Shai Halevi

Research Fellow, Algorand Foundation
shai@algorand.foundation
shaih@alum.mit.edu
http://alum.mit.edu/www/shaih

Professional Interest.

Cryptography and secure systems, Algorithms.

Employment.

2019-present: Research fellow, Algorand Foundation
1997-2019: Principal Research Staff Member, IBM Research

Professional activities.

Program co-chair, the 23rd ACM Conference on Computer and Communications Security (ACM-CCS 2016).

Program chair, the 29th International Cryptology Conference (CRYPTO 2009).

General and Program co-chair, the 3rd Theory of Cryptography Conference (TCC 2006).

Program committee member for CRYPTO 2000, EUROCRYPT 2001, CT-RSA 2002, PKC 2002, ACNS 2003, EUROCRYPT 2005, CRYPTO 2005, VietCrypt 2006, CT-RSA 2007, EUROCRYPT 2007, ISC 2007, ASIACRYPT 2007, EUROCRYPT 2008, ISC 2008, ASIACRYPT 2009, Pairing 2010, TCC 2011, Pairing 2012, PKC 2013, CRYPTO 2013, TCC 2015, Eurocrypt 2016, ACM-CCS 2017, ACNS 2018, Eurocrypt 2019

Editorial board member, ACM TISSEC, 2009-2012.

The International Association for Cryptographic Research (IACR): Membership secretary and board member 2006-2011, Director and board member 2012-2014, 2015-present. Chair of the steering committee for the Theoretical Cryptography Conference (TCC), 2013-present.

Developing an open-source library for homomorphic encryption, available off of https://github.com/homenc/HElib.

Wrote and still maintains a web-software-package for submission and review of papers to conferences (available off of http://alum.mit.edu/www/shaih/websubrev).

Invited talks at conferences and schools. Keynote ACM-CCS 2018; ICMC 2018; CRYPTO 2015; China Summer School on Lattices and Cryptography in ISCAS Beijing June 2014; PKC 2014; Tutorial on Homomorphic Encryption CRYPTO 2011; Winter School on Secure Computation and Efficiency in Bar-Ilan University Winter 2011; Usenix Security 2009; SCN 2008; TCC 2007;

Awards.

- SIGSAC Outstanding Innovation Award, 2017.
- IACR fellow, 2016.
- IBM Research 2013 Pat Goldberg Memorial Best Paper Award: “Candidate Multilinear Maps from Ideal Lattices”, Garg, Gentry, Halevi, EUROCRYPT 2013.
- Eurocrypt 2013 best-paper award, “Candidate Multilinear Maps from Ideal Lattices”, Garg, Gentry, Halevi.
- IBM Research 2012 Pat Goldberg Memorial Best Paper Award: “Homomorphic Evaluation of the AES Circuit”, Gentry, Halevi, Smart, , EUROCRYPT 2012.
- IBM Corporate Award 2007.
- IBM Research 2004 Pat Goldberg Memorial Best Paper Award: “The Random Oracle Methodology, Revisited”, Canetti, Goldreich, Halevi, Journal of the ACM.
- Certificate of Appreciation from the Kneset (the Israeli parliament), 1991.
- Technion President’s List of Distinction, 1989, 1990.

Education.

Massachusetts Institute of Technology — Cambridge, MA
Ph.D. degree in Computer Science, June 1997. Research area - Cryptography and Secure computations. Advisor: Prof. Silvio Micali.

Technion - Israel Institute of Technology — Haifa, Israel
M.Sc. degree in Computer Science, August 1993. Advisor: Prof. Assaf Schuster.
B.A. degree in Computer Science *Summa Cum Laude*, August 1991.

Patents.

- US10057057, Homomorphic evaluation including key switching, modulus switching, and dynamic noise management, 2018-08-21
- US8958555, Fast Computation of a Single Coefficient in an Inverse Polynomial, 2015-02-17
- US8903083, Fast evaluation of many polynomials with small coefficients on the same point, 2014-12-2
- US8861716, Efficient homomorphic encryption scheme for bilinear forms, 2014-10-14
- US8656186, Use of indirect data keys for encrypted tape cartridges, 2014-02-18
- US8565435, Efficient implementation of fully homomorphic encryption, 2013-10-22
- US8532289, Fast Computation Of A Single Coefficient In An Inverse Polynomial, 2013-09-10

- US8494166, Use of indirect data keys for encrypted tape cartridges, 2013-07-23
- US8422681, Non-interactive hierarchical identity-based key-agreement, 2013-04-16
- US8121286, Hash function with provable resistance to differential attacks, 2012-02-21
- US8108683, Mitigating dictionary attacks on password-protected local storage, 2012-01-31
- US8099781, Method of managing and mitigating security risks through planning, 2012-01-17
- US8087090, Fuzzy multi-level security, 2011-12-27
- US7965844, System and method for processing user data in an encryption pipeline, 2011-06-21
- US7921294 Verification of encryption key, 2011-04-05
- US7832007 Method of managing and mitigating security risks through planning, 2010-11-09
- US7530110, System and method for fuzzy multi-level security, 2009-05-05
- US7236592, Efficient stream cipher system and method, 2007-06-26
- US6578144, Secure hash-and-sign signatures, 2003-06-10
- US6317834, Biometric authentication system with encrypted models, 2001-11-13
- US6243470, Method and apparatus for advanced symmetric key block cipher with variable length key and block, 2001-06-05
- US6192129, Method and apparatus for advanced byte-oriented symmetric key block cipher with variable length key and block 2001-02-20
- US6189095, Symmetric block cipher using multiple stages with modified type-1 and type-3 feistel networks, 2001-02-13
- US6185679, Method and apparatus for a symmetric block cipher using multiple stages with type-1 and type-3 feistel networks, 2001-02-06
- US6185304, Method and apparatus for a symmetric block cipher using multiple stages

Publications.

Refereed Conferences

[BHHH19] Homomorphic Training of 30,000 Logistic Regression Models, Flavio Bergamaschi, Shai Halevi, Tzipora Halevi, and Hamish Hunt, ACNS 2019.

[HPS19] An Improved RNS Variant of the BFV Homomorphic Encryption Scheme, Shai Halevi and Yuriy Polyakov and Victor Shoup. RSA-CT 2019.

[HIKR18] Best Possible Information-Theoretic MPC, Shai Halevi, Yuval Ishai, Eyal Kushilevitz, and Tal Rabin. TCC 2018.

[CGHPS18] Doing Real Work with FHE: The Case of Logistic Regression, Jack L.H. Crawford, Craig Gentry, Shai Halevi, Daniel Platt and Victor Shoup. WAHC 2018.

[HS18] Faster Homomorphic Linear Transformations in HElib, Shai Halevi and Victor Shoup. CRYPTO 2018.

[HHPV18] Round-Optimal Secure Multi-Party Computation, Shai Halevi, Carmit Hazay, Antigoni Polychroniadou, and Muthuramakrishnan Venkitasubramaniam. CRYPTO 2018.

[AHLR18] Privacy-Preserving Search of Similar Patients in Genomic Data, Gilad Asharov, Shai Halevi, Yehuda Lindell, and Tal Rabin, PoPETS 2018.

[BHH18] Supporting Private Data on Hyperledger Fabric with Secure Multiparty Computation, Fabrice Benhamouda, Shai Halevi, and Tzipora Halevi. In the 1st IEEE Workshop on Blockchain Technologies and Applications, BTA 2018.

[BHP17] Non-Interactive Multiparty Computation without Correlated Randomness, Shai Halevi, Yuval Ishai, Abhishek Jain, Ilan Komargodski, Amit Sahai, and Eylon Yogev. Asiacrypt 2017.

[BHP17] Four Round Secure Computation without Setup, Zvika Brakerski, Shai Halevi, and Antigoni Polychroniadou. TCC 2017.

[HHSS17] Implementing BP-Obfuscation Using Graph-Induced Encoding, Shai Halevi and Tzipora Halevi and Victor Shoup and Noah Stephens-Davidowitz. ACM-CCS 2017.

[CGH17] Cryptanalyses of Candidate Branching Program Obfuscators, Yilei Chen, Craig Gentry, and Shai Halevi. EUROCRYPT 2017 (part 3), LNCS vol. 10212, pages 278–307. Springer, 2017.

[DHRW16] Spooky Encryption and its Applications, Yevgeniy Dodis, Shai Halevi, Ron D. Rothblum, Daniel Wichs. CRYPTO 2016.

[GGHZ16] Secure Multiparty Computation with General Interaction Patterns, Shai Halevi, Yuval Ishai, Abhishek Jain, Eyal Kushilevitz, Tal Rabin. ITCS 2016: 157-168.

[GGHZ16] Functional Encryption Without Obfuscation, Sanjam Garg, Craig Gentry, Shai Halevi, Mark Zhandry. TCC (A2) 2016: 480-511.

[GHJR15] Private Database Access with HE-over-ORAM Architecture, Craig Gentry, Shai Halevi, Charanjit S. Jutla and Mariana Raykova. ACNS 2015: 172-191.

[CGH+15] Zeroizing Without Low-Level Zeroes: New MMAP Attacks and their Limitations, Jean-Sébastien Coron, Craig Gentry, Shai Halevi, Tancréde Lepoint, Hemanta K. Maji, Eric Miles, Mariana Raykova, Amit Sahai and Mehdi Tibouchi. CRYPTO (1) 2015: 247-266.

[HS15] Bootstrapping for HElib, Shai Halevi and Victor Shoup. EUROCRYPT (1) 2015: 641-670.

[GGH15] Graph-Induced Multilinear Maps from Lattices, Craig Gentry, Sergey Gorbunov and Shai Halevi. TCC (2) 2015: 498-527.

[GHRW14] Outsourcing Private RAM Computation, Craig Gentry, Shai Halevi, Mariana Raykova and Daniel Wichs. FOCS 2014.

[GGHW14] On the Implausibility of Differing-Inputs Obfuscation and Extractable Witness Encryption with Auxiliary Input, Sanjam Garg, Craig Gentry, Shai Halevi and Daniel Wichs. CRYPTO 2014.

[HS14] Algorithms in HElib, Shai Halevi and Victor Shoup. CRYPTO 2014.

[GHL+14] Garbled RAM Revisited, Craig Gentry, Shai Halevi, Steve Lu, Rafail Ostrovsky, Mariana Raykova and Daniel Wichs. EUROCRYPT 2014, LNCS vol. 8441, pages 405-422, Springer 2014.

[BGG+14] Fully Key-Homomorphic Encryption, Arithmetic Circuit ABE and Compact Garbled Circuits, Dan Boneh, Craig Gentry, Sergey Gorbunov, Shai Halevi, Valeria Nikolaenko, Gil Segev, Vinod Vaikuntanathan and Dhinakaran Vinayagamurthy. EUROCRYPT 2014, LNCS vol. 8441, pages 533-556, Springer 2014.

[GGHR14] Two-round secure MPC from Indistinguishability Obfuscation, Sanjam Garg, Craig Gentry, Shai Halevi and Mariana Raykova. TCC 2014, LNCS vol. 8349, pages 74-94, Springer 2014.

[AGHS13] Discrete Gaussian Leftover Hash Lemma over Infinite Domains, Shweta Agrawal, Craig Gentry, Shai Halevi and Amit Sahai. Asiacrypt 2013, LNCS vol. 8269, pages 97-166, Springer 2013.

[GGHR+13] Candidate Indistinguishability Obfuscation and Functional Encryption for all circuits,Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. FOCS 2013, IEEE, 2013.

[GGHS+13] Attribute-Based Encryption for Circuits from Multilinear Maps, Sanjam Garg, Craig Gentry, Shai Halevi, Amit Sahai, and Brent Waters. CRYPTO 2013, LNCS vol. 8043, pages 479-499, Springer, 2013.

[GGHJ+13] Optimizing ORAM and Using It Efficiently for Secure Computation. Craig Gentry, Kenny A. Goldman, Shai Halevi, Charanjit S. Jutla, Mariana Raykova, and Daniel Wichs. Privacy Enhancing Technologies, PETS 2013, LNCS vol. 7981, pages 1-18, Springer, 2013.

[BGHWW13] Private Database Queries Using Somewhat Homomorphic Encryption, Dan Boneh, Craig Gentry, Shai Halevi, Frank Wang and David J. Wu. In ACNS 2013, LNCS vol. 7954, pages 102-118, Springer, 2013.

[GGH13] Candidate Multilinear Maps from Ideal Lattices, Sanjam Garg, Craig Gentry, and Shai Halevi, In EUROCRYPTO 2013, LNCS vol. 7881, pages 1-17, Springer, 2013. Received the best-paper award.

[BGH13] Packed Ciphertexts in LWE-Based Homomorphic Encryption, Zvika Brakerski, Craig Gentry, and Shai Halevi. In PKC 2013, LNCS vol. 7778, pages 1-13, Springer 2013.

[GHPS12] Ring Switching in BGV-Style Homomorphic Encryption Craig Gentry, Shai Halevi, Chris Peikert, and Nigel P. Smart. In SCN 2012, LNCS vol. 7485, pages 19-37, Springer, 2012.

[GHS12c] Homomorphic Evaluation of the AES Circuit. Craig Gentry, Shai Halevi, and Nigel P. Smart. In CRYPTO 2012, LNCS vol. 7417, pages 850-867, Springer, 2012.

[GHS12b] Better Bootstrapping in Fully Homomorphic Encryption. Craig Gentry, Shai Halevi, and Nigel P. Smart. In PKC 2012, LNCS vol. 7293, pages 1-16, Springer, 2012.

[GHS12a] Fully Homomorphic Encryption with Polylog Overhead. Craig Gentry, Shai Halevi, and Nigel Smart. In Eurocrypt 2012, LNCS vol. 7237, pages 465-482, Springer 2012.

[BCH12] Leakage Tolerant Interactive Protocols. Nir Bitansky, Ran Canetti, and Shai Halevi. In TCC 2012, LNCS vol. 7194, pages 266-284, Springer 2012.

[BCG+11] Program Obfuscation with Leaky Hardware, Nir Bitansky, Ran Canetti, Shafi Goldwasser, Shai Halevi, Yael Tauman Kalai, Guy N. Rothblum: ASIACRYPT 2011, LNCS 7073, pages 722-739, Springer 2011.

[GH11b] Fully Homomorphic Encryption without Squashing Using Depth-3 Arithmetic Circuits, Craig Gentry and Shai Halevi. FOCS 2011.

[HHPP11] Proofs of Ownership in Remote Storage Systems, Shai Halevi, Danny Harnik, Benny Pinkas, Alexandra Shulman-Peleg, ACM-CCS 2011.

[HLP11] Secure Computation on the Web: Computing without Simultaneous Interaction Shai Halevi, Yehuda Lindell and Benny Pinkas, In CRYPTO 2011, LNCS vol. 6841, pages 132-150, Springer, 2011.

[CCH+11] Composable Security Analysis of OS Services, Ran Canetti, Suresh Chari, Shai Halevi, Birgit Pfitzmann, Arnab Roy, Michael Steiner, and Wietse Venema. In ACNS 2011, LNCS vol. 6715, pages 431-448, Springer, 2011.

[GH11a] Implementing Gentry's Fully-Homomorphic Encryption Scheme, Craig Gentry and Shai Halevi. In EUROCRYPT 2011, LNCS vol. 6632, pages 129-148, Springer 2011.

[HL11] After-the-Fact Leakage in Public-Key Encryption, Shai Halevi and Huijia Lin. In TCC 2011, LNCS vol. 6597, pages 107-124, Springer, 2011.

[HKr11] One-Pass HMQV and Asymmetric Key-Wrapping, Shai Halevi and Hugo Krawczyk. In PKC 2011, LNCS vol. 6571, pages 317-334, Springer, 2011.

[GHV10b] i-Hop Homomorphic Encryption Schemes, Craig Gentry, Shai Halevi and Vinod Vaikuntanathan. In Advances in Cryptography - CRYPTO'10, LNCS vol. 6223, pages 155-172, Springer, 2010.

[GHV10a] A Simple BGN-type Cryptosystem from LWE, Craig Gentry, Shai Halevi and Vinod Vaikuntanathan. In Advances in Cryptography - EUROCRYPT'10, LNCS vol. 6110, pages 506-522, Springer, 2010.

[vDGHV10] Fully Homomorphic Encryption over the Integers. Marten van Dijk, Craig Gentry, Shai Halevi and Vinod Vaikuntanathan. In Advances in Cryptography - EUROCRYPT'10, LNCS vol. 6110, pages 24-43, Springer, 2010.

[CHV10] Where Do You Want to Go Today? Escalating Privileges by Pathname Manipulation, Suresh Chari, Shai Halevi, and Wietse Venema. NDSS 2010.

[AGHK09] Attacking Cryptographic Schemes Based on ”Perturbation Polynomials”, Martin Albrecht, Craig Gentry, Shai Halevi, and Jonathan Katz. 15th ACM-CCS, pages 1-10, 2009.

[GH09b] More on Key Wrapping, Rosario Gennaro and Shai Halevi. Workshop on Selected Areas in Cryptography - SAC 2009. LNCS vol. 5867, pages 53-70. Springer, 2009.

[HSH09] Using HB Family of Protocols for Privacy-Preserving Authentication of RFID Tags in a Population, Tzipora Halevi, Nitesh Saxena, and Shai Halevi. The 5th Workshop on RFID Security, 2009.

[GH09a] Hierarchical Identity Based Encryption with Polynomially Many Levels, Craig Gentry and Shai Halevi. The 6th Theory of Cryptography Conference - TCC'09. LNCS vol. 5444, pages 437-456. Springer, 2009.

[GHKRRW08] Strongly-Resilient and Non-Interactive Hierarchical Key-Agreement in MANETs, Rosario Gennaro, Shai Halevi, Hugo Krawczyk, Tal Rabin, Steffen Reidt, and Stephen D. Wolthusen. Proceedings of Computer Security - ESORICS'08, LNCS vol. 5283, pages 49-65, Springer, 2008.

[BHHO08] Circular-Secure Encryption from Decision Diffie-Hellman, Dan Boneh, Shai Halevi, Mike Hamburg, and Rafail Ostrovsky. In Advances in Cryptography - CRYPTO'08, LNCS vol. 5157, pages 108-125, Springer, 2008.

[GHJRW08] Rationality and Traffic Attraction: Incentives for Honest Path Announcements in BGP, Sharon Goldberg, Shai Halevi, Aaron D. Jaggard, Vijay Ramachandran, and Rebecca N. Wright, Proceedings of the ACM SIGCOMM 2008 conference on Data communication, pages 267-278. ACM 2008.

[GHKR08] Threshold RSA for Dynamic and Ad-Hoc Groups, Rosario Gennaro, Shai Halevi, Tal Rabin, and Hugo Krawczyk. In Advances in Cryptography - EUROCRYPT'08, LNCS vol. 4965, pages 88-107, Springer, 2008.

[HR08] Degradation and Amplification of Computational Hardness, Shai Halevi and Tal Rabin. The 5th Theory of Cryptography Conference - TCC'08. LNCS vol. 4948, pages 623-640. Springer, 2008.

[HMR08] On Seed-Incompressible Functions , Shai Halevi, Steven Myers, and Charles Rackoff. The 5th Theory of Cryptography Conference - TCC'08. LNCS vol. 4948, pages 19-36. Springer, 2008.

[HK07] Security under Key-Dependent Inputs, Shai Halevi and Hugo Krawczyk. 14th ACM-CCS, pages 466-475, 2008. ACM.

[H07] Invertible Universal Hashing and the TET Encryption Mode, S. Halevi, Advances in Cryptology - CRYPTO '07. LNCS vol. 4622, pages 412-429. Springer, 2007.

[BCHK06] Chosen-ciphertext security from identity-based encryption, D. Boneh, R. Canetti, S. Halevi and J. Katz. SICOMP 36(5), Pages 915-942, 2006. (Earlier version in EUROCRYPT'04, pages 207-222.)

[CHS06] Mitigating Dictionary Attacks on Password-Protected Local Storage, R. Canetti, S. Halevi and M. Steiner. CRYPTO 2006.

[HK06] Strengthening Digital Signatures via Randomized Hashing, S. Halevi and H. Krawczyk, CRYPTO 2006.

[BBH06] Chosen Ciphertext Secure Public Key Threshold Encryption Without Random Oracles, Dan Boneh, Xavier Boyen, and Shai Halevi, RSA-CT 2006.

[BH05] An architecture for robust pseudo-random generation and applications to `/dev/random`, Boaz Barak and Shai Halevi. 12th ACM-CCS, Pages 203-212, 2005. ACM.

[CHK+05] Universally composable password-based key exchange, R. Canetti, S. Halevi, J. Katz, Y. Lindell and P. MacKenzie. Advances in Cryptology - EUROCRYPT '05. LNCS vol. 3494, pages 404-421. Springer-Verlag, 2005.

[CHS05] Hardness amplification of computational riddles, R. Canetti, S. Halevi and M. Steiner. The 2nd Theory of Cryptography Conference - TCC'05. LNCS vol. 3378, pages 17-33. Springer, 2005.

[CHK05] Adaptively secure non-interactive public-key encryption, R. Canetti, S. Halevi, and J. Katz. The 2nd Theory of Cryptography Conference - TCC'05. LNCS vol. 3378, pages 150-168. Springer, 2005.

[H04] EME*: extending EME to handle arbitrary-length messages with associated data, S. Halevi. INDOCRYPT 2004, LNCS vol. 3348, pages 315-327. Springer, 2004.

[CHK04] Chosen-ciphertext security from identity-based encryption, R. Canetti, S. Halevi and J. Katz. Advances in Cryptology - EUROCRYPT '04. LNCS vol. 3027, pages 207-222. Springer-Verlag, 2004.

[HR04] A parallelizable enciphering mode, Shai Halevi and Phil Rogaway. The RSA conference - Cryptographer's track, RSA-CT '04. LNCS vol. 2964, pages 292-304. Springer-Verlag, 2004.

[CGH04b] On the random-oracle methodology as applied to length-restricted signature schemes, Ran Canetti, Oded Goldreich and Shai Halevi. The 1st Theory of Cryptography Conference - TCC '04. LNCS vol. 2951, pages 40-57. Springer-Verlag, 2004.

[HR03] A tweakable enciphering mode, Shai Halevi and Phil Rogaway. Advances in Cryptology - CRYPTO '03. LNCS vol. 2729, pages 482-499. Springer-Verlag, 2003.

[CHK03] A forward-secure public-key encryption scheme, Ran Canetti, Shai Halevi and Jonathan Katz. Advances in Cryptology - EUROCRYPT'03, LNCS vol. 2656, pages 255-271. Springer-Verlag, 2003.

[SECOBS] A Two Layered Approach for Securing an object store network, Alain Azagury, Ran Canetti, Michael Factor, Shai Halevi, Ealan Henis, Dalit Naor, Noam Rinetzky, Ohad Rodeh, and Julian Satran. 1st International IEEE Security in Storage Workshop (SISW 2002)

[CHJ02] Cryptanalysis of stream ciphers with linear masking, Don Coppersmith, Shai Halevi and Charanjit Jutla. Advances in Cryptology - CRYPTO '02. LNCS vol. 2442, Pages 515-532. Springer-Verlag, 2002.

[HCJ02] Scream: a software-efficient stream cipher, Shai Halevi, Don Coppersmith and Charanjit Jutla. FSE '02, LNCS vol. 2365, Pages 195-209. Springer-Verlag, 2002.

[BHH01] The modular inversion hidden number problem, Dan Boneh, Shai Halevi, and Nick Howgrave-Graham. Advances in Cryptology - ASIACRYPT '01, LNCS vol. 2248, Pages 36-51. Springer-Verlag, 2001.

[DHR00] A cryptographic solution to a game theoretic problem, Yevgeniy Dodis, Shai Halevi, and Tal Rabin. Advances in Cryptology - CRYPTO 2000. LNCS vol. 1880, Pages 112-130, Springer-Verlag, 2000.

[CGH00] Computing inverses over a shared secret modulus, Dario Catalano, Rosario Gennaro, and Shai Halevi. Advances in Cryptology - EUROCRYPT 2000. LNCS vol. 1807, Pages 190-206, Springer-Verlag, 2000.

[CDHKS00] Exposure-resilient functions and all-or-nothing transforms, R. Canetti, Y. Dodis, S. Halevi, E. Kushilevitz, and A. Sahai. Advances in Cryptology - EUROCRYPT 2000. LNCS vol. 1807, Pages 453-469, Springer-Verlag, 2000.

[BHKKR99] UMAC:Fast and secure message authentication, J. Black, S. Halevi, H. Krawczyk, T.Krovetz and P. Rogaway. In Advances in Cryptology - CRYPTO '99, pages 216-233, Springer, LNCS vol. 1666, 1999.

[GHR99] Secure hash-and-sign signatures without the random oracle, R. Gennaro, S. Halevi and T. Rabin. In Advances in Cryptography - EUROCRYPT '99, pages 123-139, Springer, LNCS vol. 1592. 1999.

[BHSV98] Many-to-one Trapdoor Functions and their Relation to Public-key Cryptosystems, M. Bellare, S. Halevi, A. Sahai and S. Vadhan. In Advances in Cryptography - CRYPTO '98, pages 283-298, Springer, LNCS vol. 1462. 1998.

[GGH97a] Public-Key Cryptosystems from Lattice Reduction Problems, O. Goldreich, S. Goldwasser and S. Halevi. In Advances in Cryptography - CRYPTO '97, pages 112-131, 1997. Springer-Verlag, LNCS vol. 1294.

[GGH97b] Eliminating Decryption Errors in the Ajtai-Dwork Cryptosystem, O. Goldreich, S. Goldwasser and S. Halevi. In Advances in Cryptography - CRYPTO '97, pages 105-111, 1997. Springer-Verlag, LNCS vol.1294.

[HK97] MMH: Message Authentication in Software in the Gbit/second Rates, S. Halevi and H. Krawczyk. In proceedings of the 4th Workshop on Fast Software Encryption, pages 172-189. Springer, LNCS vol. 1267, 1997.

[HM96] Practical and Provably-Secure Commitment Schemes from Collision-Free Hashing, S. Halevi and S. Micali. In Advances in Cryptography - CRYPTO '96, LNCS vol. 1109, pages 201-215, Springer-Verlag. 1996.

[DH01] Incremental codes, Yevgeniy Dodis, and Shai Halevi. APPROX '01, LNCS 2129, pages 75-89. Springer-Verlag, 2001.

[HKKN01] Private approximation of NP-hard functions, Shai Halevi, Robert Krauthgamer, Eyal Kushilevitz, and Kobbi Nissim. Proceedings of the 33rd annual symposium on Theory of computing - STOC '01, pages 550-559. ACM, 2001.

[BHHN00] Clock Synchronization with Faults and Recoveries, Boaz Barak, Shai Halevi, Amir Herzberg, and Dalit Naor. Proceedings of the 19th annual ACM symposium on Principles of distributed computing - PODC 2000, pages 133-142. ACM, 2000.

[GHLP99] Computing from partial solutions, A. Gal, S. Halevi, E. Petrank and D. Lipton. In Proceedings of the 14th Annual IEEE Conference on Computational Complexity, 1999.

[BHS98] Potential Function Analysis of Greedy Hot-Potato Routing, A. Ben-Dor, S. Halevi and A. Schuster. Theory Comput. Systems, vol. 31, pages 41-61 1998, Springer-Verlag. (Preliminary version appeared in PODC '94, Pages 225-234. ACM.)

[BH93] 0-1 Permanent is #P-Complete, a Simpler Proof, A. Ben-Dor and S. Halevi. In proceedings of the 2'nd Israeli Symposium on Theory and Computing Systems, pages 108-117, 1993. IEEE.

Journals

[H17] Tutorial on Homomorphic Encryption, Shai Halevi. Published as part of the book "Tutorials on the Foundations of Cryptography, Dedicated to Oded Goldreich", edited by Yehuda Lindell. Springer, 2017.

[GGHW17] On the Implausibility of Differing-Inputs Obfuscation and Extractable Witness Encryption with Auxiliary Input, Sanjam Garg, Craig Gentry, Shai Halevi and Daniel Wichs. Algorithmica (2017), 1-21. Earlier version in CRYPTO 2014.

[GGHRSW16] Hiding secrets in software: a cryptographic approach to program obfuscation. Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai and Brent Waters. Commun. ACM 59(5): 113-120 (2016)

[GHPS13] Field Switching in BGV-Style Homomorphic Encryption, Craig Gentry, Shai Halevi, Chris Peikert, and Nigel Smart. Journal of Computer Security, 21(5), 2013, pp. 663-684. Earlier version in SCN 2012.

[HK12] Smooth Projective Hashing and Two-Message Oblivious Transfer, Shai Halevi and Yael Tauman Kalai. Journal of Cryptology, 25(1), pp. 158-193, Springer, 2012.

[HSH10] Using HB Family of Protocols for Privacy-Preserving Authentication of RFID Tags in a Population, Tzipora Halevi, Nitesh Saxena, and Shai Halevi. JCS special issue on RFID System Security.

[CCG+08] Cryptanalysis of ISO/IEC 9796-1, D. Coppersmith, J.S. Coron, F. Grieu, S. Halevi, C. Jutla, D. Naccache, and J.P. Stern. Journal of Cryptology, 21(1), Pages 27-51. Springer, 2008.

[CHK07] A forward-secure public-key encryption scheme, Ran Canetti, Shai Halevi and Jonathan Katz. Journal of Cryptology, 20(3), Pages 265-294. Springer, 2007. (Earlier version in EUROCRYPT'03, pages 255-271.)

[CGH04a] The random oracle methodology, rivisited, R. Canetti, O. Goldreich and S. Halevi. JACM, vol. 51, no. 4, pages 557-594. July 2004, ACM. (Preliminary version appeared in STOC '98, Pages 209-218.)

[CHH00] Maintaining authenticated communication in the presence of break-ins, R. Canetti, S. Halevi,and A. Herzberg. Journal of Cryptology, 13(1), Pages 61-105. Springer-Verlag, 2000. (Preliminary version appeared in PODC'97, Pages 15-24, ACM.)

[HK99] Public-key cryptography and password protocols, S. Halevi and H. Krawczyk. In ACM Transactions on Information and System Security (TISSEC), Vol 2, No. 3, Pages 230-268, August 1999. ACM. (Preliminary version appeared in the 5th ACM-CCS, Pages 122-131. 1998. ACM.)

[H99] Efficient Commitment Schemes with Bounded Sender and Unbounded Receiver, S. Halevi. In Journal of Cryptology, vol. 12, no. 2, pages 77-89. Springer, 1999. (Preliminary version appeared in Advances in CRYPTO '95, Pages 84-96, Springer-Verlag.)

Manuscripts

[BDH+18] Initial Public Offering (IPO) on Permissioned Blockchain using Secure Multiparty Computation, Fabrice Benhamouda, Angelo DeCaro, Shai Halevi, Tzipora Halevi, Charanjit jutla, Yacov Manevich, and Qi Zhang. 2018.

[HPS18] An Improved RNS Variant of the BFV Homomorphic Encryption Scheme, Shai Halevi and Yuriy Polyakov and Victor Shoup. 2018.

[H15] Graded Encoding, Variations on a Scheme, Shai Halev, 2015.

[HS13] Design and Implementation of a Homomorphic-Encryption Library, Shai Halevi and Victor Shoup, 2013.

[HHJ08] The Hash Function Fugue, Shai Halevi, William E. Hall, and Charanjit S. Jutla. 2008.

[H05b] A plausible approach to computer-aided cryptographic proofs, Shai Halevi. 2005.

[HKN05] Enforcing Confinement in Distributed Storage and a Cryptographic Model for Access Control, Shai Halevi, Paul A. Karger, and Dalit Naor. 2005.

[H05a] A sufficient condition for key-privacy, Shai Halevi. 2005.

[H01] An observation regarding Jutla's modes of operation, Shai Halevi, 2001.

[MARS] MARS - a candidate cipher for AES, C. Burwick, D. Coppersmith, E. D'Avignon, R. Gennaro, S. Halevi, C. Jutla, S.M. Matyas Jr., L. O'Connor, M. Peyravian, D. Safford and N. Zunic. Presented in the 1st AES conference, 1998, NIST.

[HM98] A Stronger Notion of Proofs of Knowledge. S. Halevi and S. Micali