戦略的国際共同研究プログラム(SICORP)
EIG CONCERT-Japan 共同研究
終了報告書　概要

1. 研究課題名：「将来社会を支える次世代 IoT のための有機的レジリエント・セキュア無線ネットワーク」
2. 研究期間：令和 3 年 4 月～令和 6 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	石橋　功至	教授	電気通信大学・先端ワイヤレス・コミュニケーション研究センター	日本側PI、分散セキュア無線アーキテクチャの設計
主たる共同研究者	石川　直樹	准教授	横浜国立大学・大学院工学研究院	セキュア信号処理の設計
主たる共同研究者	佐藤　光哉	助教	電気通信大学・人工知能先端研究センター	分散機械学習の設計
研究期間中の全参加研究者数		16名		

相手側（ドイツ・スペイン・トルコ）チーム

	氏名	役職	所属	研究分担
研究代表者	Giuseppe T. F. de Abreu	Professor	Constructor University Bremen ・School of Computer Science & Engineering	EU側PI、信号処理設計
主たる共同研究者	Luis Hernández Encinas	Scientific Researcher	State Agency Spanish National Research Council・Institute of Physical and Information Technologies (ITEFI)	暗号解読法・トレードオフ解析
主たる共同研究者	Kaya Demir	Senior Researcher	TÜBİTAK・BİLGEM	ポスト量子・軽量暗号技術
研究期間中の全参加研究者数		13名		

4. 国際共同研究の概要

次世代 IoT では、超多数のデバイスが無線を介して情報を伝送し、人間社会・生活の質を向上させることが期待される。しかし、量子計算機の高度化により、現在普及しているセキュリティ技術では情報の安全性を維持できなくなる可能性があり、新たな発想に基づいたセキュリティ技術の実現が急務である。本国際共同研究では、計算量に依存しない暗号、無線通信の特性を利用した物理層セキュリティ、分散型プロトコルによるセキュリティの三つを技術的柱とし、これらを有機的に組み合わせることで、安定して高い安全性を実現する次世代の IoT 技術基盤を提案することを目的として研究を実施した。

5. 国際共同研究の成果

5-1　国際共同研究の学術成果および実施内容

3 年間の実施期間のうち、2 年間が新型コロナウイルス感染症への対策によって大幅な制約を受ける中での実施となった。しかし、査読付き論文誌 7 本（うち 4 本が日欧共著）、国

際会議発表 12 件（うち 6 件が日欧共著)、国内学会発表 4 件、国際会議ベストペーパーアワード 1 件を含む受賞 9 件と当初目標を超える極めて優れた実績を得られた。特に論文誌については通信分野における Q1 雑誌に毎年少なくとも 1 編が掲載されており、量だけでなく、高い質を伴って研究を実施できたと考えられる。以下に三つの代表的成果について概説する。

テンソル分解に基づくセルフリー大規模 MIMO：正規通信者に対して極限までビーム精度を高め、盗聴者に対する信号の漏洩を防ぐプリコーディング手法に対する検討を進めた。この手法では、送信信号を任意に極限まで所望の端末に集中させることができるため、盗聴者に関する事前情報を必要とせずにプリコーダを設計可能であり、正規通信者の周波数利用効率を最大化可能である。また、この手法はセキュアな通信に留まらず、より広義の通信に対しても適用可能であり、一般のセルフリー大規模 MIMO の上り/下り通信において、従来手法と同等な計算量でより高い周波数利用効率を達成可能なことを明らかにした。本成果は日欧共著論文として執筆し、IEEE の Q1 国際誌に掲載された [10.1109/OJCOMS.2022.3167101]。当該論文については、掲載雑誌内にて popular article となるなどその高い新規性が認められている。

隠蔽通信の非コヒーレント検出方式：無線物理層から抽出した真性乱数を効果的に活用可能な物理層暗号化技術を提案した。攻撃者が無制限の計算資源を持つ場合であっても、通信の存在自体が第三者に検知されなければ、攻撃リスクを最小限に抑えることができる。この考え方に基づく方式は隠蔽通信と呼ばれ、従来研究では、送信信号が時間領域と周波数領域の両方でガウス分布に従う場合に、検知確率を最小化できることが明らかとなっている。本研究では、対角ユニタリ行列にガウス分布に従う時空間射影を掛けることで、ガウス性の送信信号を生成する手法、および、その非コヒーレント検出を可能とする信号処理技術を考案した。従来手法と比べて、符号語の生成に必要とされる乱数を大幅に削減できるとともに、検出計算量を 1/3 程度に抑えられる。本成果は日欧共著論文として執筆し、IEEE の Q1 国際誌に掲載された [10.1109/LWC.2022.3233619]。

ブロックチェーンを用いた分散連合機械学習 (DFL)の高速化：DFL のモデル管理にブロックチェーンを導入することで、学習の高信頼化が期待できる。一方、マイニングに伴う計算遅延や通信データ量の増大が問題となる。ここでは参加端末間でデータセットに偏りのある環境を対象とした、学習/クライアントの適応選択法を設計した。学習端末群からなるデータセットの偏りの低さを目的関数とした定式化およびその一解法を示し、画像分類タスクを対象とした計算機シミュレーションにより、短時間で高精度な学習が実施できることを明らかにした。本成果は IEEE VTC2023-Fall で発表し、IEEE VTS Tokyo/Japan Chapter 2023 Young Researcher's Encouragement Award を受賞した。

5-2　国際共同研究による相乗効果

現在、6G の規格化が開始され、「アンビエント IoT」などのキーワードで関連内容が議論されている。本研究は学術的要素が強く、まだ実用化には至っていないが、6G の規格化が本格化する 2025 年までに成果をさらに推進する予定である。国内外企業との共同研究も進行中であり、規格化の可能性を探る。産学連携を通じた研究展開と人材育成が進められ、特許申請や標準化への貢献も期待される。

5-3　国際共同研究成果の波及効果と今後の展望

本研究プロジェクトが終了した後も、欧州側研究者とは引き続き共同研究を実施している。また、日本側チームでは本研究で得られた成果を基盤として、新たなプロジェクト申請の準備を進めている。以上のように、日欧の確固たる国際共同研究関係を築くことができ、今後もこの関係を継続することで、若手研究者や学生らの国際交流を活発化する。

Strategic International Collaborative Research Program (SICORP)
EIG CONCERT-Japan Joint Research Program
Executive Summary of Final Report

1. Project title : Organically Resilient and Secure Wireless Networks for Next-Generation IoT Technologies to Serve Future Connected Societies
2. Research period：April 2021 ～ March 2024
3. Main participants：

Japan-side

	Name	Title	Affiliation	Role in the research project
PI	Koji ISHIBASHI	Professor	The University of Electro-Communications	Distributed secure wireless architecture design
Co-PI	Naoki ISHIKAWA	Associate Professor	Yokohama National University	Secure signal processing design
Co-PI	Koya SATO	Assistant Professor	The University of Electro-Communications	Distributed machine learning design
Total number of participants throughout the research period： 16				

Partner（Germany, Spain, Turkey）-side

	Name	Title	Affiliation	Role in the research project
PI	Giuseppe T. F. de Abreu	Professor	Constructor University Bremen ・School of Computer Science & Engineering	Signal processing design
Co-PI	Luis Hernández Encinas	Scientific Researcher	State Agency Spanish National Research Council・Institute of Physical and Information Technologies (ITEFI)	Cryptanalysis and trade-off analysis
Co-PI	Kaya Demir	Senior Researcher	TÜBİTAK・BİLGEM	Post-Quantum and Lightweight Cryptography
Total number of participants throughout the research period： 13				

4. Summary of the international joint research

In the next-generation IoT, a large number of mobile devices communicate each other, enhancing the quality of life. However, the future development of quantum computing poses a threat to current security technologies, necessitating novel security approaches. This international collaborative research aimed to propose a next-generation IoT technology platform that combines three technological aspects: post-quantum cryptography, physical layer security, and security maintained with distributed protocols.

The Japanese team, comprising the University of Electro-Communications and Yokohama National University, contributed mainly to physical layer design and protocols based on their expertise in wireless communications. The European researchers included a Spanish team specializing in post-quantum cryptography and security analysis, a Turkish team focusing on hardware implementation and analysis, and a German team directing this

collaboration covering both wireless and security areas.

5. Outcomes of the international joint research

5-1 Scientific outputs and implemented activities of the joint research

Despite significant restrictions due to the pandemic of COVID-19 for two of the three years, our research collaboration produced exceptional results: seven peer-reviewed journal papers (four co-authored by EU-JP researchers), twelve international conference presentations (six co-authored), four domestic conference presentations, and nine awards including one Best Paper Award. Notably, at least one paper was published annually in a Q1 journal in Telecommunications. We have obtained the following three key outcomes.

Cell-free massive MIMO based on tensor decomposition: We proposed a precoding method that improves beam accuracy for legitimate user terminals and prevents signal leakage to eavesdroppers. This method can concentrate the transmitted signal to the desired terminal extensively, and the precoder can be designed without prior information about the eavesdropper. The method is applicable not only to secure communications, but also to general wireless communications. We have shown that the method can achieve higher spectral efficiency in general cell-free large-scale MIMO uplink/downlink with the same complexity as the conventional method. The paper was co-authored by EU-JP researchers and published in IEEE's Q1 journal [10.1109/OJCOMS.2022.3167101], which has been recognized as a popular article in the journal.

A non-coherent detection method for covert communication: We proposed a physical layer security technique that can utilize true random numbers extracted from wireless channels. Even if an eavesdropper has unlimited computational resources, the attack risk can be minimized if the existence of the communication itself is not detected by a third party. A scheme based on this idea is called covert communication, and previous research has shown that the detection probability can be minimized when the transmitted signal follows a Gaussian distribution in both time and frequency domains. In this research, we devised a method to generate Gaussian-distributed signals and a signal processing technique to enable its noncoherent detection. Compared to the conventional method, this method significantly reduces the number of random numbers required for codeword generation and the time complexity to 1/3 of the conventional method. The paper was co-authored by EU-JP researchers and published in IEEE's Q1 journal [10.1109/LWC.2022.3233619].

Acceleration of Blockchain-Based Decentralized Federated Learning (DFL): Introducing blockchain into DFL's model management can enhance the FL's reliability. However, the mining step raises novel problems regarding computational delays and increased communication time. To improve these problems, we designed an adaptive selection method for learning/clients targeting environments with biased datasets among participating terminals. We formulated an objective function to minimize dataset bias among training clients and presented a solver. Numerical simulations on image classification tasks demonstrated that our method can achieve high-accuracy learning in a short time. This result was presented at IEEE VTC2023-Fall and received the IEEE VTS Tokyo/Japan Chapter 2023 Young Researcher's Encouragement Award.

5-2 Synergistic effects of the joint research

As the standardization of 6G begins, with discussions around ambient IoT, the academic outcomes of our collaboration are being further developed towards 2025. Ongoing collaborations with domestic and international companies aim to explore standardization possibilities, fostering advancements through industry-academia partnerships.

5-3 Scientific, industrial or societal impacts/effects of the outputs

The collaboration with European researchers continues with the Japanese team preparing new project proposals based on the above outcomes. The strong relationship established between Japanese and European researchers will be maintained, fostering international exchanges among young researchers and students, thereby accelerating and advancing this research further.

国際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）発表件数：計 4 件
・査読有り：発表件数：計 4 件

1. H. Iimori, T. Takahashi, K. Ishibashi, G. T. F. De Abreu and W. Yu, “Grant-Free Access via Bilinear Inference for Cell-Free MIMO with Low-Coherence Pilots”, *IEEE Trans. Wireless Commun.*, **2021**, 20(11), 7694-7710, DOI: 10.1109/TWC.2021.3088125
2. K. Ando, H. Iimori, G. T. F. de Abreu and K. Ishibashi, "User-Heterogeneous Cell-Free Massive MIMO Downlink and Uplink Beamforming via Tensor Decomposition," in *IEEE Open J. Commun. Soc.*, **2022**, 3, 740-758, DOI: 10.1109/OJCOMS.2022.3167101
3. Y. Katsuki, G. T. F. de Abreu, K. Ishibashi, and N. Ishikawa, “A new noncoherent Gaussian signaling scheme for low probability of detection communications,” *IEEE Wireless Commun. Lett.*, **2023**, 12(3), 545–549, DOI: 10.1109/LWC.2022.3233619
4. Y. Katsuki, G. T. F. d. Abreu, K. Ishibashi and N. Ishikawa, "Noncoherent Massive MIMO With Embedded One-Way Function Physical Layer Security," *IEEE Trans. Inf. Forensics Secur.*, **2023**, 18, 3158-3170, DOI: 10.1109/TIFS.2023.3277255

・査読無し：発表件数：計 0 件
該当なし

＊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）：発表件数：計 2 件
・査読有り：発表件数：計 1 件

1. Y. Shibasaki, K. Iwamura, and K. Sato, "A Communication-Efficient Secure Routing Protocol for IoT Networks," *Sensors*, **2022**, 22(19), 7503, DOI: 10.3390/s22197503

・査読無し：発表件数：計 0 件
該当なし

＊その他の著作物（相手側研究チームとの共著総説、書籍など）：発表件数：計 1 件

1. 佐藤光哉, “無線設計の問題として見る分散連合機械学習,” *IEICE Fundamentals Review*, **2022**, 16(1), 7-16, DOI: 10.1587/essfr.16.1_7

＊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）：発表件数：計 0 件
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：計 5 件（うち招待講演：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：計 5 件（うち招待講演：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：計 1 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：計 4 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. Cybersecurity in Future Connected Societies (Special Session at 15th International Conference on Computational Intelligence in Security for Information Systems)、主催者：Víctor Gayoso Martíne（CSIC）・石橋功至（UEC・教授）、サラマンカ、スペイン、2022 年 9 月 7 日、参加人数 30 名程

4. 研究交流の実績（主要な実績）

【学生・研究者の派遣、受入】

・2022 年 2 月～3 月：日本から修士学生 1 名が、共著論文執筆のため約 1 ヶ月間相手研究機関に留学した。

・2022 年 10 月～2023 年 3 月・日本から学士学生 1 名が、共著論文執筆のため約 6 ヶ月間相手研究機関に留学した。

・2022 年 2 月～3 月：相手国側研究員を日本側研究機関に約 2 ヶ月間受け入れた。

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

・2022 年 2 月 14 日：令和 4 年度電気通信大学 目黒会賞

・2022 年 6 月 17 日：IEICE 無線通信システム研究会「初めての研究会」優秀発表賞

・2023 年 3 月 24 日：横浜国立大学 CREATES 論文賞

・2023 年 10 月 11 日：IEEE VTS Tokyo/Japan Chapter 2023 Young Researcher's Encouragement Award

・2023 年 11 月 21 日：WPMC2023 Best Paper Award

・2023 年 11 月 21 日：WPMC2023 Student Travel Grant

・2024 年 1 月 18 日：IEEE SPS Japan Student Journal Paper Award

・2024 年 3 月 25 日：令和 5 年度電気通信大学 学生表彰 2 件

7. その他

【オープンサイエンスにかかる取り組み】

・カオス理論に基づく通信技術三方式のオープンソース実装を MIT ライセンスで公開
https://github.com/ishikawalab/wiphy/blob/master/wiphy/examples/kaddoum2011csk.py
https://github.com/ishikawalab/wiphy/blob/master/wiphy/examples/kaddoum2011dcsk.py
https://github.com/ishikawalab/wiphy/blob/master/wiphy/examples/okamoto2012chaos.py

・プロジェクトのウェブページ（https://sites.google.com/view/concertjapan-oracle）を開設し、本研究で得られた知見をまとめたものをデリバラブルとして公開

【最終年度の議論を踏まえた研究成果の発表予定】

・富増佑太, 佐藤光哉 “ランダムウォーク SGD による故障耐性のある分散連合機械学習の検討,” 電子情報通信学会スマート無線研究会, 北海道民活動センター, 2024 年 7 月.

・内村颯汰, 安藤研吾, アブレウ ジュゼッペ, 石橋功至, "シングルキャリアサブテラヘルツ通信のための線形等化器およびビームフォーミングの同時設計," 電子情報通信学会無線通信システム研究会, 北海道立道民活動センター, 2024 年 7 月.

・三輪健太, 安藤研吾, アブレウ ジュゼッペ, 石橋功至, "環境発電を用いたセキュアな URLLC を実現するための有限符号長の最適化," 電子情報通信学会無線通信システム研究会, 北海道立道民活動センター, 2024 年 7 月.