List of Publications

Mitsugu Iwamoto,
Last modified: 1st, October, 2018.

— *Refereed Journal* —

[1] A. Espejel-Trujillo, M. Iwamoto, and M. Nakano-Miyatake, "A Proactive Secret Image Sharing Scheme with Resistance to Machine Learning Based Steganalysis," *Multimedia Tools And Applications*, vol. 77, issue 12, pp. 15161—15179, Springer, June 2018. DOI: `https://doi.org/10.1007/s11042-017-5097-8`.

[2] M. Iwamoto, K. Ohta, and J. Shikata, "Security Formalizations and Their Relationships for Encryption and Key Agreement in Information-Theoretic Cryptography," *IEEE Trans. Information Theory*, vol. 64, issue 1, pp. 654–685, 2018. DOI: `https://doi.org/10.1109/TIT.2017.2744650`

[3] R. Yashiro, T. Sugawara, M. Iwamoto, and K. Sakiyama, "Q-class Authentication System for Double Arbiter PUF," *IEICE Trans. on Fundamentals*, vol.E101–A, no.1, pp. 129–137, Jan., 2018. DOI: `https://doi.org/10.1587/transfun.E101.A.129`.

[4] T. Machida, D. Yamamoto, M. Iwamoto, and K. Sakiyama, "A New Arbiter PUF for Enhancing Unpredictability on FPGA," *The Scientific World Journal*, Volume 2015, Article ID 864812, 13 pages, doi: `http://dx.doi.org/10.1155/2015/864812`, 2015.

[5] D. Yamamoto, K. Sakiyama, M. Iwamoto, K. Ohta, M. Takenaka, K. Itoh, and N. Torii, "A new method for enhancing variety and maintaining reliability of PUF responses and its evaluation on ASICs," *J. Cryptographic Engineering*, Volume 5, Issue 3 , pp 187–199, 2015.

[6] 中曽根俊貴，李陽，岩本貢，太田和夫，崎山一男，"クロック間衝突を漏洩モデルとする新たなサイドチャネル解析と並列実装 AES 暗号ハードウェアにおける弱い鍵，" 電子情報通信学会論文誌 A, vol.J97–A, No.11, pp.695–703, 2014.

[7] K. Sakiyama, Y. Li, S. Gomisawa, Y. Hayashi, M. Iwamoto, N. Homma, T. Aoki, and K. Ohta, "Practical DFA Strategy for AES Under Limited-Access Conditions," *Journal of Information Processing*, vol. 55, No. 2, pp142–151, 2014.

[8] D. Yamamoto, K. Sakiyama, M. Iwamoto, K. Ohta, M. Takenaka, and K. Itoh, "Variety enhancement of PUF responses using the locations of random outputting RS latches," *Journal of Cryptographic Engineering*, vol. 3, issue 4, pp.197–211, Nov., 2013.

[9] M. Iwamoto, H. Koga, and H. Yamamoto, "Coding theorems for a $(2, 2)$–threshold scheme with detectability of impersonation attacks," *IEEE Trans. on Information Theory*, vol.58, no.9, pp.6194–6206, 2012. Preprint is available from `http://arxiv.org/abs/1004.4530v3`.

[10] A. E. Torujillo, M. N. Miyatake, M. Iwamoto, and H. P. Maena, "A cheating prevention EVC scheme using watermarking techniques," *Revista Facultad de Ingeniería, Univ. Antioquia*, no.63, pp. 30–42, June, 2012.

[11] M. Iwamoto, "A weak security notion for visual secret sharing schemes," *IEEE Trans. on Information Forensics and Security*, vol. 7, no. 2, pp. 372–382, 2012.

[12] K. Sakiyama, Y. Li, M. Iwamoto, and K. Ohta, "Information-Theoretic Approach to Optimal Differential Fault Analysis," *IEEE Trans. on Information Forensics and Security*, vol.7, issue 1, pp.109–120, 2012.

[13] M. Iwamoto, H. Yamamoto, and H. Ogawa, "Optimal multiple assignments based on integer programming in secret sharing schemes with general access structures," *IEICE Trans. on Fundamentals*, vol.E90–A, no.1, pp.101–112, 2007. Preprint is available from `http://arxiv.org/abs/cs.CR/0506064`.

[14] M. Iwamoto, L. Wang, K. Yoneyama, N. Kunihiro, and K. Ohta, "Visual secret sharing schemes for multiple secret images allowing the rotation of shares," *IEICE Trans. on Fundamentals*, vol.E89–A, no.5, pp.1382–1395, 2006.

[15] M. Iwamoto and H. Yamamoto, "Strongly secure ramp secret sharing schemes for general access structures," *Information Processing Letters*, vol.97, issue 2, pp.52–57, 2006. Preprint is available from `http://arxiv.org/abs/cs.CR/0506065`.

[16] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto, "Quantum Secret Sharing Schemes and Reversibility of Quantum Operations," *Physical Review A* **72**, 032318, 2005.

[17] M. Iwamoto and H. Yamamoto, "A construction method of visual secret sharing schemes for plural secret images," *IEICE Trans. on Fundamentals*, vol.E86–A, no.10, pp.2577–2588, 2003.

[18] M. Iwamoto and H. Yamamoto, "The optimal n-out-of-n visual secret sharing scheme for gray-scale images," *IEICE Trans. on Fundamentals*, vol.E85–A, no.10, pp.2238–2247, Oct., 2002

[19] H. Koga, M. Iwamoto and H. Yamamoto, "An analytic construction of the visual secret sharing scheme for color images," *IEICE Trans. on Fundamentals*, vol.E84–A, no.1, pp.262–272, Jan., 2001.

— *Survey Papers, Translations, Books* —

[20] 「数学ゲーム必勝法」小林欣吾，佐藤創（監訳），共立出版，2016. (原著 : Elwyn R. Berlekamp, John H. Conway, Richard K. Guy, "Winning Ways for Your Mathematical Plays," A K Peters/CRC Press, 2001.)，第 1 巻 第 5 章の翻訳を担当.

[21] 「暗号王になる」子供の科学，pp. 11–21，誠文堂新光社（太田和夫教授との取材協力）, 2016 年 11 月号.

[22] 「情報理論 —基礎と広がり—」 山本 博資，古賀 弘樹，有村 光晴，岩本貢（訳），共立出版, 2012. (原著 : Thomas M. Cover and Joy A. Thomas: The Elements of Information Theory, 2nd. ed. Wiley–InterScience, 2006. 担当 : 第 4, 11, 16, 17 章)

[23] M. Nakano, E. Escamilla, H. Pérez, and M. Iwamoto, "Threshold Based Visual Cryptography: A Tutorial Review," Información Tecnológica, vol.22–5, pp.107–120, 2011 (in Spanish).

[24] 電子情報通信学会編「知識ベース」，第一群, 第一編 13.3 節「秘密分散」（分担執筆），オーム社，2010（校正中）.

— *International Conferences and Workshops (Invited)* —

[25] M. Iwamoto, "Secret sharing schemes under guessing secrecy," *Cryptographic Technologies for Securing Network Storage and Their Mathematical Modeling*, MI Lecture Notes, Kyushu University, 2017.

[26] M. Iwamoto, "Security notions of visual secret sharing schemes," *International Workshop on Advanced Image Technology (IWAIT2013)*, pp.95–100, Jan., 2013.

— *International Conferences (with Review)* —

[27] Y. Watanabe, Y. Kuroki, S. Suzuki, Y. Koga, M. Iwamoto, and K. Ohta, "Card-Based Majority Voting Protocols with Three Inputs Using Three Cards," *International Symposium on Information Theory And Its Applications (ISITA2018)*, Oct., 2018, to appear.

[28] M. Iwamoto, "Worst-case guessing secrecy is meaningful in secret sharing schemes," *ICITS2017 (workshop track)*, Dec., 2017.

[29] T. Nakai, S. Shirouchi, M. Iwamoto and K. Ohta, "Four cards are enough for card-based three-input voting protocol utilizing private permutations," *ICITS2017 (conference track)*, LNCS 10681, pp. 153–165, 2016.

[30] T. Nakai, Y. Misawa, Y. Tokushige, M. Iwamoto, and K. Ohta, "Efficient Card-based Cryptographic Protocols for Millionaires' Problem Utilizing Private Permutations," *CANS2016*, LNCS 10052, pp. 350–364, 2016.

[31] K. Hayasaka, Y. Kawai, Y. Koseki, T. Hirano, K. Ohta, and M. Iwamoto, "Probabilistic Generation of Trapdoors: Reducing Information Leakage of Searchable Symmetric Encryption," *CANS2016*, LNCS 10052, pp. 500–517, 2016.

[32] T. Hirano, M. Hattori, Y. Kawai, N. Matsuda, M. Iwamoto, K. Ohta, Y. Sakai, and T. Munaka, "Simple, Secure, and Efficient Searchable Symmetric Encryption with Multiple Encrypted Indexes," *IWSEC 2016*, LNCS 9836, pp.91–110, 2016.

[33] R. Yashiro, T. Machida, M. Iwamoto, and K. Sakiyama, "Deep-Learning-Based Security Evaluation on Authentication Systems Using Arbiter PUF and Its Variants," *IWSEC 2016*, LNCS 9836, pp.267–285, 2016.

[34] Y. Kamoshida, M. Iwamoto, and K. Ohta, "Application of Joux-Lucks Search Algorithm for Multi-Collisions to MicroMint," *IWSEC2016 (poster session)*, 2016.

[35] T. Nakai, Y. Tokushige, M. Iwamoto and K. Ohta, "Toward Reducing Shuffling in Card-based Cryptographic Protocol for Millionaire Problem," *International Workshop on Information Security (IWSEC2015)*, (poster session), August, 2015.

[36] Y. Misawa, Y. Tokushige, M. Iwamoto and K. Ohta, "Comparison of Security on Coded Signs with Public/Private Code Book ," *International Workshop on Information Security (IWSEC2015)*, (poster session), August, 2015.

[37] M. Iwamoto and J. Shikata, "Construction of symmetric-key encryption with guessing secrecy," *IEEE International Symposium on Information Theory (ISIT2015)*, June, pp.725–729, 2015.

[38] T. Machida, D. Yamamoto, M. Iwamoto, and K. Sakiyama, "Implementation of Double Arbiter PUF and Its Performance Evaluation on FPGA," *20th Asia and South Pacific Design Automation Conference (ASP-DAC 2015)*, pp.6–7, 2015.

[39] T. Nishide, M. Iwamoto, A. Iwasaki, and K. Ohta, "Secure $(M+1)$st-Price Auction with Automatic Tie-Break," *The 6th International Conference on Trustworthy Systems (InTrust2014)*, LNCS 9473, pp. 422–436, 2015.

[40] M. Iwamoto, T. Omino, Y. Komano, and K. Ohta, "A New Model of Client–Server Communications under Information Theoretic Security," *IEEE Information Theory Workshop (ITW2014)*, pp. 512–516, November 5th, 2014.

[41] P. Lumyong, M. Iwamoto, and K. Ohta, "Cheating on a Visual Secret Sharing Scheme under a Realistic Scenario," *International Symposium on Information Theory and Its Applications (ISITA2014)*, pp. 546–550, October 29th, 2014.

[42] T. Machida, D. Yamamoto, M. Iwamoto, and K. Sakiyama, "A New Mode of Operation for Arbiter PUF to Improve Uniqueness on FPGA," *1st Workshop on Emerging Aspects in Information Security (EAIS'14)*, in *The Federated Conference on Coputer Science and Information Systems (FedCSIS)*, pp.877–884, September, 2014.

[43] M. Iwamoto and J. Shikata, "Secret Sharing Schemes Based on Min-entropies," *IEEE International Symposium on Information Theory (ISIT2014)*, pp.401–405, 2014. Full version: `http://arxiv.org/abs/1401.5896/` [67].

[44] K. Ohara, Y. Sakai, F. Yoshida, M. Iwamoto, and K. Ohta, "Privacy-Preserving Smart Metering with Verifiability for Both Billing and Energy Management," *The 2nd ACM ASIA Public-Key Cryptography Workshop (ASIAPKC2014)* , pp. 23–32, 2014.

[45] Y. Sasaki, Y. Tokushige, L. Wang, M. Iwamoto, and K. Ohta, "An Automated Evaluation Tool for Improved Rebound Attack: New ShiftBytes Parameters for Grøstl," Proc. of *CT-RSA2014*, LNCS 8366, pp.424–443, 2014.

[46] M. Iwamoto, T. Peyrin, and Y. Sasaki, "Limited-birthday distinguishers for hash functions—collisions beyond the birthday bound can be meaningful," *Proc. of ASIACRYPT2013*, LNCS8269, vol. 2, pp.505–523, 2013. Eprint is available from `http://eprint.iacr.org/2013/611` [68].

[47] M. Iwamoto and J. Shikata, "Information theoretic security for encryption based on conditional Rényi entropies," *Proc. of International Conference on Information Theoretic Security (ICITS)*, pp.101–121, LNSC8317, Springer-Verlag, 2013. Available from `http://eprint.iacr.org/2013/440` [69].

[48] T. Machida, T. Nakasone, M. Iwamoto, and K. Sakiyama, "A New Model of Modeling Attacks against Arbiter PUF on FPGA," *IWSEC2013*, November, 2013 (Poster Session).

[49] Y. Sasaki, W. Komatsubara, Y. Sakai, L. Wang, M. Iwamoto, K Sakiyama and K. Ohta, "Meet-in-the-Middle Preimage Attacks Revisited: New Results on MD5 and HAVAL," *SECRYPT2013*, pp.111–122, July, 2013.

[50] T. Nakasone, Y. Li, Y. Sasaki, M. Iwamoto, K. Ohta, and K. Sakiyama, "Key-Dependent Weakness of AES-Based Ciphers Under Clockwise Collision Distinguisher," *International Conference on Information Security and Cryptography (ICISC2012)*, LNCS7839, pp.395–409, Dec., 2012.

[51] K. Ohara, Y. Sakai, M. Iwamoto, and K. Ohta, "A t-resilient Unconditionally Secure First-Price Auction Protocol," *IWSEC2012* (poster session), Nov., 2012.

[52] D. Yamamoto, K. Sakiyama, M. Iwamoto, K. Ohta, T. Ochiai, M. Takenaka, and K. Itoh, "Uniqueness Enhancement of PUF Responses Based on the Locations of Random Outputting RS Latches," *CHES2011*, LNCS6917, pp.391–406, October, 2011.

[53] M. Iwamoto and K. Ohta, "Security Notions for Information Theoretically Secure Encryptions," *IEEE–ISIT 2011*, pp.1743–1747, 2011. Available from `http://arxiv.org/abs/arXiv:1106.1731v1`.

[54] M. Iwamoto and K. Ohta, "Variations of Information Theoretic Security Notions," *7-th Asia-Europe Workshop on Information Theory (AEW7)*, pp.73–76, July, 2011.

[55] A. Espejel-Trujillo, M. Nakano-Miyatake, and M. Iwamoto, "Visual Secret Sharing Schemes for Multiple Secret Images Including Shifting Operation of Shares," *6th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE 2009)*, pp.433–438, November, 2009.

[56] H. Koga, M. Iwamoto, and H. Yamamoto, "Coding Theorems for a $(2, 2)$–Threshold Scheme Secure against Impersonation by an Opponent," *IEEE-ITW 2009*, pp.188–192, Oct., 2009.

[57] M. Iwamoto, H. Yamamoto, and H. Koga, "A coding theorem for cheating-detectable $(2, 2)$-threshold blockwize secret sharing schemes," *IEEE-ISIT 2009*, pp.1308–1312, June–July, 2009.

[58] M. Iwamoto, "Weakly secure visual secret sharing schemes," *ISITA 2008*, pp.42–47, Dec., 2008.

[59] M. Iwamoto, L. Wang, K. Yoneyama, N. Kunihiro, and K. Ohta, "A remark on visual secret sharing schemes allowing the rotation of shares," *5-th Asia-Europe Workshop on Information Theory (AEW5)*, pp.37–42, October, 2006.

[60] M. Iwamoto and H. Yamamoto, "Strongly secure ramp secret sharing schemes," *IEEE-ISIT 2005*, pp.1221–1225, Sept., 2005.

[61] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto, "Quantum secret sharing schemes and reversibility of quantum operations," *ISITA 2004*, pp.1440–1445, Oct., 2004.

[62] M. Iwamoto, H. Yamamoto, and H. Ogawa, "Optimal Multiple Assignments Based on Integer Programming in Secret Sharing Schemes," *IEEE-ISIT 2004*, p.16, June–July, 2004.

[63] M. Iwamoto and H. Yamamoto, "A construction method of visual secret sharing schemes for plural secret images," *IEEE-ISIT 2003*, p.283, June–July, 2003.

[64] M. Kondo, M. Iwamoto and H. Nakamura, "Cache line impact on 3D PDE solvers," *Proceeding of ISHPC 2002*, LNCS 2327, pp.301–309, Springer-Verlag, Oct., 2002.

— International Conferences (without Review) —

[65] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto, "Quantum Ramp Secret Sharing Schemes," *The 2004 workshop on information security research supported by MEXT Grant-in-aid scientific research on proiority area, "informatics,"* presentation no.13, Tokyo, Japan, 2004.

— Preprints —

[66] M. Iwamoto, K. Ohta and J. Shikata, "Security Formalizations and Their Relationships for Encryption and Key Agreement in Information-Theoretic Cryptography," arXiv: 1410.1120, available from `http://arxiv.org/abs/1410.1120`, 2014.

[67] M. Iwamoto and J. Shikata, "Secret sharing schemes based on min-entropies," arXiv: 1401.5896, available from `http://arxiv.org/abs/1401.5896`, 2014. (full version of [43]).

[68] M. Iwamoto, T. Peyrin, and Y. Sasaki, "Limited-birthday distinguishers for hash functions—collisions beyond the birthday bound can be meaningful," *IACR Cryptology ePrint Archive*, available from `http://eprint.iacr.org/2013/611`, appeared at *ASIACRYPT2013* [46].

[69] M. Iwamoto and J. Shikata, "Information Theoretic Security for Encryption Based on Conditional Rényi Entropies," *IACR Cryptology ePrint Archive*, available from `http://eprint.iacr.org/2013/440`, to appear at *ICITS2013* [47].

[70] M. Iwamoto and K. Ohta, "Security Notions for Information Theoretically Secure Encryptions," Available from http://arxiv.org/abs/arXiv: 1106.1731v1. Appeared at *IEEE–ISIT 2011*, pp.1743–1747, 2011. [53].

[71] M. Iwamoto, H. Koga, and H. Yamamoto, "Coding theorems for a $(2, 2)$–threshold scheme with detectability of impersonation attacks," available from http://arxiv.org/abs/1004.4530v3. Appeared at *IEEE Trans. on Information Theory*, vol.58, no.9, pp.6194–6206, 2012 [9].

[72] M. Iwamoto, H. Yamamoto, and H. Ogawa, "Optimal multiple assignments based on integer programming in secret sharing schemes with general access structures," available from http://arxiv.org/abs/cs.CR/0506064. Appeared at *IEICE Trans. on Fundamentals*, vol.E90–A, no.1, pp.101–112, 2007 [13].

[73] M. Iwamoto and H. Yamamoto, "Strongly secure ramp secret sharing schemes for general access structures," available from http://arxiv.org/abs/cs.CR/0506065. Appeared at *Information Processing Letters*, vol.97, issue 2, pp.52–57, 2006 [15].

— *Domestic Conferences / Workshops (Invited)* —

[74] 岩本貢，"秘密計算の安全性～プライバシーを保ちつつどこまで計算できるか," **第 8 回バイオメトリクスと認識・認証シンポジウム**, Nov., 2018.

[75] 岩本貢，"情報理論的安全性 —さまざまな視点から—," **誤り訂正符号のワークショップ**（入門講演）, 山口県湯田温泉, September, 2017.

[76] 岩本貢，"秘密分散法と視覚復号型秘密分散法—共通点と相違点," **電子情報通信学会マルチメディア情報ハイディング・エンリッチメント研究会**（チュートリアル講演）, EMM2014–7 , pp. 35–40, May, 2014.

[77] 岩本貢，佐々木悠，"ハッシュ関数に対する制限付き誕生日識別攻撃—誕生日下界を上回る衝突攻撃の識別攻撃に対する有効性," **電子情報通信学会情報セキュリティ研究会**, ISEC2014–7, p. 49, May, 2014.

[78] 岩本貢，四方順司, "最小エントロピーに基づく秘密分散法," **暗号理論ワークショップ**, March, 2014.

[79] M. Iwamoto and J. Shikata, "Information Theoretic Cryptography based on Conditional Rényi Entropies," **暗号理論ワークショップ**, March, 2013.

[80] 山本大, 崎山一男, 岩本貢, 太田和夫, 落合隆夫, 武仲正彦, 伊藤孝一, "Uniqueness Enhancement of PUF Responses Based on the Locations of Random Outputting RS Latches," **電子情報通信学会情報セキュリティ研究会**, ISEC2011–68, p.29, 2011.

[81] 大原一真，坂井祐介，岩本貢，太田和夫，"二つの情報理論的安全なオークションプロトコル," **CompView 暗号理論ワークショップ**, Feb., 2012.

[82] M. Iwamoto and A. Russell, "関数に対する entropic security の安全性," **CompView 暗号理論ワークショップ**, Feb., 2012.

[83] M. Iwamoto and A. Russell, "Entropic Security for Predicates and Functions," 統計数理研究所共同利用研究集会（エルゴード理論，情報理論，計算機科学とその周辺）, March, 2012.

[84] 岩本貢, 太田 和夫, " 情報理論的に安全な暗号化のための安全性概念," **CompView 暗号理論ワークショップ**, Feb., 2011.

[85] 岩本貢, "秘密分散法に対する符号化定理," **電子情報通信学会 ソサイエティ大会 チュートリアル講演「情報理論的暗号理論」**, AT-1-4, Sept., 2006.

[86] 駒野雄一, 岩本 貢, 太田和夫, 崎山 一男, “PUF 応用に向けた新たな物理仮定と端末認証方式への応用,” **暗号と情報セキュリティシンポジウム** (SCIS2018), 2D1-1, 24th, Jan., 2018.

[87] 鈴木慎之介, 渡邉洋平, 岩本 貢, 太田和夫, “ロバスト秘密分散法 CFOR 方式における精密な安全性解析,” **暗号と情報セキュリティシンポジウム** (SCIS2018), 2A3-3, 24th, Jan., 2018.

[88] 黒木慶久, 古賀優太, 渡邉洋平, 岩本 貢, 太田和夫, “3 枚のカードで実現可能な 3 入力多数決プロトコル,” **暗号と情報セキュリティシンポジウム** (SCIS2018), 3B1-4, 24th, Jan., 2018.

[89] 古賀優太, 鈴木 慎之介, 渡邉 洋平, 岩本 貢, 太田 和夫, “カードを用いた複数人でのマッチングプロトコル,” **暗号と情報セキュリティシンポジウム** (SCIS2018), 3B1-5, 24th, Jan., 2018.

[90] 早坂 健一郎, 川合 豊, 小関 義博, 平野 貴人, 岩本 貢, 太田 和夫, “マルチユーザで利用可能な共通鍵型秘匿検索に向けて,” **暗号と情報セキュリティシンポジウム** (SCIS2018), 3C2-1, 25th, Jan., 2018.

[91] 野島 拓也, 渡邉 洋平, 岩本 貢, 太田 和夫, “ダミーエントリの作成方法に着目した共通鍵検索可能暗号 CGKO 方式の改良,” **暗号と情報セキュリティシンポジウム** (SCIS2018), 3C2-2, 25th, Jan., 2018.

[92] 庄司奈津, 菅原健, 岩本 貢, 崎山一男, “ブロック暗号へのプロービング攻撃における鍵復元効率の正確な評価モデル,” **暗号と情報セキュリティシンポジウム** (SCIS2018), 3D3-5, 25th, Jan., 2018.

[93] 駒野雄一, 岩本貢, 太田和夫, “誤り補正を不要とする PUF ベース端末認証方式,” **電子情報通信学会研究会研究報告**, ISEC2017-24/SITE2017-16/ICSS2017-23/EMM2017-27 pp. 123–130, July, 2017.

[94] 中井雄士，野島拓也, 岩本貢, 太田和夫, “検索可能暗号における最小漏洩情報に関する考察,” **電子情報通信学会研究会研究報告**, IT2016-128/ISEC2016-118/WBS2016-104, pp. 187–192, March, 2017.

[95] 早坂健一郎，川合 豊，小関 義博，平野 貴人，岩本貢，太田 和夫，“検索クエリからの漏洩情報を削減した効率的な共通鍵型検索可能暗号,” **暗号と情報セキュリティシンポジウム** (SCIS2017), 1D1-1, 24th, Jan., 2017.

[96] 岩本貢，四方順司，“最悪推測秘匿性を満たす秘密分散法に関する基本的性質,” **暗号と情報セキュリティシンポジウム** (SCIS2017), 1A1-4, 24th, Jan., 2017.

[97] A. Espejel-Trujillo, M. Iwamoto, “Steganalysis of Bit Replacement Steganography for a Proactive Secret Image Sharing,” **暗号と情報セキュリティシンポジウム** (SCIS2017), 1A1-6, 24th, Jan., 2017.

[98] 徳重佑樹，中井雄士，岩本貢，太田和夫，“カードを用いた複数人での金持ち比べプロトコル,” **暗号と情報セキュリティシンポジウム** (SCIS2017), 1A2-1, 24th, Jan., 2017.

[99] 城内聡志，中井雄士，岩本貢，太田和夫，“秘匿操作を用いた効率的なカードベース論理演算プロトコル,” **暗号と情報セキュリティシンポジウム** (SCIS2017), 1A2-2, 24th, Jan., 2017.

[100] 鴨志田優一，岩本貢，太田和夫，“電子決済方式 MicroMint の潜在的な偽造脅威に対する安全性評価,” **暗号と情報セキュリティシンポジウム** (SCIS2017), 1F2-6, 24th, Jan., 2017.

[101] 平野貴人，小関義博，川合豊，岩本貢，太田和夫，“リクエストベース比較可能暗号におけるシミュレーションベースの安全性,” **暗号と情報セキュリティシンポジウム** (SCIS2017), 1D2-5, 24th, Jan., 2017.

[102] 岩本貢, “マルチパーティ計算に関する安全性概念の定式化について,” **暗号と情報セキュリティシンポジウム** (SCIS2017), 2D4-3, 25th, Jan., 2017.

[103] 岩本貢，渡邉 洋平 “秘密分散型放送暗号,” **暗号と情報セキュリティシンポジウム** (SCIS2017), 4F2-2, 27th, Jan., 2017.

[104] 小美濃つかさ，駒野雄一，岩本貢，太田和夫, “長期間にわたって安全な地域医療連携システムの構築を目指して,” **第 36 回医療情報学連合大会**, （ポスターセッション）pp. 996–999, Nov., 2016.

[105] 平野貴人, 岩本貢, 太田和夫, “複数の暗号化索引を持つ共通鍵ベース秘匿検索の効率的なトラップドア生成,” **コンピューターセキュリティシンポジウム**，2C3-4, pp. 572–577, 12th, Oct., 2016.

[106] 八代理紗，藤井達哉，岩本貢，崎山一男, “Deep Learning を用いた RSA に対する単純電磁波解析,” **電子情報通信学会** *2016* **年ソサイエティ大会**, p. 90, 21st, Sept., 2016.

[107] 八代理紗，町田卓謙，岩本貢，崎山一男, “Deep Learning を用いた Double Arbiter PUF の安全性評価,” **電子情報通信学会** *2016* **年総合大会**, p. 99, 16th, Mar., 2016.

[108] 徳重佑樹，花谷嘉一，岩本貢, 太田和夫，“グループ認証付鍵交換プロトコルの weak-SK-secure 性の形式検証,” **暗号と情報セキュリティシンポジウム** (SCIS2016), 1A1–2, 19th, Jan., 2016.

[109] 平野貴人, 川合豊，太田和夫，岩本貢, “共通鍵暗号型の秘匿部分一致検索（その 1 ）,” **暗号と情報セキュリティシンポジウム** (SCIS2016), 2A1–4, 20th, Jan., 2016.

[110] 早坂 健一郎，川合 豊，平野 貴人，太田 和夫，岩本貢, “共通鍵暗号型の秘匿部分一致検索（その 2）,” **暗号と情報セキュリティシンポジウム** (SCIS2016), 2A1–5, 20th, Jan., 2016.

[111] A. E. Trujillo and M. Iwamoto, “Proactive Secret Image Sharing with Quality and Payload Trade-off in Stego-images,” **暗号と情報セキュリティシンポジウム** (SCIS2016), 3A1–2, 21st, Jan., 2016.

[112] 鴨志田優一，岩本貢, 太田和夫，“Joux-Lucks のマルチコリジョン探索アルゴリズムの MicroMint への応用,” **暗号と情報セキュリティシンポジウム** (SCIS2016), 3D1–3, 21st, Jan., 2016.

[113] 三澤 裕人，徳重 佑樹，岩本貢, 太田 和夫，“人間向け暗号/認証プロトコルの統一的安全性評価,” **暗号と情報セキュリティシンポジウム** (SCIS2016), 3E3–5, 21st, Jan., 2016.

[114] 中井雄士，三澤裕人，徳重佑樹，岩本貢, 太田和夫，“カード操作の分類とカードベース暗号プロトコル,” **暗号と情報セキュリティシンポジウム** (SCIS2016), 4A2–2, 22nd, Jan.,2016.

[115] 三澤 裕人，徳重 佑樹，岩本貢, 太田 和夫，“ブロックサインの安全性に対するコードブックの影響,” **コンピューターセキュリティシンポジウム**，3C2–2, pp. 1011–1018, 23rd, Oct., 2015.

[116] 大宮翔児，徳重佑樹，岩本貢，太田 和夫，“正規言語を用いた鍵更新可能暗号の安全性解析,” **暗号と情報セキュリティシンポジウム** (SCIS2015), 1D1–4, 2015.

[117] 岩本貢, 四方順司, “推測成功確率に基づいた安全性基準をみたす秘密分散法,” **暗号と情報セキュリティシンポジウム** (SCIS2015), 2D1–4, 2015.

[118] 岩本貢, 四方 順司, “推測確率に基づいた安全性基準をみたす暗号化方式の構成法,” **暗号と情報セキュリティシンポジウム** (SCIS2015), 2D1–5, 2015.

[119] 平野 貴人，川合 豊，岩本貢，太田 和夫，“ある CKA2 安全な検索可能暗号方式のトラップドアサイズを削減するための安全な分割手法,” **暗号と情報セキュリティシンポジウム** (SCIS2015), 2F1–4, 2015.

[120] 鴨志田 優一，徳重 佑樹，岩本貢，太田 和夫，“Joux-Lucks の 3-collisions 探索アルゴリズムに対する改良および計算量の詳細な検討,” **暗号と情報セキュリティシンポジウム** (SCIS2015), 2E2–4, 2015.

[121] 土屋 喬文，花谷 嘉一，岩本貢，太田 和夫，“Corrupt 耐性を持つセッションキー安全な秘密鍵失効機能付き Secret Handshake 方式,” **暗号と情報セキュリティシンポジウム** (SCIS2015), 3F4–1, 2015.

[122] 中井雄士，徳重佑樹，岩本貢，太田和夫，“カードを用いた効率的な金持ち比べプロトコル,” **暗号と情報セキュリティシンポジウム** (SCIS2015), 3F4–2, 2015.

[123] 徳重佑樹，中井雄士，岩本貢，太田和夫，“カードベース暗号プロトコルにおける安全な選択処理,” 暗号と情報セキュリティシンポジウム (SCIS2015), 3F4–3, 2015.

[124] 三澤裕人，徳重佑樹，岩本貢，太田和夫，“簡易なブロックサインに対する暗号理論的安全性解析,” 暗号と情報セキュリティシンポジウム (SCIS2015), 3F4–4, 2015.

[125] 町田卓謙，山本大，岩本貢，崎山一男, “FPGA 実装された Arbiter-based PUF の ユニーク性向上に向けた実装法の検討,” *Hot Channel Workshop*，東北大学，2014.

[126] P. Lumyong, M. Iwamoto, and K. Ohta, “Cheating on Visual Secret Sharing Schemes in Practical Setting,” 暗号と情報セキュリティシンポジウム (SCIS2014), 1E1–1, 2014.

[127] M. Iwamoto, T. Omino, Y. Komano, and K. Ohta, “Optimal Non-Perfectly Secure Client-Server Communications in a Symmetric Key Setting,” 暗号と情報セキュリティシンポジウム (SCIS2014), 1E3–1, 2014.

[128] 小美濃つかさ，岩本貢，駒野雄一，太田和夫, “情報理論的に安全なクライアント・サーバ暗号通信方式の応用に関する考察,” 暗号と情報セキュリティシンポジウム (SCIS2014), 1E3–2, 2014.

[129] 町田卓謙，山本大，岩本貢，崎山一男，“FPGA 実装された Arbiter PUF のユニーク性向上に向けた一考察,” 暗号と情報セキュリティシンポジウム (SCIS2014), 2A1–5, 2014.

[130] 西出隆志，岩本貢，岩崎敦，太田和夫，“自動タイブレークの仕組みを持つ第 M+1 価格暗号オークション方式,” 暗号と情報セキュリティシンポジウム (SCIS2014), 2D4–2, 2014.

[131] 土屋喬文，徳重佑樹，坂井祐介，岩本貢，太田和夫，“同時実行攻撃に耐性を持つシンプルな Secret Handshake,” 暗号と情報セキュリティシンポジウム (SCIS2014), 2D4–3, 2014.

[132] 徳重佑樹，佐々木悠，王磊，岩本貢，太田和夫，“Improved Rebound Attack 手順の自動探索手法の提案と評価,” 暗号と情報セキュリティシンポジウム (SCIS2014), 3C4–2, 2014.

[133] 町田卓謙, 中曽根俊貴, 岩本貢, 崎山一男, “FPGA 上の Arbiter PUF に対する機械学習攻撃の新たなモデル作成に向けて,” *Hot Channel Workshop* 2013.

[134] 駒野雄一, 太田和夫, 崎山一男, 岩本貢, “PUF を用いる鍵生成方法とその安全性,” *Hot Channel Workshop 2013*, (2013 年 4 月 11 日).

[135] M. Iwamoto and J. Shikata, “Revisiting Conditional Rényi Entropy and its Application to Encryption: Part I —Properties of Conditional Rényi Entropy—,” 暗号と情報セキュリティシンポジウム (SCIS2013), 1F1–3, 2013.

[136] J. Shikata and M. Iwamoto, “Revisiting Conditional Rényi Entropy and its Application to Encryption: Part II —Fano’s Inequality and Shannon’s Bound—,” 暗号と情報セキュリティシンポジウム (SCIS2013), 1F1–4, 2013.

[137] 駒野雄一，太田和夫，崎山一男，岩本貢, “PUF 出力の一部を用いるパターン照合鍵生成システムの安全性,” 暗号と情報セキュリティシンポジウム (SCIS2013), 1D2–3, 2013.

[138] 山本大，崎山一男，岩本貢, 太田和夫, 武仲正彦, 伊藤孝一, 鳥居直哉, “レスポンス数の向上手法を適用したラッチ PUF の ASIC 実装評価,” 暗号と情報セキュリティシンポジウム (SCIS2013), 2E2–2, 2013.

[139] 岩井祐樹, 福島崇文, 森山大輔, 松尾真一郎, 駒野雄一, 岩本貢, 太田和夫, 崎山一男, “巡回シフトを用いた PUF に基づくパターン照合鍵生成システムの実装評価,” 暗号と情報セキュリティシンポジウム (SCIS2013), 2E3–3, 2013.

[140] 中曽根俊貴, 李陽, 佐々木悠, 岩本貢, 太田和夫, 崎山一男, “CC-EMA と CEMA の攻撃性能の比較,” 暗号と情報セキュリティシンポジウム (SCIS2013), 3E3–2, 2013.

[141] M. Iwamoto, K. Ohara, Y. Sakai, and K. Ohta, "Information Theoretic Analysis of a t-resilient First-Price Auction Protocol," **暗号と情報セキュリティシンポジウム** (SCIS2013), 4D1–2, 2013.

[142] 駒野雄一，太田和夫，崎山一男，岩本貢，"PUF を用いるパターン照合鍵生成方法の改良," *2012* **年電子情報通信学会総合大会**，A7–9, 2012.

[143] 岩本貢, "しきい値法の一般化とその構成法," **電子情報通信学会総合大会** (公募セッション：ネットワーク符号加法と秘密分散法), AS–2–2, 2012.

[144] 大原一真, 坂井祐介, 岩本貢, 太田和夫, "情報理論的に安全な First-Price オークションプロトコル," **暗号と情報セキュリティシンポジウム** (SCIS2012), 4B1–3, 2012.

[145] 駒野雄一, 太田和夫, 崎山一男, 岩本貢, "PUF を用いる証明可能安全なパターン照合鍵生成方法," **暗号と情報セキュリティシンポジウム** (SCIS2012), 1D2-2, 2012.

[146] 岩本貢, 太田和夫, "共通鍵暗号方式における情報理論的安全性と計算量的安全性の関係," **電子情報通信学会研究会研究報告**, IT2011-5, 25–30, May, 2011.

[147] 李奇, 五味澤重友, 岩本貢, 太田和夫, 崎山一男, "Trivium のセットアップタイム違反に基づく新しい故障差分解析," **電子情報通信学会研究会研究報告**, ISEC2010-122, 333–339, March, 2011.

[148] 坂井 祐介, 岩本貢, 駒野 雄一, 太田 和夫, "FDH 署名の安全性証明の再考," **暗号と情報セキュリティシンポジウム** (SCIS2011), 4A2–1, 2011.

[149] 名渕大樹, 岩本貢, 崎山一男, 太田 和夫, "Joux-Lucks の 3-collisions 探索アルゴリズムに関する計算量の詳細な検討," **暗号と情報セキュリティシンポジウム** (SCIS2011), 4B1–4, 2011.

[150] 落合隆夫, 山本大, 伊藤 孝一, 武仲正彦, 鳥居直哉, 内田大輔, 永井利明, 若菜伸一, 岩本貢, 太田和夫, 崎山 一男, "電磁波解析における局所性と放射磁界方向について," **暗号と情報セキュリティシンポジウム** (SCIS2011), 2D3–3, 2011.

[151] 山本大, 崎山一男, 岩本貢, 太田和夫, 落合 隆夫, 武仲 正彦, 伊藤 孝一, " ラッチの乱数出力位置を利用した PUF による ID 生成／認証システムの信頼性向上手法," **暗号と情報セキュリティシンポジウム** (SCIS2011), 2D1–1, 2011.

[152] 岩本貢, 太田和夫, " 情報理論的に安全な暗号化のための安全性概念," **情報理論とその応用シンポジウム** (SITA2010), pp.202–207, 2010.

[153] M. Iwamoto, Y. Li, K. Sakiyama, and K. Ohta, "A general construction method of visual secret sharing schemes with share rotations," *Technical Report of IEICE*, ISEC2010–49, pp.67–74, 2010.

[154] 長井大地，塙知剛，岩本貢，崎山一男，太田和夫，"PUF-HB 認証プロトコルに対する能動的な攻撃," **暗号と情報セキュリティシンポジウム**, 2C2-5, Jan., 2010.

[155] 李 陽, 岩本貢, 太田和夫, 崎山一男, "画像の回転に対する新しい視覚復号型秘密分散法," **電子情報通信学会研究会研究報告**, ISEC2009-5, pp.29–36, May, 2009.

[156] 古賀弘樹, 岩本貢, 山本博資, "なりすまし攻撃を検出できる $(2,2)$ しきい値法に関する符号化定理," **電子情報通信学会研究会研究報告**, IT2008–66, ISEC2008-124, WBS2008-79, pp.143–150, March, 2009.

[157] 岩本貢, 山本博資, "漸近的にほぼ確実に不正検出可能な秘密分散法," **暗号と情報セキュリティシンポジウム**, 1F1-2, Jan., 2009.

[158] M. Iwamoto, "Weakly secure visual secret sharing schemes," **暗号と情報セキュリティシンポジウム**, 1F1-4, Jan., 2009.

[159] 岩本貢, 山本博資, "漸近的にほぼ確実に不正検出可能な秘密分散法," **情報理論とその応用シンポジウム**, pp.532–537, Oct., 2008.

[160] 田口正之, 岩本貢, “ユーザの挙動を考慮した動的鍵事前配送方式,” **情報理論とその応用シンポジウム**, pp.751-754, Nov.–Dec., 2006.

[161] 岩本貢, 王磊, 米山一樹, 國廣昇, 太田和夫，“回転を許す一般アクセス構造に対して複数の画像を隠す視覚復号型秘密分散法,” **情報理論とその応用シンポジウム**, pp.689–692, Nov., 2005.

[162] 清田耕一朗, 王磊, 岩本貢, 米山一樹, 國廣昇, 太田和夫，“画像の回転に関して複数の画像が復号可能な視覚復号型秘密分散法,” **暗号と情報セキュリティシンポジウム**, Jan., pp.49–55, 2005.

[163] 岩本貢, 山本博資, “強い秘密保護特性をもつランプ型秘密分散法,” **情報理論とその応用シンポジウム**, pp.331–334, Dec., 2004.

[164] 小川朋宏，佐々木朗，岩本貢，山本博資，“量子秘密分散法の符号化効率評価と構成法,” **情報理論とその応用シンポジウム**，pp.227–230, Dec., 2003.

[165] 岩本貢, 山本博資, 小川博久，“(k, n) しきい値法と整数計画法による秘密分散法の一般的構成法,” **電子情報通信学会研究会研究報告**, ISEC2003–11, pp.63–70, May, 2003.

[166] 岩本貢，山本博資，“一般アクセス構造に対する非理想的ランプ型秘密分散法,” **情報理論とその応用シンポジウム**, pp.227–230, Dec., 2002.

[167] 岩本貢，山本博資，“複数の秘密画像をもつ視覚復号型秘密分散法の安全性条件,” **電子情報通信学会研究報告**，ISEC2001-121, pp.51–56, Mar., 2002.

[168] 岩本貢，山本博資，“複数の画像を秘密画像とする視覚復号型秘密分散法,” **情報理論とその応用シンポジウム**, pp.565–568, Dec., 2001.

[169] 岩本貢，山本博資，“濃淡画像に対する最適な (n, n) しきい値視覚復号型秘密分散法,” **コンピュータセキュリティシンポジウム**, pp.337–342, Nov., 2001.

[170] 近藤正章，岩本貢，中村宏，“キャッシュラインを考慮した 3 次元 PDE Solver の最適化手法,” **報処理学会研究報告**，HPC-85, pp.91–96，Mar., 2001.

[171] 岩本貢，渡辺亮介，近藤正章，中村宏，朴泰祐，“NASPB CG, FT における SCIMA の性能評価,” **情報処理学会研究報告**，HPC-83, pp.31–36, Oct., 2000.

[172] H. Koga, M. Iwamoto and H. Yamamoto, “An analytic construction of the visual secret sharing scheme for color images,” *Symposium on Cryptography and Information Security*, Jan., 2000.

[173] 岩本貢，古賀弘樹，山本博資，“カラー画像に対する一般のアクセス構造をもつ視覚復号型秘密分散法の一構成法,” **情報理論とその応用シンポジウム**，pp.761–764，Dec., 1999.

— *Awards*[1] —

[174] サイバーセキュリティシンポジウム道後 2018 学生研究賞（受賞者：庄司奈津, [92] に対して）

[175] サイバーセキュリティシンポジウム道後 2017 学生研究賞（受賞者：八代理紗, [33] に対して）

[176] 電子情報通信学会貢献賞（情報理論研究専門委員会の運営及び活動に対する貢献，基礎境界ソサイエティ）2017 年 9 月.

[177] 電子情報通信学会貢献賞（基礎・境界ソサイエティ「電子広報担当幹事」としての貢献，基礎境界ソサイエティ）2015 年 9 月.

[178] 電子情報通信学会感謝状（査読委員として，基礎境界ソサイエティ）2014 年 9 月.

[1] 共著学生の受賞を含む.

[179] 電子情報通信学会感謝状（査読委員として，基礎境界ソサイエティ）2012 年 9 月.

[180] SITA 奨励賞，(SITA2004 における口頭発表，[163] に対して)，2005 年 11 月.

— *Non-Technical Articles* —

[181] 岩本貢，“国際会議 EUROCRYPT2012 参加報告,” 電子情報通信学会 ISEC 研究会研究報告, ISEC2012–47, pp.29–31, Sept., 2012.

[182] 岩本貢，“コネチカット便り,” Fundamentals Review, vol.6, no.1, pp.84–85, 2012.

[183] 岩本貢，“国際会議 ISIT2009 参加報告,” Fundamentals Review, vol.3, no.2, pp.77–78, 2009.