平成２６年度研究ステーション研究成果報告書

※学科・専攻を超えた、或いは研究室の枠を超えた複数のメンバーによる組織的な研究活動について記載してください

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）　総合情報学専攻　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　総合情報学専攻 教授 太田和夫

電気通信大学 大学院情報システム学研究科　社会知能情報学専攻 教授 田中健次

電気通信大学 大学院情報理工学研究科　総合情報学専攻 教授 崎山一男

電気通信大学 先端領域教育研究センター　特任准教授 岩本貢

電気通信大学 大学院情報システム学研究科 情報ネットワークシステム学専攻 准教授 大坐畠智

電気通信大学 大学院情報理工学研究科　総合情報学専攻 准教授 高田哲司

＜学外構成員＞

東京工業大学　大学院情報理工学研究科　計算工学専攻　教授 小池英樹

３．平成２６年度の研究の特筆すべき成果

・ID 情報を秘匿したまま認証が可能なパッシブ型 RFID タグチップの試作に成功

プレスリリース：日経産業新聞ほか 4 件、Web での情報公開 3 件

・Tor ネットワークにける通信品質改善方式の提案とその有用性検証

ネットワーク通信におけるプライバシー保護技術 Tor の性能改善方法を提案し、その実現可能性と有用性について評価を実施した.

４．平成２６年度の研究成果の公表実績

・平成２７年２月２３日 – IS シンポジウム第 19 回「信頼性とシステム安全学」開催

於:電通大 参加者４６名

５．外部資金の獲得状況

（種別・種目・相手機関(企業)・研究題目・代表者名・直接経費額・間接経費額）

1. 科研費（基盤研究(A)）日本学術振興会「次世代品質・信頼性情報システムの研究と開発」代表者名 鈴木和幸 直接経費 900 千円(分担分)
2. 科研費（基盤研究(A)）日本学術振興会「暗号ＶＬＳＩの電磁波セキュリティを確保するサイドチャネル攻撃センサの構成法と実証」代表者 永田真 直接経費 15210 千円、間接経費 3510 千円
3. 科研費（基盤研究(C)）日本学術振興会「情報理論的安全性をもつマルチキャスト通信の構築とその安全性解析」代表者 岩本貢 直接経費 1200 千円、間接経費 360 千円
4. 科研費（挑戦的萌芽）日本学術振興会「利用状況に応じた携帯端末向け個人認証の研

究」代表者 高田哲司 直接経費 900 千円、間接経費 270 千円

６．今後の研究発展

・ レーザーフォールト攻撃対策の研究を発展させ、科研費 基盤(A)の獲得を目指す

・ 当研究ステーションの Web ページを作成する

７．発表論文等（各項目ごとに記載してください。）

「雑誌論文」：

・ Kurihashi, S., Matsuno,Y., Tanaka, K.: “Enhancing Safety with a Mutual Assistance System for Automobile", SICE Journal of Control, Measurement, and System Integration, Vol.8, No.2, (2015) pp.161-170 査読有

・ Sho Endo, Yang Li, Naofumi Homma, Kazuo Sakiyama, Kazuo Ohta, Daisuke Fujimoto, Makoto Nagata, Toshihiro Katashita, Jean-Luc Danger, and Takafumi Aoki, “A Silicon-level Countermeasure against Fault Sensitivity Analysis and Its Evaluation,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., (in press).

・ Dai Yamamoto, Kazuo Sakiyama, Mitsugu Iwamoto, Kazuo Ohta, Masahiko, Takenaka, Kouichi Itoh, and Naoya Torii, “A new method for enhancing variety and maintaining reliability of PUF responses and its evaluation on ASICs Journal of Cryptographic Engineering,” J. Cryptographic Engineering, (in press).

・ 中曽根俊貴，李陽，岩本貢，太田和夫，﨑山一男，“クロック間衝突を漏洩モデルとする新たなサイドチャネル解析と並列実装 AES 暗号ハードウェアにおける弱い鍵，” 電子情報通信学会論文誌(A)，Vol.J97-A，No.11，pp.695-703，Nov.,2014.

・ Tetsuji Takada, Yuki Kokubun, “MTAPIN: multi-touch key input enhances security of PIN authentication while keeping usability”, Int’l Journal of Pervasive Computing and Communications, Vol.10, Iss.3, (2014), pp.276-290.

「学会発表」：

・Kadota, Y., Tanaka, K. : “The proposed technique of looking down the product safety level of safety standards and accident information,” Proc. of Int’l Conf. on Quality 2014, pp.930-939 (2014.11) Tokyo

・T. Nishide, M. Iwamoto, A. Iwasaki, and K. Ohta, “Secure (M+1)st-Price Auction with Automatic Tie-Break,” The 6th International Conference on Trustworthy Systems (InTrust2014), 2014-12-17, China.

・Timothy Girry Kale, Satoshi Ohzahata, Celimuge Wu, and Toshihiko Kato, “A Circuit Switching Method for Improving Congestion of Tor Network”, Proc. of the 16-th Int’l Symp. on Multimedia Network Systems and Applications (MNSA-2014), 6 pages, 2014. (China)

・Timothy Girry Kale, Satoshi Ohzahata, Celimuge Wu, and Toshihiko Kato, “Analyzing the Drawbacks of Node-Based Delays in Tor”, Proc. of CQR 2014, 6 pages, 2014.（U.S.A.）

・Takanori Machida, Dai Yamamoto, Mitsugu Iwamoto, and Kazuo Sakiyama, “Implementation of Double Arbiter PUF and Its Performance Evaluation on FPGA,” 20th Asia

and South Pacific Design Automation Conference (ASP-DAC2015), pp.6-7, (Jan., 2015). (Japan)

・Yang Li, Shugo Mikami, Dai Watanabe, Kazuo Ohta, and Kazuo Sakiyama, “Single-Chip Implementation and Evaluation of Passive UHF RFID Tag with Hash-Based Mutual Authentication,” In Proc. Workshop on RFID Security (RFIDsec’14 Asia), IOS Press, pp.3-15, (Nov., 2014). (Taiwan)

・ M. Iwamoto, T. Omino, Y. Komano, and K. Ohta, “A New Model of Client–Server Communications under Information Theoretic Security,”, IEEE Information Theory Workshop (ITW2014), pp. 512–516, November 5th, 2014. (Australia)

・ P. Lumyong, M. Iwamoto, and K. Ohta, “Cheating on a Visual Secret Sharing Scheme under a Realistic Scenario,” International Symposium on Information Theory and Its Applications (ISITA2014), pp. 546–550, October 29th, 2014. (Australia)

M. Iwamoto and J. Shikata, “Secret Sharing Schemes Based on Min-entropies,” IEEE Int’l Symp. on Information Theory (ISIT2014), pp.401–405, 2014. (USA)

・ K. Ohara, Y. Sakai, F. Yoshida, M. Iwamoto, and K. Ohta, “Privacy-Preserving Smart Metering with Verifiability for Both Billing and Energy Management,” The 2nd ACM ASIA Public-Key Cryptography Workshop (ASIAPKC2014), pp. 23–32, 2014. (Japan)

「招待講演発表」：

・ Kazuo Sakiyama, “Fault Analysis for Cryptosystems: Introduction to Differential Fault Analysis and Fault Sensitivity Analysis,” Tutorial-4: Hardware Trust in VLSI Design and Implementations, Asia and South Pacific Design Automation Conference (ASP-DAC’15), Tutorial Session, (Jan., 2015).

「図書」：

・ 田中健次・朝倉書店・「システムの信頼性と安全性」・(2014 年)、212 頁

「特許出願」：

・ 認証システム及び認証方法, 崎山一男, 李陽, 出願番号:PCT/JP2015/52576, 2015/1/29

「その他」：

・ 「ID 情報を秘匿したまま認証が可能なパッシブ型 RFID タグチップの試作に成功」企業情報、ニュースリリース, - http://www.hitachi.co.jp/New/cnews/month/2014/09/0904a.html