平成３０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．平成３０年度の研究の特筆すべき成果

（１）「レーザーフォールト攻撃に対して安全な暗号ハードウェア」（崎山教授）

レーザーフォールト攻撃に対して安全な暗号ハードウェアをセンサとの協調設計により実現し，固体素子のトップジャーナル IEEE Journal of Solid-State Circuits に論文が採択された

- https://ieeexplore.ieee.org/abstract/document/8474958

（２）「スマートコントラクトを用いたクラウド計算機資源管理のためのオフチェーン実装」（大坐畠准教授）

近年、クラウド技術が発展し、メールサーバやファイル保管、データ共有をはじめとした様々な用途に普及している。クラウドを利用することで情報資産やその保守体制を自前で持つ必要がなくなる利点があるが、データセンターとの距離によっては遅延が大きくなる問題がある。その解決策の一つとしてネットワークのエッジにもクラウド基盤を配置させるエッジクラウドコンピューティングの研究が盛んにされている。ネットワークのエッジにクラウド基盤を置くと、計算機・ネットワーク資源を提供するインフラ事業者を複数にまたがってサービスを展開することになり、リソースの管理もクラウドのような集中管理形式ではなく、分散管理の必要がある。ブロックチェーンはハッシュ関数で暗号化したブロックを利用者全員が保持

することで分散管理を可能にし、それを利用した複数のインフラ事業者にまたがったマルチドメインでのシナリオも検討されている。また、リソースの管理をするにあたってスクリプトとその実行結果を格納することができ、設定したイベントを契機に二者間の取引契約を記録できるスマートコントラクトを用いる。しかし、ブロックチェーンを扱うにあたってトランザクションが増えるほどに情報の登録に詰まりを起こすスケーラビリティの問題に直面する。そうなると手数料の高騰や登録時間の遅延が起こる。そこで、本研究では、計算機・ネットワーク資源の管理のためにブロックチェーンを用い、オフチェーンで信頼しない 2 者間での複数回の取引をサポートし、最終結果のみをチェーンに書き込むことでトランザクションの量を減らすオフチェーンの技術を導入することを提案し、その基本動作確認を行った。

（３）「かわいい効果によるセキュリティ警告改善の試み」（高田准教授）
セキュリティ警告は，その実装者が期待するほどの効果を発揮できていないという報告が多数あり，その改善が必要とされている．その改善方法として「かわいい」効果をセキュリティ警告に付与することにより，それを見た利用者から必要な行動を引き出す効果を期待しうるシステムを提案し評価を行った．その結果，警告に対して注目を引き出す効果があることが検証された．この研究結果を論文として発表し，Usable Security Workshop 2018 にて UWS 2018 論文賞を受賞した.

４．平成３０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している．詳細については項目７を参照のこと

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 1,000 千円・間接経費 300 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 5,000 千円・間接経費 1,500 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 38,800 千円・間接経費 11,640 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 3,300 千円・間接経費 990 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 1,400 千円・間接経費 420 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 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） Anjelina Espejel-Trujillo, Mitsugu Iwamoto, and Mariko Nakano-Miyatake, “A Proactive Secret Image Sharing Scheme with Resistance to Machine Learning Based Steganalysis”, Multimedia Tools And Applications, vol.77, pp. 15161–15179, 2018.（査読あり）

（２） Yohei Watanabe, Yoshihisa Kuroki, Shinnosuke Suzuki, Yuta Koga, Mitsugu Iwamoto, Kazuo Ohta “Card-Based Majority Voting Protocols with Three Inputs Using Three Cards”, Proc. International Symposium on Information Theory and Its Applications (ISITA2018), pp. 218-222, 2018.（査読あり）

（３） Takeshi Sugawara, Kazuo Sakiyama, Shoei Nashimoto, Daisuke Suzuki, Tomoyuki Nagatsuka, “Oscillator without a Combinatorial Loop and its Threat to FPGA in Data Center,” IET Electronics Letters, (accepted, 2019).（査読あり）

（４） Takeshi Sugawara, Yang Li, and Kazuo Sakiyama, “Probing Attack of Share-Serial Threshold Implementation of AES,” IET Electronics Letters, (accepted, 2019).（査読あり）

（５） Yuichi Komano, Kazuo Ohta, Kazuo Sakiyama, Mitsugu Iwamoto, and Ingrid Verbauwhede, “Single-Round Pattern Matching Key Generation Using Physically Unclonable Function,” Security and Communication Networks, vol. 2019, Article ID 1719585, 13 pages, (Jan., 2019).（査読あり）

（６） Kohei Matsuda, Tatsuya Fujii, Natsu Shoji, Takeshi Sugawara, Kazuo Sakiyama, Yu-ichi Hayashi, Makoto Nagata, and Noriyuki Miura,
“A 286 F2/Cell Distributed Bulk-Current Sensor and Secure Flush Code Eraser against Laser Fault Injection Attack on Cryptographic Processor,” IEEE Journal of Solid-State Circuits, Vol.53, No.11, pp. 3174-3182, (Nov., 2018).（査読あり）

（７） Yang Li, Momoka Kasuya, and Kazuo Sakiyama,
“Comprehensive Evaluation on an ID-Based Side-Channel Authentication with FPGA-Based AES,” Appl. Sci. 2018, 8(10), 1898, (Oct., 2018).（査読あり）

（８） Suguru Ueda, Atsushi Iwasaki, Vincent Conitzer, Naoki Ohta, Yuko Sakurai, Makoto Yokoo:
“Coalition structure generation in cooperative games with compact representations”. Autonomous Agents and Multi-Agent Systems 32(4): 503-533 (2018)（査読あり）

（９） Kota Shigedomi, Tadashi Sekiguchi, Atsushi Iwasaki, Makoto Yokoo:
“Repeated Triangular Trade: Sustaining Circular Cooperation with Observation Errors”. PRIMA 2018: pp.242-257, Oct. 2018,（査読あり）

「学会発表」：

（１） Natsu Shoji, Takeshi Sugawara, Mitsugu Iwamoto and Kazuo Sakiyama, “An Abstraction Model for 1-bit Probing Attack on Block Ciphers,” In Proc. International Conference on Computer and Communication Systems (ICCCS’19), IEEE, (Feb., 2019)

（２） Ryuga Matsumura, Takeshi Sugawara, and Kazuo Sakiyama, “A Secure LiDAR with Side-channel Fingerprinting,” In Proc. International Symposium on Computing and Networking, CANDAR Workshops (CANDARW’18), IEEE, pp.479-482, (Aug., 2018)

（３） Jean-Luc Danger, Risa Yashiro, Tarik Graba, Sylvain Guilley, Yves Mathieu, Noriyuki Miura, Abdelmalek Si-Merabet, Kazuo Sakiyama, and Makoto Nagata, “Analysis of Mixed PUF-TRNG Circuit Based on SR-Latches in FD-SOI Technology,” In Proc. Euromicro Conference on Digital System Design (DSD’18), IEEE, pp.508-515, (Aug., 2018)

（４） Shoei Nashimoto, Daisuke Suzuki, Takeshi Sugawara, Kazuo Sakiyama,”Sensor CON-Fusion: Defeating Kalman Filter in Signal Injection Attack,” In Proc. Asia Conference on Computer and Communications Security (AsiaCCS’18), ACM, pp.511-524, (Jun., 2018)

（５） Tetsuji Takada, Takaaki Abe,“Emoji-nized Log Browser: Visualization of Server-logs by Emoji for System Administrators”, Int’l Conf. on Advanced Visual Interface (AVI 2018), May 2018,

（６） Rei Yamagishi, Tetsuji Takada,“AssociPass: A User Authentication System with Word-Pairs for Security against Guess Attack”, CHI’18 EA, (CHI’18), Apr, 2018.

（７） 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, 発表日：2019 年 3 月 8 日, 場所：電気通信大学

（８） 渡邉洋平, 岩本貢, 太田 和夫
“効率的でフォワード安全な動的検索可能暗号”, 暗号と情報セキュリティシンポジウム (SCIS2019), 発表日：2019 年 1 月 24 日, 場所：びわ湖大津プリンスホテル

（９） 安部 芳紀, 山本 翔太, 岩本 貢, 太田 和夫
“不正検知可能な 3 入力多数決カードプロトコル”, 暗号と情報セキュリティシンポジウム (SCIS2019), 発表日：2019 年 1 月 24 日, 場所：びわ湖大津プリンスホテル

（１０） 山本 翔太, 安部 芳紀, 岩本 貢, 太田 和夫
“4 入力多数決を計算する効率的な Private PEZ プロトコル”, 暗号と情報セキュリティシンポジウム (SCIS2019), 発表日：2019 年 1 月 24 日, 場所：びわ湖大津プリンスホテル

（１１） 平野 貴人, 川合 豊, 小関 義博, 岩本 貢, 太田 和夫
“共通鍵型マルチユーザ検索可能暗号の検索機能拡張”, 暗号と情報セキュリティシンポジウム (SCIS2019), 発表日：2019 年 1 月 24 日, 場所：びわ湖大津プリンスホテル

（１２） Wenjia Wang, Yoshiki Abe, Mitsugu Iwamoto, and Kazuo Ohta,
“Three-Party Private Set Operation Protocols Using Polynomials and OPPRF”, 暗号と情報セキュリティシンポジウム (SCIS2019), 発表日：2019 年 1 月 23 日, 場所：びわ湖大津プリンスホテル

（１３） 江利口礼央, 國廣昇, 岩本貢
“いくつかの理想的な秘密分散法を用いた最適な複数割り当て法”, 情報理論とその応用シンポジウム (SITA2018), 発表日：2018 年 12 月 20 日, 場所：ホテルハワイアンズ

（１４） 渡邉洋平, 大原一真, 岩本貢, 太田和夫,
“現実的な結託者のもとで最もシェア長の短いロバスト秘密 分散法,”, 電子情報通信学会情報セキュリティ研究会, ISEC2018-7, 2018, 発表日：2018 年 7 月 25 日, 場所：札幌コンベンションセンター

（１５） 多賀野亮太, 田中健次:
“自動運転におけるドライバの安心感抑制による注意力向上への効果”, 計測自動制御学会 第 46 回知能システムシンポジウム、2019 年 3 月 7 日, 龍谷大学(滋賀)

（１６） 鶴飼純一郎, 田中健次:“あいまいな情報提示によるドライバ の過信軽減への効果”, 計測自動制御学会 第 46 回知能システムシンポジウム、2019 年 3 月 7 日, 龍谷大学(滋賀)

（１７） 大澤隆人, 大坐畠智, 山本嶺, 加藤聰彦,
“クラウド計算機資源管理のためのスマートコントラクトを用いたオフチェーン実装の検討”, 信学技報, Vol. 118, No. 466, pp. 61-65, 2019 年 3 月 4 日.(沖縄)

（１８） 皆川諒, 高田哲司, “「かわいい」はセキュリティ警告の効果を改善しうるか？（第2報）～心理効果による安全行動誘引の試み～”, コンピュータセキュリティシンポジウム 2018 (CSS2018), 2018 年 10 月, (長野)

「招待講演発表」：

（１） 太田和夫，“現代暗号研究の事始め ～ １つのケーススタディ ～”，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，発表年月日：2019 年 3 月 8 日，場所：電気通信大学

（２） 岩本貢，“秘密計算の安全性～プライバシーを保ちつつどこまで計算できるか”，第 8 回バイオメトリクスと認識・認証シンポジウム（SBRA），発表年月日：2018 年 11 月 20 日，場所：KDDI 飯田橋駅前ビル

（３） Kazuo Sakiyama, “Anti-tamper cryptographic hardware with analog electronics,” Mini Symposium: Crypto for long-term security and privacy (Mar., 22, 2019), The Netherlands.

（４） Kazuo Sakiyama, “Keynote: Towards Resilient IoT System – How to Evaluate Information Leakage,” The First International Workshop on Hardware Oriented Cybersecurity (HwSec2018), (Dec., 19, 2018), Vietnam.

（５） Kazuo Sakiyama, “Keynote: Hardware Security and IoT Ecosystem,” International Conference on Advanced Computing and Applications (ACOMP 2018), (Nov., 28, 2018), Vietnam.

（６） Kazuo Sakiyama, “Hardware Implementations of ECC,” Autumn school, 22nd Workshop on Elliptic Curve Cryptography, (2018 年 11 月 17 日), Japan.

「図書」：

「受賞」：

（１） 羽田野凌太さん(総合情報学科 4 年)が，2018 年 9 月 11～14 日に金沢大学 角間キャンパスで開催されたソサイエティ大会で発表した論文に対し，学術奨励賞を受賞．(2019/03/21)
– https://www.uec.ac.jp/news/prize/2019/20190322_1727.html

（２） 羽田野凌太さん（総合情報学科 4 年）が，CODE BLUE CTF の貢献に対して，感謝状贈呈．(2018/12/04)
– https://www.uec.ac.jp/news/prize/2018/20181204_1484.html

（３） 服部夢二君（情報学専攻2年）が，第80回 CSEC 研究会で行った「安全な秘密情報利用の動機付けを目的とした個人認証のゲーム化」という研究発表に対して CSEC 優秀研究賞を受賞 (2018/10/24)
– http://www.ipsj.or.jp/award/csec-award.html

（４） 皆川諒君（情報学専攻２年）が，論文「「かわいい」はセキュリティ警告の効果を改善しうるか？（第２報）～心理効果による安全行動誘引の試み～」に対して UWS2018 論文賞を受賞（2018/10/24）
- http://www.iwsec.org/uws/2018/

（５） 市野研究室、高田研究室、吉浦研究室（情報学専攻）と NTT コミュニケーションズの合同チーム「UN 頼み」が MWSCup 2018 にて当日課題優勝および総合優勝 を受賞（2018/10/24）
- http://www.iwsec.org/mws/2018/photo.html

（６） 2018/09/05 辰巳恵里奈さん（情報学専攻修士 1 年）が，2018 年 9 月 3 日～9 月 5 日に東北大学　片平さくらホールで開催された The 13th International Workshop on Security（IWSEC 2018）にて Best Poster Award を受賞（2018/09/05）
- http://www.ipsj.or.jp/award/iwsec-award3.html

「特許出願」：

（１） ″動的検索可能暗号処理システム及び動的検索可能暗号処理方法，″ 渡邉洋平，岩本貢，太田和夫，特願 2019-3908，（出願日：平成 31 年 1 月 11 日）

「その他」：ホームページ等