平成２８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（所属部局・職・氏名）　情報学専攻　准教授　高田　哲司

２．研究組織(今年度関わった全ての構成員を記してください。)

＜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 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 大座畠智
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
電気通信大学　大学院情報理工学研究科　情報学専攻　　特別研究員 渡邉洋平

＜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２８年度の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などの点から記述すること）

1). 推測秘匿性と呼ばれる情報理論的な安全性概念は，平均推測秘匿性，最適推測秘匿性に大別される．岩本らは，暗号化がラテン方陣に従う場合に，最適推測秘匿性を満たす方式は完全秘匿(と平均推測秘匿性)を満たすことを示した．しかし，最適秘匿性を満たすが，完全秘匿性も平均秘匿性も満たさない情報理論的暗号方式が存在するかについては未解決であった．今年度は，秘密分散法においてこのような非自明な最適推測安全性を満たす方式が構成できることを示した．推測秘匿性に関する理論研究としては重要な知見であると考えている．

2). 近年普及が進むクラウド環境において，ゲノム情報のような 100 年以上の長期的な安全性を必要とする情報をどう扱うべきか，という問題は重要な問題である．その問題に現代暗号理論の立場から取り組み，クラウドでの利用を想定した動的アクセス制御機能を有する放送型暗号を提案した．具体的には，暗号化時に全ユーザの中から復号可能なユーザを任意に指定できる放送型暗号について，暗号文がクラウドストレージなどの外部サーバに保存される状況を想定し，暗号文を更新することで暗号化した後でも復号可能ユーザを復号することなく変更可能な方式を提案した．数理モデル及び安

全性を定式化し，実現可能な鍵長の下界を導出した上で，その下界を満たす構成法を提案した．更に，より強い安全性モデルを満たす方式も提案した．提案方式は情報理論的に安全であり，従って柔軟なアクセス制御機能を持ちつつも長期的な安全性を保証可能である．

3). Tor ネットワークにおける通信品質改善と匿名性分析に関する研究：
通信の秘匿を提供するため P2P ネットワークを用いて匿名性を提供する Tor が普及している。しかし、Tor ネットワークでは、オニオンルーティングと通信経路を混ぜ合わせるため、通信のスループットが出ない問題がある。本研究室では、通信経路を分散させることにより、輻輳を回避する方式を提案し、Tor ネットワークエミュレータで評価をすることでその有効性を明らかにした。さらに Tor ネットワークの匿名性に対する攻撃手法を明らかにし、その分析を現在行っている。

4). 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 環境での通信の課題の一つとして送信機会の確保がある。送信機会をトラヒックの優先度に応じて変化させるために、IEEE802.11e EDCA(Enhanced Dsitributed Channel Access)では、送信フレームを 4 種類のアクセスカテゴリ(AC:Access Category)に分類し，カテゴリ毎にパラメータを変更することで優先度制御を提供する。しかし、不適切に設定された EDCA の高優先度端末（利己的な端末）と適切に設定された端末が混在している環境では、利己的な端末の送信機会が極端に多くなり、適切に設定された端末が通信機会を得られなくなる問題がある。そこで本研究室では、利己的な端末が同一の AP に存在した場合でも、Duration infration attrack を応用し、さらに，RTS/CTS で用いられている NAV(Network Allocation vector)の動的変更とキューイング手法(Modified DRR)，AP の動的な CWmin の制御を組み合わせ制御でおこなっているが、さらに、AP が利己的な端末から送信権を奪い返す仕組みを導入した。これにより，攻撃端末と競合することなく AP と端末が通信機会を得ることができる。提案方式の有効性は，コンピュータシミュレーションにより評価し，提案手法の有用性を明らかにした。

5). 不正な通信を検出するための分類器の組み合わせ方式。：
機械学習を用いた分類器の精度には FP と FN の間にトレードオフがあり、一方の精度を改善すると、他方の精度が低下し、全体としての精度をあげることが難しい。そこで本研究室では、1 つの分類器で、片方の精度のみを改善させ、それを組み合わせることで、全体の精度を改善する手法を提案している。提案方式を IDS のデータセットで評価し、その有効性を明らかにした。

４．平成２８年度の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) 「システム安全学」ワークショップを開催　平成29年3月1日 於 電気通信大学　西10号館2階大会議室，8件の発表とプロジェクト報告，2件の招待講演

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））「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」研究代表者：崎山一男　直接経費：8,100 千円，間接経費：2,430 千円
(2) 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」研究代表者:鈴木和幸，分担者　田中健次　直接経費分担額:200 千円
(3) 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」研究代表者：岩崎 敦　直接経費：4,000 千円，間接経費：1,200 千円
(4) 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」，研究代表者:四方順司（横浜国立大学），分担者:岩本貢，直接経費: 1,400 千円，間接経費:420 千円
(5) 科研費（基盤研究(C)）「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」，研究代表者:岩本貢，直接経費: 1,200 千円，間接経費:360 千円
(6) 科研費（挑戦的萌芽）「想定外事象を想定した新しいリスク評価法の提案」，研究代表者名田中健次　直接経費 1,100 千円，間接経費 330 千円
(7) 科研費（挑戦的萌芽）「利用状況に応じた携帯端末向け個人認証の研究」，研究代表者:高田哲司　直接経費:1,100 千円，間接経費:330 千円
(8) 科研費 特別研究員奨励費，「秘匿情報に対して動的アクセス制御とデータ解析を両立させる暗号理論の確立」，研究代表者: 渡邉洋平，直接経費 900 千円，関節経費 270 千円.

(9) 共同研究　富士通研究所，研究題目「ゲーム理論に基づく AI 数理技術の研究」，代表者：岩崎敦，直接経費：2,000 千円
(10) 共同研究　株式会社 東芝，研究題目「危殆化に対して長期安全なシステムを実現する情報セキュリティ基盤技術」，代表者：岩本貢，直接経費：455 千円，間接経費：45 千円
(11) 共同研究　三菱電機（株），研究題目「秘匿検索暗号の理論研究」，代表者:太田　和夫，直接経費:455 千円，間接経費:　45 千円
(12) 共同研究　トヨタIT 開発センター，研究題目:「V2X システムにおける過信に配慮した情報提示方法の検討・評価」，代表者:田中健次，直接経費:1,324 千円　間接経費:132 千円

６．今後の研究発展
（外部への発信、外部資金獲得計画を含む）

７．発表論文等（各項目ごとに記載してください。）
「雑誌論文」：著者名・論文標題・雑誌名・査読の有無・巻・発行年(西暦)及びページ

Ryoji Kurata, Naoto Hamada, Atsushi Iwasaki and Makoto Yokoo, "Controlled School Choice with Soft Bounds and Overlapping Types", Journal of Artificial Intelligence Research, 査読有, 58, 2017, pp.153-184.

Masahiro Goto, Atsushi Iwasaki, Yujiro Kawasaki, Ryoji Kurata, Yosuke Yasuda, Makoto Yokoo, "Strategyproof matching with regional minimum and maximum quotas", Artificial Intelligence, 査読有, 2016, 235, 40-57,

Y. Watanabe and J. Shikata, "Unconditionally Secure Broadcast Encryption Schemes with Trade-offs between Communication and Storage," IEICE Transactions, 査読有, vol.99-A, no.6, pp.1097-1106, 2016.

Y. Watanabe and J. Shikata, "Information-Theoretically Secure Timed-Release Secret Sharing Schemes," Journal of Information Processing, 査読有, vol.24, no.4, pp.680-689, 2016.

森康洋, 高田哲司:「秘密情報を変更せずに提供しうる安全性を柔軟に変更可能な再認式画像認証の提案」, 情報処理学会論文誌, 査読有, Vol.57, No.12, pp.2641-2653, 2016.

田中健次:「グレイゾーンにおける現場技術者と設計推進者との協調とは」, 日本品質管理学会誌『品質』, 査読無, Vol.47, No.1, pp. 39-44 (2017.1)

「学会発表」：発表者(代表)名・発表標題・学会等名・発表年月日・発表場所

Fuuki Shigenaka, Tadashi Sekiguchi, Atsushi Iwasaki, and Makoto Yokoo, "Achieving Sustainable Cooperation in Generalized Prisoner's Dilemma with Observation Errors,", the Proc. of the 31th AAAI Conference on Artificial Intelligence (AAAI-2017), to appear, 査読有.

Hiroaki Iwashita, Kotaro Ohori, Hirokazu Anai, and Atsushi Iwasaki, "Simplifying Urban Network Security Games with Cut-Based Graph Contraction,", the Proc. of the 14th International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS-2016), 205-213,

Atsushi Iwasaki, Tadashi Sekiguchi, Shun Yamamoto, and Makoto Yokoo, "Repeated multimarket contact with observation errors,", the Proc. of the 9th International Symposium on Algorithmic Game Theory (SAGT-2016), 344-345.

T. Nakai, Y. Misawa, Y. Tokushige, M. Iwamoto, and K. Ohta, "Efficient Card-based Cryptographic Protocols for Millionaires' Problem Utilizing Private Permutations", In Proc. of CANS2016, 2016 年 11 月 15 日, Milan, Italy, LNCS 10052, pp. 350-364, 2016.

K. Hayasaka, Y. Kawai, Y. Koseki, T. Hirano, K. Ohta, and M. Iwamoto, "Probabilistic Generation of Trapdoors: Reducing Information Leakage of Searchable Symmetric Encryption", CANS2016, 2016 年 11 月 15 日, Milan, Italy, LNCS 10052, pp. 500-517, 2016.

T. Hirano, M. Hattori, Y. Kawai, N. Matsuda, M. Iwamoto, K. Ohta, Y. Sakai, and T. Munaka, "Simple, Secure, and Efficient Searchable Symmetric Encryption with Multiple Encrypted Indexes", IWSEC 2016, 2016 年 9 月 13 日, Tokyo, Japan, LNCS 9836, pp.91-110, 2016.

R. Yashiro, T. Machida, M. Iwamoto, and K. Sakiyama, "Deep-Learning-Based Security Evaluation on Authentication Systems Using Arbiter PUF and Its Variants", IWSEC 2016, 2016 年 9 月 13 日, Tokyo, Japan, LNCS 9836, pp.267- 285, 2016.

Y. Kamoshida, M. Iwamoto, and K. Ohta, "Application of Joux-Lucks Search Algorithm for Multi-Collisions to MicroMint", IWSEC2016 (poster session), 2016 年 9 月 12 日, Tokyo, Japan

Phetlasy Sornxayya, Satoshi Ohzahata, Celimuge Wu, Toshihiko Kato, "Combining two sequential algorithms for classification of intrusion detection system dataset", IWSEC 2016, 2016. (poster session), 東京

Timothy Girry Kale, Satoshi Ohzahata, Celimuge Wu, Toshihiko Kato, "Evaluating Tor Modified Switching Algorithm in the Emulation Environment", Proc. of IEEE APCC 2016, 2016. インドネシア

Timothy Girry Kale, Satoshi Ohzahata, Celimuge Wu, Toshihiko Kato, "Improving the Tor Traffic Distribution with Circuit Switching Method", Proc. of IEEE HPSR 2016, 2 pages, 2016. 横浜

Takashi Sasagawa, Satoshi Ohzahata and Toshihiko Kato, "Suppressing Selfish Transmissions with Extending NAV Period and Resetting CW of Access Point in Wireless LAN", Proc. of the 5th International Workshop on Large-Scale Network Security, 6 pages,2016. 天津

Yohei Watanabe, Keita Emura, and Jae Hong Seo, "New Revocable IBE in Prime-Order Groups: Adaptively Secure, Decryption Key Exposure Resistant, and with Short Public Parameters," CT-RSA 2017, February 17th, 2017, San Francisco, CA, USA.

Yohei Watanabe, Goichiro Hanaoka, and Junji Shikata, ″Unconditionally Secure Revocable Storage: Tight Bounds, Optimal Construction, and Robustness,″ ICITS 2016, August 12th, 2016, Tacoma, WA, USA.

Takahiro Yoshizawa, Yohei Watanabe, and Junji Shikata, ″Unconditionally Secure Searchable Encryption″, CISS 2017, March 23rd, 2017, Baltimore, MD, USA.

Risa Yashiro, Takanori Machida, Mitsugu Iwamoto, and Kazuo Sakiyama, "Deep-Learning-Based Security Evaluation on Authentication Systems Using Arbiter PUF and Its Variants," In Proc. International Workshop on Security 2016 (IWSEC' 16), LNCS 9836, Springer-Verlag, pp.267-285, (Sep., 2016).

Momoka Kasuya, Takanori Machida, and Kazuo Sakiyama, "New Metric for Side-Channel Information Leakage: Case Study on EM Radiation from AES Hardware," In Proc. URSI Asia-Pacific Radio Science Conference (URSI AP-RASC' 16), (Aug., 2016).

Kazuo Sakiyama, Reina Yagasaki, Takanori Machida, Tatsuya Fujii, Noriyuki Miura, and Yu-ichi Hayashi, "Circuit-Level Information Leakage Prevention for Fault Detection," In Proc. URSI Asia-Pacific Radio Science Conference (URSI AP-RASC' 16), IEEE, (Aug., 2016).

Kazuo Sakiyama, Momoka Kasuya, Takanori Machida, Arisa Matsubara, Yunfeng Kuai, Yu-Ichi Hayashi, Takaaki Mizuki, Noriyuki Miura, and Makoto Nagata, "Physical Authentication Using Side-Channel Information," In Proc. International Conference on Information and Communication Technology (ICoICT' 16), IEEE, (May, 2016).

Shugo Mikami, Dai Watanabe, Kazuo Sakiyama, "A Performance Evaluation of Cryptographic Algorithms on FPGA and ASIC on RFID Design Flow," In Proc. International Conference on Information and Communication Technology (ICoICT' 16), IEEE, (May, 2016).

Ishigaki, Y., Matsuno, Y., Bando, K., Tanaka, K.: "A Prototype Development of Assurance Cases Tool and Experiments on SNS Discussion of Radiation Disaster," *Proc. of 13th International Conference on Information Systems for Crisis Response and Management*(ISCRAM2016), CD-ROM, Rio de Janeiro, Brasil (2016).

Bando, K., Matsuno, Y., Ishigaki, Y., Tanaka, K.:″A Prototype Implementation of a Failure Database for Information Sharing with the General Public — A Case Study on Radiation Risk Information after Fukushima Nuclear Disaster," *The 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks* (DSN 2016) Toulouse, France (2016).

Kurihashi, S., Tanaka, K.: : ″Mutual Assistance System for Automobile Safety″ , *The 13th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design, and Evaluation of Human-Machine Systems* (IFAC-HMS2016), Kyoto, 2016.

Tanaka, K., Inaba, M., Soyama, A.: "Effective teaching method for learning adaptive versatility of rules", *5th World Congress of Clinical Safety (5WCCS),* Boston USA (2016).

Matsuno, Y., Ishigaki, Y., Bando, K., Kido, H., Tanaka, K.: "Developing SNS tool for Consensus Building on Environmental Safety using Assurance Cases (Tool Paper)," *The 4th International Workshop on Assurance Cases for Software-intensive Systems (ASSURE 2016 Workshop)*, Norway (2016)

Ishigaki, Y., Matsuno, Y., Bando, K., Tanaka, K.: ″Wisdom of Crowds for Reliable Discussion and Need Finding: A Case Study of Information Sharing Regarding Radiation after the Fukushima Nuclear Disaster″, *Hawaii International Conference on System Sciences (HICSS-50)*, Hawaii (2017).

Bando, K., Matsuno, Y., Ishigaki, Y., Tanaka, K.: ″ Trend Analyses of Failures in Information Systems－A Case Study on Communications Networks and Financial Information Systems ″ *The 22nd IEEE Pacific Rim International Symposium on Dependable Computing* (PRDC 2017), New Zealand (2017).

中井雄士, 野島拓也, 岩本貢, 太田和夫,「検索可能暗号における最小漏洩情報に関する考察」, 電子情報通信学会研究会研究報告, IT2016-128/ISEC2016-118/WBS2016-104, pp. 187-192, March, 2017., Tokyo, Japan

早坂健一郎, 川合 豊, 小関 義博, 平野 貴人, 岩本貢, 太田 和夫,「検索クエリからの漏洩情報を削減した効率的な共通鍵型検索可能暗号」, 暗号と情報セキュリティシンポジウム (SCIS2017), 1D1-1, 24th, Jan., 2017., 沖縄県那覇市

岩本貢, 四方順司,「最悪推測秘匿性を満たす秘密分散法に関する基本的性質」, 暗号と情報セキュリティ シンポジウム (SCIS2017), 1A1-4, 24th, Jan., 2017., 沖縄県那覇市

A. Espejel-Trujillo, M. Iwamoto, "Steganalysis of Bit Replacement Steganography for a Proactive Secret Image Sharing", 暗号と情報セキュリティシンポジウム (SCIS2017), 1A1-6, 24th, Jan., 2017., 沖縄県那覇市

徳重佑樹, 中井雄士, 岩本貢, 太田和夫,「カードを用いた複数人での金持ち比べプロトコル」, 暗号と情報セキュリティシンポジウム (SCIS2017), 1A2-1, 24th, Jan., 2017., 沖縄県那覇市

城内聡志, 中井雄士, 岩本貢, 太田和夫,「秘匿操作を用いた効率的なカードベース論理演算プロトコル」, 暗号と情報セキュリティシンポジウム (SCIS2017) , 1A2-2, 24th, Jan., 2017., 沖縄県那覇市

鴨志田優一, 岩本貢, 太田和夫,「電子決済方式 MicroMint の潜在的な偽造脅威に対する安全性評価」, 暗号と情報セキュリティシンポジウム（SCIS2017), 1F2-6, 24th, Jan., 2017., 沖縄県那覇市

平野貴人, 小関義博, 川合豊, 岩本貢, 太田和夫,「リクエストベース比較可能暗号におけるシミュレー ションベースの安全性」, 暗号と情報セキュリティシンポジウム（SCIS2017), 1D2-5, 24th, Jan., 2017., 沖縄県那覇市

岩本貢,「マルチパーティ計算に関する安全性概念の定式化について」, 暗号と情報セキュリティシンポジウム（SCIS2017), 2D4-3, 25th, Jan., 2017., 沖縄県那覇市

岩本貢, 渡邉 洋平,「秘密分散型放送暗号」, 暗号と情報セキュリティシンポジウム（SCIS2017), 4F2-2, 27th, Jan., 2017., 沖縄県那覇市

小美濃つかさ, 駒野雄一, 岩本貢, 太田和夫,「長期間にわたって安全な地域医療連携システムの構築を目指して」, 第 36 回医療情報学連合大会,（ポスターセッション), pp. 996-999, Nov., 2016., 神奈川県横浜市

平野貴人, 岩本貢, 太田和夫,「複数の暗号化索引を持つ共通鍵ベース秘匿検索の効率的なトラップドア生成」, コンピュータセキュリティシンポジウム, 2C3-4, pp. 572-577, 12th, Oct., 2016., 秋田県秋田市

渡邉洋平,「放送型暗号における動的かつ効率的な復号権限変更」, 暗号と情報セキュリティシンポジウム 2017 (SCIS 2017) 予稿集, 4F2-1, 2017.

井田潤一, 渡邉洋平, 四方順司,「3 ラウンド対話型 Signcryption の効率的な構成法」, 暗号と情報セキュリティシンポジウム 2017 (SCIS 2017) 予稿集, 3F3-3, 2017.

吉澤貴博, 渡邉洋平, 四方順司,「推測秘匿性に基づく情報理論的に安全な検索可能暗号」, 暗号と情報セキュリティシンポジウム 2017 (SCIS 2017) 予稿集, 1D1-4, 2017.

渡邉洋平, 江村恵太,「素数位数群における効率的な鍵失効機能付き ID ベース暗号の構成法」, コンピューターセキュリティシンポジウム 2016 (CSS 2016) 予稿集, 2C1-2, pp.324–331, 2016.

吉澤貴博, 渡邉洋平, 四方順司,「情報理論的に安全な検索可能暗号の構成法について」, コンピューターセキュリティシンポジウム 2016 (CSS 2016) 予稿集, 2C3-2, pp.556–563, 2016.

渡邉洋平,「復号権限無効化機能つき放送型暗号」, 第 39 回情報理論とその応用シンポジウム (SITA 2016), 岐阜県高山市, 2016 年 12 月 15 日, 岐阜県高山市.（ポスター発表）

太田和夫,「共通鍵暗号による秘匿検索暗号のセキュリティ」, 日本銀行金融研究所ディスカッション・ペーパー・シリーズ, 2017J-05, 2017.

高田哲司, 森康洋,「1つの秘密情報で複数の安全性を提供しうる個人認証」, コンピュータセキュリティシンポジウム 2016(CSS 2016), 2016 年 10 月, 秋田県秋田市

荻野貴大,「圧力を利用した個人認証の提案」, コンピュータセキュリティシンポジウム 2016(CSS 2016), 2016 年 10 月, 秋田県秋田市 (ポスター発表)

皆川諒,「馴化による警告効果低減を抑制しうるセキュリティ警告」, コンピュータセキュリティシンポジウム 2016(CSS 2016), 2016 年 10 月, 秋田県秋田市 (ポスター発表)

山岸伶,「情報間の関連を再現する個人認証の研究」, コンピュータセキュリティシンポジウム 2016 (CSS 2016), 2016 年 10 月, 秋田県秋田市 (ポスター発表)

荻野貴大,「携帯端末における画面押し込み圧力を用い多値離散値入力の可能性検証」, インタラクション 2017, 2017 年 03 月, 東京都 (ポスター発表)

「図書」 : 著者名・出版社名・書名・発行年(西暦)及び総ページ数(共著の場合、最初と最後のページを記載)

(1) 小林欣吾, 佐藤創(監訳),「数学ゲーム必勝法」共立出版, 2016. 原著: Elwyn R. Berlekamp, John H. Conway, Richard K. Guy, "Winning Ways for Your Mathematical Plays," A K Peters/CRC Press, 2001. (第 1 巻 第 5 章の翻訳を担当).

「受賞」 : 授与団体・受賞者(代表者)名・受賞標題・受賞年月日

(1) 「学生研究賞」, サイバーセキュリティシンポジウム道後 2017, (受賞者 : 八代理紗)
(2) 「Best Presenter 賞」, 国際会議 ICoICT 2016, (受賞者 : 粕谷桃伽)
(3) Heidelberg Laureate Forum Foundation, Y. Watanabe, Invitation to 4th Heidelberg Laureate Forum, September 18th-23rd, 2016. (受賞者 : 渡邉洋平)
(4) 第 14 回 ディペンダブルシステムワークショップ最優秀論文発表賞 : 坂東幸一 (電気通信大学)、松野 裕 (日本大学)、石垣 陽、田中健次 (電気通信大学), 「市民等と障害情報を共有する障害データベースの構築の試み」(日本ソフトウェア科学会ディペンダブルシステム研究会主催), (2016.12). https://sites.google.com/site/jssstdsw/dsw2016

「その他」：ホームページ等

(1) 「暗号王になる」子供の科学, pp. 11-21, 誠文堂新光社(太田和夫教授の取材協力), 2016 年 11 月号.
(2) 渡邉洋平, “国際会議参加報告: 4th Heidelberg Laureate Forum,” Fundamentals Review, Vol. 10, No. 3, pp.220–221, 電子情報通信学会, 2017. Available at https://www.jstage.jst.go.jp/article/essfr/10/3/10_220/_pdf