Kenji Yasunaga

Last updated: December 9, 2022

Associate Professor
Department of Mathematical and Computing Science
School of Computing
Tokyo Institute of Technology
2-12-1 W8-45 Ookayama, Meguro-ku, Tokyo 152-8552 Japan

Research Interests

Coding Theory, Cryptography, Computational Complexity.
Especially, pseudorandomness, error-correcting codes, and game-theoretic cryptography.

Employment (Full-Time)

October 2021 – Present	Associate Professor at *Tokyo Institute of Technology*
August 2018 – September 2021	Associate Professor at *Osaka University*
January 2013 – July 2018	Assistant Professor at *Kanazawa University*
October 2011 – December 2012	Researcher at *Institute of Systems, Information Technologies and Nanotechnologies (ISIT)*
October 2008 – September 2011	Assistant Professor at *Tokyo Institute of Technology*
April 2008 – September 2008	Post-doctoral fellow at *Kwansei Gakuin University*

Employment (Part-Time)

October 2021 – March 2023	Guest Associate Professor at Osaka University
October 2021 – March 2022	Part-Time Lecturer at Osaka University
July 2019 – March 2020	Part-Time Lecturer at Mie University
November 2018 – March 2019	Part-Time Lecturer at Kanazawa University
April 2010 – March 2021	Part-Time Lecturer at Waseda University

Education

Doctor of Philosophy in Information Science and Technology March 2008
Graduate School of Information Science and Technology, *Osaka University*
Dissertation: Monotone Error Structure and Local Weight Distribution of Linear Codes

Master of Information Science and Technology March 2005
Graduate School of Information Science and Technology, *Osaka University*

Bachelor of Engineering March 2003
School of Engineering Science, *Osaka University*

Awards and Honors

- IEICE Engineering Sciences Society, Certificate of Appreciation for Editor Service, September 2022.
- IEICE Engineering Sciences Society, Certificate of Appreciation for Editor Service, September 2021.
- IEICE Engineering Sciences Society: Service Award (as a Guest Associate Editor of the Journal), September 2021.

- IEICE Engineering Sciences Society: Service Award (as an Associate Editor of the Journal), September 2019.
- Outstanding Paper Award (with M. Fujita and T. Koshiba), GameSec 2018.
- Kasami Award, 2008.
- Society of Information Theory and Its Applications (SITA) Encouragement Award, 2007.

Professional Activities

Editorial Committee

- Reviewer, IEICE Transactions, June 2021–Present.
- Associate Editor, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, June 2017–June 2021.
- Guest Associate Editor, IEICE Transactions of Fundamentals of Electronics, Communications and Computer Sciences, Special Section on Information Theory and Its Applications, December 2015–December 2016, December 2018–December 2019 (Secretary), November 2019–December 2020 (Secretary).
- Guest Associate Editor, IEICE Transactions of Fundamentals of Electronics, Communications and Computer Sciences, Special Section on Discrete Mathematics and Its Applications, July 2015–June 2016, July 2017–August 2018 (Secretary), August 2019–October 2020, August 2021–October 2022 (Secretary).
- Guest Associate Editor, IEICE Transactions on Information and Systems, Special Section on Foundations of Computer Science $\sim$ Developments of the Theory on Algorithms and Computation $\sim$, February 2015–March 2016, January 2016–March 2017.
- Guest Associate Editor, IEICE Transactions of Fundamentals of Electronics, Communications and Computer Sciences, Special Section on Cryptography and Information Security, January 2012–January 2013, January 2013–January 2014, January 2014–January 2015, January 2015–January 2016, November 2018–January 2020.

Program Committee

- Program Committee, 10th ACM ASIA Public-Key Cryptography Workshop (APKC 2023).
- Program Committee, 9th ACM ASIA Public-Key Cryptography Workshop (APKC 2022).
- Program Committee, 45th Symposium on Information Theory and Its Applications (SITA2022).
- Program Committee Secretary, International Symposium on Information Theory and Its Applications (ISITA2020).
- Program Committee Secretary, 41st Symposium on Information Theory and Its Applications (SITA2018).
- Program Committee, 39th Symposium on Information Theory and Its Applications (SITA2016).
- Program Committee, Fourth International Symposium on Computing and Networking (CANDAR'16).
- Program Committee, 3rd International Workshop on Information and Communication Security (WICS'16).
- Program Committee, 38th Symposium on Information Theory and Its Applications (SITA2015).
- Program Committee, 10th International Workshop on Security (IWSEC2015).

Organizing Committee

- Technical Committee, IPSJ Computer Security Group (CSEC), April 2021–March 2022.
- Organizing Committee, 44th Symposium on Information Theory and Its Applications (SITA2021).
- Publications Committee, Committee Member [A], IEICE, June 2020-June 2022.
- Technical Committee, IEICE Technical Committee on Information Theory (IT), June 2020–June 2024.
- Technical Committee, IEICE Technical Committee on Theoretical Foundations of Computing (COMP), June 2018–June 2024.
- Organizing Committee, 41st Symposium on Information Theory and Its Applications (SITA2018).
- Technical Committee, IEICE Technical Committee on Information Security (ISEC), June 2017–June 2023.
- Organizing Committee, IPSJ Computer Security Group (CSEC), April 2017–March 2021.
- Organizing Committee, 15th International Conference on Applied Cryptography and Network Security (ACNS2017).
- Organizing Committee, 40th Symposium on Information Theory and Its Applications (SITA2016).
- Organizing Committee, 9th International Conference on Provable Security (ProvSec2015).
- Organizing Committee, LA Symposium 2015, 2020, 2022 (Representative).
- Organizing Committee, Workshop on Error-Correcting Codes 2015, 2016, 2017 (Chair), 2018, 2019, 2020.
- Organizing Committee, 35th Symposium on Information Theory and Its Applications (SITA2012).
- Organizing Committee, 7th International Workshop on Security (IWSEC2012).

Teaching Experience

- Theory of Computation, Tokyo Institute of Technology, 2022.
- Foundation of Cybersecurity (Cryptography and Computational Complexity), Tokyo Institute of Technology,2022.
- Information Literacy I, II, Tokyo Institute of Technology, 2022.
- Content Security, Osaka University, 2020.
- Topics in Information Engineering, Mie University, 2019.
- Introduction to Computer Algorithms, Osaka University, 2019, 2020.
- Information Security, Osaka University, 2019, 2021.
- Introduction to Information Science, Osaka University, 2018.
- Introduction to Combinatorics, Osaka University, 2018–2021.
- Information and Computer System Engineering Laboratory 1 (C Language Programming and Algorithms), Kanazawa University, 2013–2018.
- Information Security (Assistant), Kanazawa University, 2013–2018.
- Applied Mathematics 6 — Introduction to Cryptography, Waseda University, 2010.
- Applied Mathematics 5 — Introduction to Coding Theory, Waseda University, 2010.
- Introduction to Algorithms and Data Structures (Programming Exercises), Tokyo Institute of Technology, 2009–2011.
- Automata and Formal Language Theory (Assistant), Tokyo Institute of Technology, 2008–2010.
- Theory of Computation (Assistant), Tokyo Institute of Technology, 2008–2010.
- Computational Complexity Theory (Assistant), Tokyo Institute of Technology, 2008–2010.

External Funding

- Japan Society for the Promotion of Science (JSPS), Grant-in-Aid for Scientific Research (A), Number 21H04879, "Construction of Quantum Computational Infrastructure towards Quantum Information Society," with Takeshi Koshiba (Waseda University) and others, 2021-2025.
- Japan Society for the Promotion of Science (JSPS), Grant-in-Aid for Scientific Research (C), Number 18K11159, "Exploring the Limitations of Deletion Codes," 2018–2021.
- Japan Society for the Promotion of Science (JSPS), Grant-in-Aid for Scientific Research (B), Number 17H01695, "Constructions of Cryptographic Primitives with Incentives," with Keisuke Tanaka (Tokyo Inst. of Tech.) and others, 2017–2020.
- Japan Society for the Promotion of Science (JSPS), Grant-in-Aid for Scientific Research (A), Number 16H01705, "Interpolative Expansion of Quantum Protocol Theory," with Takeshi Koshiba (Saitama University) and others, 2016–2020.
- The Ministry of Education, Culture, Sports, Science and Technology (MEXT), Grant-in-Aid for Scientific Research on Innovative Areas (Publicly Invited Research), Number 15H00851, "Exploring the Limitations in Coding Theory," 2015–2016.
- The Ministry of Education, Culture, Sports, Science and Technology (MEXT), Grant-in-Aid for Scientific Research on Innovative Areas (Publicly Invited Research), Number 25106509, "Limitations of Cryptographic Primitives with Computational Restrictions," 2013–2014.
- Japan Society for the Promotion of Science (JSPS), Grant-in-Aid for Scientific Research (A), Number 24240001, "Foundation for Theory of Quantum Protocols," with Takeshi Koshiba (Saitama University) and others, 2012–2016.
- The Telecommunications Advancement Foundation, "Research on Leakage and Tamper Resilient Cryptographic Primitives," 2012.
- Japan Society for the Promotion of Science (JSPS), Grant-in-Aid for Scientific Research (C), Number 23500010, "Cryptographic Protocols based on Game Theory," with Keisuke Tanaka (Tokyo Inst. of Tech.), 2011–2014.
- Japan Society for the Promotion of Science (JSPS), Grant-in-Aid for Young Scientists (B), Number 23700010, "Randomness and Structure in Error-Correcting Codes," 2011–2013.
- Japan Society for the Promotion of Science (JSPS), Grant-in-Aid for Young Scientists (Start-up), Number 20860079, "Constructions of Error-Correcting Codes based on Pseudorandomness," 2008–2009.

Contract Research

- NEC Corporation, 2022.

Publications

Papers in Refereed Journals

1. Kenji Yasunaga Kosuke Yuzawa. On the Limitations of Computational Fuzzy Extractors. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, volume E106-A, number 1, January 2023 (to appear).
2. Maiki Fujita, Takeshi Koshiba, Kenji Yasunaga. Perfectly Secure Message Transmission Against Rational Adversaries. *IEEE Journal on Selected Areas in Information Theory*, volume 3, issue 2, June 2022.
3. Kenji Yasunaga. Practical card-based protocol for three-input majority. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, volume E103-A, number 11, pages 1296–1298, November 2020.
4. Tomohiro Hayashi and Kenji Yasunaga. On the list decodability of insertions and deletions. *IEEE Transactions on Information Theory*, volume 66, number 9, pages 5335–5343, September 2020.

5. Kenji Yasunaga. Error correction by structural simplicity: correcting samplable additive errors. *The Computer Journal*, volume 62, issue 9, pages 1265–1276, September 2019.

6. Kenji Yasunaga and Kosuke Yuzawa. Repeated games for generating randomness in encryption. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, volume E101–A, number 4, pages 697–703, April 2018.

7. Keita Inasawa and Kenji Yasunaga. Rational proofs against rational verifiers. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, volume E100–A, number 11, pages 2392–2397, November 2017.

8. Akinori Kawachi, Yoshio Okamoto, Keisuke Tanaka, and Kenji Yasunaga. General constructions of rational secret sharing with expected constant-round reconstruction. *The Computer Journal*, volume 60, issue 5, pages 711-728, April 2017.

9. Kenji Yasunaga. Public-key encryption with lazy parties. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, volume E99–A, number 2, pages 590–600, February, 2016.

10. Eiichiro Fujisaki, Akinori Kawachi, Ryo Nishimaki, Keisuke Tanaka, and Kenji Yasunaga. Post-challenge leakage resilient public-key cryptosystem in split state model. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, volume E98–A, number 3, pages 853–862, March 2015.

11. Hitoshi Namiki, Keisuke Tanaka, and Kenji Yasunaga. Randomness leakage in the KEM/DEM framework. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, volume E97–A, number 1, pages 191–199, January 2014.

12. Kenji Yasunaga. List decoding of Reed-Muller codes based on a generalized Plotkin construction. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, volume E96–A, number 7, pages 1662–1666, July 2013.

13. Manh Ha Nguyen, Kenji Yasunaga, and Keisuke Tanaka. Leakage-resilience of stateless/stateful public-key encryption from hash proofs. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, volume E96–A, number 6, pages 1100–1111, June 2013.

14. Kenji Yasunaga and Toru Fujiwara. On correctable errors of binary linear codes. *IEEE Transactions on Information Theory*, volume 56, number 6, pages 2537–2548, June 2010.

15. Kenji Yasunaga, Toru Fujiwara, and Tadao Kasami. Local weight distribution of the (256, 93) third-order binary Reed-Muller code. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, volume E90–A, number 3, pages 698–701, March 2007.

16. Kenji Yasunaga and Toru Fujiwara. Determination of the local weight distribution of binary linear block codes. *IEEE Transactions on Information Theory*, volume 52, number 10, pages 4444–4454, October 2006.

Papers in Refereed Conferences

1. Shun Watanabe and Kenji Yasunaga. Bit Security as Computational Cost for Winning Games with High Probability. In *Advances in Cryptology – ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part III*, *Lecture Notes in Computer Science*, Springer, volume 13092, pages 161–188, December 2021.

2. Kenji Yasunaga. Replacing Probability Distributions in Security Games via Hellinger Distance. In *the 2nd Conference on Information-Theoretic Cryptography (ITC 2021)*, *Leibniz International Proceedings in Informatics (LIPIcs)*, volume 199, pages 17:1–17:5, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.

3. Kodai Sato, Kenji Yasunaga, Toru Fujiwara. A Construction of Robustly Reusable Fuzzy Extractors over Blockchains. In *Proceedings of the 2020 International Symposium on Information Theory and Its Applications (ISITA)*, pages 353-357, October 2020.

4. Kenji Yasunaga and Takeshi Koshiba. Perfectly Secure Message Transmission against Independent Rational Adversaries. In *Proceedings of the 10th Conference on Decision and Game Theory for Security (GameSec 2019)*, *Lecture Notes in Computer Science*, Springer, volume 11836, pages 563–582, October 2019.

5. Maiki Fujita, Kenji Yasunaga, and Takeshi Koshiba. Perfectly secure message transmission against rational timid adversaries. In *Proceedings of the 9th Conference on Decision and Game Theory for Security (GameSec 2018)*, *Lecture Notes in Computer Science*, Springer, volume 11199, pages 127–144, October 2018.

6. Tomohiro Hayashi and Kenji Yasunaga. On the list decodability of insertions and deletions. In *Proceedings of the 2018 IEEE International Symposium on Information Theory (ISIT 2018)*, pages 86–90, June 2018.

7. Kenji Yasunaga. Error-correcting codes against chosen-codeword attacks. In *Proceedings of the 9th International Conference on Information Theoretic Security (ICITS 2016)*, *Lecture Notes in Computer Science*, Springer, volume 10015, pages 177–189, August 2016.

8. Kenji Yasunaga. Correction of samplable additive errors. In *Proceedings of the 2014 IEEE International Symposium on Information Theory (ISIT 2014)*, pages 1066–1070, July 2014.

9. Haruna Higo, Keisuke Tanaka, and Kenji Yasunaga. Game-theoretic security for bit commitment. In *Proceedings of the 8th International Workshop on Security (IWSEC 2013)*, *Lecture Notes in Computer Science*, Springer-Verlag, volume 8231, pages 303–318, November 2013.

10. Hiroya Takahashi, Kenji Yasunaga, Masahiro Mambo, Kwangjo Kim, and Heung Youl Youm. Preventing abuse of cookies stolen by XSS. In *Proceedings of the 8th Asia Joint Conference on Information Security (AsiaJCIS 2013)*, pages 85–89, July 2013.

11. Kenji Yasunaga. Public-key encryption with lazy parties. In *Proceedings of the 8th Conference on Security and Cryptography for Networks (SCN 2012)*, *Lecture Notes in Computer Science*, Springer-Verlag, volume 7485, pages 411–425, September 2012.

12. Haruna Higo, Keisuke Tanaka, Akihiro Yamada, and Kenji Yasunaga. A game-theoretic perspective on oblivious transfer. In *Proceedings of the 17th Australasian Conference on Information Security and Privacy (ACISP 2012)*, *Lecture Notes in Computer Science*, Springer-Verlag, volume 7372, pages 29–42, July 2012.

13. Manh Ha Nguyen, Keisuke Tanaka, and Kenji Yasunaga. Leakage-resilience of stateless/stateful public-key encryption from hash proofs. In *Proceedings of the 17th Australasian Conference on Information Security and Privacy (ACISP 2012)*, *Lecture Notes in Computer Science*, Springer-Verlag, volume 7372, pages 208–222, July 2012.

14. Hitoshi Namiki, Keisuke Tanaka, and Kenji Yasunaga. Randomness leakage in the KEM/DEM framework. In *Proceedings of the 5th International Conference on Provable Security (ProvSec 2011)*, *Lecture Notes in Computer Science*, Springer-Verlag, volume 6980, pages 309–323, October 2011.

15. Keisuke Tanaka, Akihiro Yamada, and Kenji Yasunaga. Weak oblivious transfer from strong one-way functions. In *Proceedings of the 5th International Conference on Provable Security (ProvSec 2011)*, *Lecture Notes in Computer Science*, Springer-Verlag, volume 6980, pages 34–51, October 2011.

16. Manh Ha Nguyen, Kenji Yasunaga, and Keisuke Tanaka. Leakage-resilient CCA2 public-key encryption from 4-wise independent hash functions. In *Proceedings of the 2011 International Conference on Advanced Technologies for Communications (ATC/REV 2011)*, August 2011.

17. Kenji Yasunaga and Toru Fujiwara. Uncorrectable errors of weight half the minimum distance for binary linear codes. In *Proceedings of the 2008 IEEE International Symposium on Information Theory (ISIT 2008)*, July 2008.

18. Kenji Yasunaga and Toru Fujiwara. Correctable errors of weight half the minimum distance plus one for the first-order Reed-Muller codes. In *Proceedings of the 17th Symposium on Applied Algebra, Algebraic Algorithms, and Error Correcting Codes (AAECC-17), Lecture Notes in Computer Science*, Springer-Verlag, volume 4581, pages 110–119, December 2007.

19. Kenji Yasunaga and Toru Fujiwara. Relations between the local weight distributions of a linear block code, its extended code, and its even weight subcode. In *Proceedings of the 2005 IEEE International Symposium on Information Theory (ISIT 2005)*, September 2005.

20. Kenji Yasunaga and Toru Fujiwara. An algorithm for computing the local weight distribution of binary linear codes closed under a group of permutations. In *Proceedings of the 2004 International Symposium on Information Theory and Its Applications (ISITA 2004)*, pages 846–851, October 2004.

Review Articles

1. Kenji Yasunaga. Game theory in cryptography. *Computer Software*, volume 34, number 1, pages 81–92, January 2017. (in Japanese)

2. Kenji Yasunaga. Cryptography and game theory. *Sugaku Seminar*, Nippon-Hyoron-Sha, volume 53, number 10, pages25–29, October 2014. (in Japanese)

3. Kenji Yasunaga. A unified framework for understanding pseudorandom constructions from a coding theoretic perspective. *The Institute of Electronics, Information and Communication Engineers (IEICE) Fundamentals Review*, volume 5, number 1, July 2011. (in Japanese)

Technical Reports/Other Research Work

1. Shun Watanabe and Kenji Yasunaga. Unified View for Notions of Bit Security. *LA Symposium*, July 2022.

2. Shoto Kusachi and Kenji Yasunaga. Evaluating Approximation Accuracy and Information Leakage of Ranking Methods Using Few Candidates: Deterministic and Randomized. *The 44th Symposium on Information Theory and Its Applications (SITA2021), Recent Results Session*, R.2.6, December 2021.

3. Yasuaki Haseba and Kenji Yasunaga. Correcting Insertions and Deletions Using Cryptographic Hash Functions. *The 44th Symposium on Information Theory and Its Applications (SITA2021)*, 2.2.3, pages 127–131, December 2021. (in Japanese)

4. Shoto Kusachi and Kenji Yasunaga. Evaluating Ranking Methods Using Few Candidates: Deterministic and Randomized. *2021 Fall National Conference of Operations Research Society of Japan*, 2-C-6, September 2021. (in Japanese)

5. Kenji Yasunaga and Takeshi Koshiba. Game-theoretically secure message transmission against adversaries who corrupt all channels. *LA symposium*, February 2020.

6. Kenji Yasunaga and Takeshi Koshiba. Game-theoretically secure message transmission against adversaries who corrupt all channels. *The 2020 Symposium on Cryptography and Information Security (SCIS2020),* 1A2-3, January 2020.

7. Kodai Sato, Kenji Yasunaga, Naoto Yanai, and Toru Fujiwara. Fair information-sharing protocols for set union. *The 2019 Symposium on Cryptography and Information Security (SCIS2019),* 2A1-1, January 2019.

8. Haruna Higo, Keisuke Tanaka, and Kenji Yasunaga. Security against risk-averse adversaries: secure two-party protocols from a game-theoretic perspective. *The 2018 Symposium on Cryptography and Information Security (SCIS2018),* 3A1-1, January 2018.

9. Tomohiro Hayashi, Kenji Yasunaga, and Masahiro Mambo. On the security of deterministic encryption schemes for quantum adversaries. *The 2017 Symposium on Cryptography and Information Security (SCIS2017),* 4A1-1, January 2017. (in Japanese)

10. Keita Inasawa, Hayato Ecchuya, Kenji Yasunaga, and Masahiro Mambo. On the Impossibility Results of Permissionless Consensus Protocols. *The 2017 Symposium on Cryptography and Information Security (SCIS2017),* 3F3-1, January 2017. (in Japanese)

11. Kazuya Fukushima, Tomoaki Kosugi, Kenji Yasunaga, and Masahiro Mambo. Camparative evaluation of security indices used in data anoymization. *The 2017 Symposium on Cryptography and Information Security (SCIS2017),* 3B3-6, January 2017. (in Japanese)

12. Kenji Yasunaga. On efficient correctability of samplable errors. *LA Symposium*, January 2016.

13. Kosuke Yuzawa, Kenji Yasunaga, and Masahiro Mambo. On the incentive to generate randomness in repeated games. *The 2016 Symposium on Cryptography and Information Security (SCIS2016),* 3A3-4, January 2016. (in Japanese)

14. Keita Inasawa, Kenji Yasunaga, and Masahiro Mambo. Rational proofs against cheating verifiers and their application to delegated computation. *The 2016 Symposium on Cryptography and Information Security (SCIS2016),* 3A3-2, January 2016. (in Japanese)

15. Hayato Etchuya, Kenji Yasunaga, and Masahiro Mambo. A construction of signdecryption schemes from obfuscation. *The 2016 Symposium on Cryptography and Information Security (SCIS2016),* 2C3-2, January 2016. (in Japanese)

16. Keita Inasawa, Kenji Yasunaga, and Masahiro Mambo. Rational proofs for rational verifiers. *LA Symposium*, July 2015. (in Japanese)

17. Takuya Nishino, Kenji Yasunaga, and Masahiro Mambo. An analysis on PRNGs with entropy pools. *The 32nd Symposium on Cryptography and Information Security (SCIS2015),* 4E2-4, January 2015. (in Japanese)

18. Mitsuharu Ikeda, Kenji Yasunaga, and Masahiro Mambo. On the study of computational entropic security. *The 32nd Symposium on Cryptography and Information Security (SCIS2015),* 4F1-1, January 2015. (in Japanese)

19. Keita Inasawa, Kenji Yasunaga, and Masahiro Mambo. Rational proofs against reward-reducing verifiers. *The 32nd Symposium on Cryptography and Information Security (SCIS2015),* 3D3-4, January 2015. (in Japanese)

20. Hiroya Takahashi, Kenji Yasunaga, and Masahiro Mambo. Implementation of the method to prohibit abuse of stolen cookies. *The 32nd Symposium on Cryptography and Information Security (SCIS2015),* 3E1-2, January 2015. (in Japanese)

21. Kosuke Yuzawa, Kenji Yasunaga, and Masahiro Mambo. Effects of the partial password sharing for usability improvements. *The 32nd Symposium on Cryptography and Information Security (SCIS2015),* 2C1-3, January 2015. (in Japanese)

22. Kosuke Yuzawa, Kenji Yasunaga, and Masahiro Mambo. A study on computational fuzzy extractors. *The 31st Symposium on Cryptography and Information Security (SCIS2014),* 3B4-1, January 2014.

23. Haruna Higo, Kenji Yasunaga, and Keisuke Tanaka. Two-party computation and game theory. *LA Symposium*, January 2013. (in Japanese)

24. Haruna Higo, Kenji Yasunaga, and Keisuke Tanaka. Game-theoretic security of commitment. *The 30th Symposium on Cryptography and Information Security (SCIS2013),* 3C3-4, January 2012. (in Japanese)

25. Haruna Higo, Kenji Yasunaga, and Keisuke Tanaka. Toward a game-theoretic security of two-party protocol. *The 30th Symposium on Cryptography and Information Security (SCIS2013),* 3B3-3, January 2012. (in Japanese)

26. Kenji Yasunaga. Correctability of efficiently computable additive errors. *The 35th Symposium on Information Theory and Its Applications (SITA2012)*, December 2012. (in Japanese)

27. Kenji Yasunaga. Impossibility results for rational secret sharing and their avoidance. In *Proceedings of Computer Security Symposium 2012 (CSS2012)*, 1C2-1, October 2012. (in Japanese)

28. Haruna Higo, Akihiro Yamada, Kenji Yasunaga, and Keisuke Tanaka. Rationality and security in oblivious transfer. *IEICE Technical Report*, ISEC2012-34, pages 181–188, July 2012.

29. Akinori Kawachi, Yoshio Okamoto, Keisuke Tanaka, and Kenji Yasunaga. Rational secret sharing for non-simultaneous channels. *IEICE Technical Report*, IT2012–8, pages 41–46, May 2012.

30. Kenji Yasunaga. A game theoretic perspective on randomness generation and security in public-key encryption. *The 29th Symposium on Cryptography and Information Security (SCIS2012),* 3A3-2, February 2012.

31. Haruna Higo, Akihiro Yamada, Kenji Yasunaga, and Keisuke Tanaka. A game theoretic perspective on oblivious transfer. *The 29th Symposium on Cryptography and Information Security (SCIS2012),* 3B2-5, February 2012. (in Japanese)

32. Kenji Yasunaga and Maki Yoshida. On the security of ciphertext in public-key encryption. *The 29th Symposium on Cryptography and Information Security (SCIS2012),* 3A2-3, February 2012.

33. Hitoshi Namiki, Kenji Yasunaga, and Keisuke Tanaka. Randomness leakage in The KEM/DEM framework. *The 28th Symposium on Cryptography and Information Security (SCIS2011),* 2A2-2, January 2011.

34. Manh Ha Nguyen, Kenji Yasunaga, and Keisuke Tanaka. Generic constructions of leakage-resilient CCA2 stateless/stateful public-key encryption. *The 28th Symposium on Cryptography and Information Security (SCIS2011),* 2A1-3, January 2011.

35. Hirotoshi Takebe, Keisuke Tanaka, and Kenji Yasunaga. Security notions on selective opening. *The 28th Symposium on Cryptography and Information Security (SCIS2011),* 2A1-2, January 2011.

36. Akihiro Yamada, Kenji Yasunaga, and Keisuke Tanaka. Quadratically secure oblivious transfer from strong one-way functions. *The 28th Symposium on Cryptography and Information Security (SCIS2011),* 1A2-2, January 2011.

37. Kenji Yasunaga. Laziness-resilient cryptography. *The 28th Symposium on Cryptography and Information Security (SCIS2011),* 1A1-5, January 2011.

38. Hitoshi Namiki, Kenji Yasunaga, and Keisuke Tanaka. On randomness leakage in public-key encryption. *IEICE Technical Report*, COMP2010–42, pages 23–28, December 2010.

39. Akinori Kawachi, Yoshio Okamoto, Keisuke Tanaka, and Kenji Yasunaga. Constant-round reconstruction for rational secret sharing. *IEICE Technical Report*, COMP2010–41, pages 15–21, December 2010.

40. Akinori Kawachi, Yoshio Okamoto, Keisuke Tanaka, and Kenji Yasunaga. Rational players avoid rational cryptographic protocols. *LA Symposium*, February 2010.

41. Hitoshi Namiki, Kenji Yasunaga, and Keisuke Tanaka. Public-key encryption resilient to randomness leakage. *The 27th Symposium on Cryptography and Information Security (SCIS2010)*, 1A1-3, January 2010.

42. Akinori Kawachi, Yoshio Okamoto, Keisuke Tanaka, and Kenji Yasunaga. One-round reconstruction for rational secret sharing. *The 27th Symposium on Cryptography and Information Security (SCIS2010)*, 3B2-1, January 2010.

43. Akihiro Yamada, Kenji Yasunaga, and Keisuke Tanaka. Weak oblivious transfer from strong one-way permutations. *The 27th Symposium on Cryptography and Information Security (SCIS2010)*, 3B2-2, January 2010.

44. Yuuki Tan, Kenji Yasunaga, and Keisuke Tanaka Non-malleability on trapdoors in public-key encryption with keyword search. *The 27th Symposium on Cryptography and Information Security (SCIS2010)*, 3A4-3, January 2010.

45. Kenji Yasunaga. List decoding for Reed-Muller codes and its application to polar codes. *The 32th Symposium on Information Theory and Its Applications (SITA2009)*, December 2009.

46. Yoshinori Ueda, Kenji Yasunaga, and Motohiko Isaka. One-dimensional signal sets for cryptographic protocol. *The 31st Symposium on Information Theory and Its Applications (SITA2008)*, October 2008.

47. Masafumi Tominaga, Kenji Yasunaga, and Toru Fujiwara. On distance distribution of a Reed-Solomon-like code for network coding. *IEICE Technical Report*, volume 108, number 158, IT2008–9, pages 7–10, July 2008. (in Japanese)

48. Kenji Yasunaga and Toru Fujiwara. A lower bound on the number of uncorrectable errors of weight half the minimum distance. *IEICE Technical Report*, IT2007–56, pages 51–56, February 2008.

49. Kenji Yasunaga and Toru Fujiwara. Minimum weight codewords in trial sets. In *Proceedings of the 30th Symposium on Information Theory and Its Applications (SITA2007)*, pages 56–64, December 2007.

50. Kenji Yasunaga and Toru Fujiwara. On trial set and uncorrectable errors for the first-order Reed-Muller codes. In *Proceedings of the 2007 Hawaii and SITA Joint Conference on Information Theory (HISC2007)*, pages 67–72, May 2007.

51. Tingting Liu, Kenji Yasunaga, and Toru Fujiwara. Error correction, detection using double encoding in digital watermarking. In *Proceedings of the 29th Symposium on Information Theory and Its Applications (SITA2006)*, pages 565–568, November 2006. (in Japanese)

52. Kenji Yasunaga and Toru Fujiwara. Correctable errors of weight half the minimum distance for the first-order Reed-Muller codes. In *Proceedings of the 29th Symposium on Information Theory and Its Applications (SITA2006)*, pages 5–8, November 2006.

53. Kenji Yasunaga and Toru Fujiwara. Local weight distribution of the (256, 93) third-order binary Reed-Muller code. In *Proceedings of the 2006 Hawaii, IEICE and SITA Joint Conference on Information Theory (HISC2006)*, May 2006, *IEICE Technical Report*, IT2006–6, pages 31–36, June 2006.

54. Takahiro Yasuda, Kenji Yasunaga, and Toru Fujiwara. Improvement of the Seguin lower bound using the local weight distribution. In *Proceedings of the 28th Symposium on Information Theory and Its Applications (SITA2005)*, pages 435–438, November 2005. (in Japanese)

55. Kenji Yasunaga and Toru Fujiwara. The local weight distributions of transitive invariant codes and their punctured codes. In *Proceedings of the 2005 Hawaii, IEICE and SITA Joint Conference on Information Theory (HISC2005)*, pages 79–84, May 2005.

56. Kenji Yasunaga and Toru Fujiwara. Relations among the local weight distributions of a linear block code, its extended code and its even weight subcode. In *Proceedings of the 27th Symposium on Information Theory and Its Applications (SITA2004)*, pages 559–562, December 2004.

57. Kenji Yasunaga and Toru Fujiwara. The local weight distributions of the (128,50) extended binary primitive BCH code and the (128,64) Reed-Muller code. *IEICE Technical Report*, IT2004-19, pages 7–12, July 2004.

58. Kenji Yasunaga and Toru Fujiwara. An algorithm for computing the local distance profile of binary linear codes closed under a group of permutations. *IEICE Technical Report*, IT2003-47, pages 37–41, September 2003.

Invited Talks at Workshops

1. Quantifying the Security Levels of Cryptographic Primitives. *2022 IEEE Region 10 Conference (TENCON 2022)*, Hong Kong and Online, November 2022.

2. A Theoretical Framework for Quantifying Security. *Workshop on Quantum Cryptography and Post-Quantum Cryptography*

3. Usefulness of Hellinger Distance in Cryptography. *IEEE Information Theory Workshop (ITW 2021), Invited Session*, Virtually from Kanazawa, Japan, October 2021.

4. Security of Cryptographic Primitives in the Perspective of Game Theory. *SCIE/SICE Tutorial Lectures*, July 2021.

5. Expander Graphs and Error-Correcting Codes. *Experimental Designs, Codes, and Combinatorics*, Yamaguchi, November 2019.

6. Game-Theoretic Approach to Cryptographic Primitives. *CRISMATH 2017*, AIST, December 2017.

7. Imperfect Randomness and Cryptography. *Autumn School on Cryptography*, Fujikawaguchiko, Yamanashi, September 2015.

8. Protocol Security and Game Theory. *IEICE Society Conference*, September 2015.

9. Correctability of Samplable Errors. *Cryptography Workshop*, Tokyo Institute of Technology, Ookayama, February 2015.

10. Game Theory and Cryptography. *ELC Autumn School on Cryptography*, Fujikawaguchiko, Yamanashi, September 2014.

11. Computational Fuzzy Extractors. *Cryptography Workshop*, Tokyo University, Kashiwa, March 2014.

12. Black-Box Constructions and Their Limitations. *ELC Autumn School on Cryptography*, Fujikawaguchiko, Yamanashi, September 2013.

13. Public-Key Encryption with Lazy Parties. *The 6th Workshop on Secure Constructions of Public-Key Encryption and Its Applications*, Tokyo, March 2013.

14. Two-Party Computation and Game Theory. *Cryptography Workshop*, Tokyo Institute of Technology, Ookayama, February 2013.

15. Game Theory and Cryptography. *ELC Autumn School on Cryptography*, Fujikawaguchiko, Yamanashi, September 2012.

16. Ciphertext Security in Public-Key Encryption. *Cryptography Workshop*, Tokyo Institute of Technology, Ookayama, February 2012.

17. Rational Secret Sharing with Constant-Round Reconstruction. *2011 Workshop "Secret Sharing and Cloud Computing"*, Fukuoka, June 2011.

18. Reed-Solomon Codes and Pseudorandomness. *IEICE Society Conference*, September 2010.

19. Performance Analysis of Error Correcting Codes. *IEICE Technical Committee on Theoretical Foundations of Computing*, March 2009.

Seminar Talks

1. Complexity of Explicit Constructions and Range Avoidance Problems. *Establishment of a new composition method for expander graphs and its application*, the Institute of Mathematics for Industry, Kyushu University, August 2022.

2. Insertions, Deletions, and Linear Codes. *9th Workshop on Error Correcting Codes*, Virtual, September 2020.

3. List Decoding for Insertions and Deletions. *7th Workshop on Error Correcting Codes*, Morioka, Iwate, September 2018.

4. Mathematics of Blockchains and Cryptocurrencies. *Kanazawa University Cryptography Seminar*, Kanazawa University, Kakuma Campus, June 2017.

5. Exploring the Limitations in Coding Theory. *ELC General Meeting*, Campus Innovation Center Tokyo, March 2017.

6. Bounds on the Rate of Correctable Deletions. *1st Workshop on Information Theory, Coding Theory and their Applications (ICA 2017)*, Karatsu, February 2017.

7. Construction of Codes Correcting Deletions Efficiently. Chiba University, Nishi-chiba Campus, October 2016.

8. Game-Theoretic Cryptography and Computational Coding Theory. The university of Tokyo, Hongo Campus, September 2016.

9. Exploring the Limitations in Coding Theory. *ELC General Meeting*, Campus Innovation Center Tokyo, May 2015.

10. Correctability of Samplable Errors. *3rd Kanazawa University Research Forum of Tenure-Track Faculty Members*, March 2015.

11. Error Correction in Computationally Bounded Channels. *3rd Workshop on Error Correcting Codes*, Tateyama, Chiba, September 2014.

12. Limitations of Cryptographic Primitives with Computational Restrictions. *ELC General Meeting*, Campus Innovation Center Tokyo, May 2014.

13. Error Correction in Computationally Bounded Channels. *6th Young Researchers Colloquium in Computational Complexity*, Yonezawa, Yamagata, September 2013.

14. Cryptographic Protocols and Game Theory. *Kyushu University Institute for Advanced Study/ISIT Colloquium*, Fukuoka, December 2012.

15. Public-Key Encryption with Lazy Parties. *IMI Cryptography Seminar*, Fukuoka, December 2012.

16. Public-Key Encryption with Lazy Parties. *Indo Japan Joint Workshop on Cryptography*, Fukuoka, November 2012.

17. A Game-Theoretic Perspective on Oblivious Transfer. *IMI Cryptography Seminar*, Fukuoka, May 2012.

18. Randomness Leakage in Public-Key Encryption. *IMI Cryptography Seminar*, Fukuoka, November 2011.

19. Public-Key Encryption with Lazy Parties. *4th Young Researchers Colloquium in Computational Complexity*, Nasu, Tochigi, September 2011.

20. List Decoding for Reed-Muller Codes and Its Application to Polar Codes. *1st Young Researchers Colloquium in Computational Complexity*, Kyoto University, April 2010.