Curriculum Vitae

Masayuki Abe

June 2, 2019

Background

Date of Birth: 21 June 1967

Place of Birth: Yokohama, Japan

Nationality: Japanese

Language: Japanease, English

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

Education

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

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

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

Professional Experience

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.

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

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.

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.

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.

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

2013.4-present Senior Distinguished Researcher of NTT Secure Platform Laboratories.

2018.4-present Manager of Cryptography Research Laboratory in NTT Secure Platform Laboratories.

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

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

Steering Committee Member: Asiacrypt Steering Committee (2012-present)

General (Co-)Chair for Interantional Conferences: TCC'13

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.

Editorial Board :

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

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

IACR School Committee: 2014-2017.

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

Awards

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

2008.3: Recognition of Service Award (for the PC Co-Chair of ASIACCS08) from Association for Computing Machinery

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

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

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

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

Academic Experiences

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

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

2003.5: 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

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

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

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

Invited Talks in Conferences and Workshops

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.

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

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

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

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

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

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.

2011.5.31: " Signature Scheme with Efficient Proof of Validity", International Workshop on Coding and Cryptology, Qingdao, China, May 30-June 3, 2011

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.

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

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

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

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

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

2015.11.3: Asiacrypt 2015, "Structure-Preserving Cryptography"

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

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)

Publication

Journal Papers

1. Masayuki Abe, Fumitaka Hoshino, Miyako Ohkubo, "Opcount: A Pseudo-Code Performance Estimation System for Pairing-Based Cryptography", IEICE Transactions (to appear)
2. Masayuki Abe, Fumitaka Hoshino, Miyako Ohkubo "Fast and Scalable Bilinear-Type Conversion Method for Large Scale Crypto Schemes," IEICE Transactions 102-A(1): 251-269 (2019)
3. Masayuki Abe, Jan Camenisch, Rafael Dowsley, Maria Dubovitskaya, "On the Impossibility of Structure-Preserving Deterministic Primitives," J. Cryptology 32(1): 239-264 (2019)
4. Akira Takahashi, Mehdi Tibouchi, Masayuki Abe, "New Bleichenbacher Records: Fault Attacks on qDSA Signatures," IACR Transactions on Cryptographic Hardware Embedded Systems (TCHES) 2018(3): 331-371 (2018)
5. Masayuki Abe, "Variations of Even-Goldreich-Micali Framework for Signature Schemes," IEICE Transactions 100-A(1): 12-17 (2017)
6. Masayuki Abe, Melissa Chase, Bernardo David, Markus Kohlweiss, Ryo Nishimaki, Miyako Ohkubo, "Constant-Size Structure-Preserving Signatures: Generic Constructions and Simple Assumptions," J. Cryptology 29(4): 833-878 (2016)
7. Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristian Haralambiev, Miyako Ohkubo, "Structure-Preserving Signatures and Commitments to Group Elements," J. Cryptology 29(2): 363-421 (2016)
8. Ryo Hiromasa, Masayuki Abe, Tatsuaki Okamoto, "Packing Messages and Optimizing Bootstrapping in GSW-FHE," IEICE Transactions 99-A(1): 73-82 (2016)
9. Masayuki Abe, Sherman M. Chow, Kristian Haralambiev, Miyako Ohkubo, "Double-Trapdoor Anonymous Tags for Traceable Signatures," International Journal of Information Security, 2013, DOI 10.1007/s10207-012-0184-3, Vol. 12(1), pp.19–31, 2013
10. Masayuki Abe, Tatsuaki Okamoto, Kotaro Suzuki, "Message Recovery Signature Schemes from Sigma-Protocols," IEICE Trans. Fundamentals, Vol. E96-A, No.1, pp.19–31, 2013

11. Masayuki Abe, Miyako Ohkubo,"A framework for universally composable non-committing blind signatures," Intrenational Journal of Applied Cryptography (IJACT), Vol.2 No.3, pp.229-249, 2012, http://dx.doi.org/10.1504/IJACT.2012.045581.

12. Masayuki Abe, Eike Kiltz, Tatsuaki Okamoto, "Chosen Ciphertext Security with Optimal Ciphertext Overhead," IEICE Trans. Fundamentals, Vol.E93-A(1), pp.22-33, 2010.

13. Masayuki Abe, Yang Cui, Hideki Imai, Eike Kiltz, "Efficient Hybrid Encryption from ID-Based Encryption," Designs, Codes and Cryptography, Vol.54, No.3, pp.205-240, 2010.

14. Masayuki Abe, Yang Cui, Hideki Imai, Kaoru Kurosawa, "Tag-KEM from Set Partial Domain One-Way Permutations," IEICE Trans. Fundamentals, Vol.E92-A(1), pp.42-52, January 2009.

15. Miyako Ohkubo and Masayuki Abe, "On the Definitions of Anonymity for Ring Signatures," IEICE Trans. Fundamentals, Vol. E91-A(1), pp.272-282, January 2008.

16. Masayuki Abe, Rosario Gennaro, Kaoru Kurosawa, "Tag-KEM/DEM: A New Framework for Hybrid Encryption," Jounal of Cryptology, Vol. 21(1), pp.97-130, January 2008.

17. Masayuki Abe, Hideki Imai, "Flaws in Robust Optimistic Mix-Nets and Stronger Security Notions," IEICE Trans. Fundamentals, Vol. E89-A, No. 1, pp.99-105, January 2006

18. Koji Chida and Masayuki Abe, "Flexible-Routing Anonymous Networks Using Optimal Length of Ciphertext," IEICE Trans. Fundamentals, Vol. E88-A, No. 1, pp.211-221, January 2005

19. Masayuki Abe, Miyako Ohkubo and Kotaro Suzuki, "Efficient Threshold Signer-Ambiguous Signatures from Variety of Keys," IEICE Trans. Fundamentals, Vol. E87-A, No. 2, pp.471-479, February 2004

20. Masayuki Abe, Miyako Ohkubo and Kotaro Suzuki, "1-out-of-n Signatures from a Variety of Keys," IEICE Trans. Fundamentals, Vol. E87-A, No. 1, pp.131-140, January 2004

21. Masayuki Abe, "Combining Encryption and Proof of Knowledge in the Random Oracle Model," The Computer Journal, Vol. 47, pp.58-70, No. 1, pp.58-70, 2004.

22. Masayuki Abe and Kotaro Suzuki, "M+1-st Auction Using Homomorphic Encryption," IEICE Trans. Fundamentals, Vol. E86-A, No. 1, pp.136-141, January 2003

23. Fumitaka Hoshino, Masayuki Abe and Tetsutaro Kobayashi, "Lenient/Strict Batch Verification in Several Groups," IEICE Trans. Fundamentals, Vol. E86-A, No. 1, pp.64-72, January 2003

24. Masayuki Abe and Masayuki Kanda, "A Key Escrow Scheme with Time-Limited Monitoring for One-way Communication," The Computer Journal, Vol. 45, No. 6, pp.661-671, 2002, British Computer Society, 2002

25. Masayuki Abe and Tatsuaki Okamoto, "Delegation Chains Secure up to Constant Length," IEICE Trans. Fundamentals, Vol. E85-A, No. 1, pp.110-116, January, 2002

26. Miyako Ohkubo and Masayuki Abe, "A Length-invariant Hybrid Mix," IEICE Trans. Fundamentals, Vol. E84-A, No. 4, pp.931-940, April, 2001

27. Masayuki Abe and Tatsuaki Okamoto, "A signature scheme with message recovery as secure as discrete logarithm," IEICE Trans. Fundamentals, Vol. E84-A, No. 2, pp.197-204, February, 2001

28. Masayuki Abe, "Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-servers," IEICE Trans. Fundamentals, Vol. E83-A, No. 7, pp.1431-1440, July, 2000

29. Masayuki Abe, "Non-interactive and Optimally Resilient Distributed Multiplication," IEICE Trans. Fundamentals, Vol. E83-A, No. 4, pp.598-605, April, 2000

Selected Papers

1. Masayuki Abe, Charanjit S. Jutla, Miyako Ohkubo, Arnab Roy: Improved (Almost) Tightly-Secure Simulation-Sound QA-NIZK with Applications. ASIACRYPT (1) 2018: 627-656

2. Masayuki Abe, Miguel Ambrona, Miyako Ohkubo, Mehdi Tibouchi: Lower Bounds on Structure-Preserving Signatures for Bilateral Messages. SCN 2018: 3-22

3. M. Abe, D. Hofheinz, R. Nishimaki, M. Ohkubo, J. Pan, Compact Structure-preserving Signatures with Almost Tight Security", In Advances in Cryptology - CRYPTO 2017 Proceedings, pages 548-580, Springer, 2017.

4. J. Tomida, M. Abe, T. Okamoto, Efficient Functional Encryption for Inner-Product Values with Full-Hiding Security", In the proceedings of Information Security - 19th International Conference, ISC 2016, pages 408-425, Springer, 2016.

5. M. Abe, F. Hoshino, M. Ohkubo, Design in Type-I, Run in Type-III: Fast and Scalable Bilinear-Type Conversion Using Integer Programming", In Advances in Cryptology - CRYPTO 2016 Proceedings, Part 3, pages 387–415, Springer, 2016.

6. R. Hiromasa, M. Abe, T. Okamoto, Packing Messages and Optimizing Bootstrapping in GSW-FHE", In the proceedings of Public Key Cryptography 2015, pages 699-715, Springer-Verlag, 2015.

7. M. Abe, M. Kohlweiss, M. Ohkubo, M. Tibouchi, Fully Structure-Preserving Signatures and Shrinking Commitments", In the proceedings of Advances in Cryptology - EUROCRYPT 2015, Volume 9057 of Lecture Notes in Computer Science, pages 35-65, Springer-Verlag, 2015.

8. M. Abe, J. Groth, M. Ohkubo, T. Tango, "Converting Cryptographic Schemes from Symmetric to Asymmetric Bilinear Groups", In Advances in Cryptology - CRYPTO 2014 Proceedings, Part I, pages 241–260, Springer, 2014

9. M. Abe, J. Groth, M. Ohkubo, M. Tibouchi, "Structure-Preserving Signatures from Type II Pairings", In Advances in Cryptology - CRYPTO 2014 Proceedings, Part I, pages 390–407, Springer, 2014

10. M. Abe, J. Groth, M. Ohkubo, M. Tibouchi, "Unified, Minimal and Selectively Randomizable Structure-Preserving Signatures", In the Proceedings of Theory of Cryptography - 11th Theory of Cryptography Conference (TCC) 2014, pages 688–712, Springer, 2014

11. M. Abe, J. Camenisch, R. Dowsley, M. Dubovitskaya, "On the Impossibility of Structure-Preserving Deterministic Primitives", In the Proceedings of Theory of Cryptography - 11th Theory of Cryptography Conference (TCC) 2014, pages713–738, Springer, 2014

12. M. Abe, J. Camenisch, M. Dubovitskaya, R. Nishimaki, "Universally Composable Adaptive Oblivious Transfer with Access Control from Standard Assumptions, In the Proceedings of ACM Digital Identity Management Workshop (ACM DIM) 2013, pages 1-12, ACM, 2013

13. M. Abe, B. David, M. Kohlweiss, R. Nishimaki, M. Ohkubo, "Tagged One-Time Signatures: Optimal Tag Size and Tight Security, In the proceedings of Public Key Cryptography 2013, pages 312-331, Springer-Verlag, 2013

14. M. Abe, M. Chase, B. David, M. Kohlweiss, R. Nishimaki, M. Ohkubo, "Constant-Size Structure-Preserving Signatures: Generic Constructions and Simple Assumptions", In the proceedings of Advances in Cryptology - ASIACRYPT 2012, Volume 7658 of Lecture Notes in Computer Science, pages 4-24, Springer-Verlag, 2012.

15. M. Abe, K. Haralambiev, M. Ohkubo, "Group to Group Commitments Do Not Shrink", In the proceedings of Advances in Cryptology - EUROCRYPT 2012, Volume 7237 of Lecture Notes in Computer Science, pages 301-317, Springer-Verlag, 2012.

16. M. Abe, J. Groth, M. Ohkubo, "Separating Short Structure-Preserving Signatures from Non-interactive Assumptions", In the proceedings of Advances in Cryptology - ASIACRYPT 2011, Volume 7073 of Lecture Notes in Computer Science, pages 628-646, Springer-Verlag, 2011.

17. M. Abe, J. Groth, K. Haralambiev, M. Ohkubo, "Optimal Structure-Preserving Signatures in Asymmetric Bilinear Groups", In the proceedings of Advances in Cryptology - CRYPTO 2011, Volume 6841 of Lecture Notes in Computer Science, pages 649-666, Springer-Verlag, 2011.

18. M. Abe, S. S. M. Chow, K. Haralambiev, M. Ohkubo, "Double-Trapdoor Anonymous Tags for Traceable Signatures", In the proceedings of Applied Cryptography and Network Security - 9th International Conference, ACNS 2011, Volume 6715 of Lecture Notes in Computer Science, pages 183-200, Springer-Verlag, 2011.

19. M. Abe, K. Haralambiev, M. Ohkubo, "Efficient Message Space Extension for Automorphic Signatures", In the proceedings of ISC 2010, Volume 6531 of Lecture Notes in Computer Science, pages 319-330, Springer-Verlag, 2011.

20. M. Abe, G. Fuschbauer, J. Groth, K. Haralambiev, M. Ohkubo, "Structure-Preserving Signatures and Commitments to Group Elements", In the proceedings of Advances in Cryptology - CRYPTO 2010, Volume 6223 of Lecture Notes in Computer Science, pages 209-236, Springer-Verlag, 2010.

21. M. Abe, M. Ohkubo, "A Framework for Universally Composable Non-Committing Blind Signatures", In the proceedings of ASIACRYPT 2009, LNCS, Springer-Verlag, 2009

22. M. Abe, E. Kiltz, and T. Okamoto, "Compact CCA-Secrue Encryption for Messages of Arbitrary Length", In the proceedings of PKC'09, Volume 5443 of Lecture Notes in Computer Science, pages 377-392, Springer-Verlag, 2009.

23. M. Abe, E. Kiltz, and T. Okamoto, "Chosen-Cipertext Security with Optimal Ciphertext Overhead", In the proceedings of Advances in Cryptology - ASIACRYPT 2008, Volume 5350 of Lecture Notes in Computer Science, pages 355-371, Springer-Verlag, 2008.

24. M. Abe and S. Fehr, "Perfect NIZK with Adaptive Soundness", In the proceedings of Theory of Cryptography, 4th Theory of Cryptography Conference, TCC 2007, Volume 4392 of Lecture Notes in Computer Science, pages 118-136, Springer-Verlag, 2007.

25. M. Ohkubo and M. Abe, "On the Definition of Anonymity for Ring Signatures", In the proceedings of Progressin Cryptology - VIETCRYPT 2006, Volume 4341 of Lecture Notes in Computer Science, pages 157-174, Springer-Verlag, 2006.

26. M. Abe, Y. Cui, H. Imai and K. Kurosawa, "Tag-KEM from Set Partial Domain One-Way Permutations", In L. M. Batten and R. Safavi-Naini editors, Information Security and Privacy, 11th Australasian Conference, ACISP 2006, Volume 4058 of Lecture Notes in Computer Science, pages 360-370, Springer-Verlag, 2006.

27. M. Abe, R. Gennaro, K. Kurosawa, and V. Shoup, "Tag-KEM/DEM: A New Framework for Hybrid Encryption and A New Analysis of Kurosawa-Desmedt KEM", In R. Cramer editor, Advances in Cryptology - EUROCRYPT 2005, Volume 3494 of Lecture Notes in Computer Science, pages 128-146, Springer-Verlag, 2005.

28. M. Abe and S. Fehr, "Adaptively Secure Feldman VSS and Applications to Universally-Composable Threshold Cryptography", In M. K. Franklin editor, Advances in Cryptology - CRYPTO 2004, Volume 3152 of Lecture Notes in Computer Science, pages 317-334, Springer-Verlag, 2004.

29. M. Abe and H. Imai, "Flaws in Some Robust Optimistic Mix-Nets", In R. Safavi-Naini and J. Seberry editors, Information Security and Privacy, 8th Australasian Conference, ACISP 2003, Volume 2727 of Lecture Notes in Computer Science, pages 39-50, Springer-Verlag, 2003.

30. M. Abe and K. Suzuki, "Receipt-free Sealed-bid Auction", In A. H. Chan and V. D. Gligor editors, Information Security 5th International Conference, ISC 2002, Volume 2433 of Lecture Notes in Computer Science, pages 191-199, Springer-Verlag, 2002.

31. M. Abe, M Ohkubo, and K. Suzuki, "1-out-of-n Signatures from a Variety of Keys", In Y. Zheng editor, Advances in Cryptology – ASIACRYPT 2002, Volume 2501 of Lecture Notes in Computer Science, pages 415-432, Springer-Verlag, 2002.

32. M. Abe, R. Cramer, and S. Fehr, "Non-interactive Distributed Verifier Proofs and Proving Relations among Commitments", In Y. Zheng editor, Advances in Cryptology – ASIACRYPT 2002, Volume 2501 of Lecture Notes in Computer Science, pages 206-223, Springer-Verlag, 2002.

33. K. Suzuki and M. Abe, "M+1-st Price Auction using Homomorphic Encryption", In D. Naccache editor, Proceedings of Public Key Cryptosystems – PKC 2002, Volume 2274 of Lecture Notes in Computer Science, pages 115-124. Springer-Verlag, 2002.

34. M. Abe, "Securing "Encryption + Proof of Knowledge" in the Random Oracle Model", In B. Preneel editor, Topics in Cryptology - CT-RSA 2002, The Cryptographer's Track at the RSA Conference, Volume 2271 of Lecture Notes in Computer Science, pages 277-289, Springer-Verlag, 2002.

35. M. Abe and M. Ohkubo, "Provably Secure Fair Blind Signatures with Tight Revocation", In C. Boyd editor, Advances in Cryptology – ASIACRYPT 2001, Volume 2248 of Lecture Notes in Computer Science, pages 583-602, Springer-Verlag, 2001.

36. F. Hoshino, M. Abe, T. Kobayashi, "Lenient/Strict Batch Verification in Several Groups", In the proceedings of Information Security, 4th International Conference, ISC 2001, Volume 2200 of Lecture Notes in Computer Science, pages 81-94, Springer-Verlag, 2001.

37. M. Abe, "A Secure Three-Move Blind Signature Scheme for Polynomially Many Signatures", In B. Pfitzmann editor, Advances in Cryptology – EUROCRYPT 2001, Volume 2045 of Lecture Notes in Computer Science, pages 136-151, Springer-Verlag, 2001.

38. M. Abe and F. Hoshino, "Remarks on Mix-network based on Permutation Network", In K. Kim editor, Public Key Cryptography – PKC'2001, Volume 1992 of Lecture Notes in Computer Science, pages 317–324, Springer-Verlag, 2001.

39. M. Ohkubo and M. Abe "A Length-invariant Hybrid Mix", In T. Okamoto editor, Advances in Cryptology – ASIACRYPT 2000, Volume 1976 of Lecture Notes in Computer Science, pages 178-191, Springer-Verlag, 2000.

40. M. Abe and T. Okamoto, "Provably secure partially blind signatures", In Bellare editor, Advances in Cryptology – CRYPTO 2000, Volume 1880 of Lecture Notes in Computer Science, pages 271-286, Springer-Verlag, 2000.

41. M. Abe and M. Kanda "A Key Escrow Scheme with Time-Limited Monitoring for One-way Communication", In the proceedings of ACISP2000, Volume 1841 of Lecture Notes in Computer Science, pages 163-177, Springer-Verlag, 2000.

42. M. Abe, "Mix-networks on Permutation Networks", In K. Lam, E. Okamoto and C. Xing editors, Advances in Cryptology – ASIACRYPT '99, Volume 1716 of Lecture Notes in Computer Science, pages 258-273, Springer-Verlag, 1999.

43. M. Abe and T. Okamoto, "A signature scheme with message recovery as secure as discrete logarithm", In K. Lam, E. Okamoto and C. Xing editors, Advances in Cryptology – ASIACRYPT '99, Volume 1716 of Lecture Notes in Computer Science, pages 378-389, Springer-Verlag, 1999.

44. M. Abe and T. Okamoto, "Delegation Chains secure up to constant length", In V. Varadharajan and Y. Mu editors, Information and Communication Security (ICICS'99), Volume 1726 of Lecture Notes in Computer Science, pages 144-156. Springer-Verlag, 1999.

45. M. Ohkubo, F. Miura, M. Abe, A. Fujioka and T. Okamoto, "An inprovement on a practical secret voting scheme", In M. Mambo and Y. Zheng editors, The second international workshop (ISW '99), Volume 1729 of Lecture Notes in Computer Science, pages 255-264, Springer-Verlag, 1999.

46. M. Abe, "Robust Distributed Multiplication without Interaction", In M. Wiener editor, Advances in Cryptology – CRYPTO '99, Volume 1666 of Lecture Notes in Computer Science, paes 130-147, Springer-Verlag, 1999.

47. M. Abe, "Universally verifiable mix-net with verification work independent of the number of mix-servers", In K. Nyberg editor, Advances in Cryptology – EUROCRYPT'98, Volume 1403 of Lecture Notes in Computer Science, pages 437-447. Springer-Verlag, 1998.

48. S. Miyazaki, M. Abe and K. Sakurai, "Partially Blind Signature Schemes for the DSS and for the Discrete Log. based Message Recovery Signature", JW-ISC'97, 1997.

49. M. Abe and E. Fujisaki, "How to date blind signatures", In K. Kim and T. Matsumoto editors, Advances in Cryptology – ASIACRYPT'96, Volume 1163 of Lecture Notes in Computer Science, pages 244-251. Springer-Verlag, 1996.

50. M. Abe and H. Morita, "Higher radix nonrestoring modular multiplication algorithm and public-key LSI architecture with limited hardware resources", In J. Pieprzyk and R.Safavi-Naini editors, Advances in Cryptology – ASIACRYPT'94, Volume 917 of Lecture Notes in Computer Science, pages 365-375. Springer-Verlag, 1995.

Technical Reports

1. Akira Takahashi, Mehdi Tibouchi, Masayuki Abe and Tatsuaki Okamoto, "Optimizing Bleichenbacher's Attack on Schnorr-Type Signatures with Barely Biased Nonces",IEICE Technical Committee on Information Security (ISEC), Japan, January 2017. (Research Encouragment Award)

2. Kenta Kirishima, Maki Yoshida, Masayuki Abe, Miyako Ohkubo, Wataru Fujiwara, "On Finding Attacks against Hardness Assumptions in the Generic Group Model (in Japanese)," Tech. Report of IEICE, IESEC 2010-58, November 2010.

3. M. Abe, T. Okamoto, K. Suzuki, Message Recovery Signature Schemes from Sigma-Protocols", NTT Technical Review, Vol.6(1), January 2008.

4. M. Abe, K. Suzuki, A. Fujoka and M. Ohkubo, F. Hoshino,"Electronic Voting Schemes", NTT R&D, Vol. 49, pp.685–693, November, 2000.

5. M. Ookubo and M. Abe, "A Robust Length-invariant Hybrid Mix", Technical report of IEICE, ISEC-1, May, 2000.

6. M. Abe, "On Proxy Signatures and Batch Verification", Technical report of IEICE, ISEC-2, May, 2000.

7. M. Abe, "Mix-network on Permutation Networks", (Technical report of IEICE), ISEC99-10, May, 1999, (in Japanese).

8. H. Moribatake, M. Abe, A. Fujioka and J. Gohara, "Electronic Cash Scheme", NTT Review, vol.9 No.3 May, 1997.

9. K. Ohta, M. Abe, E. Fujisaki and H. Moribatake, "Electronic Money Schemes", NTT R&D, pp.931–938, Vol.44 October, 1995.

10. M. Aoyama, H. Morita and M. Abe, "PKC/FEAL LSI and its Applications for Information Security", NTT R&D, pp.923–930, Vol.44 October, 1995.

11. M. Abe and H. Morita, Hardware-oriented modular-multiplication method with quotient modification, Technical Report of IEICE, ISEC 94-1, pages 1-9, May 1994.

Symposium and Misc

1. A. Takahashi, M. Tibouchi, M. Abe, "A Fault Attack against the qDSA Signature Scheme over the Kummer Quotient of Curve25519", The 2018 Symposium on Cryptography and Information Security (SCIS2018), IEICE, Jan. 2018

2. M. Abe, F. Hoshino, M. Ohkubo, "Pseudo-Code Performance Estimation for Pairing-Based Cryptographic Schemes", The 2018 Symposium on Cryptography and Information Security (SCIS2018), IEICE, Jan. 2018

3. M. Lee, M. Abe, T. Okamoto, "Efficient Hash-based One-Time Signature Scheme based on D-Tree Authentication Structure, The 2017 Symposium on Cryptography and Information Security (SCIS2017), IEICE, Jan. 2017

4. M. Abe, "Variations of Even-Goldreich-Micali Framework for Signature Schemes (Extended Abstract), The 2017 Symposium on Cryptography and Information Security (SCIS2017), IEICE, Jan. 2017

5. J. Tomida, M. Abe, T. Okamoto, "Efficient and Perfectly-Hiding Inner-Product Encryption from Weaker Assumptions, The 2017 Symposium on Cryptography and Information Security (SCIS2017), IEICE, Jan. 2017 (in Japanese)

6. F. Hoshino, M. Abe, M. Ohkubo, "Optimal Conversion Method from Symmetric to Asymmetric Pairings, The 2016 Symposium on Cryptography and Information Security (SCIS2016), IEICE, Jan. 2016 (in Japanese)

7. J. Kume, M. Abe, T. Okamoto, "New Cryptocurrency Protocol without Proof of Work, The 2016 Symposium on Cryptography and Information Security (SCIS2016), IEICE, Jan. 2016

8. T. Kyogoku, M. Abe, T. Okamoto, "A Note on Authenticated Key Exchange in Cryptocurrency, The 2016 Symposium on Cryptography and Information Security (SCIS2016), IEICE, Jan. 2016

9. R. Hiromasa, M. Abe, T. Okamoto, "SIMD Operations in GSW-FHE, The 2015 Symposium on Cryptography and Information Security (SCIS2015), IEICE, Jan. 2015

10. J. Kume, M. Abe, T. Okamoto, "Lottery Protocol for Cryptocurrency, The 2015 Symposium on Cryptography and Information Security (SCIS2015), IEICE, Jan. 2015

11. T. Tango, M. Abe, T. Okamoto, "On Polynomial-Time Algorithm for Deciding Possibility of Pairing-Type Conversions, The 2015 Symposium on Cryptography and Information Security (SCIS2015), IEICE, Jan. 2015 (in Japanese)

12. Y. Mimasu, M. Abe, T. Okamoto, "A Secure Signature Scheme with Tight Reduction to the RSA Assumption from Indistinguishability Obfuscation, The 2015 Symposium on Cryptography and Information Security (SCIS2015), IEICE, Jan. 2015

13. T. Kyogoku, M. Lee, M. Abe, T. Okamoto, "Threshold Two-Move Password Authenticated Key Exchange Protocol, The 2015 Symposium on Cryptography and Information Security (SCIS2015), IEICE, Jan. 2015

14. Y. Mimasu, M. Abe, T. Okamoto, "Non-Interactive First-Price and Second-Price Auction Protocols Using Fully Homomorphic Encryption, The 2014 Symposium on Cryptography and Information Security (SCIS2014), IEICE, Jan. 2014

15. R. Hiromasa, M. Abe, T. Okamoto, "Multilinear Maps on LWE, The 2014 Symposium on Cryptography and Information Security (SCIS2014), IEICE, Jan. 2014

16. T. Tango, M. Abe, T. Okamoto, "Implementating Conversion Algorithm from Type-I to Type-III Pairing Groups, The 2014 Symposium on Cryptography and Information Security (SCIS2014), IEICE, Jan. 2014 (in Japanese)

17. M. Abe, M. Ohkubo, T. Mehdi, Impossibility of Symmetric Structure-Preserving Signatures with Single Verification Equation, The 2013 Symposium on Cryptography and Information Security (SCIS2013), IEICE, Jan. 2013

18. Naoyoshi Okamoae, Maki Yoshida, Kenta Kumojima, Masayuki Abe, Miyako Ohkubo, Toru Fujiwara, Automated Attack Derivation for Cryptographic Problems on Bilinear Groups, The 2011 Symposium on Cryptography and Information Security (SCIS2011), Jan. 2011

19. M. Ohkubo, M. Abe, An Efficient Signature for a Message in Group, The 2010 Symposium on Cryptography and Information Security (SCIS2010), IEICE, Jan. 2010

20. M. Ohkubo, M. Abe, Security of Universally Composable Blind Signatures Revisited, The 2009 Symposium on Cryptography and Information Security (SCIS2009), IEICE, Jan. 2009

21. M. Ohkubo, M. Abe, Similarity between Anonymity in ring Signatures and Security in Public-key Encryption, The 2007 Symposium on Cryptography and Information Security (SCIS2007), IEICE, Jan. 2007

22. M. Ohkubo, M. Abe, Security of Three-Move Blind Signature Schemes Reconsidered, The 2003 Symposium on Cryptography and Information Security (SCIS2003), 13C-4, IEICE, Jan. 2003

23. M. Ohkubo, M. Abe, K. Suzuki, S. Tsujii, Short 1-out-of-n Proofs, The 2002 Symposium on Cryptography and Information Security (SCIS2002), 4C-4, IEICE, Jan. 2002

24. M. Ohkubo and M. Abe, On public-key encryption with signature in non-separable model, The 2001 Symposium on Cryptography and Information Security, IEICE, Jan. 2001.

25. A. Fujioka, M. Abe, M. Ohkubo and F. Hoshino, "An Implementation and an Experiment of a Practical and Secure Voting Scheme", 2000 Symposium on Cyptography and Information Security (SCIS '2000), B23, 2000, (in Japanese).

26. F. Hoshino and M. Abe, "More efficient Mix-network on Permutation Networks", 2000 Symposium on Cyptography and Information Security (SCIS '2000), B23, 2000, (in Japanese).

27. M. Abe, M. Ohkubo, A. Fujioka and F. Hoshino, "An Electronic Voting Scheme with Revocable Threshold Blind Signatures", Symposium on Cyptography and Information Security (SCIS '2000), B25, 2000.

28. M. Abe, "Robust Threshold Cramer-Shoup Cryptosystem", 1999 Symposium on Cyptography and Information Security (SCIS '99), T1-1.3, 1999, (in Japanese).

29. M. Abe, M. Kanda, "A Key Escrow Scheme for Real-Time Monitoring", Symposium on Cyptography and Information Security (SCIS '98), 5.2.D, 1998.

30. M. Abe and J. Camenisch, "Partially blind signatures", In the 1997 Symposium on Cryptography and Information Security (SCIS '97), SCIS97-33D, 1997.

31. M. Abe and H. Morita, An implementation of public key LSI, The 1995 Symposium on Cryptography and Information Security, IEICE, Jan. 1995.

32. M. Abe, An LSI implementation technics for public-key schemes, In proceedings of the 1994 IEICE fall conference, A-194. IEICE, Sept. 1994.

33. M. Abe and H. Morita, Key distribution by software, In proceedings of the 1993 IEICE fall conference, A-202. IEICE, Sept. 1993.

34. S. Hangai, M. Abe, K. Miyauchi, "On Selecting Parameters for Speaker Recognition", ISIT, pp.213-216 (1991).

Books, Book Chapters

1. M. Abe, "Advances in Cryptology - ASIACRYPT 2010", LNCS 6477, ISBN 978-3-642-17372-1, Springer-Verlag, 2010.

2. M. Abe, "Topics in Cryptology - CT-RSA 2007, The Cryptographer's Track at the RSA Conference 2007", Springer-Verlag, 2007.

3. M. Abe, V. Gligor, "Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security, ASIACCS 2008", ACM.

4. IEICE, "Information Security Handbook (Sec.3.2 Foundations of Cryptographic Protocols, in Japanese)", Kyoritu Shuppan, 2003

5. M. Sipser, "Introduction to the Theory of Computation" (Translation to Japanese), April, 2000.