Curriculum Vitae

Masayuki Abe

May 18, 2025

Background

Date of Birth: 21 June 1967

Place of Birth: Yokohama, Japan

Language: Japanease, English

Office Address: 3-9-11 Midori-cho, Musashino-shi, Tokyo, 180-8585, Japan

Contact: abe.masayuki@iecl.ntt.co.jp (business), abe.masayuki.7a@kyoto-u.ac.jp (academic)

Education

2002.12 Ph.D. from University of Tokyo. #15508, "Efficient Components for Cryptographic Applications in the Discrete-Log Setting" (Supervised by Prof. Hideki Imai.)

1992.4 M.E. in electrical engineering from Science University of Tokyo. (Supervised by Prof. Seiichiro Hangai.)

1990.4 B.E. in electrical enginieering from Science University of Tokyo. (Supervised by Prof. Seiichiro Hangai.)

Professional Experience

2022.4-present NTT Fellow.

2018.4-2022.3 Manager of Cryptography Research Laboratory in NTT Laboratories.

2013.4-2022.3 Senior Distinguished Researcher of NTT Laboratories.

2013.4-2016.6 Group Leader of Crypto Research Group in NTT Secure Platform Laboratories.

2006.1-2013.3 Senior Research Scientist since October 2005 and Distinguished Scientist of NTT Information Sharing Platform Laboratories. Research on digital signatures with special features.

2004.4-2006.1 Visiting IBM T. J. Watson Research Center. Collaboration with the Crypto Group leaded by Tal Rabin. Research on hybrid encryption, zero-knowledge proofs, universally composable protocols.

1997.9-2004.3 Research Engineer of NTT Information Sharing Platform Laboratories (Senior Research Engineer since 2001, and Distinguished Scientist since 2003). Design and analysis of cryptographic primitives and protocols including electronic voting, key escrow systems, blind signatures for digital cash system, message recovery and other signature schemes with additional functionality, publicly verifiable encryption schemes, efficient multi-party computation based on cryptographic assumptions, and zero-knowledge proofs in multi-party computation.

1996.9-1997.8 Guest Researcher of ETH Zurich. Studied cryptography, especially multi-party computation, supervised by Professor Ueli Maurer.

1992.4-1996.8 Engineer of NTT Network Information Systems Laboratories. Development of fast arithmetic algorithms for cryptographic operations and their software and hardware implementation.

Professional Services

Program Committee Member for International Conferences: Asiacrypt'01, PKC'02, Asiacrypt'03, ACISP'03, ISC'03, PKC'04, FC'04, ACNS'04, CT-RSA'05, Crypto'05, PKC'06, WWW'06, VietCrypt'06, Asiacrypt'07, PKC'08, CT-RSA'08, ACNS'08, ACISP'08, Asiacrypt'08, ASIACCS'09, Asiacrypt'09, Crypto'09, ACISP'10, PKC'11, Crypto'11, Asiacrypt'11, TCC'12, SCN'12, TCC'13, CT-RSA'13, Crypto'13, PKC'14, ESORICS'14, SCN'14, Eurocrypt'14, Asiacrypt'14, Eurocrypt'15, Crypto'15, TCC'16A, FC'16, TCC'16B, Crypto'17, PKC'17, TCC'18, ACISP'18, ACNS'18, CANS'19, CT-RSA'20, RWC'20, ISC'20, CT-RSA'21, Inscript'21, ISC'21, CANS'21, TCC'21, ACNS'22, CT-RSA'22, Eurocrypt'22, ACISP'22, SCN'22, CT-RSA'23, Eurocrypt'23, RWC'23, ACMCCS'23, Asiacrypt'23, CT-RSA'24, RWC'24, CRYPTO'24, Eurocrypt'24, SCN'24, Eurocrypt'25

Program Chair for Interantional Conferences: CT-RSA'07, ASIACCS'08, Asiacrypt'10

Steering Committee Member :

- Asiacrypt Steering Committee (2012-present)
- PKC Steering Committee (2018-present)

General (Co-)Chair for Interantional Conferences and Workshops: TCC'13, QCW'22

(Co-)Organiser of Local Workshops: Workshop on Cryptography (2018.1.16, NTT-JFLI-University of Tokyo), NTT SC-Lab and NTT Research Joint Workshop (2019.12.13, Kyoto, Japan)

Editorial Board :

- Journal of Cryptology (2018-present).
- International Journal of Applied Cryptography (IJACT). (2008-2022).

Director of International Association of Cryptologic Research (IACR): 2015-2023.

IACR School Committee: 2014-2017.

IACR Election Committee: 2022-2022.

IACR Emergencry Committee: 2020-2023.

IACR Dissertation Award Committee: 2020-2023.

Academic Committee :

- Member of SCIENCE COUNCIL OF JAPAN
- Member of Advisory Board of Cryptographic Technology of Cryptography Research and Evaluation Committees(CRYPTREC)

Editor in Chief: IEICE Transactions on Fundamentals, Special Section on Cryptography and Information Security, 2017.7-2019.1.

Awards

2022.06.27 IACR Fellow. "For influential contributions to practical cryptosystems, and for exemplary service to IACR and the Asia-Pacific cryptography community."

2021.04.06: The Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology. Awards for Science and Technology, Research Category for "Leading Research on Digital Signatures for Protecting Privacy."

2020.6.15: 3rd Tokyo Academy of Physics Award from Tokyo University of Science

2019.4.10: 64th Maejima Hisoka Award for "Pioneering Research on Secure and Practical Digital Signatures and Cryptographic Protocols"

2018.4.24: SCIS Innovation Paper Award for "Pseudo-Code Performance Estimation for Pairing-Based Cryptographic Schemes"

2016.6: 53rd IEICE Achievement Award, "Pioneering Research on Cryptographic Protocols and Component Technology"

2016.4: The Ichimura Prize in Science for Excellent Achievement (48th), "Pioneering Research on Structure-Preserving Crytography for Modular Design of Cryptographic Protocols"

1999.1: SCIS Best Paper Award for "Robust Threshold Cramer-Shoup Cryptosystem" in 1999 Symposium on Cryptography and Information Security (SCIS '99), T1-1.3, 1999

Academic Experiences

2018.4-present: Guest Professor in Graduate School of Informatics, Kyoto University

2013.4-2018.3: Guest Associate Professor in Graduate School of Informatics, Kyoto University

2017.10: Lecturer of Graduate School of Science & Engineering, Tokyo Metropolitan University

2012.9-2013.1: Lecturer of Department of Information and Communication Engineering in University of Electro-Communications

2009.5-2009.7: Lecturer of Department of Complexity Science and Engineering, Graduate School of Frontier Sciences, The University of Tokyo

2003.5: Lecturer of Department of Information and Communication Engineering in University of Electro-Communications

2002.9-2003.3: Lecturer of Department of Information and Communication Technology in School of High Technology for Human Welfare in Tokai University.

1999.5: Lecturer of Department of Electronics and Computer Systems in Takushoku University.

Ph.D. Referee: For Kun Peng in Queensland University of Technology, April 2004. For Kristiyan Halarambiev in New York University, March 2011. For Shota Yamada in University of Tokyo, January 2014. For Junichi Tomida in Kyoto University, March, 2021. For Yuan Quan in Kyoto University, March, 2022.

Invited Talks in Conferences and Workshops

2025.03.28: "Zero-Knowledge Proofs and Applications: Introduction", The Institute of Electronics, Information and Communication EngineersGeneral Conference, Tokyo, Japan

2021.11.7: "Composition fo Zero-Knowledge Proofs", International Conference on Provable and Practical Security (ProvSec 2021), Guangzhou, China

2019.12.13: "On Black-Box Extensions of Non-Interactive Zero-Knowledge Arguments", NTT SC-Lab and NTT Research Joint Workshop, Kyoto, Japan.

2019.10.25: "Proving Disjunctive Relations Non-Interactively", CANS 2019, Fujou University, Fuzhou, China.

2019.3.1: "Improved (Almost) Tightly-Secure Simulation-Sound QA-NIZK with Applications", Public-key Workshop, AIST, Japan.

2018.1.16: "On the Practical Impact of Tight Security", Workshop on Cryptography, NTT-JFLI-U.Tokyo.

2015.11.3: "Structure-Preserving Cryptography", Asiacrypt 2015, Auckland.

2015.9.4: "Fully Structure-Preserving Signatures and Shrinking Commitments", ISEC Workshop, Tokyo, Japan.

2015.2.20: "Structure-Preserving Signatures from Type II Pairings", 8th Public-Key Workshop, Tokyo, Japan.

2014.3.20: "On the Impossibility of Structure-Preserving Deterministic Primitives", 7th Public-Key Workshop, Tokyo, Japan.

2013.6.27: "Tagged One-Time Signatures: Tight Security and Optimal Tag Size", 4th Jinbo-cho Cryptography Workshop, Study on PKC2013, Tokyo, Japan.

2012.9.26: "Cryptographic Tools over Bilinear Groups for Modular Design of Cryptographic Tasks", The Sixth International Conference on Provable Security (ProvSec 2012), Chengdu, China.

2012.5.18: "Separating Short Structure-Preserving Signatures from Non-Interactive Assumptions", ISEC Workshop, Tokyo, Japan.

2012.2.23: "Structure-Preserving Cryptography Part-II: Structure Preserving Commitments", 5th Workshop on Secure Construction of Public-Key Cryptosystems and its Applications, Akihabara, Japan.

2011.12.14: "Optimal Structure-Preserving Signatures in Asymmetric Bilinear Groups", ISEC Workshop, ISEC2011-71, Tokyo, Japan.

2011.5.31: " Signature Scheme with Efficient Proof of Validity", International Workshop on Coding and Cryptology, Qingdao, China.

2008.12.3: "Provable Security in Public-key Encryption Schemes", Tutorial Session in International Conference on Information Security and Cryptography 2008 (ICISC'08), Seoul, Korea.

2007.12.13: "Compact CCA-secure Encryption for Arbitrary Messages", IPA Cryptography Workshop 2007 Autumn, IPA, Tokyo, Japan.

2007.12.11: "Compact CCA-secure Encryption", Global COE Workshop, Tokyo Institute of Technology, Tokyo, Japan.

2006.2.28: "Tag-KEM/DEM: A New Framework for Hybrid Encryption", Workshop on Secure Construction of Public-Key Cryptosystems and its Applications, AIST, Tokyo, Japan.

2003.3.8: "Multi-Party Protocols and Zero-Knowledge Proofs", In 3rd JST Workshop, Tokyo, Japan.

2001.9.18: "Trend of Electronic Commerce" (in Japanese), In IEICE Kansai-branch, Osaka, Japan.

2001.1.15: "Cryptographic Solution for Electronic Voting" and "Development of Electronic Voting Systems in NTT", In the Seminar Series at the Information and Communications University, Korea.

Talks at Seminars

New York University (USA, 2005), UC Irvine (USA, 2010), École Normale Supérieure (France, 2008), Nanyang Technological University (Singapore, 2011), IBM Zurich (Switzerland, 2012), ETH Zurich (Switzerland, 2012), Karlsruhe University (Germany, 2012), Academic Center for Computing and Media Studies, Kyoto Unviersity (Japan, 2014), JAIST (Japan, 2017), Kyoto University (Japan, 2018), UESTC Chengdu (China, 2019), Nagoya University (Japan, 2019), Science University of Tokyo (Japan, 2019), Bocconi University (Italy, 2024), Sapienza – Università di Roma (Italy, 2024)

Publication

Journal Papers

[1] M. Abe, D. Hofheinz, R. Nishimaki, M. Ohkubo, and J. Pan, "Compact structure-preserving signatures with almost tight security," *J. Cryptol.*, vol. 36, no. 4, p. 37, 2023.

[2] Q. Yuan, M. Tibouchi, and M. Abe, "On subset-resilient hash function families," *Designs, Codes, and Cryptography*, vol. 90, no. 3, pp. 719–758, 2022.

[3] M. Abe and M. Ambrona, "Blind key-generation attribute-based encryption for general predicates," *Designs, Codes, and Cryptography*, vol. 90, no. 10, pp. 2271–2299, 2022.

[4] Q. Yuan, M. Tibouchi, and M. Abe, "Security notions for stateful signature schemes," *IET Information Security*, vol. 1, no. 16, pp. 1–17, 2022.

[5] C. Sun, T. Espitau, M. Tibouchi, and M. Abe, "Guessing bits: Improved lattice attacks on (EC)DSA with nonce leakage," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2022, no. 1, pp. 391–413, 2022.

[6] K. Yamashita, M. Tibouchi, and M. Abe, "On the impossibility of NIZKs for disjunctive languages from commit-and-prove NIZKs," *IEEE Access*, vol. 9, pp. 51368–51379, 2021.

[7] K. Yamashita, M. Tibouchi, and M. Abe, "A coin-free oracle-based augmented black box framework," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Special Section on Discrete Mathematics and Its Applications*, 2020. Accepted on March 24, 2020.

[8] R. C. Phan, M. Abe, L. Batten, J. H. Cheon, E. Dawson, S. D. Galbraith, J. Guo, L. C. K. Hui, K. Kim, X. Lai, D. H. Lee, M. Matsui, T. Matsumoto, S. Moriai, P. Q. Nguyen, D. Pei, D. H. Phan, J. Pieprzyk, H. Wang, H. Wolfe, D. S. Wong, T. Wu, B. Yang, S. Yiu, Y. Yu, and J. Zhou, "Advances in security research in the Asiacrypt region," *Communications of the Association for Computing Machinery*, vol. 63, no. 4, pp. 76–81, 2020.

[9] J. Tomida, M. Abe, and T. Okamoto, "Efficient inner product functional encryption with full-hiding security," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 103-A, no. 1, pp. 33–40, 2020.

[10] M. Abe, J. Camenisch, R. Dowsley, and M. Dubovitskaya, "On the impossibility of structure-preserving deterministic primitives," *Journal of Cryptology*, vol. 32, pp. 239–264, Jan. 2019.

[11] M. Abe, J. Groth, M. Kohlweiss, M. Ohkubo, and M. Tibouchi, "Efficient fully structure-preserving signatures and shrinking commitments," *Journal of Cryptology*, vol. 32, pp. 973–1025, July 2019.

[12] M. Abe, F. Hoshino, and M. Ohkubo, "Fast and scalable bilinear-type conversion method for large scale crypto schemes," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 102-A, no. 1, pp. 251–269, 2019.

[13] M. Abe, F. Hoshino, and M. Ohkubo, "Opcount: A pseudo-code performance estimation system for pairing-based cryptography," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 102-A, no. 9, pp. 1285–1292, 2019.

[14] A. Takahashi, M. Tibouchi, and M. Abe, "New Bleichenbacher records: Fault attacks on qDSA signatures," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2018, no. 3, pp. 331–371, 2018. `https://tches.iacr.org/index.php/TCHES/article/view/7278`.

[15] M. Abe, "Variations of Even-Goldreich-Micali framework for signature schemes," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 100-A, no. 1, pp. 12–17, 2017.

[16] M. Abe, M. Chase, B. David, M. Kohlweiss, R. Nishimaki, and M. Ohkubo, "Constant-size structure-preserving signatures: Generic constructions and simple assumptions," *Journal of Cryptology*, vol. 29, pp. 833–878, Oct. 2016.

[17] M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, and M. Ohkubo, "Structure-preserving signatures and commitments to group elements," *Journal of Cryptology*, vol. 29, pp. 363–421, Apr. 2016.

[18] R. Hiromasa, M. Abe, and T. Okamoto, "Packing messages and optimizing bootstrapping in GSW-FHE," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 99-A, no. 1, pp. 73–82, 2016.

[19] M. Abe, S. S. M. Chow, K. Haralambiev, and M. Ohkubo, "Double-trapdoor anonymous tags for traceable signatures," *International Journal of Information Security*, vol. 12, no. 1, pp. 19–31, 2013.

[20] M. Abe, T. Okamoto, and K. Suzuki, "Message recovery signature schemes from sigma-protocols," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 96-A, no. 1, pp. 92–100, 2013.

[21] M. Abe and M. Ohkubo, "A framework for universally composable non-committing blind signatures," *International Journal of Applied Cryptography*, vol. 2, no. 3, pp. 229–249, 2012.

[22] M. Abe, Y. Cui, H. Imai, and E. Kiltz, "Efficient hybrid encryption from ID-based encryption," *Designs, Codes, and Cryptography*, vol. 54, no. 3, pp. 205–240, 2010.

[23] M. Abe, E. Kiltz, and T. Okamoto, "Chosen ciphertext security with optimal ciphertext overhead," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 93-A, no. 1, pp. 22–33, 2010.

[24] M. Abe, Y. Cui, H. Imai, and K. Kurosawa, "Tag-KEM from set partial domain one-way permutations," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 92-A, no. 1, pp. 42–52, 2009.

[25] M. Abe, R. Gennaro, and K. Kurosawa, "Tag-KEM/DEM: A new framework for hybrid encryption," *Journal of Cryptology*, vol. 21, pp. 97–130, Jan. 2008.

[26] M. Ohkubo and M. Abe, "On the definitions of anonymity for ring signatures," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 91-A, no. 1, pp. 272–282, 2008.

[27] M. Abe and H. Imai, "Flaws in robust optimistic Mix-nets and stronger security notions," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 89-A, no. 1, pp. 99–105, 2006.

[28] K. Chida and M. Abe, "Flexible-routing anonymous networks using optimal length of ciphertext," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 88-A, no. 1, pp. 211–221, 2005.

[29] M. Abe, M. Ohkubo, and K. Suzuki, "1-out-of-n signatures from a variety of keys," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 87-A, no. 1, pp. 131–140, 2004. Conference version publised at Asiacrypt 2002.

[30] M. Abe, M. Ohkubo, and K. Suzuki, "Efficient threshold signer-ambiguous signatures from variety of keys," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E87-A, pp. 471–479, Feb. 2004.

[31] M. Abe, "Combining encryption and proof of knowledge in the random oracle model," *The Computer Journal*, vol. 47, no. 1, pp. 58–70, 2004.

[32] M. Abe and K. Suzuki, "M+1-st price auction using homomorphic encryption," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Special Section on Cryptography and Information Security*, vol. E86-A, pp. 136–141, Jan. 2003.

[33] F. Hoshino, M. Abe, and T. Kobayashi, "Lenient/strict batch verification in several groups," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E86-A, pp. 64–72, Jan. 2003.

[34] M. Abe and M. Kanda, "A key escrow scheme with time-limited monitoring for one-way communication," *The Computer Journal*, vol. 45, no. 6, pp. 661–671, 2002.

[35] M. Abe and T. Okamoto, "Delegation chains secure up to constant length," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Special Section on Cryptography and Information Security*, vol. E85-A, pp. 110–116, Jan. 2002.

[36] M. Abe and T. Okamoto, "A signature scheme with message recovery as secre as discrete logarithm," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E84-A, pp. 197–204, Feb. 2001.

[37] M. Ohkubo and M. Abe, "A length-invariant hybrid Mix," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Special Section on Fundamentals of Information and Communications*, vol. E84-A, pp. 931–940, Apr. 2001.

[38] M. Abe, "Universally verifiable Mix-net with verification work independent of the number of Mix-servers," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Special Section on Cryptography and Information Security*, vol. E83-A, pp. 1431–1440, July 2000.

[39] M. Abe, "Non-interactive and optimally resilient distributed multiplication," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Special Section on Discrete Mathematics and Its Applications*, vol. E83-A, pp. 598–605, Apr. 2000.

Conferences and Workshops with Review

[1] Masayuki Abe, Masaya Nanri, Octavio Perez-Kempner, and Mehdi Tibouchi. Interactive threshold mercurial signatures and applications. In Kai-Min Chung and Yu Sasaki, editors, *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part III*, volume 15486 of *Lecture Notes in Computer Science*, pages 69–103. Springer, 2024.

[2] Masayuki Abe, Andrej Bogdanov, Miyako Ohkubo, Alon Rosen, Zehua Shang, and Mehdi Tibouchi. CDS composition of multi-round protocols. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part IX*, volume 14928 of *Lecture Notes in Computer Science*, pages 391–423. Springer, 2024.

[3] Xiuhan Lin, Moeto Suzuki, Shiduo Zhang, Thomas Espitau, Yang Yu, Mehdi Tibouchi, and Masayuki Abe. Cryptanalysis of the peregrine lattice-based signature scheme. In Qiang Tang and Vanessa Teague, editors, *Public-Key Cryptography - PKC 2024 - 27th IACR International Conference on Practice and Theory of Public-Key Cryptography, Sydney, NSW, Australia, April 15-17, 2024, Proceedings, Part I*, volume 14601 of *Lecture Notes in Computer Science*, pages 387–412. Springer, 2024.

[4] Masayuki Abe, Miguel Ambrona, and Miyako Ohkubo. Hybrid zero-knowledge from garbled circuits and circuit-based composition of Σ-protocols. In Clemente Galdi and Duong Hieu Phan, editors, *Security and Cryptography for Networks - 14th International Conference, SCN 2024, Amalfi, Italy, September 11-13, 2024, Proceedings, Part I*, volume 14973 of *Lecture Notes in Computer Science*, pages 73–95. Springer, 2024.

[5] Quan Yuan, Mehdi Tibouchi, and Masayuki Abe. Quantum-access security of hash-based signature schemes. In Leonie Simpson and Mir Ali Rezazadeh Baee, editors, *Information Security and Privacy - 28th Australasian Conference, ACISP 2023, Brisbane, QLD, Australia, July 5-7, 2023, Proceedings*, volume 13915 of *Lecture Notes in Computer Science*, pages 343–380. Springer, 2023.

[6] Masayuki Abe, Miguel Ambrona, Andrej Bogdanov, Miyako Ohkubo, and Alon Rosen. Acyclicity programming for sigma-protocols. In Kobbi Nissim and Brent Waters, editors, *Theory of Cryptography - 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8-11, 2021, Proceedings, Part I*, volume 13042 of *Lecture Notes in Computer Science*, pages 435–465. Springer, 2021.

[7] Masayuki Abe, Miguel Ambrona, Andrej Bogdanov, Miyako Ohkubo, and Alon Rosen. Non-interactive composition of sigma-protocols via share-then-hash. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference*

on the Theory and Application of Cryptology and Information Security, December 7-11, 2020, Proceedings, volume 12493 of *Lecture Notes in Computer Science*, pages 749–773. Springer International Publishing, December 2020.

[8] Ky Nguyen, Miguel Ambrona, and Masayuki Abe. WI is almost enough: Contingent payment all over again. In Jay Ligatti, Xinming Ou, Jonathan Katz, and Giovanni Vigna, editors, *CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, USA, November 9-13, 2020*, pages 641–656. ACM, 2020.

[9] Chao Sun, Mehdi Tibouchi, and Masayuki Abe. Revisiting the hardness of binary error LWE. In Joseph K. Liu and Hui Cui, editors, *Information Security and Privacy - 25th Australasian Conference, ACISP 2020, Perth, WA, Australia, November 30 - December 2, 2020, Proceedings*, volume 12248 of *Lecture Notes in Computer Science*, pages 425–444. Springer, 2020.

[10] Kyosuke Yamashita, Mehdi Tibouchi, and Masayuki Abe. On black-box extension of a non-interactive zero-knowledge proof system for secret equality. In Karthikeyan Bhargavan, Elisabeth Oswald, and Manoj Prabhakaran, editors, *Progress in Cryptology - INDOCRYPT 2020 - 21st International Conference on Cryptology in India, Bangalore, India, December 13-16, 2020, Proceedings*, volume 12578 of *Lecture Notes in Computer Science*, pages 882–904. Springer, 2020.

[11] Masayuki Abe, Miguel Ambrona, and Miyako Ohkubo. On black-box extensions of non-interactive zero-knowledge arguments, and signatures directly from simulation soundness. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *PKC 2020: 23rd International Conference on Theory and Practice of Public Key Cryptography, Part I*, volume 121l10 of *Lecture Notes in Computer Science*, pages 558–589, Edinburgh, UK, May 2020. Springer, Heidelberg, Germany.

[12] Masayuki Abe, Charanjit S. Jutla, Miyako Ohkubo, Jiaxin Pan, Arnab Roy, and Yuyu Wang. Shorter QA-NIZK and SPS with tighter security. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019, Part III*, volume 11923 of *Lecture Notes in Computer Science*, pages 669–699, Kobe, Japan, December 8–12, 2019. Springer, Heidelberg, Germany.

[13] Kyosuke Yamashita, Mehdi Tibouchi, and Masayuki Abe. A coin-free oracle-based augmented black box framework. In Ron Steinfeld and Tsz Hon Yuen, editors, *ProvSec 2019: 13th International Conference on Provable Security*, volume 11821 of *Lecture Notes in Computer Science*, pages 265–272, Cairns, QLD, Australia, October 1–4, 2019. Springer, Heidelberg, Germany.

[14] Masayuki Abe, Charanjit S. Jutla, Miyako Ohkubo, and Arnab Roy. Improved (almost) tightly-secure simulation-sound QA-NIZK with applications. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018, Part I*, volume 11272 of *Lecture Notes in Computer Science*, pages 627–656, Brisbane, Queensland, Australia, December 2–6, 2018. Springer, Heidelberg, Germany.

[15] Masayuki Abe, Miguel Ambrona, Miyako Ohkubo, and Mehdi Tibouchi. Lower bounds on structure-preserving signatures for bilateral messages. In Dario Catalano and Roberto De

Prisco, editors, *SCN 18: 11th International Conference on Security in Communication Networks*, volume 11035 of *Lecture Notes in Computer Science*, pages 3–22, Amalfi, Italy, September 5–7, 2018. Springer, Heidelberg, Germany.

[16] Masayuki Abe, Dennis Hofheinz, Ryo Nishimaki, Miyako Ohkubo, and Jiaxin Pan. Compact structure-preserving signatures with almost tight security. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017, Part II*, volume 10402 of *Lecture Notes in Computer Science*, pages 548–580, Santa Barbara, CA, USA, August 20–24, 2017. Springer, Heidelberg, Germany.

[17] Masayuki Abe, Fumitaka Hoshino, and Miyako Ohkubo. Design in type-I, run in type-III: Fast and scalable bilinear-type conversion using integer programming. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016, Part III*, volume 9816 of *Lecture Notes in Computer Science*, pages 387–415, Santa Barbara, CA, USA, August 14–18, 2016. Springer, Heidelberg, Germany.

[18] Junichi Tomida, Masayuki Abe, and Tatsuaki Okamoto. Efficient functional encryption for inner-product values with full-hiding security. In Matt Bishop and Anderson C. A. Nascimento, editors, *ISC 2016: 19th International Conference on Information Security*, volume 9866 of *Lecture Notes in Computer Science*, pages 408–425, Honolulu, HI, USA, September 3–6, 2016. Springer, Heidelberg, Germany.

[19] Masayuki Abe, Markulf Kohlweiss, Miyako Ohkubo, and Mehdi Tibouchi. Fully structure-preserving signatures and shrinking commitments. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015, Part II*, volume 9057 of *Lecture Notes in Computer Science*, pages 35–65, Sofia, Bulgaria, April 26–30, 2015. Springer, Heidelberg, Germany.

[20] Ryo Hiromasa, Masayuki Abe, and Tatsuaki Okamoto. Packing messages and optimizing bootstrapping in GSW-FHE. In Jonathan Katz, editor, *PKC 2015: 18th International Conference on Theory and Practice of Public Key Cryptography*, volume 9020 of *Lecture Notes in Computer Science*, pages 699–715, Gaithersburg, MD, USA, March 30 – April 1, 2015. Springer, Heidelberg, Germany.

[21] Masayuki Abe, Jens Groth, Miyako Ohkubo, and Takeya Tango. Converting cryptographic schemes from symmetric to asymmetric bilinear groups. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology – CRYPTO 2014, Part I*, volume 8616 of *Lecture Notes in Computer Science*, pages 241–260, Santa Barbara, CA, USA, August 17–21, 2014. Springer, Heidelberg, Germany.

[22] Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi. Structure-preserving signatures from type II pairings. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology – CRYPTO 2014, Part I*, volume 8616 of *Lecture Notes in Computer Science*, pages 390–407, Santa Barbara, CA, USA, August 17–21, 2014. Springer, Heidelberg, Germany.

[23] Masayuki Abe, Jan Camenisch, Rafael Dowsley, and Maria Dubovitskaya. On the impossibility of structure-preserving deterministic primitives. In Yehuda Lindell, editor, *TCC 2014: 11th Theory of Cryptography Conference*, volume 8349 of *Lecture Notes in Computer Science*, pages 713–738, San Diego, CA, USA, February 24–26, 2014. Springer, Heidelberg, Germany.

[24] Masayuki Abe, Jens Groth, Miyako Ohkubo, and Mehdi Tibouchi. Unified, minimal and selectively randomizable structure-preserving signatures. In Yehuda Lindell, editor, *TCC 2014: 11th Theory of Cryptography Conference*, volume 8349 of *Lecture Notes in Computer Science*, pages 688–712, San Diego, CA, USA, February 24–26, 2014. Springer, Heidelberg, Germany.

[25] Masayuki Abe, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo. Tagged one-time signatures: Tight security and optimal tag size. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *PKC 2013: 16th International Conference on Theory and Practice of Public Key Cryptography*, volume 7778 of *Lecture Notes in Computer Science*, pages 312–331, Nara, Japan, February 26 – March 1, 2013. Springer, Heidelberg, Germany.

[26] Masayuki Abe, Melissa Chase, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo. Constant-size structure-preserving signatures: Generic constructions and simple assumptions. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology – ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 4–24, Beijing, China, December 2–6, 2012. Springer, Heidelberg, Germany.

[27] Masayuki Abe, Kristiyan Haralambiev, and Miyako Ohkubo. Group to group commitments do not shrink. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 301–317, Cambridge, UK, April 15–19, 2012. Springer, Heidelberg, Germany.

[28] Masayuki Abe. Tools over bilinear groups for modular design of cryptographic tasks (invited talk). In Tsuyoshi Takagi, Guilin Wang, Zhiguang Qin, Shaoquan Jiang, and Yong Yu, editors, *ProvSec 2012: 6th International Conference on Provable Security*, volume 7496 of *Lecture Notes in Computer Science*, page 1, Chengdu, China, September 26–28, 2012. Springer, Heidelberg, Germany.

[29] Masayuki Abe, Jens Groth, Miyako Ohkubo, Masayuki Abe, Jens Groth, and Miyako Ohkubo. Separating short structure-preserving signatures from non-interactive assumptions. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 628–646. Springer, 2011.

[30] Masayuki Abe, Sherman S. M. Chow, Kristiyan Haralambiev, and Miyako Ohkubo. Double-trapdoor anonymous tags for traceable signatures. In Javier Lopez and Gene Tsudik, editors, *ACNS 11: 9th International Conference on Applied Cryptography and Network Security*, volume 6715 of *Lecture Notes in Computer Science*, pages 183–200, Nerja, Spain, June 7–10, 2011. Springer, Heidelberg, Germany.

[31] Masayuki Abe, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Optimal structure-preserving signatures in asymmetric bilinear groups. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 649–666, Santa Barbara, CA, USA, August 14–18, 2011. Springer, Heidelberg, Germany.

[32] Masayuki Abe, Kristiyan Haralambiev, and Miyako Ohkubo. Efficient message space extension for automorphic signatures. In Mike Burmester, Gene Tsudik, Spyros S. Magliveras, and Ivana Ilic, editors, *ISC 2010: 13th International Conference on Information Security*, volume 6531

of *Lecture Notes in Computer Science*, pages 319–330, Boca Raton, FL, USA, October 25–28, 2011. Springer, Heidelberg, Germany.

[33] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. Structure-preserving signatures and commitments to group elements. In Tal Rabin, editor, *Advances in Cryptology – CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 209–236, Santa Barbara, CA, USA, August 15–19, 2010. Springer, Heidelberg, Germany.

[34] Masayuki Abe and Miyako Ohkubo. A framework for universally composable non-committing blind signatures. In Mitsuru Matsui, editor, *Advances in Cryptology – ASIACRYPT 2009*, volume 5912 of *Lecture Notes in Computer Science*, pages 435–450, Tokyo, Japan, December 6–10, 2009. Springer, Heidelberg, Germany.

[35] Masayuki Abe, Eike Kiltz, and Tatsuaki Okamoto. Compact CCA-secure encryption for messages of arbitrary length. In Stanislaw Jarecki and Gene Tsudik, editors, *PKC 2009: 12th International Conference on Theory and Practice of Public Key Cryptography*, volume 5443 of *Lecture Notes in Computer Science*, pages 377–392, Irvine, CA, USA, March 18–20, 2009. Springer, Heidelberg, Germany.

[36] Masayuki Abe, Eike Kiltz, and Tatsuaki Okamoto. Chosen ciphertext security with optimal ciphertext overhead. In Josef Pieprzyk, editor, *Advances in Cryptology – ASIACRYPT 2008*, volume 5350 of *Lecture Notes in Computer Science*, pages 355–371, Melbourne, Australia, December 7–11, 2008. Springer, Heidelberg, Germany.

[37] Masayuki Abe and Serge Fehr. Perfect NIZK with adaptive soundness. In Salil P. Vadhan, editor, *TCC 2007: 4th Theory of Cryptography Conference*, volume 4392 of *Lecture Notes in Computer Science*, pages 118–136, Amsterdam, The Netherlands, February 21–24, 2007. Springer, Heidelberg, Germany.

[38] Masayuki Abe, Yang Cui, Hideki Imai, and Kaoru Kurosawa. Tag-KEM from set partial domain one-way permutations. In Lynn Margaret Batten and Reihaneh Safavi-Naini, editors, *ACISP 06: 11th Australasian Conference on Information Security and Privacy*, volume 4058 of *Lecture Notes in Computer Science*, pages 360–370, Melbourne, Australia, July 3–5, 2006. Springer, Heidelberg, Germany.

[39] Miyako Ohkubo and Masayuki Abe. On the definition of anonymity for ring signatures. In Phong Q. Nguyen, editor, *Progress in Cryptology - VIETCRYPT 06: 1st International Conference on Cryptology in Vietnam*, volume 4341 of *Lecture Notes in Computer Science*, pages 157–174, Hanoi, Vietnam, September 25–28, 2006. Springer, Heidelberg, Germany.

[40] Masayuki Abe, Rosario Gennaro, Kaoru Kurosawa, and Victor Shoup. Tag-KEM/DEM: A new framework for hybrid encryption and a new analysis of Kurosawa-Desmedt KEM. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 128–146, Aarhus, Denmark, May 22–26, 2005. Springer, Heidelberg, Germany.

[41] Masayuki Abe and Serge Fehr. Adaptively secure feldman VSS and applications to universally-composable threshold cryptography. In Matthew Franklin, editor, *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 317–334, Santa Barbara, CA, USA, August 15–19, 2004. Springer, Heidelberg, Germany.

[42] Masayuki Abe and Hideki Imai. Flaws in some robust optimistic Mix-nets. In Reihaneh Safavi-Naini and Jennifer Seberry, editors, *ACISP 03: 8th Australasian Conference on Information Security and Privacy*, volume 2727 of *Lecture Notes in Computer Science*, pages 39–50, Wollongong, NSW, Australia, July 9–11, 2003. Springer, Heidelberg, Germany.

[43] Masayuki Abe, Ronald Cramer, and Serge Fehr. Non-interactive distributed-verifier proofs and proving relations among commitments. In Yuliang Zheng, editor, *Advances in Cryptology – ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 206–223, Queenstown, New Zealand, December 1–5, 2002. Springer, Heidelberg, Germany.

[44] Masayuki Abe, Miyako Ohkubo, and Koutarou Suzuki. 1-out-of-n signatures from a variety of keys. In Yuliang Zheng, editor, *Advances in Cryptology – ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 415–432, Queenstown, New Zealand, December 1–5, 2002. Springer, Heidelberg, Germany. Full version available: Abe, M.; Ohkubo, M.; and Suzuki, K.1-out-of-n Signatures from a Variety of Keys IEICE Trans. Fund. Electron. Commun. Comput. Sci., 87-A, 131-140, 2004.

[45] Masayuki Abe and Koutarou Suzuki. Receipt-free sealed-bid auction. In Agnes Hui Chan and Virgil D. Gligor, editors, *ISC 2002: 5th International Conference on Information Security*, volume 2433 of *Lecture Notes in Computer Science*, pages 191–199, Sao Paulo, Brazil, September 30 – October 2, 2002. Springer, Heidelberg, Germany.

[46] Masayuki Abe and Koutarou Suzuki. M+1-st price auction using homomorphic encryption. In David Naccache and Pascal Paillier, editors, *PKC 2002: 5th International Workshop on Theory and Practice in Public Key Cryptography*, volume 2274 of *Lecture Notes in Computer Science*, pages 115–124, Paris, France, February 12–14, 2002. Springer, Heidelberg, Germany.

[47] Masayuki Abe. Securing "encryption + proof of knowledge" in the random oracle model. In Bart Preneel, editor, *Topics in Cryptology – CT-RSA 2002*, volume 2271 of *Lecture Notes in Computer Science*, pages 277–289, San Jose, CA, USA, February 18–22, 2002. Springer, Heidelberg, Germany.

[48] Masayuki Abe and Miyako Ohkubo. Provably secure fair blind signatures with tight revocation. In Colin Boyd, editor, *Advances in Cryptology – ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 583–602, Gold Coast, Australia, December 9–13, 2001. Springer, Heidelberg, Germany.

[49] Masayuki Abe. A secure three-move blind signature scheme for polynomially many signatures. In Birgit Pfitzmann, editor, *Advances in Cryptology – EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 136–151, Innsbruck, Austria, May 6–10, 2001. Springer, Heidelberg, Germany.

[50] Fumitaka Hoshino, Masayuki Abe, and Tetsutaro Kobayashi. Lenient/strict batch verification in several groups. In George I. Davida and Yair Frankel, editors, *ISC 2001: 4th International Conference on Information Security*, volume 2200 of *Lecture Notes in Computer Science*, pages 81–94, Malaga, Spain, October 1–3, 2001. Springer, Heidelberg, Germany.

[51] Masayuki Abe and Fumitaka Hoshino. Remarks on Mix-network based on permutation networks. In Kwangjo Kim, editor, *PKC 2001: 4th International Workshop on Theory and Practice in Public Key Cryptography*, volume 1992 of *Lecture Notes in Computer Science*, pages 317–324, Cheju Island, South Korea, February 13–15, 2001. Springer, Heidelberg, Germany.

[52] Masayuki Abe and Masayuki Kanda. A key escrow scheme with time-limited monitoring for one-way communication. In Ed Dawson, Andrew Clark, and Colin Boyd, editors, *ACISP 00: 5th Australasian Conference on Information Security and Privacy*, volume 1841 of *Lecture Notes in Computer Science*, pages 163–177, Brisbane, Queensland, Australia, July 10–12, 2000. Springer, Heidelberg, Germany.

[53] Masayuki Abe and Tatsuaki Okamoto. Provably secure partially blind signatures. In Mihir Bellare, editor, *Advances in Cryptology – CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 271–286, Santa Barbara, CA, USA, August 20–24, 2000. Springer, Heidelberg, Germany.

[54] Miyako Ohkubo and Masayuki Abe. A length-invariant hybrid Mix. In Tatsuaki Okamoto, editor, *Advances in Cryptology – ASIACRYPT 2000*, volume 1976 of *Lecture Notes in Computer Science*, pages 178–191, Kyoto, Japan, December 3–7, 2000. Springer, Heidelberg, Germany.

[55] Masayuki Abe. Robust distributed multiplication without interaction. In Michael J. Wiener, editor, *Advances in Cryptology – CRYPTO'99*, volume 1666 of *Lecture Notes in Computer Science*, pages 130–147, Santa Barbara, CA, USA, August 15–19, 1999. Springer, Heidelberg, Germany.

[56] Masayuki Abe. Mix-networks on permutation networks. In Kwok-Yan Lam, Eiji Okamoto, and Chaoping Xing, editors, *Advances in Cryptology – ASIACRYPT'99*, volume 1716 of *Lecture Notes in Computer Science*, pages 258–273, Singapore, November 14–18, 1999. Springer, Heidelberg, Germany.

[57] Masayuki Abe and Tatsuaki Okamoto. Delegation chains secure up to constant length. In Vijay Varadharajan and Yi Mu, editors, *ICICS 99: 2nd International Conference on Information and Communication Security*, volume 1726 of *Lecture Notes in Computer Science*, pages 144–156, Sydney, Australia, November 9–11, 1999. Springer, Heidelberg, Germany.

[58] Masayuki Abe and Tatsuaki Okamoto. A signature scheme with message recovery as secure as discrete logarithm. In Kwok-Yan Lam, Eiji Okamoto, and Chaoping Xing, editors, *Advances in Cryptology – ASIACRYPT'99*, volume 1716 of *Lecture Notes in Computer Science*, pages 378–389, Singapore, November 14–18, 1999. Springer, Heidelberg, Germany.

[59] Miyako Ohkubo, Fumiaki Miura, Masayuki Abe, Atsushi Fujioka, and Tatsuaki Okamoto. An improvement on a practical secret voting scheme. In Masahiro Mambo and Yuliang Zheng, editors, *ISW'99: 2nd International Workshop on Information Security*, volume 1729 of *Lecture Notes in Computer Science*, pages 225–234, Kuala Lumpur, Malaysia, November 1999. Springer, Heidelberg, Germany.

[60] Masayuki Abe. Universally verifiable mix-net with verification work indendent of the number of mix-servers. In Kaisa Nyberg, editor, *Advances in Cryptology - EUROCRYPT '98, International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland,*

May 31 - June 4, 1998, Proceeding, volume 1403 of *Lecture Notes in Computer Science*, pages 437–447. Springer, 1998.

[61] Shingo Miyazaki, Masayuki Abe, and Kouichi Sakurai. Partially blind signature schemes for DSS and for discrete log. based message recovery signature. In *1997 Japan-Korea Joint Workshop on Information Security and Cryptography (JW-ISC'97)*, 1997.

[62] Masayuki Abe and Eiichiro Fujisaki. How to date blind signatures. In Kwangjo Kim and Tsutomu Matsumoto, editors, *Advances in Cryptology – ASIACRYPT'96*, volume 1163 of *Lecture Notes in Computer Science*, pages 244–251, Kyongju, Korea, November 3–7, 1996. Springer, Heidelberg, Germany.

[63] Masayuki Abe and Hikaru Morita. Higher radix nonrestoring modular multiplication algorithm and public-key LSI architecture with limited hardware resources. In Josef Pieprzyk and Reihaneh Safavi-Naini, editors, *Advances in Cryptology – ASIACRYPT'94*, volume 917 of *Lecture Notes in Computer Science*, pages 365–375, Wollongong, Australia, November 28 – December 1, 1995. Springer, Heidelberg, Germany.

Symposiums

[1] Peihao Li, Octavio Pérez Kempner, Mehdi Tibouchi, and Masayuki Abe. Comparision among post-quantum oblivious transfer implementations. In *The 2024 Symposium on Cryptography and Information Security (SCIS'25)*, pages 1A1–3, Fukuoka, January 2025. IEICE.

[2] Haoliang Tang, Mehdi Tibouchi, and Masayuki Abe. Optimistic fair exchange from adaptor signatures. In *The 2024 Symposium on Cryptography and Information Security (SCIS'25)*, pages 4F1–5, Fukuoka, January 2025. IEICE.

[3] Zehua Shang, MIyako Ohkubo, Mehdi Tibouchi, and Masayuki Abe. On variations of multi-round special soundness and their fiat-shamir transform. In *The 2024 Symposium on Cryptography and Information Security (SCIS'25)*, pages 2C3–1, Fukuoka, January 2025. IEICE.

[4] Yuzo Kataoka, Mehdi Tibouchi, and Masayuki Abe. A study on efficiency improvement of lattice problem-based distributed signature protocols. In *The 2024 Symposium on Cryptography and Information Security (SCIS'25)*, pages 2C4–1, Fukuoka, January 2025. IEICE.

[5] Hitoro Kaihara and Masayuki Abe Tobouchi Mehdi. Cold boot attacks on NTRU lattice-based hash-and-sign signature. In *The 2024 Symposium on Cryptography and Information Security (SCIS'25)*, pages 3B3–1, Fukuoka, January 2025. IEICE.

[6] Yuko Tamura, Masayuki Abe, Tetsuya Okuda, Yuji Tsugawa, Toshiyuki Miyazawa, Kazuki Yamamura, zo Kataoka, Yoshiharu Akabane, Tomoki Taguchi, Yuto Hirakuri, Hiroto Masuda, and Kento Yamada. A technical study of electronic cash scheme (in Japanese). In *The 2024 Symposium on Cryptography and Information Security (SCIS'25)*, pages 3F2–1, Fukuoka, January 2025. IEICE.

[7] Masaya Nanri, Octavio Perez Kempner, Mehdi Tibouchi, and Masayuki Abe. Unlinkability of distributed mercurial signatures in multi-authority. In *The 2024 Symposium on Cryptography and Information Security (SCIS'24)*, pages 2D2–2, Nagasaki, January 2024. IEICE.

[8] Yuzo Kataoka, Mehdi Tibouchi, and Masayuki Abe. Implementation of mlwe and msis assumption-based two-round n-out-of-n signature protocol. In *The 2024 Symposium on Cryptography and Information Security (SCIS'24)*, pages 2D2–1, Nagasaki, January 2024. IEICE.

[9] Moeto Suzuki, Mehdi Tibouchi, and Masayuki Abe. Improved cryptanalysis of the peregrine lattice-based signature scheme. In *The 2024 Symposium on Cryptography and Information Security (SCIS'24)*, pages 1A1–3, Nagasaki, January 2024. IEICE.

[10] Zehua Shang, MIyako Ohkubo, Mehdi Tibouchi, and Masayuki Abe. Expanding challenge space on composing generalized sigma-protocols. In *The 2024 Symposium on Cryptography and Information Security (SCIS'24)*, pages 2B3–1, Nagasaki, January 2024. IEICE.

[11] Haoliang Tang, Mehdi Tibouchi, and Masayuki Abe. Fair exchange with smart contract revisited: Combine zkcp and fairswap. In *The 2024 Symposium on Cryptography and Information Security (SCIS'24)*, pages 2B2–4, Nagasaki, January 2024. IEICE.

[12] Chao Sun, Thomas Espitau, Mehdi Tibouchi, and Masayuki Abe. Generating falcon trapdoors via gibbs sampler. In *The 2023 Symposium on Cryptography and Information Security (SCIS'23)*, pages 2A2–2, Kokura, January 2023. IEICE.

[13] Zhiyu Peng, Mehdi Tibouchi, and Masayuki Abe. Composition of zero-knowledge proof protocols from mpc-in-the-head with preprocessing. In *The 2023 Symposium on Cryptography and Information Security (SCIS'23)*, pages 1C3–4, Kokura, January 2023. IEICE.

[14] Huan Zhang, Mehdi Tibouchi, Miguel Ambrona, and Masayuki Abe. Optimistic signed exchange revisited. In *The 2023 Symposium on Cryptography and Information Security (SCIS'23)*, pages 1C3–4, Kokura, January 2023. IEICE.

[15] Zehua Shang, Mehdi Tibouchi, and Masayuki Abe. Non-interactive proof of knowledge from fiat-shamir and correlation intractable hash. In *The 2023 Symposium on Cryptography and Information Security (SCIS'23)*, pages 1C2–1, Kokura, January 2023. IEICE.

[16] Yukihiro Arakawa, Tetsuya Okuda, Tsunekazu Saitoh, Mehdi Tibouchi, and Masayuki Abe. Study on the applicability of token-based electronic cash system with an optimized currency selection algorithm to central bank digital currency (CBDC). In *The 2023 Symposium on Cryptography and Information Security (SCIS'23)*, pages 1D2–4, Kokura, January 2023. IEICE. (in Japanese).

[17] Yukihiro Arakawa, Tetsuya Okuda, Tsunekazu Saitoh, Mehdi Tibouchi, and Masayuki Abe. Preliminary study on the applicability of token-type electronic cash system to central bank digital currency (CBDC). In *The 2022 Symposium on Cryptography and Information Security (SCIS'22)*, pages 3E2–3, Osaka, January 2022. IEICE. (in Japanese).

[18] Huan Zhang, Mehdi Tibouchi, Miguel Ambrona, and Masayuki Abe. Comparison of transaction cost on different fair exchange protocols. In *The 2022 Symposium on Cryptography and Information Security (SCIS'22)*, pages 3E2–2, Osaka, January 2022. IEICE.

[19] Quan Yuan, Mehdi Tibouchi, and Masayuki Abe. Quantum-accessible security of stateless hash-based signature schemes. In *The 2022 Symposium on Cryptography and Information Security (SCIS'22)*, pages 2E5–4, Osaka, January 2022. IEICE.

[20] Chao Sun, Thomas Espitau, Mehdi Tibouchi, and Masayuki Abe. Optimal lattice trapdoor for the Klein-GPV and Peikert sampler. In *The 2022 Symposium on Cryptography and Information Security (SCIS'22)*, pages 4A1–1, Osaka, January 2022. IEICE.

[21] Zehua Shang, Mehdi Tibouchi, and Masayuki Abe. A study of non-malleability definitions on timed commitments. In *The 2022 Symposium on Cryptography and Information Security (SCIS'22)*, pages 1A3–3, Osaka, January 2022. IEICE.

[22] Kyosuke Yamashita, Mehdi Tibouchi, and Masayuki Abe. Limits on the power of commit-and-prove NIZKs. In *The 2021 Symposium on Cryptography and Information Security (SCIS'21)*, pages 3A2–4, online, January 2021. IEICE. (in Japanese).

[23] Quan Yuan, Mehdi Tibouchi, and Masayuki Abe. Security notions of stateful signature schemes. In *The 2021 Symposium on Cryptography and Information Security (SCIS'21)*, pages 4A2–1, online, January 2021. IEICE.

[24] Chao Sun, Thomas Espitau, Mehdi Tibouchi, and Masayuki Abe. Towards improving lattice attacks on (EC)DSA. In *The 2021 Symposium on Cryptography and Information Security (SCIS'21)*, pages 2A2–4, online, January 2021. IEICE.

[25] Chao Sun, Mehdi Tibouchi, and Masayuki Abe. On the hardness of lwe with non-uniform binary-error. In *The 2020 Symposium on Cryptography and Information Security (SCIS'20)*, pages 4B1–4, Kochi, January 2020. IEICE.

[26] Hideki Kano, Fumiyuki Kato, Mehdi Tibouchi, Masayuki Abe, and Sou You. Privacy-preserving deep learning using distributed SGX processing. In *The 2020 Symposium on Cryptography and Information Security (SCIS'20)*, pages 4C1–1, Kochi, January 2020. IEICE.

[27] Kyosuke Yamashita, Mehdi Tibouchi, and Masayuki Abe. The augmented black box framework and zero-knowledge proofs of plaintext equality. In *The 2020 Symposium on Cryptography and Information Security (SCIS'20)*, pages 1A1–3, Kochi, January 2020. IEICE.

[28] Hideki Kano, Mehdi Tibouchi, and Masayuki Abe. Timed-release functional encryption with Intel SGX. In *The 2019 Symposium on Cryptography and Information Security (SCIS'19)*, pages 2A3–5, Otsu, January 2019. IEICE.

[29] Kyousuke Yamashita, Mehdi Tibouchi, and Masayuki Abe. On augmented black-box constructions based on an oracle without witness indistinguishability. In *The 2019 Symposium on Cryptography and Information Security (SCIS'19)*, pages 3A3–3, Otsu, January 2019. IEICE.

[30] Chao Sun, Mehdi Tibouchi, and Masayuki Abe. Sample-time trade-off for the Arora-Ge attack on binary-error LWE. In *The 2019 Symposium on Cryptography and Information Security (SCIS'19)*, pages 4B1–2, Otsu, January 2019. IEICE.

[31] Fumitaka Hoshino, Masayuki Abe, and Miyako Ohkubo. Pairing type optimization problem and its hardness. In *The 2018 Symposium on Cryptography and Information Security (SCIS'18)*, pages 1B1–3, Niigata, January 2018. IEICE.

[32] Masayuki Abe, Fumitaka Hoshino, and Miyako Ohkubo. Pseudo-code performance estimation for pairing-based cryptographic schemes. In *The 2018 Symposium on Cryptography and Information Security (SCIS'18)*, pages 3A3–4, Niigata, January 2018. IEICE. (SCIS2018 Innovation Paper Award).

[33] Akira Takahashi, Mhedi Tibouchi, and Masayuki Abe. A fault attack against the qDSA signature scheme over the kummer quotient of Curve25519. In *The 2018 Symposium on Cryptography and Information Security (SCIS'18)*, pages 3B4–4, Niigata, January 2018. IEICE.

[34] Junichi Tomida, Masayuki Abe, and Tatsuaki Okamoto. Efficient and perfectly-hiding inner-product encryption from weaker assumptions. In *The 2017 Symposium on Cryptography and Information Security (SCIS'17)*, pages 2F1–1, Okinawa, January 2017. IEICE.

[35] Masayuki Abe. Variations of even-goldreich-micali framework for signature schemes (extended abstract). In *The 2017 Symposium on Cryptography and Information Security (SCIS'17)*, pages 4F1–4, Okinawa, January 2017. IEICE.

[36] Minseon Lee, Masayuki Abe, and Tatsuaki Okamoto. Efficient hash-based one-time signature scheme based on d-tree authentication. In *The 2017 Symposium on Cryptography and Information Security (SCIS'17)*, pages 4F1–2, Okinawa, January 2017. IEICE.

[37] Tetsuya Kyogoku, Masayuki Abe, and Tatsuaki Okamoto. A note on authenticated key exchange in cryptocurrency. In *The 2016 Symposium on Cryptography and Information Security (SCIS'16)*, pages 1A2–1, Kumamoto, January 2016. IEICE.

[38] Junichiro Kume, Masayuki Abe, and Tatsuaki Okamoto. New cryptocurrency protocol without proof of work. In *The 2016 Symposium on Cryptography and Information Security (SCIS'16)*, pages 1A2–2, Kumamoto, January 2016. IEICE.

[39] Junichiro Tomida, Masayuki Abe, and Tatsuaki Okamoto. Adaptively secure functional encryption for inner-product values. In *The 2016 Symposium on Cryptography and Information Security (SCIS'16)*, pages 2E4–4, Kumamoto, January 2016. IEICE.

[40] Fumitaka Hoshino, Masayuki Abe, and Miyako Ohkubo. Optimal conversion method from symmetric to asymmetric pairings (in japanese). In *The 2016 Symposium on Cryptography and Information Security (SCIS'16)*, pages 2D1–1, Kumamoto, January 2016. IEICE.

[41] Tetsuya Kyogoku, Minseon Lee, Masayuki Abe, and Tatsuaki Okamoto. Threshold two-move password authenticated key exchange protocol. In *The 2015 Symposium on Cryptography and Information Security (SCIS'15)*, pages 1E2–5, Kokura, January 2015. IEICE.

[42] Yudai Mimasu, Masayuki Abe, and Tatsuaki Okamoto. A secure signature scheme with tight reduction to the RSA assumption from indistinguishability obfuscation. In *The 2015 Symposium on Cryptography and Information Security (SCIS'15)*, pages 2E3–3, Kokura, January 2015. IEICE.

[43] Takeya Tango, Masayuki Abe, and Tatsuaki Okamoto. On polynomial-time algorithm for deciding possibility of pairing-type conversions. In *The 2015 Symposium on Cryptography and Information Security (SCIS'15)*, pages 2B4–5, Kokura, January 2015. IEICE.

[44] Junichiro Kume, Masayuki Abe, and Tatsuaki Okamoto. Lottery protocol for cryptocurrency. In *The 2015 Symposium on Cryptography and Information Security (SCIS'15)*, pages 3F2–4, Kokura, January 2015. IEICE.

[45] Ryo Hiromasa, Masayuki Abe, and Tatsuaki Okamoto. SIMD operations in GSW-FHE. In *The 2015 Symposium on Cryptography and Information Security (SCIS'15)*, pages 3E4–1, Kokura, January 2015. IEICE.

[46] Takeya Tango, Masayuki Abe, and Tatsuaki Okamoto. Implementating conversion algorithm from type-i to type-iii pairing groups. In *The 2014 Symposium on Cryptography and Information Security (SCIS'14)*, pages 2E1–4, Kagoshima, January 2014. IEICE.

[47] Ryo Hiromasa, Masayuki Abe, and Tatsuaki Okamoto. Multilinear maps on LWE. In *The 2014 Symposium on Cryptography and Information Security (SCIS'14)*, pages 2B3–2, Kagoshima, January 2014. IEICE.

[48] Yudai Mimasu, Masayuki Abe, and Tatsuaki Okamoto. Non-interactive first-price and second-price auction protocols using fully homomorphic encryption. In *The 2014 Symposium on Cryptography and Information Security (SCIS'14)*, pages 2D3–4, Kagoshima, January 2014. IEICE.

[49] Masayuki Abe, Miyako Ohkubo, and Mehdi Tibouchi. Impossibility of symmetric structure-preserving signatures with single verification equation. In *The 2013 Symposium on Cryptography and Information Security (SCIS'13)*, pages 2E4–3, Kyoto, January 2013. IEICE.

[50] Naoyoshi Okamae, Maki Yoshida, Kenta Kumojima, Masayuki Abe, Miyako Ohkubo, and Toru Fujiwara. Automated attack derivation for cryptographic problems on bilinear groups. In *The 2011 Symposium on Cryptography and Information Security (SCIS'11)*, pages 4F1–1, Kokura, January 2011. IEICE.

[51] Miyako Ohkubo and Masayuki Abe. An efficient signature for a message in group. In *The 2010 Symposium on Cryptography and Information Security (SCIS'10)*, pages 3A1–3, Kagawa, January 2010. IEICE.

[52] Miyako Ohkubo and Masayuki Abe. Security of universally composable blind signatures revisited. In *The 2009 Symposium on Cryptography and Information Security (SCIS'09)*, pages 3B4–3, Otsu, January 2009. IEICE.

[53] Miyako Ohkubo and Masayuki Abe. Similarity between anonymity in ring signatures and security in public-key encryption. In *The 2007 Symposium on Cryptography and Information Security (SCIS'07)*, pages 2B4–4, Nagasaki, January 2007. IEICE.

[54] Masayuki Abe and Hideki Imai. Breaking some robust Mix-nets. In *The 2003 Symposium on Cryptography and Information Security (SCIS'03)*, pages 7B–2. IEICE, 2003.

[55] Miyako Ohkubo and Masayuki Abe. Security of three-move blind signature schemes reconsidered. In *The 2003 Symposium on Cryptography and Information Security (SCIS'03)*, pages 13C–4, Hamamatsu, January 2003. IEICE.

[56] Koji Chida, Hiroyuki Kito, and Masayuki Abe. Robust and flexible hybrid mix. In *The 2003 Symposium on Cryptography and Information Security (SCIS'03)*, pages 7B–3, Hamamatsu, January 2003. IEICE.

[57] Masayuki Abe and Hideki Imai. Security definitions and modular constructions of public-key authenticated encryption schemes. In *The 2002 Symposium on Cryptography and Information Security (SCIS'02)*, pages 7A–4, Shirahama, January 2002. IEICE.

[58] Fumitaka Hoshino and Masayuki Abe. Batch verification and multiple exponentiation algorithm. In *The 2002 Symposium on Cryptography and Information Security (SCIS'02)*, pages 3A–1, Shirahama, January 2002. IEICE.

[59] Miyako Ohkubo, Masayuki Abe, Koutarou Suzuki, and Shigeo Tsujii. Short 1-out-of-n proofs. In *The 2002 Symposium on Cryptography and Information Security (SCIS'02)*, pages 4C–4. IEICE, January 2002.

[60] Miyako Ohkubo and Masayuki Abe. On public-key encryption with signature in non-separable model. In *The 2001 Symposium on Cryptography and Information Security (SCIS'01)*, pages 11B–2, Oiso, January 2001. IEICE.

[61] Masayuki Abe, Miyako Ohkubo, Atsushi Fujioka, and Fumitaka Hoshino. An electronic voting scheme with revocable threshold blind signatures. In *The 2000 Symposium on Cryptography and Information Security (SCIS'00)*, pages SCIS2000–B25, Okinawa, January 2000. IEICE.

[62] Atsushi Fujioka, Masayuki Abe, Miyako Ohkubo, and Fumitaka Hoshino. An implementation and an experiment of a practical and secure voting scheme. In *The 2000 Symposium on Cryptography and Information Security (SCIS'00)*, pages SCIS2000–C48, Okinawa, January 2000. IEICE.

[63] Fumitaka Hoshino and Masayuki Abe. More efficient Mix-network on permutation networks. In *The 2000 Symposium on Cryptography and Information Security (SCIS'00)*, pages SCIS2000–B28, Okinawa, January 2000. IEICE.

[64] Masayuki Abe and Jan Camenisch. Partially blind signature schemes. In *The 1997 Symposium on Cryptography and Information Security (SCIS'97)*, pages SCIS97–33D, Fukuoka, January 1997. IEICE.

Technical Reports

[1] A. Takahashi, M. Tibouchi, and M. Abe, "Application of the singular curve point decompression attack to the Bitcoin curve," techreport ISEC2018-28, IEICE Engineering and Science Society, Techinical Committee Conference on Information Security (ISEC), Sapporo, July 2018.

[2] A. Takahashi, M. Tibouchi, M. Abe, and T. Okamoto, "Optimizing Bleichenbacher's attack on Schnorr-type signatures with barely biased nonces," techreport ISEC2017-84, IEICE Engineering and Science Society, Techinical Committee Conference on Information Security (ISEC), Kochi, Dec. 2017. (Research Encouragement Award to the first author).

[3] K. Kirishima, M. Yoshida, M. Abe, M. Ohkubo, and W. Fujiwara, "On finding attacks against hardness assumptions in the generic group model," techreport ISEC2010-58, IEICE Engineering and Science Society, Techinical Committee Conference on Information Security (ISEC), Tsukuba, Nov. 2010. (in Japanese).

[4] M. Abe, T. Okamoto, and K. Suzuki, "Message recovery signature schemes from sigma-protocols," *NTT Technical Review*, vol. 6, Jan. 2008.

[5] G. Yamamoto, E. Fujisaki, and M. Abe, "An efficiently-verifiable zero-knowledge argument for proofs of knowledge," techreport ISEC2005-48, IEICE Engineering and Science Society, Techinical Committee Conference on Information Security (ISEC), Iwate, July 2005.

[6] M. Abe, "On proxy signatures and batch verification," techreport ISEC-2, IEICE Engineering and Science Society, Techinical Committee Conference on Information Security (ISEC), May 2000.

[7] M. Ohkubo and M. Abe, "A robust length-invariant hybrid Mix," techreport ISEC-1, IEICE Engineering and Science Society, Techinical Committee Conference on Information Security (ISEC), May 2000.

[8] M. Abe, K. Suzuki, A. Fujioka, M. Ohkubo, and F. Hoshino, "Electronic voting schemes," *NTT R&D*, vol. 49, pp. 685–693, Jan. 2000.

[9] M. Abe, "Mix-network on permutation networks," techreport ISEC99-10, IEICE Engineering and Science Society, Techinical Committee Conference on Information Security (ISEC), May 1999. (in Japanese).

[10] H. Moribatake, M. Abe, A. Fujioka, and J. Gohara, "Electronic cash scheme," *NTT Review*, vol. 9, May 1997.

[11] K. Ohta, M. Abe, E. Fujisaki, and H. Moribatake, "Electronic money schemes," *NTT R&D*, vol. 44, pp. 931–938, Oct. 1995.

[12] M. Aoyama, M. Hikaru, and M. Abe, "PKC/FEAL LSI and its applications for information security," *NTT R&D*, vol. 44, pp. 923–93, Oct. 1995.

[13] M. Abe and H. Morita, "Hardware-oriented modular-multiplication method with quotient modification," techreport ISEC94-1, IEICE Engineering and Science Society, Techinical Committee Conference on Information Security (ISEC), May 1994.

Book and Book Chapters

[1] Masayuki Abe, editor. *Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010. Proceedings*, volume 6477 of *Lecture Notes in Computer Science*. Springer, 2010.

[2] Mike Sipser. Introduction to the theory of computation, 2nd edition (japanese translation), May 2008.

[3] Masayuki Abe and Virgil D. Gligor, editors. *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security, ASIACCS 2008, Tokyo, Japan, March 18-20, 2008*. ACM, 2008.

[4] Masayuki Abe, editor. *Topics in Cryptology - CT-RSA 2007, The Cryptographers' Track at the RSA Conference 2007, San Francisco, CA, USA, February 5-9, 2007, Proceedings*, volume 4377 of *Lecture Notes in Computer Science*. Springer, 2006.

[5] IEICE, editor. *Information Security Handbook (in Japanese)*, chapter Sec.3.2 Foundations of Cryptographic Protocols. Kyouritsu SHuppan, 2003.