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：「モバイルヘルスケアにおけるプライバシー保護ビッグデータマイニングを実現するセキュア IoT 情報基盤」

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 | 菊池 浩明 | 教授 | 明治大学 総合数理学部 | 研究総括 |
| 主たる共同研究者 | 齋藤 孝道 | 教授 | 明治大学 理工学部 | 要素技術開発 |
| 主たる共同研究者 | 黄 緒平 | 研究員 | 明治大学　研究・知財戦略機構 | 開発 |
| 研究参加者 | 伊藤 聡志 | 大学院生 | 明治大学大学院先端数理科学研究科 | 開発 |
| 研究参加者 | 森 駿文 | 大学院生 | 明治大学大学院先端数理科学研究科 | 開発 |
| 研究参加者 | 山田 道洋 | 大学院生 | 明治大学大学院先端数理科学研究科 | 評価 |
| 研究期間中の全参加研究者数　22名 | | | | |

相手側チーム

| | 氏名 | 役職 | 所属 | 研究分担 |
|---|---|---|---|---|
| 研究代表者 | Chun-I Fan | 教授 | 国立中山大学 | 研究総括 |
| 研究参加者 | Jheng-Jia Huang | 大学院生 | 国立中山大学 | 開発 |
| 研究参加者 | Yi-Fan Tseng | 大学院生 | 国立中山大学 | 評価 |
| 研究参加者 | | | | |
| 研究期間中の全参加研究者数　9名 | | | | |

４．研究交流の概要

本研究はモバイルヘルスケアを実現する IoT デバイスの実現を目的としている。健康管理においては、機微なデータの盗聴、内部犯による権限外アクセスなどの脅威がある。それらに対して、CPU パワーに制約のあるデバイスでも実現可能な軽量暗号と述語暗号を導入し、プライバシー保護データマイニング(PPDM)を実現するセキュア IoT 情報基盤の開発を試みた。

本課題を解決するため、制約の多い IoT デバイス向きの軽量な認証技術スキームと軽量暗号技術を構築、健康情報の暗号文を暗号化されたままでデータマイニングする PPDM スキームを提案した。本課題を通じて、日本側はプライバシー保護データマイニングスキームの構築を行い、台湾側は認証スキーム、暗号スキームの構築を担当した。日本と台湾が交流を通じて相互的、相補的に取り組むことで、モバイルヘルスケア分野におけるセキュリティ応用の活性化を図ることが出来た。相互の得意分野が連携しており、共同プロジェクトにより大きな相乗効果が得られた。

５．研究交流の成果

５－１　共同研究の研究・開発成果

4 年間に渡る共同研究によって、IEEE Transactions Signal and Information Processing over Networks と IPSJ Journal of Information Processing (JIP)の 2 本を含む 9 件の論文発表を行った。本共同研究の目標であったモバイルヘルスケアを実現するためのセキュアな IoT デバイスと情報基盤に対して、十分な成果を上げている。特に、IEEE Transactions は、本情報通信分野における権威ある論文誌であり、そこで提案したセキュアな匿名クレデンシャルスキームは応用範囲が広く、大きな成果の一つである。また、情報処理学会 JIP にて発表したジャーナル論文では、 5000 人の脳卒中に関する現実の医療データを用いて、秘匿計算による重回帰を行っており、モバイルヘルスケアを安全に実施するという本共同研究の大きな貢献である。

５－２　国際連携による相乗効果

暗号要素技術に強い国立台湾大学の Fan 教授の研究グループと、プライバシー保護技術に精通して実装力を有する明治大学菊池研究室の大学院生が相互に交流することで、IEEE Transactions を含む 9 件の共著論文を出版することが出来た。また、2016 年度に、広島国際会議場で開催された国際会議 Mobiqutous 2016 において、モバイル IoT のセキュリティに関する国際ワークショップ Workshop on Security Technologies in the World with Internet of Things (IoTSec 2016) を共同で開催した。

５－３　共同研究成果から期待される波及効果および進展

本研究における多くの研究成果は、主に学術目的によるものであり、製品化や企業化などの実績は得られなかった。知的財産は主張せず、論文の形で広く学術コミュニティに公開することで貢献した。

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）

共同研究を通じて、日本で 3 回、台湾で 3 回の共同ワークショップを実施し、大学院生同士による英語での研究交流を図った。延べ出張人数は、日本から 22 名、台湾から 9 名であった。大学院生の多くは、これらの研究交流の機会を活用して語学力とプレゼンテーション力を付けて、議論のスキルを磨き、その後の国際会議の論文採択に繋げることが出来た。参加者の数名は、その後大学や研究機関で研究職に就いている。以上より、十分な人材育成を果たしたと評価している。

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

１．Project Title：「 Secure IoT-Based Information Platform with Privacy-Preserving Data Mining on Big Data for M-Healthcare 」

２．Project Period：January 2016 ～ March 2019

３．Main Participants：

Japan-side

| | Name | Title | Affiliation | Role |
|---|---|---|---|---|
| PI | Hiroaki Kikuchi | Professor | Meiji University | Supervisor |
| Co-PI | Takamichi Saito | Professor | Meiji University | Developer |
| Co-PI | Xuping Huang | Researcher | Meiji University | Developer |
| Collaborator | Satoshi Ito | Grad. student | Meiji University | Developer |
| Collaborator | Takafumi Mori | Grad. student | Meiji University | Developer |
| Collaborator | Michihiro Yamada | Grad. student | Meiji University | Developer |
| Total number of participating researchers in the project: 22 | | | | |

Partner-side

| | Name | Title | Affiliation | Role |
|---|---|---|---|---|
| PI | Chun-I Fan | Professor | National Sun Yat-Sen University | supervisor |
| Collaborator | Jheng-Jia Huang | Grad. student | National Sun Yat-Sen University | developer |
| Collaborator | Yi-Fan Tseng | Grad. student | National Sun Yat-Sen University | developer |
| Total number of participating researchers in the project: 9 | | | | |

４．Scope of the joint project

Mobile healthcare (m-healthcare) is a thriving issue as novel information technology. However, once the unencrypted medical records deposited in public clouds are accessed by malicious parties, the safety of the patients will face enormous threats. Thus in this research, we will propose a secure IoT-based information platform for m-healthcare with privacy-preserving data mining on big data.

Taiwanese team focused on the secure infrastructure of the system consisting of cryptographic primitives and provided an encrypted database suitable for PPDM developed by Japanese team. In collaboration, we had two workshops every year, one in Taiwan and the other in Japan, for the members to exchange the experiences, integrate the results, and strengthen the cooperation between both sides.

５．Outcomes of the joint project

５－１ Intellectual Merit

We published 9 research papers including prestigious international journal, IEEE Transactions Signal and Information Processing over Networks and IPSJ Journal of Information Processing (JIP). Hence, our purpose on secure IoT-based information platform for mobile healthcare with privacy preserving could be satisfied. One of the main results is to demonstrate our scheme for 5,000 real patient data for identify primary factor for death.

５－２ Synergy from the Collaboration

With collaboration of two international research teams, we combined the cryptographical

knowledge from Taiwan side with network security technologies form Japanese side, and succeed to publish many scientific papers. Especially, Workshop on Security Technologies in the World with Internet of Things (IoTSec 2016) was jointly organized.

５－３ Potential Impacts on Society

Our contributions are mainly in academic papers which help to give inspire to security and privacy industries in future.

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

With international workshops held in 3 times in Japan and 3 times in Taiwan, the total of 22 researchers exchanged and discussed for improvement of the collaborative study and finding future collaborations. Many of them were graduate students who improved their English skills well through the international workshops.

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）
査読あり


1. 1. H. Kikuchi, H. Yasunaga, H. Matsui and C. I. Fan, Efficient Privacy-Preserving Logistic Regression with Iteratively Re-weighted Least Squares, 2016 11th Asia Joint Conference on Information Security (AsiaJCIS), pp. 48-54, IEEE, 2016. doi.org/10.1109/ICITCS.2016.7740335
2. C. I. Fan, J. S. Wang, J. J. Huang, Y. F. Tseng, W. S. Juang and H. Kikuchi, "Flexible Authentication Protocol with Key Reconstruction in WBAN Environments", 2016 6th International Conference on IT Convergence and Security (ICITCS), pp. 1-5, IEEE, 2016. doi.org/10.1109/ICITCS.2016.7740335
3. Chun-I Fan, Yi-Fan Tseng, Jheng-Jia Huang, Shih-Fen Chen, Hiroaki Kikuchi: Multireceiver Predicate Encryption for Online Social Networks, IEEE Trans. Signal and Information Processing over Networks 3(2): 388-403 (2017) DOI: 10.1109/TSIPN.2017.2697580
4. Chien-Nan Wu, Chun-I Fan*, Jheng-Jia Huang, Yi-Fan Tseng, and Hiroaki Kikuchi, “An Efficient Signature Scheme for Anonymous Credentials,” the 5th International Conference on Applied Computing & Information Technology (ACIT 2017), Hamamatsu, Japan, July 9-13, 2017.
5. Chien-Nan Wu, Chun-I Fan, Jheng-Jia Huang, Yi-Fan Tseng, Hiroaki Kikuchi, "Probably Secure Efficient Anonymous Credential Scheme", International Journal of Software Innovation, Volume 6, Issue 3, pp. 8-35, 2018 DOI: 10.4018/IJSI.2018070102
6. Hiroaki Kikuchi, Chika Hamanag, Hideo Yasunaga, Hiroki Matsui, Hideki Hashimoto, Chun-I Fan, "Privacy-Preserving Multiple Linear Regression of Vertically Partitioned Real Medical Datasets", Journal of Information Processing, 2018, Volume 26, IPSJ, pp. 638-647, 2018. doi:10.2197/ipsjjip.26.638
7. Xuping HUANG, Hiroaki KIKUCHI, Chun-I FAN, "Privacy Preserved Spectral Analysis Using IoT mHealth Biomedical Data for Stress Estimation", 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), IEEE, pp. 793-800, 2018. DOI: 10.1109/AINA.2018.00118
8. Kodai Nagata, Hiroaki Kikuchi, Chun-I Fan, "Risk of Bitcoin Addresses to be Identified from Features of Output Addresses", 2018 IEEE Conference on Dependable and Secure Computing (DSC) federated workshop, pp. 349-354, IEEE, 2018. DOI: 10.1109/DESEC.2018.8625106
9. Chun-I Fan, Yi-Fan Tseng, Hui-Po Su, Ruei-Hau Hsu, Hiroaki Kikuchi, "Secure Hierarchical Bitcoin Wallet Scheme Against Privilege Escalation Attacks", 2018 IEEE Conference on Dependable and Secure Computing (DSC) federated workshop, pp. 349-3, Kaohsiung, Taiwan, 2018, pp. 1-8, 54, IEEE, 2018. DOI: 10.1109/DESEC.2018.8625151


＊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）


10. 新原 功一, 菊池 浩明, e ラーニングをモデルとした内部犯行の予測因子の識別, 情報処理学会論文誌, Vol. 57, No. 9, pp. 2064 - 2076, 2016.
11. Hiroaki Kikuchi, Katsumi Takahashi, "Zipf Distribution Model for Quantifying Risk of Re-identification from Trajectory Data", Journal of Information Processing, Vol. 24 (2016) No. 5 pp. 816-823. doi.org/10.2197/ipsjjip.24.816
12. 菊池 浩明, 匿名加工・再識別コンテスト Ice and Fire : 匿名加工方式とその安全性を評

価する試み, 情報処理学会論文誌,57(9), pp. 1900-1910, IPSJ, 2016.
13. 新原 功一 , 山田 道洋 , 菊池 浩明, "共有アカウント利用時における不正行為の誘発要因", 情報処理学会論文誌,58(12), pp. 1875-1889, 2017.
14. Hiroaki KIKUCHI, Takayasu YAMAGUCHI, Koki HAMADA, Yuji YAMAOKA, Hidenobu OGURI, Jun SAKUMA, "Study on Record Linkage of Anonymizied Data", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Volume E101.A (2018), Issue 1, pp. 19-28, 2018. doi.org/10.1587/transfun.E101.A.19
15. Hiroaki Kikuchi, Xuping Huang, Shigeta Ikuji, Manami Inoue, "Privacy-Preserving Hypothesis Testing for Reduced Cancer Risk on Daily Physical Activity", Journal of Medical Systems, 42: 90, Springer, pp. 1-12, 2018. DOI: 10.1007/s10916-018-0930-9
16. Ryo Nojima, Hidenobu Oguri, Hiroaki Kikuchi, Hiroshi Nakagawa, Koki Hamada, Takao Murakami, Yuji Yamaoka, Chiemi Watanabe, "How to Handle Excessively Anonymized Datasets", Journal of Information Processing, 2018, Volume 26, Pages 477-485, 2018. DOI: 10.2197/ipsjjip.26.477
17. 滋野 莉子 , 山田 道洋 , 菊池 浩明 , 坂本 真樹, "オノマトペ CAPTCHA の開発と評価", 情報処理学会論文誌,59(9), pp. 1666-1677, 2018.
18. Satoshi Ito, Hiroaki Kikuchi, "Risk of Re-identification from Payment Card Histories in Multiple Domains", 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), IEEE, pp. 934-941, 2018. DOI: 10.1109/AINA.2018.00137
19. Tomohiro Shigemoto, Shota Fujii, Ichiro Kuriama, Tetsuro Kito, Hirofumi Nakakoji, Yasuhiro Fujii, Hiroaki Kikuchi, “Development of White List Based Autonomous Evolution of Defense System for RAT Malware", 2018 13th Asia Joint Conference on Information Security (AsiaJCIS), pp. 95-101, IEEE, 2018. DOI: 10.1109/AsiaJCIS.2018.00024
20. Kota Sasa, Hiroaki Kikuchi, "Impact Assessment of Password Reset PRMitM attack with Two-factor Authentication", 2018 IEEE Conference on Dependable and Secure Computing (DSC), pp. 90-97, IEEE, 2018. DOI: 10.1109/DESEC.2018.8625132
21. Mori T., Kikuchi H., "Person Tracking Based on Gait Features from Depth Sensors", Advances in Network-Based Information Systems, NBiS 2018, Lecture Notes on Data Engineering and Communications Technologies, vol 22, pp 743-751, 2018. DOI: 10.1007/978-3-319-98530-5_65

＊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：0 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：7 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. Workshop on Security Technologies in the World with Internet of Things (IoTSec 2016), Hiroshima, Dhiren R. Patel, Chun-I Fan, Hiroaki Kikuchi, Japan, International Conference Center Hiroshima, 2016 年 11 月 28 日，参加者数 30 名程度.

４．研究交流の実績
【合同ワークショップ】
- 2016 年 8 月 20 日～28 日、明治大学中野キャンパス（東京、日本)、双方のチームメンバーを交えて研究計画を検討した。
- 2016 年 12 月 10 日～13 日、国立中山大学（台湾、高雄)、チームメンバーを交えて、研究調査結果を共有し、議論を行った。
- 2017 年 7 月 4 日～9 日、明治大学中野キャンパス（東京、日本)、チームメンバーに研究協力者を交えて、関連研究成果の共有と、共同研究の進捗状況を報告した。
- 2017 年 11 月 25 日～28 日、国立中山大学（台湾、高雄)、チームメンバーに研究協力者を加えて、共同研究の進捗状況を確認した。
- 2018 年 7 月 16 日、明治大学駿河台キャンパス（東京、日本)、チームメンバーにゲスト講師を加えて、関連分野の最新状況を入手し、成果報告を行った。
- 2019 年 1 月 3 日～6 日、国立中山大学（台湾、高雄)、チームメンバーを中心として、研究成果を整理し、今後の研究について展望した。

５．特許出願
研究期間累積出願件数：0 件

６．受賞・新聞報道等

該当なし

７．その他

該当なし

以上