国際科学技術協力基盤整備事業
日本－台湾研究交流
終了報告書　概要

１．研究課題名：「IoT デバイスのための新しい軽量暗号システムに関する研究と台湾の eHealth 環境への応用」

２．研究期間：2016 年 1 月～2019 年 3 月

３．主な参加研究者名：

日本側チーム

	氏名	役職	所属	研究分担
研究代表者	宮地 充子	教授	大阪大学・大学院工学研究科	WP1, WP2, WP3
主たる共同研究者	田中 清史	准教授	北陸先端科学技術大学院大学・先端科学技術研究科	WP1
主たる共同研究者	Chunhua SU	准教授	会津大学・情報セキュリティ学講座	WP1, WP2, WP3
主たる共同研究者	双紙 正和	准教授	広島市立大学・情報科学部	WP3
主たる共同研究者	Chen-Mou Cheng	特任准教授	大阪大学・大学院工学研究科	WP1
研究期間中の全参加研究者数　21名				

相手側チーム

	氏名	役職	所属	研究分担
研究代表者	Chien-Lung HSU	Professor	Department of Information Management, Chang-Gung University	WP4
主たる共同研究者	Kuo Hui YEH	Association Professor	Department of Information Management, National Dong Hwa University	WP4
主たる共同研究者	Kuo-Yu TSAI	Assistant Professor	Department of Applied Mathematics, Chinese Culture University	WP4
研究期間中の全参加研究者数　10名				

４．研究交流の概要

日本側では、台湾のeHealth 環境へ応用可能なIoTデバイスのための新しい軽量暗号システムに関する研究を実施した。本研究は、軽量な公開鍵暗号(WP1)、軽量な共通鍵暗号(WP2)、それらを実装したIoT機器の安全性を実現するホワイトボックス暗号(WP3)といった3つの柱で構成されている。台湾側においては、これら日本側の研究成果を応用し、安全なIoT　技術に基づいたeHealthシステムの実装検証(WP4)を行った。本研究では、WP1では軽量な楕円曲線暗号を実現し、WP2 軽量な共通鍵暗

号と、それを用いた認証方式を開発し、WP3においては、公開鍵暗号・共通鍵暗号のソフト実装の安全性強化を実現するホワイトボックスを実現した。

５．研究交流の成果

５－１　共同研究の研究・開発成果

台湾の eHealth 環境へ応用可能な IoT デバイスのための新しい軽量暗号システムに関する研究において、日本側では以下の 3 項目を実現した。

WP1 では、任意の鍵に対して安全かつ軽量、高速に実現できる楕円曲線暗号を実現した。

WP2 では、既存の軽量化共通鍵暗号の安全性を検証し、IoT 機器向けの軽量化暗号の実装検証と軽量化認証方式の開発を行った。

WP3 では、ホワイトボックス暗号実装を新たに提案した。また、圧縮困難性を持つ一般的な暗号実装方式を提案した。

台湾側では、日本側の研究成果を適用し、安全な IoT　技術に基づいた eHealth システムの実装検証（WP4）を行った。

５－２　国際連携による相乗効果

Chang-Gung University、 National Dong Hwa University とワークショップなどの交流を行うことで、セキュリティの幅広い概念について理解を深めることができた。特に、台湾の研究から、eHealth 環境等 IoT のシステムについて、日本の単独では得られない知見を得ることができた。また、台湾ウェアラブル機器という実機を用いた研究開発ができ、医療向けの安全認証システムプロトタイプや IoT 機器の管理システムの実装実験が可能となった。

５－３　共同研究成果から期待される波及効果および進展

台湾の eHealth 環境へ応用可能な IoT デバイスのための新しい軽量暗号システムに関する研究において、軽量な公開鍵暗号(WP1)は、軽量化を実現した楕円曲線暗号のアルゴリズムを提案し、ソフトウェアを構築した。また、軽量な共通鍵暗号(WP2)ではプロトタイプを実現した。これらは、台湾の eHealth 環境へ応用可能なスペックを実現しており、医療環境向けの IoT デバイスのための安全システムへの波及効果が期待できる。

５－４　研究交流の有効性・継続性（研究交流を通じた人材育成、協働関係の継続・発展性）

台湾側の学生の受け入れや逆に日本の学生を台湾の大学に派遣するなどの学生の日本と台湾の間の交流を定期的に行った。これにより、教員のみならず、学生たちも協働関係の絆を構築することが可能になった。両学生が本研究終了後も、日本と台湾の協働関係を継続し、今後、ますます社会の発展に寄与できると思われる。

Infrastructure Development for Promoting International S&T Cooperation
Japan－Taiwan Joint Research Exchange Program
Executive Summary of Final Report

１. Project Title:「New Lightweight Cryptosystems for IoT devices and application to eHealth Environments in Taiwan」

２. Project Period：1, 2016 ～ 3, 2019

３. Main Participants：

Japan-side

	Name	Title	Affiliation	Role
PI	Atsuko MIYAJI	Professor	Graduate School of Engineering, Osaka University	WP1, WP2, WP3
Co-PI	Kiyofumi Tanaka	Associate Professor	School of Information Science, JAIST	WP1
Co-PI	Chunhua Su	Associate Professor	Information Security Laboratory, The University of Aizu	WP1, WP2, WP3
Co-PI	Masakazu Soshi	Associate Professor	Graduate School of Information Sciences Dept. of Systems Engineering, Hiroshima City University	WP3
Co-PI	Chen-Mou Cheng		Graduate School of Engineering, Osaka University	WP1
Total number of participating researchers in the project: 21				

Partner-side

	Name	Title	Affiliation	Role
PI	Chien-Lung HSU	Professor	Department of Information Management, Chang-Gung University	WP4
Co-PI	Kuo Hui YEH	Association Professor	Department of Information Management, National Dong Hwa University	WP4
Co-PI	Kuo-Yu TSAI	Assistant Professor	Department of Applied Mathematics, Chinese Culture University	WP4
Total number of participating researchers in the project: 10				

４．Scope of the joint project

On Japan side, we carried out the research on new lightweight cryptographic systems for IoT devices that is applicable to Taiwan eHealth environment. The research consists of three pillars, such as lightweight public key cryptography (WP1), lightweight symmetric key cryptography (WP2), white box encryption to realize the safety of IoT devices (WP3). On Taiwan side, our collaborators carried out the implementation and verification of eHealth system (WP4), based on the secure IoT technologies that were applied from research outputs in this project from Japan side. In research exchange, WP1 realized lightweight elliptic curve cryptography, WP2 developed lightweight common key cryptography and authentication method using it, and WP3 secured the software implementation of public key cryptography / common key cryptography. We realized a white box to realize the reinforcement.

５．Outcomes of the joint project

５－１ Intellectual Merit

In the research on a new lightweight cryptographic system for IoT devices applicable to Taiwan eHealth environment, the Japan side realized the following three items.
In WP1, we have realized an elliptic curve cryptosystem that can be realized safely, lightweight and fast for any key.
In WP2, we verified the security of the existing lightweight symmetric key encryption, and implemented the verification of the lightweight encryption for IoT devices and developed the lightweight authentication method.
WP3 proposed a new implementation of white-box cryptography. We also proposed a general cryptographic implementation method with compression difficulty.
On Taiwan side, the research outputs of the Japan side were applied as the safety IoT technology, and the implementation and verification activities of the eHealth system (WP4) based on the IoT technology was performed.

５－２ Synergy from the Collaboration

Through exchanges with Chang-Gung University and National Dong Hwa University, I was able to deepen my understanding of a wide range of security concepts. In particular, from the research in Taiwan, we were able to obtain insights that cannot be obtained in Japan alone about IoT systems such as the eHealth environment. In addition, research and development using real equipment such as Taiwan wearables can be performed, and implementation experiments of safety authentication system prototype for medical treatment and management system of IoT equipment become possible.

５－３ Potential Impacts on Society

In research on a new lightweight cryptographic system for IoT devices applicable to Taiwan's eHealth environment, lightweight public key cryptography (WP1) proposed an algorithm of elliptic curve cryptography that is realized in lightweight manner and built software. We also realized a prototype for lightweight symmetric key cryptography (WP2). These have achieved specifications that can be applied to the eHealth environment in Taiwan, and a ripple effect on the safety system for IoT devices for medical environments can be expected.

５－４ Effectiveness and Continuity of Exchange (Human Resource Cultivation, Development and Sustainability of the Cooperation, etc.)

The exchange of students between Japan and Taiwan was conducted regularly, such as accepting students from Taiwan and sending Japanese students to universities in Taiwan. As a result, not only teachers but also students can construct bonds of collaborative relationships. Even after the completion of the two students, Japan-Taiwan collaboration will continue and it will be able to contribute to the development of society in the future.

共同研究における主要な研究成果リスト

１．論文発表等

＊原著論文（相手側研究チームとの共著論文）

1. Lu Zhou, Chunhua Su, Kuo-Hui Yeh and Wayne Chiu. “You Think, Therefore You Are: Transparent Authentication System with Brainwave-oriented Bio-features for IoT Networks”. IEEE Transactions on Emerging Topics in Computing(Early Access), 1-1(2017), doi: 10.1109/TETC.2017.2759306.

2. Kuo-Hui Yeh, Chunhua Su, Wayne Chiu, Lu Zhou*, “I Walk, Therefore I Am: Continuous User Authentication with Plantar Biometrics,” IEEE Communications Magazine, Vol. 56, Issue 2, February 2018, pp. 150-157. (Impact Factor of 2017 = 9.270), 10.1109/MCOM.2018.1700339.

3. Shi-Cho Cha, Ming-Shiung Chuang, Kuo-Hui Yeh, Zi-Jia Huang, Chunhua Su*, “A User-Friendly Privacy Framework for Users to Achieve Consents with Nearby BLE Devices,” IEEE Access, Vol. 6, Issue 1, March 2018, pp. 20779-20787. (Impact Factor of 2017 = 3.557), 10.1109/ACCESS.2018.2820716.

4. Lu Zhou, Kuo-Hui Yeh, Hancke Gerhard, Zhe Liu*, Chunhua Su, “Security and Privacy for the Industrial Internet of Things: An Overview of Approaches to Safeguarding Endpoints,” IEEE Signal Processing Magazine, Volume: 35, Issue: 5, September 2018, Page(s): 76-87. (Impact Factor of 2017 = 7.451), 10.1109/MSP.2018.2846297.

5. Wayne Chiu, Chunhua Su, Chuan-Yen Fan, Chien-Ming Chen, Kuo-Hui Yeh*, “Authentication with What You See and Remember in the Internet of Things,” Symmetry, Vol. 10, Issue 11, DOI: 10.3390/sym10110537, October 2018. (*Corresponding Author, Impact Factor of 2017 = 1.256), https://doi.org/10.3390/sym10110537.

6. Kuo-Hui Yeh, Chunhua Su, Jia-Li Hou, Wayne Chiu, Chien-Ming Chen*, “A Robust Mobile Payment Scheme with Smart Contract-based Transaction Repository,” IEEE Access, Vol. 6, Issue 1, December 2018, pp. 59394 - 59404. (Impact Factor of 2017 = 3.557), 10.1109/ACCESS.2018.2874021.

7. Lu Zhou, Xiong Li, Kuo-Hui Yeh, Chunhua Su, Wayne Chiu. “Lightweight IoT-based authentication scheme in cloud computing circumstance”. Future Generation Computer System. Vol.91, pp.244-251, 2019. https://doi.org/10.1016/j.future.2018.08.038

8. Shi-Cho Cha, Jyun-Fu Chen, Chunhua Su, Kuo-Hui Yeh. “A Blockchain Connected Gateway for BLE-Based Devices in the Internet of Things.” IEEE Access Vol.6, pp.24639-24649, 2018. 10.1109/ACCESS.2018.2799942

9. Lu Zhou, Chunhua Su, Kuo-Hui Yeh. “A Lightweight Cryptographic Protocol with Certificateless Signature for the Internet of Things”, ACM Transactions on Embedded Computing Systems, Vol. 18 Issue 3, In Press, 2019

＊原著論文（相手側研究チームを含まない日本側研究チームの論文）
学術誌論文＊査読有り
[Atsuko Miyaji]

10. Atsuko Miyaji and Kazumasa Omote, “Self-healing wireless sensor networks", Concurrency and Computation: Practice and Experience, 2015, Article first published online: April 2015.

10.1002/cpe.3434.

11. Ryoma Ito and Atsuko Miyaji, “How TKIP induces biases of internal states of generic RC4", Information Security and Privacy, 9144(2015), 329-342, Springer-Verlag. 10.1007/978-3-319-19962-7_19

12. Ryoma Ito and Atsuko Miyaji, “New Linear Correlations Related to State Information of RC4 PRGA Using IV in WPA", Fast Software Encryption, 9054(2015), 557-576, Springer-Verlag. 10.1007/978-3-662-48116-5_27

13. Atsuko Miyaji and Xiaonan Shi and Satoru Tanaka, “Extended Explicit Relations Between Trace", Definition Field, and Embedding Degree, Algebraic Informatics, 9270(2015), 165-175, Springer-Verlag. 10.1007/978-3-319-23021-4_15

14. Jiageng Chen, Shoichi Hirose, Hidenori Kuwakado, and Atsuko Miyaji, “A Collision Attack on a Double-Block-Length Compression Function Instantiated with 8-/9-Round AES-256", IEICE Trans., Fundamentals. Vol. E99-A, No.1(2016), 14-21.

15. Ryoma Ito and Atsuko Miyaji, “Refined Glimpse correlations of RC4", IEICE Trans., Fundamentals. Vol. E99-A, No.1(2016), 3-13.

16. Jiageng Chen, Atsuko Miyaji, Hiroyuki Sato and Chunhua Su, “Improved Lightweight Pseudo-Random Number Generators for the Low-Cost RFID Tags", IEEE, Volume1, 17-24. 10.1109/Trustcom.2015.352

17. Jiageng Chen, Atsuko Miyaji, Chunhua Su and Je Sen The, “Improved Differential Characteristic Searching Methods", IEEE, 500-508. 10.1109/CSCloud.2015.42

18. Mazumder Rashed and Atsuko Miyaji, “A New Scheme of Blockcipher Hash", IEICE Trans., Information and Systems. Vol. E99-D, No.4(2016), 796-804.

19. Ryoma Ito and Atsuko Miyaji, “Refined RC4 key correlations of internal states in WPA", IEICE Trans., Fundamentals. Communications and Computer Sciences, Vol.E99-A, No.6, 1132-1144.

20. Steven Gordon, Atsuko Miyaji, Chunhua Su, and Karin Sumongkayothin, “A Matrix based ORAM: Design, Implementation and Experimental Analysis", IEICE Trans, , Information and Systems. Vol. E99-D, No.8(2016), 2044-2055.

21. Jiageng Chen, Rashed Mazumder, Atsuko Miyaji, Chunhua Su, “Variable message encryption through blockcipher compression function", Concurrency and Computation: Practice and Experience. 10.1002/cpe.3956

22. ITO Ryoma, Atsuko MIYAJI, “Refined Construction of RC4 Key Setting in WPA", IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences Vol.E100-A No.1 pp.138-148

23. Steven Gordon, Atsuko Miyaji, Chunhua Su, and Karin Sumongkayothin, “A Matrix based ORAM: Design, Implementation and Experimental Analysis",
IEICE Trans., Information and Systems. Vol. E99-D, No.8, 2044-2055, 2016.

24. Jiageng Chen, Rashed Mazumder, Atsuko Miyaji, and Chunhua Su, “Variable message encryption through blockcipher compression function", Concurrency and Computation: Practice and Experience, Vol. 29, Issue 7, Wiley Publishers, Special Issue: Combined Special Issues on Security and privacy in social networks, 2016. doi:10.1002/cpe.3956.

25. Mazumder Rashed, Atsuko Miyaji, and Chunhua Su, “A simple authentication encryption scheme", Concurrency and Computation: Practice and Experience, Wiley Publishers, 2016. doi: 10.1002/cpe.4058.

26. Atsuko Miyaji, Kazuhisa Nakasho, Shohei Nishida, “Privacy-Preserving Integration of Medical Data A Practical Multiparty Private Set Intersection", Journal of Medical Systems, 41, 3, 37, 2017. doi: 10.1007/s10916-016-0657-4., 1-10.

27. Rashed Mazumder, Atsuko Miyaji, Chunhua Su, “Probably Secure Keyed-Function based Authenticated Encryption Schemes for Big Data”, International Journal of Foundations of Computer Science, September Issue, 2017. doi:10.1142/S0129054117400123

28. Steven Gordon, Xinyi Huang, Atsuko Miyaji, Chunhua Su, Karin Sumongkayothin, and Komwut Wipusitwarakun, “Recursive Matrix Oblivious RAM: An ORAM construction for constrained storage devices”, IEEE Trans., Information Forensics and Security, VOL.12, Issue.12(2017), 3024-3038, doi:10.1109/TIFS.2017.2730584

29. Katsuya Tanaka, Ryuichi Yamamoto, Kazuhisa Nakasho, Atsuko Miyaji, “Development of a Secure Cross-Institutional Data Collection System Based on Distributed Standardized EMR Storage”, Studies in health technology and informatics, vol.255, pp.35-39, 2018. 10.3233/978-1-61499-921-8-35

30. Mohammad Saiful Islam Mamun, Ali A Ghorbani, Atsuko Miyaji, Uyen Trang Nguyen, “SupAUTH: A new approach to supply chain authentication for the IoT”, Computational Intelligence, vol.34, No.2, pp.582-602,2018. https://doi.org/10.1111/coin.12164

31. Mohammad Saiful Islam Mamun, Chunhua Su, Anjia Yang, Atsuko Miyaji, Ali Ghorbani, “OTP-IoT: An ownership transfer protocol for the Internet of Things”, Journal of information security and applications, vol.43, pp.73-82, 2018. https://doi.org/10.1016/j.jisa.2018.10.009

32. Chen-Mou Cheng, Kenta Kodera, and Atsuko Miyaji, “Differences among summation polynomials over various forms of elliptic curves",IEICE TRANSACTIONS on Fundamentals of Electronics}, Communications and Computer Sciences. Vol.XX, No.(2019), XX-XX, in press

[Chunhua Su]
33. Lu Zhou, Jiageng Chen, Yidan Zhang, Chunhua Su, Marino Anthony James. “Security analysis and new models on the intelligent symmetric key encryption”. Computers & Security Vol.80, pp.14-24, 2019.

34. Lu Zhou, Chunhua Su, Zhen Li, Zhe Liu, Gerhard P. Hancke. “Automatic fine-grained access control in SCADA by machine learning”. Future Generation Computer System, vol.93, pp.548-559, 2019.

35. Lu Zhou, Chunhua Su, Yamin Wen, Weijie Li, Zheng Gong. “Towards practical white-box lightweight block cipher implementations for IoTs.” Future Generation Computing System. Vol. 86, pp.507-514,2018.

36. Jiageng Chen, Jesen Teh, Zhe Liu, Chunhua Su and Azman Samsudin, Yang Xiang. “Towards Accurate Statistical Analysis of Security Margins: New Searching Strategies for Differential Attacks”, IEEE Transactions on Computers, Volume: 66, Issue: 10, pp.1763 – 1777, 2017 .

国際会議論文 ＊査読有り
[Atsuko Miyaji]
37. Jiageng Chen, Shoichi Hirose, Hidenori Kuwakado, and Atsuko Miyaji, “A Collision Attack on a Double-Block-Length Compression Function Instantiated with Round-Reduced AES-256”, Information Security and Cryptology - ICISC 2014, 8949(2015), 271-285, Springer-Verlag. 10.1007/978-3-319-15943-0_17

38. Jiageng Chen, Atsuko Miyaji, Chunhua Su and Liang Zhao, “A New Statistical Approach For Integral Attack", Lecture Notes in Computer Science, 9408(2015), 345-358, Springer-Verlag. 10.1007/978-3-319-25645-0_23

39. Atsuko Miyaji and Syouhei Nishida, “A Scalable and Efficient Multiparty Private Set Intersection", Lecture Notes in Computer Science, 9408(2015), 376-368, Springer-Verlag 10.1007/978-3-319-25645-0_26

40. Steven Gordon, Atsuko Miyaji, Chunhua Su and Karin Sumongkayothin, “M-ORAM: A Matrix ORAM with logN bandwidth cost", Lecture Notes in Computer Science, 9503(2016), 3-15, Springer-Verlag. 10.1007/978-3-319-31875-2_1

41. Jiageng Chen, Atsuko Miyiaji, Chunhua Su and Je Sen The, “Accurate Estimation of the Full Differential Distribution for General Feistel Structures", Lecture Notes in Computer Science, vol 9589, vol 108-124. 10.1007/978-3-319-38898-4_7

42. Jiageng Chen, Rashed Mazumder, and Atsuko Miyaji, “A Single Key Scheduling Based Compression Function", Risks and Security of Internet and Systems. CRiSIS 2015. Lecture Notes in Computer Science, vol 9572. Springer, Cham. https://doi.org/10.1007/978-3-319-31811-0_13

43. Atsuko Miyaji and Mazumder Rashed, “A new (n, 2n) Double Block Length Hash Function based on Single Key Scheduling”, Advanced Information Networking and Applications (AINA), 2015 IEEE 29th International Conference on Advanced Information Networking and Applications, 564-570. 10.1109/AINA.2015.237

44. Steven Gordon, Atsuko Miyaji, Chunhua Su and Karin Sumongkayothin, “Analysis of Path ORAM toward Practical Utilization”, Network-Based Information Systems (NBiS), 2015 18th International Conference on, 646-651, IEEE 10.1109/NBiS.2015.113

45. Steven Gordon, Atsuko Miyaji, Chunhua Su and Karin Sumongkayothin, “Security and Experimental performance analysis of a Matrix ORAM”, IEEE International Conference on Communications (IEEE ICC'16). 10.1109/ICC.2016.7511195

46. Kaitai Liang, Atsuko Miyaji and Chunhua Su, “Secure and Traceable Framework for Data Circulation”, The 21th Australasian Conference on Information Security and Privacy(ACISP 2016), Lecture Notes in Computer Science, 9722(2016), Springer-Verlag, 376-388.

47. Rashed Mazumder, Atsuko Miyaji, and Chunhua Su, “A Simple Authentication Encryption Scheme”, Proceedings in IEEE TrustCom'16, Concurrency and Computation: Practice and Experience. 10.1002/cpe.4058

48. Rashed Mazumder, Atsuko Miyaji, and Chunhua Su, “An Efficient Construction of a Compression Function for Cryptographic Hash”, The International Cross-Domain Conference and Workshop (CD-ARES 2016), Lecture Notes in Computer Science, 9817(2016), Springer-Verlag, 124-140.

49. Rashed Mazumder, Atsuko Miyaji, and Chunhua Su, “A Blockcipher based Authentication Encryption”, The International Cross-Domain Conference and Workshop (CD-ARES 2016), Lecture Notes in Computer Science, 9817(2016), Springer-Verlag, 106-123.

50. Karin Sumongkayothin, Steven Gordon, Atsuko Miyaji, Chunhua Su, and Komwut Wipusitwarakun, “Recursive M-ORAM: A Matrix ORAM for Clients with Constrained Storage Space”, International Conference on Applications and Techniques in Information Security (ATIS 2016), Communications in Computer and Information Science (CCIS), 651(2016), Springer-Verlag, 130-141.

51. Rashed Mazumder, Atsuko Miyaji, and Chunhua Su, “A Re-visited Construction of Nonce and Associated-data based Authenticated Encryption”, The 1st US-Japan Workshop Enabling Global Collaborations in Big Data Research, 15-18.

52. Hiroshi Nomaguchi, Atsuko Miyaji and Chunhua Su, “Evaluation and Improvement of Pseudo-Random Number Generator for EPC Gen2”, The 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom'17)}, IEEE, 721-728. doi:10.1109/Trustcom/BigDataSE/ICESS.2017.305

53. Tomoaki Mimoto, Shinsaku Kiyomoto, Katsuya Tanaka and Atsuko Miyaji, “(p, N)-identifiability: Anonymity Under Practical Adversaries”, The 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom'17)}, IEEE, 721-728. doi:10.1109/Trustcom/BigDataSE/ICESS.2017.343

54. Chen-Mou Cheng, Kenta Kodera, and Atsuko Miyaji, “On the computational complexity of ECDLP for elliptic curves in various forms using index calculus”, The 20th Annual International Conference on Information Security and Cryptology (ICISC 2017)}, Lecture Notes in Computer Science, 10779(2017), Springer-Verlag, 245-263. 10.1007/978-3-319-78556-1_14

55. Rashed Mazumder, Atsuko Miyaji, and Chunhua Su, “A simple construction of encryption for a tiny domain message", The 51th Annual Conference on Information Sciences and Systems (CISS2017), IEEE, 1-6, 2017.

56. Yusuke Matsuoka and Atsuko Miyaji, “Revisited Diffusion Analysis of Salsa and ChaCha”, The 15th International Symposium on Information Theory and Its Applications (ISITA 2018), IEEE, 452-456, 2018. 10.23919/ISITA.2018.8664391

57. Shota Terada, Hideto Nakano, Shinya Okumura, Atsuko Miyaji, “An Experimental Analysis on Lattice Attacks against Ring-LWE over Decomposition Fields”, 2018 International Symposium on Information Theory and Its Applications (ISITA 2018), IEEE, pp. 306-310, (2018). 10.23919/ISITA.2018.8664308

58. Tung Chou, Yohei Maezawa, Atsuko Miyaji, “A Closer Look at the Guo–Johansson–Stankovski Attack Against QC-MDPC Codes”, International Conference on Information Security and Cryptology, LNCS, volume 11396, pp.341-353, 2018. https://doi.org/10.1007/978-3-030-12146-4_21

59. Tomoaki Mimoto, Shinsaku Kiyomoto, Seira Hidano, Anirban Basu, and Atsuko Miyaji, “The Possibility of Matrix Decomposition as Anonymization and Evaluation for Time-sequence Data", 2018 16th Annual Conference on Privacy, Security and Trust (PST), 1--7, 2018, IEEE. 10.1109/PST.2018.8514189

60. Nicolás Emilio Díaz Ferreyra, Rene Meis, Maritta Heisel, Sourya Joyee De,

Abdessamad Imine, Kai Bavendiek, Robin Adams, Sibylle Schupp, Ghada El-Haddad, Amin Shahab, Esma Aimeur, Tomoaki Mimoto, Shinsaku Kiyomoto, Seira Hidano, Anirban Basu, Atsuko Miyaji, “WELCOME MESSAGE 6 ORGANIZERS 8 REVIEW COMMITTEES 10 KEYNOTE SPEAKERS 15”, 2018 16th Annual Conference on Privacy, Security and Trust (PST). 10.1109/PST.2018.8514200

61. Ryoma Ito, Atsuko Miyaji, “New Iterated RC4 Key Correlations”, Australasian Conference on Information Security and Privacy, LNCS, volume 10946, pp.154-171, 2018. https://doi.org/10.1007/978-3-319-93638-3_10

62. Katsunari Shishido, Atsuko Miyaji, “Efficient and Quasi-accurate Multiparty Private Set Union”, 2018 IEEE International Conference on Smart Computing (SMARTCOMP), pp.309-314, 2018. 10.1109/SMARTCOMP.2018.00021

63. Yaoan Jin and Atsuko Miyaji, “Secure and Compact Elliptic Curve Cryptosystems",
The 24th Australasian Conference on Information Security and Privacy (ACISP 2019)}, Lecture Notes in Computer Science, (2019), Springer-Verlag, in press

[Masakazu Soshi]
64. Yuta Kurihara and Masakazu Soshi. “A Novel Hash Chain Construction for Simple and Efficient Authentication". In 14th Annual Conference on Privacy, Security and Trust, PST 2016, December 2016. 10.1109/PST.2016.7907012

65. Hiroaki Anada, Shunsuke Tsumori, Samiran Bag, Masakazu Soshi, Atsushi Waseda, and Kouichi Sakurai. “Short Merkle one-time signatures (poster) ". In The 12th International Workshop on Security (IWSEC), 2017.

[Chunhua Su]
66. Ye Li, Kaitai Liang, Chunhua Su and Wei Wu. “DABEHR: Decentralized Attribute-Based Electronic Health Record System with Constant-Size Storage Complexity”, The 12th International Conference on Green, Pervasive and Cloud Computing. LNCS Vol.10232, pp.611-626, Amalfi Coast, Italy, May, 2017.

67. Weizhi Meng, Fei Fei, Lijun Jiang, Zhe Liu, Chunhua Su, Jinguang Han. “CPMap: Design of Click-Points Map-Based Graphical Password Authentication”, 33rd IFIP TC 11 International Conference, SEC 2018, IFIPAICT, volume 529 pp.18-32, Poznan, Poland, September, 2018.

＊その他の著作物（相手側研究チームとの共著のみ）（総説、書籍など）

該当なし

＊その他の著作物（相手側研究チームを含まない日本側研究チームの総説、書籍など）

該当なし

２．学会発表

＊口頭発表（相手側研究チームとの連名発表）
発表件数：2 件（招待講演：2 件）

＊口頭発表（相手側研究チームを含まない日本側研究チームの発表）
発表件数：64 件（招待講演：0 件）

＊ポスター発表（相手側研究チームとの連名発表）
　　発表件数：0 件

＊ポスター発表（相手側研究チームを含まない日本側研究チームの発表）
　　発表件数：0 件

３．主催したワークショップ・セミナー・シンポジウム等の開催
1. 2016/9/28～2016/9/30 Chinese Cryptology and Information Security Association,The 10th International Conference on Network and System Security (NSS 2016), Taiwan，Taipei, NSS 2016 is the next event in a series of highly successful events of Network and System Security. Previous editions were held in: New York City, USA (2015), Xi'an, China (2014), Madrid, Spain (2013); Wu Yi Shan, China (2012); Milan, Italy (2011); Melbourne, Australia; (2010); Gold Coast, Australia (2009); Shanghai, China (2008); and Dalian, China (2007). 60 名.

2. 2017/5/31～2017/6/1 宮地 充子 宮地研究室招待講演，日本，大阪，大阪大学 E3-9F ミーティング室, 《Title》Parity Check based Redistribution of Secret Shares, 30 名

3. 2018/8/23～2018/8/29 宮地充子 日本側のチームと台湾側のチームのジョイントワークショップ, Taiwan，Taipei, Chang-Gung University, 18 名

４．研究交流の実績
【研究ミーティング】
・2016/4/20-2016/4/22: 大阪大学 Kick-off Meeting & Joint Workshop
・2017/9/15-2017/9/22: 大阪大学 Meeting & Research Workshop
・2018/7/1-2018/9/30: 会津大学 Short-term visiting, Prof. Yeh Kuo-Hui (National Donghwa University, Taiwan)が会津大学の招聘研究員として滞在し、共同研究を行った。
・2018/3/1-2018/3/10: 会津大学 Short-term visiting
・2018/11/19-2018/11/21: 大阪大学, Chinese Culture University と Chang-Gung University の教員と学生が出席し、軽量暗号の設計について議論を行った。
・2019/3/27-2019/3/31: National Donghwa University, Taiwan Meeting
Prof. Chunhua (University of Aizu, Japan)が National Donghwa University, Taiwan に訪問し，今後の共同研究を展開する MOU を締結する.

【学生・研究者の派遣、受入】
・2018/3/1-2018/5/25: 会津大学 Short-term visiting
・2018/3/28-2018/4/25: 会津大学 Short-term visiting

５．特許出願
　　研究期間累積出願件数：1 件

６．受賞・新聞報道等
1. International Conference on Applications and Technologies in Information Security(ATIS 2016), Best Paper Award, Recursive M-ORAM: A Matrix ORAM for Clients with Constrained Storage Space, ATIS 2016, CCIS, 651 (2016), Springer-Verlag, 130-141. K. Sumongkayothin, S. Gordon, A. Miyaji, C. Su, and K. Wipusitwarakun, 2016/10/28.

2. The 16th IEEE International Conference on Trust, Security and Privacy(TrustCom 2017), Best Paper Award, Evaluation and Improvement of Pseudo-Random Number Generator for

EPC Gen2,Trustcom/BigDataSE/ICESS, 2017 IEEE. H. Nomaguchi, C. Su, A. Miyaji. 2017/8/2

７．その他

【セキュリティ専門家へのアウトリーチ活動】

1. Atsuko Miyaji,
(Keynote Speak) “Elliptic Curve Cryptosystems for IoT devices”, The 19th International Conference on Information and Communications Security (ICICS 2017), Beijing, China, December, 2017.
国際会議 ICICS2017 の招待講演で日本台湾のジョイント研究を紹介

2. Atsuko Miyaji, (Keynote Speak) “Privacy-Preserving Big Data Analysis”, The 10th International Conference on Network and System Security (NSS 2016).
国際会議 NSS2016 の招待講演で日本台湾のジョイント研究を紹介

3. Bo-Yuan Peng, Bo-Yin Yang, Yuan-Che Hsu, Yu-Jia Chen, Di-Chia Chueh, Chen-Mou Cheng, and Atsuko Miyaji, “Flexible and scalable implementation of elliptic-curve cryptography on FPGA,” invited paper at the 13th International SoC Design Conference (ISOCC 2016), Jeju, Korea, October 2016.
国際会議 ISOCC 2016 の招待講演で日本台湾のジョイント研究を紹介

【一般市民へのアウトリーチ活動】

1. 宮地 充子 ,
(招待講演) “How to Enhance the Security of IoT Devices”, LINE and Intertrust Security Summit Exploring
Technologies for Trusted Apps and Services, Tokyo, May 2017.
LINE の招待講演で日本台湾のジョイント研究を紹介
LINE　のワークショップで日本台湾のジョイント研究を紹介

【大学生向けアウトリーチ活動】

1. 宮地 充子 ,
「数論と計算科学の情報セキュリティへの応用−ビッグデータのセキュアな利活用」
金沢大学 理学談話会（数学・計算科学分野），2016 年 11 月 21 日（月）.
金沢大学の招待講演で日本台湾のジョイント研究を紹介

2. 宮地 充子,
「効率的なプライバシを考慮した他機関のデータ解析について」
第 16 回フィジカルヘルスフォーラム，2016 年 3 月 17 日.
第 16 回フィジカルヘルスフォーラムの招待講演で日本台湾のジョイント研究を紹介

以上