Yohei Watanabe

Curriculum Vitae

Graduate School of Informatics and Engineering,
The University of Electro-Communications,
928, Building E-3, 1-5-1 Chofugaoka, Chofu, 182-8585, Japan

Phone: +81-42-443-5822
E-mail: watanabe@uec.ac.jp

Last updated: March 12, 2023

Research Interests

Modern cryptography in terms of both information theory and complexity theory.
Especially:

- ▷ Searchable symmetric encryption and encrypted database.
- ▷ Information-theoretic cryptographic protocols.
- ▷ Public-key cryptosystems over bilinear/traditional groups.
- ▷ Updatable cryptography.

Education

- ▷ **Ph.D. in Information Science**, Yokohama National University.
  Thesis: Cryptography with Timed Access Control
  Supervisor: Asso. Prof. Dr. Junji Shikata — March 2016
- ▷ **M.S. in Engineering**, Yokohama National University. — March 2013
- ▷ **B.S. in Engineering**, Yokohama National University. — March 2011

Experience

- ▷ **Research Fellow**, Japan Datacom Co., Ltd., Japan. — Aug. 2020 – present
- ▷ **Invited Advisor**, Security Fundamental Laboratory, Cybersecurity Research Institute, NICT, Japan. — Apr. 2020 – present
- ▷ **Collaborative Researcher**, Cyber Physical Security Research Center (CPSEC), AIST, Japan. — Apr. 2020 – present
- ▷ **Assistant Professor**, Department of Informatics, Graduate School of Informatics and Engineering, the University of Electro-Communications, Japan. — Dec. 2019 – present
- ▷ **Excellent Young Researcher**, Leading Initiative for Excellent Young Researchers, MEXT, Japan. — Dec. 2019 – present
- ▷ **Researcher**, Security Fundamental Laboratory, Cybersecurity Research Institute, NICT, Japan. — Oct. 2018 – Nov. 2019
- ▷ **JSPS Research Fellow (PD)**, the University of Electro-Communications, Japan.
  Host researcher: Asso. Prof. Dr. Mitsugu Iwamoto — Apr. 2016 – Sep. 2018
- ▷ **Collaborative Researcher**, Information Technology Research Institute (ITRI), AIST, Japan. — Apr. 2016 – Sep. 2018
- ▷ **JSPS Research Fellow (DC1)**, Yokohama National University, Japan.
  Host researcher: Asso. Prof. Dr. Junji Shikata — Apr. 2013 – Mar. 2016
- ▷ **Technical Trainee**, ITRI, AIST, Japan. — Apr. 2015 – Mar. 2016
- ▷ **Technical Trainee**, Research Institute for Secure Systems (RISEC), AIST, Japan. — May 2014 – Mar. 2015

Awards and Honers

- ▷ **Best Paper Award** at ProvSec 2022, 2022.
- ▷ **CSS 2022 Best Paper Award** at CSS 2022 (domestic conference in Japan), 2022.
- ▷ **CSS 2020 Encouragement Research Award** at CSS 2020 (domestic conference in Japan), 2020.
- ▷ **CSS 2019 Encouragement Research Award** at CSS 2019 (domestic conference in Japan), 2019.
- ▷ **IEEE Information Theory Society Japan Chapter Young Researcher Best Paper Award** at ISITA 2018, 2018.
- ▷ **CSS 2018 Best Paper Award** at CSS 2018 (domestic conference in Japan), 2018.
- ▷ **Invitation to 4th Heidelberg Laureate Forum**, 2016.
- ▷ **SCIS Paper Award** at SCIS 2016 (domestic conference in Japan), 2016.
- ▷ **CSS 2014 Student Paper Award** at CSS 2014 (domestic conference in Japan), 2014.
- ▷ **Best Poster Award** at IWSEC 2014, 2014.
- ▷ **JSPS Research fellowship for young scientists (PD)**, 2016 – 2019.
- ▷ **JSPS Research fellowship for young scientists (DC1)**, 2013 – 2016.
- ▷ **Paper(s) invited to special issues of journal(s)**:
  - Invited to International Journal of Applied Cryptography (IJACT) from ACISP 2015.

Committees

- ▷ **Editor:** IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences.
  - ENG Edition: Editor (Jun. 2023 – May 2024).
  - JPN Edition: Editor (Jun. 2022 – May 2024).
  - Special Issue on Information Theory and its Applications: Guest editor (2020).
- ▷ **Program Committees:** APKC 2023, APKC 2022, ITW 2021, IWSEC 2021, APKC 2021, IWSEC 2020, APKC 2020, IWSEC 2019, APKC 2019, APKC 2018 (co-Chair).
- ▷ **Local Organizing Committees:** IWSEC 2023, SCIS 2023, PKC 2022 (co-Chair), IWSEC 2022, CSS 2021, IWSEC 2021, SCIS 2021, CSS 2019, IWSEC 2019, IWSEC 2018.
- ▷ **Others:** CRYPTREC Cryptographic Technique Investigation WG (Advanced Cryptography) Member (May 2022 – Mar. 2023).

Teaching

At UEC

- ▷ Fall 2022: *Cryptography*, *Advanced Topics on Cryptography*, *Cryptography and Information Security*, *Information Security Engineering Laboratory.*
- ▷ Fall 2021: *Cryptography*, *Advanced Topics on Cryptography*, *Cryptography and Information Security*, *Information Security Engineering Laboratory.*
- ▷ Fall 2020: *Cryptography*, *Cryptography and Information Security* , *Information Security Engineering Laboratory.*
- ▷ Fall 2019: *Cryptography.*

At Other Universities

- ▷ Spring 2023: *Computer Literacy* (Japan Women's University).
- ▷ Spring & Fall 2022: *Computer Literacy* (Japan Women's University).
- ▷ Spring & Fall 2021: *Computer Literacy* (Japan Women's University).
- ▷ Spring & Fall 2020: *Computer Literacy* (Japan Women's University).
- ▷ Fall 2019: *Computer Literacy* (Japan Women's University).
- ▷ Spring 2019: *Computer Literacy* (Japan Women's University), *Project Learning* (Yokohama National University).
- ▷ Fall 2018: *Computer Literacy* (Japan Women's University).

Research Grants

- ▷ JSPS Grant-in-Aid for Scientific Research (A), "真に高機能暗号の社会展開に資する物理・視覚暗号 (# 22H*****)," CI (PI: Goichiro Hanaoka). April 2023 – March 2026
- ▷ JSPS Grant-in-Aid for Scientific Research (B), "Towards Encrypted Search Protocols with Flexible Search Functions and High Efficiency (# 21H03341)," PI. April 2021 – March 2025
- ▷ JSPS Grant-in-Aid for Scientific Research (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 (# 21H03395)," CI (PI: Mitsugu Iwamoto). April 2021 – March 2025
- ▷ JSPS Grant-in-Aid for Scientific Research (S), "Resilience Enhancement of IoT Ecosystem by Cryptographic Technologies (# 18H05289)," CI (PI: Kazuo Sakiyama).
  June 2018 – March 2023
  (Joined in April 2020)
- ▷ JSPS Grant-in-Aid for Scientific Research (C), "Searchable Symmetric Encryption for a Long Term Use (# 18K11293)," CI (PI: Kazuo Ohta).
  April 2018 – March 2022
  (Joined in April 2020, and extended to March 2023)
- ▷ MEXT Leading Initiative for Excellent Young Researchers (LEADER), PI.
  December 2019 – March 2021
- ▷ JSPS Grant-in-Aid for Young Scientists (B), "Improvement of security and efficiency of identity-based encryption schemes resilient to key leakage (# 17K12697)," PI.
  April 2017 – March 2021
- ▷ JSPS Grant-in-Aid for Scientific Research (B), "推測秘匿性に基づく情報理論的暗号理論の新展開 (# 17H01752)," CI (PI: Mitsugu Iwamoto).
  April 2017 – March 2021
  (extended to March 2022)
- ▷ Grant-in-Aid for JSPS Fellows (# 16J10532), "Simultaneous Realization of Dynamic Access Control and Data Analysis for Encrypted Data," PI.
  April 2016 – March 2019
- ▷ Grant-in-Aid for JSPS Fellows (#13J03998), "時刻で制御可能な暗号基礎技術の研究開発," PI.
  April 2013 – March 2016

Edited Volumes

[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.

Peer-Reviewed Journal Articles

[4] H. Kobayashi, Y. Watanabe, K. Minematsu, and J. Shikata, "Tight Lower Bounds and Optimal Constructions of Anonymous Broadcast Encryption and Authentication," Designs, Codes and Cryptography, vol. xx, pp. yyy–zzz, Springer, 2023. (To appear)

[5] Y. Abe, T. Nakai, Y. Watanabe, M. Iwamoto, and K. Ohta, "A Computationally Efficient Card-Based Majority Voting Protocol with Fewer Cards in the Private Model," IEICE Transactions, vol. E106-A, no. 3, pp. 315–324, IEICE, 2023.

[6] Y. Watanabe, T. Seito, and J. Shikata, "Multi-Designated Receiver Authentication Codes: Models and Constructions," IEICE Transactions, vol. E106-A, no. 3, pp. 394–405, IEICE, 2023.

[7] 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. 1559–1579, IEICE, 2022.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

Peer-Reviewed Conference Papers

[22] Y. Liu, Y. Watanabe, and J. Shikata "Forward and Backward Private Dynamic Searchable Encryption with Better Space Efficiency," In: CISS 2023, pp. xxx–yyy, IEEE, 2023. (To appear)

[23] K. Asano, K. Emura, A. Takayasu, and Y. Watanabe, "A Generic Construction of CCA-secure Attribute-based Encryption with Equality Test," In: ProvSec 2022, LNCS 13600, pp. 3–19, Springer, 2022. **[Best Paper Award]**

[24] 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)

[25] 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)

[26] 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.

[27] 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.

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

[29] 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.

[30] 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.

[31] 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.

[32] 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.

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

[34] 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.

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

[36] 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]**

[37] 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.

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

[39] 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.

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

[41] 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.

[42] 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.

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

[44] 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.

[45] 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, Springer, 2015.

[46] 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.

[47] 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.

[48] 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.

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

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

[51] 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.

[52] 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.

[53] 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.

[54] 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.

[55] 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.

[56] 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.

Non Peer-Reviewed Posters

[57] 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.

[58] 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.

[59] 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.

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

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

Invited Talks

[62] "Unconditionally Secure Revocable Storage," IWSEC 2015, Japan, 2015.

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