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　４ 年　 ６ 月　 ３ 日現在

機関番号：３４３１５
研究種目：基盤研究(B)（一般）
研究期間：2018～2020
課題番号：１８Ｈ０３３０７

研究課題名（和文）ストリーム暗号カオス総合システムに関する実証的研究

研究課題名（英文）Empirical study on integrated chaos-based stream cipher

研究代表者
宮野　尚哉（MIYANO, Takaya）

立命館大学・理工学部・教授

研究者番号：１０３１２４８０

交付決定額（研究期間全体）：（直接経費）　　12,000,000円

研究成果の概要（和文）：本研究は、耐量子暗号を指向したストリーム暗号カオス総合システムの実証的研究である。基本要素は、疑似乱数生成器、秘密鍵交換システム、および、鍵共有確認システムである。これらはカオス力学系を応用して構成される。
　研究代表者と研究協力者の間で、油絵画像データの暗号通信実験を行った。データの暗号化・復号は完全に遂行され、本暗号システムは実際の通信ネットワーク上で実施可能であることが実証された。

研究成果の学術的意義や社会的意義
本研究を通して開発されたストリーム暗号カオス総合システムは、耐量子暗号として、一般ユーザーが利用可能な通信ネットワーク上で実行可能であり、従来の研究において類似例はない。本システムは古典コンピュータ上で安価に実装することができる。この点が量子暗号との顕著な相違点である。実用的な量子計算機の実現が予想される現代において、通信の秘匿性を保証する新しい秘話通信技術となる可能性がある。

研究成果の概要（英文）：This study is concerned with an integrated chaos-based stream cipher consisting of a pseudorandom number generator based on a large-scale chaotic map, a method for exchanging a secret key with randomized coupled chaotic oscillators, a logistic hash function to confirm the identity of the exchanged secret keys. We performed an experiment of the secure communication of image data and found that the encryption and decryption of the data were performed within a practical time. The present results indicate the applicability of our stream cipher to practical secure communications.

研究分野：非線形科学

キーワード：カオス　ストリーム暗号　疑似乱数　ハッシュ関数　ローレンツモデル　ロジスティックモデル　暗号通信　秘密鍵交換

１．研究開始当初の背景

(1) 現在用いられている暗号技術には、秘密鍵方式の代表例として AES（Advanced Encryption Standard)、公開鍵方式の代表例として RSA（Rivest-Shamir-Adleman）がある。量子計算機は、その原理が 1985 年に Deutsch によって発見されて以来、着実に研究が進められ、近年、著しい進展を見せている。量子計算に特化して開発された Shor のアルゴリズムと Grover のアルゴリズムは、RSA や AES のセキュリティを脅かす新しい科学技術である。暗号解読者による量子計算機の利用が暗号開発の前提条件となるという意味で、今後開発されるべき暗号技術は耐量子暗号と呼ばれる。

(2) 研究代表者の研究グループでは、量子鍵配送と疑似乱数発生器としてのカオス動力学モデルを併用したストリーム暗号システムを開発してきた。この暗号システムでは大規模カオス動力学モデルである拡張ローレンツ方程式のネットワーク構造を定義する 2 進係数ベクトルが秘密鍵として使用され、量子鍵配送によって送信者と受信者の間で共有される。量子鍵配送は実用化が間近であり、専用の人工衛星が海外で試験運用されつつある。量子鍵配送は最も安全な対称鍵配送技術であるが、その運用には高価なハードウェアシステムが必要であり、近い将来、一般ユーザーが量子鍵配送を利用できるかは不明である。

(3) このような学術的背景の下、本研究課題の核心をなす「問い」は、送信者認証、秘密鍵配送、および、暗号化を統一的な科学・技術的手法に基づいて効率よく構成する我が国独自の暗号システムであって、かつ、耐量子暗号の要請に応えるものが実現可能かどうかであった。

２．研究の目的

(1) 大自由度カオス動力学モデルとその動的挙動、即ち、カオス同期を活用したストリーム暗号カオス総合システムは一般ユーザーが利用しやすい耐量子暗号となり得るかどうかを実証的に研究することを目的とする。本カオス暗号システムの基本要素である動力学モデルは、研究代表者の研究グループが独自に発見した拡張ローレンツ写像である。この写像モデルから生成される 2 進疑似乱数によって平文を暗号化するストリーム暗号方式を全システムの基盤とする。拡張ローレンツ写像を特徴付ける 2 進ベクトル係数が秘密鍵を構成する。

(2) 秘密鍵配送には、送信者と受信者が有するローレンツ振動子間のカオス同期と同期誤差測定に基づく暗号鍵推定を用いる。送信者と受信者は、物理乱数を付加されたカオス時系列を一定の時間間隔で交換する。物理乱数によるランダム化のために、暗号解読者による暗号鍵推定は非常に困難となるだろう。このような設計思想に基づく秘密鍵交換方法は従来にはない独自の手法であるが、実際の通信ネットワーク上で実現可能かどうか実証的に明かにしなければならない。

(3) 本研究におけるストリーム暗号カオス総合システムのセキュリティ上の最大のリスクは、暗号解読者が量子計算機と Grover のアルゴリズムを用いてキーストリームから暗号鍵を同定する可能性である。このリスクが実際に問題になるかどうかを理論的に解明することも本研究における重要な課題である。

３．研究の方法

(1) 本カオス総合システムを構成する疑似乱数発生器、秘密鍵配送アルゴリズム、および、秘密鍵確認用ハッシュ関数は、研究代表者のグループが開発した動力学モデル、および、結合カオス振動子系における完全同期に基づいて構成される。これら 3 要素技術を最適に統合する手法と通信プロトコルを決定して、ソフトウェアとハードウェアの両者を用いたストリーム暗号カオス総合システムを製作する。研究代表者と研究分担者は、それぞれ、滋賀県草津市および宮城県仙台市に所在の研究機関に所属するので、これらの地域を結ぶインターネット上で秘密鍵交換

と暗号文送信について暗号通信実験を行う。

(2) 量子計算機による秘密鍵同定の可能性を検証するために、研究代表者は最も単純なロジスティック写像の暗号鍵としての 128 ビット初期条件の同定という問題について量子論理ゲートと Grover のアルゴリズムを適用する方法を研究する。

(3) 本研究の研究期間は 3 年間であるが、COVID-19 感染拡大の影響を受けて、令和 4 年度まで繰越された。研究を担うのは、研究代表者と連携研究者（いずれも立命館大学理工学部に所属）、および、研究代表者（東北大学電気通信研究所に所属）である。これらの期間において、以下のように研究を推進した。秘密鍵交換のためのアルゴリズムと通信プロトコル、および、秘密鍵確認用ハッシュ関数を研究代表者が所属する機関で開発し、Python 言語を用いてソフトウェア化する。研究分担者が所属する機関では、疑似乱数を高速で生成する専用ハードウェアシステムを設計し、ハードウェア化する。これらの要素技術を統合したカオスストリーム暗号システムを小型コンピュータ（Raspberry Pi 4 Model B）に実装し、インターネットを用いて暗号通信実験を行い、性能評価と問題点の摘出を行う。実験結果と理論的分析を通して、耐量子暗号システムとしての実用性を評価する。

４．研究成果

(1) 本研究開始時には、高次元常微分方程式系である拡張ローレンツ方程式の数値計算によって2進疑似乱数生成を行っていたが、動作速度が低速であったため、新しい疑似乱数生成システムとして拡張ローレンツ写像を開発した。この写像モデルは拡張ローレンツ方程式を単に漸化式に変換したものではない。そのため、拡張ローレンツ写像による2進疑似乱数の複雑さを NIST SP800-22 乱数検定テストによって精密に評価した。SP800-22 は15種類の統計検定からなるが、拡張ローレンツ写像による2進疑似乱数は、そのいずれにも合格することが確認された。拡張ローレンツ写像の集積回路化は、研究分担者のグループによって実現された（図1）。

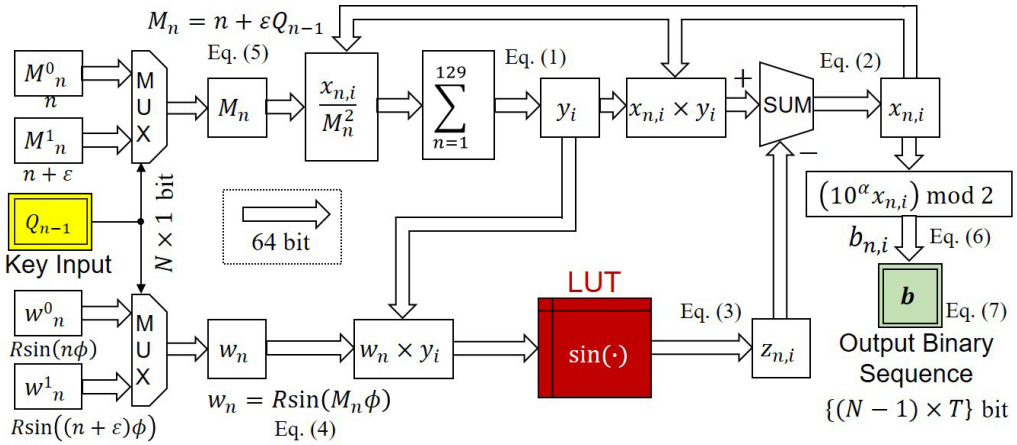

図1　拡張ローレンツ写像モデルのFPGAによるハードウェア化

(2) 本ストリーム暗号システムでは、拡張ローレンツ写像を特徴付けるN次元2進ベクトル係数が秘密鍵として用いられる。送信者と受信者の間での秘密鍵共有は、結合ローレンツ振動子系の完全カオス同期を利用して実行される。送信者と受信者は従来のローレンツ方程式に従う振動子を利用するが、各ローレンツ振動子が生成するカオス時系列に物理乱数を付加する。送信者と受信者が交換するカオス時系列は、それぞれ、物理乱数によってランダム化されているので、盗聴者は、送信者と受信者のランダム化前のカオス時系列を再現することが不可能である。カオス時系列のランダム化にもかかわらず、送信者と受信者のローレンツ振動子は、完全

同期する。この事実は、本研究により理論的かつ実験的に実証された。ランダム化結合ローレンツ振動子系の完全カオス同期を利用して、送信者と受信者による秘密鍵共有は安全に実行することが可能である（図2，図3）。

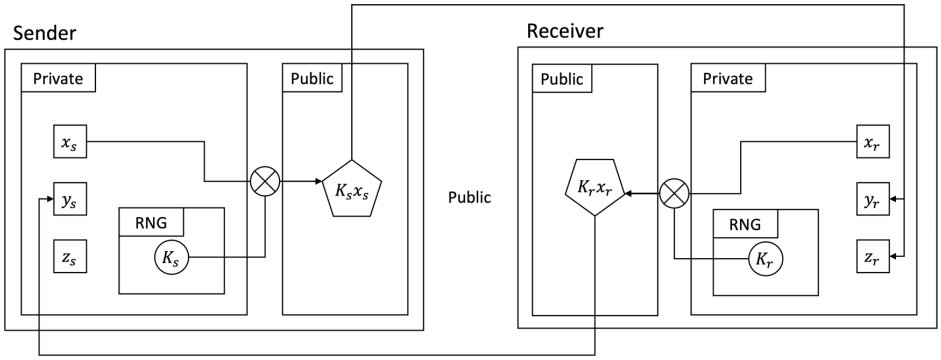

図2　ランダム化結合ローレンツ振動子系のブロック図

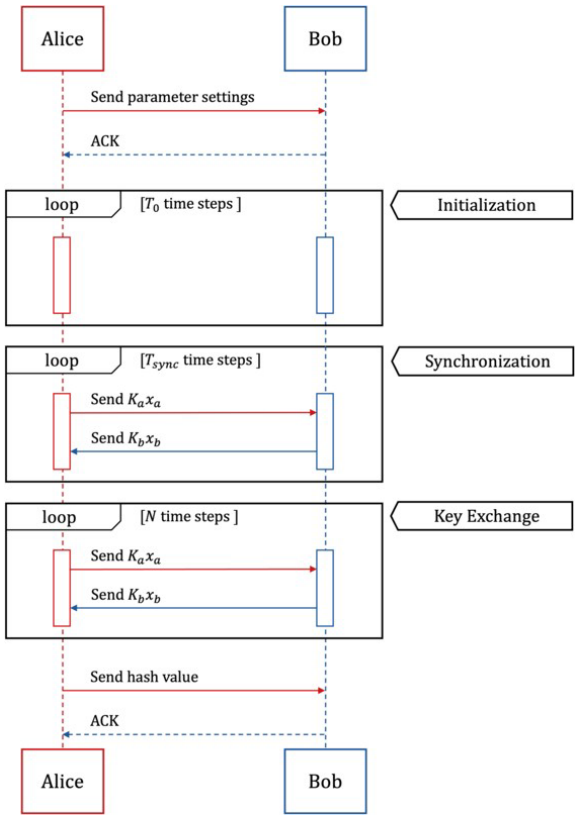

図3　送信者（Alice）と受信者（Bob）間のカオス時系列交換プロセス

ランダム化結合ローレンツ振動子系の完全カオス同期からのカオス時系列推定は量子計算機を用いて多項式時間内に実行することは困難であると推定される。この意味で、本秘密鍵交換手法は耐量子暗号システムを実現する。

(3) 送信者と受信者で交換される秘密鍵の同一性は、ロジスティック写像に基づくハッシュ関数、即ち、ロジスティックハッシュ関数のハッシュ値によって検証される。ロジスティックハッシュ関数は、本研究によって発見された新しいハッシュ関数である（図4）。

$$
\begin{aligned}
&\textit{input } \boldsymbol{Q} \\
&N \leftarrow length(\boldsymbol{Q}) \\
&\boldsymbol{H} \leftarrow zeros(N) \\
&K \leftarrow ceil\left(\frac{N}{D}\right) \\
&flag \leftarrow true \ \ if\ K \neq \frac{N}{D} \ \ else\ false \\
&x \leftarrow 0 \\
&for\ k = 1,\ 2,\ \ldots,\ K \ \ do \\
&\quad D \leftarrow N\%D \ \ if\ (flag\ and\ k == K) \ \ else\ D \\
&\quad u_k \leftarrow 0 \\
&\quad for\ j = 1,\ 2,\ \ldots, D \ \ do \\
&\qquad u_k \leftarrow u_k + \frac{Q_{j+(k-1)D}}{2^j} \\
&\quad end\ do \\
&\quad x \leftarrow x + u_k \\
&end\ do \\
&x \leftarrow \frac{x}{K} \\
&for\ n = 1,\ 2,\ \ldots,\ N \ \ do \\
&\quad L_{loop} \leftarrow L_0 \ \ if\ Q_n == 0 \ \ else\ L_1 \\
&\quad for\ l = 1,\ 2,\ \ldots,\ L_{loop}\ do \\
&\qquad x \leftarrow 4x(1-x) \\
&\quad end\ do \\
&\quad H_n \leftarrow 0 \ \ if\ 0 < x < \frac{1}{2} \ \ else\ 1 \\
&end\ do \\
&\textit{output } \boldsymbol{H}
\end{aligned}
$$

図4　ロジスティックハッシュ関数の擬似コード

(4) 研究代表者と研究分担者が所属するそれぞれの研究機関の間で、インターネットを介して暗号通信実験を行った。秘密鍵長をN＝256 と設定し、ヨハネス・フェルメールの油絵レプリカ画像を平文に用いた。

図5　通信実験において復号された平文画像（真珠の耳飾りをつけた少女）

秘密鍵交換には2分以内、画像データの通信には5分以内の時間を要したが、データの暗号化・復号は完全に遂行され、本ストリーム暗号通信は実施可能であることが実証された（図5）。

５．主な発表論文等

〔雑誌論文〕　計5件（うち査読付論文　5件／うち国際共著　0件／うちオープンアクセス　4件）

１．著者名 K. Miyauchi, Y. Horio, T. Miyano, K. Cho	４．巻 E11-N
２．論文標題 Design of the nonlinear look-up table in the chaotic pseudorandom number generator based on augmented Lorenz map	５．発行年 2020年
３．雑誌名 Nonlinear Theory and Its Applications, IEICE	６．最初と最後の頁 571－579
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/nolta.11.571	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 K. Shiozawa, T. Miyano	４．巻 100
２．論文標題 Symbolic diffusion entropy rate of chaotic time series as a surrogate measure for the largest Lyapunov exponent	５．発行年 2019年
３．雑誌名 Physical Review E	６．最初と最後の頁 032221-1－6
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevE.100.032221	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 Kenichiro Cho, Takaya Miyano	４．巻 9
２．論文標題 Intermittent and partial synchrony of coupled augmented Rossler oscillators	５．発行年 2018年
３．雑誌名 Nonlinear Theory and Its Applications, IEICE	６．最初と最後の頁 36-48
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/nolta.9.36	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 長憲一郎, 宮野尚哉	４．巻 J101-A
２．論文標題 拡張Lorenz写像に基づくストリーム暗号方式とその性能評価	５．発行年 2018年
３．雑誌名 電子情報通信学会論文誌	６．最初と最後の頁 210-218
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 K. Onuki, K. Cho, Y. Horio, T. Miyano	4．巻 69
2．論文標題 Secret-Key Exchange Through Synchronization of Randomized Chaotic Oscillators Aided by Logistic Hash Function	5．発行年 2022年
3．雑誌名 IEEE Transactions on Circuits and Systems -I	6．最初と最後の頁 1655-1667
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TCSI.2022.3140762	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 －

〔学会発表〕　計14件（うち招待講演　0件／うち国際学会　3件）

1．発表者名 K. Miyauchi, Y. Horio, T. Miyano, K. Cho
2．発表標題 Design Method for Nonlinear LUT in Pseudorandom Number Generator Based on Augmented Lorenz Map
3．学会等名 2019 International Symposium on Nonlinear Theory and its Applications（国際学会）
4．発表年 2019年

1．発表者名 大西真史，深津祐貴，大抜倖司朗，宮野尚哉
2．発表標題 拡張Rossler方程式に基づく交代型カオス同期を用いた暗号鍵配送
3．学会等名 電子情報通信学会非線形問題研究会
4．発表年 2020年

1．発表者名 宮内清孝，堀尾喜彦，宮野尚哉，長憲一郎
2．発表標題 拡張Lorenz写像に基づく疑似乱数生成ハードウェアにおけるビット長削減の検討
3．学会等名 電子情報通信学会　2019年ソサイエティ大会
4．発表年 2019年

１．発表者名
Takaya Miyano, Kenichiro Cho

２．発表標題
Chaos-based stream cipher using a star network of chaotic maps

３．学会等名
2018 International Symposium on Information Technology and Its Applications（国際学会）

４．発表年
2018年

１．発表者名
Kazuki Kajita, Hiroshi Gotoda, Takaya Miyano

２．発表標題
Estimation of a surrogate measure for the largest Lyapunov exponent from the information entropy of symbolic dynamics

３．学会等名
2018 International Symposium on Nonlinear Theory and Its Applications（国際学会）

４．発表年
2018年

１．発表者名
宮野尚哉，梶田和希，後藤田浩

２．発表標題
記号力学系の情報エントロピーの増大速度に基づく最大リアプノフ指数の推定

３．学会等名
電子情報通信学会非線形問題研究会

４．発表年
2018年

１．発表者名
長憲一郎，大西真史，宮野尚哉

２．発表標題
間歇結合型カオス振動子群の部分同期に基づくメッセージ転送

３．学会等名
電子情報通信学会非線形問題研究会

４．発表年
2019年

１．発表者名
宮野尚哉，梶田和希，後藤田浩

２．発表標題
記号力学系の情報エントロピーに基づく動的不安定性の推定

３．学会等名
日本物理学会2018年秋季大会

４．発表年
2018年

１．発表者名
宮内清孝，堀尾喜彦，宮野尚哉，長憲一郎

２．発表標題
拡張Lorenz写像に基づく疑似乱数生成器のハードウェア実装に向けての考察

３．学会等名
電子情報通信学会総合大会

４．発表年
2019年

１．発表者名
高橋惇人，堀尾喜彦，宮野尚哉，長憲一郎

２．発表標題
拡張Lorenz写像に基づく暗号通信プログラムの実装

３．学会等名
東北大学電気通信研究所 共同プロジェクト研究・非線形ワークショップ合同研究会

４．発表年
2019年

１．発表者名
宮内清孝，堀尾喜彦，宮野尚哉，長憲一郎

２．発表標題
拡張Lorenz写像に基づく疑似乱数生成器のハードウェア実装に向けて

３．学会等名
東北大学電気通信研究所 共同プロジェクト研究・非線形ワークショップ合同研究会

４．発表年
2019年

１．発表者名
大抜倖司朗，宮野尚哉

２．発表標題
ランダム化された結合Lorenz振動子系における同期

３．学会等名
電子情報通信学会非線形問題研究会

４．発表年
2021年

１．発表者名
大抜倖司朗，堀尾喜彦，宮野尚哉

２．発表標題
ランダム化された結合Lorenz振動子系における同期に基づく秘密鍵共有

３．学会等名
第44回情報理論とその応用シンポジウム

４．発表年
2021年

１．発表者名
大抜倖司朗，長憲一郎，堀尾喜彦，宮野尚哉

２．発表標題
ランダム化されたLorenz振動子系における同期現象を用いた秘密鍵交換

３．学会等名
電子情報通信学会非線形問題研究会

４．発表年
2022年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
宮野研究室ホームページ
http://www.ritsumei.ac.jp/se/~tmiyano/index.html

海外における報道
https://www.eurekalert.org/news-releases/941968
https://cointelegraph.com/authors/andrew-singer

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	堀尾　喜彦 (Horio Yoshihiko) (60199544)	東北大学・電気通信研究所・教授 (11301)	

	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
連携研究者	長　憲一郎 (Cho Kenichiro) (00755514)	立命館大学・理工学部・講師 (34315)	

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