２０２２年度研究ステーション研究成果報告書

１．研究ステーション名　　情報セキュリティ研究ステーション
　　研究代表者名（所属部局・職・氏名）　情報学専攻 准教授 高田 哲司

２．研究組織

＜学内構成員＞

電気通信大学	大学院情報理工学研究科	情報学専攻	教授	田中 健次
電気通信大学	大学院情報理工学研究科	情報学専攻	教授	崎山 一男
電気通信大学	大学院情報理工学研究科	情報学専攻	教授	岩本 貢
電気通信大学	大学院情報理工学研究科	情報学専攻	教授	大坐畠 智
電気通信大学	大学院情報理工学研究科	情報学専攻	准教授	岩崎 敦
電気通信大学	大学院情報理工学研究科	情報学専攻	准教授	高田 哲司
電気通信大学	大学院情報理工学研究科	情報学専攻	助教	渡邉 洋平

＜学外構成員＞
　東京工業大学　情報理工学院　情報工学系　教授　小池 英樹

３．２０２２年度の研究の特筆すべき成果

成果１）自動運転シミュレータで生成したデータを用いた連合学習による物体検出

近年の自動運転技術の向上に伴い，自動車が生成するデータ量も急激に増加している．そのため，機械学習を用いてデータを処理することが必要であるが，従来の手法では複数の自動車から生成された生データを中央サーバで集約・管理していたため，ユーザのプライバシを侵害する危険性があった．連合学習ではデータを集約することなく，各車両で生成されたモデルの更新差分を集約することで学習が行われるため，データを他者に送信する必要がない．しかし、連合学習の実用化を考えると，各車両が自車両内で完結して画像データに対する教師あり学習での正解ラベルを作成し，連合学習を行う手法が望まれるが，このような手法は確立されていない．そのため，既存の研究では画像データに対応する既知の正解ラベルが与えられて評価実験が行われ，現実的な利用形態での評価ができない状況となっている．

本研究では自動運転における物体検出において，Multiple Object Tracking を利用することによって各車両がローカルに画像へラベル付けを行い，そのデータをもとに連合学習を行う手法を提案した．さらに車両に搭載されたセンサが検知する物体までの距離を変化させて生成したデータセットを検証データとして使用し，評価することにより，どのような状況下でのデータを用いると高い精度で学習が行えるのかの評価を行った．

成果２）個人認証の「のぞき見」に対する対策手法の改良

覗き見攻撃は携帯端末での個人認証において現実的に起こりうる脅威の1つである．この脅威に対する対策手法として，携帯端末の振動機能を利用した個

人認証手法が複数提案されている．しかしそれらの手法には認証に時間がかかるという実用面の課題がある．そこで本研究では，振動機能を利用した既存手法の1つに対し，ユーザインタフェース改良を図ることによって，覗き見攻撃に対する安全性を維持しながら既存手法より認証時間を短縮することを試みた．1つは入力操作に必要な情報の取得時間を短縮させるものであり，もう1つは直感的な入力操作方法の導入である．この提案に基づく認証システムをAndroidアプリケーションとして実装し，実験参加者による評価実験を行った．実験結果から，改良対象となったシステムとの比較で認証時間を平均6秒短縮することに成功した．また安全性についても想定脅威に対して同等程度の安全性が維持されることが確認された．さらに，振動を利用した他の既存認証手法とも比較議論を行い，提案手法が先行研究の手法よりも操作負担が低く，安全性を危殆化させうる問題点が少ない手法であることを示した

４．２０２２年度の研究成果の公表実績

【ニュースリリース】人工知能・機械学習分野の国際学会「UAI2022」にて論文採択 ーマルチエージェント環境における学習を安定化させる手法を提案ー
https://www.uec.ac.jp/news/announcement/2022/20220715_4643.html

【プレスリリース】AI Lab、人工知能分野のトップカンファレンス「IJCAI」にて2本の共著論文採択　ーマッチング問題および推薦システムにおける性能向上に繋がる手法を提案ー
https://www.cyberagent.co.jp/news/detail/id=27679

なお構成員の研究成果は，国内外の学術会議で発表されている．詳細については項目７．「発表論文等」を参照されたい．

５．外部資金の獲得状況

1. 科研費（基盤研究(Ｓ)）日本学術振興会
「暗号技術によるIoTエコシステムのレジリエンス向上」
代表者：崎山一男・分担者：岩本貢，渡邉洋平
直接経費　149,500千円・間接経費 44,850千円

2. 科研費（基盤研究(Ｂ)）日本学術振興会
「十分統計量に基づくシミュレーションベース安全性の深化」
代表者：岩本貢・分担者：渡邉洋平
直接経費 13,300千円・間接経費3,990千円

3. 科研費（基盤研究(Ｂ)）日本学術振興会
「公開鍵暗号の識別不可能性に対する総合的評価技術の開発」
代表者：四方順司・ 分担者：岩本貢
直接経費 13,200千円・間接経費3,960千円

4. 科研費（基盤研究(B)）日本学術振興会
「広範な検索機能と高い効率性を両立する秘匿検索技術の実現」
代表者：渡邉洋平
直接経費 13,000千円・間接経費3,900千円

5. 科研費（基盤研究（C））日本学術振興会
「長期運用に耐えうる共通鍵暗号による秘匿検索暗号」
代表者：太田和夫・分担者：岩本貢，渡邉洋平
直接経費 3,200千円・間接経費 960千円

6. 科研費（基盤研究（A））日本学術振興会
「データ駆動型インセンティブ工学の構築」
代表者：岩崎敦
直接経費 20,800千円・間接経費 6,240千円

7. 科研費（挑戦的研究（萌芽））日本学術振興会
「不完全情報下での逐次的意思決定：部分観測マルコフ決定過程解放の探索」
代表者：岩崎敦
直接経費 5,000千円・間接経費 1,500千円

６．今後の研究発展

メンバー間および外部研究者との研究協力をさぐりつつ，外部資金の獲得を目指す

７．発表論文等

「雑誌論文」：

G. Takatoi, T. Sugawara, K. Sakiyama, Y. Hara-Azumi, and Y. Li, “The Limits of Timing Analysis and SEMA on Distinguishing Similar Activation Functions of Embedded Deep Neural Networks,” Appl. Sci., 12(9), (2022), 査読あり,
https://doi.org/10.3390/app12094135

Y. Abe, T. Nakai, Y. Watanabe, M. Iwamoto, K. Ohta, “A Computationally Efficient Card-Based Majority Voting Protocol with Fewer Cards in the Private Model,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E106.A, Issue 3, pp.315-324 (2023), 査読あり
https://doi.org/10.1587/transfun.2022CIP0021

Y. Watanabe, T. Nakai, K. Ohara, T. Nojima, Y. Liu, M. Iwamoto, K. Ohta, “How to Make a Secure Index for Searchable Symmetric Encryption, Revisited,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E105.A, Issue 12, pp.1559-1577, (2022), 査読あり
https://doi.org/10.1587/transfun.2021EAP1163

Y. Watanabe, T.Seito, J. Shikata,
“Multi-Designated Receiver Authentication Codes: Models and Constructions,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E106.A, Issue 3, pp.394-405, (2023). 査読あり
https://doi.org/10.1587/transfun.2022TAP0015

西野上 和真, 五十嵐 瞭平, 岩崎 敦,
“私的観測下の繰り返し囚人のジレンマにおける協力のダイナミクス”, 情報処理学会論文誌, Vol.63, No.4, pp.1138-1148, (2022). 査読あり
http://doi.org/10.20729/00217615

江原 知志, 高田 哲司,
“録画による覗き見攻撃に安全な個人認証のユーザインタフェース改良による実用性向上”, 情報処理学会論文誌, Vol.63, No.4, pp.1082-1093, (2002). 査読あり
http://doi.org/10.20729/00217611

「学会発表」：

K. Asano, K. Emura, A. Takayasu, Y. Watanabe, “A Generic Construction of CCA-secure Attribute-based Encryption with Equality Test,” Int’l Conf. on Provable and Practical Security (ProvSec 2022), (2022).
https://doi.org/10.1007/978-3-031-20917-8_1

T. Kitahara, R. Hira, Y. Hara-Azumi, D. Miyahara, Y. Li, K. Sakiyama,
“Optimized Software Implementations of Ascon, Grain-128AEAD, and TinyJambu on ARM Cortex-M0,” 10th Int’l Symp. on Computing and Networking Workshops (CANDARW), pp.316-322, (2022).
https://doi.ieeecomputersociety.org/10.1109/CANDARW57323.2022.00030

Y. Komano, M. Iwamoto, K. Ohta, K. Sakiyama,
“Lightweight Authentication Using Noisy Key Derived from Physically Unclonable Function,”, 15th Int’l Conf. on Security for Information Technology and Communications (SecITC’22), (2022).
https://easychair.org/smart-program/SECITC2022/

M. Shimano, K. Sakiyama, D. Miyahara,
“Towards Verifying Physical Assumption in Card-Based Cryptography,”, 15th Int’l Conf. on Security for Information Technology and Communications (SecITC’22), (2022).
https://easychair.org/smart-program/SECITC2022/

Y. Watanabe, K. Ohara, M. Iwamoto, K.Ohta, “Efficient Dynamic Searchable Encryption with Forward Privacy under the Decent Leakage,” ACM Conf. on Data and Application Security and Privacy (CODASPY 2022), pp.312-323, (2022),
https://doi.org/10.1145/3508398.3511521

S. Shimizu, T. Nakai, Y. Watanabe, M. Iwamoto, “An Improvement of Multi-Party Private Set Intersection Based on Oblivious Programmable PRFs,” Int’l Symp. on Information Theory and Its Applications (ISITA), (2022).

A. Doi, T. Ono, T. Nakai, K. Shinagawa, T. Watanabe, K. Nuida, M. Iwamoto, ”Card-based Cryptographic Protocols for Private Set Intersection,” Int’l Symp. on Information Theory and Its Applications (ISITA), (2022).

K. Emura, R. Ito, S. Kanamori, R. Nojima, Y. Watanabe, “State-free End-to-End Encrypted Storage and Chat Systems based on Searchable Encryption,” Int’l Conf. on Enterprise Information Systems (ICEIS 2022), pp.106-113, (2022).
https://doi.org/10.5220/0011045200003179

K. Abe, M. Sakamoto, K. Toyoshima, A. Iwasaki,
“Mutation-Driven Follow the Regularized Leader for Last-Iterate Convergence in Zero-Sum Games,” 38th Conf. on Uncertainty in Artificial Intelligence (UAI 2022), 10 pages, (2022).

K. Abe, J. Komiyama, A. Iwasaki,
“Anytime Capacity Expansion in Medical Residency Match by Monte Carlo Tree Search,” Thirty-First International Joint Conference on Artificial Intelligence (IJCAI 2022), pp.3-9, (2022).
https://doi.org/10.24963/ijcai.2022/1

T. Takada, D. Schwarz, “Design Exploration for Better Security of Recognition-based Image Authentication in Mobile Environment”, Int’l Conf. on Advances in Mobile Computing and Multimedia Intelligence (MoMM 2022), pp.71-77, (Nov. 2022).
https://doi.org/10.1007/978-3-031-20436-4_7

西澤慧悟, 崎山一男, 原祐子, 李陽, “相互補助相関電力解析の正解鍵順位と鍵復元率の調査,” 2023年暗号と情報セキュリティシンポジウム (SCIS’23), 2E2-4, 7 pages, (Jan., 2023).

天野龍乃如, 崎山一男, 原祐子, 李陽, “シミュレーションによるニューラルネットワークの乗算に対するサイドチャネル攻撃の考察,” 2023年暗号と情報セキュリティシンポジウム (SCIS’23), 3E1-1, 7 pages, (Jan., 2023).

淺野 京一, 渡邉 洋平, “CCA安全な鍵更新可能公開鍵暗号の安全性解析と効率的な一般的構成法,” 2023年暗号と情報セキュリティシンポジウム (SCIS’23), 3A1-5, (Jan., 2023).

平野 貴人, 渡邉 洋平, 岩本 貢, 太田 和夫, “マルチユーザ検索可能暗号の安全性と効率性の向上”, 2023年暗号と情報セキュリティシンポジウム (SCIS’23), 3A3-4, (Jan., 2023).

嶌野雅久, 崎山一男, 宮原大輝, ” カードベース暗号における物理仮定に対する脅威とその対策に関する検討, ”コンピュータセキュリティシンポジウム (CSS’22), 8 pages, (Oct., 2022).

横山佳紀, 高田哲司, ”推測攻撃対策を意図したペア情報による個人認証手法の安全性・利便性評価：単語ペアと絵文字ペアの比較（第２報）”, コンピュータセキュリティシンポジウム(CSS’22), 8 pages, (Oct. 2022).

土井アナスタシヤ, 小野知樹, 安部 芳紀, 渡邉 洋平, 岩本 貢, “カードを用いた秘匿和集合プロトコル”, コンピュータセキュリティシンポジウム (CSS’22), (Oct. 2022).

田中健次, ”想定外事象を想定したノンテクニカルスキル融合型の信頼性・安全性方法論について”, 日本品質管理学会 第128回研究発表会、(May. 2022).

中島　淳, 大坐畠　智, 山本　嶺,
自動運転シミュレータで距離を考慮して生成したデータを用いたFederated Learningによる物体検出, IEICE RISING 2022, 京都.

「招待講演発表」：

渡邉 洋平, ”Recent Progress in Searchable Encryption,” IMI共同利用研究集会 高度化する暗号技術と数学的技法の進展, 福岡県福岡市, 2022/11/08.

「図書」：

特になし

「受賞」：

「優秀論文賞」
コンピュータセキュリティシンポジウム2022（CSS 2022），土井アナスタシヤ他・「カードを用いた秘匿和集合プロトコル」・2022年10月
https://www.uec.ac.jp/news/prize/2022/20221114_4938.html

「Best Paper Award」
16th Int'l Conf. on Provable and Practical Security（ProvSec 2022），淺野京一他，「A Generic Construction of CCA-secure Attribute-based Encryption with Equality Test」，2022年11月
https://www.uec.ac.jp/news/prize/2022/20221114_4937.html

「SCIS論文賞」
2022年暗号と情報セキュリティシンポジウム2022（SCIS 2022），阿部 芳紀他，「秘匿置換を用いた効率的なn入力多数決カードプロトコル」，2023年1月
https://www.uec.ac.jp/news/prize/2023/20230130_5117.html

「情報セキュリティ研究奨励賞」
2022年暗号と情報セキュリティシンポジウム2022（SCIS 2022），淺野京一他，「LWE仮定に基づく適応的CCA安全な平文一致確認可能IDベース暗号の効率的な構成」，2023年1月
https://www.uec.ac.jp/news/prize/2023/20230130_5117.html

「特許出願」：

特になし

「その他」：

特になし

以上.