様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ５ 月　 ８ 日現在

機関番号：１５３０１
研究種目：挑戦的研究（開拓）
研究期間：2019～2023
課題番号：１９Ｈ０５５７９・２０Ｋ２０４８４

研究課題名（和文）ICTおよび暗号技術を駆使した医療情報セキュア管理システムの構築

研究課題名（英文）Construction of a medical information secure management system with ICT and encryption technology

研究代表者
野上　保之（Nogami, Yasuyuki）

岡山大学・環境生命自然科学学域・教授

研究者番号：６０３１４６５５

交付決定額（研究期間全体）：（直接経費）　　19,500,000円

研究成果の概要（和文）：インターネットを中心とするICT技術の急速な進化は、医療の分野にも大きな変革と新たな価値の創出をもたらす。ネット上に情報クラウドサーバを配置し、医師・患者・製薬メーカーなど参画メンバが各々に情報を提供し、これを共有することで高度な医療を提供する。共有される情報には、電子カルテ・ゲノムデータなど重要なものが含まれ、漏えい・改ざん されないよう運用されなければならない。ネットを活用することによる利便性を損なうことなく、極秘ビッグデータを守ることが要求される。そのような情報をいかに活用しながらも厳密に保護するか、そのような技術をどのように実現するかはAI・DX・BigData時代の喫緊の課題である。

研究成果の学術的意義や社会的意義
例えば臨床データ群は、数百フィールド×数十万人×（テキスト＋画像・ゲノムデータ）に及ぶ複雑な極秘ビッグデータとなる。これに対し、広く使われているAES暗号や楕円曲線暗号をそのまま用いるのではなく、従来にないアプローチとして、数学的に「同型」と呼ばれる構造を巧みに用いることで、無数の暗号計算の組み合わせと暗号データの表現方法により構成し、これらをシャッフルして用いることで、そのデータがどのように暗号化されているか識別できないようにする「暗号拡散法」を開発する。この暗号技術をベースとしつつ、新たな秘密分散法を組合せ、利便性を損なわない、極めてセキュアな医療情報データベース構築法が実現される。

研究成果の概要（英文）：The rapid evolution of ICT technology, centered on the Internet, will bring about major changes and the creation of new value in the medical field. An information cloud server will be placed on the internet, and participating members such as doctors, patients, and pharmaceutical manufacturers will each provide information and share it to provide advanced medical care. The information to be shared includes important information such as electronic medical records and genome data, and must be operated to prevent leakage or falsification. It is necessary to protect confidential big data without sacrificing the convenience of using the Internet. How to utilize such information while strictly protecting it, and how to implement such technology, are urgent issues in the age of AI, DX, and Big Data.

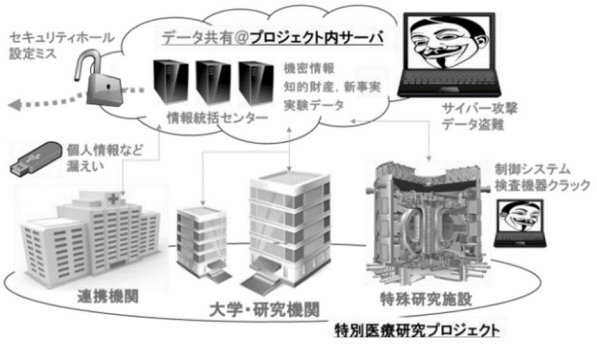
研究分野：情報セキュリティ

キーワード：情報セキュリティ　メールセキュリティ　暗号　秘密分散

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属します。

１．研究開始当初の背景

インターネットを中心とするICT技術の急速な進化は、医療の分野にも大きな変革と新たな価値の創出をもたらす。ネット上に情報クラウドサーバを配置し、医師・患者・製薬メーカーなど参画メンバが各々に情報を提供し、これを共有することで高度な医療を提供する。共有される情報には、電子カルテ・ゲノムデータなど重要なものが含まれ、漏えい・改ざん されないよう運用されなければならない（右図）。しかし現実は、人間がシステム全体を見渡すことはできず、サイバー攻撃などによる情報漏えいが危惧される。ネットを活用することによる利便性を損なうことなく、極秘ビッグデータを守ることが要求される。そのような情報をいかに活用しながらも厳密に保護するか、そのような技術をどのように実現するかはAI・DX・BigData時代の喫緊の課題である。

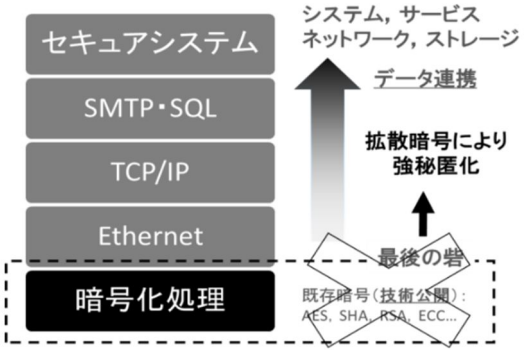


２．研究の目的

本研究では、岡山大学で研究を進める次世代のがん治療法であるホウ素中性子捕捉療法（BNCT）の臨床データ群を主たるターゲットとして、未来の日本の医療を代表する技術・知財・臨床データを、ICT技術および暗号技術を高度に駆使して、利便性を損うことなく、かつ強固に守る高度な医療情報セキュリティ技術の確立を目指す。具体的には、その臨床データ群は数百フィールド×数十万人×（テキスト＋画像・ゲノムデータ）に及ぶ複雑な極秘ビッグデータとなる。これに対し、広く使われているAES暗号や楕円曲線暗号をそのまま用いるのではなく、従来にないアプローチとして、数学的に「同型」と呼ばれる構造を巧みに用いることで、無数の暗号計算の組み合わせと暗号データの表現方法により構成し、これらをシャッフルして用いることで、そのデータがどのように暗号化されているか識別できないようにする「暗号拡散法」を開発する。無線通信技術における周波数拡散法から着想を得ている。この暗号技術をベースとしつつ、新たな秘密分散法を組合せ、電子メール・リモート閲覧などの利便性を損なわない、極めてセキュアな医療情報データベース構築法を開発する。

３．研究の方法

本研究では、次世代の医療情報システム・医療機器クラウド連携システムの根幹となり得る、セキュア医療情報データベースシステムの構築を試みる。具体的には、広く使われているAES暗号や楕円曲線暗号をそのまま用いるのではなく、「同型」と呼ばれる数学的な写像構造を巧みに用いることで、無数の暗号計算の組合せと暗号データの表現方法により、医療情報の「強秘匿化」を実現する。同型で無数の写像構造をシャッフルして用いることで、そのデータがどの方式で暗号化されているか識別できないようにする「暗号拡散法（拡散暗号）」を開発する（右図）。無線通信技術における周波数拡散法（Frequency Hopping）から着想を得ている。これまでにも、国家機密・軍事機密を代表とする極秘情報は独自に暗号化されており、盗聴されても乱数と見分けがつかない。そのような拡散暗号と秘密分散法を組合せ、電子メール・リモート閲覧など利便性を損なうことなく、強秘匿化した医療情報データベースシステムを構築する。具体的には、(1)拡散暗号によりデータ暗号化とユーザ認証を実現するため、膨大な種類の非線形写像を用いた秘密鍵暗号と、柔軟に暗号強度を変えられる公開鍵暗号を開発し、これらによる暗号拡散法を提案し、一方でその厳密な安全性の評価を行う。そして、(2)拡散暗号による暗号化データを適切にブロック化して複数サーバに秘密分散保存・運用する手法を開発し、転送の際に発生するTCPインキャストの問題を回避しながら快適にデータ通信する手法を導入する。一方で、(3)様々なノウハウを含みうる電子メール・接続認証（ユーザ認証）についても(1)、(2)を適用してセキュアに運用できるようプロトコル実装する。



４．研究成果

データ暗号化・ユーザ認証のための拡散暗号とその安全性評価について、軽量暗号や検索可能な AES 暗号も含め、アルゴリズム開発を完了した。また、楕円曲線暗号と楕円ペアリング暗号の両方で、実装最適化のためのアルゴリズム効率化とそのスケーラビリティ（拡散するため）についての研究開発を進めている。とくに前者については、世界最高速実装を達成することができている（BLS 曲線を用いたペアリング暗号）。メールシステムについて、メールの送信者から受信者までのエンドツーエンドでの暗号化通信に対して拡散暗号方式を適用するために、電子メールクライアント Thunderbird の拡張に取り組んだ。まずは，GnuPG で実装された暗号方式を Thunderbird で利用するためのアドオンである Enigmail に対して動的プログラム解析を行い、Enigmail の動作を理解し Enigmail のソースコード内で GnuPG に対して暗号処理を依頼する箇所を特定した。続いて、疑似的な拡散暗号方式（GnuPG で実装済みであるが Enigmail では利用されていない暗号方式）を Enigmail で利用できるように、Enigmail のソースコードに対して拡張を施した。これに関連して、SELinuxCIL を利用した不要なセキュリティポリシ削減手法、および VMM によるプログラム実行時のライブラリ情報取得機能の設計についても検討を進めた。極秘ビッグデータ超セキュア化のための分散格納機構の開発については、本研究ではデータ量の削減手法を提案している。データを n 個のブロックに分割し、一定数のブロックを各サーバに保持するが、この際、任意の k 個のサーバが保持するすべてのブロックを集めることにより元データが復元できるように保持する。これにより、従来法に比して、データ量は各段に削減できる。

そのような過程により、これをメールデータの暗号化・ユーザ認証として実装するために Thunderbird に対して独自実装することができた。より具体的には、暗号強度を自在に変えることができる乗算アルゴリズムを C 言語および JavaScript として実装した。JavaScript 実装については、必ずしも大きな整数での実装が効率よく働かないため、本研究の成果が有効に働く。具体的には、30 ビット程度の整数演算をベースとしつつ、暗号の強度を上げるためにベクトルの次元数を上げることで 3000 ビットクラスの強度を実現する。その際に、安全性の観点からその群の位数が小さな素因数をもたないようにするために、十分安全な大きな素因数をもつようにパラメータを選択し、そのパラメータを用いることで実現する。一方で、その暗号の拡散性を実現するためのパラメータを自在に選べるようにできることを確認できた。そのようなことも踏まえ、その拡散性をセッションキー・ワンタイムパスワード的に使えるように実現した。その際の秘密分散法についてもより軽量化した実装として実現することができており、さらなる安全性強度を実現できる。なお、ユーザ認証に関しては、ElGamal 暗号および楕円曲線暗号をベースとした公開鍵認証を実装・実現している。

しかし以上のような効率化の一方で、ベクトル乗算アルゴリズムのあるパラメータの大小に計算効率が大きくかかわるため、このままではその計算処理時間の大小によってパラメータの大小が解析される可能性がある。したがって、当初よりそのパラメータをセッションキーのように用いる通信（メール通信）を考えていたが、そこにサイドチャネル的な攻撃の可能性が残ることとなる。この問題を解消するために、そのパラメータを自在に選べることは確保しつつも、その大小に大きく依存しない計算アルゴリズムを開発し、平均的に効率よくベクトル乗算を行えるものを提案・実装した。これを、具体的な医療データの暗号化の方にも実装する準備を進め、楕円曲線暗号をベースとした公開鍵認証のみでなく、さらなる安全性拡張を実施している。これは、実際に医療データを考えたとき、例えばゲノム情報など機微な個人情報をより厳格に保護するためである。そのための改ざん耐性やエビデンスの確保のためにブロックチェーン技術との相性について検討を進めた。具体的には、イーサリアムネットワークを用いた実現できている。しかし今後の課題としては、その際の手数料として発生する GAS 代を低減しなければならない。また更なる研究計画として、準同型暗号などと組み合わることも考えている。

以上をまとめると、拡散暗号方式を完成させ、これをメールデータの暗号化・ユーザ認証として実装するために Thunderbird に対して独自実装し、暗号強度を自在に変えることができる乗算アルゴリズムを C 言語および JavaScript として実装した。それは必ずしも大きな整数での実装が効率よく働かないため、その効率化い、合わせてサイドチャネル的な攻撃の可能性を発見し、そのパラメータを自在に選べることは確保しつつ、その大小に大きく依存しない計算アルゴリズムを開発した。これにより、平均的に効率よくベクトル乗算を行えるものを提案・実装した。これを具体的な医療データの暗号化には、イーサリアムネットワークも応用しつつ、楕円曲線暗号をベースとした公開鍵認証のみでなく、さらなる安全性拡張を実施することを考えた。

今後は、本研究成果の横展開・拡張応用として、現時点でとくにデータ保護・改ざん対策に乏しい GPS データの暗号化（改ざん対策）などでも活用できないか検討を進めている。そのための改ざん耐性やエビデンスの確保のためにブロックチェーン技術との相性について、本研究開発の成果も踏まえつつ検討を進めている。一方で、そのデータ自身は暗号化して秘匿する必要があるため、準同型暗号を適用すべく研究を進めている。また、秘密分散手法については、さらにそのデータサイズが大きくなる可能性も含めて、データサーバ連携についても考察を進めている。

５．主な発表論文等

〔雑誌論文〕　計9件（うち査読付論文　9件／うち国際共著　2件／うちオープンアクセス　3件）

１．著者名 Yuta Kodera, Ryoichi Sato, Md. Arshad Ali, Takuya Kusaka, and Yasuyuki Nogami	４．巻 24(6)
２．論文標題 Transition Probability Test for an RO-Based Generator and the Relevance between the Randomness and the Number of ROs	５．発行年 2022年
３．雑誌名 Entropy	６．最初と最後の頁 780
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 H. Nasu, Y. Kodera and Y. Nogami	４．巻 22(13)
２．論文標題 A Business-to-Business Collaboration System That Promotes Data Utilization While Encrypting Information on the Blockchain	５．発行年 2022年
３．雑誌名 Proceedings of MDPI Sensors	６．最初と最後の頁 1-12
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 H. Miura, S. Kanzawa, R. Matsumura, Y. Kodera, T. Kusaka and Y. Nogami	４．巻 11
２．論文標題 Sophisticated Analysis of a Method to Eliminate Fruitless Cycles for Pollard’s Rho Method with Skew Frobenius Mapping over a Barreto-Naehrig Curve	５．発行年 2021年
３．雑誌名 International Journal of Networking and Computing	６．最初と最後の頁 231-250
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 [1]D. Hattori, Y. Takahashi, T. Tatara, Y. Nanjo, T. Kusaka and Y. Nogami	４．巻 NA
２．論文標題 An Optimal Curve Parameters for BLS12 Elliptic Curve Pairing and Its Efficiency Evaluation	５．発行年 2021年
３．雑誌名 Proceedings of International Conference on Consumer Electronics-Taiwan 2021 (ICCETW)	６．最初と最後の頁 NA
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Kuniaki Tsuji, Shiden Kishimoto, Yuya Tarutani, Yukinobu Fukushima and Tokumi Yokohira	4．巻 NA
2．論文標題 A Secret Sharing Scheme to Reduce the Total Data Size	5．発行年 2021年
3．雑誌名 International Conference on ICT Convergence 2021 (ICTC 2021)	6．最初と最後の頁 163-166
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Nakamura Toru、Ito Hiroshi、Kiyomoto Shinsaku、Yamauchi Toshihiro	4．巻 12835
2．論文標題 (Short Paper) Evidence Collection and Preservation System with Virtual Machine Monitoring	5．発行年 2021年
3．雑誌名 The 16th International Workshop on Security (IWSEC 2021), Lecture Notes in Computer Science (LNCS)	6．最初と最後の頁 64～73
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-85987-9_4	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Kodera Yuta、Taketa Yuki、Kusaka Takuya、Nogami Yasuyuki、Uehara Satoshi	4．巻 NA
2．論文標題 Equivalent Keys of a Nonlinear Filter Generator Using a Power Residue Symbol	5．発行年 2020年
3．雑誌名 Advances in Information and Computer Security - 15th International Workshop on Security, IWSEC 2020, Proceedings, Springer Science and Business Media Deutschland GmbH.	6．最初と最後の頁 23～36
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-58208-1_2	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Y. Kodera, M. A. Ali, T. Miyazaki, T. Kusaka, Y. Nogami, S. Uehara and R. H. M. Zaragoza	4．巻 E102-A, 12
2．論文標題 Algebraic Group Structure of the Random Number Generator: Theoretical Analysis of NTU sequence(s)	5．発行年 2019年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences	6．最初と最後の頁 1659-1667
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E102.A.1659	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 NORIMATSU Takashi, NAKAMURA Yuichi, YAMAUCHI Toshihiro	4．巻 E106.D
2．論文標題 Policy-Based Method for Applying OAuth 2.0-Based Security Profiles	5．発行年 2023年
3．雑誌名 IEICE Transactions on Information and Systems	6．最初と最後の頁 1364～1379
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2022ICP0004	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計34件（うち招待講演　0件／うち国際学会　16件）

1．発表者名 S. Kanzawa, H. Miura, Y. Kodera, Y. Nogami and T. Kusaka
2．発表標題 Effectiveness of a Method to Eliminate Fruitless Cycles for Pollard's Rho Method
3．学会等名 2022 37th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC)（国際学会）
4．発表年 2022年

1．発表者名 Kazuma Ikesaka, Yuki Nanjo, Yuta Kodera, Takuya Kusaka, and Yasuyuki Nogami
2．発表標題 Improvement of Final Exponentiation for a Pairing on FK12 Curve and its Implementation
3．学会等名 2022 37th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC)（国際学会）
4．発表年 2022年

1．発表者名 Tomoya Hikida, Yasuyuki Nogami, Md. Arshad Ali, Yuta Kodera
2．発表標題 Comaparison of conversion matrices for a compact AES-CTR defined over an isomorphic field
3．学会等名 2022 37th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC)（国際学会）
4．発表年 2022年

１．発表者名
Kazuma Ikesaka, Yuki Nanjo, Yuta Kodera, Takuya Kusaka and Yasuyuki Nogami

２．発表標題
Improvement of Final Exponentiation for a Pairing on FK12 Curve and its Implementation

３．学会等名
the 10th International Symposium on Computing and Networking (CANDAR) (国際学会)

４．発表年
2022年

１．発表者名
Duan M., Kodera Y., Ishihara N., Nogami Y., Kusaka T.

２．発表標題
Design and Implementation of a Practical Control System for an Air-conditioner with IoT Sensor Nodes

３．学会等名
2022 37th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC) (国際学会)

４．発表年
2022年

１．発表者名
Kanzawa S., Miura H., Nogami Y., Kodera Y., Kusaka T.

２．発表標題
A Method to Eliminate Fruitless Cycles for Pollard's Rho Method by Splitting a Seed-point Table for a Random Walk

３．学会等名
the 10th International Symposium on Computing and Networking (CANDAR) (国際学会)

４．発表年
2022年

１．発表者名
Tomohiro Iida, Kazuma Ikesaka, Yuta Kodera, Takuya Kusaka and Yasuyuki Nogami

２．発表標題
Improvement of Optimal-Ate Pairing on Cocks-Pinch Curve with Embedding Degree 6 in Affine Coordinates

３．学会等名
the 10th International Symposium on Computing and Networking (CANDAR) (国際学会)

４．発表年
2022年

１．発表者名
Takahiro Baba, Kensuke Baba, Toshihiro Yamauchi

２．発表標題
Malware Classification by Deep Learning Using Characteristics of Hash Functions

３．学会等名
the 36th International Conference on Advanced Information Networking and Applications (AINA-2022)（国際学会）

４．発表年
2022年

１．発表者名
[2]飯田 智宏，服部 大地，松村 陸矢，南條 由紀，小寺 雄太，日下 卓也，野上 保之

２．発表標題
BLS12曲線上のペアリングにおけるG2上の有理点生成の高速化

３．学会等名
SCIS2022

４．発表年
2022年

１．発表者名
池坂和真，南條由紀，小寺雄太，日下卓也，野上保之

２．発表標題
FK12曲線上のペアリングにおける最終べきアルゴリズムの改良

３．学会等名
SCIS2022

４．発表年
2022年

１．発表者名
濱田泰誠，樽谷優弥，福島行信，横平徳美

２．発表標題
TCPインキャスト回避法の性能比較

３．学会等名
電子情報通信学会2022年総合大会， B-6-41，通信講演論文集

４．発表年
2022年

１．発表者名
辻普明，谷優弥，福島行信，横平徳美

２．発表標題
総データ量の低減を指向した秘密分散法

３．学会等名
電子情報通信学会2022年総合大会， B-6-81，通信講演論文集

４．発表年
2022年

１．発表者名
伊藤 寛史，中村 徹，磯原 隆将，山内 利宏

２．発表標題
VMMを用いたプログラム実行時の証拠取得機能における取得対象の拡張と改ざん耐性の向上

３．学会等名
2022年暗号と情報セキュリティシンポジウム（SCIS2022）

４．発表年
2022年

１．発表者名
馬場 隆寛，馬場 謙介，山内 利宏

２．発表標題
ハッシュ関数の特徴を用いた深層学習によるマルウェア分類

３．学会等名
第20回情報科学技術フォーラム（FIT2021）

４．発表年
2021年

１．発表者名
R. Matsumura, Y. Takahashi, Y. Nanjo, T. Kusaka and Y. Nogami

２．発表標題
Implementation and Evaluation of Ate Pairings on Elliptic Curves with Embedding Degree 10 Applied Type-II All-One Polynomial Extension Field of Degree 5

３．学会等名
Proceedings of International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), pp. 336-341, Nagoya, JPN, July 2020（国際学会）

４．発表年
2020年

１．発表者名
H. Miura, R. Matsumura, T. Kusaka and Y. Nogami

２．発表標題
Analysis of a method to eliminate fruitless cycles for Pollard ' s rho method with skew Frobenius mapping over a Barreto-Naehrig curve

３．学会等名
Proceedings of CANDAR/Track5, pp. 160-166, Online, Nov. 2020.（国際学会）

４．発表年
2020年

１．発表者名
K. Yoshimoto, Y. Uetake, Y. Kodera, T. Kusaka and Y. Nogami

２．発表標題
Evaluating Side-Channel Resistance Using Low Order Rational Points Against Curve25519 and an Associated Quadratic Twist

３．学会等名
Proceedings of International Journal of Networking and Computing (IJNC), vol. 10, no. 2, pp. 144-158, July 2020（国際学会）

４．発表年
2020年

１．発表者名
伊藤 寛史，中村 徹，清本 晋作，山内 利宏

２．発表標題
VMMによるプログラム実行時のライブラリ情報取得機能の設計

３．学会等名
2021年暗号と情報セキュリティシンポジウム（SCIS2021）論文集

４．発表年
2021年

１．発表者名
多田羅 友也，小寺 雄太，日下 卓也，野上 保之

２．発表標題
Cascaded NTU 系列の線形複雑度に関する 考察

３．学会等名
第 6 回有限体理論とその擬似乱数系列生成への応用ワークショップ;，pp. 12-17，Sep. 2020

４．発表年
2020年

１．発表者名
高谷 つぐみ，小寺 雄太，野上 保之

２．発表標題
暗号向け乱数生成における非線形フィルタの設計に関する考察

３．学会等名
第 6 回有限体理論とその擬似乱数系列生成への応用ワークショップ;，pp．12-17，Sep．2020

４．発表年
2020年

１．発表者名
佐藤陵一，小寺雄太，野上保之

２．発表標題
リングオシレータを用いた小規模な物理乱数生成回路の設計及び乱数性評価

３．学会等名
第 6 回有限体理論とその擬似乱数系列生成への応用ワークショップ;，pp．12-17，Sep．2020

４．発表年
2020年

１．発表者名
齋藤 凌也，山内 利宏

２．発表標題
typeattributeset宣言の置き換えによるSELinuxの不要なポリシの細粒度な 削減手法の提案

３．学会等名
情報処理学会シンポジウムシリーズ コンピュータセキュリティシンポジウム 2019（CSS2019）

４．発表年
2019年

１．発表者名
伊藤 寛史，中村 徹，橋本 真幸，山内 利宏

２．発表標題
仮想計算機モニタによるプログラム実行の証拠保全システムの設計

３．学会等名
2020年電子情報通信学会総合大会

４．発表年
2020年

１．発表者名
Y. Kodera, T. Kusaka and Y. Nogami

２．発表標題
Classifying a Random Number Generators Based on a Statistical Feature of the Distribution of Bits

３．学会等名
Workshop on Finite Field Theory and its Application for Pseudo-Random Sequences

４．発表年
2019年

１．発表者名
松村陸矢，高橋裕人，多田羅友也，南條由紀，日下卓也，野上保之

２．発表標題
埋め込み次数10のペアリング曲線の実装とその評価

３．学会等名
情報理論とその応用シンポジウム

４．発表年
2019年

１．発表者名
松本年史，日下卓也，野上保之

２．発表標題
鍵更新機能を追加したMKSEおよびKASE方式に関する一考察

３．学会等名
情報理論とその応用シンポジウム

４．発表年
2019年

１．発表者名
武田祐樹，小寺雄太，日下卓也，野上保之

２．発表標題
非線形フィルタの適用による群をなす2 値擬似乱数系列の生成

３．学会等名
有限体理論とその擬似乱数系列生成への応用ワークショップ

４．発表年
2019年

１．発表者名
多田羅友也，小寺雄太，日下卓也，野上保之

２．発表標題
識別不能性証明のためのある幾何系列に対する考察

３．学会等名
有限体理論とその擬似乱数系列生成への応用ワークショップ

４．発表年
2019年

１．発表者名
松本年史，日下卓也，野上保之，中西透

２．発表標題
属性ベース検索可能暗号の構成

３．学会等名
2020年暗号と情報セキュリティシンポジウム

４．発表年
2020年

１．発表者名
Y. Kodera, Y. Taketa, T. Kusaka and Y. Nogami

２．発表標題
Decomposing the Inverse of a Masked Vector in an Isomorphic Galois Field for Perfectly Masked S-Box

３．学会等名
International Symposium on Computing and Networking（国際学会）

４．発表年
2019年

１．発表者名
H. Miura, R. Matsumura, K. Ikuta, S. Joichi, T. Kusaka and Y. Nogami

２．発表標題
A preliminary study on methods to eliminate short fruitless cycles for Pollard's rho method for ECDLP over BN curves

３．学会等名
International Workshop on Information and Communication Security（国際学会）

４．発表年
2019年

１．発表者名
K. Yoshimoto, Y. Uetake, Y. Kodera, T. Kusaka and Y. Nogami

２．発表標題
Evaluating a Side-Channel Resistance against Order 4 Rational Points in Arduino Cryptography Library

３．学会等名
International Symposium on Computing and Networking（国際学会）

４．発表年
2019年

１．発表者名
Y. Uetake, K. Yoshimoto, Y. Kodera, L. Weissbart, T. Kusaka and Y. Nogami

２．発表標題
A Side-Channel Attack using Order 8 Rational Points against Curve25519 on an 8-Bit Microcontroller

３．学会等名
International Symposium on Computing and Networking（国際学会）

４．発表年
2019年

１．発表者名
Tatsuki Ishii, Kuniaki Tsuji, Yuya Tarutani, Yukinobu Fukushima and Tokumi Yokohira

２．発表標題
Improvement of a Secret Sharing Scheme to Reduce the Total Data Size

３．学会等名
International Conference on ICT Convergence 2023 (ICTC 2023)（国際学会）

４．発表年
2023年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
競争的資金に関する情報
http://isec.ec.okayama-u.ac.jp/home/funds_jp.html

6．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	日下　卓也（甲本卓也） (Kusaka Takuya) (00336918)	岡山大学・自然科学学域・准教授 (15301)	
研究分担者	福島　行信 (Fukushima Yukinobu) (00432625)	岡山大学・自然科学学域・准教授 (15301)	
研究分担者	横平　徳美 (Yokohira Tokumi) (50220562)	岡山大学・ヘルスシステム統合科学学域・教授 (15301)	
研究分担者	山内　利宏 (Yamauchi Toshihiro) (80359942)	岡山大学・自然科学学域・教授 (15301)	

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

8．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関