02-01062

暗号システムの安全性を向上させる暗号化モードに関する研究（継続）

桑 門 秀 典　神戸大学 工学部 助教授

1 はじめに

1.1 背景と目的

安全な通信を実現するためには，できるだけ解読困難な暗号を利用することが望ましいが，一般的に解読困難な暗号は，その暗号化・復号に多くの時間やメモリを必要とする。しかし，最近，暗号化をする前に平文に適切な変換を行うこと（暗号化モードと呼ぶ）によって既存の暗号システムの安全性を，効率をあまり犠牲にすることなく，向上できることが明らかにされつつある。これまでに，目的に応じて様々な暗号化モードが提案されている。例えば，適応的選択平文攻撃に対して安全性を向上させる暗号化モード，鍵の全数探索に対して安全性を向上させる暗号化モード，暗号文の改ざんを検出する暗号化モードなどがある。

これらの暗号化モードの目的は各々異るが，平文に適切な冗長を付加するという手法は共通である。平成14年度に貴財団から研究助成を頂き，平文に付加する冗長の性質に着目し，個別の暗号化モードにより実現されてきた安全性の向上を同時に実現する暗号化モードの研究を行った[4]。その結果，これまでに提案された幾つかの暗号化モードの特徴を兼ねそろえた暗号化モードを考案できた。また，研究の過程において，高い安全性を実現するためには，以下のことが避けられないことが判明した。

問題点(a)　実時間で逐次的に暗号化・復号することが難しい。

問題点(b)　暗号文の一部でも欠落すると，全体が復号不可能になる。

問題点(c)　暗号文のデータ量が平文のデータ量より多くなる。

一般的には，安全性の高い暗号化モードを利用することが望ましい。しかし，安全性をやや低下させて，上記(a)(b)(c)を改善したほうが良いアプリケーションもある。そこで，平成15年度の研究目的は，上記(a)(b)(c)の問題を解決しつつ，できるだけ高い安全性を有する暗号化モードの考案することである。

1.2 本研究の概要

平成15年度の研究内容は，大きく二つに分かれる。一つめは，問題点(a)を解決するために，できるだけ効率のよい暗号化モードを考案することである。二つめは，問題点(c)を解決するために，暗号文のデータ量と平文のデータ量が等しい暗号化モードを考案することである。

どちらの場合においても，本研究では，all-or-nothing 暗号化モードに着目した。all-or-nothing 暗号化モードは，秘密鍵を使わずに平文を撹拌するスクランブル部と秘密鍵を使ってデータを暗号化する暗号化部の二つから構成される。そして，スクランブル部に all-or-nothing transform を用いると，暗号化モード全体として自動的に非分離特性をもつ。したがって，暗号化部に他の暗号化モードを用いると，その暗号化モードの特徴も暗号化モード全体としてもつことになる。

問題点(a)の解決（２章）： 優れた all-or-nothing transform である optimal asymmetric encryption padding[2]に暗号化機能を付加し，暗号化部を省略することにより，処理速度の向上を目指した[5]。

問題点(c)の解決（３章，４章）： データ量が不変な all-or-nothing transform については，情報理論的立場からの研究はあった。しかし，その安全性の定義は，データ量が増加する all-or-nothing transform の安全性の定義と比較すると，弱いものであった。一方，データ量が増加する all-or-nothing transform の安全性の定義は非常に厳しく，データ量が不変な all-or-nothing transform ではその定義を満足することができなかった。そこで，本研究では，まず，データ量が不変な all-or-nothing transform に適した安全性の定義を与えた。そして，その

定義の下で安全となるデータ量が不変な all-or-nothing transform を提案した。

2　効率的な非分離暗号化モード

2.1　アルゴリズム

ビット系列の連接を $\|$ で，ビット毎の排他的論理和を $\oplus$ で表す。h を $\{0,1\}^*$ から $\{0,1\}^\ell$ へのハッシュ関数，g を $\{0,1\}^\ell$ から $\{0,1\}^*$ への擬似乱数生成器とする。m を L ビットの平文とする。送信者と受信者の二者が共有する ℓ ビットの鍵を k とする。ℓ ビットの乱数系列をrとし，平文 m を以下のように暗号化する。

$$c^{(1)} = m \oplus g(r),$$
$$c^{(2)} = r \oplus k \oplus h(c^{(1)}).$$

暗号文は，$c = c^{(1)} \| c^{(2)}$ である。

提案暗号化モードは，optimal asymmetric encryption padding[2]に似ている。optimal asymmetric encryption padding は秘密鍵を必要としないスクランブルであるが，提案暗号化モードは秘密鍵を必要とする暗号化であることに注意しよう。

2.2　安全性の検討

ハッシュ関数 h が以下の性質をもつとする。

1．任意の y に対して，$y = h(x)$ を満たす x を求めることが難しい。また，$h(x) = h(z)$ となる x,z を求めることが難しい。
2．多くの $(x, H(x))$ の組が与えられても，新しい入力 x に対する $h(x)$ の値を部分的でさえ予測することは難しい。

次に，擬似乱数生成器 g が以下の性質をもつとする。

1．$y = G(x)$ が与えれたとき，x を求めることが難しい。
2．y が部分的にわかっているとき，残りの部分を求めることが難しい。

h と g が上記の性質をみたすとき，平文と暗号文の組から提案暗号化モードの鍵を求めることは，$y = G(x)$ が与えれたときに x を求めることと等価であることが証明される[5]。

3　All-or-Nothing Transform の安全性の定義

3.1　データ量増加の場合の従来の定義

All-or-nothing transform (AONT) は，直観的には以下のように定義される[7]。

定義 1　s 個の ℓ ビットのブロック $m_1, m_2, \ldots, m_s$（平文ブロック）を s' 個の ℓ ビットのブロック $m_1, m_2, \ldots, m_s$（擬似平文ブロック）に変換する F を考える。F が以下の条件を満たすとき，F を all-or-nothing transform（AONT）という。

1．F は可逆な変換である。
2．F とその逆変換は効率良く実行できる。
3．もし擬似平文ブロックが一つでも未知ならば，どの平文ブロックに対しても，その平文ブロックの如何なる関数も計算することは難しい。

AONT はその変換に秘密情報を用いていないので，AONT は暗号化関数でないことに注意しよう。もし $s = s'$ ならばデータ量不変 AONT と言い，もし $s < s'$ ならばデータ量増加 AONT と言う。データ量増加 AONT の実現例として，package transform[7]が提案されている。

定義 1 は直観的で分かりやすい定義ではあるが，AONT の安全性を定量的に議論するには，三番目の条件を定量的に定義する必要がある。そこで，Boyko[3]は，識別不可能性と強秘匿の観点から四つの定義を与えた。さらに，その四つの定義の下で，optimal asymmetric encryption padding[2]が最も安全な AONT であることを示した。一方，その四つの定義の下で安全であるためには，データ量増加 AONT でなければならず，如何なる

データ量不変 AONT もその四つの定義の下では安全ではないことが容易に示される。

3.2 データ量不変の場合の従来の定義

Stinson[8]は，定義 1 を情報理論的立場から再定義した。

定義 2 $M_1, M_2, \ldots, M_s$ を $\{0,1\}^{\ell}$ 上の値をとる確率変数とし，F を実変数 $m_1, m_2, \ldots, m_s$ の関数とする。確率変数 $X_1, X_2, \ldots, X_s$ が $F(M_1, M_2, \ldots, M_s)$ によって与えられるとする。もし確率変数が以下の条件を満たすならば，F を無条件に安全な AONT（UAONT）という。

1．$H(X_1, X_2, \ldots, X_s \mid M_1, M_2, \ldots, M_s) = H(M_1, M_2, \ldots, M_s \mid X_1, X_2, \ldots, X_s) = 0.$

2．任意の $i, j = 1, 2, \ldots, s$ に対して，$H(M_i \mid X_1, X_2, \ldots, X_{j-1}, X_{j+1}, \ldots, X_s) = H(M_i)$ が成立する。

ここで，H はエントロピー関数である。

定義 2 の一つめの条件が，定義 1 の一つめの条件に対応している。定義 2 の二つめの条件が定義 1 の三つめの条件に対応しているように考えられるが，正確には少し異なることに注意しよう。定義 2 の二つめの条件は，任意の擬似平文ブロックが一つ未知であれば，平文ブロックの任意の一つが決定できないことを意味している。しかし，二つの平文ブロックの関係（例えば，二つの平文ブロックの和の値）については何も述べていないので，決定できるかもしれない。それに対して，定義 1 の三つめの条件はそれも計算量的に不可能であることを意味している。したがって，定義 2 は，一つの平文ブロックが無条件に安全であることを述べているが，それ以外の安全性については何も保証していない。

定義 2 は $s = s'$ であるので，データ量不変 AONT である。文献[8]では，定義 2 を満たすデータ量不変 AONT として，線形関数を利用した AONT（線形 UAONT）が提案されている。定義 2 の条件は，(s, s, s) ランプ型秘密分散方式[9]の条件と等価である。したがって，定義 2 を満たすような効率的な関数 F は存在するが，定義 2 を満たし，かつ $s > s'$ となる関数 F は存在しないことが導かれる[9]。

3.3 提案する安全性の定義

変換の前後でデータ量が変化しないことは，通信コストや記憶容量が最小であるという実用的利点となる。一方，Boyko の定義の下では安全なデータ量不変 AONT は存在せず，Stinson の定義の下では，一つの平文ブロックの安全性しか保証できない。そこで，本研究では，一つの平文ブロックに対しては無条件に安全であり，その他の平文ブロックに対しては識別不可能という観点から,データ量不変 AONT の安全性の定義を与える。

Alice と Bob が行う以下のようなゲームを考えよう。変換 F を構成している基本関数のオラクルを O とし，Alice と Bob が入力 x に対する基本関数の値を知るためには，O に尋ねなければならないと仮定する。まず，Alice は平文ブロックを任意に選び，それに対する擬似平文ブロックを O を用いて計算する。Alice は，これを何回か繰り返した後，不完全な平文ブロックを二つ作成する。

$$\vec{m}_0 \setminus m_{0,i_0} = (m_{0,1}, m_{0,2}, \ldots, m_{0,i_0-1}, \phi, m_{0,i_0+1}, \ldots, m_{0,s}),$$
$$\vec{m}_1 \setminus m_{1,i_1} = (m_{1,1}, m_{1,2}, \ldots, m_{1,i_1-1}, \phi, m_{0,i_1+1}, \ldots, m_{1,s}),$$

ここで，ϕ は空ブロックを表し，少なくとも一つの i に対して，$m_{0,i} \neq m_{1,i}$ である。Alice は，$\vec{m}_0 \setminus m_{0,i_0}$ と $\vec{m}_1 \setminus m_{1,i}$ と消失ブロック位置 j を Bob に渡す。Bob は，秘密に $b \in \{0,1\}$ を選び，さらに m_{b,i_b} をランダムに $\{0,1\}^{\ell}$ を選ぶ。Bob は，完全な平文ブロック

$$\vec{m}_b = (m_{b,1}, m_{b,2}, \ldots, m_{b,i_b-1}, m_{b,i_b}, m_{b,i_b+1}, \ldots, m_{b,s}),$$

を作り，それに対する擬似平文ブロック $\vec{x}_b$ を O を用いて計算する。

$$\begin{aligned}\vec{x}_b &= (x_{b,1}, x_{b,2}, \ldots, x_{b,s}) \\ &= F(\vec{m}_b).\end{aligned}$$

Bob は，$\vec{x}_b$ の j 番目のブロックを空ブロック ϕ に置き換えた不完全な擬似平文 $\vec{x}_b \setminus x_{b,j}$ を Alice に返す。

$$\vec{x}_b \setminus x_{b,j} = (x_{b,1}, x_{b,2}, \ldots, x_{b,j-1}, \phi, x_{b,j+1}, \ldots, x_{b,s}).$$

Alice は $\vec{x}_b \setminus x_{b,j}$ を受け取った後，Alice は平文ブロックを任意に選び，それに対する擬似平文ブロックを O を用いて計算する。Alice は，O との対話を何回か繰り返した後，Bob が選んだ b の値を推測する。

定義 3　変換 F を UAONT とする。上記のゲームにおいて，Alice が O にアクセスした回数を q_A 回，Alice の推測が正しい確率を $0.5+\epsilon_A$ とする。このとき，F を(q_A,ϵ_A)-識別可能という。もし q_A が ℓ の多項式であり，ϵ_A が無視できる程小さいならば，F は定義 3 の下で識別不可能という。

この定義は，Boyko の定義と Stinson の定義の中間に位置するものであり，データ量不変 AONT に対して十分な安全性を与えていると考えている。なお，定義 3 の下で，線形 UAONT は識別不可能ではない。また，文献[6]のマスキングプロセスは，定義 3 の下で識別不可能であることは証明されていない。

4　新しい All-or-Nothing Transform

ハッシュ関数 h と擬似乱数生成器 g を用いたデータ量不変 AONT を提案する。そして，3.3章で定義した識別不可能性を満たすための h と g の性質を明らかにする。

4.1　アルゴリズム

h を $\{0,1\}^{\ell(s-1)}$ から $\{0,1\}^{\ell}$ へのハッシュ関数，g を $\{0,1\}^{\ell}$ から $\{0,1\}^{\ell(s-1)}$ への擬似乱数生成器とする。ここで，s は平文ブロック数である。

平文ブロックを $m_1,m_2,\ldots,m_s(m_i\in\{0,1\}^{\ell})$ としたとき，擬似平文ブロック $x_1,x_2,\ldots,x_s$ は，以下のようにして計算される。まず，μ_s を

$$\mu_s = h(m_1 \| m_2 \| \ldots \| m_{s-1}).$$

とし，$x_1,x_2,\ldots,x_{s-1}$ を次式で計算する。

$$x_1 \| x_2 \| \ldots \| x_{s-1} = (m_1 \| m_2 \| \ldots \| m_{s-1}) \oplus g(\mu_s \oplus m_s).$$

そして，x_s を

$$x_s = (\mu_s \oplus m_s) \oplus h(x_1 \| x_2 \| \ldots \| x_{s-1}).$$

で計算する。このアルゴリズムの $s=4$ の場合を**図 1** に示す。なお，この変換の逆変換アルゴリズムは明らかなので，省略する。

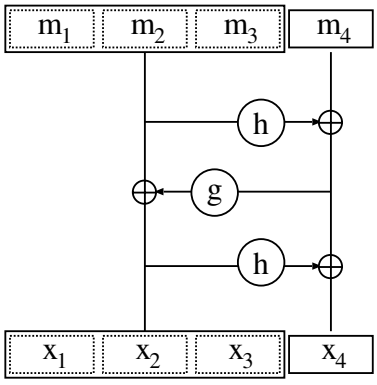

図 1　提案する AONT.

上記アルゴリズムは 3 ラウンドで構成されており，その点は BEAR と LION [1]に似ている。ここで，ラウンドとは，左右のブロック間の操作の回数である。しかし，上記アルゴリズムは秘密鍵を使用しないスクランブルアルゴリズムであるが，BEAR と LION は秘密鍵を使用する暗号化アルゴリズムであることに注意しよう。

また，上記アルゴリズムは，マスキングプロセス[6]とも構造が似ている。上記アルゴリズムは，アンバランス型 3 ラウンド Feistel 構造であるが，マスキングプロセスはバランス型 4 ラウンド Feistel 構造である。アンバランス型とは，左右のブロック数が異なることを意味し，バランス型とは，左右のブロック数が同じであることを意味する。上記アルゴリズムの方がラウンド数が少ないので，処理速度が高速であることが期待できる。また，アンバランス型 3 ラウンド Feistel 構造に対しては，3.3章で定義した識別不可能性を満たすための h と g の条

件が4.2章で示されるが，バランス型 4 ラウンド Feistel 構造に対しては，3.3章で定義した識別不可能性を満たすための条件は明らかにされていない。

4.2 安全性の検討

まず，以下の三つの条件を満たせば，4.1章の提案アルゴリズムは UAONT となる。

性質 1

1．h と g が決定的アルゴリズムである。

2．$y, w_i \in \{0,1\}^{\ell}$ とし，$y = h(w_1 \| w_2 \| \ldots \| w_{s-1})$ とおく。任意の i に対して，$w_j (j \neq i)$ を全て固定し，w_i が $\{0,1\}^{\ell}$ 上を一様に変化するとき，y も $\{0,1\}^{\ell}$ 上一様に変化する。

3．$y_i, w \in \{0,1\}^{\ell}$ とし，$y_1 \| y_2 \| \ldots \| y_{s-1} = g(w)$ とおく。もし w が $\{0,1\}^{\ell}$ 上を一様に変化するとき，任意のに対して，y_i も $\{0,1\}^{\ell}$ 上を一様に変化する。これは，y_i が各々独立ではないことを意味する。つまり，ある y_i を決定すれば，他の $y_j (j \neq i)$ は全て一意に決定されることを意味する。

集合 y と $\bar{y}$ を以下のように定義する。

$$y = \{g(w) \mid w \in \{0,1\}^{\ell}\},\ \bar{y} = \{y \mid y \in \{0,1\}^{\ell(s-1)} \ and\ y \notin y\}.$$

O_g を入力 w に対して $g(w)$ を計算するオラクル，$O_{\bar{g}}$ をランダムな $y \in \bar{y}$ を返すオラクルとする。このとき，Alice と Bob による以下のようなゲームを考える。Alice は O_g に何回かアクセスした後，Bob に $w \in \{0,1\}^{\ell}$ を与える。Bob は，$b \in \{0,1\}$ をランダムに選ぶ。もし $b = 0$ ならば，Bob は O_g を用いて $y_0 = g(w)$ を計算し，それを Alice に返す。もし $b = 1$ ならば，Bob は $O_{\bar{g}}$ から y_1 を得て，それを Alice に返す。Alice は y_b を受け取った後，O_g に何回かアクセスする。最後に，Alice は，Bob が選んだ b の値を推測する。ここで，Alice が Bob に与えた w は，このゲーム中に O_g に入力してない値であり，Alice はゲーム中 $O_{\bar{g}}$ にはアクセスできない。

定義 4　上記のゲームにおいて，Alice は，O_g に q'_A 回アクセスし，Alice の推測が正しい確率は $0.5 + \epsilon'_A$ とする。このとき，g は (q'_A, ϵ'_A)-識別可能という。もし q'_A が ℓ の多項式であり，ϵ'_A が無視できる程小さいならば，g は識別不可能な擬似乱数生成器という。

g が識別不可能な擬似乱数生成器ならば，4.1章の提案アルゴリズムが定義 3 の下で識別不可能であることが証明できる。

5 まとめと今後の課題

平成15年度は，実用的な観点から，処理速度の向上とデータ量の不変の二つについて研究を行った。処理速度の向上については，all-or-nothing 暗号化モードにおけるスクランブル部と暗号化部の統合を行った。データ量の不変については，まず，適切な安全性の定義を与え，それを満たす all-or-nothing transform を提案した。

今後の課題としては，提案した安全性の定義の拡張が残されている。今回提案した安全性の定義は，消失する部分がブロック単位であることを前提にしているので，これをビット単位にまで細分化する必要がある。この拡張は，理論的なだけでなく，実用的にも意味がある。例えば，古いデータが記録された CD-ROM を捨てる場合，データの流出を防ぐために通常物理的に壊される。その物理的破壊によって少なくとも一つのブロックが消失しているとき，4 章で提案した方法を用いていれば，破壊されていない部分からデータが流出しないことが保証される。しかし，その物理的破壊によって消失する部分がブロック単位でない場合には，そのような保証はない。したがって，ブロック単位よりも小さい部分が不連続的に消失している場合についての考察が必要である。

参考文献

[1] R.Anderson and E. Biham, “Two practical and provably secure block ciphers: BEAR and LION,” Fast Software Encryption FSE ’96, Lecture Notes in Computer Science, vol. 1039, pp.113－120, 1996.

[2] M.Bellare and P. Rogaway, “Optimal asymmetric encryption,” Lecture Notes in Computer Science Advanced in Cryptology - EUROCRYPT ’94, vol. 950, pp.92-111, 1994.

[3] V.Boyko, “On the security properties of OAEP as an all-or-nothing transform, ” Advances in Cryptology - CRYPTO ’99, Lecture Notes in Computer Science, vol.1666, pp.503-518, 1999.

[4] 桑門秀典，“暗号システムの安全性を向上させる暗号化モードに関する研究，”電気通信普及財団研究調査

報告書 (http://www.taf.or.jp/publication/kjosei_18/pdf/037.pdf), 18号, 01-01059, pp.269-274, 2003.
[5] H.Kuwakado and H.Tanaka, "Strongly non-separable encryption mode for throwing a media away," Technical Report of IEICE, vol.103, no.417, pp.15-18, 2003.
[6] D.B.Johnson, S.M.Matyas, and M.Peyravian, "Encryption of long blocks using a short-block encryption procedure," http://grouper.ieee.org/groups/1363/P1363a/contributions/peyrav.pdf, 1996.
[7] R.L.Rivest, "All-or-nothing encryption and the package transform," Fast Software Encryption FSE '97, Lecture Notes in Computer Science, vol.1267, pp.210－218, 1997.
[8] D.R. Stinson, "Something about all or nothing (transform)," Designs, Codes and Cryptography, vol.22, pp.133-138, 2001.
[9] H.Yamamoto, "On secret sharing systems using (k, L, n) threshold scheme," IECE Transactions, vol.J68-A, no.9, pp.945-953, 1985.

〈発 表 資 料〉

題　　名	掲 載 誌 ・ 学 会 名 等	発 表 年 月
Strongly non-separable encryption mode for throwing a media away	電子情報通信学会技術研究報告 情報セキュリティ	2003年11月