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．設置期間

２０２１年０４月０１日　～　２０２６年０３月３１日

３．研究組織(設置期間中かかわった、全ての構成員を記載してください。)

※所属機関・部局・職は現在のもの、もしくは離脱時のものを記して下さい。

＜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	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	岩崎 敦
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
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　情報理工学院　情報工学系　教授　小池 英樹

４．研究の特筆すべき成果

（研究の主な成果、得られた成果の国内外における位置づけとインパクト、今後の展望などの点から記述すること）

成果１）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を用いたルーティングプロトコルの実現。

従来の ICN（Information Centric Network）では，ルータは受信した Interest に対しそれが要求するコンテンツ名を既知としてルーティングを行ってきた．しかし，そのコンテンツ情報をユーザがどのように取得・把握し，そのコンテンツ要求を行う Interest が発行されてどのように Interest のルーティングが行われるかという，コンテンツ管理とルーティングとを組み合わせて通信を行う手法について検討がなされていない．

そこで本研究では，CCN におけるブロックチェーンを用いたリンクステート型ルーティング手法を提案する．本提案手法は，コンテンツ情報をブロックチェーン上に登録することにより，ユーザが CCN 上のコンテンツを把握し，そのコンテンツに対しルーティングを行うことでコンテンツを取得する．また，これらのコンテンツ情報はそれぞれ配信権利も含めてブロックチェーン上で管理することで，その流通管理も可能としている．さらに，ブロックチェーンを用いたコンテンツ管理に基づき FIB の冗長なエントリを削除することができるため，従来手法と比較し FIB サイズを削減している．この提案手法を設計し，CCN プラットフォーム Cefore に実装し，性能評価をした．

５．研究成果の公表実績

（主催した研究会・シンポジウム、研究成果の発信状況等）

1. 岩本教授が国際会議 IEEE ITW 2021（2021 年 10 月 17～21 日開催，https://www.itw2021.org/ の Technical Program Co-Chair を務めた

2. 渡邉助教が国際会議 PKC 2022（2022 年 3 月 8～11 日開催，https://pkc.iacr.org/2022/ の General Co-Chair を務めた

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「発表論文」を参照頂きたい．

６．外部資金の獲得状況

（代表的な資金獲得１０件以内）

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
「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 7,600 千円・間接経費 2,280 千円
3. 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

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（挑戦的研究（萌芽））日本学術振興会
「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：岩本貢　直接経費 4,900 千円・間接経費 1,470 千円
6. 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
7. 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
8. 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

７．発表論文等（各項目とも、代表的な５件以内）

「雑誌論文」：

Go TAKAMI and Takeshi SUGAWARA and Kazuo SAKIYAMA and Yang LI,
"Mixture-Based 5-Round Physical Attack against AES: Attack Proposal and Noise Evaluation",
IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E105.A, Issue 3, (2021)
https://doi.org/10.1587/transfun.2021CIP0016

K. Emura, J.H.Seo, and Y. Watanabe,
“Efficient revocable identity-based encryption with short public parameters”,
Theoretical Computer Science, Vol. 863, pp.127-155, (2021.04).
https://doi.org/10.1016/j.tcs.2021.02.024

K. Emura, A. Takayasu, and Y. Watanabe,
”Efficient identity-based encryption with Hierarchical key-insulation from HIBE”,
Designs, Codes and Cryptography, Vol. 89, pp.2397—2431, (2021).
https://doi.org/10.1007/s10623-021-00926-z

K. Emura, S.Katsumata, Y.Watanabe,
“Identity-based encryption with security against the KGC: A formal model and its instantiations”,
Theoretical Computer Science, Vol.900, pp.97-119, (2022.01).
https://doi.org/10.1016/j.tcs.2021.11.021

K. Emura, A. Takayasu, Y. Watanabe,
” Adaptively secure revocable hierarchical IBE from *k*-linear assumption”,
Design, Codes and Cryptography, 89, pp.1535—1574, (2021).
https://doi.org/10.1007/s10623-021-00880-w

「学会発表」：

S. Tokunaga, S. Ohzahata and R. Yamamoto, "A Link State Routing Method for CCN with Blockchain," 2021 Ninth International Symposium on Computing and Networking Workshops (CANDARW), 2021, pp. 49-55, (2021.11.26)

Y.Ishigaki, K. Tanaka,
“Smartphone Solutions for Citizen-Centered Risk Monitoring in Environmental Disaster Situations”,
Digital Services in Crisis, Disaster, and Emergency Situations, IGI Global, 2021, pp. 1-30. https://doi.org/10.4018/978-1-7998-6705-0.ch001

Tetsuji Takada and Mitsuhiro Yoshida,
” Pict-Place Authentication: Recognition-based Graphical Password using Image Layout for Better Balance of Security and Operation Time”,
14th Biannual Conf. of the Italian SIGCHI chapter, (2021.07),

浅野 京一, 岩本 貢, 渡邉 洋平,
“秘密鍵の漏洩耐性を有する鍵隔離暗号”,
コンピュータセキュリティシンポジウム (CSS 2021), pp.997-1004, (2021.10)

五十嵐瞭平，岩崎敦，
“ほぼ公的観測下の囚人のジレンマにおける協力のダイナミクス”，
第２０回情報科学技術フォーラム（FIT 2021），(2021.08)，情報処理学会

「受賞」：

「FIT 論文賞」
授与団体：第 20 回情報科学技術フォーラム FIT2021
受賞者：五十嵐 瞭平 ，岩崎敦
受賞論文：「ほぼ公的観測下の囚人のジレンマにおける協力のダイナミクス」
受賞年月日： ２０２１年０９月
https://www.ipsj.or.jp/award/fit_ronbun.html

「船井ベストペーパ賞」
授与団体：第 20 回情報科学技術フォーラム FIT2021
受賞者：坂本充生， 阿部拳之， 岩崎敦
受賞論文：見間違えのある繰り返し囚人のジレンマにおける方策勾配法に関する研究
受賞年月日：２０２１年０９月
https://www.ipsj.or.jp/award/funai_best-paper.html

以上．