Vol.2010-CSEC-50 No.10
2010/7/1

可変 S-box による共通鍵暗号の安全性向上についての研究

中山　俊一郎[†]　　長瀬　智行[†]　吉岡　良雄[†]

本報告では，可変 S-box のための新しい変換アルゴリズムを提案する.可変 S-box は差分/線形解読法に対して安全性を向上させるため, AES の S-box の線形変換処理を秘密鍵によって動的に変更する手法である[2]. 提案した手法について差分/線形解読法による安全性評価を行い, MADP／MALHP において 安全性が AES より高くなるという結果を得た．しかしながら，HMDP／MALHP に関しては AES には及ばなかった.

Research on a Mutable S-box for Public key Cryptography

Shunichiro Nakayama[†], Tomoyuki Nagase[†] and Yoshio Yoshioka[†]

This report proposes a new transformation's algorithm for a mutable S-box which has been proposed in [2] to improve the complexity of the S-Box's structure and to provide an optimal degree of resistance against differential cryptanalysis and especially the linear cryptanalysis. The structure of the AES S-box has been expanded and modified to be congruent with the proposed algorithm and to obtain appropriate nonlinearity of the S-box. The Cryptanalysis of the new algorithm model is based on the maximum average differential probability (MADP) and maximum average linear hull probability (MALHP). The results show that proposed model significantly improves MADP and MALHP. Furthermore, the results that have been obtained exhibit good enough confusions to achieve high security level.

1. はじめに

現在，最も利用されている共通鍵暗号の解読方法として統計的な性質を利用した差分／線形解読法がある．これは非線形変換処理部における　入出力の値の確率を基に鍵を推測する方法である．共通鍵暗号を使用する上で，これらの解読から安全性を確保するには，鍵が推測される前に鍵を変更する必要がある．

筆者らは，差分／線形解読法での攻撃に対する安全性を向上させるため，非線形変換処理に動的な線形変換処理を組み合わせて，入出力パターンを増やす手法を提案した[2]. 更なる安全性の向上を図るため暗号鍵データを基に線形変換処理部を動的に変更する S-box の作成を行った．

本論文は，差分/線形解読法に対する安全性を向上させるため，AES (Advanced Encryption Standard)の S-box の線形変換処理を秘密鍵によって動的に変更する可変 S-box(M_S-box)を提案する．そして，この方法に対する安全性の評価を行い，検討を加える．

2. 可変 S-box の提案

AES の S-box は，図 1 に示すように非線形変換処理と線形変換処理から成り立っている．前者の非線形変換は入力 x に対し，ガロア体 GF(2^8)で逆元を取る．後者は次式で示されるアフィン変換である．

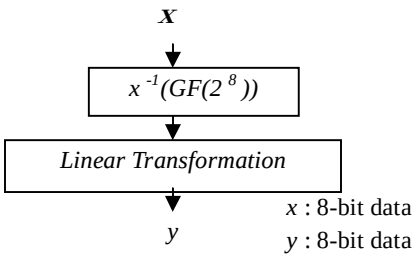

図 1　AES の S-box
Figure 1 S-box of AES

† 弘前大学大学院理工学研究科
Graduate School of Science and Technology, Hirosaki University

Vol.2010-CSEC-50 No.10
2010/7/1

$$\begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} \oplus \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \quad (1)$$

この式において排他的論理和を行う数値は$(63)_{16}$であり，1-byte のデータとして扱うことができる．

筆者らが最初に提案した可変 S-box (M_S-box. ver.1)の構成について以下に説明する．まず，このアルゴリズムのフローチャートは図 2 のようになる．大きな改良点は，本来 GF(2^8)での逆元演算を 1 回行うだけであったが，逆元演算を 3 回に増やしたことである．すなわち，入力データ x(8-bit)に対して，ガロア体 GF(2^8)での逆元演算を行い，これを T_1 とする．T_1 を *SP* 部において秘密鍵を用いた並び替えを行い，T_2(5-bit)と T_3(3-bit)とする．これらの逆元をそれぞれ演算し，T_4，T_5 とする．*SP* 部においてこの 2 つを結合し T_6 とし，T_6 に対して線形変換処理を行い，出力値 y を決定する．なお，AES 内部での線形変換処理は式(1)である．

このような改良を行った結果，本来 1 通りの出力しか持たない AES の S-box が 48 通りの出力を持つ処理部として改良することができた．しかし，特定の値が入力されると秘密鍵を作用させても全ての出力が同じになってしまうことが明らかになった．ここで，SP 部において，5-bit と 3-bit で分割した理由は，ガロア体の位数の次数が奇数の時の方が差分／線形解読法に対して安全であるからである[3].

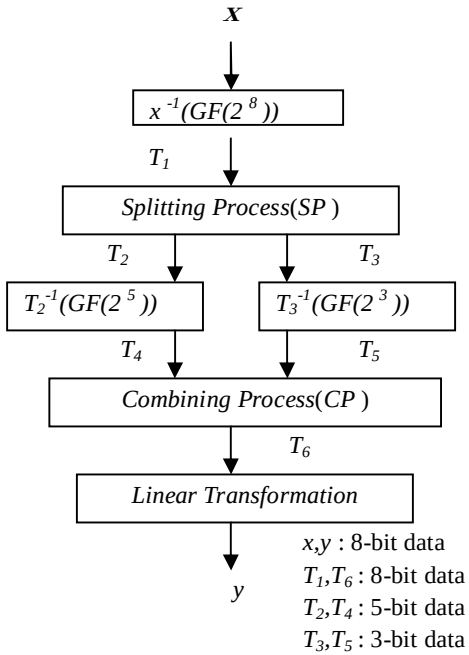

図 2 M_S-box.ver.1 のフローチャート
Figure 2 Flow chart of M_S-box.ver.1

次に，本論文の中心となる M_S-box.ver.2 の構成について図 2 を用いて以下に説明する．まず，入力データ x（8-bit）に対して，ガロア体 GF(2^8)における逆元を求めこれを T_1 とする．次に動的線形変換処理を行い，これを T_2 とする．その後，SP 部において T_3(5-bit)と T_4(3-bit)に分割する．T_3 および T_4 の逆元をそれぞれ演算し T_5，T_6 とする．その後，CP 部にて T_5 と T_6 を連結し，出力値 y を決定する．

M_S-box ver.1 との違いは，線形変換処理を動的にし，ガロア体を使用する逆元演算部と入れ替えたことである．この理由は，前述したように M_S-box ver.1 では特定の値を入力すると，全出力が一定の値しか出力しなくなる．例を挙げると$(00)_{16}$ が入力されると秘密鍵によって変化する 48 種類の全ての出力が$(63)_{16}$ で統一されてしまう．この問題を解決するために線形変換部と非線形変換部を入れ替えた．

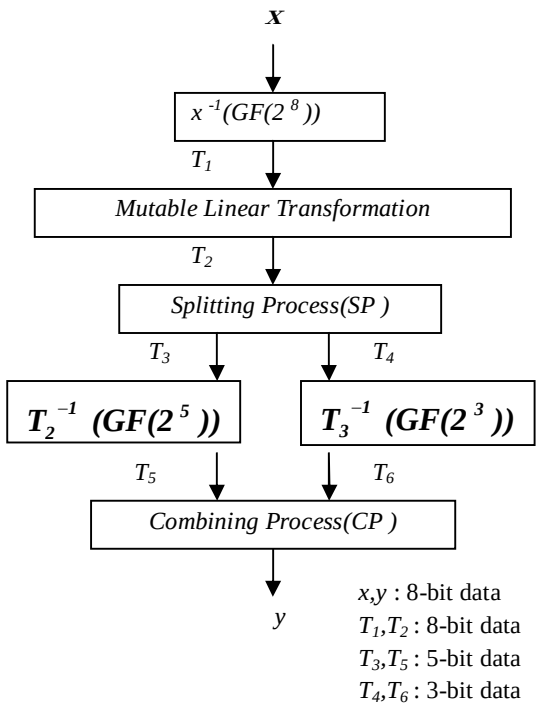

図 3　M_S-box.ver.2 のフローチャート
Figure 3　Flow chart of　M_S-box.ver.2

M_S-box の入出力パターンはパラメータ initial point(α)と kernel value(N)によって決まる．そして，これらのαとNは，SP 部において 15-bit のサブ鍵(Sub Key)から算出される．αとNの範囲は，各々0≦α≦7，2≦N≦7 となっており，入出力パターンは 48 通りとなる．AES の S-box におけるアフィン変換では 8×1 行列の値として$(63)_{16}$が使われていたため，M_S-box ver.1 においても$(63)_{16}$を使っていた．しかし，αとNの入出力パターンに対して$(63)_{16}$よりも安全性において有効な値があることが分かった．そこで，次式のように，アフィン変換の排他的論理和の被データ(m_0～m_7)を可変にした．

$$\begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} \oplus \begin{pmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \\ m_6 \\ m_7 \end{pmatrix} \quad (2)$$

これによって，入出力パターンが 48 通りから $48\times 2^8=12288$ 通りに増やすことができる．そして，αとNの入出力パターンに対して，安全性において有効な値の一部を表 1 に示した．この中から差分／線形解読法に対して強い安全性を有する動的線形変換，およびαとNの組み合わせを選ぶことによって安全性を高めることができる．
表 1 の有効な値に対するαとNによる排他的論理和の値 *XOR*-data は，図 4 に示すように秘密鍵から導き出されるサブ鍵 15 ビットを 5 ビットずつ分け，次式のように排他的論理和をとることである．

$$XOR-\text{data} = (A \oplus B \oplus C) \bmod (M) \quad (3)$$

ここで，*M* は表 1 における count 列の値である．これを利用する場合，処理を速くするため，αとNの値を事前に計算しておき，該当する剰余 *XOR*-data を求めるようにする．

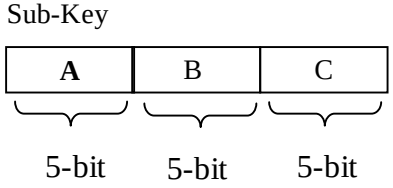

図 4　スケジューリングアルゴリズム
Figure 4 Scheduling Algorithm

表 1　αとNの値に対する有効なアフィン変換の値
Table 1 Value of effective affine-transformation to value of α and N

α	*N*	*count*	*XOR*
0	2	14	{17}{1f}{6c}{7e}{a0}{a4}{b2}{c5}{d3}{d8}{e3}{ed} {f3}
	3	18	{15}{17}{48}{58}{7a}{84}{86}{8d}{9a}{a1}{b6}{ce}{cf}{d7} {d8}{da}{e1}
⋮	⋮	⋮	⋮
7	6	22	{1a}{24}{29}{30}{34}{4f}{51}{55}{59}{6a}{73}{81}{85}{88} {8d}{90}{9a}{c9}{da}{de}{e9}{ff}
	7	18	{0e}{23}{43}{47}{49}{60}{89}{91}{ab}{b0}{bc}{da}{e8}{ec} {f7}{f8}{f9}{fb}

3. 安全性評価

本論文における安全性評価は，差分／線形解読法によって行う．そして，最大差分(MDP)／線形(MLP)確率および最大平均差分(MADP)／線形(MALHP)確率を算出し，比較評価する．ただし，M_S-box は，αとN，および *XOR*-data によって S-box の値が変化するので，取りうる全ての入出力パターンについて最大差分(MDP)／線形(MLP)確率を求め，その中の最大の値を M_S-box の最大差分(MADP)／線形(HMLP)確率とする．この値を従来の最大差分(MDP)／線形(MLP)確率と区別するために，Highest Maximum Differential／Linear Probability とする．これによって 792 通りの出力がこの解読法に対する強さを調べることができる．その中でも一番脆弱だった値を表 2 に示す．なお，これらの安全性評価に用いた式は付録に示してある．

表 2　セキュリティレベルの比較
Table 2 Comparison of security levels

	MADP	MALHP	HMDP	HMLP
AES	2^{-6}	2^{-6}	2^{-6}	2^{-6}
M_S-box ver.1	$2^{-6.40}$	$2^{-6.67}$	$2^{-4.19}$	$2^{-3.36}$
M_S-box Ver.2	$2^{-7.15}$	$2^{-7.33}$	$2^{-4.68}$	2^{-4}

表 2 の結果から，MADP／MALHP に関して，標準となる AES の値から比べ M_S-box ver.1 の安全性は高くなっており，M_S-box ver.2 に関してはさらに高くなっていることが分かる．これは出力パターンを増加させたことと，図 4 に示すスケジューリングを適用したためである
HMDP／HMLP に関しては，M_S-box ver.1 よりも M_S-box ver.2 の安全性が高くなっているため，改良には成功しているが，従来の AES と比べて安全性が低い．αと N の値によってアフィン変換の値を選択するように改良したが，更なる改良が必要である．

4. おわりに

本論文では，差分/線形解読法に対する安全性を向上させるため，共通鍵暗号アルゴリズムである AES の S-box を秘密鍵で動的に変更する手法を提案した．改良点としては線形変換を動的な処理にして非線形変換と入れ替えを行い出力値に変化を与えた．それによって入出力パターンは 792 個に増えた．次に，この方法に対する安全性の評価を行い，MADP／MALHP において，安全性が従来の AES より高くなるという結果を得た．しかしながら，HMDP／MALHP に関しては，AES には及ばなかった．
今後の課題としては，HMDP／HMLP の安全性に対する改良を行うことである．

参考文献

[1] J. Daemen and V. Rijmen, “The Design of Rijndael: AES – The Advanced Encryption Standard,” Springer-Verlag. 2002.
[2] A. Watanabe, H. Haruki, S. Shimotomai, T. Saito, T. Nagase, Y. Yoshioka and Y. Hasegawa,” A New Mutable Nonlinear Transformation Algorithm for S-box,” IEEE, AINA 07, Vol.1, pp.246-251, 2007.
[3] Mitsuru MATSUI, “Block Encryption Algorithm MISTY,” ISEC96-11, 1996.
[4] Teruyoshi YAMAGUCHI, Tomonori HASHIYAMA and Shigeru OKUMA, “A New Encryption Using Dynamic Reconfiguration of S-Box and Its Security against Cryptanalysis,” IEICE, Vol.J86-A No.8 pp.860-871, Aug. 2003.
[5] Data encryption standard (DES), FIPS PUB 46-2, Dec.30, 1993.

付録

1．安全性評価に関して

まず，評価に用いる変数名を以下に説明する．

$x : S-box$への入力

$y : S-box$からの出力

$F(x) : x$をyに変換する関数$(S-box)$

$\Delta x : x$の差分

$\Delta y : y$の差分

$\oplus$:ビット単位でのXOR演算

$\#\{x\} : x$の個数

k:可変$S-box$として機能させるための変数

$\Gamma x, \Gamma y : x, y$の入出力マスクペア

以降において，安全性評価に用いた公式を以下に示す．

差分確率 DP：Differential Probability

$$DP^f(\Delta x, \Delta y) \stackrel{def}{=} \frac{\#\{x \mid F(x) \oplus F(x \oplus \Delta x) = \Delta y\}}{2^n} \tag{A.1}$$

線形確率 LP：Linear Probability

$$LP^f(\Gamma x, \Gamma y) \stackrel{def}{=} \left(2\frac{\#\{x \mid x \bullet \Gamma x = F(x) \bullet \Gamma y\}}{2^n} - 1\right)^2 \tag{A.2}$$

最大差分確率 MDP：Maximum DP

$$MDP \stackrel{def}{=} \max_{\Delta x(\neq 0), \Delta y} DP^f(\Delta x, \Delta y) \tag{A.3}$$

最大線形確率 MLP：Maximum LP

$$MLP \stackrel{def}{=} \max_{\Gamma x, \Gamma y(\neq 0)} LP^f(\Gamma x, \Gamma y) \tag{A.4}$$

HMDP：Highest MDP

$$HMDP \stackrel{def}{=} \max_{\Delta x(\neq 0), \Delta y} MDP_k(\Delta x, \Delta y) \tag{A.5}$$

HMLP：Highest MLP

$$HMLP \stackrel{def}{=} \max_{\Gamma x, \Gamma y(\neq 0)} MLP_k(\Gamma x, \Gamma y) \tag{A.6}$$

平均差分確率 ADP：Average DP

$$ADP^f(\Delta x, \Delta y) \stackrel{def}{=} \frac{1}{2^t}\sum_k \frac{\#\{x \mid F_k(x) \oplus F_k(x \oplus \Delta x) = \Delta y\}}{2^n} \tag{A.7}$$

平均線形確率 ALP：Average LP

$$ALP^f(\Gamma x, \Gamma y) \stackrel{def}{=} \frac{1}{2^t}\sum_k \left(2\frac{\#\{x \mid x \bullet \Gamma x = F_k(x) \bullet \Gamma y\}}{2^n} - 1\right)^2 \tag{A.8}$$

最大平均差分確率 MADP：Maximum ADP

$$MADP \stackrel{def}{=} \max_{\Delta x(\neq 0), \Delta y} ADP^f(\Delta x, \Delta y) \tag{A.9}$$

最大平均線形確率 MALHP： Maximum Average Linear Hull Probability

$$MALHP \stackrel{def}{=} \max_{\Gamma x, \Gamma y(\neq 0)} ALP^f(\Gamma x, \Gamma y) \tag{A.10}$$