渡邉 洋平 (Watanabe, Yohei)

Curriculum Vitae

電気通信大学 大学院情報理工学研究科
情報学専攻 岩本・渡邉研究室
〒 182-8585 東京都調布市調布ヶ丘 1-5-1

Tel: 042-443-5822
E-mail: watanabe@uec.ac.jp
最終更新日: 2022 年 8 月 5 日

研究分野

現代暗号理論．特に，

- ▷ 検索可能暗号技術.
- ▷ 情報理論的暗号技術.
- ▷ 公開鍵暗号，特に，ペアリング暗号.
- ▷ 更新可能暗号技術.

略歴

2007 年 3 月 新潟県立新発田高等学校 卒業

2007 年 4 月 – 2011 年 3 月 横浜国立大学 工学部 電子情報工学科

2011 年 4 月 – 2013 年 3 月 横浜国立大学 大学院環境情報学府 情報メディア環境学専攻 博士課程前期

2013 年 4 月 – 2016 年 3 月 横浜国立大学 大学院環境情報学府 情報メディア環境学専攻 博士課程後期

2013 年 4 月 – 2016 年 3 月 日本学術振興会特別研究員 (DC1).
受入研究者: 四方 順司 准教授 (横浜国立大学)

2014 年 5 月 – 2015 年 3 月 独立行政法人 産業技術総合研究所 セキュアシステム研究部門 技術研修生.

2015 年 4 月 – 2016 年 3 月 国立研究開発法人 産業技術総合研究所 情報技術研究部門 技術研修生.

2016 年 4 月 – 2018 年 9 月 日本学術振興会特別研究員 (PD).
受入研究者: 岩本 貢 准教授 (電気通信大学)

2016 年 4 月 – 2018 年 9 月 電気通信大学 大学院情報理工学研究科 特別研究員.

2016 年 4 月 – 2018 年 9 月 国立研究開発法人 産業技術総合研究所 情報技術研究部門 協力研究員.

2018 年 10 月 – 2019 年 11 月 国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所
セキュリティ基盤研究室 研究員.

2019 年 12 月 – 現在 **電気通信大学 大学院情報理工学研究科 情報学専攻 助教**.

2019 年 12 月 – 現在 文部科学省 卓越研究員事業 卓越研究員.

2020 年 4 月 – 現在 国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所
セキュリティ基盤研究室 招へい専門員.

2020 年 4 月 – 現在 国立研究開発法人 産業技術総合研究所
サイバーフィジカルセキュリティ研究センター 外来研究員.

2020 年 8 月 – 現在 ジャパンデータコム株式会社 特別研究員.

学位

- ▷ **学士 (工学)**, 横浜国立大学. 2011 年 3 月
- ▷ **修士 (工学)**, 横浜国立大学. 2013 年 3 月
- ▷ **博士 (情報学)**, 横浜国立大学.
  学位論文: Cryptography with Timed Access Control
  指導教員: 四方 順司 准教授 2016 年 3 月

受賞歴等

- ▷ CSS2020 奨励賞, [74] に対して, 2020.
- ▷ CSS2019 奨励賞, [76] に対して, 2019.
- ▷ IEEE Information Theory Society Japan Chapter Young Researcher Best Paper Award, [32] に対して, 2018.
- ▷ CSS2018 優秀論文賞, [81] に対して, 2018.
- ▷ 4th Heidelberg Laureate Forum 招待, 2016.
- ▷ 2015 年度横浜国立大学大学院環境情報学府学生表彰, 2016.
- ▷ SCIS 論文賞, [105] に対して, 2016.
- ▷ CSS2014 学生論文賞, [109] に対して, 2014.
- ▷ IWSEC 2014 Best Poster Award, [124] に対して, 2014.
- ▷ 日本学術振興会特別研究員制度 (PD), 2016 – 2019.
- ▷ 日本学術振興会特別研究員制度 (DC1), 2013 – 2016.
- ▷ 2012 年度横浜国立大学大学院環境情報学府学生表彰, 2013.

講義

学内担当科目

- ▷ 2022 年度後期: 暗号理論, 暗号理論特論, 暗号情報セキュリティ, セキュリティ情報学実験.
- ▷ 2021 年度後期: 暗号理論, 暗号理論特論, 暗号情報セキュリティ, セキュリティ情報学実験.
- ▷ 2020 年度後期: 暗号理論, 暗号情報セキュリティ, セキュリティ情報学実験.
- ▷ 2019 年度後期: 暗号理論.

学外担当科目

- ▷ 2022 年度: 基礎情報処理 5 (前期; 日本女子大学), 基礎情報処理 2 4 (後期; 日本女子大学).
- ▷ 2021 年度: 基礎情報処理 5 (前期; 日本女子大学), 基礎情報処理 2 4 (後期; 日本女子大学).
- ▷ 2020 年度: 基礎情報処理 C (前期; 日本女子大学), 基礎情報処理 Q (後期; 日本女子大学).
- ▷ 2019 年度: 基礎情報処理 C (前期; 日本女子大学), プロジェクトラーニング (前期; 横浜国立大学), 基礎情報処理 Q (後期; 日本女子大学).
- ▷ 2018 年度: 基礎情報処理 Q (後期; 日本女子大学).

委員活動

- ▷ **編集委員:** IEICE 和文論文誌 A 編集幹事 (2022 – 現在), IEICE 英文論文誌 A Guest Editor (2020 SITA 特集号).
- ▷ **プログラム委員:** APKC 2022, ITW 2021, IWSEC 2021, APKC 2021, IWSEC 2020, APKC 2020, IWSEC 2019, APKC 2019, APKC 2018 (co-Chair).
- ▷ **実行委員:** SCIS 2023, PKC 2022 (co-Chair), IWSEC 2022, CSS 2021, IWSEC 2021, SCIS 2021, CSS 2019, IWSEC 2019, IWSEC 2018.

競争的研究資金

- ▷ 日本学術振興会 科研費 基盤研究 (B), "広範な検索機能と高い効率性を両立する秘匿検索技術の実現 (課題番号 21H03341)," 研究代表者. 2021 年 4 月 – 2025 年 3 月 (予定).
- ▷ 日本学術振興会 科研費 基盤研究 (B), "十分統計量に基づくシミュレーションベース安全性の深化 (課題番号 21H03395)," 研究分担者 (研究代表者: 岩本貢). 2021 年 4 月 – 2025 年 3 月 (予定).
- ▷ 日本学術振興会 科研費 基盤研究 (S), "暗号技術による IoT エコシステムのレジリエンス向上 (課題番号 18H05289)," 研究分担者 (研究代表者: 崎山一男). 2018 年 6 月 – 2023 年 3 月 (予定, 2020 年 4 月参画).
- ▷ 日本学術振興会 科研費 基盤研究 (C), "長期間運用に耐えうる共通鍵暗号による秘匿検索暗号 (課題番号 18K11293)," 研究分担者 (研究代表者: 太田和夫). 2018 年 4 月 – 2022 年 3 月 (2020 年 4 月参画, 2023 年 3 月まで延長).
- ▷ 文部科学省 科学技術人材育成費補助金（卓越研究員事業), 研究代表者. 2019 年 12 月 – 2021 年 3 月.
- ▷ 日本学術振興会 科研費 若手研究 (B), "鍵漏洩に耐性のある ID ベース暗号の高安全かつ高効率な実現 (課題番号 17K12697)," 研究代表者. 2017 年 4 月 – 2021 年 3 月.
- ▷ 日本学術振興会 科研費 基盤研究 (B), "推測秘匿性に基づく情報理論的暗号理論の新展開 (課題番号 17H01752)," 研究分担者 (研究代表者: 岩本貢). 2017 年 4 月 – 2021 年 3 月 (2022 年 3 月まで延長).
- ▷ 日本学術振興会 科研費 特別研究員奨励費, "秘匿情報に対して動的アクセス制御とデータ解析を両立させる暗号理論の確立 (課題番号 16J10532)," 研究代表者. 2016 年 4 月 – 2019 年 3 月.
- ▷ 日本学術振興会 科研費 特別研究員奨励費, "時刻で制御可能な暗号基礎技術の研究開発 (課題番号 13J03998)," 研究代表者. 2013 年 4 月 – 2016 年 3 月.

著書等出版物

[1] G. Hanaoka, J. Shikata, and Y. Watanabe, *Public-Key Cryptography – PKC 2022*, Part I, Virtual Event, March 8-11, 2022. LNCS 13177, Springer, 2022.

[2] G. Hanaoka, J. Shikata, and Y. Watanabe, *Public-Key Cryptography – PKC 2022*, Part II, Virtual Event, March 8-11, 2022. LNCS 13178, Springer, 2022.

[3] K. Emura, J.H. Seo, and Y. Watanabe, *Proceedings of the 5th ACM Asia Public-Key Cryptography Workshop (APKC 2018)*, Incheon, Korea, June 4, 2018. ACM, 2018.

査読付き論文誌論文

[4] Y. Watanabe, T. Seito, and J. Shikata, "Multi-Designated Receiver Authentication Codes: Models and Constructions," IEICE Transactions, vol. E106-A, no. 3, pp. yyy–zzz, IEICE, 2023. (To appear)

[5] Y. Watanabe, T. Nakai, K. Ohara, T. Nojima, Y. Liu, M. Iwamoto, and K. Ohta, "How to Make a Secure Index for Searchable Symmetric Encryption, Revisited," IEICE Transactions, vol. E105-A, no. 12, pp. yyy–zzz, IEICE, 2022. (To appear)

[6] Y. Abe, T. Nakai, Y. Kuroki, S. Suzuki, Y. Koga, Y. Watanabe, M. Iwamoto, and K. Ohta, "Efficient Card-based Majority Voting Protocols," New Generation Computing, vol. 40, pp. 173–198, Springer, 2022.

[7] K. Emura, S. Katsumata, and Y. Watanabe, "Identity-Based Encryption with Security against the KGC: A Formal Model and Its Instantiations," Theoretical Computer Science, vol. 900, pp. 97–119, Elsevier, 2022.

[8] K. Emura, A. Takayasu, and Y. Watanabe, "Efficient Identity-Based Encryption with Hierarchical Key-Insulation from HIBE," Designs, Codes and Cryptography, vol. 89(10), pp. 2397–2431, Springer, 2021.

[9] K. Emura, A. Takayasu, and Y. Watanabe, "Adaptively Secure Revocable Hierarchical IBE from k-linear Assumption," Designs, Codes and Cryptography, vol. 89(7), pp. 1535–1574, Springer, 2021.

[10] K. Emura, J.H. Seo, and Y. Watanabe, "Efficient Revocable Identity-based Encryption with Short Public Parameters," Theoretical Computer Science, vol. 863, pp. 127–155, Elsevier, 2021.

[11] A. Takayasu and Y. Watanabe, "Revocable Identity-based Encryption with Bounded Decryption Key Exposure Resistance: Lattice-based Construction and More," Theoretical Computer Science, vol. 849, pp. 64–98, Elsevier, 2021.

[12] H. Anada, A. Kanaoka, N. Matsuzaki, and Y. Watanabe, "Key-Updatable Public-Key Encryption with Keyword Search (Or: How to Realize PEKS with Efficient Key Updates for IoT Environments)," International Journal of Information Security, vol. 19, pp. 15–38, Springer, 2020.

[13] K. Ohara, Y. Watanabe, M. Iwamoto, and K. Ohta, "Multi-Party Computation for Modular Exponentiation based on Replicated Secret Sharing," IEICE Transactions, vol. 102-A, no.9, pp. 1079–1090, IEICE, 2019.

[14] J. Shikata and Y. Watanabe, "Identity-based Encryption with Hierarchical Key-insulation in the Standard Model," Designs, Codes and Cryptography, vol. 87(5), pp. 1005–1033, Springer, 2019.

[15] A. Prasitsupparote, Y. Watanabe, J. Sakamoto, J. Shikata, and T. Matsumoto,"Implementation and Analysis of Fully Homomorphic Encryption in Resource-Constrained Devices," International Journal of Digital Information and Wireless Communications (IJDIWC), vo.8(4), pp. 288–303, SDIWC Library, 2018.

[16] Y. Watanabe and J. Shikata, "Timed-Release Computational Secret Sharing and Threshold Encryption," Designs, Codes and Cryptography, vol. 86(1), pp. 17–54, Springer, 2018.

[17] Y. Ishida, J. Shikata, and Y. Watanabe, "CCA-secure Revocable Identity-based Encryption Schemes with Decryption Key Exposure Resistance," International Journal of Applied Cryptography (IJACT), vol. 3, no.3, pp. 288–311, Inderscience Publishers, 2017.

[18] Y. Watanabe and J. Shikata, “Information-Theoretically Secure Timed-Release Secret Sharing Schemes,” Journal of Information Processing, vol. 24, no.4, pp. 680–689, IPSJ, 2016.

[19] Y. Watanabe and J. Shikata, “Unconditionally Secure Broadcast Encryption Schemes with Trade-offs between Communication and Storage,” IEICE Transactions, vol. 99-A, no.6, pp. 1097–1106, IEICE, 2016.

査読付き国際会議論文

[20] A. Doi, T. Ono, T. Nakai, K. Shinagawa, Y. Watanabe, K. Nuida, and M. Iwamoto, “Card-based Cryptographic Protocols for Private Set Intersection,” In: ISITA 2022, pp. xxx–yyy, IEEE, 2022. (To appear)

[21] S. Shimizu, T. Nakai, Y. Watanabe, and M. Iwamoto, “An Improvement of Multi-Party Private Set Intersection Based on Oblivious Programmable PRFs,” In: ISITA 2022, pp. xxx–yyy, IEEE, 2022. (To appear)

[22] K. Emura, R. Ito, S. Kanamori, R. Nojima, and Y. Watanabe, “State-free End-to-End Encrypted Storage and Chat Systems based on Searchable Encryption,” In: ICEIS 2022, pp. 106–113, SciTePress Digital Library, 2022.

[23] Y. Watanabe, K. Ohara, M. Iwamoto, and K. Ohta, “Efficient Dynamic Searchable Encryption with Forward Privacy under the Decent Leakage,” In: ACM CODASPY 2022, pp. 312–323, ACM, 2022.

[24] T. Seito, J. Shikata, and Y. Watanabe, “Multi-Designated Receiver Authentication-Codes with Information-Theoretic Security,” In: CISS 2022, pp. 84–89, IEEE, 2022.

[25] H. Kobayashi, Y. Watanabe, and J. Shikata, “Asymptotically Tight Lower Bounds in Anonymous Broadcast Encryption and Authentication,” In: IMACC 2021, LNCS 13129, pp. 105–128, Springer, 2021.

[26] M. Ebina, J. Mita, J. Shikata, and Y. Watanabe, “Efficient Threshold Public Key Encryption from the Computational Bilinear Diffie–Hellman Assumption,” In: APKC 2021, pp. 23–32, ACM Press, 2021.

[27] Y. Watanabe, N. Yanai, and J. Shikata, “Anonymous Broadcast Authentication for Securely Remote-Controlling IoT Devices,” In: AINA 2021, LNNS 226, pp. 679–690, Springer, 2021.

[28] T. Uemura, Y. Watanabe, Y. Li, N. Miura, M. Iwamoto, K. Sakiyama, and K. Ohta, “A Key Recovery Algorithm Using Random Key Leakage from AES Key Schedule,” In: ISITA 2020, pp. 382–386, IEEE, 2020.

[29] J. Ida, J. Shikata, and Y. Watanabe, “On the Power of Interaction in Signcryption,” In: ISITA 2020, pp. 348–352, IEEE, 2020.

[30] K. Emura, S. Katsumata, and Y. Watanabe, “Identity-Based Encryption with Security against the KGC: A Formal Model and Its Instantiation from Lattices,” In: ESORICS 2019, LNCS 11736, pp. 113-133, Springer, 2019.

[31] A. Prasitsupparote, Y. Watanabe, and J. Shikata, “Implementation and Analysis of Fully Homomorphic Encryption in Wearable Devices,” ISDF 2018. pp. 1–14, SDIWC Library, 2018.

[32] Y. Watanabe, Y. Kuroki, S. Suzuki, Y. Koga, M. Iwamoto, and K. Ohta, "Card-Based Majority Voting Protocols with Three Inputs Using Three Cards," In: ISITA 2018, pp. 218–222, IEEE, 2018. **[IEEE Information Society Japan Chapter Young Researcher Best Paper Award]**

[33] H. Anada, A. Kanaoka, N. Matsuzaki, and Y. Watanabe, "Key-updatable Public-key Encryption with Keyword Search: Models and Generic Constructions," In: ACISP 2018, LNCS 10946, pp. 341–359, Springer, 2018.

[34] Y. Watanabe, "Broadcast Encryption with Guessing Secrecy," In: ICITS 2017, LNCS 10681, pp. 39–57, Springer, 2017.

[35] A. Takayasu and Y. Watanabe, "Lattice-based Revocable Identity-based Encryption with Bounded Decryption Key Exposure Resistance," In: ACISP 2017, Part I, LNCS 10342, pp. 184–204, Springer, 2017.

[36] T. Yoshizawa, Y. Watanabe, and J. Shikata, "Unconditionally Secure Searchable Encryption," In: CISS 2017, pp. 1–6, IEEE, 2017.

[37] Y. Watanabe, K. Emura, and J.H. Seo, "New Revocable IBE in Prime-Order Groups: Adaptively Secure, Decryption Key Exposure Resistant, and with Short Public Parameters," In: CT-RSA 2017, LNCS 10159, pp. 432–449, Springer, 2017.

[38] Y. Watanabe, G. Hanaoka, J. Shikata, "Unconditionally Secure Revocable Storage: Tight Bounds, Optimal Construction, and Robustness," In: ICITS 2016, LNCS 10015, pp. 213–237, Springer, 2016.

[39] S. Tomita, Y. Watanabe, and J. Shikata, "Sequential Aggregate Authentication Codes with Information Theoretic Security," In: CISS 2016, pp. 192–197, 2016.

[40] Y. Watanabe and J. Shikata, "Identity-based Hierarchical Key-insulated Encryption without Random Oracles," In: PKC 2016, Part I, LNCS 9614, pp. 255–279, Springer, 2016.

[41] Y. Watanabe and J. Shikata, "Constructions of Unconditionally Secure Broadcast Encryption from Key Predistribution Systems with Trade-offs between Communication and Storage, " In: ProvSec 2015, LNCS 9451, pp. 489–502, 2015.

[42] K. Emura, L. T. Phong, and Y. Watanabe, "Keyword Revocable Searchable Encryption with Trapdoor Exposure Resistance and Re-generateability, " In: IEEE TrustCom 2015, vol. 1, pp. 167–174, IEEE, 2015.

[43] Y. Ishida, Y. Watanabe, and J. Shikata, "Constructions of CCA-secure Revocable Identity-based Encryption," In: ACISP 2015, LNCS 9144, pp. 174–191, Springer, 2015.

[44] Y. Watanabe and J. Shikata, "Timed-Release Secret Sharing Schemes with Information Theoretic Security," In: BalkanCryptSec 2014, LNCS 9024, pp. 219–236, Springer, 2014.

[45] Y. Watanabe and J. Shikata, "Timed-Release Computational Secret Sharing Scheme and Its Applications," In: ProvSec 2014, LNCS 8782, pp. 326–333, Springer, 2014.

[46] S. Hajime, Y. Watanabe, and J. Shikata, "Information-Theoretically Secure Entity Authentication in the Multi-user Setting," In: ICISC 2013, LNCS 8565, pp. 400–417, Springer, 2013.

[47] N. Takei, Y. Watanabe, and J. Shikata, "Unconditionally Secure Blind Authentication Codes in the Manual Channel Model," In: The 3rd International Symposium on Engineering, Energy and Environment (3rd ISEEE), pp. 297–302, 2013.

[48] T. Seito, Y. Watanabe, K. Kinose, and J. Shikata, "Unconditionally Secure Anonymous Group Authentication with an Arbiter," In: The 3rd International Symposium on Engineering, Energy and Environment (3rd ISEEE), pp. 291–296, 2013.

[49] A. Kubai, J. Shikata, and Y. Watanabe, "Information-Theoretically Secure Aggregate Authentication Code: Model, Bounds, and Constructions," In: CD-ARES Workshops, MoCrySEn 2013, LNCS 8128, pp. 16–28, Springer, 2013.

[50] Y. Watanabe, T. Seito and J. Shikata, "Information-Theoretic Timed-Release Security: Key-Agreement, Encryption and Authentication Codes," In: ICITS 2012, LNCS 7412, pp. 167–186, Springer, 2012.

査読付き紀要論文

[51] N. Takei, Y. Watanabe, and J. Shikata, "Information-Theoretically Secure Blind Authentication Codes without Verifier's Secret Keys," Josai Mathematical Monograph 8, pp. 115–133, Graduate School of Sciences, Josai University, 2015.

[52] T. Seito, Y. Watanabe, K. Kinose, and J. Shikata, "Information-Theoretically Secure Anonymous Group Authentication with Arbitration: Formal Definition and Construction," Josai Mathematical Monograph 7, pp. 85–110, Graduate School of Sciences, Josai University, 2014.

国内会議論文（査読無）

[53] 竹内健, 渡邉洋平, 矢内直人, 竹久達也, 四方順司, 中尾康二, "IoT 機器のための遠隔安全制御システム," 電子情報通信学会情報通信システムセキュリティ研究会, ICSS2022-3, 2022-SPT-46(25), pp. 1–6, 2022.

[54] 渡邉洋平, 矢内直人, 四方順司, "IoT ネットワークにおける検証者指定署名方式," 暗号と情報セキュリティシンポジウム 2022 (SCIS 2022) 予稿集, 1E2-1, 2022.

[55] 平野貴人, 川合豊, 小関義博, 渡邉洋平, 岩本貢, 太田和夫, "鍵失効可能な検索可能暗号," 暗号と情報セキュリティシンポジウム 2022 (SCIS 2022) 予稿集, 1E2-5, 2022.

[56] 淺野京一, 岩本貢, 渡邉洋平, "効率的な漏洩耐性鍵隔離暗号," 暗号と情報セキュリティシンポジウム 2022 (SCIS 2022) 予稿集, 1A4-2, 2022.

[57] 安部芳紀, 中井雄士, 渡邉洋平, 岩本貢, 太田和夫, "秘匿置換を用いた効率的な n 入力多数決カードプロトコル," 暗号と情報セキュリティシンポジウム 2022 (SCIS 2022) 予稿集, 1F4-2, 2022.

[58] 岩成慶太, 中井雄士, 渡邉洋平, 栃窪孝也, 岩本貢, "一様で閉じたシャッフルの効率的な実装," 暗号と情報セキュリティシンポジウム 2022 (SCIS 2022) 予稿集, 2F4-3, 2022.

[59] 植村友紀, 渡邉洋平, 李陽, 三浦典之, 岩本貢, 崎山一男, 太田和夫, "プロービング攻撃による漏洩情報を用いた AES 鍵復元アルゴリズムの改良," 暗号と情報セキュリティシンポジウム 2022 (SCIS 2022) 予稿集, 1F2-2, 2022.

[60] 小林大航, 渡邉洋平, 峯松一彦, 四方順司, "匿名放送型暗号及び認証における非漸近的タイトな下界と最適構成法について," 暗号と情報セキュリティシンポジウム 2022 (SCIS 2022) 予稿集, 1A4-3, 2022.

[61] 清水聖也, 中井雄士, 渡邉洋平, 岩本貢, "出力埋め込み可能な紛失擬似ランダム関数に基づく多者間秘匿積集合プロトコルの効率化," 暗号と情報セキュリティシンポジウム 2022 (SCIS 2022) 予稿集, 3E3-6, 2022.

[62] 淺野京一, 岩本貢, 渡邉洋平, “秘密鍵の漏洩耐性を有する鍵隔離暗号,” コンピューターセキュリティシンポジウム 2021 (CSS 2021) 予稿集, 3E4-3, pp. 997–1004, 2021.

[63] 土井アナスタシヤ, 中井雄士, 品川和雅, 渡邉洋平, 岩本貢, “カードを用いた秘匿共通集合プロトコル,” コンピューターセキュリティシンポジウム 2021 (CSS 2021) 予稿集, 1E4-3, pp. 343–348, 2021.

[64] 小林大航, 渡邉洋平, 四方順司, “匿名放送型暗号における下界再考と匿名放送型認証への応用,” コンピューターセキュリティシンポジウム 2021 (CSS 2021) 予稿集, 3E4-2, pp. 989–996, 2021.

[65] 江村恵太, 金森祥子, 野島良, 渡邉洋平, “検索可能暗号を用いた暗号化ストレージ・チャットシステムの実装評価,” 電子情報通信学会情報セキュリティ研究会, ISEC2021-5, pp. 19–24, 2021.

[66] 小林大航, 渡邉洋平, 四方順司, “匿名放送型認証における安全性概念の関係性と認証子サイズの下界について,” 電子情報通信学会情報セキュリティ研究会, ISEC2021-3, pp. 187–194, 2021.

[67] 渡邉洋平, 矢内直人, 四方順司, “IoT ネットワークにおける匿名放送型認証技術,” 暗号と情報セキュリティシンポジウム 2021 (SCIS 2021) 予稿集, 3B3-4, 2021.

[68] 根岸奎人, 渡邉洋平, 岩本貢, “視覚復号型秘密分散法における任意の改ざんを検知する手法,” 暗号と情報セキュリティシンポジウム 2021 (SCIS 2021) 予稿集, 2F1-1, 2021.

[69] 初貝恭祐, 安部芳紀, 中井雄士, 品川和雅, 渡邉洋平, 岩本貢, “時間ドロボー問題に対する健全性誤りのない物理的ゼロ知識証明,” 暗号と情報セキュリティシンポジウム 2021 (SCIS 2021) 予稿集, 2F1-2, 2021.

[70] 植村友紀, 渡邉洋平, 李陽, 三浦典之, 岩本貢, 崎山一男, 太田和夫, “AES 鍵スケジュールからの固定ビット数漏洩を用いた鍵復元アルゴリズムの性能評価,” 暗号と情報セキュリティシンポジウム 2021 (SCIS 2021) 予稿集, 2B3-2, 2021.

[71] 平野貴人, 川合豊, 小関義博, 渡邉洋平, 岩本貢, 太田和夫, “検索可能暗号の鍵更新について,” 暗号と情報セキュリティシンポジウム 2021 (SCIS 2021) 予稿集, 3B2-1, 2021.

[72] 穂鷹珠里, 渡邉洋平, 清藤武暢, 四方順司, “検証機能権限の制御が可能な放送型認証の構成,” 暗号と情報セキュリティシンポジウム 2021 (SCIS 2021) 予稿集, 3B3-5, 2021.

[73] 清水聖也, 安部芳紀, 中井雄士, 品川和雅, 渡邉洋平, 岩本貢, “紛失通信ベース三者間秘匿積集合プロトコルにおけるラウンド数の削減,” 暗号と情報セキュリティシンポジウム 2021 (SCIS 2021) 予稿集, 4B1-4, 2021.

[74] 渡邉洋平, 大原一真, 岩本貢, 太田和夫, “より少ない漏洩の下で安全な動的検索可能暗号への変換手法,” コンピューターセキュリティシンポジウム 2020 (CSS 2020) 予稿集, 1D4-2, pp. 297–304, 2020. **[CSS2020 奨励賞]**

[75] 渡邉洋平 “フォワード安全かつ検索時通信量が最適な動的検索可能暗号,” 暗号と情報セキュリティシンポジウム 2020 (SCIS 2020) 予稿集, 3B3-2, 2020.

[76] 渡邉洋平, 大原一真, 岩本貢, 太田和夫, “(強) フォワード安全な動的検索可能暗号の効率的な構成,” コンピューターセキュリティシンポジウム 2019 (CSS 2019) 予稿集, 3D2-2, pp. 1203–1210, 2019. **[CSS2019 奨励賞]**

[77] 渡邉洋平, 岩本貢, 太田和夫, “効率的でフォワード安全な動的検索可能暗号,” 暗号と情報セキュリティシンポジウム 2019 (SCIS 2019) 予稿集, 3C1-3, 2019.

[78] 江村恵太, 勝又秀一, 渡邉洋平 “鍵生成センタに対して安全な ID ベース暗号,” 暗号と情報セキュリティシンポジウム 2019 (SCIS 2019) 予稿集, 2A3-1, 2019.

[79] 高安敦, 渡邉洋平, 江村恵太, “より効率的で適応的に安全な鍵失効機能付き ID ベース暗号の構成,” 暗号と情報セキュリティシンポジウム 2019 (SCIS 2019) 予稿集, 2A3-2, 2019.

[80] 海老名将宏, 渡邉洋平, 四方順司, “探索問題の困難性に基づく効率的なしきい値公開鍵暗号の構成,” 暗号と情報セキュリティシンポジウム 2019 (SCIS 2019) 予稿集, 2A4-4, 2019.

[81] 海老名将宏, 渡邉洋平, 四方順司, “CBDH 仮定に基づく効率的な閾値公開鍵暗号,” コンピューターセキュリティシンポジウム 2018 (CSS 2018) 予稿集, 3A2-3, pp. 746–753, 2018. [**CSS2018 優秀論文賞**]

[82] 松崎なつめ, 穴田啓晃, 金岡晃, 渡邉洋平, “鍵更新機能付き検索可能暗号 : 効率化に向けた一工夫,” コンピューターセキュリティシンポジウム 2018 (CSS 2018) 予稿集, 3A3-1, pp. 814–821, 2018.

[83] 渡邉洋平, 大原一真, 岩本貢, 太田和夫, “現実的な結託者のもとで最もシェア長の短いロバスト秘密分散法,” 電子情報通信学会情報セキュリティ研究会，ISEC2018-7, 2018.

[84] 渡邉洋平, “SXDH 仮定に基づく短いパラメータ長を達成する放送型暗号,” 暗号と情報セキュリティシンポジウム 2018 (SCIS 2018) 予稿集, 3A3-3, 2018.

[85] 黒木慶久, 古賀優太, 渡邉洋平, 岩本貢, 太田和夫, “3 枚のカードで実現可能な 3 入力多数決プロトコル,” 暗号と情報セキュリティシンポジウム 2018 (SCIS 2018) 予稿集, 3B1-4, 2018.

[86] 古賀優太, 鈴木慎之介, 渡邉洋平, 岩本貢, 太田和夫, “カードを用いた複数人でのマッチングプロトコル,” 暗号と情報セキュリティシンポジウム 2018 (SCIS 2018) 予稿集, 3B1-5, 2018.

[87] 鈴木慎之介, 渡邉洋平, 岩本貢, 太田和夫, “ロバスト秘密分散法 CFOR 方式における精密な安全性解析,” 暗号と情報セキュリティシンポジウム 2018 (SCIS 2018) 予稿集, 2A3-3, 2018.

[88] 野島拓也, 渡邉洋平, 岩本貢, 太田和夫, “ダミーエントリの作成方法に着目した共通鍵検索可能暗号 CGKO 方式の改良,” 暗号と情報セキュリティシンポジウム 2018 (SCIS 2018) 予稿集, 3C2-2, 2018.

[89] 松崎なつめ, 穴田啓晃，金岡晃，渡邉洋平, “鍵更新機能付き検索可能暗号の一般的構成,” 暗号と情報セキュリティシンポジウム 2018 (SCIS 2018) 予稿集, 4A2-6, 2018.

[90] 渡邉洋平, 穴田啓晃，松崎なつめ, “鍵更新機能付き検索可能暗号：鍵隔離モデルによる実現,” コンピューターセキュリティシンポジウム 2017 (CSS 2017) 予稿集, 2E3-2, pp. 741–748, 2017.

[91] 松崎なつめ, 穴田啓晃，渡邉洋平, “鍵更新機能付き検索可能暗号：公開鍵更新モデルによる実現,” コンピューターセキュリティシンポジウム 2017 (CSS 2017) 予稿集, 2E3-1, pp. 734–740, 2017.

[92] 松崎なつめ, 穴田啓晃, 渡邉洋平, “鍵更新可能な検索可能暗号の一提案 ～検索可能代理人再暗号化の適用について～,” 電子情報通信学会情報セキュリティ研究会, ISEC2017-5, pp. 1–6, 2017.

[93] 渡邉洋平, “放送型暗号における動的かつ効率的な復号権限変更,” 暗号と情報セキュリティシンポジウム 2017 (SCIS 2017) 予稿集, 4F2-1, 2017.

[94] 岩本貢, 渡邉洋平, “秘密分散型放送暗号,” 暗号と情報セキュリティシンポジウム 2017 (SCIS 2017) 予稿集, 4F2-2, 2017.

[95] 井田潤一, 渡邉洋平, 四方順司, “3 ラウンド対話型 Signcryption の効率的な構成法,” 暗号と情報セキュリティシンポジウム 2017 (SCIS 2017) 予稿集, 3F3-3, 2017.

[96] 吉澤貴博, 渡邉洋平, 四方順司, “推測秘匿性に基づく情報理論的に安全な検索可能暗号,” 暗号と情報セキュリティシンポジウム 2017 (SCIS 2017) 予稿集, 1D1-4, 2017.

[97] 渡邉洋平, 江村恵太, “素数位数群における効率的な鍵失効機能付き ID ベース暗号の構成法,” コンピューターセキュリティシンポジウム 2016 (CSS 2016) 予稿集, 2C1-2, pp. 324–331, 2016.

[98] 吉澤貴博, 渡邉洋平, 四方順司, “情報理論的に安全な検索可能暗号の構成法について,” コンピューターセキュリティシンポジウム 2016 (CSS 2016) 予稿集, 2C3-2, pp. 556–563, 2016.

[99] 渡邉洋平, 四方順司, “スタンダードモデルにおける ID ベース階層型鍵隔離暗号の構成法,” 暗号と情報セキュリティシンポジウム 2016 (SCIS 2016) 予稿集, 2E3-2, 2016.

[100] 井田潤一, 渡邉洋平, 四方順司, “多人数モデルにおける対話型 Signcryption の安全性概念と構成法,” 暗号と情報セキュリティシンポジウム 2016 (SCIS 2016) 予稿集, 2C3-3, 2016.

[101] 吉澤貴博, 渡邉洋平, 四方順司, “情報理論的安全性を持つ検索可能暗号の一般的モデルとその構成法,” 暗号と情報セキュリティシンポジウム 2016 (SCIS 2016) 予稿集, 2C2-1, 2016.

[102] 渡邉洋平, 四方順司, “暗号文長と秘密鍵長間のトレードオフをもつ情報理論的に安全な放送型暗号の構成法,” コンピューターセキュリティシンポジウム 2015 (CSS 2015) 予稿集, 2C2-1, pp. 395–402, 2015.

[103] 井田潤一, 渡邉洋平, 四方順司, “対話型署名機能付き暗号化方式,” コンピューターセキュリティシンポジウム 2015 (CSS 2015) 予稿集, 2C3-3, pp. 600–607, 2015.

[104] 吉澤貴博, 渡邉洋平, 四方順司, “情報理論的に安全な検索可能暗号,” コンピューターセキュリティシンポジウム 2015 (CSS 2015) 予稿集, 3C4-4, pp. 1321–1326, 2015.

[105] 渡邉洋平, 花岡悟一郎, 四方順司, “暗号文の耐改変性と復号権限の変更機能をもつ情報理論的に安全な放送型暗号,” 暗号と情報セキュリティシンポジウム 2015 (SCIS 2015) 予稿集, 2D1-2, 2015. [**SCIS 論文賞**]

[106] 石田優, 渡邉洋平, 四方順司, “CCA 安全かつ暗号文長が短い鍵失効機能付き ID ベース暗号の構成法,” 暗号と情報セキュリティシンポジウム 2015 (SCIS 2015) 予稿集, 2D3-4, 2015.

[107] 河西真瑠那, 清藤武暢, 渡邉洋平, 四方順司, “Canetti-Halevi-Katz 変換による代理人再暗号化方式の一般的構成法,” 暗号と情報セキュリティシンポジウム 2015 (SCIS 2015) 予稿集, 2F2-3, 2015.

[108] 富田信一朗, 渡邉洋平, 四方順司, “情報理論的に安全な順序検証型多重認証方式,” 暗号と情報セキュリティシンポジウム 2015 (SCIS 2015) 予稿集, 2D1-3, 2015.

[109] 渡邉洋平, 四方順司, “受信者集合を変更可能な情報理論的安全性に基づく放送型暗号,” コンピューターセキュリティシンポジウム 2014 (CSS 2014) 予稿集, 3E1-1, pp. 920–927, 2014. [**CSS2014 学生論文賞**]

[110] 石田優, 渡邉洋平, 四方順司, “選択暗号文攻撃に対して安全な鍵失効機能付き ID ベース暗号,” コンピューターセキュリティシンポジウム 2014 (CSS 2014) 予稿集, 1E4-4, pp. 292–299, 2014.

[111] 渡邉洋平, 四方順司, “計算量的に安全なタイムリリース秘密分散法,” 暗号と情報セキュリティシンポジウム 2014 (SCIS 2014) 予稿集, 3F1-5, 2014.

[112] 渡邉洋平, 四方順司, “情報理論的に安全なタイムリリース秘密分散法,” コンピューターセキュリティシンポジウム 2013 (CSS 2013) 予稿集, 2C2-4, pp. 443–450, 2013.

[113] 武井教泰, 渡邉洋平, 四方順司, “検証者の秘密鍵を必要としない情報理論的に安全なブラインド認証方式,” コンピューターセキュリティシンポジウム 2013 (CSS 2013) 予稿集, 2C3-3, pp. 526–533, 2013.

[114] 渡邉洋平, 清藤武暢, 四方順司, “情報理論的に安全なタイムリリース暗号化方式及びメッセージ認証方式の下界について,” コンピューターセキュリティシンポジウム 2012 (CSS 2012) 予稿集, 2C4-2, pp. 601–608, 2012.

[115] 一将吾, 渡邉洋平, 四方順司, “グループにおける情報理論的に安全な相手認証方式,” コンピューターセキュリティシンポジウム 2012 (CSS 2012) 予稿集, 2C4-1, pp. 595–600, 2012.

[116] 渡邉洋平, 清藤武暢, 四方順司, “情報理論的に安全なタイムリリース鍵共有方式のアプリケーションについて,” 暗号と情報セキュリティシンポジウム 2012 (SCIS 2012) 予稿集, 4B2-2, 2012.

[117] 清藤武暢, 渡邉洋平, 四方順司, “情報理論的に安全な Key-Insulated Key-Agreement と Timed-Release Key-Agreement の関係性について,” 暗号と情報セキュリティシンポジウム 2012 (SCIS 2012) 予稿集, 4B2-1, 2012.

[118] 渡邉洋平, 清藤武暢, 四方順司, “時刻情報で制御する情報理論的に安全な鍵共有方式,” コンピューターセキュリティシンポジウム 2011 (CSS 2011) 予稿集, 3C3-2, pp. 738–743, 2011.

ポスター発表（査読無）

[119] H. Anada, A. Kanaoka, N. Matsuzaki, and Y. Watanabe, “Key-updatable Public-key Encryption with Keyword Search: An Efficient Construction,” IWSEC 2018, Sendai, Japan, 2018.

[120] 渡邉洋平, “復号権限無効化機能つき放送型暗号,” , 第 39 回情報理論とその応用シンポジウム (SITA 2016), 岐阜県高山市, 2016.

[121] Y. Watanabe, G. Hanaoka, and J. Shikata, “How to Provide Long-term Security and Required Functionality for Cloud Storage,” Yokohama Environment and Information Sciences (YEIS) International Forum, Yokohama, Japan, 2015.

[122] Y. Ishida, Y. Watanabe, and J. Shikata, “Constructions of Strongly Secure Revocable Identity-based Encryption,” Yokohama Environment and Information Sciences (YEIS) International Forum, Yokohama, Japan, 2015.

[123] Y. Watanabe, G. Hanaoka, and J. Shikata, “How to Provide Long-term Security and Required Functionality for Cloud Storage,” PRIVAGEN 2015, Japan, 2015.

[124] Y. Watanabe and J. Shikata, “Information-Theoretically Secure Revocable-Storage Broadcast Encryption,” IWSEC 2014, Japan, 2014. [**Best Poster Award**]

招待講演

[125] “情報理論的安全性に基づく放送型暗号 ～古典的結果と最近の進展～” 電子情報通信学会 情報理論研究会, IT2017-9, 2017.

[126] “Unconditionally Secure Revocable Storage,” IWSEC 2015, Japan, 2015.

[127] “Timed-Release Cryptography -Two Theoretical Approaches to Achieve Security,” JSPS-DST Asian Academic Seminar 2013 (AAS 2013), Japan, 2013.

口頭発表

[128] “ファイルの安全な追加・削除・検索が可能な暗号システム,” JST 新技術説明会, 2019 年 7 月 (特許 [129] に関して).

特許

[129] 特開 2020-112773, “動的検索可能暗号処理システム及び動的検索可能暗号処理方法,” 渡邉洋平, 岩本貢, 太田和夫 (公開日: 2020 年 7 月 27 日).

報道発表

[130] “暗号化したデータ クラウドで利用容易,” 日本経済新聞, 2019 年 8 月 5 日.

解説記事

[131] 太田和夫, 岩本貢, 渡邉洋平 (取材協力), “暗号 個人情報を守る数学,” ニュートン別冊 数学の世界 現代編 (増補第 2 版), pp. 98–115, Newton Press, 2021.

[132] 渡邉洋平, “検索可能暗号：データベースシステムの安全な運用に向けて,” ケミカルエンジニヤリング, vol. 65, no. 9, pp. 552–560, 化学工業社, 2020.

[133] 四方順司, 渡邉洋平, “情報理論的暗号技術について,” 情報処理, vol. 55, no. 3, pp. 260–267, 2014 年 3 月号, 情報処理学会, 2014.

非専門記事

[134] 渡邉洋平, “国際会議参加報告: 4th Heidelberg Laureate Forum,” Fundamentals Review, vol. 10, no. 3, pp. 220–221, 電子情報通信学会, 2017.