List of Publications

Mitsugu Iwamoto,
Last modified: 3rd June, 2022.

— Refereed Journal —

[1] Y. Watanabe, T. Nakai, K. Ohara, T. Nojima, Y. Liu, M. Iwamoto, and K. Ohta, "How to make a secure index for searchable symmetric encryption, revisited," *IEICE Transactions on Fundamentals*, vol. -, pp. –, to appear 2022.

[2] Y. Abe, T. Nakai, Y. Kuroki, S. Suzuki, Y. Koga, Y. Watanabe, M. Iwamoto, and K. Ohta, "Efficient card-based majority voting protocols," *New Generation Computing*, vol. 40, pp. 173–198, 2022.

[3] T. Nakai, S. Shirouchi, Y. Tokushige, M. Iwamoto, and K. Ohta, "Secure computation for threshold functions with physical cards: Power of private permutations," *New Generation Computing*, vol. 40, pp. 95–113, 2022.

[4] T. Nakai, Y. Misawa, Y. Tokushige, M. Iwamoto, and K. Ohta, "How to solve millionaires' problem with two kinds of cards," *New Gener. Comput.*, vol. 39, no. 1, pp. 73–96, 2021.

[5] K. Matsuda, S. Tada, M. Nagata, Y. Komano, Y. Li, T. Sugawara, M. Iwamoto, K. Ohta, K. Sakiyama, and N. Miura, "An IC-level countermeasure against laser fault injection attack by information leakage sensing based on laser-induced opto-electric bulk current density," *Japanese Journal of Applied Physics*, vol. 59, p. SGGL02, Feb. 2020.

[6] K. Ohara, Y. Watanabe, M. Iwamoto, and K. Ohta, "Multi-party computation for modular exponentiation based on replicated secret sharing," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 102-A, no. 9, pp. 1079 – 1090, 2019.

[7] Y. Komano, K. Ohta, K. Sakiyama, M. Iwamoto, and I. Verbauwhede, "Single-round pattern matching key generation using physically unclonable function," *Secur. Commun. Networks*, vol. 2019, pp. 1719585:1 – 1719585:13, 2019.

[8] A. Espejel-Trujillo, M. Iwamoto, and M. Nakano-Miyatake, "A proactive secret image sharing scheme with resistance to machine learning based steganalysis," *Multim. Tools Appl.*, vol. 77, no. 12, pp. 15161 – 15179, 2018.

[9] M. Iwamoto, K. Ohta, and J. Shikata, "Security formalizations and their relationships for encryption and key agreement in information-theoretic cryptography," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 654 – 685, 2018.

[10] R. Yashiro, T. Sugawara, M. Iwamoto, and K. Sakiyama, "Q-class authentication system for double arbiter PUF," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 101-A, no. 1, pp. 129 – 137, 2018.

[11] 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. Cryptogr. Eng.*, vol. 5, no. 3, pp. 187 – 199, 2015.

[12] T. Machida, D. Yamamoto, M. Iwamoto, and K. Sakiyama, "A new arbiter PUF for enhancing unpredictability on FPGA," *The Scientific World Journal*, vol. 2015, p. 864812, 2015.

[13] 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," *J. Inf. Process.*, vol. 22, no. 2, pp. 142 – 151, 2014.

[14] T. Nakasone, Y. Li, M. Iwamoto, K. Ohta, and K. Sakiyama, "New side-channel analysis using clockwise collision leakage model and weak keys on parallelized AES hardware," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci. (Japanese Edition)*, vol. J97 – A, pp. 695 – 703, Nov. 2014.

[15] 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," *J. Cryptogr. Eng.*, vol. 3, no. 4, pp. 197 – 211, 2013.

[16] M. Iwamoto, "A weak security notion for visual secret sharing schemes," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 2, pp. 372 – 382, 2012.

[17] K. Sakiyama, Y. Li, M. Iwamoto, and K. Ohta, "Information-theoretic approach to optimal differential fault analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 1, pp. 109 – 120, 2012.

[18] M. Iwamoto, H. Koga, and H. Yamamoto, "Coding theorems for a $(2, 2)$-threshold scheme with detectability of impersonation attacks," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 6194 – 6206, 2012.

[19] A. Espejel-Trujillo, M. Nakano-Miyatake, M. Iwamoto, and H. Pérez-Meana, "A cheating prevention evc scheme using watermarking techniques," *Revista Facultad de Ingeniería Universidad de Antioquia*, no. 63, pp. 30 – 42, 2012.

[20] M. Iwamoto, H. Yamamoto, and H. Ogawa, "Optimal multiple assignments based on integer programming in secret sharing schemes with general access structures," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 90-A, no. 1, pp. 101 – 112, 2007.

[21] M. Iwamoto and H. Yamamoto, "Strongly secure ramp secret sharing schemes for general access structures," *Information Processing Letters*, vol. 97, no. 2, pp. 52–57, 2006.

[22] 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. Fundam. Electron. Commun. Comput. Sci.*, vol. 89-A, no. 5, pp. 1382 – 1395, 2006.

[23] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto, "Quantum secret sharing schemes and reversibility of quantum operations," *Phys. Rev. A*, vol. 72, p. 032318, Sep. 2005.

[24] M. Iwamoto and H. Yamamoto, "A construction method of visual secret sharing schemes for plural secret images," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 86, pp. 2577–2588, Oct. 2003.

[25] M. Iwamoto and H. Yamamoto, "The optimal n-out-of-n visual secret sharing scheme for gray-scale images," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 85, pp. 2238–2247, oct 2002.

[26] H. Koga, M. Iwamoto, and H. Yamamoto, "An analytic construction of the visual secret sharing scheme for color images," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 84, pp. 262 – 272, Jan. 2001.

— *International Conference (Invited)* —

[1] M. Iwamoto, "Secret sharing schemes under guessing secrecy," in *Cryptographic Technologies for Securing Network Storage and Their Mathematical Modeling, MI Lecture Notes, Kyushu University*, pp. 25–37, 2017.

[2] M. Iwamoto, "Security notions of visual secret sharing schemes," in *International Workshop on Advanced Image Technology, Nagoya, Japan, 7–8 January*, pp. 95–100, 2013.

— *International Conference (Refereed)* —

[1] Y. Watanabe, K. Ohara, M. Iwamoto, and K. Ohta, "Efficient dynamic searchable encryption with forward privacy under the decent leakage," in *CODASPY '22: Twelveth ACM Conference on Data and Application Security and Privacy, Baltimore, MD, USA, April 24 - 27, 2022* (A. Joshi, M. Fernández, and R. M. Verma, eds.), pp. 312–323, ACM, 2022.

[2] Y. Abe, M. Iwamoto, and K. Ohta, "How to detect malicious behaviors in a card-based majority voting protocol with three inputs," in *International Symposium on Information Theory and its Applications, ISITA 2020, virtual, Oct. 24 – 27*, pp. 377 – 381, IEEE, Oct. 2020.

[3] T. Uemura, Y. Watanabe, Y. Li, T. Miura, M. Iwamoto, K. Sakiyama, and K. Ohta, "A key recovery algorithm using random key leakage from aes key schedule," in *International Symposium on Information Theory and its Applications, ISITA 2020, virtual, Oct. 24 – 27*, pp. 382 – 386, IEEE, Oct. 2020.

[4] Y. Abe, M. Iwamoto, and K. Ohta, "Efficient private PEZ protocols for symmetric functions," in *Theory of Cryptography - 17th International Conference, TCC 2019, Nuremberg, Germany, December 1 – 5, 2019, Proceedings, Part I* (D. Hofheinz and A. Rosen, eds.), vol. 11891 of *Lecture Notes in Computer Science*, pp. 372 – 392, Springer, 2019.

[5] K. Matsuda, S. Tada, M. Nagata, Y. Li, T. Sugawara, M. Iwamoto, K. Ohta, K. Sakiyama, and N. Miura, "An information leakage sensor based on measurement of laser-induced opto-electric bulk current density," vol. 2019, pp. 501 – 502, 2019.

[6] R. Eriguchi, N. Kunihiro, and M. Iwamoto, "Optimal multiple assignment schemes using ideal multipartite secret sharing schemes," in *IEEE International Symposium on Information Theory, ISIT 2019, Paris, France, July 7 – 12, 2019*, pp. 3047 – 3051, IEEE, 2019.

[7] N. Shoji, T. Sugawara, M. Iwamoto, and K. Sakiyama, "An abstraction model for 1-bit probing attack on block ciphers," in *IEEE 4th International Conference on Computer and Communication Systems, ICCCS 2019, Singapore, February 23 – 25, 2019*, pp. 502 – 506, IEEE, 2019.

[8] Y. Watanabe, Y. Kuroki, S. Suzuki, Y. Koga, M. Iwamoto, and K. Ohta, "Card-based majority voting protocols with three inputs using three cards," in *International Symposium on Information Theory and Its Applications, ISITA 2018, Singapore, October 28 – 31, 2018*, pp. 218 – 222, IEEE, 2018.

[9] T. Nakai, S. Shirouchi, M. Iwamoto, and K. Ohta, "Four cards are sufficient for a card-based three-input voting protocol utilizing private permutations," in *Information Theoretic Security - 10th International Conference, ICITS 2017, Hong Kong, China, November 29 – December 2, 2017, Proceedings* (J. Shikata, ed.), vol. 10681 of *Lecture Notes in Computer Science*, pp. 153 – 165, Springer, 2017.

[10] R. Yashiro, T. Machida, M. Iwamoto, and K. Sakiyama, "Deep-learning-based security evaluation on authentication systems using arbiter PUF and its variants," in *Advances in Information and Computer Security - 11th International Workshop on Security, IWSEC 2016, Tokyo, Japan, September 12 – 14, 2016, Proceedings* (K. Ogawa and K. Yoshioka, eds.), vol. 9836 of *Lecture Notes in Computer Science*, pp. 267 – 285, Springer, 2016.

[11] 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," in *Advances in Information and Computer Security - 11th International Workshop on Security, IWSEC 2016, Tokyo, Japan, September 12 – 14, 2016, Proceedings* (K. Ogawa and K. Yoshioka, eds.), vol. 9836 of *Lecture Notes in Computer Science*, pp. 91 – 110, Springer, 2016.

[12] K. Hayasaka, Y. Kawai, Y. Koseki, T. Hirano, K. Ohta, and M. Iwamoto, "Probabilistic generation of trapdoors: Reducing information leakage of searchable symmetric encryption," in *Cryptology and Network Security - 15th International Conference, CANS 2016, Milan, Italy, November 14 – 16, 2016, Proceedings* (S. Foresti and G. Persiano, eds.), vol. 10052 of *Lecture Notes in Computer Science*, pp. 350 – 364, 2016.

[13] T. Nakai, Y. Tokushige, Y. Misawa, M. Iwamoto, and K. Ohta, "Efficient card-based cryptographic protocols for millionaires' problem utilizing private permutations," in *Cryptology and Network Security - 15th International Conference, CANS 2016, Milan, Italy, November 14 – 16, 2016, Proceedings* (S. Foresti and G. Persiano, eds.), vol. 10052 of *Lecture Notes in Computer Science*, pp. 500 – 517, 2016.

[14] T. Machida, D. Yamamoto, M. Iwamoto, and K. Sakiyama, "Implementation of double arbiter PUF and its performance evaluation on FPGA," in *The 20th Asia and South Pacific Design Automation Conference, ASP-DAC 2015, Chiba, Japan, January 19 – 22, 2015*, pp. 6 – 7, IEEE, 2015.

[15] M. Iwamoto and J. Shikata, "Constructions of symmetric-key encryption with guessing secrecy," in *IEEE International Symposium on Information Theory, ISIT 2015, Hong Kong, China, June 14 – 19, 2015*, pp. 725 – 729, IEEE, 2015.

[16] T. Machida, D. Yamamoto, M. Iwamoto, and K. Sakiyama, "A new mode of operation for arbiter PUF to improve uniqueness on FPGA," in *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems, Warsaw, Poland, September 7 – 10, 2014* (M. Ganzha, L. A. Maciaszek, and M. Paprzycki, eds.), vol. 2 of *Annals of Computer Science and Information Systems*, pp. 871 – 878, 2014.

[17] Y. Sasaki, Y. Tokushige, L. Wang, M. Iwamoto, and K. Ohta, "An automated evaluation tool for improved rebound attack: New distinguishers and proposals of shiftbytes parameters for grøstl," in *Topics in Cryptology - CT-RSA 2014 - The Cryptographer's Track at the RSA Conference 2014, San Francisco, CA, USA, February 25 – 28, 2014. Proceedings* (J. Benaloh, ed.), vol. 8366 of *Lecture Notes in Computer Science*, pp. 424 – 443, Springer, 2014.

[18] T. Nishide, M. Iwamoto, A. Iwasaki, and K. Ohta, "Secure $(M+1)$ st-price auction with automatic tie-break," in *Trusted Systems - 6th International Conference, INTRUST 2014, Beijing, China, December 16 – 17, 2014, Revised Selected Papers* (M. Yung, L. Zhu, and Y. Yang, eds.), vol. 9473 of *Lecture Notes in Computer Science*, pp. 422 – 437, Springer, 2014.

[19] K. Ohara, Y. Sakai, F. Yoshida, M. Iwamoto, and K. Ohta, "Privacy-preserving smart metering with verifiability for both billing and energy management," in *ASIAPKC'14, Proceedings of the 2nd ACM Workshop on ASIA Public-Key Cryptography, June 3, 2014, Kyoto, Japan* (K. Emura, G. Hanaoka, and Y. Zhao, eds.), pp. 23 – 32, ACM, 2014.

[20] M. Iwamoto and J. Shikata, "Secret sharing schemes based on min-entropies," in *2014 IEEE International Symposium on Information Theory, Honolulu, HI, USA, June 29 – July 4, 2014*, pp. 401 – 405, IEEE, 2014.

[21] P. Lumyong, M. Iwamoto, and K. Ohta, "Cheating on a visual secret sharing scheme under a realistic scenario," in *International Symposium on Information Theory and its Applications, ISITA 2014, Melbourne, Australia, October 26 – 29, 2014*, pp. 575 – 579, IEEE, 2014.

[22] M. Iwamoto, T. Omino, Y. Komano, and K. Ohta, "A new model of client-server communications under information theoretic security," in *2014 IEEE Information Theory Workshop, ITW 2014, Hobart, Tasmania, Australia, November 2 – 5, 2014*, pp. 511 – 515, IEEE, 2014.

[23] M. Iwamoto, T. Peyrin, and Y. Sasaki, "Limited-birthday distinguishers for hash functions - collisions beyond the birthday bound can be meaningful," in *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1 – 5, 2013, Proceedings, Part II* (K. Sako and P. Sarkar, eds.), vol. 8270 of *Lecture Notes in Computer Science*, pp. 504 – 523, Springer, 2013.

[24] M. Iwamoto and J. Shikata, "Information theoretic security for encryption based on conditional rényi entropies," in *Information Theoretic Security - 7th International Conference, ICITS 2013, Singapore, November 28 – 30, 2013, Proceedings* (C. Padró, ed.), vol. 8317 of *Lecture Notes in Computer Science*, pp. 103 – 121, Springer, 2013.

[25] 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," in *SECRYPT 2013 - Proceedings of the 10th International Conference on Security and Cryptography, Reykjavík, Iceland, 29 – 31 July, 2013* (P. Samarati, ed.), pp. 111 – 122, SciTePress, 2013.

[26] T. Nakasone, Y. Li, Y. Sasaki, M. Iwamoto, K. Ohta, and K. Sakiyama, "Key-dependent weakness of aes-based ciphers under clockwise collision distinguisher," in *Information Security and Cryptology - ICISC 2012 - 15th International Conference, Seoul, Korea, November 28 – 30, 2012, Revised Selected Papers* (T. Kwon, M. Lee, and D. Kwon, eds.), vol. 7839 of *Lecture Notes in Computer Science*, pp. 395 – 409, Springer, 2012.

[27] 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," in *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 – October 1, 2011. Proceedings* (B. Preneel and T. Takagi, eds.), vol. 6917 of *Lecture Notes in Computer Science*, pp. 390 – 406, Springer, 2011.

[28] M. Iwamoto and K. Ohta, "Security notions for information theoretically secure encryptions," in *2011 IEEE International Symposium on Information Theory Proceedings, ISIT 2011, St. Petersburg, Russia, July 31 – August 5, 2011* (A. Kuleshov, V. M. Blinovsky, and A. Ephremides, eds.), pp. 1777 – 1781, IEEE, 2011.

[29] M. Iwamoto, H. Yamamoto, and H. Koga, "A coding theorem for cheating-detectable $(2, 2)$-threshold blockwise secret sharing schemes," in *IEEE International Symposium on Information Theory, ISIT 2009, June 28 – July 3, 2009, Seoul, Korea, Proceedings*, pp. 1308 – 1312, IEEE, 2009.

[30] A. Espejel-Trujillo, M. Nakano-Miyatake, and M. Iwamoto, "Visual secret sharing schemes for multiple secret images including shifting operation of shares," in *6th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE 2009)*, pp. 433 – 438, Nov. 2009.

[31] H. Koga, M. Iwamoto, and H. Yamamoto, "Coding theorems for a $(2, 2)$-threshold scheme secure against impersonation by an opponent," in *2009 IEEE Information Theory Workshop, ITW 2009, Taormina, Italy, October 11 – 16, 2009*, pp. 188 – 192, 2009.

[32] M. Iwamoto, "Weakly secure visual secret sharing schemes," in *International Symposium on Information Theory and its Applications, ISITA 2008, Aukland, New Zealand, December 7 – 10*, pp. 1221 – 1225, IEEE, Oct. 2008.

[33] M. Iwamoto and H. Yamamoto, "Strongly secure ramp secret sharing schemes," in *Proceedings of the 2005 IEEE International Symposium on Information Theory, ISIT 2005, Adelaide, South Australia, Australia, 4 – 9 September 2005*, pp. 1221 – 1225, IEEE, 2005.

[34] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto, "Quantum secret sharing schemes and reversibility of quantum operations," in *International Symposium on Information Theory and its Applications, ISITA 2004, Parma, Italy, 10 – 13 October*, pp. 1440 – 1445, IEEE, Oct. 2004.

[35] M. Iwamoto, H. Yamamoto, and H. Ogawa, "Optimal multiple assignments based on integer programming in secret sharing schemes," in *Proceedings of the 2004 IEEE International Symposium on Information Theory, ISIT 2004, Chicago Downtown Marriott, Chicago, Illinois, USA, June 27 – July 2, 2004*, p. 16, IEEE, 2004.

[36] M. Iwamoto and H. Yamamoto, "A construction method of visual secret sharing schemes for plural secret images," in *2003 IEEE International Symposium on Information Theory, Yokohama, Japan, 29 June – 4 July 2003*, p. 283, IEEE, 2003.

[37] M. Kondo, M. Iwamoto, and H. Nakamura, "Cache line impact on 3d PDE solvers," in *High Performance Computing, 4th International Symposium, ISHPC 2002, Kansai Science City, Japan, May 15 – 17, 2002, Proceedings* (H. P. Zima, K. Joe, M. Sato, Y. Seo, and M. Shimasaki, eds.), vol. 2327 of *Lecture Notes in Computer Science*, pp. 301 – 309, Springer, 2002.

— *Translations* —

[1] (Japanese translation) *Thomas M. Cover and Joy A. Thomas: The Elements of Information Theory, 2nd. ed. Wiley–InterScience, 2006*, published by Kyoritsu-shuppan, 2012 (In charge of translating Chapters 4, 11, 16, and 17) .

[2] (Japanese translation) *E. Berlekamp, J. Conway, and R. Guy, Winning Ways for Your Mathematical Plays, 2001*, published by Kyoritsu-shuppan, 2012 (In charge of translating Chapter 4).