２０１９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　　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　太田和夫
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　准教授　大坐畑智
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　岩本貢
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

＜学外構成員＞

東京工業大学　大学院情報理工学院　情報工学系　教授　小池英樹

３．２０１９年度の研究の特筆すべき成果

（１）電子情報通信学会 学術奨励賞 受賞（崎山教授）

指導学生が「レーザー光を使った音情報の漏えいに対する安全性評価」の題目で電子情報通信学会ソサイエティ大会で講演し，学術奨励賞を受賞した

－ https://www.uec.ac.jp/news/prize/2020/20200325_2475.html

（２）暗号理論に関するトップ会議である TCC (Theory of Cryptography Conference)に論文が採択された（太田教授，岩本准教授）

．修士１年生が筆頭著者であることも特筆に値する．また国内会議，研究会での受賞が２件，国際会議での best poster award が１件となった

（３）「クラウド環境における分散資源管理のためのブロックチェーン技術の適用」（大坐畑准教授）

近年、エッジクラウドコンピューティングにおいてドメインを跨いだリソースを利用する場合、互いの環境から参照することができるパブリックな環境下でリソース情報を管理する必要がある。しかし、単純にパブリックな環境で管理すればいいという問題ではなく、ホスティング環境の選定や管理者の擁立、リソース情報に基づいた利用料金の支払いなどの別の問題が生じてくる。

本研究では、リソース管理をブロックチェーンで代替することで、これらの問題点を解消する。提案方式において例として kubernetes のリソース管理の代替するにあたり必要な機能を検討し明らかにし、提案方式を設計・実装し、kubernetes 標準の etcd を用いた場合とブロックチェーンで代替した場合を比較するために実機実験を行った。

（４） 「ブロックチェーンを用いた CCN ルータに対するコンテンツ登録」（大坐畠准教授）
セコンテンツ情報の登録においてトランザクションに格納する内容の再設計を行い，登録されたコンテンツ情報を検索する手法を提案した．また Interest パケットに固有の ID を記載することで転送を行う方式を提案し，CCN プラットフォームである Cefore に実装し評価を行った．さらに実装システム上でトランザクション承認時間の分布を解析し，採掘難易度，トランザクション発行数，ブロックサイズ等のパラメータによるトランザクション承認時間等への影響を評価した．

４．２０１９年度の研究成果の公表実績

研究成果の多くは学術論文という形で公表を行なっている．詳細については項目７を参照のこと

（１） 研究会主催開催：Workshop on Cryptography Using Physical Tools,
日時：2019 年 12 月 19 日
場所：電気通信大学 東３号館 306 室
世話人：岩本准教授，渡邉助教

５．外部資金の獲得状況

（１）科研費（基盤研究(C)）「長期間運用に耐えうる共通鍵暗号による秘匿検索暗号」代表者名 太田和夫 研究分担者 岩本貢　直接経費 800 千円・間接経費 240 千円
（２）科研費(基盤研究(C))「New Paradigm to Construct Public Key Cryptographic Schemes for lightweight Devices with Provable Security against Quantum Attackers」代表者名 Santoso Bagus 研究分担者 太田和夫　直接経費 900 千円・間接経費 270 千円
（３）科研費（基盤研究(B)）「情報理論的暗号理論における統一的パラダイムの深化，発展とその応用」代表者名 四方順司 研究分担者 太田和夫，岩本貢 直接経費 4,400 千円・間接経費 1,320 千円
（４）科研費（基盤研究(S)）「暗号技術による IoT エコシステムのレジリエンス向上」代表者名 崎山一男 研究分担者 太田和夫，岩本貢　直接経費 31,100 千円・間接経費 9,330 千円
（５）科研費（基盤研究(B)）「推測秘匿性に基づく情報理論的暗号理論の新展開」 代表

者名 岩本貢　直接経費 3,400 千円・間接経費 1,020 千円

（６）科研費（挑戦的研究(萌芽)）「論理学を基にした暗号プロトコルの安全性証明と構築手法の深化」代表者名 岩本貢　直接経費 1,700 千円・間接経費 510 千円

（７）科研費（基盤研究(Ｂ)）　日本学術振興会「ゲーム理論的資源配分メカニズムの定量的評価基盤の構築」代表者名 岩崎敦　直接経費 4,300 千円・間接経費 1,290 千円

（８）科研費（基盤研究(Ａ)）「リスクモードとオンラインモニタリング技術高度化に着目した未然防止体系の新展開」代表者 鈴木和幸 研究分担者 田中健次 直接経費 7,400 千円・間接経費 2,220 千円

（９）科研費（基盤研究(Ｂ)）「想定外事象を想定した従来手法とノンテクスキルとの融合型高信頼性・安全性方法論」代表者 田中健次 直接経費 2,300 千円 間接経費 690 千円

６．今後の研究発展

現在取り組んでいるテーマを発展させ．得られた研究成果は速やかに学会等で発表を行う．

７．発表論文等

「雑誌論文」：

（１） Kazuo Sakiyama, Tatsuya Fujii, Kohei Matsuda, and Noriyuki Miura, “Flush Code Eraser: Fast Attack Response Invalidating Cryptographic Sensitive Data,” IEEE Embedded Systems Letters, 2019. (https://ieeexplore.ieee.org/document/8884144)

（２） Akiko Toh, Yang Li, Kazuo Sakiyama, Takeshi Sugawara, “Fingerprinting Light Emitting Diodes Using Spectrometer,” IET Electronics Letters, Vol.55, Issue 24, pp.1295–1297, 2019. (https://ieeexplore.ieee.org/document/8918210)

（３） Takeshi Sugawara, Natsu Shoji, Kazuo Sakiyama, Kohei Matsuda, Noriyuki Miura, and Makoto Nagata, “Side-Channel Leakage from Sensor-Based Countermeasures against Fault Injection Attack,” Microelectronics Journal, Vol. 90, pp.63-71, 2019. (https://www.sciencedirect.com/science/article/pii/S0026269218309534)

（４） K. Ohara, Y. Watanabe, M. Iwamoto, and K. Ohta, “Multi-Party Computation for Modular Exponentiation based on Replicated Secret Sharing,” IEICE Trans. on Fundamentals, vol.102-A, no.9, pp.1079 – 1090, 2019. (https://doi.org/10.1587/transfun.E102.A.1079)

（５） Kazuma Ohara, Keita Emura, Goichiro Hanaoka, Ai Ishida, Kazuo Ohta, and Yusuke Sakai,”Shortening the Libert-Peters-Yung Revocable Group Signature Scheme by Using the Random Oracle Methodology,” Special Section on Discrete Mathematics and Its Applications, IEICE Transactions, vol.102-A, no.9, pp.1101－1117, 2019.

(https://doi.org/10.1587/transfun.E102.A.1101)

（６） 平野伸将, 榎本 恵, 関根道昭, 田中健次, “高齢運転者における複数同時危険事象の認識に視覚的な注意喚起が与える影響”, ヒューマンインタフェース学会論文誌, 21/ 1, pp.111-120 (2019.4). (https://doi.org/10.11184/his.21.1_111).

（７） 田中健次, 坂東幸一, 津本周作, 佐藤直樹, “医療界でのインシデント情報を活用したリスク対応”, 横幹連合会誌「横幹」, Vol.13, No.2, pp.84-90 (2019.10).

（８） 山岸伶, 高田哲司, “推測攻撃に対する安全性改善を目的とした単語ペアの集合を秘密とする個人認証”, 情報処理学会論文誌, Vol.60, No.4, pp.1119-1128, 情報処理学会, Apr, 2019.（http://id.nii.ac.jp/1001/00195417/ ）.

（９） 皆川諒, 高田哲司, “「かわいい」画像を用いた行動誘引によるセキュリティ警告の効果改善”, 情報処理学会論文誌, Vol.61, No.3, pp.726-736, 情報処理学会, March 2020. (http://id.nii.ac.jp/1001/00204189/).（査読あり）

「学会発表」：

（１） Yang Li, Ryota Hatano, Sho Tada, Kohei Matsuda, Noriyuki Miura, Takeshi Sugawara, and Kazuo Sakiyama, “Side-Channel Leakage of Alarm Signal for a Bulk-Current-Based Laser Sensor,” *In Proc. International Conference on Information Security and Cryptology* (Inscrypt’19), LNCS 12020, Springer-Verlag, (Dec., 2019). (https://link.springer.com/chapter/10.1007%2F978-3-030-42921-8_20).

（２） Risa Yashiro, Yohei Hori, Toshihiro Katashita, and Kazuo Sakiyama, “A Deep Learning Attack Countermeasure with Intentional Noise for a PUF-based Authentication Scheme,” *In Proc. International Conference on Security for Information Technology and Communications* (SecITC’19) , LNCS, Springer-Verlag, (Nov., 2019). (https://link.springer.com/chapter/10.1007/978-3-030-41025-4_6).

（３） Hakuei Sugimoto, Ryota Hatano, Natsu Shoji, and Kazuo Sakiyama, “Validating the DFA Attack Resistance of AES (Short Paper),” *In Proc. International Symposium on Foundations & Practice of Security* (FPS’19), LNCS, Springer-Verlag, (Nov., 2019). (https://link.springer.com/chapter/10.1007/978-3-030-45371-8_25).

（４） Koichi Bando, Kenji Tanaka："Attempt to Extract Similar Cases by Applying Multilayer Perceptron to a Failure Database," *Proc. of 24th IEEE Pacific Rim International Symposium on Dependable Computing* (PRDC 2019), pp.57-58, Kyoto（2019.11）, (https://ieeexplore.ieee.org/abstract/document/8952153).

（５） Yoshiki Abe, Mitsugu Iwamoto, Kazuo Ohta, “Efficient Private PEZ Protocols for Symmetric Functions,” *Theory of Cryptography Conference* (TCC2019), pp.372–392, Dec. 2019. (https://link.springer.com/chapter/10.1007/978-3-030-36030-6_15)

（６） Yoshiki Abe, Mitsugu Iwamoto, Kazuo Ohta, “How to improve the private PEZ protocol for general functions,” *The 14th International Workshop on Security* (IWSEC2019), poster session, Aug., 2019, Tokyo.

（７） R. Eriguchi, N. Kunihiro, and M. Iwamoto,“Optimal Multiple Assignment Schemes Using Ideal Multipartite Secret Sharing Schemes,” *IEEE International Symposium on Information Theory* (ISIT2019), pp.3047–3051, 2019. (https://ieeexplore.ieee.org/abstract/document/8849591)

（８） A.Iwasaki, T.Sekiguchi, S.Yamamoto, and M.Yokoo, "Repeated Multimarket Contact with Private Monitoring: A Belief-Free Approach,", *The proceedings of the 34th AAAI Conference on Artificial Intelligence* (AAAI-2020), (Feb. 2020). (https://www.aaai.org/Papers/AAAI/2020GB/AAAI-IwasakiA.8710.pdf)

（９） 植村友紀，李陽，三浦典之，岩本貢，崎山一男，太田和夫，“鍵のランダムな漏洩に対する AES 鍵スケジュール復元アルゴリズム,” 暗号と情報セキュリティシンポジウム（SCIS）2020 予稿集, 2B1-1, 2020 年 1 月.

（１０） 竹牟禮薫，坂井祐介，Bagus Santoso，花岡悟一郎，太田和夫，“事前通信モデルにおけるペアリングを用いない集約署名,” 暗号と情報セキュリティシンポジウム（SCIS）2020 予稿集, 2A2-5, 2020.年 1 月

（１１） 品川和雅，三浦典之，岩本貢，崎山一男，太田和夫，“気泡検出器を用いたゼロ知識非破壊検査,” 暗号と情報セキュリティシンポジウム（SCIS）2020 予稿集, 2E2-3, 2020.年 1 月

（１２） 安部芳紀，岩本貢，太田和夫，“任意の始集合を持つ関数を計算する private PEZ プロトコル,” 暗号と情報セキュリティシンポジウム（SCIS）2020 予稿集, 3C1-5, 2020 年 1 月.

（１３） 安部芳紀，岩本貢，太田和夫，“任意の関数を計算する private PEZ プロトコルの改善,” コンピューターセキュリティシンポジウム 2019（CSS 2019）予稿集, 2F4-4, pp.894-901, 2019 年 10 月.

（１４） 渡邉洋平，大原一真，岩本貢，太田和夫 “(強)フォワード安全な動的検索可能暗号の効率的な構成,” コンピューターセキュリティシンポジウム 2019（CSS 2019）予稿集, 3D2-2, pp.1203-1210, 2019 年 10 月.

（１５） 坂東幸一，田中健次，「障害データベースへの機械学習適用の試み（その 3）」，第 81 回 FTC 研究会， 2019 年 7 月（茨城）

（１６） 大石雄大，高田哲司，
“機械学習による悪意ある Web ブラウザ拡張機能検出の試み: 良性/悪性の挙動の差に基づくデータを用いて”，コンピュータセキュリティシンポジウム 2019（CSS 2019），2019 年 10 月，（長崎）

（１７） 吉田光宏，高田哲司，
“画像選択から画像配置へ：操作負担に考慮した 2 段階回答による画像認証の安全性改善”，コンピュータセキュリティシンポジウム 2019（CSS 2019），2019 年 10 月，（長崎）

（１８） 吉田光宏，高田哲司，
“Pict Place Shuffle: 情報配置と間接入力による再認式画像認証の改良”，インタラクション 2020、2020 年 3 月，（東京）

「招待講演発表」：

（１） 安部芳紀, “Recent Progress on Private PEZ Protocols,” Workshop on Cryptography Using Physical Tools, 東京, 2019 年 12 月 17 日.

（２） Kazuo Ohta, “Strong Forward Privacy for Dynamic Searchable Encryption,” Seminar at Google – Searchable Encryption Talk, New York, NY, USA, Jul. 25th, 2019.

（３） Kazuo Ohta, “Card-based Majority Voting Protocols with Three Inputs Using Three Cards,” the International Secure Multi-party Computation Forum, Zhejiang, China, Jun. 1st, 2019.

「受賞」 :

（１） 電子情報通信学会ソサイエティ大会 学術奨励賞:
星野翔（Ⅱ類セキュリティ情報学4年 崎山研究室）が, 2019 年 9 月 10 日～13 日に大阪大学豊中キャンパスにて行われた電子情報通信学会ソサイエティ大会における講演において学術奨励賞を受賞. (2019/03/23)

（２） CSS2019 奨励賞:
渡邉洋平, 大原一真, 岩本貢, 太田和夫 “(強)フォワード安全な動的検索可能暗号の効率的な構成,” コンピューターセキュリティシンポジウム 2019 (CSS 2019) 予稿集, 3D2-2, pp.1203-1210, Oct. 2019

（３） IWSEC 2019 Best Poster Award:
Yoshiki Abe, Mitsugu Iwamoto, Kazuo Ohta, “How to improve the private PEZ protocol for general functions,” The 14th International Workshop on Security (IWSEC2019), poster session, Aug., 2019, Tokyo.

（４） ISEC 研究奨励賞:
安部 芳紀, 山本 翔太, 岩本 貢, 太田 和夫, “初期文字列が 29 文字の 4 入力多数決 Private PEZ プロトコル,” 電子情報通信学会情報理論・情報セキュリティ・ワイドバンドシステム合同研究会, IT2018-111, ISEC2018-117, WBS2018-112. pp. 223-228, Mar. 2019.

「特許出願」

「その他」 : ホームページ等