部局	大学院工学研究科
専攻・講座	電気電子工学専攻　電子情報講座
氏名	白石　善明

略歴（学歴，職歴，受賞）	
年　　月	（学　　歴）
1991 年　3 月	京都府立嵯峨野高等学校卒業
1991 年　4 月	愛媛大学工学部情報工学科入学
1995 年　3 月	同　上　卒業
1995 年　4 月	愛媛大学大学院理工学研究科情報工学専攻博士前期課程入学
1997 年　3 月	同　上　修了
1997 年　4 月	東京工業大学大学院理工学研究科電気・電子工学専攻博士後期課程入学
1999 年　3 月	同　上　第 2 年次転出
1999 年　3 月	徳島大学大学院工学研究科システム工学専攻博士後期課程第 2 年次転入学
2000 年　3 月	同　上　修了
2000 年　3 月	博士（工学）（徳島大学）
年　　月	（職　　歴）
1998 年　1 月	(有)ナオゼンネットワークス　代表取締役社長（2002 年 3 月まで）
2002 年　4 月	近畿大学理工学部情報学科　講師
2006 年　4 月	名古屋工業大学大学院工学研究科情報工学専攻　助教授
2007 年　4 月	名古屋工業大学大学院工学研究科情報工学専攻　准教授
2013 年　10 月	神戸大学大学院工学研究科電気電子工学専攻　准教授
2017 年　12 月	神戸大学数理・データサイエンスセンター　配置
2024 年　4 月	神戸大学大学院工学研究科電気電子工学専攻　教授

年　　月	(受　　賞)
2002 年　5 月	電子情報通信学会オフィスシステム研究賞　（電子情報通信学会オフィスシステム研究専門委員会）
2003 年　9 月	暗号と情報セキュリティシンポジウム 20 周年記念賞　（電子情報通信学会情報セキュリティ研究専門委員会）
2006 年　1 月	2005 年暗号と情報セキュリティシンポジウム論文賞　（電子情報通信学会情報セキュリティ研究専門委員会）
2007 年　8 月	情報処理学会マルチメディア，分散，協調とモバイルシンポジウム（DICOMO 2007）優秀論文賞　（情報処理学会 DICOMO シンポジウムプログラム委員会）
2008 年　8 月	情報処理学会マルチメディア，分散，協調とモバイルシンポジウム（DICOMO 2008）優秀論文賞　（情報処理学会 DICOMO シンポジウムプログラム委員会）
2011 年　8 月	情報処理学会マルチメディア，分散，協調とモバイルシンポジウム（DICOMO 2011）優秀論文賞　（情報処理学会 DICOMO シンポジウムプログラム委員会）
2012 年　5 月	電子情報通信学会 LOIS 功労賞　（電子情報通信学会ライフインテリジェンスとオフィス情報システム研究専門委員会）
2013 年　8 月	情報処理学会マルチメディア，分散，協調とモバイルシンポジウム（DICOMO 2013）優秀論文賞　（情報処理学会 DICOMO シンポジウムプログラム委員会）
2015 年　1 月	情報処理学会高度交通システム研究会優秀論文賞　（情報処理学会高度交通システムとスマートコミュニティ研究会）
2017 年　4 月	電子情報通信学会関西支部活動功労賞　（電子情報通信学会関西支部）
2020 年 10 月	情報処理学会コンピュータセキュリティシンポジウム最優秀デモンストレーション賞　（情報処理学会コンピュータセキュリティシンポジウムプログラム委員会）
2021 年　3 月	電子情報通信学会教育功労賞　（電子情報通信学会）
2021 年　8 月	情報処理学会マルチメディア，分散，協調とモバイルシンポジウム（DICOMO 2021）優秀論文賞　（情報処理学会 DICOMO シンポジウムプログラム委員会）
2022 年　1 月	暗号と情報セキュリティシンポジウムイノベーション論文賞　（電子情報通信学会情報セキュリティ研究専門委員会）
2023 年　6 月	電子情報通信学会情報通信システムセキュリティ研究賞　（電子情報通信学会情報通信システムセキュリティ研究専門委員会）

教　育　研　究　上　の　業　績

（著　　書）

1. 白石善明
   コンピュータネットワークの高信頼化に関する研究
   徳島大学博士論文，全 63p.（2000）
2. 森井昌克，曽根直人，白石善明，他 4 名
   ここからはじめる オペレーティングシステム基礎の基礎 Windows2000 システム編，ソフトバンクパブリッシング社，2002 年
   （分担執筆）第 2 章 pp.51-90 を担当
3. 堀内克明他編，白石善明，他 215 名
   プロフェッショナル英和辞典 SPED TERRA 物質・工学編，小学館，2004 年

（分担執筆）情報通信工学分野の 150 程度の項目を担当

4. 神保雅一，白石善明，他 7 名
暗号とセキュリティ，オーム社，2010 年
（分担執筆）第 9 章 pp.105-119 を担当

5. 小澤誠一他編，白石善明，他 12 名
データサイエンスの考え方，オーム社，2021 年
（分担執筆）第 13 章 pp.247-260 を担当

(学 術 論 文)

※ Web of Science に登録されている学術誌等に掲載されている論文等
(a. 学会誌，専門誌等に掲載された論文)

1. 森井昌克，白石善明，他 4 名
広域インターネット上での静止および動画像配送実験
画像電子学会誌，第 27 巻，第 3 号，pp.253-262，1998 年

2. 白石善明，白河芳徳，他 3 名
プロキシキャッシュサーバによる地域 HTTP-IXP の構築とその評価実験
システム制御情報学会論文誌，Vol.13，No.4，pp.168-178，2000 年

3. 白石善明，森井昌克，他 2 名
非線形コンバイナ型乱数生成器の特性 ― 線形複雑度，相互情報量，無相関性について ―
電子情報通信学会論文誌 A，Vol.J83-A，No.10，pp.1169-1179，2000 年

4. 白石善明，福田洋治，森井昌克
ネットワークのサービス品質管理を容易化するセキュリティプロトコルの一方式
電子情報通信学会論文誌 D-I，Vol.J85-D-I, No.7, pp.614-625，2002 年

5. 竹森敬祐，田中俊昭，中尾康二，大東俊博，三宅崇之，白石善明，森井昌克
Web サーバリモート監視システムの実装および評価
情報処理学会論文誌，第 43 巻，第 8 号，pp.2542-2551，2002 年

6. 白石善明，孝富士武史，森井昌克
パケット往復時間の予測誤差を使った乱数生成法
情報処理学会論文誌，第 44 巻，第 8 号，pp.2170-2177，2003 年

7.※ Y. Fukuta, Y. Shiraishi, M. Morii,
A Method for Improving Fast Correlation Attack Using Parity Check Equations Modifications
IEICE Trans. Fundamentals, Vol.E86-A, No.8, pp.2155-2158, 2003

8.※ Y. Shiraishi, T. Ohigashi, M. Morii,
Internal-State Reconstruction of a Stream Cipher RC4
IEICE Trans. Fundamentals, Vol.E86-A, No.10, pp.2636-2638, 2003

9. 中居大昭，岩野桂太，毛利公美，福田洋治，白石善明
特定少数グループ向け P2P 型バックアップシステム
情報科学技術レターズ，第 5 巻，pp.411-414，2006 年

10. 市川幸宏，伊沢亮一，白石善明，森井昌克
メモリ上に展開されたコードを使うウイルス解析支援システム
情報処理学会論文誌，第 47 巻，第 8 号，pp.2524-2534，2006 年

11. 福田洋治，白石善明，森井昌克
組織内システムにおいてエンティティの行動を管理するネットワークサービスアクセス制御
電子情報通信学会論文誌 D，Vol.J89-D，No.12，pp.2564-2578，2006 年

12. 越智洋司，大西佑樹，井口信和，白石善明，向井苑生
顔認識技術を利用した受講者撮影支援システムの提案と試作
教育システム情報学会誌，Vol.24，No.4，pp.301-310，2007 年

13.※ T. Ohigashi, Y. Shiraishi, M. Morii
New Weakness in the Key-Scheduling Algorithm of RC4
IEICE Trans. Fundamentals, Vol.E91-A, No.1, pp.3-11, 2008

14. 矢口隆明，岩田彰，白石善明
在宅介護サービスにおける現場知を基にしたチームケアの知識流通システムの開発と評価
情報文化学会誌，第 16 巻，第 2 号，pp.12-20，2009 年

15. 白石善明，福田洋治，他 2 名
社会ネットワーク分析を用いたスパム対策：固有ベクトル中心性に基づくメールフィルタリング
情報処理学会論文誌，第 51 巻，第 3 号，pp.1-11，2010 年

16. 矢口隆明，岩田彰，白石善明，横山淳一
チームケアの知識流通支援システムの開発と評価 －在宅ケアサービス記録の電子的共有に基づく情報連携－
日本医療情報学会論文誌「医療情報学」，第 29 巻，第 2 号，pp.63-73，2010 年

17. Y. Shiraishi, M. Mohri, Y. Fukuta
A Server-Aided Computation Protocol Revisited for Confidentiality of Cloud Service
Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol.2, No.2, pp.83-94, 2011

18. 毛利公美，伴拓也，白石善明
ActionScript による η_Tペアリング演算ライブラリー
電子情報通信学会論文誌 D，Vol.J95-D，No.4，pp.799-811，2012 年

19. 掛井 将平，脇田 知彦，毛利 公美，白石 善明，野口 亮司
TPM を用いたオフライン型タイムスタンプ
情報処理学会論文誌，第 53 巻，第 9 号，pp.2117-2129，2012 年

20. 榊原宏章，白石善明，岩田彰
低消費電力化のための実行タスクの動的なプロセッサリソース割り当て方式
情報処理学会論文誌 コンシューマ・デバイス＆システム，Vol.3，No.3，pp.11-19，2013 年

21. 掛井将平，毛利公美，白石善明
TPM を用いた順序認証システムのためのアプリケーションフレームワーク
電子情報通信学会論文誌 D，Vol.J97-D，No.3，pp.514-522，2014 年

22. 岡崎亮介，廣友雅徳，毛利公美，白石善明
平時から災害時へ連続的に利用可能な被災者を直接的に支援するデュアルパーパス情報共有システム
情報処理学会論文誌，第 55 巻，第 8 号，pp.1778-1786，2014 年

23. 奥村香保里，毛利公美，白石善明，岩田彰
プライバシー情報を登録する利用者の安心感の要因に関する調査
情報処理学会論文誌，第 55 巻，第 9 号，pp.2159-2167，2014 年

24. 成瀬猛，毛利公美，白石善明
前方秘匿性を満たす属性失効機能付き属性ベース暗号
情報処理学会論文誌，第 55 巻，第 10 号，pp.2256-2264，2014 年

25. 岡崎亮介，毛利公美，白石善明

複数の SNS と連携する災害時支援システムのアプリケーション開発のためのデータ入出力統合フレームワーク
電子情報通信学会論文誌 D，Vol.J97-D，No.12，pp.1696-1700，2014 年

26. 福田洋治，白石善明，毛利公美
イベント・アクション制御に基づくファイルシステムの提案
電子情報通信学会論文誌 D，Vol.J97-D，No.12，pp.1701-1704，2014 年

27. 白石善明，神薗雅紀，他 2 名
Windows API フックを用いた通信監視による不正な PDF ファイルの検知
電子情報通信学会論文誌 D，Vol.J97-D，No.12，pp.1719-1721，2014 年

28. 福田洋治，白石善明，毛利公美
当事者のプライバシーを考慮したログの保管とその監査の手法
電子情報通信学会論文誌 D，Vol.J97-D，No.12，pp.1729-1732，2014 年

29. M. Sato, M. Mohri, H. Doi, Y. Shiraishi,
Ciphertext Diverge-Merge Scheme of Identity-Based Encryption for Cloud-Based File Transmission Service
International Journal of Digital Information and Wireless Communications, Vol.5, No.1, pp.52-59, 2015

30. 奥村香保里，毛利公美，白石善明，岩田彰
情報システム・サービスの利用者の安心感と納得感の要因に関する調査
情報処理学会論文誌，第 56 巻，第 3 号，pp.932-941，2015 年

31.※ T. Naruse, M. Mohri, Y. Shiraishi
Provably secure attribute-based encryption with attribute revocation and grant function using proxy re-encryption and attribute key for updating
Human-centric Computing and Information Sciences, Vol.5, No.8, 13pages, 2015

32. T. Nakai, H. Muller, E. Bagarinao, K. Tomida, Y. Shiraishi, M. Niinimaki
A review of medical grids and their direction - A Swiss/Japanese perspective
International Journal of Research Studies in Computing, Vol.4, No.1, pp.15-23, June 2015

33. K. Tomida, H. Doi, M. Mohri, Y. Shiraishi
Ciphertext Divided Anonymous HIBE and Its Transformation to Identity-Based Encryption with Keyword Search
Journal of Information Processing, Vol.23, No.5, pp.562-569, Sep. 2015

34. M. Sato, M. Mohri, H. Doi, Y. Shiraishi
Partially Doubly-Encrypted Identity-Based Encryption Constructed from a Certain Scheme for Content Centric Networking
Journal of Information Processing, Vol.24, No.1, pp.2-8, Jan. 2016

35.※ S. Kakei，M. Mohri, Y. Shiraishi, M. Morii
SSL Client Authentication with TPM
IEICE Transactions on Information and Systems, Vol.E99-D, No.4, pp.1052-1061, April 2016

36.※ H. Tian, Y. Otsuka, M. Mohri, Y. Shiraishi, and M. Morii
Leveraging In-Network Caching in Vehicular Network for Content Distribution
International Journal of Distributed Sensor Networks, vol. 2016, Article ID 8972950, 9 pages, 2016. DOI:10.1155/2016/8972950

37. 福田洋治，白石善明，毛利公美
プライバシー保護と法的証明力確保を伴うログの部分開示の一方式
電子情報通信学会和文論文誌 D，Vol.J99-D, No.10, pp.1022-1033, 2016 年

38. 廣友雅徳，阿比留咲紀，一ノ瀬渚，福田洋治，毛利公美，白石善明
医療情報システム利用者の安心感の要因に関する調査
電子情報通信学会和文論文誌 D，Vol.J99-D, No.10, pp.1050-1054, 2016 年

39. M. Alowish, Y. Takano, Y. Shiraishi, M. Morii
Performance Evaluation of a Cluster Based Routing Protocol for VANETs
Journal of Communications, Vol.12, No.2, pp.137-144, February 2017

40.※ K. Nomura, M. Mohri, Y. Shiraishi, M. Morii
Multi-Group Signature Scheme for Simultaneous Verification by Neighbor Services
IEICE Transactions on Information and Systems, Vol.E100-D, No.8, pp.1770-1779, August 2017

41.※ K. Nomura, M. Mohri, Y. Shiraishi, M. Morii
Attribute Revocable Multi-Authority Attribute-Based Encryption with Forward Secrecy for Cloud Storage
IEICE Transactions on Information and Systems, Vol.E100-D, No.10, pp.2420-2431, October 2017

42.※ Y. Shiraishi, K. Nomura, 他 3 名
Attribute Revocable Attribute-Based Encryption with Forward Secrecy for Fine-Grained Access Control of Shared Data
IEICE Transactions on Information and Systems, Vol.E100-D, No.10, pp.2432-2439, October 2017

43.※ Y. Shiraishi, M. Hirotomo, 他 2 名
Delivering CRL with Low Bit Rate Network Coded Communication for ITS
IEICE Transactions on Information and Systems, Vol.E100-D, No.10, pp.2440-2448, October 2017

44.※ Y. Shiraishi, M. Kamizono, 他 2 名
Multi-Environment Analysis System for Evaluating the Impact of Malicious Web Sites Changing Their Behavior
IEICE Transactions on Information and Systems, Vol.E100-D, No.10, pp.2449-2457, October 2017

45. 古川凌也，永井達也，熊谷裕志，神薗雅紀，白石善明，他４名
Android アプリケーションのライブラリからみた脆弱性分析
情報処理学会論文誌，第 58 巻，第 12 号，pp.1843-1855，2017 年

46. 西尾祐哉，廣友雅徳，神薗雅紀，福田洋治，毛利公美，白石善明
マルチ環境解析と JavaScript 解析を組み合せた悪性 Web サイトのクローキング分析手法
情報処理学会論文誌，第 59 巻，第 9 号，pp.1624-1638，2018 年

47. 伊藤大貴，永井達也，野村健太，近藤秀紀，神薗雅紀，白石善明，他５名
スレットインテリジェンスのためのダイアモンドモデルに基づく脅威情報分析システム
電子情報通信学会論文誌（D），Vol.J101-D，No.10，pp.1427-1437，2018 年

48.※ D. Ito, K. Nomura, M. Kamizono, Y. Shiraishi, 他 3 名
Modeling Attack Activity for Integrated Analysis of Threat Information
IEICE Transactions on Information and Systems, Vol.E101-D, No.11, pp.2658-2664, 2018

49.※ H. Ito, M. Hirotomo, Y. Fukuta, M. Mohri, Y. Shiraishi
Zero-Knowledge Identification Scheme Using LDPC Codes
IEICE Transactions on Information and Systems, Vol.E101-D, No.11, pp.2688-2697, 2018

50. 竹尾淳，稲吉陽一朗，白石善明，他 3 名
HPKI 認証の特長を考慮した在宅医療介護システムにおける患者情報の開示先制御
情報処理学会論文誌，第 60 巻，第 6 号，pp.1228-1237，2019 年

51.※ H. Tian, Y. Shiraishi, 他 2 名
CCN-Based Vehicle-to-Vehicle Communication in DSRC for Content Distribution in Urban

Environments
IEICE Transactions on Information and Systems, Vol.E102-D No.9, pp.1653-1664, 2019.

52.※ T. Nagai, M. Kamizono, Y. Shiraishi, 他 4 名
A Malicious Web Site Identification Technique Using Web Structure Clustering
IEICE Transactions on Information and Systems, Vol.E102-D No.9, pp.1665-1672, 2019.

53.※ T. Tsuchida, M. Takita, Y. Shiraishi, 他 3 名
Authentication Scheme Using Pre-Registered Information on Blockchain
IEICE Transactions on Information and Systems, Vol.E102-D, No.9, pp.1676-1678, 2019.

54.※ S. Nakagawa, T. Nagai, H. Kanehara, K. Furumoto, M. Takita, Y. Shiraishi, 他 4 名
Character-Level Convolutional Neural Network for Predicting Severity of Software Vulnerability from Vulnerability Description
IEICE Transactions on Information and Systems, Vol.E102-D, No.9, pp.1679-1682, 2019.

55. T. Nagai, M. Takita, K. Furumoto, Y. Shiraishi, 他 4 名
Understanding Attack Trends from Security Blog Posts Using Guided-topic Model
Journal of Information Processing, Vol.27, pp.802-809, 2019.

56.※ Y. Takano, H.-J. Su, Y. Shiraishi, M. Morii
A spatial-temporal subspace-based compressive channel estimation technique in unknown interference MIMO channels
IEEE Transactions on Signal Processing, vol.68, pp.300-313, DOI 10.1109/TSP.2019.2959223, 2019.

57.※ M. Alowish, Y. Shiraishi, 他 3 名
A novel software-defined networking controlled vehicular named-data networking for trustworthy emergency data dissemination and content retrieval assisted by evolved interest packet
International Journal of Distributed Sensor Networks, vol.16, no.3, 12 pages, 2020, DOI 10.1177/1550147720909280.

58.※ M. Alowish, Y. Shiraishi, 他 3 名
Stabilized Clustering Enabled V2V Communication in NDN-SDVN Environment for Content Retrieval
IEEE Access, vol. 8, pp.135138-135151, 2020.

59.※ S. Kakei, Y. Shiraishi, 他 4 名
Cross-Certification towards Distributed Authentication Infrastructure: A Case of Hyperledger Fabric
IEEE Access, vol. 8, pp. 135742-135757, 2020.

60.※ K. Nomura, Y. Shiraishi, 他 2 名
Secure Association Rule Mining on Vertically Partitioned Data Using Private-Set Intersection
IEEE Access, vol. 8, pp. 144458-144467, 2020.

61. 古川 凌也, 白石 善明, 森井 昌克
SoK：データ駆動型社会に向けたセキュリティ分野へのオントロジの活用に関する一考察
情報処理学会論文誌，第 61 巻，第 12 号，pp.1802-1813，2020 年.

62. T.T. Thein, Y. Ezawa, S. Nakagawa, K. Furumoto, Y. Shiraishi, 他 3 名
Paragraph-based Estimation of Cyber Kill Chain Phase from Threat Intelligence Reports
Journal of Information Processing, vol.28, pp.1025-1029, 2020.

63.※ R. Nagasawa, K. Furumoto, M. Takita, Y. Shiraishi, 他 4 名
Partition-then-Overlap Method for Labeling Cyber Threat Intelligence Reports by Topics over Time
IEICE Transactions on Information and Systems, Vol.E104-D, No.5, pp.556-561, 2021.

64. 中川舜太，白石善明，他 3 名
単語のトピック固有度を用いた脆弱性記述に基づく脆弱性特性の自動評価

情報処理学会論文誌，第 62 巻，第 12 号，pp.2024-2028，2021 年.

65. 廣友雅徳，池田貴志，福田洋治，毛利公美，白石善明
ブロックチェーンを用いたログ保存システム
電子情報通信学会論文誌，Vol.J105-D，No.1，pp.106-109，2022.

66.※ M. Alowish, Y. Shiraishi, 他 2 名
Three Layered Architecture for Driver Behavior Analysis and Personalized Assistance with Alert Message Dissemination in 5G Envisioned Fog-IoCV
Future Internet, vol.14, no.1, DOI:10.3390/fi14010012, 29pages, 2022.

67.※ C. Tomita, M. Takita, K. Fukushima, Y. Nakano, Y. Shiraishi, M. Morii
Extracting the Secrets of OpenSSL with RAMBleed
Sensors, Vol.22, No.3586, 17pages, 2022.

68.※ N. Yoshimura, H. Kuzuno, Y. Shiraishi, M. Morii
DOC-IDS: A Deep Learning-Based Method for Feature Extraction and Anomaly Detection in Network Traffic
Sensors, Vo.22, No.4405, 19pages, 2022.

69. 添田綾香，長澤龍成，白石善明，他 4 名
サイバー攻撃分析のためのセキュリティレポート検索システム
電子情報通信学会論文誌（D），Vol. J105-D, No. 10, pp.603-613，2022.

70.※ Y. Osada, R. Nagasawa, Y. Shiraishi, 他 5 名
Multi-labeling with topic models for searching security information
Annals of Telecommunications, Springer, Vol. 77, pp.777-788, 2022.

71. 松井勇太，白石善明，他 5 名
グラフ埋め込みによる Ethereum の不正取引アカウント検知
情報処理学会論文誌，Vol. 63, No. 12, pp.1770-1775，2022.

72.※ Y. Ezawa, S. Kakei, Y. Shiraishi, 他 2 名
Blockchain-based Cross-Domain Authorization System for User-Centric Resource Sharing
Blockchain: Research and Applications, Vo.22, No.4405, 19pages, 2023.

73. K. Kumagai, S. Kakei, Y. Shiraishi, S. Saito
Distributed Public Key Certificate-Issuing Infrastructure for Consortium Certificate Authority using Distributed Ledger Technology
Security and Communication Networks, Article ID 9559439, 20pages, 2023.

74.※ K. Nomura, Y. Takata, H. Kumagai, M. Kamizono, Y. Shiraishi, 他 2 名
Investigations of electronic signatures for construction of trust services
IEICE Transactions on Information and Systems, Vol.E106-D, No.9, pp.1436-1451, 2023. [Invited Paper]

75.※ T.T. Thein, Y. Shiraishi, M. Morii
Few-shot Learning-based Malicious IoT Traffic Detection with Prototypical Graph Neural Networks
IEICE Transactions on Information and Systems, Vol.E106-D, No.9, pp.1480-1489, 2023.

76.※ T.T. Thein, Y. Shiraishi, M. Morii
Malicious domain detection based on decision tree
IEICE Transactions on Information and Systems, Vol.E106-D, No.9, pp.1490-1494, 2023.

77.※ S. Kakei, H. Seko, Y. Shiraishi, S. Saito
Design of Enclosing Signing Keys by All Issuers in Distributed Public Key Certificate-Issuing Infrastructure

IEICE Transactions on Information and Systems, Vol.E106-D, No.9, pp.1495-1498, 2023.

78.※ T.T. Thein, Y. Shiraishi, M. Morii
Personalized federated learning-based intrusion detection system: Poisoning attack and defense
Future Generation Computer Systems, Vol.153, pp.182-192, DOI:10.1016/j.future.2023.10.005, 2024.

(b. 国際会議等の Proceedings に掲載された論文)

1. Y. Shiraishi, M. Morii, 他 2 名
On a Secure Design of Nonlinear Combiner Generator for Stream Cipher
Proc. of 1998 International Symposium on Information Theory and Its Applications, pp.44-47, 1998

2. Y. Shiraishi, M. Morii
On Differential Correlation Immunity of Nonlinear Combiner Generator with Memory for Stream Ciphers
Proc. of 2000 International Symposium on Information Theory and Its Applications, pp.66-69, 2000

3. Y. Shiraishi, M. Morii
A Stream Cipher System Using Nonlinear Combiner Generator with Reconfigurable LFSRs
Proc. of 2002 International Symposium on Information Theory and Its Applications, pp.643-646, 2002

4. Y. Fukuta, Y. Shiraishi, M. Morii
Improvement of Fast Correlation Attack using Parity Check Equations
Proc. of 2002 International Symposium on Information Theory and Its Applications, pp.659-662, 2002

5. Y. Shiraishi, T. Kuribayashi, M. Morii
Center Management Type Intrusion Detection System
Proc. of the 7th World Multiconference on Systemics, Cybernetics and Informatics, Vol.III, pp.377-381, 2003

6. Y. Shiraishi, Y. Fukuta, M. Morii
Remote Access VPN with Port Protection Function by Mobile Codes
Proc. of the 4th International Workshop on Information Security Applications, Lecture Notes in Computer Science, Vol.2908, pp.16-26, 2003

7. Y. Shiraishi, T. Ohigashi, M. Morii
An Improved Internal-State Reconstruction Method of a Stream Cipher RC4
Proc. of the IASTED International Conference on Communication, Network, and Information Security, pp.132-135, 2003

8. Y. Shiraishi, Y. Fukuta, M. Morii
Port Randomized VPN by Mobile Codes
Proc. of 2004 IEEE Consumer Communications and Networking Conference, pp.671-673, 2004

9. Y. Fukuta, Y. Shiraishi, M. Morii
Performance Analysis of APP Decoding-Based Fast Correlation Attacks
Proc. of 2004 International Symposium on Information Theory and its Applications, pp.953-958, 2004

10. Y. Shiraishi, Y. Fukuta, M. Morii
Access Control by Service Connector with Single Sign-On Function
Proc. of the 9th World Multiconference on Systemics, Cybernetics and Informatics, Vol.II, pp.255-259, 2005

11. T. Ohigashi, Y. Shiraishi, M. Morii
FMS Attack-Resistant WEP Implementation Is Still Broken ---Most IVs Leak A Part of Key Information---
Proc. of 2005 International Conference on Computational Intelligence and Security, Lecture Notes in

Artificial Intelligence, Vol.3802, Part II, pp.17-26, 2005

12. T. Ohigashi, Y. Shiraishi, M. Morii
A Categorizing-Guessed-Values Approach for the Key Recovery Attack against WEP
Proc. of 2006 International Symposium on Information Theory and its Applications, pp.403-408, 2006

13. Y. Shiraishi, Y. Fukuta, M. Morii
A Filter Check System for Defeating Attacks which employ IP Source Address Spoofing
Proc. of the 11th World Multi-Conference on Systemics, Cybernetics and Informatics, Vol.II, pp.289-292, 2007

14. Y. Ochi, Y. Etoh, N. Iguchi, S. Mizobuchi, Y. Shiraishi, 他 5 名
A Practice of Interactive English Class On a Multipoint/Interactive Remote Lecture Environment
Proc. of the 8th International Conference on Information Technology Based Higher Education and Training, pp.294-297, 2007

15. T. Yamamoto, Y. Fukuta, M. Mohri, M. Hirotomo, Y. Shiraishi
A Distribution Scheme of Certificate Revocation List by Inter-Vehicle Communication using a Random Network Coding
Proc. of 2012 International Symposium on Information Theory and its Applications, pp.392-395, 2012

16. T. Matsukawa, T. Yamamoto, Y. Fukuta, M. Hirotomo, M. Mohri, Y. Shiraishi
Controlling Signature Verification of Network Coded Packet on VANET
Proc. of the 12th International Conference on ITS Telecommunications, pp.679-683, 2012

17. S. Kakei, M. Mohri, Y. Shiraishi, R. Noguchi
Offline Time-Stamping System: Its Design and Implementation
Proc. of the 2012 IEEE International Conference on Control System, Computing and Engineering, pp.404-409, 2012

18. S. Kakei, M. Mohri, Y. Shiraishi, R. Noguchi
Offline Time-Stamping Using TPM and Its Java Library
Proc. of the 2012 IEEE Symposium on Computer Applications and Industrial Electronics, pp.64-69, 2012

19. T. Hirai, M. Hirotomo, M. Mohri, Y. Shiraishi
Migration of Application Data to REST-Based Online Storage Service
Proc. of the 7th Ubiquitous Information Technologies and Applications, Lecture Notes in Electrical Engineering, No.214, pp.223-231, 2012

20. K. Tomida, M. Mohri, Y. Shiraishi
Keyword Searchable Encryption with Access Control from a Certain Identity-Based Encryption
Proc. of the 8th International Conference on Future Information Technology, Lecture Notes in Electrical Engineering, No.276, pp.113-118, 2013

21. T. Naruse, M. Mohri, Y. Shiraishi
Attribute-Based Encryption with Attribute Revocation and Grant Function Using Proxy Re-encryption and Attribute Key for Updating
Proc. of the 8th International Conference on Future Information Technology, Lecture Notes in Electrical Engineering, No.276, pp.119-125, 2013

22. M. Sato, M. Mohri, H. Doi, Y. Shiraishi
Doubly Encrypted Identity-Based Encryption for File Transfer Service
Proc. of the 8th International Conference on Future Information Technology, Lecture Notes in Electrical Engineering, No.276, pp.139-144, 2013

23. Y. Kitamura, M. Mohri, Y. Shiraishi, A. Iwata
Direct Accessible Filter Using Succinct Data Structure for Packet Filtering
Proc. of 2014 Second International Symposium on Computing and Networking, pp.514-518, 2014

24. H. Tian, Y. Otsuka, M. Morhi, Y. Shiraishi, M. Morii
LCE In-Network Caching on Vehicular Networks for Content Distribution in Urban Environments
Proc. of the Seventh International Conference on Ubiquitous and Future Networks, pp.551-556, 2015.

25. Y. Shiraishi, M. Mohri, 他 2 名
A Three-Party Optimistic Certified Email Protocol Using Verifiably Encrypted Signature Scheme for Line Topology
The 2nd IEEE International Conference on Cyber Security and Cloud Computing, pp.260-265, Nov. 2015.

26. Y. Kitamura, M. Mohri, Y. Shiraishi, A. Iwata
Storage-Efficient Tree Strucure with Level-Ordered Unary Degree sequence for Packet Classification
Proc. of 2015 Third International Symposium on Computing and Networking, pp.487-490, Dec. 2015.

27. K. Nomura, M. Mohri, Y. Shiraishi, M. Morii
Attribute Revocable Attribute-Based Encryption for Decentralized Disruption-Tolerant Military Networks
Proc. of 2015 Third International Symposium on Computing and Networking, pp.491-494, Dec. 2015.

28. D. Ito, M. Mohri, Y. Shiraishi, M.Morii
Cloud Storage with Key-Value Stores over Content-Centric Networking Architecture
Proc. of 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, 6pages, Oct. 2016.

29. D. Ito, M. Mohri, Y. Shiraishi, M. Morii
Virtual Storage and Area Limited Data Delivery over Named Data Networking
Proc. of 14th Annual IEEE Consumer Communications & Networking Conference, pp.95-102, Jan. 2017.

30. K. Nomura, M. Mohri, Y. Shiraishi, M. Morii
A Multi-Group Signature Scheme for Local Broadcasting
Proc. of 14th Annual IEEE Consumer Communications & Networking Conference, pp.449-454, Jan. 2017.

31. M. Hirotomo, Y. Nishio, M. Kamizono, Y. Fukuta, M. Mohri, Y. Shiraishi
Efficient Method for Analyzing Malicious Websites by Using Multi-Environment Analysis System
Proc. of 12th Asia Joint Conference on Information Security, pp.48-54, Aug. 2017.

32. Y. Shiraishi, Y. Fukuta, 他 2 名
Estimating and Forwarding Unreceived Symbols for Random Network Coded Communication
Proc. of 11th International Conference on Computational Intelligence and Communication Networks, pp.53-57, Jan. 2019.

33. Y. Ezawa, M. Takita, Y. Shiraishi, 他 5 名
Designing Authentication and Authorization System with Blockchain
Proc. of 14th Asia Joint Conference on Information Security, pp.111-118, Aug. 2019.

34. M. Hirotomo, H. Ito, Y. Fukuta, M. Mohri, Y. Shiraishi
Identification Scheme Based on the Binary Syndrome Decoding Problem Using High-Density Parity-Check Matrices
Proc. of 14th Asia Joint Conference on Information Security, pp.127-133, Aug. 2019.

35. T. Tsuchida, M. Hirotomo, H. Ito, M. Takita, Y. Shiraishi, 他 4 名
A Signature Scheme Based on the Syndrome Decoding Problem Using LDPC Codes
Proc. of 14th Asia Joint Conference on Information Security, pp.142-145, Aug. 2019.

36. S. Ogiso, M. Mohri, Y. Shiraishi
Transparent Provable Data Possession Scheme
Proc. of IEEE International Symposium on Networks, Computers and Communications, 5 pages, Oct. 2020.

37. S. Kakei, Y. Shiraishi, S. Saito
Simplifying Dynamic Public Key Certificate Graph for Certification Path Building in Distibuted Public Key Infrastructure
Proc. of the 12th International Conference on ICT Convergence, 6 pages, Oct. 2021.

38. T. Tsutsui, Y. Shiraishi, M. Morii
Systemization of Vulnerability Information by Ontology for Impact Analysis
2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion, pp.1126-1134, 2021.

39. R. Furukawa, D. Ito, Y. Takata, H. Kumagai, M. Kamizono, Y. Shiraishi, M. Morii
Fake News Detection via Biased User Profiles in Social Networking Sites
The 20th IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, pp.136-145, 2021.

40. Y. Takano, H.-J. Su, Y. Shiraishi, M. Morii
A Cache-Aided Power Optimization Technique for Adaptive Secure Transmission Systems
Proc. of 2022 IEEE 33rd Annual International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 1122-1127, 2022.

41. S. Kakei, Y. Shiraishi, S. Saito
Granting Access Privileges Using OpenID Connect in Permissioned Distributed Ledgers
Proc. of Security and Privacy in Communication Networks, pp. 290-308, 2022.

42. S. Nakajima, T. Inoue, Y. Shiraishi, M. Morii
Attack Techniques and Countermeasures against Kr00k using CSA
Proc. of the tenth International Symposium on Computing and Networking, pp.130-136, 2022.

43. K. Kimura, Y. Shiraishi, M. Morii
A New Approach to Disabling SSL/TLS: Man-in-the-Middle Attacks are still Effective
Proc. of the eleventh International Symposium on Computing and Networking, 2023. (in print)

44. T. Inoue, K. Kuriyama, Y. Shiraishi, M. Morii
Encryption Invalidation Attacks: Is your Wi-Fi encryption really working?
Proc. of the eleventh International Symposium on Computing and Networking, 2023. (in print)

45. S. Jung, K. Furumoto, T. Takahashi, Y. Shiraishi
Model Selection for Continuous Operation of Automated Vulnerability Assessment System
Proc. of ACM Conference on Computer and Communications Security, 2023. (in print)

(c．国内会議の論文集)

1. 矢田久美子，白石善明，毛利公美
アプリケーションの実装時組み込み型手順提示機構の提案と評価
第 8 回情報科学技術フォーラム講演論文集，第 4 巻，pp.101-108，2009 年

2. 矢田久美子，白石善明，毛利公美
情報共有を円滑にするための明示的な返信を不要とするコミュニケーションツール

第 9 回情報科学技術フォーラム講演論文集，第 4 巻，pp.147-150，2010 年

3. 白石善明，福山悠，毛利公美
グループ化した蓄積情報を活用する知識継承の一手法
第 10 回情報科学技術フォーラム講演論文集，第 4 巻，pp.147-152，2011 年

4. 白石善明，佐々木啓，他 2 名
センターから端末への動的なコードの配布・実行・検証機構
第 11 回情報科学技術フォーラム講演論文集，第 4 巻，pp.45-50，2012 年

5. 奥村晃弘，白石善明，岩田彰
スマートハウスにおける電力変動からの不正アクセス検知の検討
第 12 回情報科学技術フォーラム講演論文集，第 4 巻，pp.87-90，2013 年

6. 榊原宏章，白石善明，岩田彰
プロセッサ抽象化 API 利用アプリケーションの並列処理タスクへのプロセッシングエレメントの動的な配分機構の Android 実装
第 12 回情報科学技術フォーラム講演論文集，第 4 巻，pp.105-110，2013 年

7. 福田洋治，白石善明，他 2 名
医療クラウドサービスの間接的利用の不安因子について
第 13 回情報科学技術フォーラム講演論文集，第 4 巻，pp.59-62，2014 年

8. 白石善明，中井敏晴，他 4 名
長期追跡研究のための複数機関にある匿名化データの共有におけるセキュリティ対策の検討
第 14 回情報科学技術フォーラム講演論文集，第 4 巻，pp.61-64，2015 年

(d. 研究機関の紀要，報告等に掲載された論文)

該当なし

（学　術　講　演）

1. 鈴木貴史，白石善明，溝渕昭二
メールの送受信関係に基づくフィルタリングの提案とそのベイジアンフィルタとの連携
マルチメディア，分散，協調とモバイル（DICOMO2007）シンポジウム予稿集（CD-ROM），pp.481-492，2007 年

2. 村田純一，白石善明，福田洋治
内部攻撃を検知可能なモバイル端末向け動的グループ鍵共有プロトコル
マルチメディア，分散，協調とモバイル（DICOMO2008）シンポジウム予稿集（CD-ROM），pp.1007-1016，2008 年

3. 伴拓也，毛利公美，白石善明，野口亮司
ActionScript による η_Tペアリング演算ライブラリ
マルチメディア，分散，協調とモバイル（DICOMO2011）シンポジウム予稿集（CD-ROM），pp.1285-1295，2011 年

4. 成瀬猛，毛利公美，白石善明
前方秘匿性を満たす属性失効機能付き属性ベース暗号
マルチメディア，分散，協調とモバイル（DICOMO2013）シンポジウム予稿集（CD-ROM），pp.215-221，2013 年

5. T. Matsukawa, T. Yamamoto, Y. Fukuta, M. Hirotomo, M. Mohri, Y. Shiraishi
Reading Out Scheme for Digitally Signed Random Network Coded Communication on VANET
Technical Report of Information Processing Society of Japan (Intelligent Transport Systems), 2014-ITS-56(6), pp.1-7, 2014

6. 川原大弥, 山崎康平, 瀧田 愼, 白石善明, 森井昌克
ホログラム QR コードの開発 ～2 層化された QR コードとその原理～
暗号と情報セキュリティシンポジウム予稿集，2E4-1，8 ページ，2021 年

7. 添田綾香，長澤龍成，長田侑樹，白石善明，他 4 名
サイバー攻撃分析のためのセキュリティ情報検索システム
マルチメディア，分散，協調とモバイル（DICOMO2021）シンポジウム予稿集（CD-ROM），pp.874-882，2021 年

8. 榎本秀平，葛野弘樹，山田浩史，白石善明，森井昌克
ランサムウェアに対する実行遅延タスクスケジューラの提案と評価
電子情報通信学会情報通信システムセキュリティ研究会，vol.122, no.ICSS-244, pp.49-54，2022 年

（上記以外に 397 編）

論文等の略語の説明

ACM = Association for Computing Machinery
API = Application Programming Interface
APP = A Posteriori Probability
CCN = Content-Centric Networking
CRL = Certificate Revocation List
CRYPTREC = Cryptography Research and Evaluation Committees
CSA = Channel Switch Announcement
DICOMO = Multimedia, Distributed, Cooperative, and Mobile
DOC-IDS = Deep One-class Classification for Intrusion Detection System
DSRC = Dedicated Short-Range Communications
FMS = Fluhrer-Mantin-Shamir
HTTP-IXP = Hypertext Transfer Protocol-Internet Exchange Point
IASTED = International Association of Science and Technology for Development
ID = Identity
IEEE = Institute of Electrical and Electronics Engineers
IEICE = Institute of Electronics, Information and Communication Engineers
IoCV = Internet of Connected Vehicles
IoT = Internet of Things
IP = Internet Protocol
ITS = Intelligent Transport Systems
IV = Initialization Vector
Kr00k = Key Reinstallation Attacks
LAN = Local Area Network
LCE = Leave Copy Everywhere
LDPC = Low Density Parity Check
LFSR = Linear Feedback Shift Register
LOIS = Life Intelligence and Office Information Systems
MIMO = Multi-Input Multi-Output
NDN = Named Data Networking
OpenID = Open Identity
OpenSSL = Open Secure Socket Layer
P2P = Peer-to-Peer
QR = Quick Response
RC4 = Rivest's Cipher 4
REST = Representational State Transfer
SDVN = Software-Defined Vehicular Network
SNS = Social Networking Services
SoK = Systematization of Knowledge
SSL/TLS = Secure Socket Layer/Transport Layer Security
TPM = Trusted Platform Module
VANET = Vehicular Ad-Hoc Network
VPN = Virtual Private Network
WEP = Wired Equivalent Privacy
WIC = Web Intelligence Consortium
Wi-Fi = Wireless Fidelity
5G = 5th Generation