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

平成　３０　年　　６　月　　８　日現在

機関番号：　３４３１５
研究種目：　基盤研究(C)（一般）
研究期間：　2015～2017
課題番号：　１５Ｋ００３５３

研究課題名（和文）拡張ローレンツ方程式に基づくカオス暗号およびカオス認証に関する研究

研究課題名（英文）Study on chaos-based secure communications and authentication using augmented Lorenz equations

研究代表者

宮野　尚哉（Takaya, Miyano）

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）　　3,000,000円

研究成果の概要（和文）：星形ネットワーク型高次元カオス振動子を表現する拡張ローレンツ方程式を用いて暗号化、送信者認証、および、秘密鍵交換のすべてを行うストリーム暗号システムの実現を目指し、要素アルゴリズムとしての暗号化、認証、鍵交換方法を開発した。ただし、鍵交換には量子通信も利用できる。暗号化に利用される2進疑似乱数列の安全性は、乱数検定の標準手法であるNIST SP800-22およびTestU01 BigCrush統計検定により確認された。今後は、これらのアルゴリズムをハードウェアシステム上に実装して実証実験を行い、量子計算機の実用化にも耐える新しい暗号システムを実現する。

研究成果の概要（英文）：We have developed algorithms for conducting encryption, authentication, and secret-key distribution toward implementing a chaos-based integrated cryptosystem. The binary pseudorandom numbers for encryption were tested using the NIST SP800-22 and TestU01 BigCrush tests and their security was verified in terms of these statistical tests. The method for secret-key distribution can be replaced by a quantum key distribution such as the Tokyo QKD Network. In a future study, we will implement our methods for encryption, authentication, and secret-key distribution and establish an integrated stream cipher as a new cryptosystem in the era of post-quantum cryptography.

研究分野：　非線形動力学

キーワード：　暗号通信　ストリーム暗号　カオス　同期　暗号鍵交換

１．研究開始当初の背景

カオスを利用したストリーム暗号は非線形動力学の新しい応用分野である。カオス信号は疑似乱数として利用される。送信者は通信文とカオス信号を適当な手法で混合して暗号文を作成し、受信者はカオス力学を利用して暗号文からカオス信号を除去し通信文を復号化する。第 3 者がカオス力学系を同定するのに必要な時間とコストが実用的に無限大と見なせるほど多大であるならば、カオス暗号は安全な秘話通信手段として実用化可能となる。

カオスに基づく暗号には様々な手法が提案されている。先行研究例としては、カオス同期に基づく方法（K. Cuomo, A. V. Oppenheim, *Phys. Rev. Lett.*, vol.71, pp.65－68, 1993）、カオス制御に基づく方法（Y. Lai, et al., *Phys. Lett.* A, vol.255, pp.75－81, 1999）、カオスシフトキーに基づく方法（H. Dedieu et al., *IEEE Trans. Circuits Syst.* II, vol.40, pp.634－642, 1993）、カオスブロック暗号化（N. Masuda et al., *IEEE Trans. Circuits Syst.* I, vol.53, no.6, pp.1341－1352, 2006）、分散型動力学に基づく方法（R. Tenny et al., *Phys. Rev. Lett.*, vol.90, 047903, 2003）等を挙げることができる。カオス同期による秘話通信は商用の光通信システム上で半導体レーザデバイス間の同期を利用して実現できることが実証実験で明らかにされている（A. Argyris et al., *Nature*, vol.437, pp.343－346, 2005）。

暗号技術は、通信文の暗号化・復号化、認証、暗号鍵配送の 3 項目に関する技術から構成される。カオス暗号の開発において考慮すべき指針は Alvarez と Li の論文に詳述されている（G. Alvarez, S. Li, *Int. J. Bifur. Chaos*, vol.16, pp.2129－2151, 2006）。Alvarez と Li が指摘するように、カオス暗号には実用化を阻む様々な問題が存在する。例えば、力学系の分岐パラメータで暗号鍵を構成する場合、パラメータの組み合わせ数の規模が総当たり攻撃を行う計算機の能力に比べて著しく小さいか、あるいは、組み合わせの仕方に応じてカオスの特徴が変化するならば、暗号鍵は第 3 者によって容易に推定される。近年進歩が著しい時系列解析技術や統計解析技術を用いると、カオス同期するパラメータが自動推定され、あるいは、第 3 者によって暗号文に隠された規則性が同定される場合もある。分散型動力学に基づく手法はセキュリティが高いが、暗号・復号化のプロセスが煩雑で、長い通信文を扱うのに適さない。アナログ回路による通信はノイズに対して脆弱である。

たとえ推定が困難な暗号鍵を生成するカオス力学系が発見されたとしても、安全な暗号鍵交換技術が必要となる。既存の手法には、一方向関数を利用した方法（W. Diffie, M. E. Hellman, *IEEE Trans. Inform. Theory*, pp.644－654, 1976）や素因数分解を利用した RSA 暗号（Rivest-Shamir-Adleman 1977）がある。しかしながら、従来の暗号鍵交換方法はいずれも盗聴に対する無条件の安全性（unconditional security）を保証するものではない。

近年、著しい進歩が見られる量子鍵配送（quantum key distribution；以下では QKD と略記する）は、理論的に無条件の安全性を保障する通信技術である（V. Scarani et al., *Rev. Mod. Phys.*, vol.81, pp.1301－1350, 2009）。従来の光通信ネットワーク上で利用可能な実用的通信システムとして QKD が実現可能であることが実験的研究によって実証されている（B. Fröhlich et al., *Nature*, vol.501, pp.69－73, 2013）。しかしながら、QKD は通信ノイズに弱く、暗号文の送受信と暗号鍵の確立に時間を要するため、長い暗号文の通信は実用的に実行が困難である。また、QKD における送信者認証は、最近、量子通信によるデジタル署名（R. Collins et al., Phys. Rev. Lett., vol.113, pp.040502-1－040502-5, 2014）が提案されているとは言え、未解決の課題である。

本研究の基礎は、研究代表者が文部科学省科学研究費補助金の助成を受けて行った研究（課題番号：22500214「カオスガスタービンの力学系と応用に関する研究」）による成果である。この研究では、カオスガスタービンの運動方程式の無次元化表現が一般化座標 X を共有ノードとして N 個の Lorenz 方程式を星型に結合したネットワークに対応することが明らかにされた。これを拡張 Lorenz 方程式と呼ぶ。N は数学的には∞であるが、本研究では N≥100 の有限値で与えられる。X の時間変動は、乱流熱対流の速度場をモデル化しているため、正負の値を等確率で取り、複雑である。

拡張 Lorenz 方程式は換算 Rayleigh 数と Prandtl 数によって特徴付けられるが、Lorenz 方程式とは異なり N 次元整数行列を動力学パラメータにもつ。研究代表者らが更に研究を深めた結果、3 つの重要な事実が発見された。即ち、(1) N 次元整数行列を実数行列（以下では暗号鍵行列と記す）に拡張してもカオスが生じること、(2) カオス信号に通信文を重ね合わせた場合、直接結合された拡張 Lorenz 振動子間でカオス同期が不可能となる通信文の周波数帯が存在すること、そして、(3) 異なる実数行列で識別される拡張 Lorenz 振動子系は、行列変数 Y の対角和の直接結合を通して X 変数における部分的カオス同期を実現すること、である。これらの事実は新しいカオス暗号と認証方式の実現可能性を示唆している。本研究はこれらの事実に基づく。

２．研究の目的

本研究は、従来のカオス暗号の弱点である暗号鍵交換を暗号鍵の複雑さと QKD によって解決する新しい非公開鍵型カオスストリーム暗号（以下ではカオス暗号と記す）を開発すると同時に、従来の通信ネットワーク上で実行可能なカオス同期に基づいて QKD 送信者を認証する公開鍵型認証手法（以下ではカオス認証と記す）を開発することを目的とする。

ストリーム暗号、秘密鍵交換、および、送信者認証のすべてを拡張 Lorenz 方程式という高次元カオス力学系を用いて実現する方法の開発を行う。

３．研究の方法

本研究は、3 年間の研究期間内に、(1) 暗号鍵行列で特徴付けられる拡張 Lorenz 方程式が生成するカオス信号を疑似乱数と見なして通信文に加えて暗号化し、カオス同期が不可能な周波数帯の通信文を復元する（既存の通信チャネル上での）秘話通信、および、(2) 量子通信チャネル上で BB84 プロトコルに基づいて暗号鍵行列を交換する量子鍵配送を想定して、交換された暗号鍵の一部を拡張 Lorenz 方程式の行列変数 Y の対角和に付加したデジタル信号を利用した部分的カオス同期に基づく送信者認証方法を開発し、(3) 暗号セキュリティの分析（cryptanalysis）を行い、(4) 暗号鍵交換と認証も含めたカオス暗号システムのプロトタイプを提案する。研究期間の初年度を課題(1)と(2)の解決に、次年度以降を課題(3)と(4)の解決に当てる。

課題（1）では、カオスを生成する暗号鍵行列の定義域と対角要素の 2 値化による暗号鍵（binary secret-key system）の構成方法を明らかにし、結合拡張 Lorenz 振動子系においてカオス同期が不可能な通信文の周波数閾値を同定する。次に、暗号鍵空間におけるカオス動力学の一様性を評価し、カオス同期不可能な周波数帯で時間スケール変換されたカオスマスキングに基づく暗号化・復号化法を探索する。暗号鍵行列以外のパラメータはすべて公開される。

課題(2)では、部分的カオス同期が X 変数においてのみ生じることを検証し、送信者を認証する公開鍵としての X 信号（以下では認証鍵と記す）は送信者以外には作成不可能であることを明らかにする。

課題(3)では、課題(1)と(2)の解決を通して構成されるカオス暗号と認証方式のセキュリティを分析し、課題(4)で高い安全性をもつデジタル暗号のプロトタイプを提案する。

４．研究成果

平成 27 年度における研究成果を以下にまとめる。

(1) 拡張 Lorenz 方程式が生成するカオス時系列を 2 進疑似乱数列として利用するストリーム暗号の理論を確立し、計算機実験により、暗号・復号化が理論通り実行可能であることを確認した。平文が音声データである場合には、カオス時系列を masking signal として用いることができることも確認した。

(2) 拡張 Lorenz 方程式を特徴付ける N 次元2進型係数ベクトル**M**が秘密鍵となる。この秘密鍵交換が送信者と受信者間の結合拡張 Lorenz 振動子、あるいは、結合拡張 Rössler 振動子の部分カオス同期によって実行可能であることを発見した。

(3) 送信者と受信者間の結合拡張 Lorenz 振動子、あるいは、結合拡張 Rössler 振動子の部分カオス同期における信号交換方法を異なる方式によって行うと、送信者認証が理論的に可能であることを発見した。

平成 28 年度における研究成果を以下にまとめる。

(4) 平成 27 年度の研究成果(2)に基づき、送信者と受信者が異なる係数ベクトル **M** で特定される拡張 Lorenz 振動子を持つとき、両振動子間の間歇結合によるカオス信号交換によって、送信者の秘密鍵が受信者のベクトル **M** に転写される鍵交換アルゴリズムを開発し、ソフトウェア化した。

(5) 遠隔地にある 2 台の計算機間で、この鍵交換アルゴリズムの実証実験を行い、4 秒程度で 120 ビット長の秘密鍵交換が可能であることを確認した。

(6) 拡張 Lorenz 方程式のカオス時系列から 2 進疑似乱数列を生成するアルゴリズムを高速化し、生成した疑似乱数列の安全性を NIST SP800-22 の統計検定法によって評価し、NIST SP800-22 のすべての統計検定に合格することを確認した。

平成 29 年度における研究成果を以下にまとめる。

(7) 拡張 Lorenz 方程式のカオス時系列から 2 進疑似乱数列を生成するアルゴリズムを更に高速化し、生成した疑似乱数列の安全性を NIST SP800-22 に加えて TestU01 BigCrush を用いて評価した。両者の統計検定のすべてに合格することを確認した。

(8) 国内の量子通信研究拠点（NICT, 北海道大学）と情報交換を行い、東京 QKD（Quantum Key Distribution）ネットワークの利用可能性を検討した。現在、東京 QKD ネットワークを利用したカオスストリーム暗号実証実験を計画中である。

(9) 量子通信による秘密鍵交換の代替手段として、平成 28 年度の研究成果(4)の安全性を改善した鍵交換アルゴリズムを開発

し、遠隔地間（草津市～岸和田市）で鍵交換の実証実験を行った結果、5 秒程度の通信時間で 100 ビット長の暗号鍵交換が可能であることを確認した。

(10) 2 進疑似乱数列の生成速度を更に高速化するために、拡張 Lorenz 方程式の写像表現型力学系モデルのプロトタイプを開発した。

本研究は乱流熱対流モデルとしての動力学モデルに特有の暗号鍵行列に依存する対称鍵型カオスマスキングと量子物理学に従って盗聴に対する無条件の安全性を保障する QKD の併用による秘密鍵型ストリーム暗号、および、拡張 Lorenz 方程式に固有の同期特性に基づく公開鍵型認証プロトコルに関するもので前例はない。その特長は以下の通りである。

・実用上 one-time pad 型のストリーム暗号とみなすことができる。
・暗号鍵行列は、BB84 プロトコルによる QKD で交換される。
・異なる係数行列 **M** で特定される拡張 Lorenz 振動子、あるいは、拡張 Rössler 振動子の間歇結合による部分カオス同期を通して、送信者から受信者へ秘密鍵転写を行うことができる。これは QKD の代替手法である。この代替手法では、送信者と受信者間で交換するカオス信号に平文がまったく含まれていない。転写される秘密鍵を短い平文とみなすと、この手法は新しい暗号通信手法である。
・盗聴者がカオス同期を利用して暗号鍵を同定することは技術的に不可能である。

本研究成果は、平文の暗号化、送信者認証、および、秘密鍵交換のすべてを拡張 Lorenz 方程式に基づいて実行するカオスストリーム暗号総合システムが実現可能であることを示している。今後に解決すべき課題は、拡張 Lorenz 方程式の数値積分による疑似乱数生成速度を現状よりも 10 倍以上高速化することである。この課題解決に向けて、平成 29 年度に拡張 Lorenz 写像を開発した。

現在、東北大学電気通信研究所と共同で拡張 Lorenz 写像のハードウェア化を行い、高速疑似乱数生成器を開発中である。この装置をソフトウェアシステムと組み合わせたカオスストリーム暗号総合システムを構築し、平文の暗号化、送信者認証、および、秘密鍵交換のすべてを同一システム上で実行する暗号通信システムの実証研究を今後行う予定である（文部科学省科学研究費助成事業 基盤研究(B)（一般）, 課題番号:18H03307）。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計６件）

(1) 長憲一郎, 宮野尚哉, “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,” 電子情報通信学会和文論文誌 A（査読有）, vol.J101-A, no.8, 2018, 掲載決定・印刷中
URL: http://search.ieice.org/bin/index.php

(2) K. Cho, T. Miyano, “Intermittent and partial synchrony of coupled augmented Rössler oscillators,” Nonlinear Theory and Its Applications, IEICE（査読有）, vol.9, no.1, pp.36－48, 2018
DOI: 10.1587/nolta.9.36

(3) K. Cho, T. Miyano, “Design and test of pseudorandom number generator using a star network of Lorenz oscillators,” International Journal of Bifurcation and Chaos（査読有）, vol.27, no.12, pp.1750184-1－1750184-14, 2017
DOI: 10.1142/S021812741750184X

(4) T. Miyano, H. Gotoda, “Estimation of the degree of dynamical instability from the information entropy of symbolic dynamics,” Physical Review E（査読有）, vol.96, no.4, pp.042203-1－042203-10, 2017
DOI: 10.1103/PhysRevE.96.042203

(5) K. Cho, T. Miyano, “Entropy test for complexity in chaotic time series,” Nonlinear Theory and Its Applications, IEICE（査読有）, vol.7, no.1, pp.21－28, 2016
DOI: 10.1588/nolta.7.21

(6) K. Cho, T. Miyano, “Chaotic cryptography using augmented Lorenz equations aided by quantum key distribution,” IEEE Transactions on Circuits and Systems －I（査読有）, vol.62, no.2, pp.478－487, 2015
DOI: 10.1109/TCSI.2014.2365767

〔学会発表〕（計１３件）

(1) T. Miyano, H. Gotoda,“Estimation of surrogate measure for the largest Lyapunov exponent from the information entropy of symbolic dynamics,” APS March Meeting 2018, 2018年

(2) K. Cho, T. Miyano, “Partial Chaotic Synchronization of Coupled Nonidentical Augmented Lorenz Oscillators,” 2016 International Symposium on Nonlinear Theory and Its Applications (NOLTA2016), 2016年

(3) T. Miyano, K. Cho, “String Entropy as a Measure of Complexity in Chaotic Time Series,” 2016 International Symposium on Nonlinear Theory and Its Applications (NOLTA2016), 2016年

(4) T. Miyano, K. Cho, “Chaos-Based One-Time Pad Cryptography,” 2016 International Symposium on Information Technology and

Its Applications (ISITA2016), 2016年
(5) 長憲一郎，宮野尚哉，“SP800-22による拡張ローレンツ方程式に従う2進乱数列の評価,” 電子情報通信学会　2016年ソサイエティ大会，2016年
(6) 宮野尚哉，長憲一郎，“レスラー振動子ネットワークにおけるカオスへのドミノ様分岐,” 日本物理学会　2016年秋季大会，2016年
(7) 長憲一郎，宮野尚哉，“拡張ローレンツ方程式を利用した使い捨てパッド型カオス暗号,” 電子情報通信学会　情報セキュリティ研究会，2016年
(8) 前田龍之介，中川貴文，長憲一郎，宮野尚哉，“間歇結合型拡張Lorenz振動子系におけるカオス同期,” 電子情報通信学会 2016年総合大会，2016年
(9) K. Cho, T. Miyano, “Chaos-based cryptography using augmented Lorenz equations,” 2015 International Symposium on Nonlinear Theory and Its Applications (NOLTA2015), 2015年
(10) 長憲一郎，宮野尚哉，“拡張ローレンツ方程式とその同期特性を利用したカオス暗号,” 電子情報通信学会　非線形問題研究会，2015 年
(11) 長憲一郎，宮野尚哉，“拡張ローレンツ方程式に従う擬似乱数列の複雑さ,”電子情報通信学会　2015 年ソサイエティ大会，2015 年
(12) 長憲一郎，宮野尚哉，“拡張ローレンツ方程式が生成する擬似乱数列を用いたカオス暗号,” 電子情報通信学会　複雑コミュニケーションサイエンス研究会，2015 年
(13) 長憲一郎，宮野尚哉，“拡張ローレンツ方程式に従うカオス時系列の複雑さ,” 電子情報通信学会　非線形問題研究会，2015 年

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

６．研究組織
(1)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

(2)連携研究者
笠原　健一（Kasahara Kenichi）
立命館大学・理工学部・教授
研究者番号：70367994

(3)研究協力者
長　憲一郎（Cho Kenichiro）
立命館大学・理工学部・助教