平成２５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　　情報メディアシステム学専攻　教授　小池　英樹

２．研究組織

＜学内構成員＞

電気通信大学　大学院情報システム学研究科 情報ﾒﾃﾞｨｱｼｽﾃﾑ学専攻　教授　小池英樹
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　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

３．平成２５年度の研究の特筆すべき成果

- 相互認証 IC チップの試作
- 日本信頼性学会 2012 年度優秀記事コラム賞受賞 (2013.06.12 受賞)
- 匿名通信 Tor ネットワークを介した通信は，スループットが出ないことが知られているが、その詳細分析は不十分であった。そこで測定用のノードを実際の Tor ネットワークに参加させ、どこで遅延が起きているのかを分析した
- 暗証番号認証においてその入力方法をタッチパネルの応用により拡張し、利用者への負担を最小限にしつつ、安全性を改善する認証手法を開発した
- スマートフォンを対象とし，その振動機能を応用することにより第三者に認証行為を録画されても入力した値が漏えいしない認証方法を開発した

４．平成２５年度の研究成果の公表実績

IS シンポジウム 第 18 回 「信頼性とシステム安全学」 平成 26 年 2 月 27 日 参加者数 48 名

５．外部資金の獲得状況

1. 株式会社 富士通研究所、「暗号デバイスのセキュリティ脅威に関する研究」、太田和夫(分担者) 500,000 円

2. 株式会社 東芝研究開発センター、「長期安全性を実現する効率的な暗号基盤技術の開発」、太田和夫(分担者) 715,000 円

3. 三菱電機株式会社、「ハッシュ関数および秘匿検索暗号の理論研究」、太田和夫(分担者) 500,000 円

4. 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、900,000 円

６．今後の研究発展

- 相互認証 IC チップの性能と安全性評価
- 社会学的検知から信頼性と安全性に関する研究を行う
- 匿名通信 Tor ネットワークの輻輳を回避する仕組みを解明する
- 個人認証における安全性と利便性の両立に向けた研究を行う

７．発表論文等

「雑誌論文」：Kazuo Sakiyama, Yang Li, Shigeto Gomisawa, Yu-ichi Hayashi, Mitsugu Iwamoto, Naofumi Homma, Takafumi Aoki, and Kazuo Ohta, “Practical DFA Strategy for AES Under Limited-Access Conditions,” Journal of Information Processing, Vol.55, No.2, (Feb., 2014).

「雑誌論文」：Dai Yamamoto, Kazuo Sakiyama, Mitsugu Iwamoto, Kazuo Ohta, Masahiko Takenaka, and Kouichi Itoh, “Variety Enhancement of PUF Responses Using the Locations of Random Outputting RS Latches,” J. Cryptographic Engineering, Vol.3(4), pp.197-211, (Nov., 2013).

「雑誌論文」：Ishigaki, Y., Matsumoto, Y., Ichimiya, R., Tanaka, K.：”Development of Mobile Radiation Monitoring System Utilizing Smartphone and Its Field Tests in Fukushima,” *IEEE Sensors Journal,* Vol.13, No.10, pp.3520-3526 (2013.10).

「雑誌論文」：田中健次：「安全対策の落とし穴-その仕組みと仕掛け」, 患者安全 推進ジャーナル, No.32, pp.17-32 (2013.7)

「学会発表」：Yu Sasaki, Yuuki Tokushige, Lei Wang, Mitsugu Iwamoto, and Kazuo Ohta, “An Automated Evaluation Tool for Improved Rebound Attack: New ShiftBytes Parameters for Grøstl,” Proc. of CT-RSA2014, LNCS8366, pp.424-443, Feb., 2014.

「学会発表」：Shugo Mikami, Dai Watanabe, and Kazuo Sakiyama, “A Comparative Study of Stream Ciphers and Hash Functions for RFID Authentications,” In Proc. The 2013 Workshop on RFID and IoT Security (RFIDsec’13 Asia), IOS Press, pp.83-94, (Nov., 2013).

「学会発表」:Yang Li, Yu-ichi Hayashi, Arisa Matsubara, Naofumi Homma, Takafumi Aoki, Kazuo Ohta and Kazuo Sakiyama, “Yet Another Fault-Based Leakage in Non-Uniform Faulty Ciphertexts,” In Proc. The Sixth International Symposium on Foundations & Practice of Security (FPS’13), LNCS, Springer-Verlag, (Oct., 2013).

「学会発表」：Toshiki Nakasone, Kazuo Sakiyama, Yang Li, and Kazuo Ohta, “Exploration of the CC-EMA Attack Towards Efficient Evaluation of EM Information Leakage,” In Proc. International Symposium on Electromagnetic Compatibility (EMC EUROPE) 2013, IEEE, pp.411-414,(Sep., 2013).

「学会発表」：Timothy Girry Kale, Satoshi Ohzahata, Celimuge Wu, and Toshihiko Kato, “Effectiveness of Performance Flag Selection for Enhancing the Tor Circuit”,Proc. of APNOMS 2013, 3 pages, 2013 (Poster session)

「学会発表」：Timothy Girry Kale, Satoshi Ohzahata, Celimuge Wu, and Toshihiko Kato、”Analyzing the Drawbacks of Node-Based Delays in Tor”、CQR 2014、2014

「学会発表」：Tetsuji TAKADA and Yuki KOKUBUN、”Extended PIN Authentication Scheme Allowing Multi-touch Key Input”、Proc. of Advances in Mobile Computing & Multimedia (MoMM 2013)、2013, Austria.

「学会発表」：Hayate Goto and Tetsuji Takada、”Visual Anomaly Detection of Network Connections in a Personal Computer”、IEEE Pacific Visualization 2014、Mar 2014、横浜

「学会発表」：石塚正也, 高田哲司、”振動機能を応用した携帯端末での個人認証における覗き見攻撃対策手法”、コンピュータセキュリティシンポジウム 2013、Oct 2013、高松

「学会発表」：尼子雄大、高田哲司、”情報視覚化による DBD(Drive-by Downlaod)攻撃対策の一検討”、情報処理学会 CSEC 研究会、Mar 2014、東京

「受賞」：日本信頼性学会、坂東幸一(田中教授)、2012 年度優秀記事コラム賞受賞 2013/06/12,

「受賞」：電子情報通信学会 NS 研究会、Timorhy Girry Kale(大坐畠准教授), 第 1 回 英語セッション奨励賞, 2013, http://www.ieice.org/cs/ns/jpn/awards.html

「受賞」：情報処理学会 インタラクション 2014、石塚正也(高田准教授)、インタラクティブ発表賞, 2014/02/28、http://www.interaction-ipsj.org/2014/program.html

「特許出願」：入力支援プログラム、入力支援方法および情報処理装置、石塚正也, 高田哲司、特願 2014-055942、2014/03/19、国内

「その他」：ホームページ等