**Marten van Dijk** Curriculum Vitae
Email: vandijk@engr.uconn.edu

## 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

## Professional Experience

***ECE Department, University of Connecticut*** 2016 - present
Charles H. Knapp Associate Professor

***ECE Department, University of Connecticut*** 2013 - 2015
Associate Professor

***MIT Computer Science and Artificial Intelligence Laboratory*** 2013
Research Scientist

***RSA Laboratories*** 2010 - 2012
Consultant Research Analyst

***MIT Computer Science and Artificial Intelligence Laboratory*** 2005 - 2010
Research Scientist

***Philips Research Laboratories, the Netherlands*** 2001 - 2005
Visting research scientist at MIT CSAIL

***Philips Research Laboratories, the Netherlands***
Research Scientist in the Digital Signal Processing group 1996 - 2001

***Chinese University of Hong Kong*** 1996
Cryptology Research Associate

## Teaching Experience

Lecturer "Secure Computation and Storage (ECE 6095 / CSE 5095)" Spring 2016
Lecturer "Microprocessor Application Lab (ECE 3411)" Fall 2015
Lecturer "Natural Computing (ECE 6095)" Spring 2015
Lecturer "Numerical Methods in Scientific Computing (ECE 3431 / CSE 3802)" Fall 2015
Lecturer "Microprocessor Application Lab (ECE 3411)" Spring 2014
Recitation instructor "Computer System Engineering (6.033)" at MIT Spring 2013
Lecturer "Mathematics for Computer Science (6.042)" at MIT Fall 2010
Lecturer "Design and Analysis of Algorithms (6.046)" at MIT Spring 2009
Lecturer "Mathematics for Computer Science (6.042)" at MIT Fall 2008

Recitation instructor "Computer System Engineering (6.033)" at MIT Spring 2008
Teaching assistant "Introduction to Algorithms (6.046)" at MIT Spring 2007
Teaching assistant "Introduction to Algorithms (6.046)" at MIT Fall 2005

Invited as a guest lecturer by the Euler Institute for Discrete Mathematics and its Applications (EIDMA) to develop and teach a series of 4 lectures on secret sharing every two years, as part of an advanced cryptography course for graduate students from various Dutch and Belgium universities. 1996-2001

Teaching assistant at the Eindhoven University of Technology in the Netherlands for the courses Matrix Theory I and II over two consecutive years for undergraduate students in architecture and business. 1992-1994

## Awards

A. Richard Newton Technical Impact Award in Electronic Design Automation 2015
AEGIS: Architecture for Tamper-Evident and TamperResistant Processing selected for inclusion in the 25 years of International Conference on Supercomputing" 2014
CCS Best Student Paper Award (one of 3) 2013
NYU-Poly AT&T Best Applied Security Paper Award, 3rd place 2012
Nominated for best paper award Eurocrypt'10 (Invited to J. Cryptology, one of 3 papers selected) 2010
ACSAC'02 outstanding student paper award, http://www.acsac.org/ 2002

Charles H. Knapp Associate Professor 2016
Electrical and Computing Engineering Research Award (UConn) 2015

## Funding

NSF (Self-Recovering Certificate Authorities using Backward and Forward Secure Key Management) for $325K 2016
Comcast Center for Excellence (User and Embedded Systems Authentication) for $65K plus an additional $35K fellowship 2016
Comcast Center for Excellence (several projects) for $195K plus an additional $96K fellowship 2015
NSF Frontier (A Modular Approach to Cloud Security) for $10M 2014
MURI (Development of Universal Theory for Evaluation and Design of Nanoscale Devices) for $7.5M 2014
UTRC (Tagged Architectures for Hardware Trojan Detection) for $25K 2014
CHASE (Gideon: A High Performance HW Interface for Guaranteed Detection of Executed Injected Malicious Code) for $100K 2013
NSF (Applications and Evolution of TPM Technology) for $500K 2007

## 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. Gehrmann, 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 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.

[22] Ulrich Rührmair and Marten van Dijk, On the practical use of physical unclonable functions in oblivious transfer and bit commitment protocols. J. Cryptographic Engineering 3(1): p. 17-28, 2013.

[23] M. van Dijk, A. Juels, A. Oprea, and R. L. Rivest, FlipIt: The Game of "Stealthy Takeover", J. Cryptology 26(4): p. 655-713, 2013.

[24] C. Fletcher, M. van Dijk, and S. Devadas, Lets stop trusting software with our sensitive data, The Last Byte, Design and Test, IEEE 30(2): p. 103-104, 2013.

[25] S.K. Haider, D.M. Shila, and M. van Dijk, Security Agents for Embedded Intrusion Detection, Circuit Cellar 297, April 2015.

[26] C. Herder, L. Ren, M. van Dijk, M.-D. Yu, and S. Devadas, Trapdoor Computational Fuzzy Extractors and Stateless Cryptographically-Secure Physical Unclonable Functions, accepted for publication in IEEE Transactions on Dependable and Secure Computing.

## Conference Contributions

[27] M. van Dijk, A linear construction of perfect secret sharing schemes, Advances in Cryptology - Eurocrypt'94, LNCS 950, p. 23-34, 1995.

[28] 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.

[29] 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.

[30] 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.

[31] M. van Dijk and A. Koppelaar, High rate reconciliation, Proc. of ISIT'97, June 28 - July 4, p. 92, 1997.

[32] M. van Dijk, "The optimal linear worst-case information rate", Proc. of ISIT'97, June 28 - July 4, p. 89, 1997.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] M. van Dijk and R. Motwani, Generalised Trellis Termination, $2^{nd}$ International Symposium on Turbo Codes and Related Topics, Brest, France, September 2000, 255-258, 2000.

[39] M. van Dijk, S. Baggen, and L. Tolhuizen, Coding for Informed Decoders, Proc. of ISIT 2001, p. 202, 2001.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] D. Woodruff and M. van Dijk, Cryptography in an unbounded computational model, Advances in Cryptology - Eurocrypt 2002, LNCS 2332, 149-164, 2002.

[46] 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.

[47] 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.

[48] 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.

[49] 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.

[50] 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.

[51] 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.

[52] 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.

[53] 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.

[54] 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.

[55] 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.

[56] M. van Dijk and D. Woodruff, Asymptotical optimal communication for torus based cryptography, Advances in Cryptology - Crypto 2004, LNCS 3152, p. 157-178, 2004.

[57] 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.

[58] 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.

[59] 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.

[60] M. van Dijk and P. Tuyls, Secure biometrics, European Signal Processing Conference (EUSIPCO 2005), 2005.

[61] 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.

[62] L.F.G. Sarmenta, 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.

[63] 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.

[64] M. van Dijk, J. Rhodes, L.F.G. Sarmenta, 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.

[65] L.F.G. Sarmenta, M. van Dijk, J. Rhodes, and S. Devadas, Offline count-limited certificates, Proceedings of the 2008 ACM Symposium on Applied Computing (SAC'08), 2008.

[66] V. Costan, L.F.G. Sarmenta, M. van Dijk, and S. Devadas, The trusted execution module: commodity general purpose trusted computing, CARDIS 2008.

[67] M.A. Kinsy, M.H. Cho, T. Wen, E. Suh, M. van Dijk, and S. Devadas, Bandwidth-sensitive deadlock-free oblivious routing, ISCA 2009.

[68] M. van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan, Fully homomorphic encryption over the integers, Eurocrypt 2010, 24-43, 2010.

[69] M. van Dijk and A. Juels, On the impossibility of cryptography alone for privacy-preserving cloud computing, HotSec 2010.

[70] T. Denning, K. D. Bowers, M. van Dijk and A. Juels: Exploring implicit memory for painless password recovery, CHI 2011, 2615-2618, 2011.

[71] K. D. Bowers, M. van Dijk, A. Juels, A. Oprea, R. L. Rivest, How to tell if your cloud files are vulnerable to drive crashes, ACM Conference on Computer and Communications Security 2011, 501-514, 2011.

[72] U. Rührmair and M. van Dijk: Practical security analysis of PUF-based two-player protocols, CHES 2012, 251-267, 2012.

[73] Marten van Dijk, Ari Juels, Alina Oprea, Ronald L. Rivest, Emil Stefanov, Nikos Triandopoulos, Hourglass schemes: how to prove that cloud files are encrypted. ACM Conference on Computer and Communications Security 2012, 265-280, 2012.

[74] C. Fletcher, M. van Dijk and S. Devadas, Secure processor architecture for encrypted computation on untrusted programs, STC'12, 2012.

[75] C. Fletcher, M. van Dijk and S. Devadas, Towards an interpreter for efficient encrypted computation, CCSW'12, 2012.

[76] K. D. Bowers, M. van Dijk, R. Griffin, A. Juels, A. Oprea, R. L. Rivest and N. Triandopoulos, Defending against the unknown enemy: Applying FlipIt to system security, GameSec'12, 2012.

[77] E. Stefanov, M. van Dijk, A. Oprea and A. Juels, Iris: A scalable cloud file system with efficient integrity checks, ACSAC'12, 2012.

[78] Ulrich Rührmair and Marten van Dijk. PUFs in Security Protocols: Attack Models and Security Evaluations. IEEE Symposium on Security and Privacy 2013: p. 286-300, 2013.

[79] L. Ren, X. Yu, C. Fletcher, M. van Dijk, and S. Devadas. Design Space Exploration and Optimization of Path Oblivious RAM in Secure Processors. In Proceedings of the International Symposium on Computer Architecture (ISCA) 2013, pp 571-582. Available at IACR Cryptology ePrint Archive, Report 2012/76.

[80] L. Ren, C.W. Fletcher, X. Yu, M. van Dijk and S. Devadas. Integrity Verification for Path Oblivious-RAM. IEEE High Performance Extreme Computing Conference (HPEC) 2013.

[81] E. Stefanov, M. van Dijk, E. Shi, C.W. Fletcher, L. Ren, X. Yu, and S. Devadas. Path ORAM: An Extremely Simple Oblivious RAM Protocol. Proceedings of the ACM Conference on Computer and Communications Security (CCS) 2013. Available at IACR Cryptology ePrint Archive, Report 2013/280.

[82] X. Yu, C.W. Fletcher, L. Ren, M. van Dijk and S. Devadas. Generalized External Interaction with Tamper-Resistant Hardware with Bounded Information Leakage. CCSW'13, 2013.

[83] C.W. Fletcher, L. Ren, X. Yu, M. van Dijk, O. Khan and S. Devadas. Suppressing the Oblivious RAM timing channel while making information leakage and program efficiency trade-offs. HPCA 2014: 213-224.

[84] M. van Dijk and U. Rührmair. Protocol attacks on advanced PUF protocols and countermeasures. DATE 2014: 1-6.

[85] M. van Dijk and U. Rührmair. PUF Interfaces and their Security. ISVLSI 2014.

[86] G.E. Suh, C.W. Fletcher, D.E. Clarke, B. Gassend, M. van Dijk, and S. Devadas. Author retrospective AEGIS: architecture for tamper-evident and tamper-resistant processing. ICS 25th Anniversary 2014: 68-70.

[87] V. Grindle, S.K. Haider, J. Magee, and M. van Dijk. Virtual Fingerprint – Image-Based Authentication Increases Privacy for Users of Mouse-Replacement Interfaces. HCI International 2015.

[88] C.W. Fletcher, L. Ren, A. Kwon, M. van Dijk, and S. Devadas. Freecursive ORAM: [Nearly] Free Recursion and Integrity Verification for Position-based Oblivious RAM. ASPLOS 2015: 103-116.

[89] C. Fletcher, L. Ren, A. Kwon, M. van Dijk, E. Stefanov, D. Serpanos, and S. Devadas. Tiny ORAM: A Low-Latency, Low-Area Hardware ORAM Controller. FCCM 2015.

[90] A. Masab, S.K. Haider, F. Hijaz, M. van Dijk, and O. Khan. Exploring the Performance Implications of Memory Safety Primitives in Many-core Processors Executing Multi-threaded Workloads. HASP 2015.

[91] X. Yu, S.K. Haider, L. Ren, C.W. Fletcher, A. Kwon, M. van Dijk, and S. Devadas. PrORAM: dynamic prefetcher for oblivious RAM. ISCA 2015: 616-628.

[92] L. Ren, C. Fletcher, A. Kwon, E. Stefanov, E. Shi, M. van Dijk, and S. Devadas. Constants Count: Practical Improvements to Oblivious RAM. Usenix Security 2015.

[93] S.K. Haider, M. Ahmad, F. Hijaz, A. Patni, E. Johnson, M. Seita, Omer Khan, and M. van Dijk. M-MAP: Multi-Factor Memory Authentication for Secure Embedded Processors. IEEE International Conference on Computer Design (ICCD 2015).

[94] M. van Dijk. Hardware Security and its Adversaries. TrustED 2015.

[95] S. Devadas, M. van Dijk, C.W. Fletcher, L. Ren, E. Shi, and D.Wichs. Onion ORAM: A Constant Bandwidth Blowup Oblivious RAM. TCC 2016.

## Book Chapters

[96] 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

[97] 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.

[98] 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.

[99] M. van Dijk and U. Rührmair, Physical unclonable functions in cryptographic protocols: Security proofs and impossibility results. IACR Cryptology ePrint Archive 2012: 228, 2012.

## Issued Patents

[100] 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.

[101] 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.

[102] 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.

[103] 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.

[104] 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.

[105] 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.

[106] 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.

[107] M.E. van Dijk, C.P.M.J. Baggen, and L.M.G.M. Tolhuizen, Coding for informed decoders, US 7103829, 2006.

[108] 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.

[109] 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.

[110] 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.

[111] M.E. van Dijk and F.M.J. Willems, Embedding auxiliary data in an information signal, US 7392453, 2008.

[112] M.E. van Dijk, System and method of reliable forward secret key sharing with physical random functions, US 7653197, 2010.

[113] D. Clarke, B. Gassend, M. van Dijk and S. Devadas, Authentication of integrated circuits, US 7840803, 2010.

[114] M.E. van Dijk and P.T. Tuyls, Proof of execution using random function, US 7877604, 2011.

[115] P.T. Tuyls, E. Verbitskiy, B. Schoenmakers, and M.E. van Dijk, Securely computing a similarity measure, US 8281148, 2012.

[116] A. Juels, M.E. van Dijk, A.M. Oprea, R.L. Rivest, E.P. Stefanov, Remote verification of file protections for cloud storage, US 8346742, 2013.

[117] M. van Dijk, A. Juels, B.W. Fitzgerald, and G. Matthews, Providing a security-sensitive environment, US 8621649, 2013.

[118] M. van Dijk, K.D. Bowers, S. Curry, S.P. Doyle, W.M. Duane, A. Juels, M.J. O'Malley, N. Triandopoulos, and R. Zolfonoon, Soft token posture asessment, US 8683563, 2014.

[119] M. van Dijk, K.D. Bowers, S. Curry, and N. Triandopoulos, Scheduling soft token data transmission, US 8683570, 2014.

[120] E.P. Stefanov, M.E. van Dijk, A.M. Oprea, and A. Juels, Scalable cloud file system with efficient integrity checks, US 8706701, 2014.

[121] M. van Dijk, K.D. Bowers, S. Curry, S.P. Doyle, N. Triandopoulos, and R. Zolfonoon, Providing authentication codes which include token codes and biometric factors, US 8752146, 2014.

[122] M. van Dijk, K.D. Bowers, S. Curry, S.P. Doyle, N. Triandopoulos, and R. Zolfonoon, Detecting soft token copies, US 8752156, 2014.

[123] E.P. Stefanov, M.E. van Dijk, A.M. Oprea, and A. Juels, Remote verification of file protections for cloud data storage, US 8799334, 2014.

[124] K.D. Bowers, M.E. van Dijk, A. Juels, A.M. Oprea, R.L. Rivest, and N. Triandopoulos, Graph-based approach to deterring persistent security threats, US 8813234, 2014.

[125] R. Stockton, R.D. Hopley, M. van Dijk, A. Juels, and N. Triandopoulos, Variable epoch scheduler for proactive cryptography systems, US 8817988, 2014.

[126] M. van Dijk, K.D. Bowers, S. Curry, S.P. Doyle, E. Kolman, N. Triandopoulos, and R. Zolfonoon, Managing user access with mobile device posture, US 8819769, 2014.

[127] M. van Dijk, K.D. Bowers, J.G. Brainard, S. Curry, S.P. Doyle, M.J. O'Malley, and N. Triandopoulos, Controlling a soft token running within an electronic apparatus, US 8875263, 2014.

[128] S. Devadas, M. van Dijk, and C.W. Fletcher, Technique for secure computation, US 8909967, 2014.

[129] M. van Dijk, S.J. Curry, R.D. Hopley, J.G. Linn, A.M. Oprea, and R. Kenneth, Methods and apparatus for mediating access to derivatives of sensitive data, US 8978159, 2015.

[130] A. Juels, N. Triandopoulos, R. Rivest, and M. van Dijk, Methods and apparatus for embedding auxiliary information in one-time passcodes, US 8984609, 2015.

[131] R. Hodgman, M.E. van Dijk, and E. Kolman, Distributed anonymized communications, US 9015231, 2015.

[132] M. van Dijk, N. Triandopoulos, A. Juels, and R. Rivest, Forward secure pseudorandom number generation resilient to forward clock attacks, US 9083515, 2015.

[133] A. Juels, N. Triandopoulos, M.E. van Dijk, Methods and apparatus for authenticating a user using multi-server one-time passcode verification, US 9118661, 2015.

[134] S. Curry and M. van Dijk, Software license management with drifting component, US 9122878, 2015.

[135] J. Brainard, N. Triandopoulos, M. van Dijk, and A. Juels, Event-based data signing via time-based one-time authentication passcodes, US 9225717, 2015.

[136] A. Juels, A.M. Oprea, M.E. van Dijk, and E.P. Stefanov, Remote verification of file protections for cloud data storage, US 9230114, 2016.

[137] A. Juels, N. Triandopoulos, M. van Dijk, J. Brainard, R. Rivest, and K. Bowers, Configurable one-time authentication tokens with improved resilience to attacks, US 9270655, 2016.

[138] A. Juels, N. Triandopoulos, M. van Dijk, J. Brainard, R. Rivest, and K. Bowers, Server methods and apparatus for processing passcodes generated by configurable one-time authentication tokens, US 9294473, 2016.

[139] E.P. Stefanov, M.E. van Dijk, A.M. Operea, and A. Juels, Scalable cloud file system with efficient integrity checks, US 9323765, 2016.

## Theses

[140] M. van Dijk, *Graph algorithms*, Master's thesis, Eindhoven University of Technology, The Netherlands, 1991. Anne Kaldewaij, advisor.

[141] M. van Dijk, *Wyner's wire-tap channel and its cryptographic application*, Master's thesis, Eindhoven University of Technology, The Netherlands, 1993. Henk van Tilborg, advisor.

[142] M. van Dijk, *Secret key sharing and secret key generation*, PhD Thesis, Eindhoven University of Technology, The Netherlands, 1997. Henk van Tilborg, advisor.