Kenji Yasunaga

Last updated: February 20, 2017

Faculty of Electrical and Computer Engineering
Institute of Science and Engineering
Kanazawa University
Kakuma-machi, Kanazawa, 920-1192, Japan

Email: yasunaga@se.kanazawa-u.ac.jp
URL: http://yasunaga.w3.kanazawa-u.ac.jp/
Phone: +81 76 234 4896

Research Interests

Coding Theory, Cryptography, Computational Complexity.
Especially, pseudorandomness in coding theory and cryptography, and rationality in cryptography.

Employment

January 2013 – Present	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*

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

- Kasami Award, 2008.
- Society of Information Theory and Its Applications (SITA) Encouragement Award, 2007.

Professional Activities

- Guest Associate Editor, IEICE Transactions of Fundamentals of Electronics, Communications and Computer Sciences, Special Section on Information Theory and Its Applications, December 2015–present.
- 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–present.
- Guest Associate Editor, IEICE Transactions on Information and Systems, Special Section on Foundations of Computer Science ∼ Developments of the Theory on Algorithms and Computation ∼, February 2015–March 2016. January 2016–present.

- 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.
- Program Committee, the 39th Symposium on Information Theory and Its Applications (SITA2016).
- Program Committee, the Fourth International Symposium on Computing and Networking (CANDAR'16).
- Program Committee, the 3rd International Workshop on Information and Communication Security (WICS'16).
- Program Committee, the 38th Symposium on Information Theory and Its Applications (SITA2015).
- Program Committee, the 10th International Workshop on Security (IWSEC2015).
- Organizing Committee Chair, Workshop on Error-Correcting Codes 2017.
- Organizing Committee, the 15th International Conference on Applied Cryptography and Network Security (ACNS2017).
- Organizing Committee, Workshop on Error-Correcting Codes 2016.
- Organizing Committee, the 40th Symposium on Information Theory and Its Applications (SITA2016).
- Organizing Committee, the 9th International Conference on Provable Security (ProvSec2015).
- Organizing Committee, LA Symposium 2015.
- Organizing Committee, Workshop on Error-Correcting Codes 2015.
- Organizing Committee, the 35th Symposium on Information Theory and Its Applications (SITA2012).
- Organizing Committee, the 7th International Workshop on Security (IWSEC2012).

Teaching Experience

- Information and Computer System Engineering Laboratory 1 (C Language Programming and Algorithms), Kanazawa University, 2013–present.
- Information Security (Assistant), Kanazawa University, 2013–present.
- 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 16H01705, "Linear Development of Quantum Protocol Theory," with Takeshi Koshiba (Saitama University) and others, 2016–2020, ¥32,100,000.
- 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, ¥3,500,000.
- 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, ¥3,100,000.

- 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, ¥33,300,000.
- The Telecommunications Advancement Foundation, "Research on Leakage and Tamper Resilient Cryptographic Primitives," 2012, ¥1,250,000.
- 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, ¥3,900,000.
- 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, ¥2,800,000.
- 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, ¥2,530,000.

Publications

Papers in Refereed Journals

1. Akinori Kawachi, Yoshio Okamoto, Keisuke Tanaka, and Kenji Yasunaga. General constructions of rational secret sharing with expected constant-round reconstruction. *The Computer Journal*, to appear.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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. Kenji Yasunaga. Error-correcting codes against chosen-codeword attacks. In *Proceedings of the 9th International Conference on Information Theoretic Security (ICITS 2016)*.
2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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. 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 (SCIS2016),* 4A1-1, January 2017. (in Japanese)

2. 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 (SCIS2016),* 3F3-1, January 2017. (in Japanese)

3. 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 (SCIS2016),* 3B3-6, January 2017. (in Japanese)

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

5. 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)

6. 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)

7. 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)

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

9. 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)

10. 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)

11. 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)

12. 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)

13. 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)

14. 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.

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

16. 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)

17. 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)

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

19. 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)

20. 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.

21. 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.

22. 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.

23. 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)

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

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

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

31. 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.

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

33. 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.

34. 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.

35. 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.

36. 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.

37. 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.

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

39. 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)

40. 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.

41. 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.

42. 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.

43. 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)

44. 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.

45. 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.

46. 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)

47. 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.

48. 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.

49. 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.

50. 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. Imperfect randomness and cryptography. *Autumn School on Cryptography*, Fujikawaguchiko, Yamanashi, September 2015.

2. Protocol security and game theory. *IEICE Society Conference*, September 2015.

3. Correctability of samplable errors. *Cryptography Workshop*, Tokyo Institute of Technology, Ookayama, February 2015.

4. Game theory and cryptography. *ELC Autumn School on Cryptography*, Fujikawaguchiko, Yamanashi, September 2014.

5. Computational fuzzy extractors. *Cryptography Workshop*, Tokyo University, Kashiwa, March 2014.

6. Black-box constructions and their limitations. *ELC Autumn School on Cryptography*, Fujikawaguchiko, Yamanashi, September 2013.

7. Public-key encryption with lazy parties. *The 6th Workshop on Secure Constructions of Public-Key Encryption and Its Applications*, Tokyo, March 2013.

8. Two-party computation and game theory. *Cryptography Workshop*, Tokyo Institute of Technology, Ookayama, February 2013.

9. Game theory and cryptography. *ELC Autumn School on Cryptography*, Fujikawaguchiko, Yamanashi, September 2012.

10. Ciphertext security in public-key encryption. *Cryptography Workshop*, Tokyo Institute of Technology, Ookayama, February 2012.

11. Rational secret sharing with constant-round reconstruction. *2011 Workshop "Secret Sharing and Cloud Computing"*, Fukuoka, June 2011.

12. Reed-Solomon codes and pseudorandomness. *IEICE Society Conference*, September 2010.

13. Performance analysis of error correcting codes. *IEICE Technical Committee on Theoretical Foundations of Computing*, March 2009.

Seminar Talks

1. Construction of codes correcting deletions efficiently. Chiba University, Nishi-chiba Campus, October 2016.

2. Game-theoretic cryptography and computational coding theory. The university of Tokyo, Hongo Campus, September 2016.

3. Exploring the limitations in coding theory. *ELC General Meeting*, Campus Innovation Center Tokyo, May 2015.

4. Correctability of samplable errors. *The 3rd Kanazawa University Research Forum of Tenure-Track Faculty Members*, March 2015.

5. Error correction in computationally bounded channels. *The 3rd Workshop on Error Correcting Codes*, Tateyama, Chiba, September 2014.

6. Limitations of cryptographic primitives with computational restrictions. *ELC General Meeting*, Campus Innovation Center Tokyo, May 2014.

7. Error correction in computationally bounded channels. *The 6th Young Researchers Colloquium in Computational Complexity*, Yonezawa, Yamagata, September 2013.

8. Cryptographic protocols and game theory. *Kyushu University Institute for Advanced Study/ISIT Colloquium*, Fukuoka, December 2012.

9. Public-key encryption with lazy parties. *IMI Cryptography Seminar*, Fukuoka, December 2012.

10. Public-key encryption with lazy parties. *Indo Japan Joint Workshop on Cryptography*, Fukuoka, November 2012.

11. A game-theoretic perspective on oblivious transfer. *IMI Cryptography Seminar*, Fukuoka, May 2012.

12. Randomness leakage in public-key encryption. *IMI Cryptography Seminar*, Fukuoka, November 2011.

13. Public-key encryption with lazy parties. *The 4th Young Researchers Colloquium in Computational Complexity*, Nasu, Tochigi, September 2011.

14. List decoding for Reed-Muller codes and its application to polar codes. *The 1st Young Researchers Colloquium in Computational Complexity*, Kyoto University, April 2010.