安永 憲司（やすなが けんじ）

最終更新日： 2017 年 11 月 28 日

金沢大学 理工研究域 電子情報学系 助教

住所	920-1192 金沢市角間町
E-mail	yasunaga@se.kanazawa-u.ac.jp
URL	http://yasunaga.w3.kanazawa-u.ac.jp/
電話番号	076-234-4896

研究分野

符号理論，暗号理論，計算の複雑さ理論.
特に，符号理論や暗号理論における擬似ランダムネスの理論，ゲーム理論の視点による暗号理論.

職歴（専任）

平成 20 年 4 月 – 平成 20 年 9 月	関西学院大学 理工学研究科 ヒューマンメディア研究センター 博士研究員
平成 20 年 10 月 – 平成 23 年 9 月	東京工業大学 大学院情報理工学研究科 数理・計算科学専攻 特任助教 （グローバル COE「計算世界観の深化と展開」（代表：渡辺治） 特任助教を兼ねる）
平成 23 年 10 月 – 平成 24 年 12 月	（財）九州先端科学技術研究所 情報セキュリティ研究室 研究員
平成 25 年 1 月 – 現在	金沢大学 理工研究域 電子情報学系 助教

職歴（非常勤）

平成 22 年 4 月 – 平成 23 年 3 月	早稲田大学 教育学部 数学科 担当授業：応用数学５（符号理論入門），応用数学６（暗号理論入門）

学歴

平成 11 年 4 月　大阪大学 基礎工学部 情報科学科 入学
平成 15 年 3 月　大阪大学 基礎工学部 情報科学科 卒業
平成 15 年 4 月　大阪大学 大学院情報科学研究科 マルチメディア工学専攻 博士前期課程 入学
平成 17 年 3 月　大阪大学 大学院情報科学研究科 マルチメディア工学専攻 博士前期課程 修了
平成 17 年 4 月　大阪大学 大学院情報科学研究科 マルチメディア工学専攻 博士後期課程 入学
平成 20 年 3 月　大阪大学 大学院情報科学研究科 マルチメディア工学専攻 博士後期課程 修了

学位

平成 15 年 3 月　学士（工学） 大阪大学
平成 18 年 3 月　修士（情報科学） 大阪大学
平成 20 年 3 月　博士（情報科学） 大阪大学

受賞歴

平成 18 年　情報理論とその応用学会（SITA）奨励賞
平成 20 年　第 2 回嵩賞

教育歴

- オートマトンと数理言語論，補助講師，東京工業大学，2008–2010 年度.
- 計算の理論，補助講師，東京工業大学，2008–2010 年度.
- 計算量理論，補助講師，東京工業大学，2008–2010 年度.
- アルゴリズムとデータ構造，プログラミング演習担当，東京工業大学，2009–2011 年度.
- 応用数学５（符号理論入門），講師，早稲田大学，2010 年度.
- 応用数学６（暗号理論入門），講師，早稲田大学，2010 年度.
- 情報セキュリティ論，補助講師，金沢大学，2013 年度–現在.
- 情報システム工学実験第１（C 言語によるアルゴリズムの設計と実装），金沢大学，2013 年度–現在.

学会活動

- 論文誌編集
  - 電子情報通信学会 Special Section on Cryptography and Information Security 英文論文 小特集編集委員, 2012 年 1 月–2013 年 1 月, 2013 年 1 月–2014 年 1 月, 2014 年 1 月–2015 年 1 月, 2015 年 1 月–2016 年 1 月.
  - 電子情報通信学会 Special Section on Foundations of Computer Science ∼ Developments of the Theory on Algorithms and Computation ∼ 英文論文誌 小特集編集委員会, 2015 年 2 月–2016 年 3 月, 2016 年 1 月–2017 年 3 月.
  - 電子情報通信学会 Special Section on Discrete Mathematics and Its Applications 英文論文 小特集編集委員, 2015 年 7 月–2016 年 6 月, 2016 年 9 月–2017 年 9 月, 2017 年 8 月–現在 (編集幹事).
  - 電子情報通信学会 Special Section on Information Theory and Its Applications 英文論文 小特集編集委員, 2015 年 12 月–2016 年 12 月.
  - 電子情報通信学会 基礎・境界ソサイエティ論文誌 編集委員, 2017 年 6 月–現在.
- プログラム委員
  - The 10th International Workshop on Security (IWSEC2015), Program Committee.
  - 第 38 回情報理論とその応用シンポジウム (SITA2015), プログラム委員.
  - 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.
  - 第 39 回情報理論とその応用シンポジウム (SITA2016), プログラム委員.
  - 第 41 回情報理論とその応用シンポジウム（SITA2018），プログラム委員会幹事.
- 運営委員
  - The 7th International Workshop on Security (IWSEC2012), Organizing Committee.
  - 第 35 回情報理論とその応用シンポジウム（SITA2012），実行委員.
  - 誤り訂正符号のワークショップ 2015, 実行委員.
  - LA シンポジウム 2015, 実行委員.
  - The 9th International Conference on Provable Security (ProvSec2015), Organizing Committee.
  - 誤り訂正符号のワークショップ 2016, 実行委員.

– 第 39 回情報理論とその応用シンポジウム（SITA2016），実行委員.
– The 15th International Conference on Applied Cryptography and Network Security (ACNS2017), Organizing Committee.
– 誤り訂正符号のワークショップ 2017, 実行委員長.
– 情報処理学会 コンピュータセキュリティ研究運営委員会 運営委員, 2017 年 4 月–現在.
– 電子情報通信学会 情報セキュリティ研究専門委員会 専門委員, 2017 年 6 月–現在.
– 誤り訂正符号のワークショップ 2018, 実行委員.

外部獲得資金

- 「擬似ランダム性にもとづく性能のよい誤り訂正符号の構成に関する研究」日本学術振興会 科学研究費補助金 若手研究（スタートアップ）, 20860079，2008–2009 年度，研究代表者.
- 「誤り訂正符号に潜むランダムネスと構造の解明」日本学術振興会 科学研究費補助金 若手研究（B），23700010，2011–2013 年度，研究代表者.
- 「ゲーム理論にもとづく暗号プロトコル」日本学術振興会 科学研究費補助金 基盤研究（C）（一般），23500010，2011–2014 年度，研究分担者.
- 「情報漏洩や改竄に耐性のある暗号技術に関する研究」財団法人電気通信普及財団 研究調査助成金，2012 年度，研究代表者.
- 「量子プロトコル理論の深化」日本学術振興会 科学研究費補助金 基盤研究（A）（一般），24240001，2012–2016 年度，研究分担者.
- 「計算構造制限下での暗号技術の限界解明」文部科学省 科学研究費補助金 新学術領域研究 (研究領域提案型)，公募研究，25106509，2013–2014 年度，研究代表者.
- 「符号理論における計算限界の解明」文部科学省 科学研究費補助金 新学術領域研究 (研究領域提案型), 公募研究, 15H00851, 2015–1016 年度，研究代表者.
- 「量子プロトコル理論の線的展開」日本学術振興会 科学研究費補助金 基盤研究 （A）（一般）, 16H01705, 2016–2020 年度，研究分担者.
- 「インセンティブを考慮した暗号基盤技術の構築」日本学術振興会 科学研究費補助金 基盤研究 （B）（一般）, 17H01695, 2017–2020 年度，研究分担者.

研究業績

査読付き学術論文誌

1. 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.
2. 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.
3. 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.
4. 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.
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. 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.
7. 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.
8. 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.
9. 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.
10. Keita Inasawa, 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.

査読付き国際会議

1. 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.
2. 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.
3. 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, volume 4581, pages 110–119, December 2007.
4. 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.
5. 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.
6. 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, volume 6980, pages 34–51, October 2011.
7. 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, volume 6980, pages 309–323, October 2011.
8. 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, volume 7372, pages 29–42, July 2012.
9. 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 In-*

formation Security and Privacy (ACISP 2012), *Lecture Notes in Computer Science*, Springer, volume 7372, pages 208–222, July 2012.

10. 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, volume 7485, pages 411–425, September 2012.
11. 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.
12. 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, volume 8231, pages 303–318, November 2013.
13. 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.
14. 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.

解説論文・記事

1. 安永憲司. 符号理論の視点による擬似ランダム構造の統一的理解. **電子情報通信学会 基礎・境界ソサイエティ** *Fundamentals Review*, volume 5, number 1, 2011 年 7 月.
2. 安永憲司. 暗号とゲーム理論. **数学セミナー**, 日本評論社, volume 53, number 10, pages 25–29, 2014 年 10 月.
3. 安永憲司. 暗号におけるゲーム理論. **コンピュータソフトウェア**, volume 34, number 1, pages 81–92, 2017 年 1 月.

研究会等その他の発表

1. 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.
2. 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.
3. 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.
4. 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.
5. 安田 隆広, 安永 憲司, 藤原 融. Seguin 下界の局所重み分布を用いた改善. **第 *28* 回 情報理論とその応用シンポジウム** *(SITA2005)* **予稿集**, pages 435–438, 2005 年 11 月.
6. 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.
7. 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.

8. Tingting Liu, 安永憲司, 藤原融. 2 重符号化を用いた電子透かし抽出誤り訂正・検出法. **第 *29* 回 情報理論とその応用シンポジウム** *(SITA2006)* **予稿集**, pages 565–568, 2006 年 11 月.
9. 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.
10. 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.
11. 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.
12. 富永 昌文, 安永 憲司, 藤原 融. ネットワーク符号化におけるリード・ソロモン型符号の距離分布について. **電子情報通信学会 技術研究報告**, volume 108, number 158, IT2008-9, pages 7–10, 2008 年 7 月.
13. Yoshinori Ueda, Kenji Yasunaga, and Motohiko Isaka. One-dimensional signal sets for cryptographic protocol. In *Proceedings of the 31th Symposium on Information Theory and Its Applications (SITA2008)*, October 2008.
14. Kenji Yasunaga. List decoding for Reed-Muller codes and its application to polar codes. In *Proceedings of the 32th Symposium on Information Theory and Its Applications (SITA2009)*, December 2009.
15. Yuuki Tan, Kenji Yasunaga, and Keisuke Tanaka Non-malleability on trapdoors in public-key encryption with keyword search. *The 2010 Symposium on Cryptography and Information Security (SCIS2010)*, 3A4-3, January 2010.
16. Akihiro Yamada, Kenji Yasunaga, and Keisuke Tanaka. Weak oblivious transfer from strong one-way permutations. *The 2010 Symposium on Cryptography and Information Security (SCIS2010)*, 3B2-2, January 2010.
17. Akinori Kawachi, Yoshio Okamoto, Keisuke Tanaka, and Kenji Yasunaga. One-round reconstruction for rational secret sharing. *The 2010 Symposium on Cryptography and Information Security (SCIS2010)*, 3B2-1, January 2010.
18. Hitoshi Namiki, Kenji Yasunaga, and Keisuke Tanaka. Public-key encryption resilient to randomness leakage. *The 2010 Symposium on Cryptography and Information Security (SCIS2010)*, 1A1-3, January 2010.
19. Akinori Kawachi, Yoshio Okamoto, Keisuke Tanaka, and Kenji Yasunaga. Rational players avoid rational cryptographic protocols. *LA Symposium*, February 2010.
20. 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.
21. Hitoshi Namiki, Kenji Yasunaga, and Keisuke Tanaka. On randomness leakage in public-key encryption. *IEICE Technical Report*, COMP2010–42, pages 23–28, December 2010.
22. Kenji Yasunaga. Laziness-resilient cryptography. *The 28th Symposium on Cryptography and Information Security (SCIS2011),* 1A1-5, January 2011.
23. 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.
24. 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.
25. 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.
26. Hitoshi Namiki, Kenji Yasunaga, and Keisuke Tanaka. Randomness leakage in the KEM/DEM frame-

work. *The 28th Symposium on Cryptography and Information Security (SCIS2011),* 2A2-2, January 2011.

27. 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.
28. 肥後 春菜, 山田 章央, 安永 憲司, 田中 圭介. 紛失通信のゲーム理論的考察. **第 *29* 回 暗号と情報セキュリティシンポジウム** *(SCIS2012)*, 3B2-5, 2012 年 2 月.
29. 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.
30. Akinori Kawachi, Yoshio Okamoto, Keisuke Tanaka, and Kenji Yasunaga. Rational secret sharing for non-simultaneous channels. *IEICE Technical Report*, IT2012–8, pages 41–46, 2012.
31. 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.
32. 安永 憲司. 合理的な秘密分散における不可能性とその回避方法. **コンピュータセキュリティシンポジウム** *2012 (CSS2012)*, 1C2-1, 2012 年 10 月.
33. 安永 憲司. 効率的に計算可能な加法的誤りの訂正可能性. **第 *35* 回 情報理論とその応用シンポジウム** *(SITA2012)*, 2012 年 12 月.
34. 肥後 春菜, 安永 憲司, 田中 圭介. 二者間プロトコルのゲーム理論的な安全性に向けて. **第 *30* 回 暗号と情報セキュリティシンポジウム** *(SCIS2013)*, 3B3-3, 2013 年 1 月.
35. 肥後 春菜, 安永 憲司, 田中 圭介. コミットメントのゲーム理論的安全性. **第 *30* 回 暗号と情報セキュリティシンポジウム** *(SCIS2013)*, 3C3-4, 2013 年 1 月.
36. 肥後 春菜, 安永 憲司, 田中 圭介. 二者間計算とゲーム理論. *LA* **シンポジウム**, 2013 年 1 月.
37. 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.
38. 湯澤 孝介, 安永 憲司, 満保 雅浩. ユーザビリティ向上のための部分的パスワード共有による影響. **第 *32* 回 暗号と情報セキュリティシンポジウム** *(SCIS2015)*, 2C1-3, 2015 年 1 月.
39. 高橋 寛弥, 安永憲司, 満保雅浩. cookie 漏洩に起因する被害の低減手法の構築と考察. **第 *32* 回 暗号と情報セキュリティシンポジウム** *(SCIS2015)*, 3E1-2, 2015 年 1 月.
40. 稲澤 啓太, 安永 憲司, 満保 雅浩. 検証者が報酬を下げることができない合理的な証明. **第 *32* 回 暗号と情報セキュリティシンポジウム** *(SCIS2015)*, 3D3-4, 2015 年 1 月.
41. 池田 光晴, 安永憲司, 満保雅浩. 計算量的なエントロピー安全性に関する考察. **第 *32* 回 暗号と情報セキュリティシンポジウム** *(SCIS2015)*, 4F1-1, 2015 年 1 月.
42. 西野 卓也, 安永 憲司, 満保 雅浩. エントロピープール付き擬似乱数生成器の性能分析. **第 *32* 回 暗号と情報セキュリティシンポジウム** *(SCIS2015)*, 4E2-4, 2015 年 1 月.
43. 稲澤 啓太, 安永 憲司, 満保 雅浩. 合理的な検証者に対する合理的な証明. *LA* **シンポジウム**, 2015 年 7 月.
44. 越中谷 隼人, 安永 憲司, 満保 雅浩. 難読化技術を用いたサインディクリプション方式の構成. *2016* **年 暗号と情報セキュリティシンポジウム** *(SCIS2016)*, 2C3-2, 2016 年 1 月.
45. 稲澤 啓太, 安永 憲司, 満保 雅浩. 検証者の不正を防ぐ合理的な証明とその委託計算への応用. *2016* **年 暗号と情報セキュリティシンポジウム** *(SCIS2016)*, 3A3-2, 2016 年 1 月.
46. 湯澤 孝介, 安永 憲司, 満保 雅浩. 繰り返しゲームを用いた乱数生成のインセンティブに関する考察. *2016* **年 暗号と情報セキュリティシンポジウム** *(SCIS2016)*, 3A3-4, 2016 年 1 月.
47. 安永 憲司. サンプル可能な誤りの効率的な訂正可能性について. *LA* **シンポジウム**, 2016 年 1 月.
48. 福嶋 雄也, 小杉 友晃, 安永 憲司, 満保 雅浩. 匿名化に用いられる安全性指標の比較評価. *2017* **年 暗号と情報セキュリティシンポジウム** *(SCIS2017)*, 3B3-6, 2017 年 1 月.
49. 稲澤 啓太, 越中谷 隼人, 安永 憲司, 満保 雅浩. 非許可型コンセンサスプロトコルの不可能性に関する考察. *2017* **年 暗号と情報セキュリティシンポジウム** *(SCIS2017)*, 3F3-1, 2017 年 1 月.
50. 林 智弘, 安永 憲司, 満保 雅浩. 量子攻撃者に対する決定性暗号方式の安全性. *2017* **年 暗号と情報セキュリ**

ティシンポジウム *(SCIS2017)*, 4A1-1, 2017 年 1 月.

招待講演

1. 誤り訂正符号の訂正能力分析. **電子情報通信学会コンピュテーション研究会**, 2009 年 3 月.
2. Reed-Solomon 符号と擬似ランダム性. **電子情報通信学会ソサイエティ大会**, 2010 年 9 月.
3. Rational Secret Sharing with Constant-Round Reconstruction. *2011 Workshop "Secret Sharing and Cloud Computing"*, 九州大学伊都キャンパス, 2011 年 6 月.
4. 公開鍵暗号における暗号文の安全性. *CompView* **暗号理論ワークショップ**, 東工大蔵前会館, 2012 年 2 月.
5. ゲーム理論と暗号理論. *ELC* **暗号理論秋学校**, 河口湖セントビレッヂ, 山梨県南都留郡富士河口湖町, 2012 年 9 月.
6. 二者間プロトコルとゲーム理論. **暗号理論ワークショップ**, 東京工業大学大岡山キャンパス, 2013 年 2 月.
7. なまけもの暗号. **第** *6* **回公開鍵暗号の安全な構成とその応用ワークショップ**, 筑波大学東京キャンパス文京校舎, 2013 年 3 月.
8. ブラックボックス構成とその限界. *ELC* **暗号理論秋学校**, 河口湖セントビレッヂ, 山梨県南都留郡富士河口湖町, 2013 年 9 月.
9. 計算量的ファジィ抽出器. **暗号理論ワークショップ**, 東京大学柏キャンパス, 2014 年 3 月.
10. ゲーム理論と暗号. *ELC* **暗号理論秋学校**, 河口湖セントビレッヂ, 山梨県南都留郡富士河口湖町, 2014 年 9 月.
11. サンプル可能な誤りの訂正可能性. **暗号理論ワークショップ**, 東京工業大学大岡山キャンパス, 2015 年 2 月.
12. プロトコルの安全性とゲーム理論, **電子情報通信学会ソサイエティ大会**, 2015 年 9 月.
13. 不完全な乱数と暗号, **暗号理論秋学校**, 河口湖セントビレッヂ, 山梨県南都留郡富士河口湖町, 2015 年 9 月

セミナー等での講演

1. List decoding for Reed-Muller codes and its application to polar codes. **第一回計算量理論若手の会**, 京都大学吉田キャンパス, 2010 年 4 月.
2. なまけもの暗号. **第四回計算量理論若手の会**, ホテルグリーンパール那須, 栃木県那須郡那須町, 2011 年 9 月.
3. Randomness leakage in public-key encryption. *IMI* **暗号学セミナー**, 九州大学伊都キャンパス, 2011 年 11 月.
4. A game-theoretic perspective on oblivious transfer. *IMI* **暗号学セミナー**, 九州大学伊都キャンパス, 2012 年 5 月.
5. Public-key encryption with lazy parties. **インド-日本研究交流暗号ワークショップ**, 九州先端科学技術研究所, 2012 年 11 月.
6. Public-key encryption with lazy parties. *IMI* **暗号学セミナー**, 九州大学伊都キャンパス, 2012 年 12 月.
7. 暗号プロトコルとゲーム理論. **九州大学高等研究院/九州先端科学技術研究所 研究交流会**, 九州大学伊都キャンパス, 2012 年 12 月.
8. Error correction in computationally bounded channels. **第六回計算量理論若手の会**, 米沢旅館春木屋, 山形県米沢市, 2013 年 9 月.
9. 計算構造制限下での暗号技術の限界解明, *ELC* **平成** *26* **年度第** *1* **回領域会議**, 東京工業大学キャンパスイノベーションセンター, 2014 年 5 月.
10. 計算量制限通信路における誤り訂正, **第** *3* **回 誤り訂正符号のワークショップ**, 千葉県館山市鳩山荘松庵, 2014 年 9 月.
11. サンプル可能な誤りの訂正可能性. **第** *3* **回 金沢大学テニュア・トラック教員研究成果発表会**, 2015 年 3 月.
12. 符号理論における計算限界の解明. *ELC* **平成** *27* **年度第** *1* **回領域会議**, 東京工業大学キャンパスイノベー

ションセンター, 2015 年 5 月.

13. ゲーム理論的な暗号理論と計算量的な符号理論. 東京大学 本郷キャンパス, 2016 年 9 月.
14. 削除誤りを効率的に訂正する符号の構成法. 千葉大学 西千葉キャンパス, 2016 年 10 月.
15. 訂正可能な削除割合の限界. **第 *1* 回情報理論および符号理論とその応用ワークショップ**, 佐賀県唐津市, 2017 年 2 月.
16. 符号理論における計算限界の解明. *ELC* **平成 *28* 年度第 *2* 回領域会議**, 東京工業大学キャンパスイノベーションセンター, 2017 年 3 月.
17. ブロックチェーン・暗号通貨の数理. **金沢大学暗号理論勉強会**, 金沢大学角間キャンパス, 2017 年 6 月.