様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　６　月　１５　日現在

機関番号：　３７４０１
研究種目：　若手研究(B)
研究期間：　2013～2015
課題番号：　２５８２０１６７

研究課題名（和文）カオスに基づく暗号用非線形変換関数の設計

研究課題名（英文）Design of cryptographicaly nonlinear transformation based on chaos

研究代表者
吉岡　大三郎（YOSHIOKA, Daisaburo）

崇城大学・情報学部・准教授

研究者番号：７０４３５１４７

交付決定額（研究期間全体）：（直接経費）　　1,900,000円

研究成果の概要（和文）：本研究では，整数上カオス写像の設計と暗号への応用を検討した．簡単な整数演算に基づく一対一カオス写像の構成法を与え，共通鍵暗号方式で重要なS-boxを設計し，既存のAESのS-boxと比較した．その結果，解読耐性となる差分確率が98%向上し，標準的なCMOSプロセスで実装した場合，回路面積72%，消費電力84%の改善を達成した．また，計算機実装で有用となる２べき剰余環上で一対一写像となるChebyshev写像に基づく公開鍵暗号系の安全解析を行い，その暗号が多項式時間で解読可能となることを明らかにした．

研究成果の概要（英文）：The purpose of this study is the design of chaotic map over finite sets and its applications to cryptography. Firstly, we propose to construct one-to-one chaotic maps over integer sets. Since S-box is the most important portion in block cipher, we design low complexity S-boxes based on the chaotic maps. As a result, difference probability of the proposed S-boxes is improved by about 98% compared with that of AES. Moreover, the area and power consumption of the proposed S-box circuits are improved compared with that of AES by about 72% and 84%, respectively. We also evaluate the security of public-key cryptography based on Chebyshev polynomials modulo powers of two. Unfortunately, it is revealed that the cryptosystem is not secure by our security analysis.

研究分野：　情報通信

キーワード：　カオス　共通鍵暗号　S-box　公開鍵暗号　Chebyshev多項式　２べき剰余環

１．研究開始当初の背景

通信内容の秘匿性の確保をはじめ，改ざん検出から認証技術にまで応用される暗号は，情報セキュリティを支える主要素技術である．暗号は，共通鍵暗号方式と公開鍵暗号方式に大別される．近年の IoT(Internet of Things)時代への期待が高まるにつれ，実装コストに優れる暗号の需要が急速に高まり，その研究が盛んに行われている．

秘匿性確保のために使用される共通鍵暗号方式では，標準暗号 DES(Data Encryption Standard) や AES(Advanced Encryption Standard)がよく知られている [1]. 共通鍵暗号では共通鍵の事前共有が問題となり，その解決手法として，公開鍵暗号や鍵交換アルゴリズムが用いられる．公開鍵暗号方式では，べき乗剰余関数に基づく RSA やディフィー・ヘルマン鍵交換方式がよく知られている [2].

暗号変換に用いられる暗号用関数として，有限体を用いる代数的手法がよく知られている．一方で，規則から得られる不規則現象“カオス”の暗号化への応用も盛んに研究されている．しかしながら，カオス写像は実数演算上で定義されること，および暗号化への応用の際，復号化を可能にするための１対１写像の設計が必要となり，既存の手法と比べて効率よいディジタル実装法が提案されていなかった．

２．研究の目的

本研究の目的は，ソフトウェアおよびハードウェア実装効率に優れる整数上１対１カオス写像の設計と暗号への応用である．

（１）整数上カオス写像に基づく共通鍵暗号用 S-box の設計

共通鍵暗号方式のブロック暗号では，非線形変換関数 S-box が暗号全体の安全性および実装パフォーマンスを決定するため，その設計がとりわけ重要とされている．この暗号用 S-box として，DES でみられるようなランダム変換に基づく手法や，AES にみられるガロア拡大体の逆元とアフィン変換を用いる手法がよく知られている [1]．S-box の解読耐性向上のためには長ビット化が有効である反面，長ビット化による回路規模の増大が問題となり，現在まで 4 ビットか 8 ビット S-box が主として用いられている．

本研究では，簡単な整数演算のみに基づく一対一カオス写像の構成法を与え，計算効率に優れる暗号用 16 ビット S-box を設計する．解読耐性と実装効率の両面から最適構成となる S-box を設計し，その性能評価ならびに既存の S-box と比較し，本提案手法の有効性を実証する．

（２）2 べき剰余環上 Chebyshev 写像の公開鍵暗号への応用

ディフィーとヘルマンが提案したべき乗剰余関数に基づく鍵交換方式にみられるように，公開鍵暗号方式では可換性と一方向性を有する関数の使用が求められる [2]．可換性を有する多項式として，Chebyshev 多項式が知られる．Chebyshev 多項式はカオスを呈する一次元写像としてもよく知られている．また，Chebyshev 多項式の次数を求める問題の効率解法の有無が明らかでなく，公開鍵暗号系への応用が期待されていた．

2 べき剰余上では剰余演算が実質不要のため，合成数上の剰余を用いる RSA 暗号や有限体上の楕円曲線暗号などの既存手法と比べて，演算コストを大幅に抑えられる．しかしながら，RSA 暗号などで用いられるべき乗関数は 2 べき剰余上では Pohlig –Hellman 法により容易に解けてしまう [3]．可換な多項式はべき乗関数か Chebyshev 多項式，それら線形変換から得られる多項式に限られるため [4]，2 べき剰余上で公開鍵暗号系を構築できるただ一つの候補が Chebyshev 多項式といえる． しかしながら，Chebyshev 多項式に基づく公開鍵暗号系の安全性については不明確であった．そこ本研究では，2 べき剰余環上 Chebyshev 写像に基づく公開暗号系の安全性解析を目的とする．

３．研究の方法

・研究目的（１）に対する研究方法

カオス写像は多対一であり，通常のディジタル実装では一対一写像とならない．よって，いかに効率よいディジタル実装で一対一カオス写像を実現するかが課題であった．そこで本研究では，カオス写像の分割と置換に基づく新しい整数上一対一カオス写像の構成法を与えた．とくに，区分線形カオス写像を用いることで，簡単な整数演算のみに基づく一対一写像の明示式が得られる．平文を初期値とし，その写像の繰り返しにより暗号用 S-box を設計する．

設計する S-box の解読耐性と実装効率は，用いる置換に大きく依存する．代表的な暗号解読法として，差分解読法と線形解読法が知られ，それら解読法への耐性のためには，S-box の差分確率と線形確率が低いことが望まれている．そこで，差分確率と線形確率を評価し，それらの小さい値を得る置換を探索する．本研究では，16 ビット S-box を設計するため，長ビット化の恩恵により，従来より用いられる 8 ビット S-box よりも解読耐性の向上が期待できる．

本研究で提案する暗号用非線形変換 S-box は，簡単な組み合わせ論理回路により実装できる．例として 16 ビット S-box とすると，１クロックで m ビット上位ビットするシフトレジスタと，１対１写像を構成するための置換関数 P を組み合わせ論理回路により設計する．ここで，P は m ビット入力 m ビット出力の論理関数であり，その設計は容易である．m が大きいほど，非線形性が増すため暗号に適するが，置換部の回路が複雑となるため，適切なパラメータを検討する．また，置換部

の回路は，クワイン法による論理関数の最適化を行い，論理素子数が十分小さな置換を設計する．

ハードウェア記述言語 Verilog-HDL(Hardware Description Language)を用いた回路設計を行う．また標準的な CMOS(Complementary Metal-Oxide Semiconductor)プロセスによる論理合成，配置配線を行い，回路面積，動作周波数，消費電力を測定し，最適な構成を検証する．

・研究目的（２）に対する研究方法

ある有限集合上で一対一写像を与える多項式は置換多項式と呼ばれる．暗号や擬似乱数生成において，置換多項式が重要となる．2 べき剰余上で奇数次 Chebyshev 写像は，置換多項式となることが知られていた [5]．また，2 べき剰余上 Chebyshev 写像の次数の周期的性質は石井によって明らかにされていた [6]．また，偶数初期値の場合に Chebyshev 写像の次数決定問題が，多項式時間で解けることが明らかとされていた [7]．しかしながら，2 べき剰余上 Chebyshev 写像の次数決定問題の完全解法は未解決であった．

2 べき剰余上で置換多項式となる奇数次 Chebyshev 写像の繰り返し計算により，周期系列が得られる．そこで本研究では，Chebyshev 写像から得られる周期系列の周期的性質を解析し，次数決定問題解法につながる性質を明らかにする．

４．研究成果

・研究目的（１）に対する研究成果

まず，カオス写像の分割と置換に基づく新しい整数上一対一カオス写像の構成法を与えた．とくに，区分線形カオス写像を用いることで，簡単な整数演算のみに基づく一対一写像が得られる．平文を初期値とし，その写像の繰り返し計算により暗号用 S-box が設計できる．

十分な非線形を有するために置換部を 5 ビット置換とし，16 ビット S-box を設計した．解読耐性評価である差分確率を求めた結果，AES の 8 ビット S-box と比較して，98.2%の改善を達成した．提案する S-box は簡単な計算式で与えられるため，ガロア拡大体の計算が必要な AES の S-box と比べ，16 ビット化してもソフトウェア実装ははるかに容易である．また，提案する 16 ビット S-box を標準的なスタンダードセルを用いた 0.18 μm CMOS プロセス上で実装し，評価した．その結果，AES の 8 ビット S-box と比べて，回路面積は 72.6%，消費電力は 84.3%の改善を達成した．

S-box はブロック暗号で最も回路規模の大きい部分である．よって提案する 16 ビット S-box を用いることにより，ブロック暗号全体で必要な S-box を少なく抑えられる．例として，128 ビットブロック暗号の場合，8 ビット S-box では 16 個必要となるのに対して，提案する 16 ビット S-box では 8 個のみで構築できる．よって，ブロック暗号全体でみたときのハードウェア実装効率は，これまで提案されたどの方式よりも大幅に改善できると期待される．

・研究目的（２）に対する研究成果

まず，2 べき剰余環上 Chebyshev 写像から得られる周期系列の周期がすべて 2 べきとなることを明らかにした．その結果に基づき，初期値と鍵空間の関係を導出した．不適切な初期値を用いた場合，鍵交換の鍵のパラメータの探索空間が減少し，解読が容易となる場合があることを示した．

安全性の完全解析を目指し検討をすすめ，Chebyshev 写像の初期値と次数と周期の関係を明らかにした．その結果より，与えた初期値と次数から得られる系列の周期長が明示的に与えられた．加えて，Chebyshev 写像の次数分岐の性質を導出し，次数分岐の関係から完全 2 分木が構築できる．その結果に基づき，Chebyshev 写像の次数決定問題が，ビット数の高々3 乗の多項式時間で解けることを明らかにした．つまり，2 べき剰余環上で Chebysyhev 写像に基づく公開鍵暗号系は安全ではないことを明らかにした．

2 べき剰余環上で可換な多項式はべき乗関数と Chebyshev 写像のみである．2 べき剰余上べき乗関数の離散対数問題は，pohlig-Hellman 法で容易に解け，2 べき剰余上 Chebyshev 多項式の次数決定問題も本成果により効率解法が存在する．つまり，実装において有用な 2 べき剰余環上で公開鍵暗号系を構築可能な可換な多項式は，残念ながら存在しないと結論づけられた．

＜引用文献＞

1. J. Daemen and V. Rijmen, “The design of Rijndael,” Springer, 238 ページ, 2002.

2. W. Diffie and M. E. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, vol.IT-22, No.6, pp.644--654, Nov, 1976.

3. S. Pohlig and M. Hellman, "An Improved Algorithm for Computing Logarithms over GF(p) and its Cryptographic Significance" IEEE Transactions on Information Theory (24), pp.106--110, 1978.

4. H. D. Block and H. P. Thielman, “Commutative polynomials,” Quart. J. Math., Oxford Ser. (2) 2, pp. 241–243, 1951.

5. K. Umeno, “Key exchange by Chebyshev polynomials modulo 2^w,” Proc. of INA-CISC, pp.95--97, 2005.

6．石井雅治，”2 冪剰余環上 Chebyshev 多項式の周期性と電子署名，” 日本応用数理学会論文誌, vol.18, no.2, pp.257--265, 2008.

7．石井雅治，吉本明宜，“2 冪剰余環の既約剰余類群の構造の暗号への応用，”日本応用数理学会論文誌，vol.19，no.1，pp.57--71，2009.

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 3 件）

① Daisaburo Yoshioka and Kento Kawano, “Periodic properties of Chebyshev polynomial sequences over the residue ring $Z/2^kZ$,” IEEE Transactions on Circuits and Systems II, 査読有，2016. (in press)
DOI：10.1109/TCSII.2016.2531058

② Daisaburo Yoshioka and Yuta Dainobu, “On some properties of Chebyshev polynomial sequences modulo 2^k,” Nonlinear Theory and Its Applications (NOLTA), IEICE, 査読有，Vol.6, No.3, pp.443--452, 2015.
DOI：http://doi.org/10.1587/nolta.6.443

③ Daisaburo Yoshioka and Akio Tsuneda, “The design of low complexity S-boxes based on a discretized piecewise linear chaotic map,” IEICE Transactions Fundamentals, 査読有， Vol.E97-A, No.6, pp.1396--1404, 2014.

〔学会発表〕（計 8 件）

①河野健人，吉岡大三郎，"$Z/3^kZ$ 上チェビシェフ多項式から得られる系列の周期，" 電子情報通信学会 2016 年総合大会，p.350，平成 28 年 3 月 16 日, 九州大学（福岡県福岡市）.

② 小野琢磨, 吉岡大三郎, "整数上カオス写像に基づく 16 ビット S-box の設計とハードウェア実装," 第 23 回電子情報通信学会九州支部学生会講演会, 講演番号 A-15，平成 27 年 9 月 4 日，福岡大学（福岡県福岡市）.

③ 河野健人，吉岡大三郎, "2 べき剰余環上チェビシェフ多項式の次数決定問題の一解法," 電子情報通信学会 非線形問題研究会(NLP), vol.115, no.150, pp.53--56,平成 27 年 7 月 22 日，ぴぱの湯ゆ～りん館（北海道美唄市）

④ Daisaburo Yoshioka and Yuta Dainobu "Some properties of sequences generated by Chebyshev polynomials modulo 2^k," Proc. of IEEE International Symposium on Circuits & Systems (ISCAS), pp.846--849, Lisbon(Portugal), May 25, 2015.

⑤ 吉岡大三郎, "剰余環 $Z/2^kZ$ 上のチェビシェフ多項式から得られる系列の諸性質," 2015 年暗号と情報セキュリティシンポジウム(SCIS), 講演番号 4A2-2，平成 27 年 1 月 23 日, 小倉リーガロイヤルホテル（福岡県北九州市）

⑥ 台信雄太，吉岡大三郎, "2 べき剰余環上のチェビシェフ多項式から得られる系列の周期," 2014 年暗号と情報セキュリティシンポジウム(SCIS), 講演番号 1C2-4，平成 26 年 1 月 21 日, 城山観光ホテル（鹿児島県鹿児島市）

⑦ 吉岡大三郎, "テント型シフト写像に基づく S-box の設計と評価," 2014 年暗号と情報セキュリティシンポジウム(SCIS), 講演番号 3A3-1，平成 26 年 1 月 23 日, 城山観光ホテル（鹿児島県鹿児島市）

⑧ Daisaburo Yoshioka, "Hardware implementable S-box based on a discretized piecewise linear chaotic map," Proc. of 9th IEEE International Wireless Communications & Mobile Computing Conference (IWCMC), pp.1120--1125, July 3, 2013, Cagliari(Italy)

６．研究組織
(1)研究代表者
吉岡 大三郎（YOSHIOKA Daisaburo）
崇城大学・情報学部・准教授
研究者番号：70435147