IoT デバイス実装可能な軽量カオス暗号の設計

研究代表者　　吉岡　大三郎　　崇城大学情報学部情報学科　教授

1 序論

あらゆるモノがネットワークにつながる高度情報化社会の実現が,「モノのインターネット」IoT(Internet of things)というキーワードで近年表現されている．パソコンやスマートフォンといった従来型の情報端末に加えて，自動車や家電，センサー，ロボットなど様々なモノがネットワークにつながると期待されている．そのようなネットワーク社会の実現においては，プライバシー情報の秘匿や改ざん検知のためのセキュリティ機能が必須となる．その情報セキュリティを支える主要素技術として暗号が挙げられる．

暗号は主として共通鍵暗号方式と公開鍵暗号方式に大別される．公開鍵暗号は共通鍵暗号で使用する鍵の共有に使用され，メッセージの暗号化には計算効率の優れる共通鍵暗号方式が専ら使用されている．共通鍵暗号方式として，1970 年代に策定された標準暗号 DES(Data Encryption Standard)や 2000 年に策定された次世代標準暗号 AES(Advanced Encryption Standard)が広く実用化されている[1].

近年では，車載機器や小型センサー，IC チップ，RFID(Radio Frequency Identification)などの IoT 端末に効率よく実装可能な軽量暗号（Lightweight Cryptography）の研究開発が活発であり，多くの方式が学会等で提案されている[2]-[8]．軽量暗号は，省メモリなソフトウェア実装や回路規模の小さいハードウェア実装を特徴とし，回路規模の小型化は RFID や IC カードをはじめとする回路実装面積の要求条件が厳しいアプリケーションで特に重要な要件となる．車載機器や小型情報家電，センサー等で広く用いられる組み込みマイコンは ROM（Read Only Memory）や RAM（Random Access Memory）のサイズが限られているので，省メモリで実装できる暗号が求められている．また，メモリや車載機器などのリアルタイム性が求められるアプリケーションでは，暗号・復号処理に必要な処理時間が短いことも求められる．それら指標を達成する軽量暗号は，IoT や CPS(Cyber Physical System)といった次世代ネットワークサービスを展開する上で有効なセキュリティ技術になると期待されている[8].

共通鍵暗号方式のブロック暗号は，混乱部と拡散部で構成されるラウンド関数の繰り返しにより設計されることが一般的である．拡散部は平文の変化を暗号文全体に拡散するものであり，線形変換が使用される．混乱部は平文から暗号文への非線形変換を行い，S-box(Substitution box)と呼ばれる変換関数が用いられる．S-box は暗号全体の唯一の非線形変換部のため，ブロック暗号全体の安全性と実装コストに直結する重要部分となっている．この S-box の設計手法として，AES や Camellia などで使用されるガロア拡大体の逆元とアフィン変換に基づく手法や DES や PRESENT，PRINCE などで使用されるランダム置換が知られている．一般的に S-box の長ビット化は非線形ならびに解読耐性向上につながるものの，その回路規模の増大が問題とされ，現在まで 8 ビットか 4 ビット S-box しか用いられていない.

一方で，離散力学系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, カオス写像は実数上で定義されるので, 充分な演算精度を持つ計算機による実数演算が必要となる．そのような計算機による演算に加えて，復号化を保証する一対一写像を得るために複雑な前処理を加えるなど，実装効率の面で課題がある方式が多くみられていた．実装性に優れた手法として，明示的な 1 対 1 写像関係を導入した Fredrich による整数値上の 2 次元 Baker 写像を用いる手法[9]や, Masuda らが提案した整数値上の 1 対 1 テント写像に基づく S-box 関数がある[10]．これらは簡単な算術演算のみのためソフトウェア実装が容易である一方で，ハードウェア実装の議論がされておらず，既存の暗号化と比べてその実装効率は期待できない.

そこで本研究では，上記カオスに基づく暗号化の問題点を克服するために，区分線形カオス写像に基づく整数値上の 1 対 1 写像の新しい構成法を与え，S-box を設計する． 一般的に，暗号の計算において計算量の多くが剰余計算に占められている．唯一の例外として，2 べき剰余環においてはビット以上の桁上がりを無視することがそのまま剰余計算になるため，大幅に計算量が少ない．そこで本研究では，デジタル実装に適する 2 べき剰余環上に離散力学系を展開し，安全性と軽量性を両立する新しい軽量暗号を提案する．また，提案した暗号の安全性と実装性能を評価し，既存暗号の AES と比較することで，本研究の有効性を実証する.

2 軽量カオス暗号

2-1 一対一カオス写像に基づく 16bit S-box の設計

デジタル実装に適した 2 べき剰余環上一対一カオス写像を設計するために，式(1)に定義される 2^m 区間を有する区分線形写像 $\tau(x)$:$I\rightarrow I$=[0,1]を用いる．

$$\tau(x)|I_i = (-1)^i 2^m x \bmod 1 \tag{1}$$

ここで，I_i=[2^i,2^i+1,…2^i+2^m-1]と定義する．m=3 の区分線形写像 $\tau(x)$を図 1 に示す．

ある初期値 x_0 から式(1)の繰り返し計算により得られる実数値系列は不規則な振る舞いとなり，その自己相関関数はデルタ関数的となることが知られている．しかしながら，実数演算を必要とすること，図で示されるように一対一写像でないため，復号に相当する逆写像が定義できず，暗号には適さない．

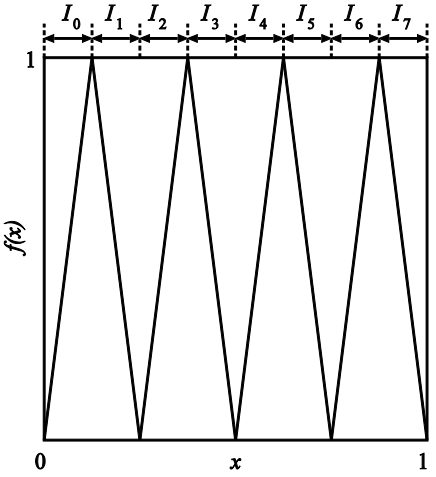

図 1:区分線形写像(m=3)

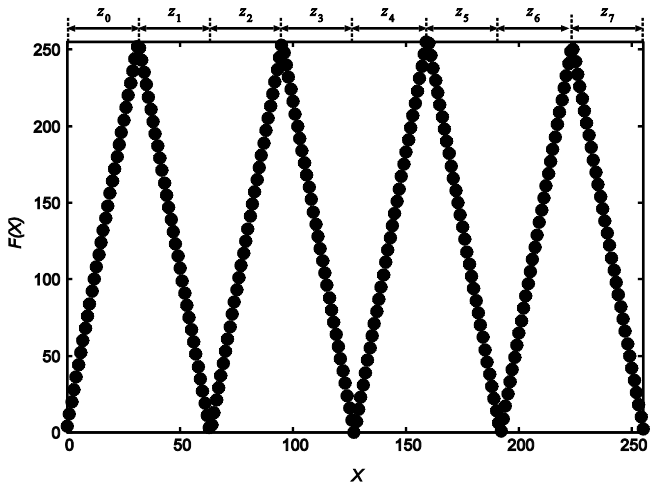

図 2:整数上一対一写像 F(m=3,k=8)

そこで本研究では，τ を近似する整数上一対一写像 F を以下に提案する．k を S-box のビット数とし，Z={0,1,…,2^k-1}と定義する．式(1)の整数近似写像として，式(2)を提案する．

$$F(X)|_{z_i} = \begin{cases} 2^m X \bmod 2^k + P\,(i) & i = 0,2,\ldots \\ -2^m X - 2^m \bmod 2^k + P\,(i) & i = 1,3,\ldots \end{cases} \tag{2}$$

ここで，P は F を一対一写像にするための m ビット置換と定義する．図 2 は k=8,m=3 の整数上一対一写像 F を示しており，τ を近似することが確認される．

式(2)を用いて，k ビット入力値 X から k ビット出力 Y を得る S-box を以下に定義する．

$$Y=S(X)=F^N(X) \tag{3}$$

ここで，N は写像 F の繰り返し数を表す．繰り返し数 N を十分大きくすれば，ランダムに近い変換になると期待される．また，写像 F は一対一写像になるので，その逆写像 F^{-1} が導出され

$$F^{-1}(X) = \begin{cases} \dfrac{X}{2^m} + 2^{k-m}\ P^{-1}(\mathrm{j}) & P^{-1}(\mathrm{j}) = 0,2,\ldots \\ -\dfrac{X}{2^m} + 2^{k-m} - 1 + 2^{k-m}P^{-1}(\mathrm{j}) & P^{-1}(\mathrm{j}) = 1,3,\ldots \end{cases} \tag{4}$$

ここで，j=X mod 2^m である．復号は F^{-1} を用いて，

$$X=S^{-1}(Y)=F^{-N}(Y) \tag{5}$$

として実行される．

また，一対一写像 F の計算は式(2)の簡単な整数演算のみを使用するため，その計算は極めて容易である．加えて，写像 F はクロック毎に m(m>2)ビット上位ビットシフトするシフトレジスタと，一対一写像を構成するための置換関数 P を実現する組み合わせ論理回路により回路実装できる．図 3 にその回路のブロック図を示す．

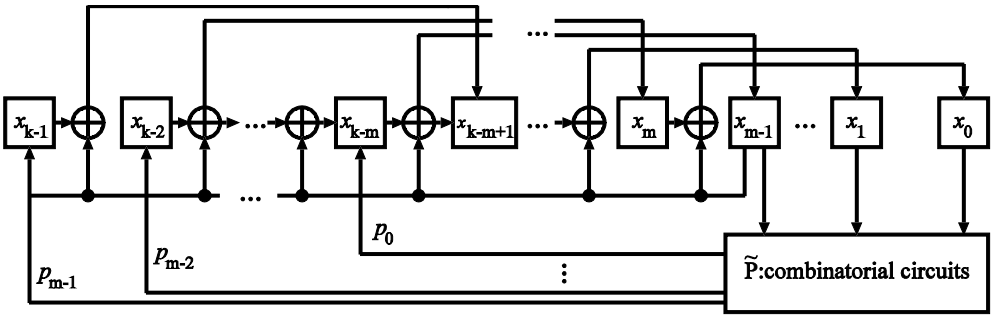

図 3: 写像 F のデジタル回路

整数 X と $Y = F(X)$ の 2 進展開をそれぞれ,

$$X = \sum_{n=0}^{k-1} x_n \, 2^{k-1-n} \tag{6}$$

$$Y = \sum_{n=0}^{k-1} y_n \, 2^{k-1-n} \tag{7}$$

とおく. 式(2) の $2^m X \bmod 2^k$ の演算は m ビットシフトに相当し，一方で$-2^m X - 2^m \bmod 2^k$ はその先頭 $k-m$ ビット反転で実行される．これらふたつの状態の判別は x_{m-1} が 0 か 1 で可能である.また置換 P の回路は x_0, $x_1,\ldots,x_{m-1}$ の m ビット入力を持つ m 個の論理関数 $p_0,p_1,\ldots,p_{m-1}$ で構成される．

一般的に S-box の長ビット化は非線形ならびに解読耐性向上につながるものの，その回路規模の増大が問題となる．DES などで用いられるランダム変換では，真正乱数を利用して事前に得られたランダム変換をメモリや LUT(Look Up Table)に保存するので，メモリサイズがビット数の指数オーダーで大きくなる．回路実装においても，k 入力 k 出力論理式の項数がビット数の指数オーダーで増えるため，回路規模が増大する．よって，ランダム変換ではこれまで 4 ビット S-box しか用いられていない．S-box の 8 ビット化はガロア体を用いることで達成され，ガロア体演算回路によりランダム変換よりも回路規模を抑えることが可能となった．しかしながら，16 ビットのガロア体演算回路の回路規模は大きくなるため，16 ビット以上はこれまで用いられていない.

一方で本研究で提案する整数上カオス写像に基づく S-box は，シフトレジスタと組み合わせ論理回路のみの実装となり，16 ビット化も可能である．提案回路のハードウェア実装評価のため，ハードウェア記述言語 Verilog-HDL を用いて論理記述を行い，Synopsys 社 Design Compiler による論理合成，東京大学 VDEC が提供する 0.8μm 三洋オンセミスタンダードセルライブラリを用いた実装評価を行った．k=16 とし，提案回路は置換 P のビット数 m で回路規模が異なるため，m=3,4,5 で評価した．その結果を表 1 にまとめる．

表1:回路面積(k=16)

	m=3	m=4	m=5
回路面積[μm^2]	44,928	56,979	73,476

表 2 SubBytes の回路面積

LUT[μm^2]	272,727
合成体[μm^2]	185,913

比較のため，AES の k=8 ビット S-box である SubBytes の回路実装も行った. SubBytes の回路実装手法として, LUT から論理合成ツールによる自動実装と, 合成体演算回路による実装が知られる. 合成体演算回路は, SubBytes の最もコンパクトな回路実装手法として知られる. 表1の結果と同様の設計条件の下評価した結果, LUT を用いた場合の回路面積は 272,727 μm^2 となり, 合成体を用いた手法で 185,913 μm^2 となった. 合成体回路に基づく SubBytes と比べ, 提案回路は k=16, m=5 の時で半分以下の回路面積を達成している. よって提案手法により, コンパクトな回路実装による 16 ビット S-box が設計できた.

次に，提案する 16 ビット S-box の解読耐性評価を行った．共通鍵暗号の一般的な攻撃手法として差分解読法と線形解読法が挙げられ，S-box の差分確率と線形確率がこれら解読法の耐性評価の指標となる．差分確率 DP は平文差分と暗号文差分の統計的偏りを表し，線形確率 LP は平文・暗号文間の線形近似式を評価するものであり，以下の式で与えられる[13],[14].

$$DP = \max_{\triangle X \neq 0, \triangle Y} \frac{\#\{X | F(X) \oplus S(X \oplus \triangle X\} = \triangle Y\}}{2^k} \tag{8}$$

$$LP = \max_{a,b \neq 0} \left(\frac{\#\{X | X \cdot a = S(X) \cdot b\}}{2^{k-1}} - 1\right)^2 \tag{9}$$

DP と LP はともに低いことが望ましく，AES の S-box である SubBytes は DP=LP=2^{-6} であることが理論的に導出されている．

そこで，本研究で提案する整数上カオス写像に基づく S-box の DP と LP を評価した．提案する S-box の DP と LP は，繰り返し数 N に依存するため，N が 30 まで DP と LP を評価し，その結果を図にのせる．ここでは ビット数を k=16, 置換 P のビット数を m=5 としている．図より，N が 20 までは N の回数を増やすほど DP と LP の値が改善され，最良値で DP=0.000275<2^{-11}, LP=0.000562<2^{-11} を達成していることがわかる．また，図中の破線は AES の SubBytes の DP と LP の結果であり，提案する S-box の方が DP と LP が低いことが確認される．これは，式(3)と(4)で示されるように，ビット数 k が大きいほど DP と LP は小さくなる傾向があることから，k=16 の提案 S-box の方が k=8 の SubBytes より改善できたと説明される．

以上の結果をまとめると, 提案する整数上カオス写像の繰り返しを用いることで, AES の SubBytes より回路規模を抑えた k=16 ビット S-box を設計可能となり, ビット数を増やすことにより差分確率と線形確率の大幅な改善も達成された.

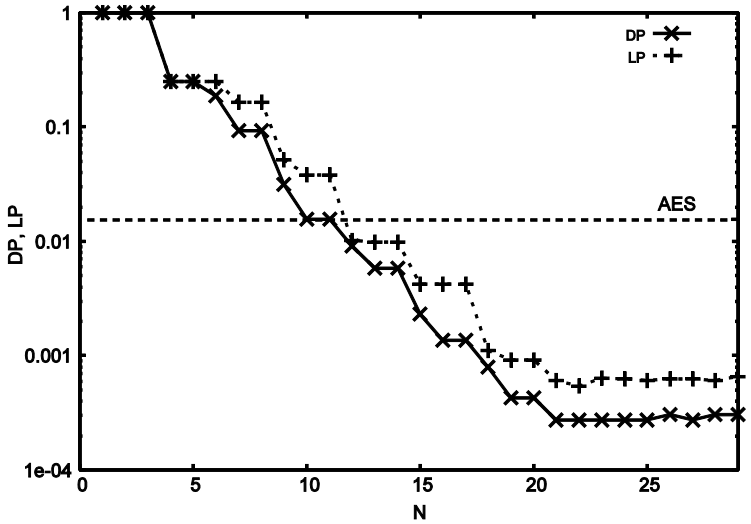

図 4：DP と LP

2-2 暗号復号共有回路

本研究で提案する整数上カオス写像 F の演算は m ビット上位シフト，逆写像 F^{-1} は，m ビット下位シフトを基本とする．これらは，暗号・復号を制御入力により切り替える両方向シフトレジスタを用いて実装可能である．また，F には置換 P を必要とし，F^{-1} には P^{-1} を必要とするので，暗号・復号を考えると，図 5 に示すような m ビット入力 m ビット出力論理回路 P と P^{-1} と暗号･復号を切り替える m ビットマルチプレクサが必要となる．

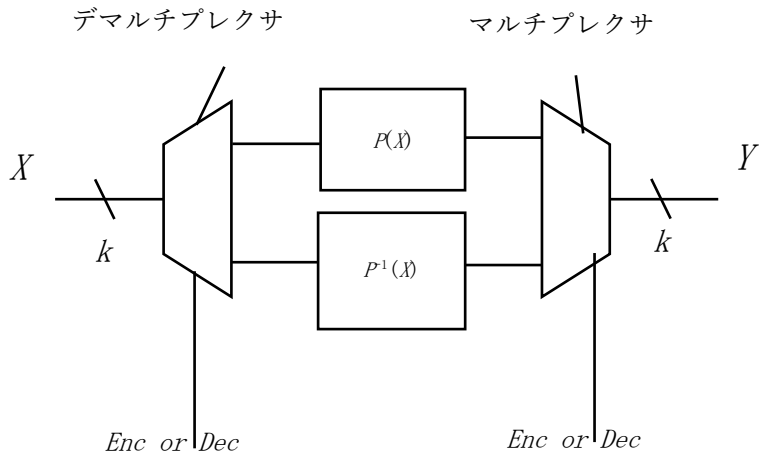

図 5：置換 P の暗号・復号回路

本研究では，復号回路 P^{-1} の回路実装を簡略化するために，以下を満たす置換 Q を P に作用させることで逆置換 P^{-1} を得る手法を提案した．

$$P^{-1}=Q\circ P\circ Q \tag{5}$$

ここで置換 Q は P と同じ m ビット置換であり，$\circ$は置換の合成演算を表す．入力 X を置換 F で変換し，出力 Y を得たとする．出力 Y を X へ戻すために，出力 Y に対して置換 P を作用させた後，もう一度置換 F，置換 P で変換を行うことで，入力 X に戻す逆置換を行う．

例として，m=3 ビット置換 P の例を式(6)に示す．

$$P=\begin{pmatrix}0&1&2&3&4&5&6&7\\3&7&5&4&0&2&6&1\end{pmatrix} \tag{6}$$

式(5)を満たす置換 Q として，以下が挙げられる．

$$Q=\begin{pmatrix}0&1&2&3&4&5&6&7\\4&1&2&3&0&5&6&7\end{pmatrix} \tag{7}$$

この例では，X=0 で Y=F(0)=3 が得られるので，Y=3 から P(3)=3→F(3)=4→P(4)=0 となり，$Q\circ P\circ Q$ の演算により入力値 0 に戻ることが確認される．

式(3)の置換 P の逆置換 P^{-1} の回路は，3 ビット入力を $x_0x_1x_2$，3 ビット出力を $y_0y_1y_2$ とすると，簡略化した積和形論理式は以下に求められる．

$$y_0=\overline{x_0}\,\overline{x_1}+x_1\overline{x_2}$$
$$y_1=x_0\overline{x_2}+\overline{x_1}x_2$$
$$y_2=\overline{x_0}\,\overline{x_1}x_2+\overline{x_0}x_1\overline{x_2}+x_0\overline{x_1}\,\overline{x_2}+x_0x_1x_2$$

一方で Q では，X=0 と X=4 の値のみ入れ替えている．つまり，値の入れ替えを行う X=0，4 の場合の論理回路を作ればよく，その他の入力値の時はそのまま出力値にすればよい．入れ替え部回路の出力をp_0'，p_1'，p_2'とすると，論理式は$p_0'=\overline{x_1}\,\overline{x_2}$となる．．図 4 に P と P^{-1}= $Q\circ P\circ Q$ を 1 ビットセレクタで切り替える暗号・復号回路を示す．提案手法の回路実装では，P の論理回路を 2 つ必要とするが，図 5 に示す P と P^{-1} を実装する場合よりも簡単化されると期待できる．

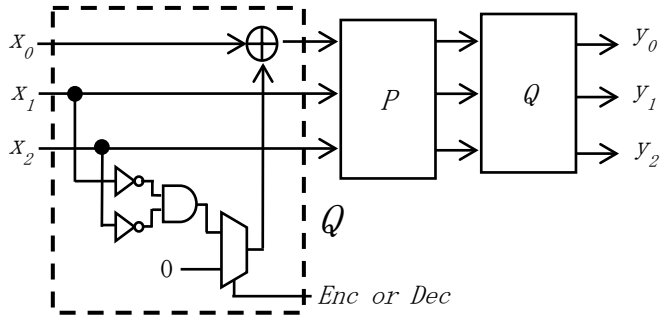

図 6:置換・逆置換回路

図 6 に示しように置換 Q を用意することで，復号回路の簡略化が達成されることがわかる．問題は任意の置換で式(4)を満たす Q が得られるかであるが，これが可能なことを，次に示す．

命題：P，Q を k ビット置換とすると，任意の P で式(5)を満たす $Q(\neq P^{-1})$が存在する．

証明：(4)の両辺に P を作用させると

$$P^{-1}\circ P=Q\circ P\circ Q\circ P$$
$$I=(Q\circ P)^2$$

と導出される．ここで I は k ビット恒等置換とし，任意の$x \in \{0,1,\ldots,2^k-1\}$で，$I(x)=x$ を満たす．置換は合成演算で閉じており，$Q\circ P$ も置換となる．上式より $Q\circ P$ は，2 回作用させると恒等置換になる置換を意味し，これは $Q\circ P$ を巡回置換として表記したときに，長さが高々2 となるものである．$P\neq P'$なら $Q\circ P\neq Q'\circ P$ のため，$Q\circ P$ から任意の置換を得ることができ，巡回置換の長さが高々2 となる置換が必ず存在する． ■

置換 Q の総数は $2^k!$で与えられ，式(5)を満たす逆置換可能な置換 Q の総数は式（8）で与えれる．

$$\sum_{i=1}^{2^{k-1}} {}_{2^k}C_{2^k-2i} \times \prod_{j=1}^{i} 2j-1 \qquad (8)$$

2 つの式を比較すると $2^k!$の方が増加する速度が速く，逆置換可能な P の割合は急速に減少してく．そこで，任意の F に対して逆置換可能な P を効率よく構成する手法を提案する．

前節で述べた逆置換回路は図 3 の入替部で回路規模が決まる．よって，入れ替えの数が少ないほど回路構成が小さくなると考えられる．そこで，任意の置換 F に対して，入れ替え数が最小となる置換 P を構成するアルゴリズムを以下に示す．

1. (初期化)： 置換 P を M 個の巡回置換の積として表現し，

$$\mathrm{P}=\prod_{i=1}^{M}\sigma_i$$

また，各巡回置換 σ_i の長さ N_i とし，

$$\sigma_i=(a_0^i,a_1^i,\ldots,a_{N-1}^i)$$

とする．Q は恒等置換とする．つまり，i=0,1,…,2^k-1 に対し，$Q(i)=i$ としておく．$j\leftarrow 1$ として処理 2 へ

2. (終了条件)： $j>M$ なら終了，でなければ 3 を実行する．
3. (長さの判定)： $N_j\leqq 2$ なら $j\leftarrow j+1$ を実行し，処理 2 へ．そうでなければ処理 4 を実行．
4. (P の構成) ：すべての m=1,…,$\left\lceil\frac{N_i}{2}\right\rceil$-1 に対して，$Q(a_{2m}^j)\leftarrow a_{2(m-1)}^j$を実行．$N_j$が偶数の時 $Q(a_0^j)\leftarrow a_{Nj-2}^j$，

N_jが奇数の時 $Q(a_0^j)\leftarrow a_{Nj-1}^j$．$j\leftarrow j+1$ として処理 2 へ．

提案手法では，置換 P の巡回置換 $\sigma_i=(a_0^i,a_1^i,\ldots.a_{Ni-1}^i)$の長さが 3 以上の偶数の時，$QP$ により $(a_0^i,a_1^i)(a_2^i,a_3^i)\ldots(a_{N-2}^i,a_{N-1}^i)$とすべて長さ 2 の巡回置換を構成する．このことは，$P(a_{2m}^i)=a_{2m+1}^i$，から $Q(a_{2m+1}^i)=a_{2m+1}^i$，$P(a_{2m+1}^i)=a_{2m+2}^i$，$Q(a_{2m+2}^i)=a_{2m}^i$ より，Q∘Pは，長さ 2 の巡回置換(a_{2m}^i,a_{2m+1}^i)を持つこと

から示される．長さが 3 以上のとき奇数の時も同様にして，$(a_0^i, a_1^i)(a_2^i, a_3^i)\ldots(a_{N-3}^i, a_{N-2}^i)(a_{2N-1}^i)$と長さ 2 と長さ 1 の巡回置換を構成することが示される．

2-3 128 ビット軽量カオス暗号の設計

共通鍵暗号方式のブロック暗号は，混乱部と拡散部で構成されるラウンド関数の繰り返しにより設計されることが一般的である．混乱部では，本研究で提案する 16bit S-box を 8 個用いて 128 ビット暗号を構築できる．拡散部では S-box 出力値の変化と暗号鍵が全体によく混ざるように混合変換(Mixing 変換)を使用する．この暗号を軽量カオス暗号と名付け，その概要図を図 7 に示す．

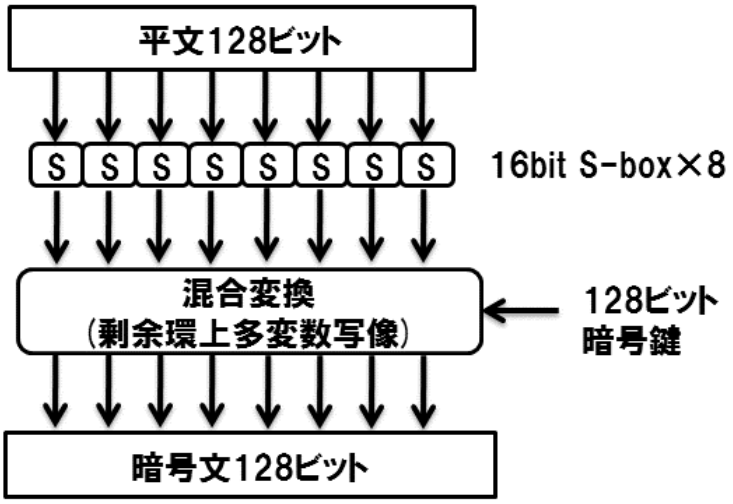

図 7:軽量カオス暗号のブロック図

一般的にブロック暗号の回路面積は，混乱部に相当する S-box で大部分を占める．そこで，東京大学 VDEC が提供する 0.8μm 三洋オンセミスタンダードセルライブラリを用いた ASIC 実装評価を行った表 1 と表 2 の結果を用いて 128 ビットブロック暗号の回路面積を試算する．まず AES では，SubBytes の LUT 方式では 16 × 272, 727 = 4, 363, 632 μm^2，合成体では 16 × 185, 913 = 2, 974, 608 μm^2 必要である．一方で提案する軽量カオス暗号では 16 ビット S-box を 8 個使用するだけなので，8×73,476 = 587, 808 μm^2 となる．128 ビット暗号回路として比較した場合，LUT 方式より約 0.13 倍，合成体より約 0.20 倍程度の回路面積に縮小できる．回路規模の制約が厳しい IC チップや RFID などの小型デバイスなどの実装を考えた場合，提案する軽量カオス暗号は特に有効と考えられる．

3 まとめ

本研究は，不規則な振る舞いを示すカオス写像に基づく整数上一対一写像の構成法を与え，その繰り返し計算による S-box の構成法を与えた．簡単な整数演算のみを用いるため，ソフトウェア実装・ハードウェア実装が容易となり，国内外でも例のない 16 ビット S-box が実現できた．128 ビットブロック暗号の場合，16 ビット S-box を 8 個のみで暗号が構築でき，16 ビット化の恩恵による S-box の非線形性も大幅に向上する．また，提案する S-box は共役変換に基づく暗号・復号回路の共通化も可能であり，S-box の復号回路実装を不要とする点も応用上のみならず，学術上においても重要な成果になると期待できる．

近年，AES よりも回路規模を抑えた軽量暗号として PRESENT(欧州)，LED(シンガポール), Piccolo(Sony), TWINE(NEC)などが提案されている．これらは 4 ビット S-box を用いるので，S-box 数を抑えるために 64 ビット暗号で提案されており，一度に暗号化できるビット数が少ないことはデメリットである．また 4 ビット S-box の非線形性が良くないため，ラウンドと呼ばれる暗号用変換処理を 30 回以上必要とすることから，処理時間にも課題がある．一方で本研究で提案する S-box は 16 ビットのため，差分確率・線形確率が向上するため，ラウンド数も少ないと期待できる．

これまで，カオスの暗号化への応用も盛んに研究されていたが，実数計算や暗号用一対一写像を構成するための複雑な前処理が必要とされるなど，それら手法の多くは実装効率の問題が挙げられていた．本研究で提案する軽量カオス暗号は，AES などの既存手法と比べて実装効率に優れるはじめてのカオス暗号であり，離散力学系カオスの暗号への応用を大きく前進させるものと考える．

【参考文献】

[1] J. Daemen and V. Rijmen, ”The Design of Rijndael”, Springer, 2002.

[2] 青木，市川，神田，松井，盛合，中嶋，時田，“128 ビットブロック暗号 Camellia”，電子情報通信学会技術研究報告 ISEC2000-6, May 2000.

[3] 白井，渋谷，秋下，盛合，岩田，“128 ビットブロック暗号 CLEFIA，″電子情報通信学会技術研究報告，ISEC2007-1 (2007-05)，2007.

[4] A.Bogdanov, L.R.Knudsen, G.Leander, C.Paar, A.Poschmann, M.J.B.Robshaw, Y.Seurin, and C.Vikkelsoe, ”PRESENT: an ultra-lightweight block cipher”,CHES,Proceedings,vol 4727 of Lecture Notes in Computer Science, pp.450-466. Springer, 2007.

[5] J.Borghoff, A.Canteaut, T.Guneysu, E.Kavun, M.Knezevic, L.R.Knudsen, G.Leander, V.Nikov, C.Paar, C.Rechberger, P.Rombouts, S.S.Thomsen, and T.Yalcin, ”PRINCE - A low latency block cipher for pervasive computing applications”. ed. ASIACRYPT2012, Proceedings,vol 7658 of Lecture Notes in Computer Science, pp 208-225. Spinger, 2012.

[6] T.Suzaki, K.Minematsu, S.Morioka and E.Kobayashi, ”TWINE: A Lightweight, Versatile Block Cipher,” ECRYPT Workshop on Lightweight Cryptography November 28-29, 2011.

[7] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai, “Piccolo: An Ultra-Lightweight Blockcipher.” CHES 2011,LNCS 6917, pp. 342-357, 2011.

[8] CRYPTREC 軽量暗号ワーキンググループ，”CRYPTREC 暗号技術ガイドライン(軽量暗号)”，2017.

[9] J. Fridrich, “Symmetric ciphers based on two dimensional chaotic maps”, Int. J. Bifurcation and Chaos, Vol. 8, No. 6, pp.1259-1284, 1998.

[10] N. Masuda and K. Aihara, “Cryptosystems with discretized chaotic maps,” IEEE Trans. Circuits and Systems I, vol.49, pp.28-40, 2006.

[11] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, “A compact Rijndael hardware architecture with S-Box optimization,”ASIACRYPT 2001, pp.239-254, 2001.

[12] S. Morioka and A. Satoh, “A logic design methodology of low-power AES cryptographic circuits,” ISPJ Journal, vol.44, no.5, pp.1321-1328, 2003. (in Japanese)

[13] E. Biham and A. Shamir, “Differential cryptanalysis of DES-like cryptosystems,” Advances in Cryptology-CRYPTO’90, Springer-Verlag, pp.2-21, 1991.

[14] M. Matsui, “Linear cryptanalysis method for DES cipher,”Proc. Eurocrypt 93 Advances in Cryptology, pp.386-397,1994

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
置換の合成に基づく逆置換の生成	電子情報通信学会九州支部学生会講演会	2020 年 9 月
置換の合成に基づく逆置換の構成法	電子情報通信学会非線形問題研究会 (NLP)	2021 年 6 月