Kazuo SAKIYAMA
﨑山 一男

The University of Electro-Communications
Department of Informatics
East 3-907, Chofugaoka
Chofu, Tokyo 182-8585, JAPAN

Phone: +81-42-443-5767
Fax: +81-42-443-5291
Email: sakiyama@uec.ac.jp
Homepage: http://www.sakiyama-lab.jp/

Personal

Born on August 18, 1971.

Japanese.

Education

B. Eng. Osaka University, 1994.

M. Eng. Electrical Engineering, Osaka University, 1996.

M. S. Electrical Engineering, University of California, Los Angeles, 2003.

Ph. D. Electrical Engineering, Katholieke Universiteit, Leuven, 2007.

Employment

Hitachi, Ltd., Semiconductor and IC division (now Renesas Electronics) 1996–2004.

Katholieke Universiteit Leuven (Post-Doctoral Researcher) 2007–2008.

The University of Electro-Communications (Associate Professor) 2008–2013.

The University of Electro-Communications (Professor) 2013–.

Publications

I *Books, Book Chapters*

1. Kazuo Sakiyama, Yu Sasaki, and Yang Li, "Security of Block Ciphers: From Algorithm Design to Hardware Implementation," ISBN 978-1-118-66001-0, Wiley, (Jul., 2015).
2. Kazuo Sakiyama and Masayuki Terada (Eds.), "Advances in Information and Computer Security – 8th International Workshop on Security, IWSEC 2013, Okinawa, Japan, November 18-20, 2013. Proceedings. Lecture Notes in Computer Science 8231," ISBN 978-3-642-41383-4, Springer, (Nov., 2013).
3. "ユニーク＆エキサイティングサイエンス," 梶谷 誠 (監修), ISBN 978-4-7649-0442-2, 近代科学社, 分担執筆, 﨑山一男, "第 2 章 暗号がつなぐ人と人工物とのコミュニケーション: 暗号とプライバシーと RFID システム," pp.45–70, (Mar., 2013).

4. Junko Takahashi, Toshinori Fukunaga, Shigeto Gomisawa, Yang Li, Kazuo Sakiyama, and Kazuo Ohta, "Fault Injection and Key Retrieval Experiments on Evaluation Board," Chapter in Marc Joye and Michael Tunstall editors, Fault Analysis in Cryptography, ISBN 978-3-642-29655-0, Springer, (Jul., 2012).
5. Kazuo Sakiyama and Lejla Batina, "Arithmetic for Public-key Cryptography," Chapter in I. Verbauwhede editor, Secure Integrated Circuits and Systems, ISBN 978-0-387-71827-9, Springer, (Feb., 2010)
6. Lejla Batina and Kazuo Sakiyama, "Compact Public-key Implementations for RFID and Sensor Nodes," Chapter in I. Verbauwhede editor, Secure Integrated Circuits and Systems, ISBN 978-0-387-71827-9, Springer, (Feb., 2010).
7. Lejla Batina, Kazuo Sakiyama, and Ingrid Verbauwhede, "Architectures for public-key cryptography," Chapter in Vojin G. Oklobdzija, editor, Digital Systems and Applications, ISBN 978-0-849-38619-0, CRC press, (Nov., 2007).

II *Journal Papers*

1. Shugo Mikami, Dai Watanabe, Yang Li, and Kazuo Sakiyama, "Fully Integrated Passive UHF RFID Tag for Hash-Based Mutual Authentication Protocol," The Scientific World Journal, Hindawi, Volume 2015 (2015), Article ID 498610, 11 pages, (Aug., 2015).
2. Takanori Machida, Dai Yamamoto, Mitsugu Iwamoto, and Kazuo Sakiyama, "A New Arbiter PUF for Enhancing Unpredictability on FPGA," The Scientific World Journal, Hindawi, Volume 2015 (2015), Article ID 864812, 13 pages, (Aug., 2015).
3. Dai Yamamoto, Kazuo Sakiyama, Mitsugu Iwamoto, Kazuo Ohta, Masahiko Takenaka, Kouichi Itoh, and Naoya Torii, "A new method for enhancing variety and maintaining reliability of PUF responses and its evaluation on ASICs Journal of Cryptographic Engineering," J. Cryptographic Engineering, Vol.5(3), pp.187-199, (Sep., 2015).
4. Sho Endo, Yang Li, Naofumi Homma, Kazuo Sakiyama, Kazuo Ohta, Daisuke Fujimoto, Makoto Nagata, Toshihiro Katashita, Jean-Luc Danger, and Takafumi Aoki, "A Silicon-level Countermeasure against Fault Sensitivity Analysis and Its Evaluation," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., Vol.23, No.8, pp.1429-1438, (Aug., 2015).
5. 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, (Nov., 2014).
6. Daisuke Fujimoto, Noriyuki Miura, Makoto Nagata, Yuichi Hayashi, Naofumi Homma, Takafumi Aoki, Yohei Hori, Toshihiro Katashita, Kazuo Sakiyama, Thanh-Ha Le, Julien Bringer, Pirouz Bazargan-Sabet, Shivam Bhasin, and Jean-Luc Danger, "Power Noise Measurements of Cryptographic VLSI Circuits Regarding Side-Channel Information Leakage," IEICE Trans. Electronics, Vol. E97-C, No.4, pp.272-279, (Apr., 2014).
7. Christophe Clavier, Jean-Luc Danger, Guillaume Duc, M. Abdelaziz Elaabid, Beno î t G é rard, Sylvain Guilley, Annelie Heuser, Michael Kasper, Yang Li, Victor Lomn é , Daisuke Nakatsu, Kazuo Ohta, Kazuo Sakiyama, Laurent Sauvage, Werner Schindler, Marc St ö ttinger, Nicolas Veyrat-Charvillon, Matthieu Walle, Antoine Wurcker, "Practical improvements of side-channel attacks on AES: feedback from the 2nd DPA contest, " J. Cryptographic Engineering, Vol.4(1), pp.1-16, (Apr., 2014).
8. Kazuo Sakiyama, Yang Li, Shigeto Gomisawa, Yu-ichi Hayashi, Mitsugu Iwamoto, Naofumi Homma, Takafumi Aoki, and Kazuo Ohta, "Practical DFA Strategy for AES Under Limited-Access Conditions," Journal of Information Processing, Vol.22, No.2, (Feb., 2014).

9. Dai Yamamoto, Kazuo Sakiyama, Mitsugu Iwamoto, Kazuo Ohta, Masahiko Takenaka, and Kouichi Itoh, "Variety Enhancement of PUF Responses Using the Locations of Random Outputting RS Latches," J. Cryptographic Engineering, Vol.3(4) pp.197-211, Springer, (Nov., 2013).

10. Shugo Mikami, Hirotaka Yoshida, Dai Watanabe, Kazuo Sakiyama, "Correlation Power Analysis and Countermeasure on the Stream Cipher Enocoro-128v2," IEICE Trans. Fundam. Electron. Commun. Comput. Sci., Vol.96-A, No.3, pp.697-704, (Mar., 2013).

11. Yang Li, Kazuo Ohta, and Kazuo Sakiyama, "A New Type of Fault-Based Attack: Fault Behavior Analysis," IEICE Trans. Fundam. Electron. Commun. Comput. Sci., Vol.A96-A, No.1, pp.177-184, (Jan., 2013).

12. 小池彩歌, 李陽, 中津大介, 太田和夫, 﨑山一男, "複数の要因に対する新たな故障感度解析," 電子情報通信学会論文誌 (A), Vol.J95-A, No.10, pp.751-755, (Oct., 2012).

13. Miroslav Knezevic, Kazuyuki Kobayashi, Jun Ikegami, Shin'ichiro Matsuo, Akashi Satoh, Unal Kocabas, Junfeng Fan, Toshihiro Katashita, Takeshi Sugawara, Kazuo Sakiyama, Ingrid Verbauwhede, Kazuo Ohta, Naofumi Homma, and Takafumi Aoki, "Fair and Consistent Hardware Evaluation of Fourteen Round Two SHA-3 Candidates," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., Vol.20, No.5, pp.827–840, (May, 2012).

14. Kazuo Sakiyama, Yang Li, Mitsugu Iwamoto, and Kazuo Ohta, "Information-Theoretic Approach to Optimal Differential Fault Analysis," IEEE Trans. Inf. Forensic Secur., Vol.7, No.1, pp.109-120, (Feb., 2012).

15. Yang Li, Kazuo Ohta, and Kazuo Sakiyama, "New Fault-Based Side-Channel Attack using Fault Sensitivity,"IEEE Trans. Inf. Forensic Secur., Vol.7, No.1, pp.88-97, (Feb., 2012).

16. Junko Takahashi, Toshinori Fukunaga, Kazuo Sakiyama, "Differential Fault Analysis on Stream Cipher MUGI,"IEICE Trans. Fundam. Electron. Commun. Comput. Sci., Vol.A95-A, No.1, pp.242-251, (Jan., 2012).

17. Yang Li, Kazuo Ohta, and Kazuo Sakiyama, "Toward Effective Countermeasures Against An Improved Fault Sensitivity Analysis," IEICE Trans. Fundam. Electron. Commun. Comput. Sci., Vol.A95-A, No.1, pp.234-241, (Jan., 2012).

18. Lei Wang, Yu Sasaki, Wataru Komatsubara, Kazuo Sakiyama, Kazuo Ohta, "Meet-in-the-Middle (Second) Preimage Attacks on Two Double-Branch Hash Functions RIPEMD and RIPEMD-128," IEICE Trans. Fundam. Electron. Commun. Comput. Sci., Vol.A95-A, No.1, pp.100-110, (Jan., 2012).

19. Kazuo Sakiyama, Miroslav Knezevic, Junfeng Fan, Bart Preneel, and Ingrid Verbauwhede, "Tripartite Modular Multiplication," Integration-VLSI J., Vol.44, Issue 4, pp.259-269, (Apr., 2011).

20. Yang Li, Kazuo Sakiyama, Shinichi Kawamura, and Kazuo Ohta, "Power Analysis against a DPA-resistant S-box Implementation Based on the Fourier Transform," IEICE Trans. Fundam. Electron. Commun. Comput. Sci., Vol.A94-A, No.1, pp.191-199, (Jan., 2011).

21. Bagus Santoso, Kazuo Ohta, Kazuo Sakiyama, Goichiro Hanaoka, "An Efficient Authentication for Lightweight Devices by Perfecting Zero-Knowledgeness," IEICE Trans. Fundam. Electron. Commun. Comput. Sci., Vol.A94-A, No.1, pp.92-103, (Jan., 2011).

22. Lei Wang, Kazuo Ohta, Yu Sasaki, Kazuo Sakiyama, and Noboru Kunihiro, "Cryptanalysis of Two MD5-Based Authentication Protocols: APOP and NMAC," IEICE Trans. Inf. & Syst., Vol.E93-D, (May, 2010).

23. Kazuo Sakiyama and Kazuo Ohta, "On Clock-based Fault Analysis Attack for an AES Hardware Using RSL," IEICE Trans. Fundam. Electron. Commun. Comput. Sci., Vol.E93-A, No.01, pp.172-179, (Jan., 2010).

24. Yong Ki Lee, Kazuo Sakiyama, Lejla Batina, and Ingrid Verbauwhede, "Elliptic Curve Based Security Processor for RFID," IEEE Trans. Comput., Vol.57, No.11, pp.1514-1527, (Nov., 2008).

25. Junfeng Fan, Kazuo Sakiyama, and Ingrid Verbauwhede, "Elliptic Curve Cryptography on Embedded Multicore Systems," Des. Autom. Embed. Syst., Vol.12, No.3, pp.231-242, (Sep., 2008).

26. Kazuo Sakiyama, Lejla Batina, Bart Preneel, and Ingrid Verbauwhede, "Multi-core Curve-based Cryptoprocessor with Reconfigurable Modular Arithmetic Logic Units over GF(2^n)," IEEE Trans. Comput., Vol.56, No.9, pp.1269-1282, (Sep., 2007).

27. Kazuo Sakiyama, Lejla Batina, Bart Preneel, and Ingrid Verbauwhede, "HW/SW Co-design for Public-Key Cryptosystems on the 8051 Micro-controller, Computers & Electrical Engineering," Vol.33, No.5-6, pp.324-332, (Sep., 2007).

28. Kazuo Sakiyama, Lejla Batina, Bart Preneel, and Ingrid Verbauwhede, "High-performance Public-key Cryptoprocessor for Wireless Mobile Applications," Mob. Netw. Appl., Vol.12, No.4, pp.245-258, (Aug., 2007).

29. Kazuo Sakiyama, Nele Mentens, Lejla Batina, Bart Preneel, and Ingrid Verbauwhede, "Reconfigurable Modular Arithmetic Logic Unit Supporting High-performance RSA and ECC over GF(p)," International Journal of Electronics, Vol.94, No.5, pp.501-514, (May, 2007).

30. Shenglin Yang, Kazuo Sakiyama, and Ingrid Verbauwhede, "Efficient and Secure Fingerprint Verification for Embedded Devices," EURASIP J. Adv. Signal Process., Vol.2006, No.1-11, (May, 2006).

31. Young-Jae Cho, Takashi Hirakawa, Kazuo Sakiyama, Hiroaki Okamoto, and Yoshihiro Hamakawa, "EL/PL hybrid device enhanced by UV emission from ZnF_2:Gd thin film electroluminescence," J. Korean. Phys. Soc., Vol.30(1997), pp.S65-S68, (Jun., 1997).

32. Young-Jae Cho, Takashi Hirakawa, Kazuo Sakiyama, Hiroaki Okamoto, and Yoshihiro Hamakawa, "ZnF_2:Gd Thin Film Electroluminescent Device," Appl. Surf. Sci., Vol.113-114 (1997), pp.705-708, (Apr., 1997).

III *Conference Papers (with Peer Reviews)*

1. Momoka Kasuya, Takanori Machida, and Kazuo Sakiyama, "New Metric for Side-Channel Information Leakage: Case Study on EM Radiation from AES Hardware," In Proc. URSI Asia-Pacific Radio Science Conference (URSI AP-RASC'16), IEEE, (to appear in Aug., 2016).

2. Kazuo Sakiyama, Reina Yagasaki, Takanori Machida, Tatsuya Fujii, Noriyuki Miura, and Yu-ichi Hayashi, "Circuit-Level Information Leakage Prevention for Fault Detection," In Proc. URSI Asia-Pacific Radio Science Conference (URSI AP-RASC'16), IEEE, (to appear in Aug., 2016).

3. Kazuo Sakiyama, Momoka Kasuya, Takanori Machida, Arisa Matsubara, Yunfeng Kuai, Yu-ichi Hayashi, Takaaki Mizuki, Noriyuki Miura, and Makoto Nagata, "Physical Authentication Using Side-Channel Information," In Proc. International Conference on Information and Communication Technology (ICoICT'16), IEEE, (May, 2016).

4. Shugo Mikami, Dai Watanabe, Kazuo Sakiyama, "A Performance Evaluation of Cryptographic Algorithms on FPGA and ASIC on RFID Design Flow," In Proc. International Conference on Information and Communication Technology (ICoICT'16), IEEE, (May, 2016).

5. Reina Yagasaki and Kazuo Sakiyama, "Artifact-Metric-Based Authentication for Bottles of Wine," In Proc. International Workshop on Security 2015 (IWSEC'15), LNCS 9241, Springer-Verlag, pp.335-344, (Aug., 2015).

6. Kazuo Sakiyama, Takanori Machida, and Arisa Matsubara, "Advanced Fault Analysis Techniques on AES," In Proc. Joint IEEE International Symposium on Electromagnetic Compatibility and EMC Europe (EMC'15), pp.230-234, IEEE, (Aug., 2015).

7. Takanori Machida, Dai Yamamoto, Mitsugu Iwamoto, and Kazuo Sakiyama, "Implementation of Double Arbiter PUF and Its Performance Evaluation on FPGA," 20th Asia and South Pacific Design Automation Conference (ASP-DAC'15), pp.6-7, IEEE, (Jan., 2015).

8. Yang Li, Shugo Mikami, Dai Watanabe, Kazuo Ohta, and Kazuo Sakiyama, "Single-Chip Implementation and Evaluation of Passive UHF RFID Tag with Hash-Based Mutual Authentication," In Proc. Workshop on RFID Security (RFIDsec'14 Asia), IOS Press, pp.3-15, (Nov., 2014).

9. Takanori Machida, Dai Yamamoto, Mitsugu Iwamoto, and Kazuo Sakiyama, "A New Mode of Operation for Arbiter PUF to Improve Uniqueness on FPGA," In Proc. The Federated Conference on Computer Science and Information Systems (FedCSIS), 1st Workshop on Emerging Aspects in Information Security (EAIS'14), IEEE, pp.871-878 (Sep., 2014).

10. Dai Yamamoto, Masahiko Takenaka, Kazuo Sakiyama, and Naoya Torii, "Security Evaluation of Bistable Ring PUFs on FPGAs using Differential and Linear Analysis," In Proc. The Federated Conference on Computer Science and Information Systems (FedCSIS), 1st Workshop on Emerging Aspects in Information Security (EAIS'14), IEEE, pp.911-918 (Sep., 2014).

11. Dai Yamamoto, Masahiko Takenaka, Kazuo Sakiyama, and Naoya Torii, "A Technique using PUFs for Protecting Circuit Layout Designs against Reverse Engineering," In Proc. International Workshop on Security 2014 (IWSEC'14), LNCS 8639, Springer-Verlag, pp.158-253, (Sep., 2014).

12. Yang Li, Toshiki Nakasone, and Kazuo Sakiyama, "Software and Hardware Co-Verification for Privacy-Enhanced Passive UHF RFID Tags," In Proc. 2014 IEEE International Symposium on Electromagnetic Compatibility (EMC'14), IEEE, pp.752-757 (Aug., 2014).

13. Daisuke Fujimoto, Noriyuki Miura, Makoto Nagata, Yuichi Hayashi, Naofumi Homma, Takafumi Aoki, Yohei Hori, Toshihiro Katashita, Kazuo Sakiyama, Thanh-Ha Le, Julien Bringer, Pirouz Bazargan-Sabet, Shivam Bhasin, and Jean-Luc Danger, "Correlation Power Analysis using Bit-Level Biased Activity Plaintexts against AES Core with Countermeasures," in Proc. 2014 International Symposium on Electromagnetic Compatibility, Tokyo (EMC'14/Tokyo), IEEE, pp 306-309, 14P2-A3, (May, 2014).

14. Yang Li, Toshiki Nakasone, Kazuo Ohta, Kazuo Sakiyama, "Privacy-Mode Switching: Toward Flexible Privacy Protection for RFID Tags in Internet of Things," In Proc. The 11th Annual IEEE Consumer Communications & Networking Conference (CCNC'14), IEEE, pp.519-520, (Jan., 2014).

15. Shugo Mikami, Dai Watanabe, and Kazuo Sakiyama, "A Comparative Study of Stream Ciphers and Hash Functions for RFID Authentications," In Proc. The 2013 Workshop on RFID and IoT Security (RFIDsec'13 Asia), IOS Press, pp.83-94, (Nov., 2013).

16. Yang Li, Yu-ichi Hayashi, Arisa Matsubara, Naofumi Homma, Takafumi Aoki, Kazuo Ohta and Kazuo Sakiyama, "Yet Another Fault-Based Leakage in Non-Uniform Faulty Ciphertexts," In Proc. The Sixth International Symposium on Foundations & Practice of Security (FPS'13), LNCS 8352, pp.272-287, Springer-Verlag, (Oct., 2013).

17. Daisuke Fujimoto, Noriyuki Miura, Makoto Nagata, Yuichi Hayashi, Naofumi Homma, Yohei Hori, Toshihiro Katashita, Kazuo Sakiyama, Thanh-Ha Le, Julien Bringer, Pirouz Bazargan-Sabet, Jean-Luc Danger, "On-chip power noise measurements of cryptographic VLSI circuits and interpretation for

side-channel analysis," In Proc. International Symposium on Electromagnetic Compatibility (EMC EUROPE) 2013, IEEE, pp.405-410, (Sep., 2013).

18. Toshiki Nakasone, Kazuo Sakiyama, Yang Li, and Kazuo Ohta, "Exploration of the CC-EMA Attack Towards Efficient Evaluation of EM Information Leakage," In Proc. International Symposium on Electromagnetic Compatibility (EMC EUROPE) 2013, IEEE, pp.411-414, (Sep., 2013).

19. Yu Sasaki, Wataru Komatsubara, Lei Wang, Mitsugu Iwamoto, Kazuo Ohta, and Kazuo Sakiyama, "Meet-in-the-Middle Preimage Attacks Revisited: New Results on MD5 and HAVAL," International Conference on Security and Cryptography (SECRYPT'13), LNCS, Springer-Verlag, (Jul., 2013).

20. Yu Sasaki, Yang Li, Hikaru Sakamoto and Kazuo Sakiyama, "Coupon Collector's Problem for Fault Analysis — High Tolerance for Noisy Fault Injections," In Proc. Financial Cryptography and Data Security 2013 (FC'13), LNCS 7859, Springer-Verlag, pp.213–220, (Apr., 2013).

21. Yang Li, Sho Endo, Nicolas Debande, Naofumi Homma, Takafumi Aoki, Thanh-Ha Le, Jean-Luc Danger, Kazuo Ohta, Kazuo Sakiyama, "Exploring the Relations Between Fault Sensitivity and Power Consumption," In Proc. Constructive Side-Channel Analysis and Secure Design (COSADE'13), LNCS 7864, Springer-Verlag, pp.137–153 (Mar., 2013).

22. Yang Li, Kazuo Ohta, and Kazuo Sakiyama, "An Extension of Fault Sensitivity Analysis Based on Clockwise Collision," In Proc. International Conferences on Information Security and Cryptology 2012 (Inscript'12), LNCS 7763, Springer-Verlag, pp.46–59, (Nov., 2012).

23. Toshiki Nakasone, Yu Sasaki, Yang Li, Mitsugu Iwamoto, Kazuo Ohta, and Kazuo Sakiyama, "Key-Dependent Weakness of AES-Based Ciphers Under Clockwise Collision Distinguisher," In Proc. International Conference on Information Security and Cryptology 2012 (ICISC'12), LNCS 7839, Springer-Verlag, pp.395-409, (Nov., 2012).

24. Yu Sasaki, Lei Wang, Yasuhiro Takasaki, Kazuo Sakiyama, and Kazuo Ohta, "Boomerang Distinguishers for Full HAS-160 Compression Function," In Proc. International Workshop on Security 2012 (IWSEC'12), LNCS 7631, Springer-Verlag, pp.156-169, (Nov., 2012).

25. Lei Wang, Yu Sasaki, Kazuo Sakiyama, and Kazuo Ohta, "Cryptanalysis of 3D Cipher and 3D-based Hash Function," In Proc. International Workshop on Security 2012 (IWSEC'12), LNCS 7631, Springer-Verlag, pp.170-181, (Nov., 2012).

26. Sho Endo, Yang Li, Naofumi Homma, Kazuo Sakiyama, Kazuo Ohta, and Takafumi Aoki, "An Efficient Countermeasure against Fault Sensitivity Analysis Using Configurable Delay Blocks," In Proc. Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC'12), IEEE, pp.95-102, (Sep., 2012).

27. Sho Endo, Yuichi Hayashi, Naofumi Homma, Takafumi Aoki, Toshihiro Katashita, Yohei Hori, Kazuo Sakiyama, Makoto Nagata, Jean-Luc Danger, Thanh-Ha Le and Pirouz Bazargan Sabet, "Measurement of Side-Channel Information from Cryptographic Devices on Security Evaluation Platform: Demonstration of SPACES Project," SICE Annual Conference 2012, pp.313 – 316, (Aug., 2012).

28. Yu Sasaki, Lei Wang, Yasuhide Sakai, Kazuo Sakiyama, and Kazuo Ohta, "Three-Subset Meet-in-the-Middle Attack on Reduced XTEA," In Proc. International Conference on Cryptology in Africa (Africacrypt'12), LNCS 7374, Springer-Verlag, pp.138-154, (Jul. 2012).

29. Takuma Koyama, Lei Wang, Yu Sasaki, Kazuo Sakiyama, and Kazuo Ohta, "New Truncated Differential Cryptanalysis on 3D Block Cipher," In Proc. International Conference on Information Security Practice and Experience (ISPEC'12), LNCS 7232, Springer-Verlag, pp.109-125, (Apr., 2012).

30. Yu Sasaki, Naoyuki Takayanagi, Kazuo Sakiyama, and Kazuo Ohta, "Experimental Verification of Super-Sbox Analysis — Confirmation of Detailed Attack Complexity," In Proc. International Workshop on Security 2011 (IWSEC'11), LNCS 7038, Springer-Verlag, pp.178-192, (Nov., 2011).

31. Yu-ichi Hayashi, Shigeto Gomisawa, Yang Li, Naofumi Homma, Kazuo Sakiyama, Takafumi Aoki, and Kazuo Ohta, "Intentional Electromagnetic Interference for Fault Analysis on AES Block Cipher IC," In Proc. International Workshop on Electromagnetic Compatibility of Integrated Circuits (EMCCOMPO'11), IEEE, pp.235-240, (Nov., 2011).

32. Dai Yamamoto, Kazuo Sakiyama, Mitsugu Iwamoto, Kazuo Ohta, Takao Ochiai, Masahiko Takenaka, Kouichi Itoh, "Uniqueness Enhancement of PUF Responses Based on the Locations of Random Outputting RS Latches," In Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES'11), LNCS 6917, Springer-Verlag, pp.390-406, (Sep., 2011).

33. Amir Moradi, Oliver Mischke, Christof Paar, Yang Li, Kazuo Ohta, Kazuo Sakiyama, "On the Power of Fault Sensitivity Analysis and Collision Side-Channel Attack in a Combined Setting," In Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES'11), LNCS 6917, Springer-Verlag, pp.292-311, (Sep., 2011).

34. Hikaru Sakamoto, Yang Li, Kazuo Ohta, and Kazuo Sakiyama, "Fault Sensitivity Analysis Against Elliptic Curve Cryptosystems," In Proc. Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC'11), IEEE, pp.11-20, (Sep., 2011).

35. Yang Li, Kazuo Ohta, and Kazuo Sakiyama, "Revisit Fault Sensitivity Analysis on WDDL-AES," In Proc. International Symposium on Hardware-Oriented Security and Trust (HOST'11), IEEE, pp.148-153, (Jun., 2011).

36. Yoshikazu Hanatani, Miyako Ohkubo, Shin'ichiro Matsuo, Kazuo Sakiyama, Kazuo Ohta, "A Study on Computational Formal Verification for Practical Cryptographic Protocol: The Case of Synchronous RFID Authentication," In Proc. Real-Life Cryptographic Protocols and Standarization (RLCPS'11), LNCS 7126, Springer-Verlag, pp.70-87, (Feb., 2011).

37. Lei Wang, Yu Sasaki, Wataru Komatsubara, Kazuo Ohta, and Kazuo Sakiyama, "(Second) Preimage Attacks on Step-Reduced RIPEMD/RIPEMD-128 with a New Local-Collision Approach," In Proc. RSA Conference 2011, Cryptographer's Track (CT-RSA'11), LNCS 6558, Springer-Verlag, pp.197-212, (Mar., 2011).

38. Yu Sasaki, Yang Li, Lei Wang, Kazuo Sakiyama, and Kazuo Ohta, "Non-full-active Super-Sbox Analysis: Applications to ECHO and Grøstl," In Proc. Advances in Cryptology — ASIACRYPT'10, LNCS 6477, Springer-Verlag, pp.38-55, (Dec., 2010).

39. Junko Takahashi, Toshinori Fukunaga, and Kazuo Sakiyama, "Fault Analysis on Stream Cipher MUGI," In Proc. International Conference on Information Security and Cryptology (ICISC'10), LNCS 6829, Springer-Verlag, pp.420-434, (Dec. 2010).

40. Daisuke Nakatsu, Yang Li, Kazuo Sakiyama, and Kazuo Ohta, "Combination of SW Countermeasure and CPU Modification on FPGA Against Power Analysis," In Proc. International Workshop on Information Security Applications (WISA'10), LNCS 6513, Springer-Verlag, pp.258-272, (Aug., 2010).

41. Yang Li, Kazuo Sakiyama, Shigeto Gomisawa, Toshinori Fukunaga, Junko Takahashi, and Kazuo Ohta, "Fault Sensitive Analysis," In Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES'10), LNCS 6225, Springer-Verlag, pp.320-334, (Aug., 2010).

42. Kazuyuki Kobayashi, Jun Ikegami, Miroslav Knezevic, Eric Xu Guo, Shin'ichiro Matsuo, Sinan Huan, Leyla Nazhandali, Ü nal Kocaba ş , Junfeng Fan, Akashi Satoh, Patrick Schaumont, Ingrid Verbauwhede, Kazuo Sakiyama, and Kazuo Ohta, "Prototyping Platform for Performance Evaluation of

SHA-3 Candidates," In Proc. International Symposium on Hardware-Oriented Security and Trust (HOST'10), IEEE, pp.60-63, (Jun., 2010).

43. Yang Li, Kazuo Sakiyama, Lejla Batina, Daisuke Nakatsu, and Kazuo Ohta, "Power Variance Analysis Breaks a Masked ASIC Implementations of AES," In Proc. Design, Automation and Test in Europe (DATE'10), ACM, pp.1059-1064, (Mar., 2010).
44. Masami Izumi, Jun Ikegami, Kazuo Sakiyama, and Kazuo Ohta, "Improved Countermeasure against Address-bit DPA for ECC Scalar Multiplication," In Proc. Design, Automation and Test in Europe (DATE'10), ACM, pp.981-984, (Mar., 2010).
45. Bagus Santoso, Kazuo Ohta, Kazuo Sakiyama, and Goichiro Hanaoka, "Improving Efficiency of An 'On the Fly' Identification Scheme by Perfecting Zero-Knowledgeness," In Proc. RSA Conference 2009, Cryptographer's Track (CT-RSA'10), (Mar., 2010).
46. Yang Li, Kazuo Sakiyama, Shinichi Kawamura, Yuichi Komano, and Kazuo Ohta, "Security Evaluation of a DPA-resistant S-Box Based on the Fourier Transform," In Proc. Eleventh International Conference on Information and Communications Security (ICICS'09), LNCS 5927, Springer-Verlag, pp.3-16, (Dec., 2009).
47. Lei Wang, Yu Sasaki, Kazuo Sakiyama, and Kazuo Ohta, "Bit-Free Collision: Application to APOP Attack," In Proc. International Workshop on Security 2009 (IWSEC'09), LNCS 5824, Springer-Verlag, pp.3-21, (Oct., 2009).
48. Kazuo Sakiyama, Tatsuya Yagi, and Kazuo Ohta, "Fault Analysis Attack against an AES Prototype Chip Using RSL," In Proc. RSA Conference 2009, Cryptographer's Track (CT-RSA'09), LNCS 5473, Springer-Verlag, pp.429-443, (Apr., 2009).
49. Masami Izumi, Kazuo Sakiyama, and Kazuo Ohta, "A New Approach for Implementing the MPL Method toward Higher SPA Resistance," In Proc. International Conference on Availability, Reliability and Security (ARES'09), pp.181-186, (Mar., 2009).
50. Miroslav Knezevic, Kazuo Sakiyama, Junfeng Fan, and Ingrid Verbauwhede, "Modular Multiplication in GF(2n) without Pre-computational Phase," In International Workshop on the Arithmetic of Finite Fields (WAIFI'08), LNCS 5130, Springer-Verlag, pp.77-87, (Jul., 2008).
51. Miroslav Knezevic, Kazuo Sakiyama, Yong Ki Lee, and Ingrid Verbauwhede, "On the High-Throughput Implementation of RIPEMD-160 Hash Algorithm," In Proc. 19th IEEE International Conference on Application-specific Systems, Architectures and Processor (ASAP'08), IEEE, pp.85-90, (Jul., 2008).
52. Junfeng Fan, Lejla Batina, Kazuo Sakiyama, and Ingrid Verbauwhede, "FPGA Design for Algebraic Tori-Based Public-Key Cryptography," In Proc. Design, Automation and Test in Europe (DATE'08), ACM, pp.1292-1297, (Mar., 2008).
53. Junfeng Fan, Kazuo Sakiyama, and Ingrid Verbauwhede, "Montgomery Modular Multiplication Algorithm on Multi-Core Systems," In Proc. IEEE Workshop on Signal Processing Systems (SIPS'07), IEEE, pp.261-266, (Oct., 2007).
54. Nele Mentens, Kazuo Sakiyama, Lejla Batina, Bart Preneel, and Ingrid Verbauwhede, "A Side-channel Attack Resistant Programmable PKC Coprocessor for Embedded Applications," In Proc. International Symposium on Systems, Architectures, MOdeling and Simulation (IC-SAMOS'07), IEEE, pp.194-200, (Jul., 2007).
55. Lejla Batina, Nele Mentens, Kazuo Sakiyama, Bart Preneel, and Ingrid Verbauwhede, "Public-Key Cryptography on the Top of a Needle," In Proc. IEEE International Symposium on Circuits and Systems (ISCAS'07), Special Session: Novel Cryptographic Architectures for Low-Cost RFID, IEEE, pp.1831-1834, (May, 2007).

56. Kazuo Sakiyama, Elke De Mulder, Bart Preneel, and Ingrid Verbauwhede, "Side-channel Resistant System-level Design Flow for Public-key Cryptography," In Proc. 2007 Great Lakes Symposium on VLSI (GLSVLSI'07), ACM, pp.144-147, (Mar., 2007).

57. Nele Mentens, Kazuo Sakiyama, Bart Preneel, and Ingrid Verbauwhede, "Efficient Pipelining for Modular Multiplication Architectures in Prime Fields," In Proc. 2007 Great Lakes Symposium on VLSI (GLSVLSI'07), ACM, pp.534-539, (Mar., 2007).

58. Kazuo Sakiyama, Lejla Batina, Bart Preneel, and Ingrid Verbauwhede, "Superscalar Coprocessor for High-speed Curve-based Cryptography," In Cryptographic Hardware and Embedded Systems (CHES'06), LNCS 4249, Springer-Verlag, pp.415-429, (Oct., 2006).

59. Lejla Batina, Nele Mentens, Kazuo Sakiyama, Bart Preneel, and Ingrid Verbauwhede, "Low-Cost Elliptic Curve Cryptography for Wireless Sensor Networks," In Third European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS'06), LNCS 4357, Springer-Verlag, pp.6-17, (Sep., 2006).

60. Lejla Batina, Alireza Hodjat, David Hwang, Kazuo Sakiyama, and Ingrid Verbauwhede, "Reconfigurable Architectures for Curve-based Cryptography on Embedded Micro-controllers," In Proc. 16th International Conference on Field Programmable Logic and Applications (FPL'06), IEEE, pp.667-670, (Aug., 2006).

61. Nele Mentens, Kazuo Sakiyama, Lejla Batina, Ingrid Verbauwhede, and Bart Preneel, "FPGA-Oriented Secure Data Path Design: Implementation of a Public Key Coprocessor," In Proc. 16th International Conference on Field Programmable Logic and Applications (FPL'06), IEEE, pp.133-138, (Aug., 2006).

62. Kazuo Sakiyama, Lejla Batina, Bart Preneel, and Ingrid Verbauwhede, "HW/SW Co-design for Accelerating Public-Key Cryptosystems over GF(p) on the 8051 μ-controller," In Proc. World Automation Congress (WAC'06), 6 pages, (Jul., 2006).

63. Kazuo Sakiyama, Elke De Mulder, Bart Preneel, and Ingrid Verbauwhede, "A Parallel Processing Hardware Architecture for Elliptic Curve Cryptosystems," In Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'06), IEEE, pp.III-904-III-907, (May, 2006).

64. Kazuo Sakiyama, Bart Preneel, and Ingrid Verbauwhede, "A Fast Dual-Field Modular Arithmetic Logic Unit and Its Hardware Implementation," In Proc. IEEE International Symposium on Circuits and Systems (ISCAS'06), IEEE, pp.787-790, (May, 2006).

65. Kazuo Sakiyama, Nele Mentens, Lejla Batina, Bart Preneel, and Ingrid Verbauwhede, "Reconfigurable Modular Arithmetic Logic Unit for High-performance Public-key Cryptosystems," In International Workshop on Applied Reconfigurable Computing (ARC'06), LNCS 3985, Springer-Verlag, pp.347-357, (Mar., 2006).

66. Patrick Schaumont, Kazuo Sakiyama, Alireza Hodjat, and Ingrid Verbauwhede, "Embedded Software Integration for Coarse-grain Reconfigurable Systems," In Proc. IEEE 18th International Parallel and Distributed Processing Symposium (IPDPS'04), IEEE, pp.137-142, (Apr., 2004).

67. Shenglin Yang, Kazuo Sakiyama, and Ingrid Verbauwhede, "A Compact and Efficient Fingerprint Verification System for an Embedded Device," In Proc. 37th Asilomar Conference on Signals, Systems and Computers, pp.2058-2062, (Nov., 2003).

68. Patrick Schaumont, Kazuo Sakiyama, Yi Fan, David Hwang, Shenglin Yang, Alireza Hodjat, Bo-Cheng Lai, and Ingrid Verbauwhede, "Testing ThumbPod: Softcore Bugs are Hard to Find," In Proc. IEEE International High Level Design Validation and Test Workshop (HLDVT'03), IEEE, pp.77-82, (Nov., 2003).

69. David Hwang, Patrick Schaumont, Yi Fan, Alireza Hodjat, Bo-Cheng Lai, Kazuo Sakiyama, Shenglin Yang, and Ingrid Verbauwhede, "Design flow for HW/SW Acceleration Transparency in the Thumbpod Secure Embedded System," In Proc. 40th Design Automation Conference (DAC'03), ACM, pp.60-65, (Jun., 2003).

70. Kazuo Sakiyama, Patrick Schaumont, David Hwang, and Ingrid Verbauwhede, "Teaching Trade-offs in System-level Design Methodologies," In Proc. IEEE Microelectronic Systems Education (MSE'03), IEEE, pp.62-63, (Jun., 2003).

71. Kazuo Sakiyama, Patrick Schaumont, and Ingrid Verbauwhede, "Finding the best System Design Flow for a High-Speed JPEG Encoder," In Proc. 8th Asia and South Pacific Design Automation Conference (ASP-DAC'03), ACM, pp.577-578, (Jan., 2003).

72. Young-Jae Cho, Takashi Hirakawa, Kazuo Sakiyama, Hiroaki Okamoto, and Yoshihiro Hamakawa, "ZnF_2:Gd UV Emitting Electroluminescent Device," In Proc. 8th International Workshop on Electroluminescence, Wissenschaft und Technik Verlag, pp.347-350 (Aug. 1996).

73. Young-Jae Cho, Takashi Hirakawa, Kazuo Sakiyama, Hiroaki Okamoto, and Yoshihiro Hamakawa, "ZnF_2:Gd Thin Film Electroluminescent Devices," In Proc. 8th International Conference Solid Films and Surface, (Jul., 1996).

IV *Lecture, Tutorial, and Panel Discussion*

1. Dagstuhl Seminar 16202, "Hardware Security," (16-20, May, 2016).

2. Yang Li, Kazuo Sakiyama, "Review Fault Attacks on ECC Implementations with Fault Sensitivity Analysis," A-SSCC 2015 レビュー講演, IEEE SSCS Japan/Kansai Chapter Technical Seminar, (2016 年 1 月 13 日).

3. Yang Li, Kazuo Sakiyama, "Review Fault Attacks on ECC Implementations with Fault Sensitivity Analysis," IEEE Asian Solid-State Circuits Conference 2015, (A-SSCC'15), (Nov., 10th, 2015).

4. Kazuo Sakiyama, "Hardware Implementations of ECC," Summer school on real-world crypto and privacy, (2015 年 6 月 4 日).

5. 崎山一男, "暗号ハードウェアからの情報漏洩," 日本学術振興会シリコン超集積化システム第 165 委員会, (2015 年 5 月 15 日).

6. Kazuo Sakiyama, "Fault Analysis for Cryptosystems: Introduction to Differential Fault Analysis and Fault Sensitivity Analysis," Tutorial-4: Hardware Trust in VLSI Design and

7. Implementations, Asia and South Pacific Design Automation Conference (ASP-DAC'15), Tutorial Session, (Jan., 2015).

8. NII Shonan Meeting, "Design Methods for Secure Hardware," (15-19, Sep., 2014).

9. 李陽, 崎山一男, "Two Topics in Cryptographic Hardware: Coupon DFA and Secure RFID," Compview 暗号理論ワークショップ 2013, (2013 年 2 月 21 日).

10. 崎山一男, 李陽, " 故障感度解析の可能性," Hot Channel Workshop 2012, (2012 年 9 月 5 日).

11. 崎山一男, "故障感度解析とその応用について," 16 回情報科学研究科セミナー@JAIST, (2012 年 3 月 5 日).

12. 崎山一男, "Fault Behavior Analysis," Compview 暗号理論ワークショップ 2012, (2012 年 2 月 21 日).

13. 崎山一男, "Fault Sensitivity Analysis," Compview 暗号理論ワークショップ 2011, (2011 年 2 月 21 日).

14. Kazuo Sakiyama, "A New Fault Analysis Attack (joint work with Yang Li and Kazuo Ohta)," 2010 Japan-Taiwan Joint Research Symposium on Cryptography and Next IT-society, (Nov. 16th, 2010).
15. Kazuo Sakiyama, "Cryptanalysis and Side-channel Analysis – Approach to Optimal Differential Fault Analysis (joint work with Yang Li and Kazuo Ohta)," Forum Math-for-Industry 2010, (Oct. 22nd, 2010).
16. パネルセッション "暗号技術の実装について," CRYPTREC シンポジウム 2010, (2010 年 3 月 2 日)
17. "暗号理論に関する問題提起と討論," Compview 暗号理論ワークショップ 2010, (2010 年 2 月 25 日).
18. 崎山一男, "サイドチャネル攻撃への対策とその副作用," RSA Conference Japan 2009, クラストラック：暗号技術の最新動向 (RC-03), (2009 年 6 月 10 日).
19. Lejla Batina and Kazuo Sakiyama, "Compact Implementations for RFID and Sensor Nodes," Special Interest Workshops – Secure Embedded Implementations, Design, Automation and Test in Europe (DATE'07), (Apr., 2007).

V *Articles*

1. 崎山一男, 太田 和夫, "現代暗号を脅かす「サイドチャネル攻撃」とは,"「科学」報告・解説, 岩波書店, Vol.78, No.10, pp.1080-1083, (2008 年 10 月).

VI *Other Conference Papers*

1. 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," IEICE2016 年総合大会, (Mar., 2016).
2. 粕谷桃伽, 町田卓謙, 崎山一男, "サイドチャネル情報における固有性解析," IEICE2016 年総合大会（学生ポスターセッション）, (Mar., 2016).
3. 藤本大介, 照屋唯紀, 崎山一男, 本間尚文, 池田誠, 永田真, 松本勉, "並列化 RNS アーキテクチャによる高速ペアリング実装に関する検討," 2016 年暗号と情報セキュリティシンポジウム (SCIS2016), 2C4-3, 6 pages, (Jan., 2016).
4. 松田航平, 三浦典之, 永田真, 林優一, 藤井達哉, 矢ヶ﨑玲奈, 崎山一男, "レーザーフォールト注入時の IC 基板電位変動のオンチップ測定," 2016 年暗号と情報セキュリティシンポジウム (SCIS2016), 2F1-4, 6 pages, (Jan., 2016).
5. 粕谷桃伽, 町田卓謙, 崎山一男, "AES 暗号を用いたサイドチャネル認証における識別可能なデバイス数," 2016 年暗号と情報セキュリティシンポジウム (SCIS2016), 1F2-3, 4 pages, (Jan., 2016).
6. 藤井達哉, 粕谷桃伽, 町田卓謙, 崎山一男, "DE0-nano を用いたサイドチャネル認証," コンピュータセキュリティシンポジウム 2015（CSS2015）デモンストレーション（ポスター）セッション, (Oct., 2015).
7. 粕谷桃伽, 町田卓謙, 崎山一男, "漏洩電磁波を用いたサイドチャネル認証の基礎実験," IEICE2015 年ソサイエティ大会, (Sep., 2015).
8. 矢ヶ﨑玲奈, 崎山一男, "ワイン瓶の透過光を用いた人工物メトリクスに関する研究," IEICE2015 年総合大会, (Mar., 2015).
9. 酒井芳章, 崎山一男, "Android 端末に向けた新たな認証システム," IEICE2015 年総合大会（学生ポスターセッション）, (Mar., 2015).
10. 川述優, 崎山一男, "物理特性の変更が可能な RO-PUF," IEICE2015 年総合大会（学生ポスターセッション）, (Mar., 2015).

11. 松原有沙, 町田卓謙, 崎山一男, “ランダム故障混入時の AES 暗号回路への故障利用攻撃,” IEICE2015 年総合大会（学生ポスターセッション）, (Mar., 2015).
12. 松原 有沙, 町田 卓謙, 林優一, 崎山 一男, “サイドチャネル認証の為の漏洩モデルに関する一考察,” 2015 年暗号と情報セキュリティシンポジウム (SCIS2015), 3A2-1, 6 pages, (Jan., 2015).
13. カイ 云峰, 李 陽, 町田 卓謙, 崎山 一男, “AES ハードウェア実装の任意ラウンドにおける消費電力制御,” 2015 年暗号と情報セキュリティシンポジウム (SCIS2015), 3A2-2, 7 pages, (Jan., 2015).
14. 三上修吾, 渡辺大, 崎山一男, “バッファを用いた軽量擬似乱数生成器のグリッチ削減方法とハードウェア実装評価,” コンピュータセキュリティシンポジウム 2014（CSS2014）, 1C3, 6 pages, (Oct., 2014).
15. 松原有沙, 李陽, 林優一, 崎山一男, “サイドチャネル認証に向けた基礎的考察,” ISEC2014-10, pp.1-8, (Jul., 2014).
16. Yang Li and Kazuo Sakiyama, “Toward Practical Solution to Unsuccessful Write Operation on Non-Volatile Memory of Passive RFID Tags,” Poster Session, ASIACCS2014 (Jun., 2014).
17. 稲毛契, 藤井威生, 高橋謙三, 山尾泰, 崎山一男, “ICT 国際 PBL (1)：国際性と実践力に優れた高度専門人材育成,” IEICE2014 年総合大会, (Mar., 2014).
18. 大竹健太, 稲毛契, 戴競擇, 藤井威生, 山尾泰, 崎山一男, “ICT 国際 PBL (2)：無線ネットワークによるロボットカー制御プロジェクト,” IEICE2014 年総合大会, (Mar., 2014).
19. 中曽根俊貴, 崎山一男, “ICT 国際 PBL (3)：ハッシュ関数 SHA-256 の高速実装,” IEICE2014 年総合大会, (Mar., 2014).
20. 福井言葉, 船橋鴻志, 高橋謙三, 山尾泰, 小島年春, 崎山一男, “ICT 国際 PBL(4):ディジタル信号処理,” IEICE2014 年総合大会, (Mar., 2014).
21. 藤本大介, 田中大智, 三浦典之, 永田真, 林優一, 本間尚文, 青木孝文, 堀洋平, 片下敏広, 崎山一男, Thanh-Ha Le, Julien Bringer, Pirouz Bazargan-Sabet, Shivam Bhasin, Jean-Luc Danger, “チップ内外での電源電圧取得によるサイドチャネル漏洩情報の一考察,” 2014 年 暗号と情報セキュリティシンポジウム (SCIS2014), 2A3-3, 6 pages, (Jan., 2014).
22. 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,” 2014 年 暗号と情報セキュリティシンポジウム (SCIS2014), 2A1-5, 5 pages, (Jan., 2014).
23. 三上修吾, 渡辺大, 崎山一男, “バッファを用いた軽量擬似乱数生成器のハードウェア実装と評価,” 2014 年 暗号と情報セキュリティシンポジウム (SCIS2014), 2A2-1, 7 pages, (Jan., 2014).
24. Takanori Machida, Toshiki Nakasone, Mitsugu Iwamoto, and Kazuo Sakiyama, “A New Model of Modeling Attacks against Arbiter PUF on FPGA,” Poster Session, IWSEC2013 (Nov., 2013).
25. Yang Li, Toshiki Nakasone, and Kazuo Sakiyama, “Toward Applications of SRAM Retention Time as Battery-Less Timer for RFID Tags,” Poster Session, IWSEC2013 (Nov., 2013).
26. 町田卓謙, 中曽根俊貴, 崎山一男, “Arbiter PUF の FPGA 実装における評価手法と脆弱性,” ISEC2013-18, pp.53-58, (Jul., 2013).
27. 松原有沙, 蒯云峰, 李陽, 中曽根俊貴, 太田和夫, 崎山一男, “AES 暗号回路における信号遷移回数を用いたサイドチャネル情報に関する考察,” ISEC2013-45, pp.331-338, (Jul., 2013).
28. Yang Li, Hikaru Sakamoto, Iwamasa Nishikado, Takafumi Saito, Kazuo Ohta, Kazuo Sakiyama, “Toward Flexible Privacy Protection for RFID Tags Using Privacy-Mode Switching,” IEICE2013 年総合大会, (Mar., 2013).

29. 中曽根俊貴, 李陽, 崎山一男, “システム上にある SRAM の電荷保持時間と PUF 特性を利用した DoS 攻撃対策,” IEICE2013 年総合大会, (Mar., 2013).
30. 佐々木悠, 李陽, 阪本光, 崎山一男, “クーポンコレクタ問題を利用したノイズに強い飽和フォールト攻撃,” IEICE2013 年総合大会, (Mar., 2013).
31. 松原有沙, 李 陽, 太田和夫, 崎山一男, “故障混入時の AES 暗号ハードウェアの脆弱性について,” IEICE2013 年総合大会（学生ポスターセッション）, (Mar., 2013).
32. 遠藤翔, 李陽, 本間尚文, 崎山一男, 藤本大介, 永田真, 太田和夫, 青木孝文, “故障感度隠蔽のための効率的な対策とその評価,” 2013 年 暗号と情報セキュリティシンポジウム (SCIS2013), 1E1-5, 8 pages, (Jan., 2013)
33. 駒野雄一, 太田和夫, 岩本貢, 崎山一男, “PUF 出力の一部を用いるパターン照合鍵生成システム,” 2013 年 暗号と情報セキュリティシンポジウム (SCIS2013), 1D2-3, 8 pages, (Jan., 2013)
34. 三上修吾, 渡辺大, 本間尚文, 崎山一男, “RFID 認証プロトコル向け軽量暗号アルゴリズムの実装評価,” 2013 年 暗号と情報セキュリティシンポジウム (SCIS2013), 2E2-1, 8 pages, (Jan., 2013)
35. 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,” 2013 年 暗号と情報セキュリティシンポジウム (SCIS2013), 2E2-2, 8 pages, (Jan., 2013)
36. 岩井佑樹, 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,” 2013 年 暗号と情報セキュリティシンポジウム (SCIS2013), 2E3-3, 8 pages, (Jan., 2013)
37. 松原有沙, 李陽, 太田和夫, 崎山一男, “Mechanism Analysis for Non-Uniform Mapping of Faulty S-box – Case Study of AES-COMP – ,” 2013 年 暗号と情報セキュリティシンポジウム (SCIS2013), 3E3-1, 6 pages, (Jan., 2013)
38. 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,” 2013 年 暗号と情報セキュリティシンポジウム (SCIS2013), 3E3-2, 8 pages, (Jan., 2013)
39. Toshiki Nakasone, Daisuke Nakatsu, Yang Li, Kazuo Ohta, and Kazuo Sakiyama, “Locality Randomization for EMA-Resistant AES Hardware,” In Proc. Triangle Symposium on Advanced ICT 2012 (TriSAI’12), 4 pages, (Sep., 2012).
40. Yang Li, Daisuke Nakatsu, Kazuo Ohta, and Kazuo Sakiyama, “Key Recovery with Less Power Traces Using DPA Contest Data,” Poster Session, CHES2012 (Sep., 2012).
41. 李陽, 太田和夫, 崎山一男, “Sensitive-Data Dependency of Faulty Behavior and Its Application,” 2012 年 暗号と情報セキュリティシンポジウム (SCIS’12), 3C1-3E, 7 pages, (Feb., 2012).
42. 中曽根俊貴, 中津大介, 李陽, 太田和夫, 崎山一男, “クロック間衝突を利用した電磁波解析,” 2012 年 暗号と情報セキュリティシンポジウム (SCIS’12), 3C1-1, 8 pages, (Feb., 2012).
43. 小池彩歌, 李陽, 中津大介, 太田和夫, 崎山一男, “IR ドロップを利用した故障感度解析と高温環境下における影響,” 2012 年 暗号と情報セキュリティシンポジウム (SCIS’12), 2C3-3, 7 pages, (Jan., 2012).
44. 中津大介, 李陽, 太田和夫, 崎山一男, “テンプレートを利用した時系列電力解析,” 2012 年 暗号と情報セキュリティシンポジウム (SCIS’12), 2C2-5, 6 pages, (Jan., 2012).
45. 高橋順子, 阪本光, 福永利徳, 冨士仁, 崎山一男, “Access-Driven Cache Attack の自動的な攻撃評価手法の提案,” 2012 年 暗号と情報セキュリティシンポジウム (SCIS’12), 2C2-2, 7 pages, (Jan., 2012).

46. 三上修吾, 吉田博隆, 渡辺大, 崎山一男, “Threshold Implementation を利用したストリーム暗号 Enocoro-128 v2 の相関電力解析対策,” 2012 年 暗号と情報セキュリティシンポジウム (SCIS’12), 2C2-1, 6 pages, (Jan., 2012).

47. 小松原航, 王磊, 佐々木悠, 崎山一男, 太田和夫, “54 ステップの SHA-0 への原像攻撃,” 2012 年 暗号と情報セキュリティシンポジウム (SCIS’12), 1C1-1, 8 pages, (Jan., 2012).

48. 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,” 2012 年 暗号と情報セキュリティシンポジウム (SCIS’12), 1D2-2, 8 pages, (Jan., 2012).

49. 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, “[招待講演] Uniqueness Enhancement of PUF Responses Based on the Locations of Random Outputting RS Latches,” ISEC2011-66, p.29, (Dec., 2011).

50. 李陽, 太田和夫, 崎山一男, “［招待講演］マスク対策 AES に対する誤り暗号文を用いた故障感度解析～CHES2011 での発表のレビュー～,” ISEC2011-66, p.25, (Dec., 2011).

51. 伊豆哲也, 猪俣敦夫, 桶屋勝幸, 川端健, 駒野雄一, 崎山一男, 酒見由美, 佐藤証, 須賀祐治, 高木剛, 高橋順子, 角尾幸保, 盛合志帆, 堀洋平, 本間尚文, 渡辺大, “国際会議 CHES2011 報告,” ISEC2011-66, p.21-24, (Dec., 2011).

52. 阪本光, 李陽, 太田和夫, 崎山一男, “クロック間衝突を用いた楕円曲線暗号実装に対する故障感度解析,” ISEC2011-49, pp.101-108, (Nov., 2011).

53. Toshiki Nakasone, Daisuke Nakatsu, Yang Li, Kazuo Ohta, and Kazuo Sakiyama, “First Experimental Results of Correlation-Enhanced EMA Collision Attack,” Poster Session, CHES’11 (Sep., 2011).

54. Takuma Koyama, Yu Sasaki, Kazuo Sakiyama, and Kazuo Ohta, “Rebound Attack on 3D Block Cipher,” In Proc. Triangle Symposium on Advanced ICT 2011 (TriSAI’11), pp.220-224, (Aug., 2011).

55. Yasuhide Sakai, Yu Sasaki, Lei Wang, Kazuo Ohta, and Kazuo Sakiyama, “Preimage Attacks on 5-Pass HAVAL Reduced to 158-Steps and One-Block 3-Pass HAVAL,” Industrial Track Session, ACNS’11, 14 pages, (Jun., 2011).

56. Qi Li, Shigeto Gomisawa, Mitsugu Iwamoto, Kazuo Ohta, and Kazuo Sakiyama, “New Differential Fault Analysis on Trivium Based on Setup-Time Violations,” ISEC2010-122, pp.333-339, (Mar., 2011).

57. 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,” 2011 年 暗号と情報セキュリティシンポジウム (SCIS’11), 2D1-1, 8 pages, (Jan., 2011).

58. 岩井祐樹, 太田和夫, 崎山一男,“故障感度解析を利用した PUF の実現について,” 2011 年 暗号と情報セキュリティシンポジウム (SCIS’11), 2D1-3, 8 pages, (Jan., 2011).

59. 高柳真如, 佐々木悠, 李陽, 太田和夫, 崎山一男, “7 及び 8 ラウンド既知鍵 AES 識別機の実装,” 2011 年 暗号と情報セキュリティシンポジウム (SCIS’11), 2B2-4, 7 pages, (Jan., 2011).

60. 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,” 2011 年 暗号と情報セキュリティシンポジウム (SCIS’11), 2D3-3, 8 pages, (Jan., 2011).

61. 李陽, 太田和夫, 崎山一男, “Self-Template Fault Sensitivity Analysis,” 2011 年 暗号と情報セキュリティシンポジウム (SCIS’11), 3D3-1, 8 pages, (Jan., 2011).

62. 阪本光, 李陽, 太田和夫, 崎山一男, “楕円曲線暗号実装に対する Fault Sensitivity Analysis,” 2011 年 暗号と情報セキュリティシンポジウム (SCIS’11), 3D3-2, 8 pages, (Jan., 2011).

63. 五味澤重友, 王磊, 太田和夫, 山口和彦, 崎山一男, “HMAC-MD5 へのフォールト解析攻撃,” 2011 年 暗号と情報セキュリティシンポジウム (SCIS’11), 3D3-3, 8 pages, (Jan., 2011).

64. 松田和也, 川合豊, 崎山一男, 太田 和夫, “再暗号化鍵匿名性を満たす ID ベースプロキシ再暗号化方式,” 2011 年 暗号と情報セキュリティシンポジウム (SCIS’11), 3F3-6, 8 pages, (Jan., 2011).

65. 中津大介, 太田和夫, 崎山一男, “AES-128 に対する複数ラウンド CPA,” 2011 年 暗号と情報セキュリティシンポジウム (SCIS’11), 3D4-1, 8 pages, (Jan., 2011).

66. 酒井靖英, 佐々木悠, 王磊, 崎山一男, 太田和夫, “158step の 5-pass HAVAL と 1-Block 3-pass HAVAL への原像攻撃,” 2011 年 暗号と情報セキュリティシンポジウム (SCIS’11), 4B1-2, 8 pages, (Jan., 2011).

67. 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,” 2011 年 暗号と情報セキュリティシンポジウム (SCIS’11), 4B1-4, 8 pages, (Jan., 2011).

68. Naoyuki Takayanagi, Yang Li, Kazuo Sakiyama, and Kazuo Ohta, “Effective Verification for Known-Key Distinguisher by Using Extended Differential Path,” In Proc. Triangle Symposium on Advanced ICT 2010 (TriSAI’10), pp.284-287, (Oct., 2010).

69. Qi Li, Kazuo Sakiyama, Lei Wang, and Kazuo Ohta, “Another Differential Fault Analysis on Trivium,” In Proc. Triangle Symposium on Advanced ICT 2010 (TriSAI’10), pp.247-252, (Oct., 2010).

70. 岩本貢, 李陽, 崎山一男, 太田和夫, “回転操作が可能な視覚復号型秘密分散法の一般的構成法,” ISEC2010-49, pp.67-74, (Sep., 2010).

71. 花谷嘉一, 大久保美也子, 松尾真一郎, 太田和夫, 崎山一男, “CryptoVerif を用いた RFID 向け相互認証プロトコルの安全性証明の検討,” 日本応用数理学会 2010 年度年会 FAIS セッション, (Sep., 2010).

72. Shin’ichiro Matsuo, Miroslav Knezevic, Patrick Schaumont, Ingrid Verbauwhede, Akashi Satoh, Kazuo Sakiyama and Kazuo Ohta, “How Can We Conduct Fair and Consistent Hardware Evaluation for SHA-3 Candidate?” The Second SHA-3 Candidate Conference, (Aug., 2010).

73. Yu Sasaki, Yang Li, Lei Wang, Kazuo Sakiyama, and Kazuo Ohta, “New Non-Ideal Properties of AES-Based Permutations: Applications to ECHO and Grøstl,” The Second SHA-3 Candidate Conference, (Aug., 2010).

74. 小林和幸, 池上淳, 松尾真一郎, 崎山一男, 太田和夫, “SASEBO-GII を用いた SHA-3 候補のハードウェア性能評価,” 第 15 回共同研究成果報告会, pp.29-30, (Jun., 2010).

75. 太田和夫, 王磊, 崎山一男, “強識別不可能性理論と SHA-3 プロジェクト ～ハッシュ関数設計のための理論研究と実装研究の現状～,” ISEC2009-104, pp.159-166, (Mar., 2010).

76. 塙知剛, 川合豊, 崎山一男, 太田和夫, “HB-MAC 認証プロトコルに対する受動的攻撃,” 2010 年 暗号と情報セキュリティシンポジウム (SCIS’10), 1E2-1, 6 pages, (Jan., 2010).

77. 五味澤重友, 泉雅巳, 李陽, 高橋順子, 福永利徳, 佐々木 悠, 崎山一男, 太田 和夫, “AES 暗号実装へのフォールト解析攻撃における適用範囲の拡大と解析効率の向上,” 2010 年 暗号と情報セキュリティシンポジウム (SCIS’10), 2B1-1, 6 pages, (Jan., 2010).

78. Yang Li, Shigeto Gomisawa, Kazuo Sakiyama, and Kazuo Ohta, “An Information Theoretic Perspective on the Differential Fault Analysis against AES,” 2010 Symposium on Cryptography and Information Security (SCIS’10), 2B1-2, 6 pages, (Jan., 2010).

79. 長井大地, 塙知剛, 太田和夫, 崎山一男, 岩本貢, “PUF-HB プロトコルに対する中間者攻撃,” 2010 年 暗号と情報セキュリティシンポジウム (SCIS’10), 2C2-5, 6 pages, (Jan., 2010).

80. 中津大介, 李陽, 崎山一男, 太田和夫, “DPA 耐性のあるソフトウェア実装のための安全な CPU,” 2010 年 暗号と情報セキュリティシンポジウム (SCIS’10), 2B3-1, 6 pages, (Jan., 2010).

81. 泉雅巳, 崎山一男, 太田和夫, 佐藤証, “公開鍵暗号の SPA/DPA 耐性向上に向けた対策アルゴリズムの再考,” 2010 年 暗号と情報セキュリティシンポジウム (SCIS’10), 2B3-2, 6 pages, (Jan., 2010).

82. 松田和也, 坂井祐介, 太田和夫, 崎山一男, “Katz らの Leakage Resilient t-time 署名の解析,” 2010 年 暗号と情報セキュリティシンポジウム (SCIS’10), 2B3-4, 6 pages, (Jan., 2010).

83. 池上淳, 小林和幸, 崎山一男, 太田和夫, “SASEBO-GII を用いた SHA-3 候補のハードウェア性能評価,” 2010 年 暗号と情報セキュリティシンポジウム (SCIS’10), 4F1-2, 6 pages, (Jan., 2010).

84. Bagus Santoso, Kazuo Ohta, Kazuo Sakiyama, and Goichiro Hanaoka, “Performance Comparison of Lightweight Public-Key Identification Schemes,” WISP Summit - First workshop on Wirelessly Powered Sensor Networks and Computational RFID, (Nov., 2009).

85. Yang Li, Mitsugu Iwamoto, Kazuo Ohta, and Kazuo Sakiyama, “Visual Secret Sharing Schemes Allowing Arbitrary Rotation Angles of Shares,” In Proc. Triangle Symposium on Advanced ICT 2009 (TriSAI’09), Tokyo, Japan, pp.33-38, (Oct., 2009).

86. Tomotaka Hanawa, Kazuo Sakiyama, and Kazuo Ohta, “Cryptoanalysis of Duc-Kim Key Exchange Protocol Proposed at TriSAI’08,” In Proc. Triangle Symposium on Advanced ICT 2009 (TriSAI’09), Tokyo, Japan, pp.39-42, (Oct., 2009).

87. Daisuke Nakatsu, Yang Li, Kazuo Sakiyama, and Kazuo Ohta, “Comparison of Masked S-boxes in Hardware Implementation,” In Proc. Triangle Symposium on Advanced ICT 2009 (TriSAI’09), Tokyo, Japan, pp.176-181, (Oct., 2009).

88. Shigeto Gomisawa, Masami Izumi, Kazuo Sakiyama, and Kazuo Ohta, “An Extension of Differential Fault Analysis Attack of AES,” In Proc. Triangle Symposium on Advanced ICT 2009 (TriSAI’09), Tokyo, Japan, pp.185-188, (Oct., 2009).

89. Bagus Santoso, Kazuo Ohta, Kazuo Sakiyama, and Goichiro Hanaoka, “Improving Efficiency of an ’On the Fly’ Identification Scheme by Perfecting Zero-Knowledgeness,” ISEC2009-30, pp.161-168, (Jul., 2009).

90. Yang Li, Mitsugu Iwamoto, Kazuo Ohta, and Kazuo Sakiyama, “A Novel Construction Method for Visual Secret Sharing Schemes Allowing Rotation of Shares,” ISEC2009-5, pp.29-36, (May, 2009).

91. Yang Li, Mengyu Zhu, Wang Lei, Kazuo Ohta, and Kazuo Sakiyama, “Visual Secret Sharing Schemes for Multiple Secret Images Allowing the 90-degree Rotation of Shares,” 2009 Symposium on Cryptography and Information Security (SCIS’09), 1F1-3, 8 pages, (Jan., 2009).

92. Lei Wang, Yu Sasaki, Kazuo Ohta, and Kazuo Sakiyama, “MD5 チャレンジ・レスポンスプロトコルへの速い攻撃,” 2009 Symposium on Cryptography and Information Security (SCIS’09), 2A2-1, 8 pages, (Jan., 2009).

93. 八木達哉, 崎山一男, 太田和夫, “高周波クロックによる RSL 技術を用いた AES へのフォールト攻撃実験,” 2009 年 暗号と情報セキュリティシンポジウム (SCIS’09), 2A3-2, 8 pages, (Jan., 2009).

94. 泉 雅巳, 崎山一男, 太田和夫, “フォールト混入時における RSL 技術による暗号回路モデルを用いた安全性解析,” 2009 年 暗号と情報セキュリティシンポジウム (SCIS’09), 2A3-3, (Jan., 2009).

95. Bagus Santoso, Kazuo Ohta, and Kazuo Sakiyama, “Yet Another New ”On the Fly” Identification Scheme: Reducing Memory Cost by Improving Zero-Knowledgeness,” 3A2-4, 2009 Symposium on Cryptography and Information Security (SCIS’09), 8 pages, (Jan., 2009).

96. Masami Izumi, Kazuo Sakiyama, Kazuo Ohta, "Does The Montgomery Powering Ladder Method Really Offer SPA Resistance?" Triangle Symposium on Advanced ICT 2008 (TriSAI'08), 6 pages, (Oct., 2008).

97. Yong Ki Lee, Kazuo Sakiyama, Lejla Batina, Ingrid Verbauwhede, "A Compact ECC Processor for Pervasive Computing," In the Workshop Record of the ECRYPT Workshop, Secure Component and System Identification (SECSI'08), 14 pages, (Mar., 2008).

98. Lejla Batina and Kazuo Sakiyama, "Compact Implementations for RFID and Sensor Nodes," Special Interest Workshops - Secure Embedded Implementations, Design, Automation and Test in Europe (DATE'07), (Apr., 2007).（招待講演）

99. Junfeng Fan, Kazuo Sakiyama, and Ingrid Verbauwhede, "Elliptic Curve Cryptography on Embedded Multicore Systems," In the Workshop Record of the Workshop on Embedded Systems Security (WESS'07), 6 pages, (Oct., 2007).

100. Junfeng Fan, Kazuo Sakiyama, and Ingrid Verbauwhede, "Montgomery Modular Multiplication Algorithm for Multi-core Systems," In the Workshop Record of the ECRYPT Workshop, Software Performance Enhancement for Encryption and Decryption (SPEED'07), 12 pages, (Jun., 2007).

101. Caroline Vanderheyden, Junfeng Fan, Kazuo Sakiyama, and Ingrid Verbauwhede, "Exploring Tradeoffs between Area, Performance and Security in HW/SW Co-design of ECC," In the Workshop Record of the Western European Workshop on Research in Cryptology (WeWoRC'07), 2 pages, (Jul., 2007).

102. Kazuo Sakiyama, Lejla Batina, Nele Mentens, Bart Preneel, and Ingrid Verbauwhede, "Small Footprint ALU for Public-key Processors for Pervasive Security," In the Workshop Record of the ECRYPT Workshop on RFID Security 2006, 12 pages, (Jul., 2006).

103. Lejla Batina, Sandeep Kumar, Joseph Lano, Kerstin Lemke, Nele Mentens, Christoph Paar, Bart Preneel, Kazuo Sakiyama, and Ingrid Verbauwhede, "Testing Framework for eSTREAM Profile II Candidates," In the Workshop Record of the ECRYPT Workshop, SASC - The State of the Art of Stream Ciphers, 9 pages, (Feb., 2006).

104. Kazuo Sakiyama, Lejla Batina, Patrick Schaumont, and Ingrid Verbauwhede, "HW/SW Co-design for TA/SPA-resistant Public-Key Cryptosystems," In the Workshop Record of the ECRYPT Workshop on CRyptographic Advances in Secure Hardware (CRASH'05), 8 pages, (Sep., 2005).

105. Young-Jae Cho, Takashi Hirakawa, Kazuo Sakiyama, Hiroaki Okamoto and Yoshihiro Hamakawa, "EL/PL Hybrid Device Enhanced by UV Emission from ZnF_2:Gd Thin Film Electroluminescence," 8th Seoul International Symposium on the Physics of Semiconductors and Applications (ISPSA'96), Seoul, Korea, Oct. 21-22, 1996.

106. 平川孝, 崎山一男, 趙永載, 濱川圭弘, "ZnF_2:Gd を用いた EL-PL 複合素子 (II) ," 第 57 回応用物理学会学術講演会講演予稿集, Vol.43, No.3, p.1210, (Sep., 1996).

107. 崎山一男, 趙永載, 濱川圭弘, "ZnF_2:Gd を用いた EL-PL 複合素子," 第 56 回応用物理学会学術講演会講演予稿集, Vol.56, No.3, p.1085, (Aug., 1995).

VII その他（*Patents, Research Funds*）

1. 日本学術振興会 (JSPS) 科学研究費補助金 基盤研究 (A)：レーザーフォールト攻撃による情報漏洩を防ぐ耐タンパー技術の総合的研究, 研究代表者, H27-H30.

2. 日本学術振興会 (JSPS) 科学研究費補助金 基盤研究 (A)：暗号ＶＬＳＩの電磁波セキュリティを確保するサイドチャネル攻撃センサの構成法と実証, 研究代表者：永田真, H26-H28（研究分担者として）.

3. 情報通信研究機構 (NICT) 高度通信・放送研究開発委託研究「軽量暗号プロトコルの省リソースデバイスに対する実装効率向上の研究開発」（電通大研究代表者として）, H24-H26.
4. 日本学術振興会 (JSPS) 科学研究費補助金 基盤研究 (C)：実装性を考慮した省リソースデバイス向け暗号プロトコル設計理論の研究, 研究代表者：松尾真一, H24-H26（研究分担者として）.
5. 科学技術振興機構 (JST) 戦略的国際科学技術協力推進事業（共同研究型）「日本—フランス共同研究」：組込みシステムにおける暗号プロセッサの物理攻撃に対する安全性評価, 電通大チーム研究代表者, H22-H25.
6. 日本学術振興会 (JSPS) 科学研究費補助金 基盤研究 (C)：サイドチャネル攻撃の限界追及と情報漏洩メカニズムの解明, 研究代表者, H22-H24.
7. 日本学術振興会 (JSPS) 科学研究費補助金 基盤研究 (C)：暗号プリミティブの安全性検証の自動化への展開, 研究分担者, H19-H21.
8. 崎山一男, 李陽, “認証システム及び認証方法,” PCT/JP2015/52576.
9. 山本大, 武仲正彦, 伊藤孝一, 落合隆夫, 岩本貢, 太田和夫, 崎山一男, “個体別情報生成装置及び個体別情報生成方法,” 特願 2011-278999, 特開 2013-131867.
10. 山本大, 落合隆夫, 武仲正彦, 伊藤孝一, 崎山一男, 岩本貢, 太田和夫, “温度センサ、暗号化装置、暗号化方法、及び個体別情報生成装置,” 特願 2011-279000, 特開 2013-130434.
11. 山本大, 落合隆夫, 武仲正彦, 伊藤孝一, 崎山一男, 岩本貢, 太田和夫, “温度センサ、暗号化装置、暗号化方法、及び個体別情報生成装置,” 特願 2011-279001, 特開 2013-131868.
12. 山本大, 武仲正彦, 伊藤孝一, 落合隆夫, 崎山一男, 岩本貢, 太田和夫, “個体別情報生成装置、暗号化装置、認証装置、及び個体別情報生成方法,” 特願 2011-279002, 特開 2013-131869.
13. 駒野雄一, 太田和夫, 崎山一男, “暗号化鍵生成装置およびプログラム,” 特願 2011-275637, 特開 2013-126221.
14. 佐々木悠, 崎山一男, 太田和夫, “回路故障検出装置、回路故障検出方法,” 特願 2010-275596, 特開 2012-122931.
15. 中谷浩茂, 梶山智史, 鍋嶋秀生, 太田和夫, 崎山一男, “電気錠システム,” 特願 2010-168367, 特開 2012-026225.
16. サントソバグス, 崎山一男, 太田和夫, “本人確認システム,” 特願 2008-289266, 特開 2010-118796.
17. Kazuyuki Takizawa, Ikuya Arai, and Kazuo Sakiyama, “Broadcast station synchronization method and mobile terminal,” US 7620410, CN 200510116964, KR 1020050102377.
18. 滝澤和之, 荒井郁也, 崎山一男, “放送局同期方式、及び携帯端末機,” 特願 2004-315589, 特開 2006-129142, 特許第 4411184 号.
19. Ingrid Verbauwhede, Patrick Schaumont, David Hwang, Bo-Cheng Lai, Shenglin Yang, Kazuo Sakiyama, Yi Fan, and Alireza Hodjat, “System for Biometric Signal Processing with Hardware and Software Acceleration,” US 20070038867.
20. 崎山一男, 原博隆, 杉田憲彦, 長谷昌, 堀仁一, “バッファ制御装置及び半導体集積回路,” 特願平 11-121208, 特開 2000-310985.