Cryptology - Eurocrypt 2002, LNCS 2332, 149-164, 2002.
- [41] D. Clarke, B. Gassend, T. Kotwal, M. Burnside, M. van Dijk, S. Devadas, and R. Rivest, The untrusted computer problem and camera-based authentication, Proceedings of Pervasive 2002, 114-124, 2002.
- [42] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, Silicon physical random functions, Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS'02), November 2002.
- [43] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, Controlled Physical Random Functions, Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC'02), best student paper award, 149-160, December 2002.
- [44] B. Gassend, D. Clarke, G.E. Suh, M. van Dijk, and S. Devadas, Caches and hash trees for efficient memory integrity verification, Proceedings of the Ninth International Symposium on High Performance Computer Architecture (HPCA-9), 295-306, 2003.
- [45] P. Tuyls, T. Kevenaar, G.J. Schrijen, A.A.M. Staring, and M. van Dijk, Visual crypto displays enabling secure communications, Proceedings of the First International Conference on Security in Pervasive Computing, LNCS 2802, 271-284, 2003.
- [46] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, Delay-based circuit authentication and applications, Proceedings of the 2003 ACM Symposium on Applied Computing (SAC'03), 294-301, 2003.
- [47] G.E. Suh, D. Clarke, B. Gassend, M. van Dijk, and S. Devadas, The AEGIS processor architecture for tamper-evident and tamper-resistant processing, Proceedings of the 17th Annual ACM International Conference on Supercomputing (ICS'03), June 2003.
- [48] D. Clarke, S. Devadas, M. van Dijk, B. Gassend, and G.E. Suh, Incremental multiset hashes and their application to integrity checking, Advances in Cryptology - Asiacrypt 2003, LNCS 2894, 188-207, 2003.
- [49] G.E. Suh, D. Clarke, B. Gassend, M. van Dijk, and S. Devadas, Efficient memory integrity verification and encryption for secure processors, Proceedings of the 36th Annual IEEE/ACM International Symposium on Microarchitecture, 339-351, 2003.

- [50] J.W. Lee, D. Lim, B. Gassend, G.E. Suh, M. van Dijk, and S. Devadas, A technique to build a secret key in integrated circuits for identification and authentication applications, 2004 Symposium on VLSI Circuits, p. 176-179, 2004.
- [51] M. van Dijk and D. Woodruff, Asymptotical optimal communication for torus based cryptography, Advances in Cryptology - Crypto 2004, LNCS 3152, p. 157-178, 2004.
- [52] D. Clarke, G.E. Suh, B. Gassend, A. Sudan, M. van Dijk, and S. Devadas, Towards constant bandwidth overhead integrity checking of untrusted data, IEEE Symposium on Privacy and Security 2005.
- [53] M. van Dijk, R. Granger, D. Page, K. Rubin, A. Silverberg, M. Stam, and D. Woodruff, Practical cryptography in high dimensional tori, Advances in Cryptology - Eurocrypt 2005, p. 234-250, 2005.
- [54] M. van Dijk and P. Tuyls, Robustness, reliability and security of biometric key distillation in the information theoretical setting, Proc. of the 26th Symposium on Information Theory in the Benelux, 2005.
- [55] M. van Dijk and P. Tuyls, Secure biometrics, European Signal Processing Conference (EU-SIPCO 2005), 2005.
- [56] B. Gassend, C.W. O'Donnell, W. Thies, A. Lee, M. van Dijk, and S. Devadas, Predicting secondary structure of all-helical proteins using hidden Markov support vector machines, PRIB 2006, p. 93-104, 2006.
- [57] L.F.G. Sarmanta, M. van Dijk, C.W. O'Donnell, J. Rhodes, and S. Devadas, Virtual monotonic counters and count-limited objects using a TPM without a trusted OS, The First ACM Workshop on Scalable Trusted Computing (ACM STC'06), 2006.
- [58] C.W. O'Donnell, G.E. Suh, M. van Dijk, and S. Devadas, Memoization attacks and copy protection in partitioned applications, Proceedings of the 2007 IEEE Workshop on Information Assurance (IAW 2007), 2007.
- [59] M. van Dijk, J. Rhodes, L.F.G. Sarmanta, and S. Devadas, Offline untrusted storage with immediate detection of forking and replay attacks, The 2nd ACM Workshop on Scalable Trusted Computing (ACM STC'07), 2007.
- [60] L.F.G. Sarmanta, M. van Dijk, J. Rhodes, and S. Devadas, Offline count-limited certificates, Proceedings of the 2008 ACM Symposium on Applied Computing (SAC'08), 2008.
- [61] V. Costan, L.F.G. Sarmanta, M. van Dijk, and S. Devadas, The trusted execution module: commodity general purpose trusted computing, CARDIS 2008.
- [62] M.A. Kinsy, M.H. Cho, T. Wen, E. Suh, M. van Dijk, and S. Devadas, Bandwidth-sensitive deadlock-free oblivious routing, ISCA 2009.

## Book Chapters

- [63] B. Gassend, M. van Dijk, D. Clarke, and S. Devadas. Controlled physical random functions. Chapter 14 in *Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*, eds. P. Tuyls, B. Skoric, and T. Kevenaar, Springer, 235-254, 2007.

## Reports

- [64] E. Torlak, M. van Dijk, B. Gassend, D. Jackson, and S. Devadas, Knowledge flow analysis for security protocols, <http://arxiv.org/abs/cs/0605109>, 2006.
- [65] M. van Dijk, E. Torlak, B. Gassend, and S. Devadas, A generalized two-phase analysis of knowledge flows in security protocols, <http://arxiv.org/abs/cs/0605097>, 2006.

## Issued Patents

- [66] M.E. van Dijk, W.M.J.M. Coene, and C.P.M.J. Baggen, Method of decoding a stream of channel bits of a signal relating to a binary channel signal into a stream of source bits of a signal relating to a binary source signal, US 6362754, 2002.
- [67] H.D.L. Hollmann, M.E. van Dijk, and P.J. Lenoir, Method and device for executing a decrypting mechanism through calculating a standardized modular exponentiation for thwarting timing attacks, US 6366673, 2002.
- [68] M.E. van Dijk, L.M.G.M. Tolhuizen, J.A.H.M. Kahlman, C.P.M.J. Baggen, M. Hattori, K. Yamamoto, T. Narahara, and S. Senshu, Encoding multiword information by wordwise interleaving, US 6367049, 2002.
- [69] M.E. van Dijk, L.M.G.M. Tolhuizen, and C.P.M.J. Baggen, Method and apparatus for encoding multiword information with error locative clues directed to low protectivity words, US 6378100, 2002.
- [70] J.P.M.G. Linnartz, M.J.J.J.-B. Maes, A.A.C.M. Kalker, G.F.G. Depovere, P.M.J. Rongen, C.W.F. Vriens, M.E. van Dijk, Device for optically scanning a record carrier, US 6415040, 2002.
- [71] M.E. van Dijk, W.M.J.M. Coene, and C.P.M.J. Baggen, Information carrier, device for encoding, method for encoding, device for decoding and method for decoding, US 6529147, 2003.
- [72] M.E. van Dijk, W.M.J.M. Coene, and C.P.M.J. Baggen, Information carrier, device for encoding, method for encoding, device for decoding and method for decoding, US 6650257, 2003.
- [73] M.E. van Dijk, C.P.M.J. Baggen, and L.M.G.M. Tolhuizen, Coding for informed decoders, US 7103829, 2006.
- [74] C.P.M.J. Baggen, M.E. van Dijk, and W.M.J.M. Coene, Method of storing or decoding a stream of bits, US 7174497, 2007.
- [75] M.E. van Dijk and K. Yamamoto, Method and apparatus for embedding an additional layer of error correction into an error correcting code, US 7188295, 2007.
- [76] M.E. van Dijk, , K. Yamamoto, and M. Hattori, Method and apparatus for embedding an additional layer of error correction into an error correcting code, US 7340663, 2008.
- [77] M.E. van Dijk and F.M.J. Willems, Embedding auxiliary data in an information signal, US 7392453, 2008.

## Pending Patents

- [78] M.E. van Dijk, Method for encoding a stream of bits of a binary source signal into a stream of bits of a binary channel signal, US 2001/0026594, 2001.

- [79] J.C. Talstra, M.J.J.-B. Maes, H.D.L. Hollmann, and M.E. van Dijk, Copy protection system, US 2002/0026587, 2002.
- [80] S. Egner, C.P.M.J. Baggen, and M.E. van Dijk, Method for generating a serial bitstream comprising information for synchronization, US 2002/0106044, 2002.
- [81] A. Gorokhov, M.E. van Dijk, and A.G.C. Koppelaar, Transmission system for transmitting a multilevel signal, US 2002/0136318, 2002.
- [82] W.M.J.M Coene, M.E. van Dijk, and C.P.M.J. Baggen, Method and device for encoding information words, method and device for decoding information words, storage medium and signal, US 2002/0157055, 2002.
- [83] A.A.M. Staring, M.E. van Dijk, and P.T. Tuyls, Secure data input dialogue using visual cryptography US 2005/0044395, 2005.
- [84] P.T. Tuyls, T.A.M. Kevenaar, G.J. Schrijen, and M.E. van Dijk, Polynomial-based multi-user key generation and authentication method and system. US 2005/0265550, 2005.
- [85] P.T. Tuyls, M.E. van Dijk, B. Schoenmakers, A method and system for generating a common secret. US 2006/0050886, 2006.
- [86] T. Akkermans, A.A.M. Staring, M.E. van Dijk, and P.T. Tuyls, Record carrier with distributed decryption information. US 2006/0104449, 2006.
- [87] P.T. Tuyls and M.E. van Dijk, Key synchronization in a visual cryptographic systems. US 2006/0210080, 2006.
- [88] M.E. van Dijk and P.T. Tuyls, Proof of execution using random function, US 2007/0039046, 2007.
- [89] S. Devadas, B. Gassend, M. van Dijk, and D. Clarke, Controlling access to device-specific information, US 2007/0183194, 2007.
- [90] M.E. van Dijk, Sharing a secret by using random function, US 2008/0059809, 2008.
- [91] M.E. van Dijk, System and method of reliable forward secret key sharing with physical random functions, US 2008/0044027, 2008.
- [92] P.T. Tuyls and M.E. van Dijk, Polynomial-based key distribution system and method, US 2008/0253558, 2008.
- [93] P.T. Tuyls, E. Verbitskiy, B. Schoenmakers, and M.E. van Dijk, Securely computing a similarity measure, US 2009/0006855, 2009.

## Theses

- [94] M. van Dijk, *Graph algorithms*, Master's thesis, Eindhoven University of Technology, The Netherlands, 1991.
- [95] M. van Dijk, *Wyner's wire-tap channel and its cryptographic application*, Master's thesis, Eindhoven University of Technology, The Netherlands, 1993.
- [96] M. van Dijk, *Secret key sharing and secret key generation*, PhD Thesis, Eindhoven University of Technology, The Netherlands, 1997.