略歴・業績一覧

2019/06/1

氏名

阿部 正幸

生年月日

1967(S.42).6.21 (51 歳)

現職

NTT 情報流通プラットフォーム研究所
暗号理論研究室 上席特別研究員 暗号室長

略歴

1990(H.02).3	東京理科大学工学部電気工学科卒業
1992(H.04).3	同大学院電気工学専攻科修士課程修了 NTT 情報通信網研究所勤務
1996.9-1997.8	スイス連邦工科大学チューリッヒ校(ETH Zurich) 客員研究員
1999(H.11).1	NTT 情報流通プラットフォーム研究所勤務
2001(H.13).10	同研究所 主任研究員
2003(H.13).4	同研究所 特別研究員
2004(H.16).4	IBM T. J. Watson Research Center 勤務
2004(H.16).10	NTT 情報流通プラットフォーム研究所 主幹研究員
2012(H.24).4	NTT セキュアプラットフォーム研究所 主幹研究員・特別研究員
2013(H.25).4	同研究所 セキュリティ基盤研究グループ グループリーダー(2016.6 迄)
2013(H.25).4	同研究所 主幹研究員・上席特別研究員（2019.3 迄）
2017(H.30).4	同研究所 暗号理論研究室 暗号室長（現職）
2019(H.31).4	同研究所 上席特別研究員（現職）

学位

2002 (H14)年 12 月 13 日　博士（工学）　東京大学　第 15508 号
“Efficient Components for Cryptographic Applications in the Discrete-Log Setting”

業務経験

’92～’94暗号認証 LSI 設計開発．主にべき乗剰余演算部の論理設計を担当
’94～’95暗号認証用 C ライブラリ開発．内部仕様，インタフェース仕様の決定，アルゴリズムの選定，コーディングを担当
’95～’96電子現金プロトコル開発．プロトコル設計，コーディングを担当
’97～’01電子投票プロトコル開発．プロトコル設計，コーディングを担当
’01～’02ISO 標準化国内委員

研究略歴

’92～’94	高速べき乗演算アルゴリズムの研究
’95～’96	電子現金方式の研究
’95～’01	ブラインド署名の研究
’97～’98	鍵供託方式の研究
’96～’06	効率的な一般的マルチパーティープロトコルの研究
’97～’01	電子投票プロトコルの研究
’98～’01	匿名通信路の研究
’99～	高機能署名安全性の研究
’99～	暗号安全性の研究

’09～　群構造維持暗号系の研究
’18～　非対話ゼロ知識証明の研究

所属学会等

1992(H.04).4　電子通信学会（至現在）
1994(H.06).11　International Association for Cryptographic Research (IACR) (至現在)

委員の委嘱等

1999(H.11).5　拓殖大学電子工学科　客員講師
2002(H.14).9　東海大学 開発工学部 情報通信工学科　非常勤講師
2003(H.15).5　電気通信大学 情報通信工学科 非常勤講師
2004(H.16).4　Queensland University of Technology (Australia) 学位論文評価委員(指導教官: Colin Boid 教授)
2007(H.19).9　International Journal of Applied Cryptography 編集委員（至現在)
2009(H.21).4　東京大学新領域創成科学研究科複雑理工学専攻 非常勤講師
2011(H.23). 3　New York University (USA) 学位論文審査委員 Kristiyan Halarambiev 氏 (指導教官: Victor Shoup 教授)
2012(H.24).9-12　電気通信大学 情報通信工学科 非常勤講師
2013(H.25).4 ~　京都大学大学院情報学研究科 社会情報学専攻 客員准教授（至 2018.3）
2013(H.25).11　東京大学新領域創成科学研究科複雑理工学専攻 山田翔太氏 博士論文審査員
2014(H.26).1 ~　IACR（国際暗号学会）School Committee（至 2017.12）
2015(H.27).1 ~　IACR（国際暗号学会）理事（至現在)
2017(H.29).10　首都大学東京 非常勤講師
2018(H.30).4　京都大学大学院情報学研究科 社会情報学専攻 客員教授（現職）

国際会議の委員等　※年次は会議開催年

2001(H.13)　Asiacrypt 2001
2003(H.15)　PKC’03, ACISP’03, ISC’03, Asiacrypt2003
2004(H.16)　PKC’04, FC’04, ACNS’04
2005(H.17)　CT-RSA’05, Crypto’05
2006(H.18)　PKC’06, WWW’06, VietCrypt
2007(H.19)　Asiacrypt’07
2008(H.20)　PKC’08, CT-RSA’08, ACNS’08, ACISP’08, Asiacrypt’08
2009(H.21)　ASIACCS’09, Crypto’09, SAC’09, Asiacrypt’09
2010(H.22)　ACISP'10
2011(H.23)　PKC’11, Crypto’11, Asiacrypt’11
2012(H.24)　TCC’12, SCN’12
2013(H.25)　TCC’13, CT-RSA’13, Crypto’13
2014(H.26)　PKC’14, Eurocrypt’14, ESORICS 2014, SCN 2014, Asiacrypt'14
2015(H.27)　Eurocrypt'15, Crypto'15
2016(H.28)　TCC'16A, FC'16, TCC'16B
2017(H.29)　PKC'17, Crypto'17
2018(H.30)　TCC’18, ACISP’18, ACNS’18

2019(H.31)　CANS'19, CT-RSA'20

国際会議のプログラム委員長・運営委員長等

2007(H.19)　CT-RSA'07 (Program Chair)
2008(H.20)　AsiaCCS'08 (Program Co-Chair)
2010(H.22)　Asiacrypt'10 (Program Chair)
2013(H.25)　TCC'13 (General Co-Chair)

招待講演(国内・国際会議・ワークショップ等)

2001(H.13).1.15　ICU, Korea, The Seminar series at the Information and Communications University, "Cryptographic Solution for Electronic Voting", "Development of Electronic Voting Systems in NTT"
2001(H.13).9.18　電気通信学会関西支部セミナー　"EC の動向"
2003(H.15).3.8　第 3 回 JST 領域探索研究会, "Multi-Party Protocols and Zero-Knowledge Proofs"
2006(H.18).2.28　産業技術総合研究所, 公開鍵暗号の安全な構成とその応用ワークショップ, "Tag-KEM/DEM: A New Framework for Hybrid Encryption"
2007(H.19).12.11　東京工業大学 21 世紀 Global COE プログラム ワークショップ, "Compact CCA-secure Encryption"
2007(H.19).12.13 情報処理推進機構(IPA) Cryptography Workshop 2007 Autumn, "Compact CCA-secure Encryption for Arbitrary Messages"
2008(H.20).12.3　International Conference on Information Security and Cryptography 2008 (ICISC'08, Seoul, Korea), "Provable Security in Public-key Encryption Schemes"
2011(H.23).5.31　International Workshop on Coding and Cryptology, Qingdao, China, "Signature Scheme with Efficient Proof of Validity"
2012(H.24).2.23　5th Workshop on Secure Construction of Public-Key Cryptosystems and its Applications, Akihabara, Japan, "Structure-Preserving Cryptography Part-II: Structure Preserving Commitments"
2012(H.24).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(H.25).6.27　4th Jinbo-cho Cryptography Workshop, Study on PKC2013, "Tagged One-Time Signatures: Tight Security and Optimal Tag Size"
2014(H.26).12.25　Kyoto University Media Center, "Bit Commitment and Zero-Knowledge Proof System"
2014(H.26).3.20　7th Public-Key Workshop, "On the Impossibility of Structure-Preserving Deterministic Primitives"
2015(H27).2.20　8th Public-Key Workshop, "Structure-Preserving Signatures from Type II Pairings"
2015(H.27).9.4　ISEC Workshop, "Fully Structure-Preserving Signatures and Shrinking Commitments"
2015(H.27).11.3　Asiacrypt 2015, "Structure-Preserving Cryptography"
2017(H.29).7.7　JAIST, "Practical Impact of Tight Security Reductions"
2018(H.30).1.16　Workshop on Cryptography, NTT-JFLI-U.Tokyo, "On the Practical Impact of Tight Security"
2019(H.31).3.1　Public-Key Workshop, Improved (Almost) Tightly-Secure Simulation-Sound QA-NIZK with Applications

セミナー等講演

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), JAIST (Japan, 2017), Kyoto University (Japan, 2018)

表彰

1999(H.11)	SCIS 論文賞：“Robust Threshold Cramer-Shoup Cryptosystem", 1999 Symposium on Cryptography and Information Security (SCIS '99), T1-1.3, 1999
2008(H.20)	“Recognition of Service Award” (for the PC Co-Chair of ASIACCS’08) from Association for Computing Machinery
2016(H.28).4	第 48 回 市村学術賞 功績賞 「相互接続を実現する群構造維持暗号系に関する先駆的研究」
2016(H.28).6.2	電子情報通信学会 第 53 回（平成 27 年度）業績賞 「暗号プロトコル・要素技術に関する先導的研究」
2018(H.30).4.24	SCIS イノベーション論文賞 “Pseudo-Code Performance Estimation for Pairing-Based Cryptographic Schemes”
2019(H.31).4.10	第 64 回 前島密賞「安全かつ利便性の高い電子署名および暗号プロトコルの先導的研究」

著作

論文誌

1. M. Abe, “Non-Interactive and Optimally Resilient Distributed Multiplication", IEICE Trans. Fundamentals, Vol. E83-A, No. 4, pp.598-605, April, 2000
2. M. 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
3. M. Abe and T. 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
4. M. Ohkubo and M. Abe, “A Length-Invariant Hybrid Mix", IEICE Trans. Fundamentals, Vol. E84-A, No. 4, pp.931-940, April, 2001
5. M. Abe and T. Okamoto, “Delegation Chains Secure up to Constant Length", IEICE Trans. Fundamentals, Vol. E85-A, No. 1, pp.110-116, January, 2002
6. 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, British Computer Society, 2002
7. F. Hoshino, M. Abe and T. Kobayashi, “Lenient/Strict Batch Verification in Several Groups", IEICE Trans. Fundamentals, Vol. E86-A, No. 1, pp.64-72, January 2003
8. M. Abe and K. Suzuki, “M+1-st Auction Using Homomorphic Encryption", IEICE Trans. Fundamentals, Vol. E86-A, No. 1, pp.136-141, January 2003
9. M. 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
10. M. Abe, M. Ohkubo and K. Suzuki, “1-out-of-n Signatures from a Variety of Keys", IEICE Trans. Fundamentals, Vol. E87-A, No. 1, pp.131-140, January 2004
11. M. Abe, M. Ohkubo and K. Suzuki, “Efficient Threshold Signer-Ambiguous Signatures from Variety of Keys" IEICE Trans. Fundamentals, Vol. E87-A, No. 2, pp.471-479, February 2004
12. K. Chida and M. Abe, “Flexible-Routing Anonymous Networks Using Optimal Length of Ciphertext", IEICE Trans. Fundamentals, Vol. E88-A, No. 1, pp.211-221, January 2005
13. M. Abe, H. Imai, “Flaws in Robust Optimistic Mix-Nets and Stronger Security Notions" IEICE Trans. Fundamentals, Vol. E89-A, No. 1, pp.99-105, January 2006
14. M. Abe, R. Gennaro, K. Kurosawa, “Tag-KEM/DEM: A New Framework for Hybrid Encryption" Journal of Cryptology, Vol. 21(1), pp.97-130, January 2008.
15. M. Ohkubo and M. Abe, “On the Definitions of Anonymity for Ring Signatures", IEICE

Trans. Fundamentals, Vol. E91-A(1), pp.272-282, January 2008.
16. M. Abe, Y. Cui, H. Imai, K. Kurosawa, “Tag-KEM from Set Partial Domain One-Way Permutations", IEICE Trans. Fundamentals, Vol.E92-A(1), pp.42-52, January 2009.
17. M. Abe, Y. Cui, H. Imai, E. Kiltz, “Efficient Hybrid Encryption from ID-Based Encryption", Designs, Codes and Cryptography, Vol.54, No.3, pp.205-240, 2010
18. M. Abe, E. Kiltz, T. Okamoto, “Chosen Ciphertext Security with Optimal Ciphertext Overhead", IEICE Trans. Fundamentals, Vol.E93-A(1), pp.22-33, 2010.
19. M. Abe, M. Ohkubo, “A Framework for Universally Composable Non-Committing Blind Signatures", International Journal of Applied Cryptography, Vol.2 No.3, pp.229-249, 2012, http://dx.doi.org/10.1504/IJACT.2012.045581
20. M. Abe, T. Okamoto, K. Suzuki, “Message Recovery Signature Schemes from Sigma-Protocols", IEICE Trans. Fundamentals, Vol. E96-A, No.1, 2013
21. M. Abe, S.M. Chow, K. Haralambiev, M. Ohkubo, “Double-Trapdoor Anonymous Tags for Traceable Signatures”, International Journal of Information Security, 2013, DOI 10.1007/s10207-012-0184-3
22. Ryo Hiromasa, Masayuki Abe, Tatsuaki Okamoto, “Packing Messages and Optimizing Bootstrapping in GSW-FHE,” IEICE Transactions 99-A(1): 73-82 (2016)
23. 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)
24. 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)
25. Masayuki Abe, “Variations of Even-Goldreich-Micali Framework for Signature Schemes,” IEICE Transactions 100-A(1): 12-17 (2017)
26. 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)
27. Masayuki Abe, Jan Camenisch, Rafael Dowsley, Maria Dubovitskaya, “On the Impossibility of Structure-Preserving Deterministic Primitives,” J. Cryptology 32(1): 239-264 (2019)
28. 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)
29. Masayuki Abe, Fumitaka Hoshino, Miyako Ohkubo, “Opcount: A Pseudo-Code Performance Estimation System for Pairing-Based Cryptography”, IEICE Transactions (to appear)

査読付き国際会議

1. 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.
2. 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.
3. 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.
4. 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.
5. M. Abe, “Robust Distributed Multiplication without Interaction", In M. Wiener editor, Advances in Cryptology CRYPTO '99, Volume 1666 of Lecture Notes in Computer Science,

pages 130-147, Springer-Verlag, 1999.
6. M. Ohkubo, F. Miura, M. Abe, A. Fujioka and T. Okamoto, “An Improvement 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.
7. M. Abe and T. Okamoto, “Delegation Chains Secure up to Constant Length", In V. Varadhara-jan and Y. Mu editors, Information and Communication Security (ICICS'99), Volume 1726 of Lecture Notes in Computer Science, pages 144-156. Springer-Verlag, 1999.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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, pages178-191, Springer-Verlag, 2000.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. M. Abe, R. Cramer, and S. Fehr, “Non-Interactive Distributed Verifier Proofs and Proving Relations among Commitments", In Y. Zheng editor, Advances in Cryptology ASI-ACRYPT 2002, Volume 2501 of Lecture Notes in Computer Science, pages 206-223, Springer-Verlag, 2002.
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.
26. 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.
27. 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.
28. 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.
29. M. Abe, E. Kiltz, and T. Okamoto, “Compact CCA-Secure 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.
30. M. Abe, M. Ohkubo, “A Framework for Universally Composable Non-Committing Blind Signatures", In the proceedings of ASIACRYPT 2009, LNCS, Springer-Verlag, 2009
31. 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.
32. 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.
33. 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.
34. 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.
35. 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.
36. 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.
37. 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.
38. 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, Springer-Verlag, 2013

39. M. Abe, Jan Camenisch, Maria Dubovitskaya, Ryo Nishimaki, “Universally Composable Adaptive Oblivious Transfer with Access Control from Standard Assumptions”, In the Proceedings of ACM Digital Identity Management Workshop (ACM DIM) 2013.
40. 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
41. 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
42. 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
43. 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
44. 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.
45. 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.
46. 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.
47. 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.
48. 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.
49. Masayuki Abe, Miguel Ambrona, Miyako Ohkubo, Mehdi Tibouchi: Lower Bounds on Structure-Preserving Signatures for Bilateral Messages. SCN 2018: 3-22
50. Masayuki Abe, Charanjit S. Jutla, Miyako Ohkubo, Arnab Roy: Improved (Almost) Tightly-Secure Simulation-Sound QA-NIZK with Applications. ASIACRYPT (1) 2018: 627-656

技術報告

1. 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.
2. 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
3. K. Ohta, M. Abe, E. Fujisaki and H. Moribatake, “Electronic Money Schemes", NTT R&D, pp.931-938, Vol.44 October, 1995
4. H. Moribatake, M. Abe, A. Fujioka and J. Gohara, “Electronic Cash Scheme", NTT Review, vol.9 No.3 May, 1997
5. M. Abe, “Mix-network on Permutation Networks", Technical report of IEICE, ISEC99-10, May, 1999
6. M. Abe, “On Proxy Signatures and Batch Verification", Technical report of IEICE, ISEC-2, May, 2000
7. M. Ookubo and M. Abe, “A Robust Length-Invariant Hybrid Mix", Technical report of IEICE, ISEC-1, May, 2000

8. M. Abe, K. Suzuki, A. Fujioka and M. Ohkubo, F. Hoshino, ”Electronic Voting Schemes", NTT R&D, Vol. 49, pp.685-693, November, 2000
9. M. Abe, T. Okamoto, K. Suzuki, “Message Recovery Signature Schemes from Sigma-Protocols", NTT Technical Review, Vol.6(1), January 2008.
10. 雲島健太、吉田真紀、阿部正幸、大久保美也子、藤原融、 “Generic Model における困難性仮定への攻撃の数式処理を用いた導出”, Technical Report of IEICE, ISEC 2010-58, Nov. 2010
11. 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)

シンポジウム・他

1. S. Hangai, M. Abe, K. Miyauchi, “On Selecting Parameters for Speaker Recognition", ISITA, pp.213-216 (1991)
2. M. Abe and H. Morita, Key distribution by software, In proceedings of the 1993 IEICE fall conference, A-202. IEICE, Sept. 1993.
3. M. Abe, An LSI implementation technics for public-key schemes, In proceedings of the 1994 IEICE fall conference, A-194. IEICE, Sept. 1994.
4. M. Abe and H. Morita, An implementation of public key LSI, The 1995 Symposium on Cryptography and Information Security, (SCIS '95), Jan. 1995.
5. M. Abe and J. Camenisch, “Partially blind signatures", In the 1997 Symposium on Cryptography and Information Security (SCIS '97), SCIS97-33D, 1997.
6. M. Abe, M. Kanda, “A Key Escrow Scheme for Real-Time Monitoring", Symposium on Cryptography and Information Security (SCIS '98), 5.2.D, 1998
7. M. Abe, “Robust Threshold Cramer-Shoup Cryptosystem", 1999 Symposium on Cryptography and Information Security (SCIS '99), T1-1.3, 1999, (in Japanese)
8. M. Abe, M. Ohkubo, A. Fujioka and F. Hoshino, “An Electronic Voting Scheme with Revocable Threshold Blind Signatures", Symposium on Cryptography and Information Security (SCIS '2000), B25, 2000
9. F. Hoshino and M. Abe, “More efficient Mix-network on Permutation Networks", 2000 Symposium on Cryptography and Information Security (SCIS '2000), B23, 2000, (in Japanese)
10. A. Fujioka, M. Abe, M. Ohkubo and F. Hoshino, “An Implementation and an Experiment of a Practical and Secure Voting Scheme", 2000 Symposium on Cryptography and Information Security (SCIS '2000), B23, 2000, (in Japanese)
11. M. Ohkubo and M. Abe, “On Public-Key Encryption with Signature in Non-Separable Model”, The 2001 Symposium on Cryptography and Information Security (SCIS 2001), B5, Jan. 2001.
12. 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
13. 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
14. 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
15. M. Ohkubo, M. Abe, “Security of Universally Composable Blind Signatures Revisited”, The 2009 Symposium on Cryptography and Information Security (SCIS2009), IEICE, Jan. 2009
16. M. Ohkubo, M. Abe, “An Efficient Signature for a Message in Group”, The 2010 Symposium on Cryptography and Information Security (SCIS2010), IEICE, Jan. 2010
17. 岡前直由、吉田真紀、雲嶋健太、阿部正幸、大久保美也子、藤原融、 “Bilienar Group に関する困難性仮定への攻撃導出”、 2011 年暗号と情報セキュリティシンポジウム (SCIS2011), Jan. 2011
18. 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
19. 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
20. R. Hiromasa, M. Abe, T. Okamoto, "Multilinear Maps on LWE, The 2014 Symposium on Cryptography and Information Security (SCIS2014), IEICE, Jan. 2014
21. 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
22. 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
23. 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
24. 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)
25. J. Kume, M. Abe, T. Okamoto, "Lottery Protocol for Cryptocurrency, The 2015 Symposium on Cryptography and Information Security (SCIS2015), IEICE, Jan. 2015
26. R. Hiromasa, M. Abe, T. Okamoto, "SIMD Operations in GSW-FHE, The 2015 Symposium on Cryptography and Information Security (SCIS2015), IEICE, Jan. 2015
27. T. Kyogoku, M. Abe, T. Okamoto, "A Note on Authenticated Key Exchange in Cryptocurency, The 2016 Symposium on Cryptography and Information Security (SCIS2016), IEICE, Jan. 2016
28. 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
29. 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)
30. 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)
31. 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
32. 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
33. 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
34. 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

書籍

1. M.Sipser 著, 渡辺治, 大田和夫監訳, 阿部正幸, 植田広樹, 田中圭介, 藤岡淳 共訳, "計算理論の基礎", 共立出版. April, 2000
2. 土居範久 監修, "情報セキュリティ辞典", ISBN-978-4320120709, 共立出版, 2003
3. M. Abe, V. Gligor, "Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security, ASIACCS 2008", ACM
4. M. Abe, "Topics in Cryptology - CT-RSA 2007, The Cryptographer's Track at the RSA Conference 2007", Springer-Verlag, 2007.
5. M. Abe, "Advances in Cryptology - ASIACRYPT 2010", LNCS 6477, ISBN 978-3-642-17372-1, Springer-Verlag, 2010.