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）　総合情報学専攻 准教授 高田哲司

２．設置期間

平成２３年０４月０１日　～　平成２８年０３月３１日

３．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 大学院情報理工学研究科	総合情報学専攻	教授 吉浦裕 （～平成 24 年 3 月 31 日）
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 大学院情報理工学研究科	総合情報学専攻	准教授 岩本貢 （平成 27 年 5 月 1 日～）
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 大座畠智
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	准教授 岩崎敦 （平成 27 年 8 月 1 日～）
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 （平成 23 年 4 月 1 日～）

＜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

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）

- P2P ファイル交換システムにおいてファイル流通制御を実現する方式を開発，情報漏洩対策の可能性を模索し

た

- 匿名通信 Tor ネットワークにおける中継ノード選択方式及びスループット改善を目的とした通信遅延分析(通信品質・性能改善)の研究を行った．原因が Tor ルータ内のバッファにあることを特定し，改善方法として輻輳の発生しているルートを特定し，ルートを切り替える手法を提案した
- Social Network Service(SNS)における個人情報漏洩について推定可能性に関わる研究を行った
- 人間の作業やヒューマンエラーを防ぐための安全対策に潜む落とし穴を明らかにし，その防止のためのトータルセキュリティ・マネジメントについて研究を行い，特に人間がエラーしやすいグレイゾーンを考慮した安全保証と危機回避について研究を行った
- インターネットコンテンツからの個人情報の漏洩検知と防止技術，データベース保護技術，Web なりすまし検知技術について研究を行った
- 利便性と安全性のより良いバランスを目指した新たな個人認証技術について研究を行った
- 携帯端末における状況依存の脅威に対して安全性を確保しうる個人認証の研究を行った．
  - 端末の振動機能を応用した，録画攻撃に対する秘密情報の漏洩を防ぎうる，暗証番号入力手法の開発．
  - 1つの秘密情報で複数の確率的安全性を提供しうる画像を用いた個人認証の　提案．
- 不正行為者の行動分析のための囮システム「ハニーポット」の国際アライアンス The Honeynet Project(http://www.honeynet.org/)に参画し，不正アクセス手法に関する情報交換を行った
- 認証 IC チップの実装と安全性の実証に関わる研究を行った
- ID 情報を秘匿に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した
- 政府関係会議に委員として参加し，セキュリティ対策に関する貢献を行った
  - 経済産業省「コンピュータセキュリティ早期警戒態勢整備委員会」
  - 経済産業省「新世代情報セキュリティ対策委員会」
  - 経済産業省「ボット対策委員会」
- 報理論的暗号分野において，近年議論が活発な「推測確率による安全性」に関する基本的な結果を得た．特に，共通鍵暗号における，推測確率の平均値・最悪値による安全性規準と，通常の完全秘匿性との関係を明確化したことは，このテーマの最も基礎的な成果の一つになると考える．
- 無線 LAN における利己的な端末の生成するトラヒックの制御に関する研究：無線 LAN の課題として，送信機会の確保がある．送信機会は決められたカテゴリーに応じて行われ，優先度制御が行われるが，不適切な設定により利己的な端末が存在すると適切な設定の端末に送信機会が得られなくなる問題がある．そこで既存の提案を改善し，Access Point が利己的な端末から送信権を奪い返す仕組みを導入し，その有効性を明らかにした．

５．研究成果の公表実績

- 第 16 回「信頼性とシステム安全学シンポジウム」,平成 24 年 2 月 28 日，参加者数 81 名
- 第 17 回「信頼性とシステム安全学シンポジウム」,平成 25 年 2 月 28 日，参加者数 66 名
- 日経産業新聞(1 月 16 日，6 面)「情通機構など　物理的特性使い　IC チップ暗号化」
- 化学工業日報(1 月 16 日，8 面)「M2M 用暗号・認証 IC チップの安全性実証　NICT など　実装コ

ストも削減」

- 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
- IS シンポジウム 第 19 回「信頼性とシステム安全学」, 平成 27 年 2 月 23 日, 於:電気通信大学, 参加者数 46 名
- IS シンポジウム 第 20 回「信頼性とシステム安全学」, 平成 28 年 3 月 01 日, 於:電気通信大学, 参加者数 47 名
- 「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, 日立製作所 ニュースリリース(2014 年 9 月 4 日),
  - http://www.hitachi.co.jp/New/cnews/month/2014/09/0904a.html

６．外部資金の獲得状況

1) 科研費(基盤研究(C)) 日本学術振興会「プライバシー保護のための個人情報の検知および照合技術の研究」
代表者名 吉浦裕 直接経費 3,900,000 円・間接経費 1,170,000 円

2) 科研費(基盤研究(B)) 「グレイゾーンでの判断能力向上を目指したリスクマネジメント論の体系化」
代表者名 田中健次 直接経費 5,300,000 円・間接経費 1,590,000 円

3) 科研費(基盤研究(A)) 「次世代品質・信頼性情報システムの研究と開発」
代表者 鈴木和幸 直接経費 36,000,000 円・間接経費 10,800,000 円

4) 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」
代表者名 鈴木和幸 分担者 田中健次 直接経費 400,000 円

5) 産学連携 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

6) 産学連携 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調査・研究」,
代表者名 岩本貢 直接経費 455,000 円・間接経費 45,000 円

7) 産学連携 株式会社 富士通研究所,「ゲーム理論を活用した新電力市場の設計や新サービス創出」
代表者名 岩崎敦 直接経費 2,000,000 円

8) 産学連携 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

9) 産学連携 株式会社東芝,「長期安全な運用を実現する情報セキュリティ基盤技術」
代表者名 岩本貢 直接経費 650,000 円・間接経費 65,000 円

10) 産学連携 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」,
分担者 太田和夫 500,000 円

11) 産学連携 三菱電機株式会社,「秘匿検索暗号およびハッシュ関数の理論研究」,
代表者名 太田和夫 分担者 岩本貢 直接経費 455,000 円・間接経費 45,000 円

12) 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 22,300,000 円・間接経費 6,690,000 円

13) 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 3,800,000 円・間接経費 1,140,000 円

14) 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構築とその応用」
代表者名 四方順司(横浜国立大学)分担者 太田和夫 直接経費 700,000 円・間接経費 210,000 円

15) 科研費(基盤研究(A))「レーザーフォールト攻撃による情報漏洩を防ぐ耐タンパー技術の総合的研究」
代表者名 崎山一男 直接経費 9,700,000 円・間接経費 2,910,000 円

16) 科研費(挑戦的萌芽)「サイドチャネル情報を用いた認証システムの構築と安全性評価」
研究代表者 崎山一男 直接経費 1,000,000 円・間接経費 300,000 円

17) 科研費(基盤研究(B))「最適化にもとづく電力市場メカニズム設計のための理論的基盤の構築」
代表者名 岩崎敦 直接経費 4,000,000 円・間接経費 1,200,000 円

18) 科研費(挑戦的萌芽)「想定外を想定した新しいリスク評価法の提案」
代表者名 田中健次 直接経費 1,100,000 円・間接経費 330,000 円

19) 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 2,800,000 円・間接経費 840,000 円

７．発表論文等(各項目とも、代表的な５件以内)

「雑誌論文」

- 加藤慧,小宮山功一朗,瀬古敏智,一瀬友祐,河野耕平,中山心太,吉浦裕:
  コンテンツベースフィッシング検知手法大規模実例評価と改良,日本セキュリティマネジメント学会誌, Vol.25, No.2, pp.42-56, 2011 年 9 月.
- T. Yamada, I. Echizen, H. Yoshiura:
  PC-based Real-time Video Watermark Embedding System Independent of Platform for Parallel Computing, LNCS Trans. on Data Hiding and Multimedia Security, LNCS 7110, pp.15-33. Nov. 2011.
- 中澤 大暁,吉田 雅裕,大坐畠 智,中尾 彰宏,川島 幸之助,
  Winny ネットワークにおける 検索クエリの遮断によるファイル流通制御方式,電子情報通信学会和文論文誌 B,Vol.95-B, No. 5, pp. 636-648, 2012.(ネットワークシステム研究会推薦論文)
- 稲葉緑, 田中健次:
  「水害時の避難へのモチベーションに影響を及ぼす情報提示内容についての実験的検討」, 日本災害情報学会誌 災害情報, No.10, 127-136 (2011.4)
- 稲葉 緑,田中健次,宇佐美 稔,戸塚康男:
  「医療現場での作業中断によるヒューマンエラーの分類と要因」医療の質・安全学会誌,Vol.6, No.3, pp.313-331 (2011.9).

- Shugo Mikami, Hirotaka Yoshida, Dai Watanabe, Kazuo Sakiyama,
  “Correlation Power Analysis and Countermeasure on the Stream Cipher Enocoro-128v2,”
  IEICE Trans. Fundam. Electron. Commun. Comput. Sci.,Vol.96-A, No.3, pp.697-704, (Mar., 2013).
- Yang Li, Kazuo Ohta, and Kazuo Sakiyama,
  “A New Type of Fault-Based Attack: Fault Behavior Analysis,” IEICE Trans. Fundam. Electron. Commun. Comput. Sci., Vol.A96-A, No.1, pp.177-184, (Jan., 2013).
- Naoto Kiribuchi, Ryo Kato, Takashi Nishide, Tsukasa Endo, Hiroshi Yoshiura:
  Batch Logical Protocols for Efficient Multi-party Computation, IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E95-A, No.10, pp.1718-1728,Oct. 2012.
- Naoto Kiribuchi, Ryo Kato, Takashi Nishide, Tsukasa Endo, Hiroshi Yoshiura:
  Reducing Communication Complexity of Random Number Bitwise-Sharing for Efficient Multi-party Computation, Journal of Information Processing, Vol.20, No.4, pp.861-870, Aug. 2012.
- 坂東幸一,田中健次:
  「新聞報道は事故をどう報じているか一金融情報システム事故を例にと って」日本信頼性学会誌,Vol.34,No.6, pp.416-423,2012.
- 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).
- 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).
- 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).
- 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)
- 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.

- Y. Kawai, G. Hanaoka, K. Ohta, and N. Kunihiro,
  "A limitation on security evaluation of cryptographic primitives with fixed keys", Security Comm. Networks, DOI: 10.1002/sec.1457.(Feb., 2016).
- S. Mikami, D. Watanabe, Y. Li, and K. Sakiyama,
  "Fully Integrated Passive UHF RFID Tag for Hash-Based Mutual Authentication Protocol," The Scientific World Journal, Hindawi, Volume 2015 (2015), Article ID 498610, 11 pages, (Aug., 2015).
- T. Machida, D. Yamamoto, M. Iwamoto, and K. Sakiyama,
  "A New Arbiter PUF for Enhancing Unpredictability on FPGA," The Scientific World Journal, Hindawi, Volume 2015 (2015), Article ID 864812, 13 pages, (Aug., 2015).
- D. Yamamoto, K. Sakiyama, M. Iwamoto, K. Ohta, M. Takenaka, K. Itoh, and N. 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, Vol.5(3), pp.187-199, (Sep., 2015).
- T. G. Kale, S. Ohzahata, C. Wu and T. Kato,
  "Reducing Congestion in the Tor Network with Circuit Switching", Journal of Information Processing, vol.23, no.5, pp.589-602, (Sep., 2015).
- M. Goto, A. Iwasaki, Y. Kawasaki, R. Kurata, Y. Yasuda, and M. Yokoo,
  Strategy-proof matching with regional minimum and maximum quotas, Artificial Intelligence, Vol.235, pp.40-57, (Feb., 2016).
- 石塚正也, 高田哲司,
  " CCC:携帯端末での暗証番号認証における振動機能を応用した覗き見攻撃対策手法", 情

報処理学会論文誌, Vol.56, No.9, pp.1877-1888, (Sep., 2015).

- 高橋雅香, 高田哲司,
  ”Android マルウェアの対策行動へ利用者を誘導する警告ダイアログの提案と評価”, 情報処理学会論文誌, Vol.56, No.12, pp.2302-2312, (Dec., 2015).

「学会論文」

- N. Kiribuchi, T. Nishide, T. Endo, H. Yoshiura:
  Accelerating Multiparty Computation by Efficient Random Number Bitwise-Sharing Protocols, Proc. of the 12th Intl. Workshop on Information Security Applications (WISA2011), LNCS 7115, pp.187-020, 2011.
- N. Kiribuchi, R. Kato, T. Nishide, H. Yoshiura:
  Batching Multiple Protocols to Improve Efficiency of Multi-party Computation, Proc. of the 7th Intl. Conf. on Information Security and Cryptology (Inscrypt'2011), 2011.
- T. Kale, S. Ohzahata, T. Kato,
  Improving Tor Circuit Performance with Guard Relay Nodes, IEICE 総合大会,BS-3-14, 2012.
- 田中健次:
  「安全保証と危険回避の使い分けに関する一考察 ―使用説明書と警告表示のあり方―」第 41 回信頼性・保全性シンポジウム発表報文集,JUSE, pp.373-378 (2011.7) (第 41 回信頼性・保全性シンポジウム特別賞受賞)
- Bando,K., Tanaka K.:
  ″ Trend Analysis of Accidents and Dependability Improvement in Financial Information Systems,″ 17th IEEE Pacific Rim International Symposium on Dependable Computing, California, pp.234-243 (2011.12).
- Midori Hirose, Akira Utsumi, Hiroshi Yoshiura:
  A Private Information Detector for Controlling Circulation of Private Information through Social Networks, 2nd International Workshop on Resilience and IT-Risk in Social Infrastructures (RISI 2012),Prague, Czech, Aug. 2012.
- Tomotaka Okuno, Hiroshi Yoshiura:
  Identifying Anonymous Posts of Job Seekers, 21st USENIX Security Symposium (USENIX Security '12), Bellevue, US, Aug. 2012, poster session.
- Yutaka Nishiwaki, Hiroshi Yoshiura:
  Virtualizing Secret-Shared Database System, 21st USENIX Security Symposium (USENIX Security '12), Bellevue, US, Aug. 2012, poster session.
- 益尾文里, 高田哲司:
  ″似顔絵認証: 情報認知の個人差を用いた記憶照合型個人認証への推測 攻撃に対する安全

性向上策の提案″, コンピュータセキュリティシンポジウム 2012 (CSS 2012), 情報処理学会コンピュータセキュリティ研究会, in CD-ROM, Nov. 2012

- Timothy Girry Kale・Satoshi Ohzahata・Toshihiko Kato,
  A Performance Enhancement Method of Tor Circuit by Employing Flags Selection on Cooperative Relays, 信学技報, vol. 112, no. 307, IN2012-118, pp. 45-50, 2012.
- 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.
- 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).
- 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).
- 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).
- 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)
- Timothy Girry Kale, Satoshi Ohzahata, Celimuge Wu, and Toshihiko Kato,
  "Analyzing the Drawbacks of Node-Based Delays in Tor", CQR 2014, 2014
- Tetsuji TAKADA and Yuki KOKUBUN,
  "Extended PIN Authentication Scheme Allowing Multi-touch Key Input", Proc. of Advances in Mobile Computing & Multimedia (MoMM 2013), 2013.
- Hayate Goto and Tetsuji Takada,
  "VisualAnomalyDetectionofNetwork Connections in a Personal Computer", IEEE Pacific Visualization 2014, Mar., 2014.
- 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

- 尼子雄大, 高田哲司,
  ”情報視覚化による DBD(Drive-by Download)攻撃対策の一検討”, 情報処理学会 CSEC 研究, Mar., 2014
- 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)

- T. Nakai, Y. Tokushige, M. Iwamoto and K. Ohta,
  "Toward Reducing Shuffling in Card-based Cryptographic Protocol for Millionaire Problem", International Workshop on Information Security, (IWSEC 2015), 26th, August, 2015.
- Y. Misawa, Y. Tokushige, M. Iwamoto and K. Ohta,
  "Comparison of Security on Coded Signs with Public/Private Code Book", International Workshop on Information Security (IWSEC2015), 26th, August, 2015.
- Y. Sakai, K. Emura, J.C.N. Schuldt, G. Hanaoka, and K. Ohta,
  "Dynamic Threshold Public-key Encryption with Decryption Consistency from Static Assumptions", Australasian Conf. on Information Security and Privacy (ACISP 2015), 29 June 2015, Brisbane, Australia.
- M. Iwamoto and J. Shikata,
  "Construction of symmetric-key encryption with guessing secrecy", IEEE International Symposium on Information Theory (ISIT2015),pp.725—729, 15th, June, 2015, Hong-Kong
- R. Yagasaki and K. Sakiyama,
  "Artifact-Metric-Based Authentication for Bottles of Wine," In Proc. International Workshop on Security 2015 (IWSEC'15), LNCS 9241, Springer-Verlag, pp.335-344, (Aug., 2015), Nara, Japan.
- K. Sakiyama, T. Machida, and A. Matsubara,
  "Advanced Fault Analysis Techniques on AES," In Proc. Joint IEEE International Symposium on Electromagnetic Compatibility and EMC Europe (EMC'15), pp.230-234, IEEE, Aug., 2015, Dresden, Germany.
- T. G. Kale, S. Ohzahata, C. Wu, and T. Kato,
  "Evaluation of Dynamic Circuit Switching to Reduce Congestion in Tor", Proc. of ITNAC 2015, pp. 326-331, Nov. 2015. (Australia)
- Y. Ishigaki, Y. Matasumoto, Y. Matsuno, and K. Tanaka,
  "Trust Establishment in Participatory Radiation Sensing", The 9th IFIP WG 11.11 Int'l Conf. on Trust Management (IFIPTM 2015), May, 2015, Hamburg, Germany
- K. Tanaka, and M. Inaba,
  "Effective double-check methods regarding the accuracy and required time of the verification process in medication preparation", 4th World Congress of Clinical Safety (4WCCS), Sep., 2015, Vienna, Austria.
- K. Bando, Y. Matsuno, and K. Tanaka,
  "Failure Analyses of Communications Systems and Networks by Publicly Available Failure Information from the viewpoint of Dependability", the 21st IEEE Pacific Rim Int'l Symp. on Dependable Computing (PRDC 2015), pp.139-148, Nov., 2015, Zhangjiajie, China.

- H. Iwashita, K. Ohori, H. Anai, and A. Iwasaki,
  “Simplifying Urban Network Security Games with Cut-Based Graph Contraction”, the proceedings of the 14th International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS-2016), May 2016.
- R. Kurata, M. Goto, A. Iwasaki, M. Yokoo,
  “Controlled School Choice with Soft Bounds and Overlapping Types”, the proceedings of the 29th AAAI Conference on Artificial Intelligence (AAAI-2015), 951-957, Jan. 2015.
- A. Iwasaki, E. Fujita, T. Todo, H. Iwane, H. Anai, M. Guo, M. Yokoo,
  “Parametric Mechanism Design via Quantifier Elimination”, AAMAS 2015: 1885-1886
- M. Goto, R. Kurata, N. Hamada, A. Iwasaki, M. Yokoo,
  “Improving Fairness in Nonwasteful Matching with Hierarchical Regional Minimum Quotas”, AAMAS 2015: 1887-1888
- A. Iwasaki, T. Sekiguchi, S. Yamamoto, M. Yokoo,
  “How Is Cooperation/Collusion Sustained in Repeated Multimarket Contact with Observation Errors?”, 2015 AAAI Fall Symposium on Sequential Decision Making for Intelligent Agents
- H. Goto and T. Takada:
  ″Anomalous Network Communication Detection System By Visual Pattern On A Client Computer”, 30th Annual ACM Symp. on Applied Computing(ACM SAC 2015), Salamanca, Spain, pp.1263--1269, Apr. 2015
- T. Takada, and K. Amako,
  “A Visual Approach for Detecting Drive-by Download Attacks”, 8th Int’l Symp. on Visual Information Communication and Interaction (VINCI 2015), Tokyo, Japan, pp.162-163, (Aug. 2015).
- T. Takada, and M. Ishizuka,
  “Chameleon Dial: Repeated Camera-recording Attack Resilient PIN input scheme”, ACM Int’l Joint Conf. on Pervasive and Ubiquitous Computing (UbiComp 2015), Osaka, Japan, pp.365-368, (Sep., 2015).
- S. Mochizuki, and T. Takada,
  “Client-Oriented Web Alteration Detection System using Link Change State of a Web Page based on Past and Current Page Content”, 17th Int’l Conf. on Information Integration and Web-based Applications & Services (iiWAS 2015), (Dec., 2015).
- 八代理紗, 町田卓謙, 岩本貢, 崎山一男,
  “Deep Learning を用いた Double Arbiter PUF の安全性評価”, 電子情報通信学会 2016 年総合大会, 16th, Mar., 2016. 福岡県(九州大学), p. 99
- 徳重佑樹, 花谷嘉一, 岩本貢, 太田和夫,
  ”グループ認証付鍵交換プロトコルの weak-SK-secure 性の形式検証”, 暗号と情報セキュリティシンポジウム(SCIS2016), 19th, Jan., 2016. (熊本市)

- 平野貴人, 川合豊, 太田和夫, 岩本貢,
  “共通鍵暗号型の秘匿部分一致検索(その1)”, 暗号と情報セキュリティシンポジウム(SCIS2016), 20th, Jan., 2016. (熊本市)
- 早坂健一郎, 川合豊, 平野貴人, 太田和夫, 岩本貢,
  “共通鍵暗号型の秘匿部分一致検索(その 2)”, 暗号と情報セキュリティシンポジウム(SCIS2016), 20th, Jan., 2016.(熊本市)
- A. E. Trujillo and M. Iwamoto,
  “Proactive Secret Image Sharing with Quality and Payload Trade-off in Stego-images”, 暗号と情報セキュリティシンポジウム(SCIS2016), 21st, Jan., 2016.(熊本市)
- 鴨志田優一, 岩本貢, 太田和夫,
  ”Joux-Lucks のマルチコリジョン探索アルゴリズムのMicroMint への応用”, 暗号と情報セキュリティシンポジウム(SCIS2016), 21st, Jan., 2016, (熊本市)
- 三澤裕人, 徳重佑樹, 岩本貢, 太田和夫,
  ”人間向け暗号/認証プロトコルの統一的安全性評価”, 暗号と情報セキュリティシンポジウム(SCIS2016), 21st, Jan., 2016.(熊本市)
- 中井雄士, 三澤裕人, 徳重佑樹, 岩本貢, 太田和夫,
  ”カード操作の分類とカードベース暗号プロトコル”, 暗号と情報セキュリティシンポジウム(SCIS2016), 22nd, Jan.,2016.(熊本市)
- 三澤裕人, 徳重佑樹, 岩本貢, 太田和夫,
  “ブロックサインの安全性に対するコードブックの影響”, コンピュータセキュリティシンポジウム(CSS 2015), 23rd, Oct., 2015. (長崎市), pp.1011-1018,
- 徳重佑樹, 三澤裕人, 吉田文晶, 上床昌也, 岩本貢, 太田和夫,
  ″物理的復元が容易な音響秘密分散法″, 電子情報通信学会マルチメディア情報ハイディング・エンリッチメント研究会 (EMM), 6 pages, 2015 年 5 月, (京都府)
- 島野雄貴, 岩崎敦,
  “ゲーム理論を用いた警備計画における最適な乱択化に関する研究”,
  日本 OR 学会春季研究発表会, 2016 年 3 月 17 日, (神奈川県横浜市)
- 岩崎敦,
  “マッチングメカニズムの戦略的側面とその展開”, 経営情報学会 2015 年秋季全国研究発表会, 2015 年 11 月 29 日, 沖縄コンベンションセンター(沖縄県宜野湾市)
- 望月翔太, 高田哲司,
  “Webページ内リンク情報の変化に基づくWeb改ざん検知の有効性検証”, コンピュータセキュリティシンポジウム 2015 (CSS 2015), pp.504-511, (長崎県長崎市)
- 森康洋, 高田哲司,
  “回答候補画像の追加と正解画像の集中配置による再認式画像認証の安全性改善と操作負担抑制”, コンピュータセキュリティシンポジウム 2015 (CSS 2015), pp.787-794, (長崎県長崎市)

「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).
- 岩崎敦, ”最適化と繰り返しゲーム: 動的環境における意思決定”, 第 27 回 RAMP シンポジウム, 2015 年 10 月 16 日, 静岡大学浜松キャンパス(静岡県浜松市)

「図書」

- 田中謙次,「システムの信頼性と安全性」, 朝倉書店, 212 頁, (2014 年)
- K. Sakiyama, Y. Sasaki, and Y. Li,
  “Security of Block Ciphers: From Algorithm Design to Hardware Implementation,” ISBN 978-1-118-66001-0, Wiley, (Jul., 2015).

「受賞」

- 平成 22 年度情報処理学会論文賞 (平成 23 年 6 月受賞)
  (受賞論文) 志村, 宮崎, 西出, 吉浦氏,「秘密分散データベースの構造演算を可能にするマルチパーティプロトコルを用いた関係代数演算」
- 平成 22 年度日本・セキュリティマネジメント学会論文賞(平成 23 年 6 月受賞)
  (受賞論文) 渡辺, 片岡, 内海, 吉浦氏,「SNS 上のテキストからプライバシー情報を検知するシステムの構想と予備評価」
- 第 41 回信頼性・保全性シンポジウム特別賞受賞
- International Workshop on Security (IWSEC)にて Best Paper Award 受賞.(Nov., 2012)
  (受賞論文) Yu Sasaki, Lei Wang, Yasuhiro Takasaki, Kazuo Sakiyama, and Kazuo Ohta, “Boomerang Distinguishers for Full HAS-160 Compression Function, ”International Workshop on Security” (IWSEC).
- 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,
- 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/es-awards.html

- 情報処理学会 インタラクション 2014, 石塚正也, 高田哲司, インタラクティブ発表賞, 2014/02/28, http://www.interaction-ipsj.org/2014/program.html
- 平成27年度 日経品質管理文献賞:田中健次
  「システムの信頼性と安全性」(朝倉書店. 2014)
  Web: http://www.juse.or.jp/deming/award/1074.html
- CSS 2015 最優秀デモンストレーション賞:藤井達哉, 粕谷桃伽, 町田卓謙, 崎山一男,
  DE0-nano を用いたサイドチャネル認証, 2015年10月22日
  Web: http://www.iwsec.org/css/2015/demo.htm

「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
- 「認証システムおよび認証方法」, 崎山一男, 李陽, 出願番号:PCT/JP2015/52576, 2015/1/29