暗号利用モード XTS の安全性に関する調査及び評価

日本電気株式会社
峯松 一彦

2019 年 1 月

概要

本報告書は，ブロック暗号を利用した暗号利用モード（秘匿モード）である XTS の安全性評価を行い，その結果を報告するものである．XTS は IEEE Storage in Security Workgroup (SISWG) により，ハードディスクや USB メモリなどのストレージデバイスの暗号化の標準方式として設計された暗号利用モードである．2007 年には IEEE Standard P1619-2007 [IEE] として標準化されている．これに続いて 2010 年には，米国 国立標準技術研究所（National Institute of Standards and Technology, NIST) が，IEEE で標準化された仕様に対して若干のパラメータの制約を加えた上で，XTS を NIST の推奨する方式として選定した．NIST 推奨を記述した仕様書（実質的な標準化文書）として NIST SP800-38E [Dwo10] を発行している．

XTS 自体は汎用的な暗号利用モードとして定義することが可能であり，したがって任意のブロック暗号を用いることが可能である．しかし，上記の IEEE 標準化および NIST 推奨方式としては，利用するブロック暗号は AES に固定して仕様を定め，この場合の利用モードを XTS-AES と名付けて仕様を標準化している．本報告書では一般的な暗号利用モードとしての XTS および XTS-AES に関し， IEEE, NIST の標準化文書および関連文献を精査し安全性を評価した．以下に評価結果の概要を記す．

1. IEEE および NIST の標準化文書においては，安全性評価に関する言及は参考文献の引用程度で，明確には述べられていない．しかし，XTS がベースとする XEX に関しては Rogaway による論文 [Rog04] が存在し，また NIST へのパブリックコメント [LM06] において XEX と XTS の違いを考慮したうえでの安全性証明が与えられている．このことから，XTS のコアであるブロック単位の暗号化処理に関しては安全といえる．
2. XTS はブロック単位での暗号化（ Narrow-Block Encryption ）を行うため，ブロック単位の暗号化処理が安全であっても，提供できる安全性については本質的な限界がある．しかし，CBC などで暗号化するよりも高い安全性を有しており，現実的な安全性と効率のトレードオフから考えると妥当である．

3. XTS において Ciphertext Stealing (CTS) を用いた場合の安全性は平文の分布によるため，理論的評価は困難であり，積極的に利用を推奨する根拠に乏しい．ただし，単一平文での暗号文のみ攻撃が可能になる，などの致命的な問題を生じることはない．本来は CTS ではなく 2 ブロックの Tweakable ブロック暗号モードを用いるべきであろう．
4. XTS の安全性証明により，鍵を変えずに処理するデータ量が $2^{n/2}$ ブロック（n はブロックサイズ）より十分小さければ安全であることが知られているが，反対に $2^{n/2}$ ブロック以上のデータを処理した場合の影響について，ストレージ暗号化のシンプルなモデルにおいて平文回復攻撃の検討を行った．結果として，1 ラウンド Even-Mansour 暗号の鍵回復攻撃を応用することができると判明した．攻撃計算量は XTS-AES では 2^{64} 以上であり，必要とするデータが大量であるため，すぐさま現実的な脅威とはなるものではない．しかし，例えば $n = 64$ の 64 ビットブロック暗号を用いた場合では現実的な問題といえる．
5. XTS で規定されたブロック暗号である AES-128 および AES-256 については，学術的にも現実的にも攻撃は見つかっておらず，高い安全性を有すると考えられる．

以上の評価により，XTS-AES は全体としては現実的に安全であるという結論を得た．ただし，最終ブロックが $n = 128$ ビット未満の場合には CTS を用いることになり，保証される理論的安全性が特に明確でなく，このケースには注意が必要である．さらに利用における誤りやサイドチャネル攻撃の影響，また AES でなく 64 ビットブロック暗号などのよりブロックサイズの小さい暗号を使うことは一般に勧められない．

目次

図目次

1　はじめに

本報告書では，ブロック暗号利用モード XTS の安全性評価を行い，その結果を報告する．

XTS は IEEE Storage in Security Workgroup (SISWG) により，ストレージの暗号化の標準方式として設計された暗号利用モードであり，IEEE P1619 [IEE] として制定されている．米国国立標準技術研究所（National Institute of Standards and Technology, NIST) は同じ方式にわずかにパラメータの制約を加え，推奨方式として選定し，SP800-38E [Dwo10] を発行している．いずれも XTS を AES（より厳密には AES-128 ないし AES-256）で実現するものとして仕様を定め，この場合の利用モードを XTS-AES と名付けている．

簡便のため本報告書では，XTS と述べた場合には用いるブロック暗号を限定せず，汎用的なブロック暗号利用モードとして扱い，XTS-AES と述べた場合には AES を使っているものとして扱う．報告書としては，XTS を中心に議論と評価を進めるものとする．

XTS の特徴は，Tweak（調整値）と呼ばれる値を付加的に利用して暗号化を行う点にある．Tweak は通常のカウンター（CTR）モードや CBC モードといった暗号利用モードにおける初期ベクトル（Initialization Vector, IV）と形式的には類似するが，機能的には異なるものであり，例えば同じ Tweak 値で複数の平文を暗号化することが想定されている．なお，XTS は暗号化のみを目的とし，メッセージ認証の機能を持たない．

技術的には，XTS は，Rogaway により提案された XEX モード [Rog04] をベースとし，鍵の扱いや平文がブロック長の整数倍でない場合の処理（Ciphertext Stealing, CTS）を加えたものとなっている．ちなみに XTS という名前は，NIST においては XEX Tweakable Block Cipher with Ciphertext Stealing の略とされているが，IEEE においては XEX encryption mode with Tweak and ciphertext Stealing であるとされている[*1]．

XTS および XTS-AES は HDD や USB メモリの暗号化方式として普及している．代表例としては Windows 10 の Bitlocker や，Apple の MAC OS 向

[*1] CRYPTREC レポート [Rog11] では XEX-based Tweaked CodeBook mode (TCB) with ciphertext Stealing であるとされている．

け FileVault2，また TrueCrypt [*2], VeraCrypt [*3], dm-crypt [*4]などのよく知られたディスク/ファイル暗号化ソフトウェアで採用されている．

本報告書の構成について述べる．まず 2 章において必要な記法について準備を行い，3 章で XTS の仕様について説明する．次に，4 章において主要な参考文献をもとに安全性評価を行う．5 章において，2012 年に発行された CRYPTREC レポートでの XTS の安全性評価内容に関して検討を行い，6 章では数学的な安全性が保証される範囲よりも大量のデータを暗号化することで実現する攻撃（バースデー攻撃）の検討を加える．7 章では上記の内容に含まれなかった関連文献について考察する．最後に 8 章で結論をまとめる．

2 準備

2.1 記法

まず本報告書で用いる基本的な数学的記法を述べる．二つのバイナリ系列 x と y について，$x\|y$ を x と y のビット連結とする．また $|x|$ を x のビット長とする．所与の n について，$|x|_n = \lceil |X|/n \rceil$ とする．これは x の n-bit ブロック数をあらわす．また，s を正整数とし，s ビット以上のバイナリ系列 x について，$\mathtt{lsb}_s(x)$ と $\mathtt{msb}_s(x)$ をそれぞれ x の右端と左端の s ビットとする．すべてのバイナリ系列の空間を $\{0,1\}^*$ で表し，任意のバイナリ系列 $M \in \{0,1\}^*$ について $(M_1, \ldots, M_m) \xleftarrow{n} M$ を，M の n-bit ブロックへの分割とする．すなわち $M_1 \| \ldots \| M_m = M$，$m = |M|_n$ で $1 \leq i \leq m-1$ について $|M_i| = n$，$|M_m| \in \{1, \ldots, n\}$ である．

変数 X が集合 $\mathcal{X}$ 上の一様乱数であるとき，$X \xleftarrow{\$} \mathcal{X}$ と表記する．

正の整数 a と $c \leq a$ に対して，

$$(a)_c \stackrel{\text{def}}{=} (a) \cdot (a-1) \cdot (a-2) \cdot \cdots \cdot (a-(c-1))$$

とする．

[*2] http://truecrypt.sourceforge.net/

[*3] https://www.veracrypt.fr/en/Home.html

[*4] https://wiki.archlinux.org/index.php/dm-crypt

2.2 鍵付き関数，ブロック暗号，Tweakable ブロック暗号

関数 $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ が鍵付き関数であるとは，第一引数が一様乱数 $K \xleftarrow{\$} \mathcal{K}$ であることをいう．$F(K, X)$ を $F_K(X)$ とも表記する．また鍵付き関数 $E : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$ が任意の $K \in \mathcal{K}$ について E_K が $\mathcal{X}$ 上の置換となるとき，鍵付き置換とよぶ．任意の鍵付き置換 E_K について，逆関数を E_K^{-1} で表す．よって任意の $K \in \mathcal{K}$ について

$$E_K(X) = Y \Leftrightarrow E_K^{-1}(Y) = X$$

となる．E が暗号学的安全性（後述）を持つとき，E はブロック暗号と呼ばれる共通鍵暗号の基本的要素となる．

ブロック暗号を拡張した概念として Liskov ら [LRW02] により提案されたのが Tweakable ブロック暗号 （Tweakable Block cipher, TBC) である．TBC は外部パラメータである Tweak（調整値）を暗号化と復号に用いる．Tweak は鍵と同様にメッセージ空間上の置換を指定するパラメータであるが，公開された値であることが特徴である．すなわち，Tweak T, 平文 M, 暗号文 C について，鍵 K を用いた Tweakable ブロック暗号の暗号化関数を $C = \widetilde{E}_K(T, M)$，復号関数を $M = \widetilde{E}_K^{-1}(T, C)$ とすると，

$$\begin{aligned} &\widetilde{E}_K^{-1}(\widetilde{E}_K(M, T), T) = M, \\ &\widetilde{E}_K(\widetilde{E}_K^{-1}(C, T), T) = C \end{aligned} \tag{1}$$

をあらゆる T, K, M および C で満たす．したがって Tweak が固定された TBC は通常のブロック暗号となる．

3 XTS の仕様

3.1 概要

本章では主に IEEE Standard 1619 [IEE] を参考に XTS の仕様を説明する．IEEE ではブロックサイズは $n = 128$ ビットであるとし，用いるブロック暗号が AES の場合のみで仕様を記述しているが，本報告では可能な限り一般的に記述を行う．

XTS は汎用的なブロック暗号のモードである．暗号化対象は平文 M であり，その空間を $\mathcal{M} = \{0,1\}^n$ とする．ブロック暗号 $E : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$ の鍵

を二つ用いる．XTS-AES の場合であれば，E が AES であり，用いる AES の鍵長は，[IEE] では 128 ビット鍵二つと 256 ビット鍵二つの場合が推奨されている．したがって XTS-AES の全体の鍵としては，それぞれ 256 と 512 ビットとなる．一方，[Dwo10] では特に二つの鍵長のパターンに具体的な推奨や制約を定義していない．なお，[IEE] では 128 ビット鍵二つを用いる場合を XTS-AES-128, 256 ビット鍵二つを用いる場合を XTS-AES-256 と呼んでいるため，全体の鍵長との違いに注意が必要である．XTS の暗号化関数 $\mathrm{XTS.Enc}_K$ への入力は，

- 平文 $M \in \{0,1\}^*$
- Tweak $T \in \{0,1\}^n$

である．ここでの Tweak は，一般に平文が格納されるストレージデバイスのアドレス, 例えばハードディスクの暗号化であれば, 処理対象のセクタの番号, が用いられる．鍵 K はブロック暗号二つの鍵の連結, すなわち $K = (K_1, K_2) \in \mathcal{K}^2$ である．K_1 と K_2 は独立に一様に選択される．Tweak は一般の暗号利用モードにおける初期ベクトル（Initialization Vector, IV）とは性格が異なる．IV は，カウンター値や乱数といった，繰り返しが起きないことを前提とし，あくまで平文の内容などとは独立に，かつ正規の利用者が決定するであるものに対し，tweak は繰り返しが起きることも想定される上，攻撃シナリオによっては攻撃者がコントロールすることも想定される．形式上は，XTS-AES は可変長平文に対する TBC となっているが，後述のようにこの入力空間に対する標準的な安全性は有さない．なお， Tweak はリトルエンディアンで入力されることとなっており，平文 M の長さについては，固定であって最低 $n = 128$ ビットであり，$|M|_n$ は 2^{20} を超えないこととされている．したがって

$$128 \leq |M| \leq 2^{27} (= 2^{20} \cdot 128)$$

が平文長の制約となる．

XTS の復号関数 $\mathrm{XTS.Dec}_K$ への入力は，同様に

- 暗号文 C，ただし $128 \leq |C| \leq 2^{27} (= 2^{20} \cdot 128)$,
- Tweak $T \in \{0,1\}^n$

である．また，暗号化と復号で用いた tweak が同じであれば，平文と暗号文とは対応する．すなわち，

$$\mathrm{XTS.Dec}_K(\mathrm{XTS.Enc}_K(M,T),T) = M \tag{2}$$

が任意の M と T について成立する．

実際の暗号化は，平文 M を 128 ビットブロックの系列 $(M_1, M_2, \ldots, M_m)$ へ分解し，各 M_i へ Tweak から生成されたマスク系列を加算しつつ，ECB モード暗号化を行い，さらに出力側にも同マスクを加算するものである．ただし最後のブロック M_m が 128 ビットに満たない場合（不完全ブロック，partial block とも呼ばれる）は，Ciphertext Stealing（CTS）と呼ばれる処理を導入する．この処理により，

- $|M_m| = n$ のときは式 (2) に従い全部のブロックを暗号化
- $|M_m| < n$ のときは (M_{m-1}, M_m) に対して Ciphertext Stealing を実行し $|C_{m-1}| = n$，$|C_m| = |M_m|$ なる (C_{m-1}, C_m) を生成

という処理の分岐が発生する．

3.2 詳細仕様

まず，ブロック単位の暗号化処理，復号処理としてそれぞれ XTSb_K と XTSb_K^{-1} を定義する．正の整数 $m < 2^n$ に対して XTS のメッセージ長を最大 nm ビットとし，鍵 $K = K_1 \| K_2$, 128 ビットブロック平文 M, 暗号文 C, Tweak $\overline{T} = (T, D) \in \overline{\mathcal{T}} = \{0,1\}^n \times \{1, \ldots, m\}$ に対して

$$
\begin{aligned}
&\mathrm{XTSb}_K(M, \overline{T}) = S \oplus E_{K_1}(M \oplus S), \\
&\mathrm{XTSb}_K^{-1}(C, \overline{T}) = S \oplus E_{K_1}^{-1}(C \oplus S), \\
&S = E_{K_2}(T) \otimes \alpha^D
\end{aligned}
\tag{3}
$$

とする．この式において，α は事前に定義されたガロア体 $\mathrm{GF}(2^n)$ の生成元であり，$A \otimes B$ は A と B を $\mathrm{GF}(2^n)$ の元とみなした，すなわち多項式の係数ベクトルとみなしたうえでの乗算である．XTS-AES では $n = 128$ であり，ガロア体の生成多項式は辞書順で最初の既約多項式である

$$
\mathtt{x}^{128} + \mathtt{x}^7 + \mathtt{x}^2 + \mathtt{x} + 1
$$

を用いている．これは $\mathrm{GF}(2^n)$ 上の演算を用いる他の多くの暗号利用モードと同様である．$\alpha \otimes X$ は，X を左 1 ビットシフトしたのち，キャリーがあれば生成多項式に応じた定数（バイナリで 10000111，すなわち十進法で 135）を

XOR することと同値である;

$$\alpha \otimes X = \begin{cases} X \ll 1 \text{ if } \mathtt{msb}_1(X) = 0; \\ (X \ll 1) \oplus 0^{120}10000111 \text{ if } \mathtt{msb}_1(X) = 1. \end{cases} \tag{4}$$

なお XTS の暗号学的安全性は選択した既約多項式には依存しない.

次に，128 ビット以上の長さを持つ平文 M に対する XTS 暗号化を説明する．まず，M を 128 ビットずつ先頭から部分系列 $M_1, M_2, \ldots, M_m$ に分割，すなわち

$$(M_1, M_2, \ldots, M_m) \xleftarrow{n} M$$

とする．ここで $M_1, \ldots, M_{m-1}$ は 128 ビットであるが，最後の M_m は $1 \leq |M_m| \leq 128$ である．次に M_i for $1 \leq i \leq m-1$ について $C_i = \mathrm{XTSb}_K(M_i, (T, i))$ として暗号文ブロックを得る．最後のブロック長 $s = |M_m| < n$ の場合，(M_{m-1}, M_m) について XTSb_K を CBC 暗号化におけるブロック暗号とみなした Ciphertext Stealing を行う．すなわち $\mathrm{XTSb}_K(M_{m-1}, (T, m-1))$ の前半 s ビットを C_m とし，後半 $n-s$ ビットを M_m の後ろに連結したのち，$\mathrm{XTSb}_K(*, (T, m))$ で暗号化し，これを C_{m-1} とする.

上記の XTS 暗号化の手順を Algorithm 1 に記し，対応する XTS 復号処理を Algorithm 2 に記す.

また完全ブロックに対する XTS 暗号化を図 4 に，XTS 復号を図 5 に，最終 2 ブロックに対する CTS 暗号化を図 6 に，対応する CTS 復号を図 7 にそれぞれ表す.

XTSb_K 自体は n ビットメッセージと Tweak $\overline{T}$ を用いた Tweakable ブロック暗号とみることが可能である.

3.3 XEX: 単一鍵での XTS

XTS のブロック暗号化はもともと Rogaway により提案された XEX [Rog04] から導かれている．XEX では $K = K_1 = K_2$ として単一の鍵としており，暗号化処理と復号処理は,

$$\begin{aligned} &\mathrm{XEXb}_K(M, \overline{T}) = S \oplus E_K(M \oplus S), \\ &\mathrm{XEXb}_K^{-1}(C, \overline{T}) = S \oplus E_K^{-1}(C \oplus S), \\ &S = E_K(T) \otimes \alpha^D, \\ &\overline{T} = (T, D) \end{aligned} \tag{5}$$

Algorithm
$\mathrm{XTS}_K.\mathrm{Enc}_K(M, T)$

1. $(M_1, \ldots, M_m) \xleftarrow{n} M$
2. **for** $i = 1$ **to** $m - 1$ **do**
3. $\quad C_i \leftarrow \mathrm{XTSb}_K(M_i, (T, i))$
4. **end for**
5. **if** $|M_m| = n$ **then**
6. $\quad C_m \leftarrow \mathrm{XTSb}_K(M_m, (T, m))$
7. **else**
8. $\quad C_m \leftarrow \mathtt{msb}_{|M_m|}(C_{m-1})$
9. $\quad D \leftarrow \mathtt{lsb}_{n-|M_m|}(C_{m-1})$
10. $\quad \widetilde{M}_m \leftarrow M_m \,\|\, D$
11. $\quad C_{m-1} \leftarrow \mathrm{XTSb}_K(\widetilde{M}_m, (T, m))$
12. $C \leftarrow (C_1, C_2, \ldots, C_m)$
13. **return** C

図 1　XTS 暗号化

となる．また，XTS と XEX の重要な違いとして，XTSb_K では $D = 0$ を使えるのに対して，XEXb_K では $D = 0$ は使えないという事実がある．この理由については後述する．

4　XTS の安全性

4.1　準備

XTS の安全性については，NIST も IEEE もごく簡単に Rogaway の XEX [Rog04] への言及を行い，XEX が証明可能安全であると述べているに過ぎない．XTS の安全性証明に関する具体的な記述は Liskov と Minematsu による NIST へのパブリックコメント [LM06] にある．これをもとに，安全性評価を行う．

本章ではまず，平文，暗号文とも長さが常に n の倍数であるケース，すなわ

Algorithm

$\mathrm{XTS}_K.\mathrm{Dec}_K(C, T)$

1. $(C_1, \ldots, C_m) \xleftarrow{n} C$
2. **for** $i = 1$ **to** $m - 1$ **do**
3. $\quad M_i \leftarrow \mathrm{XTSb}_K^{-1}(C_i, (T, i))$
4. **if** $|C_m| = n$ **then**
5. $\quad M_m \leftarrow \mathrm{XTSb}_K^{-1}(C_m, (T, m))$
6. **else**
7. $\quad M_m \leftarrow \mathtt{msb}_{|C_m|}(M_{m-1})$
8. $\quad D \leftarrow \mathtt{lsb}_{n-|M_m|}(M_{m-1})$
9. $\quad \widetilde{C}_m \leftarrow C_m \,\|\, D$
10. $\quad M_{m-1} \leftarrow \mathrm{XTSb}_K^{-1}(\widetilde{C}_m, (T, m))$
11. $M \leftarrow (M_1 \,\|\, M_2 \,\|\, \ldots \,\|\, M_m)$
12. **return** M

図 2　XTS 復号

ち Ciphertext Stealing の必要がない場合を考える．

なお平文と暗号文の長さが 128 の倍数でない場合の安全性の定義については，これは IEEE, NIST ともに明確な記述はないため，6 章にて別途考察する．

■疑似ランダム置換, 強疑似ランダム置換　Tweakable ブロック暗号の安全性の基準を説明するために，まず疑似ランダム置換および強疑似ランダム置換の説明からはじめる．$\{0,1\}^n$ 上のランダム置換 $\mathsf{P}_n : \{0,1\}^n \to \{0,1\}^n$ を考える．P_n はあらゆる n ビット置換（全部で $2^n!$ 個存在する）の中から一様に選択されており，任意の異なる d 入力 $x_1, \ldots, x_d \in \{0,1\}^n$，$1 \le d \le 2^n$ について

$$\begin{aligned}&\Pr[\mathsf{P}_n(x_1) = y_1, \ldots, \mathsf{P}_n(x_d) = y_d] \\ &= \begin{cases} \frac{1}{2^n \cdot (2^n-1) \ldots (2^n-d+1)} & \text{if } y_1, \ldots, y_d \text{ are unique} \\ 0 & \text{otherwise.} \end{cases}\end{aligned} \tag{6}$$

を満たし，かつ同じ入力には常に同じ出力を返すことになる．n ビットブロック暗号 $E_K : \{0,1\}^n \to \{0,1\}^n$ が疑似ランダム置換であるとは，オラクルが

Algorithm $\mathrm{XTSb}_K(X, \overline{T})$	**Algorithm** $\mathrm{XTSb}_K^{-1}(Y, \overline{T})$
1. $(K_1, K_2) \xleftarrow{n} K$	1. $(K_1, K_2) \xleftarrow{n} K$
2. $(T, D) \leftarrow \overline{T}$	2. $(T, D) \leftarrow \overline{T}$
3. $S \leftarrow E_{K_2}(T) \otimes \alpha^D$	3. $S \leftarrow E_{K_2}(T) \otimes \alpha^D$
4. $Y \leftarrow S \oplus E_{K_1}(X \oplus S)$	4. $X \leftarrow S \oplus E_{K_1}^{-1}(Y \oplus S)$
5. **return** Y	5. **return** X

図 3　XEXb_K および XEXb_K^{-1}

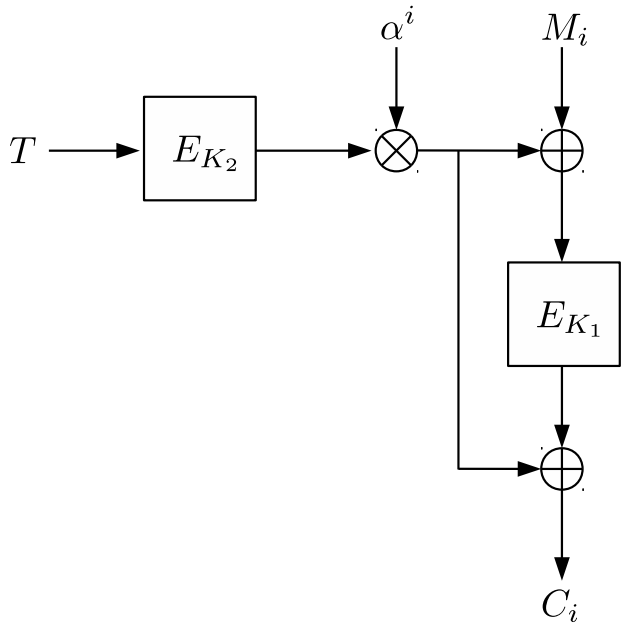

図 4　XTS 暗号化，完全ブロック

E_K か P_n かをランダムなコイン $b \in \{0,1\}$ に従って選択し，攻撃者がこのオラクルに選択平文を質問することで両者を判別，すなわち b を推測するゲームを考えたとき，正しく判別することが質問回数を含めて計算量的に困難であることを言う．

ここで，オラクル O_E へ平文 M を与えて暗号文 C をもらい，最終的に 2 値判定を行う攻撃者 $\mathcal{A}$ を考え，この $\mathcal{A}$ の判定結果が 1 であるイベントを $\mathcal{A}^{O_E} \Rightarrow 1$ と表記すると，E_K と P_n との選択平文攻撃による判別が計算量的に困難であ

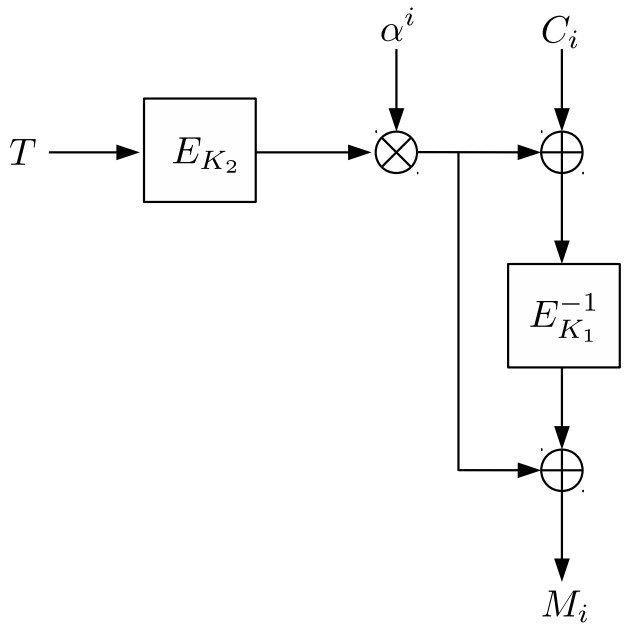

図 5　XTS 復号，完全ブロック

るとは，平文を質問する攻撃者 $\mathcal{A}$ によるアドバンテージ

$$\mathbf{Adv}^{\mathtt{prp}}_{E_K}(\mathcal{A}) \stackrel{\text{def}}{=} |\Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{E_K} \Rightarrow 1] - \Pr[\mathcal{A}^{\mathsf{P}_n} \Rightarrow 1]| \tag{7}$$

が現実的な計算量の $\mathcal{A}$ について無視できるほど小さいことをいい，これを満たす E_K は疑似ランダム置換（Pseudorandom Permutation, PRP）と呼ばれる．

同様に，E_K と P_n との選択暗号文攻撃による判別が計算量的に困難であるとは，平文もしくは暗号文を任意の順序で質問する攻撃者 $\mathcal{A}$ によるアドバンテージ

$$\mathbf{Adv}^{\mathtt{prp}}_{E_K}(\mathcal{A}) \stackrel{\text{def}}{=} |\Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{(E_K, E_K^{-1})} \Rightarrow 1] - \Pr[\mathcal{A}^{(\mathsf{P}_n, \mathsf{P}_n^{-1})} \Rightarrow 1]| \tag{8}$$

が現実的な計算量の $\mathcal{A}$ について無視できるほど小さいことをいい，これを満たす E_K は強疑似ランダム置換（Strong Pseudorandom Permutation, SPRP）と呼ばれる．ただし $\mathcal{A}^{(E_K, E_K^{-1})} \Rightarrow 1$ は，平文 M をオラクル E_K を与えて暗号文 C をもらうか，暗号文 C をオラクル E_K^{-1} へ与えて平文 M をもらうかを繰り返し，最終的な 2 値出力が 1 となるイベントを意味する．

選択暗号文攻撃は選択平文攻撃を含むため，定義より強疑似ランダム置換は常に疑似ランダム置換でもある．

なお，本来これらの定義は n について漸近的である．すなわち厳密な意味での “現実的な計算量”とは，入力長 n に対する多項式時間を指し，“無視でき

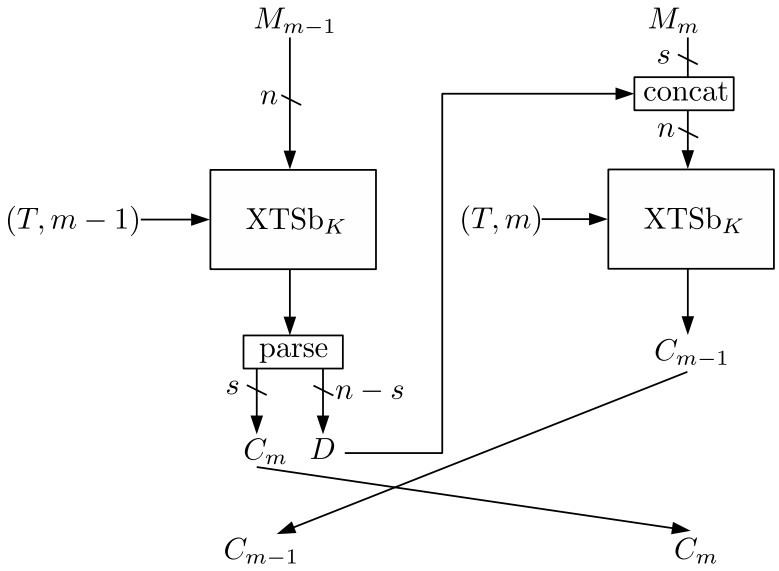

図 6　XTS 暗号化，Ciphertext Stealing

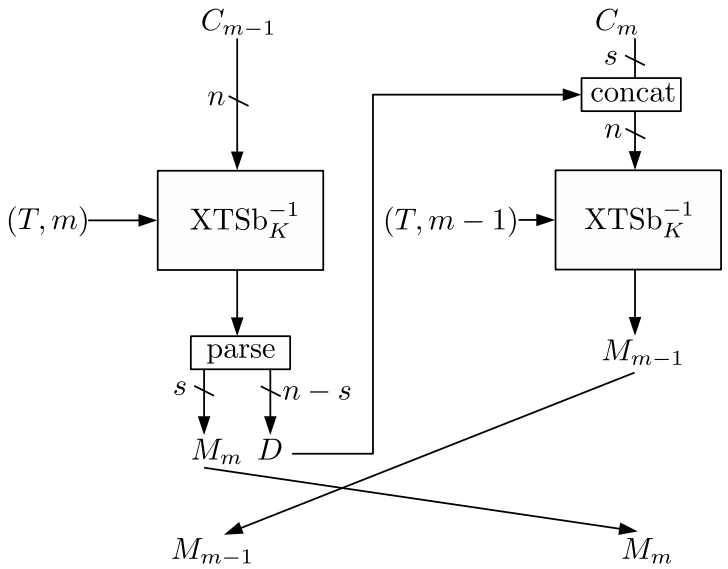

図 7　XTS 復号，Ciphertext Stealing

るほど小さい”とは，n を十分大きくとれば任意の n の多項式の逆数よりも小さくなることを指す．すなわちある計算量のもと達成可能な最大のアドバンテージを $\kappa(n)$ とすれば，任意の多項式 $p(n)$ について，n を十分大きくとることにより $\kappa(n) < 1/p(n)$ が達成されることを意味する．従って疑似ランダム置換とは，本来，n をパラメータとした暗号の族に対して定義されるべきものであるが，本報告書では慣用的な表現として，固定されたブロック長のブ

ロック暗号についても疑似ランダム置換という表現を適用する．例えばもし $E_K : \{0,1\}^n \to \{0,1\}^n$ が強疑似ランダム置換であるという場合，単に式 (8) が一般的な意味において十分小さい，ということを意味する．XTS の実際の証明においては，全体の安全性が用いる E_K の選択暗号文攻撃における判別困難性（式 (8)）で表現できればよく，従って E_K への条件を表すにはこのような慣用表現で十分である．

■Tweakable 強疑似ランダム置換　Tweakable ブロック暗号に関しても，疑似ランダム置換と同様の安全性基準を定義することが可能である．定性的には，異なる tweak ごとに，独立な（強）疑似ランダム置換のようとして振る舞うことが安全性の基準となる．

具体的に，tweak を $T \in \mathcal{T}$, 平文，暗号文をそれぞれ $M, C \in \mathcal{M} = \{0,1\}^n$ とし，TBC 暗号化関数と復号関数

$$\widetilde{E}_K : \mathcal{M} \times \mathcal{T} \to \mathcal{M}$$
$$\widetilde{E}_K^{-1} : \mathcal{M} \times \mathcal{T} \to \mathcal{M}$$

を考える．さらに，独立な $|\mathcal{T}|$ 個の n-bit 一様ランダム置換の集合 $\widetilde{\mathsf{P}}_{n,\mathcal{T}}$ を用いて，Tweakable 一様ランダム置換とその逆関数である

$$\widetilde{\mathsf{P}}_{n,\mathcal{T}} : \mathcal{M} \times \mathcal{T} \to \mathcal{M}$$
$$\widetilde{\mathsf{P}}_{n,\mathcal{T}}^{-1} : \mathcal{M} \times \mathcal{T} \to \mathcal{M}$$

をそれぞれ定義する．

Tweakable ブロック暗号（ないし一様ランダム置換）への選択平文攻撃とは，tweak と平文を与えて暗号文をもらうものであり，選択暗号文攻撃は tweak と暗号文を与えて平文をもらうものである．この考えに基づき，Tweakable(強) 疑似ランダム置換を定義することができる．すなわち，$\widetilde{E}_K$ が

$$\mathbf{Adv}^{\mathtt{tprp}}_{\widetilde{E}_K}(\mathcal{A}) \stackrel{\text{def}}{=} |\Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{\widetilde{E}_K} \Rightarrow 1] - \Pr[\mathcal{A}^{\widetilde{\mathsf{P}}_{n,\mathcal{T}}} \Rightarrow 1]| \tag{9}$$

が現実的な計算量の選択平文攻撃を行う $\mathcal{A}$ について無視できるほど小さいとき，これを Tweakable 疑似ランダム置換（Tweakable PRP, TPRP）と呼び，

$$\mathbf{Adv}^{\mathtt{tsprp}}_{\widetilde{E}_K}(\mathcal{A}) \stackrel{\text{def}}{=} |\Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{(\widetilde{E}_K, \widetilde{E}_K^{-1})} \Rightarrow 1] - \Pr[\mathcal{A}^{(\widetilde{\mathsf{P}}_{n,\mathcal{T}}, \widetilde{\mathsf{P}}_{n,\mathcal{T}}^{-1})} \Rightarrow 1]| \tag{10}$$

が現実的な計算量の選択暗号文攻撃を行う $\mathcal{A}$ について無視できるほど小さいとき，これを Tweakable 強疑似ランダム置換（Tweakable SPRP, TSPRP）と呼ぶ．

強疑似ランダム置換が疑似ランダム置換であるのと同様，Tweakable 強疑似ランダム置換は Tweakable 疑似ランダム置換でもある．本報告書では原則的に「安全な」Tweakable ブロック暗号とは，Tweakable 強疑似ランダム置換のことを指すものとする．

4.2 XTS の安全性定義

Tweakable 強疑似ランダム置換はあくまでブロック単位の処理に関する安全性の定義であり，XTS の全体的な機能である，複数ブロックからなる可変長平文の Tweakable な暗号化の安全性を定義するものではない．

XTS の暗号化機能は，いわゆる Narrow-block encryption (NBE) と呼ばれるものに相当する．NBE に対応する適切な邦訳が（報告者の知る限り）存在しないが，NBE は入力を 1 つの大きいブロックとみなした場合に，入力を複数の固定長ブロックに分割して処理し，なおかつ固定長ブロック間の処理結果の伝搬がないか，あるいは限定されている状態を指す暗号化方式であるといえる．便宜的に，本報告書では NBE を「弱いブロック暗号化」と呼び，後述する Wide-block encryption (WBE) ，すなわち「強いブロック暗号化」と区別することにする．

グローバルな tweak が n ビット，平文が mn ビット（ただし m は正の整数）の NBE は，Tweak の空間 $\mathcal{T} = \{0,1\}^n \times \{1,\ldots,m\}$ をもつ n ビットブロック Tweakable ブロック暗号 $\widetilde{E}_K$ を用いて実現される．グローバルな tweak を T，平文 M を $M = M_1 \,\|\, M_2 \,\|\, \ldots \,\|\, M_m$，ただし $i = 1,\ldots,m$ について $|M_i| = n$ としたとき，$\widetilde{E}_K$ を用いた NBE の暗号文は

$$C_j = \widetilde{E}_K(M_j, (T, j)),\ \text{for all } j = 0,\ldots,m \tag{11}$$

となる．この暗号化方式を $\mathrm{NBE}[\widetilde{E}_K]$ と表すことにする．この表記の元では，XTS は $\mathrm{NBE}[\mathrm{XTSb}_K]$ と等価である．

（弱いブロック暗号化として）理想的な NBE を $\mathsf{NBE} \stackrel{\mathrm{def}}{=} \mathrm{NBE}[\widetilde{\mathsf{P}}_{n,\mathcal{T}}]$ と定義する．この上で XTS の安全性として妥当と考えられるのは，NBE と XTS_K との選択暗号文攻撃における判別困難性でアドバンテージで評価することであろう．すなわち以下の指標となる．

$$|\Pr[K \stackrel{\$}{\leftarrow} \mathcal{K} : \mathcal{A}^{(\mathrm{NBE}[\mathrm{XTSb}_K], \mathrm{NBE}^{-1}[\mathrm{XTSb}_K])} \Rightarrow 1] - \Pr[\mathcal{A}^{(\mathsf{NBE}, \mathsf{NBE}^{-1})} \Rightarrow 1]| \tag{12}$$

しかしながら，両者の判別は部品として用いる XTSb_K と $\widetilde{\mathsf{P}}_{n,\mathcal{T}}$ の判別以上

に容易にはならないため，ブロック単位の処理が Tweakable 強疑似ランダム置換であるかどうかで評価すれば十分である．従って，XTS の安全性は，ブロック単位の Tweakable ブロック暗号 XTSb_K が Tweakable 強疑似ランダム置換であるかどうかで決まる．つまり

$$\begin{aligned}&\mathbf{Adv}^{\mathtt{tsprp}}_{\mathrm{XTSb}_K}(\mathcal{A})\\&= |\Pr[K \xleftarrow{\$} \mathcal{K} : \mathcal{A}^{(\mathrm{XTSb}_K, \mathrm{XTSb}_K^{-1})} \Rightarrow 1] - \Pr[\mathcal{A}^{(\widetilde{\mathsf{P}}_{n,\mathcal{T}}, \widetilde{\mathsf{P}}^{-1}_{n,\mathcal{T}})} \Rightarrow 1]| \qquad (13)\end{aligned}$$

で評価すればよいと結論される．XTSb_K がブロック暗号 E を用いている場合，$\mathbf{Adv}^{\mathtt{sprp}}_E(\mathcal{B})$ が十分小さいという仮定のもと，$\mathcal{A}$ をモジュールとして使う攻撃者 $\mathcal{B}$ を用いて $\mathbf{Adv}^{\mathtt{tsprp}}_{\mathrm{XTSb}_K}(\mathcal{A})$ の十分小さい上界が導出できれば，安全であるといえる．

あるいは，攻撃者 $\mathcal{A}, \mathcal{B}$ の代わりに，それらが用いる質問回数など攻撃パラメータのリストを θ とし，パラメータ θ を用いたあらゆる攻撃のアドバンテージの最大値を $\mathbf{Adv}^{\mathtt{tsprp}}_{\mathrm{XTSb}_K}(\theta)$ とし，これを評価してもよい．この場合，θ の関数である θ' を導入して，$\mathbf{Adv}^{\mathtt{tsprp}}_{\mathrm{XTSb}_K}(\theta)$ の上界を $\mathbf{Adv}^{\mathtt{sprp}}_E(\theta')$ を用いて評価するという方法になる．両者は表現形式の違いのみで，評価方法として本質的な差はない．

なお，前述したようにここでは平文長がブロックの倍数である場合に説明を限定している．平文長がブロックの倍数でない場合を含めた場合については 6 章を参照のこと．

4.3 弱いブロック暗号化（NBE) と強いブロック暗号化（WBE）の違いについて

弱いブロック暗号化（NBE）は，グローバルな tweak が固定された場合には，ECB モードの鍵をブロックごとに変えながら暗号化するモードに相当する．従ってブロックごとの入力の違いが他のブロックへ影響を与えず，これを用いた攻撃が考えられる．

例えば，HDD の暗号化に XTS を用いる場合，同じセクタに保管された暗号文を二つ入手した場合，ブロックの入れ替えを行うと対応する復号結果の平文ブロックも同じく入れ替えが起きる．これは，IEEE の仕様書において mix-and-match と呼ばれる攻撃に相当する．また，tweak が固定され，かつ最初の平文ブロックだけ変化しない場合，他の平文ブロックに依らず最初の暗号文ブロックだけは変化しないことになる．

このように，弱いブロック暗号化は提供しうる秘匿性について本質的な限界がある．これに対して，より強い安全性を保証する強いブロック暗号化（Wide-block encryption (WBE)）と呼ばれる暗号機能が考えられる．これは，シンプルに複数ブロックを入力とする Tweakable 強疑似ランダム置換を構成するものである．この場合，グローバルな tweak が固定されたもと，どれだけわずかな平文の違いでも暗号文全体へその違いが波及し，全体としてランダムな値となるため，より高い秘匿性を保証できる．暗号化処理に状態変数（時刻や，今までの暗号化の回数など）が存在しない場合では，実質的に暗号学的に一番強い安全性を提供するものである．

強いブロック暗号化を実現するブロック暗号利用モードも数多く研究されているが，原理的に 2 パス以上の処理が必要となるため，逐次処理ができない上に弱いブロック暗号化よりも計算量が多くなるという問題がある．

一方，弱いブロック暗号化は，ある程度ランダムネスを持った平文およびに暗号文については，処理の結果が乱数と判別困難となり，十分な安全性を有する．また，暗号文の一部を反転させるなどのシンプルな選択暗号文攻撃に対する耐性があるという点で，カウンターモードや CBC モードなどと比べて安全性は高いといえる．

従って NBE と WBE は達成する安全性のレベルと，必要とする計算量においてトレードオフの関係にある．弱いブロック暗号化は，実際に XTS がそうであるように，実質的に ECB モード相当の計算量で可能である点から，このトレードオフを勘案しても現実にはメリットがあるといえる．ただし，データ長やその分布，可能性のある攻撃のシナリオなどに応じて，鍵の更新頻度を適切に設定することが重要である．

特に，実際に使われる tweak の値にバリエーションが少なく，また平文のエントロピーが低い場合には XTS を含め，一般的に弱いブロック暗号化は適していないため使用を避けるべきといえる．一方，平文のエントロピーが低い場合でも，実際に使われる tweak の値にバリエーションが多く，また，ほぼランダムであると見なせる場合には安全である．これは，ストレージの暗号化において，データユニットのアドレスとして tweak を用いるケースなどが相当すると言える．

4.4 強いブロック暗号化の実現方法

強いブロック暗号化の実現方法についても従来研究をいくつか紹介しておく．例えば古典的な Naor-Reingold による方式 [NR97] では，4 段のフェイステル型暗号化の形をとり，中間の 2 段の段関数を疑似ランダム関数で実現し，上下の 1 段をユニバーサルハッシュ関数で実現するものである．後者は例えば多項式ハッシュ（平文ブロックを係数とした GF(2^n) 上の多項式を鍵で評価するもの）で実現可能である．モダンな暗号利用モードとしては，ブロック暗号のみを用いるものと，ブロック暗号とユニバーサルハッシュ関数を組み合わせたものとに大別される．前者のモードでは CMC [HR03], EME [HR04] などが知られており，後者は HCH [CS08]，HCTR [WFW05]，HSE [MM07] などが知られている．前者は m 入力ブロックにつきブロック暗号が $2m + O(1)$ 回，後者は m ブロック入力でのユニバーサルハッシュ関数 2 回とブロック暗号 $m + O(1)$ 回を必要とするため，通常の暗号化と比べて処理量は多い．

4.5 ブロック暗号の安全性に対する仮定の妥当性

XTS の安全性証明は，すべて用いるブロック暗号が強疑似ランダム置換であるという仮定に基づくものである．

一般的にブロック暗号の安全性は，暗号とランダム置換との選択平文攻撃ないしは選択暗号文攻撃による判別が鍵の全数探索より少ない計算量で可能かどうかを基準としている．この基準を満たすブロック暗号はそれぞれ疑似ランダム置換および強疑似ランダム置換とみなせ，一般的なブロック暗号利用モードにおいて安全性帰着が可能となるため，安全に使用することが可能である．ただし，攻撃者のモデルやブロック暗号の鍵の使い方が一般的なものと異なる利用モードの場合，安全性証明のためにさらに特殊な要件がブロック暗号に必要とされる場合もある．

XTS-AES の場合，AES へ有効な選択暗号文攻撃が発見されていない限り，強疑似ランダム置換であると見なすことができ，XTS-AES の安全性が AES の安全性に帰着できることになる．

AES について，現在のところの暗号解析結果としては，いずれの鍵長においてもフルラウンド攻撃には至っていない．例えば AES-128 においては最良の攻撃可能段数は 7 であり，不能差分攻撃で計算量 $O(2^{107})$ [BLNS18]，中間一

致攻撃で計算量 $O(2^{99})$ [DFJ13] と知られている．同様に AES-192，AES-256 に対する最良攻撃はそれぞれ 8 段と 9 段までである．なお，AES-256 では関連鍵攻撃（related-key attack）と呼ばれる攻撃がフルラウンドの攻撃を可能とすることが報告されている [BK09]．しかし，関連鍵攻撃は鍵へ攻撃者が特定の差分値を与えることができるモデルであり，XTS が想定する通常の攻撃モデルから逸脱している．また関連鍵攻撃を通常の選択平文および暗号文攻撃へ変換する一般的手法は存在しない．従って，AES が強疑似ランダム置換であるという仮定は全ての鍵長で現状でも信頼できるものといえる．

4.6 ブロック単位暗号化の安全性

前述のように，NIST も IEEE も，XTS は安全性が証明された Rogaway [Rog04] の XEX モードに標準的なテクニックである Ciphertext Stealing を組み合わせているので，安全であると言及している．

しかしながら，実際にはパブリックコメント [LM06] にあるように，XTS の構成は XEX をベースとしているものの，安全性の証明自体は Liskov らの暗号利用モードの証明，およびその改良である [Min06] がベースとなる．

これは，XEX がブロック暗号の鍵を一つしか使用しないのに対し，XTS では二つ使用するところが原因となっている．これらの違いが証明に及ぼす影響を説明する．

まず，情報理論的な安全性を議論するために，n ビットブロック暗号 E_{K_1}, E_{K_2} の代わりに二つの独立な n ビットランダム置換 P_1, P_2 を用いた XTSb_K の暗号化処理および復号処理を $\mathrm{XTSb}_{\mathsf{P}_1,\mathsf{P}_2}$，$\mathrm{XTSb}^{-1}_{\mathsf{P}_1,\mathsf{P}_2}$ とする．式 (5) 同様に

$$\begin{aligned}
&\mathrm{XTSb}_{\mathsf{P}_1,\mathsf{P}_2}(M,\overline{T}) = S \oplus \mathsf{P}_1(M \oplus S),\\
&\mathrm{XTSb}^{-1}_{\mathsf{P}_1,\mathsf{P}_2}(C,\overline{T}) = S \oplus \mathsf{P}_1^{-1}(C \oplus S),\\
&S = \mathsf{P}_2(T) \otimes \alpha^D
\end{aligned} \tag{14}$$

となる．簡便のため，$\mathrm{XTSb}_{\mathsf{P}_1,\mathsf{P}_2}$ を方式そのものを指す意味でも用いるものとする．

同様に単一の P を用いた $\mathrm{XEXb}_{\mathsf{P}}$ も定義される：

$$\begin{aligned}
&\mathrm{XEXb}_{\mathsf{P}}(M,\overline{T}) = S \oplus \mathsf{P}(M \oplus S),\\
&\mathrm{XEXb}^{-1}_{\mathsf{P}}(C,\overline{T}) = S \oplus \mathsf{P}^{-1}(C \oplus S),\\
&S = \mathsf{P}(T) \otimes \alpha^D.
\end{aligned} \tag{15}$$

ただし，$\overline{T} = (T, D)$ で $D \in \{1, \ldots, m\}$. なお $D = 0$ のときにはシンプルな攻撃が存在する．

ブロック暗号 E を用いた XEXb_K に対して q 回の選択暗号文攻撃を行う $\mathcal{A}$ を考える．この時の安全性は，$\mathcal{A}$ をサブルーチンとし，E_K に対して q 回の選択暗号文攻撃を行う攻撃者 $\mathcal{A}'$ について，

$$\begin{aligned}
&\mathbf{Adv}^{\mathtt{tsprp}}_{\mathrm{XEXb}_K}(\mathcal{A}) \\
&\leq \mathbf{Adv}^{\mathtt{tsprp}}_{\mathrm{XEXb}_\mathtt{P}}(\mathcal{A}) + \mathbf{Adv}^{\mathtt{sprp}}_{E_K}(\mathcal{A}') && (16)\\
&\leq \mathbf{Adv}^{\mathtt{sprp}}_{E_K}(\mathcal{A}') + \frac{9.5q^2}{2^n} && (17)
\end{aligned}$$

であると [Rog04] で証明されている．

しかし [Rog04] の XEX の証明は XTS（より正確には XTSb_K）には直接適用できず，Liskov らの結果（[LRW02] の Theorem 2）およびそれを改良した Minematsu の結果（[Min06] の Theorem 1）を用いる必要がある．

4.7 安全性証明

前の節で述べた Liskov らの結果はゲームベースの安全性証明に基づき，Minematsu の結果は Maurer による Random System フレームワーク [Mau02] に基づいている．ここでは，近年の安全性証明技法において支配的となりつつある，Patarin が 90 年代に提唱した Coefficient-H （あるいは H-Coefficient ） [Pat08] と呼ばれる手法での証明の概要を示す．ここで証明するのは $\mathbf{Adv}^{\mathtt{tsprp}}_{\mathrm{XTSb}_{\mathtt{P}_1,\mathtt{P}_2}}(\mathcal{A})$ の上界である．攻撃者 $\mathcal{A}$ の計算量には制約をおかず，クエリ回数を高々 q 回とする．

■Coefficient-H の概説　Coefficient-H は，攻撃者 $\mathcal{A}$ がオラクルと対話を行うゲームにおいて，対話の結果（すなわちクエリとそれに対応するレスポンス）を Transcript と呼ばれる変数リストで表す．i 番目のクエリを $X_i \in \mathcal{X}$, そのレスポンスを $Y_i \in \mathcal{Y}$ とし，攻撃者が q 回のクエリを行うとすれば，Transcript は確率変数のリスト Θ であり，

$$\Theta = (X_1, Y_1), \ldots, (X_q, Y_q)$$

と書ける．Transcript Θ の確率分布はゲームと攻撃者 $\mathcal{A}$ によって決まる．$X^i = (X_1, \ldots, X_i)$，$Y^i = (Y_1, \ldots, Y_i)$ と表記するものとする．このとき，攻撃者 $\mathcal{A}$ は X^{i-1}，Y^{i-1} から X_i を定め，オラクル O は X^i，Y^{i-1} から Y_i を定

めることから，一般に

$$\Pr_{O,\mathcal{A}}[\Theta = \theta] \tag{18}$$

$$= \prod_{i=1}^{q} \Pr_{O}[Y_i = y_i | X^i = x^i, Y^{i-1} = y^{i-1}] \tag{19}$$

$$\cdot \prod_{i=1}^{q} \Pr_{\mathcal{A}}[X_i = x_i | X^{i-1} = x^{i-1}, Y^{i-1} = y^{i-1}] \tag{20}$$

と書ける．

ゲームにおいて対話の最後に $\mathcal{A}$ が 0 ないし 1 の出力を行うとし，二つの異なるゲーム Game1 と Game2 のそれぞれでオラクル が O_1 と O_2 であるとすると，二つのゲームでの $\mathcal{A}$ が 1 を出力する確率の絶対値差が O_1 と O_2 の識別に関する Advantage に相当する．

攻撃者 $\mathcal{A}$ と二つのゲームが与えられたとき，Advantage は二つの Transcript の分布間の統計距離（statistical distance あるいは (total) variational distance）と一致することが知られている．

ここで，Advantage を最大化する攻撃者は一般に決定的（deterministic）であることが知られている．決定的な攻撃者では，時点 i までで得たクエリとレスポンスの対 $(X_1, Y_1), \ldots, (X_i, Y_i)$ から次のクエリ X_{i+1} は確定的に定まり，クエリの総数が q であれば $(X_1, Y_1), \ldots, (X_q, Y_q)$ から 2 値出力も確定的である．従って，決定的な攻撃者に対する Advantage の評価においては攻撃者のランダムネスは考慮せず，確率空間としてはオラクルのみを考慮すればよい（つまり，式 (20) は常にある x_i で確率 1 をとるものとして計算する）．この事実より決定的な攻撃者による Advantage の最大値を導出すればよいといえる．

典型的に，Coefficient-H では二つのゲームを real world, ideal world と呼称する．

統計距離の上界を評価するにあたり，Patarin は以下の重要な補題を示した．任意の real world (オラクル O_1）, ideal world（オラクル O_2）を考え，決定的な攻撃者 $\mathcal{A}$ を固定し，その Transcript Θ 全体の空間を $\mathcal{TS}$ とする．Ideal world において生起確率が非ゼロである Transcript の値，すなわち

$$\Pr_{\text{ideal}}[\Theta = \theta] > 0$$

なる $\theta \in \mathcal{TS}$ を attainable と呼び，attainable な θ 全体を $\mathcal{TS}_{\text{attainable}}$ とする．

Lemma 4.1. $\mathcal{TS}_{attainable}$ のある部分集合 $\mathcal{S}$ について，

$$\Pr_{ideal}[\Theta \in \mathcal{S}] \leq \epsilon_1 \tag{21}$$

がある $\epsilon_1 \in [0,1]$ で成立し，また任意の $\theta \in \mathcal{TS}_{attainable} \setminus \mathcal{S}$ について，

$$\frac{\Pr_{real}[\Theta = \theta]}{\Pr_{ideal}[\Theta = \theta]} \geq 1 + \epsilon_2 \tag{22}$$

がある $\epsilon_2 \in [0,1]$ で成立するとする．

このとき，O_1 と O_2 の識別の *Advantage* は

$$\mathbf{Adv}^{\mathtt{ind}}_{O_1,O_2}(\mathcal{A}) \leq \epsilon_1 + \epsilon_2 \tag{23}$$

である．

一般に $\mathcal{S}$ は判別を可能とするような Bad Transcript の集合であり，いわゆる Bad Event を記述するものである．

■XTS の証明　XTS のブロック暗号化の安全性証明を行うにあたって，real world をオラクル $\mathrm{XTSb}_{\mathsf{P}_1,\mathsf{P}_2}$（すなわち二つのランダム置換 P_1 と P_2 を用いた XTS）とし，Ideal world をオラクル $\widetilde{\mathsf{P}}_{n,\mathcal{T}}$ とする．ただし Tweak 空間は XTS の最大ブロック数 m について $\mathcal{T} = \{0,1\}^n \times \{1,\ldots,m\}$ である．3.2 節でみたように $m < 2^n$ である．

攻撃者は暗号化クエリ $(M,\overline{T})$ もしくは復号クエリ $(C,\overline{T})$ が可能である．判別には効果がないため，重複したクエリはしないものとする．すなわち，ある時点で $(M,C,\overline{T})$ という対を一つのクエリとそのレスポンスから得ていた場合，暗号化クエリ $(M,\overline{T})$ ないし復号クエリ $(C,\overline{T})$ は行わないものとする．

i 回目のクエリで得られた平文，暗号文対と用いた Tweak をそれぞれ $M^{(i)} \in \{0,1\}^n$，$C^{(i)} \in \{0,1\}^n$，$\overline{T}^{(i)} = (T^{(i)}, D^{(i)}) \in \mathcal{T}$ とする．$1 \leq D^{(i)} \leq m < 2^n$ である．本来は暗号化クエリと復号クエリのいずれかであるが，これを表す 1 ビット情報は実際安全性証明において不要であるため，Transcript に含めない．したがって Transcript は以下のように定義される．

$$\Theta = (M^{(1)}, C^{(1)}, \overline{T}^{(1)}), \ldots, (M^{(q)}, C^{(q)}, \overline{T}^{(q)}).$$

また，内部の P_1 への入力と出力を以下で表す．

$$X^{(i)} = \mathsf{P}_2(T^{(i)}) \otimes \alpha^{D^{(i)}} \oplus M^{(i)}, \tag{24}$$

$$Y^{(i)} = \mathsf{P}_2(T^{(i)}) \otimes \alpha^{D^{(i)}} \oplus C^{(i)}. \tag{25}$$

ここで，Real world においては，攻撃者の q 回のクエリがすべて終わったのちに $V^{(i)} = \mathsf{P}_2(T^{(i)})$ をすべての $i = 1, \ldots, q$ について攻撃者へ公開するものとする．攻撃者は得られた $(M^{(1)}, C^{(1)}, \overline{T}^{(1)}), \ldots, (M^{(q)}, C^{(q)}, \overline{T}^{(q)})$ に $V^{(1)}, \ldots, V^{(q)}$ を加えて最後の予測を行うことができる．Transcript にも加えて，

$$\Theta = (M^{(1)}, C^{(1)}, V^{(1)}, \overline{T}^{(1)}), \ldots, (M^{(q)}, C^{(q)}, V^{(q)}, \overline{T}^{(q)})$$

とする．

Ideal world においては，$\widetilde{\mathsf{P}}$ と独立なランダム置換 P' を導入し，$V^{(i)} = \mathsf{P}'(T^{(i)})$ for $i = 1, \ldots, q$ を生成し，同様に攻撃者の q 回のクエリがすべて終わったのちに公開するものとする．また，X と Y はレスポンスに関わらないダミー変数として，Real world 同様に生成する:

$$X^{(i)} = \mathsf{P}'(T^{(i)}) \otimes \alpha^{D^{(i)}} \oplus M^{(i)} \tag{26}$$

$$Y^{(i)} = \mathsf{P}'(T^{(i)}) \otimes \alpha^{D^{(i)}} \oplus C^{(i)} \tag{27}$$

いずれの world においても $(M^{(i)}, V^{(i)}, D^{(i)})$ から $X^{(i)}$ が一意に定まり，$(C^{(i)}, V^{(i)}, D^{(i)})$ から $Y^{(i)}$ が一意に定まることに注意する．

V を攻撃者に公開しているが，予測に用いる情報が増えるのみなので攻撃者に有利となり，Advantage は減ることはない．この変更したゲームでの Advantage の上界評価を行う．このように，方式の内部変数のいくつかを Transcript から確定的に定まるように攻撃者に公開するテクニックはよく使われており，公開する変数を適切に選択することで Coefficient-H における証明の複雑さを下げる効果がある．

Bad Transcript の集合 $\mathcal{S}$ を，ある 異なる $i, j \in \{1, \ldots, q\}$ について

$$X^{(i)} = X^{(j)} \text{ あるいは } Y^{(i)} = Y^{(j)} \tag{28}$$

を満たすものとする．

Ideal world で $\mathcal{S}$ が起きる確率を評価する．

$$
\begin{aligned}
&\Pr_{\text{ideal}}[\Theta \in \mathcal{S}] \\
&= \Pr_{\text{ideal}}[{}^{\exists} i, j \in \{1, \ldots, \} : i \neq j, X^{(i)} = X^{(j)} \text{ or } Y^{(i)} = Y^{(j)}], \\
&\leq \Pr_{\text{ideal}}[{}^{\exists} i, j \in \{1, \ldots, \} : i \neq j, X^{(i)} = X^{(j)}], \\
&+ \Pr_{\text{ideal}}[{}^{\exists} i, j \in \{1, \ldots, \} : i \neq j, Y^{(i)} = Y^{(j)}], \qquad (29) \\
&\leq \sum_{i \neq j} \Pr_{\text{ideal}}[X^{(i)} = X^{(j)}] + \sum_{i \neq j} \Pr_{\text{ideal}}[Y^{(i)} = Y^{(j)}], \qquad (30) \\
&\leq \sum_{i \neq j} \Pr_{\text{ideal}}[\alpha^{D^{(i)}} V^{(i)} \oplus \alpha^{D^{(j)}} V^{(j)} = M^{(i)} \oplus M^{(j)}], \qquad (31) \\
&+ \sum_{i \neq j} \Pr_{\text{ideal}}[\alpha^{D^{(i)}} V^{(i)} \oplus \alpha^{D^{(j)}} V^{(j)} = C^{(i)} \oplus C^{(j)}]. \qquad (32)
\end{aligned}
$$

ここで，ある i, j について確率

$$\Pr[\alpha^{D^{(i)}} V^{(i)} \oplus \alpha^{D^{(j)}} V^{(j)} = M^{(i)} \oplus M^{(j)}] \qquad (33)$$

の最大値を評価する．まず，$\widetilde{\mathsf{P}}$ の性質より，$\overline{T}^{(i)} (= (T^{(i)}, D^{(i)})) = \overline{T}^{(j)} (= (T^{(i)}, D^{(i)}))$ のときには $M^{(i)} \neq M^{(j)}$ および $C^{(i)} \neq C^{(j)}$ が成立する．従って $V^{(i)}$ と $V^{(j)}$ は同一の一様乱数であり，

$$\alpha^{D^{(i)}} V^{(i)} \oplus \alpha^{D^{(j)}} V^{(j)} = 0^n$$

である．よって式 (33) の確率は 0 である．$\overline{T}^{(i)} \neq \overline{T}^{(j)}$ のケースを二つに分ける．

- まず $T^{(i)} \neq T^{(i)}$ の場合，$V^{(i)}$ と $V^{(j)}$ はそれぞれ重複のない空間で一様に分布するため，$\alpha^{D^{(i)}} V^{(i)} \oplus \alpha^{D^{(j)}} V^{(j)} = \delta$ はどの $\delta \in \{0,1\}^n$ についても高々確率 $1/(2^n - 1)$ である．
- 次に $T^{(i)} = T^{(i)}$ の場合，$V^{(i)}$ と $V^{(j)}$ が同一のランダムな変数で，$D^{(i)} \neq D^{(i)}$ であるので，

  $$\alpha^{D^{(i)}} V^{(i)} \oplus \alpha^{D^{(j)}} V^{(j)} = (\alpha^{D^{(i)}} + \alpha^{D^{(j)}}) V^{(i)}$$

  である．α が生成元であり，$D^{(i)}, D^{(j)} < 2^n$ であることから $(\alpha^{D^{(i)}} + \alpha^{D^{(j)}})$ はゼロ元以外の $\mathrm{GF}(2^n)$ の元となる．したがって式 (33) の確率は $1/2^n$ である．

全体として，式 (33) の確率はどの $i \neq j$ についても高々 $1/(2^n - 1)$ とわかる．

同様に，

$$\Pr[\alpha^{D^{(i)}} V^{(i)} \oplus \alpha^{D^{(j)}} V^{(j)} = C^{(i)} \oplus C^{(j)}] \leq \frac{1}{2^n - 1} \tag{34}$$

も得られる．

これらの上界を式 (32) へ適用することで，

$$\begin{aligned}
&\Pr_{\text{ideal}}[^{\exists} i, j \in \{1, \ldots, \} : i \neq j, X^{(i)} = X^{(j)} \text{ or } Y^{(i)} = Y^{(j)}], \\
&\leq 2 \sum_{i \neq j} \frac{1}{2^n - 1}, && (35) \\
&\leq \binom{q}{2} \frac{4}{2^n}, && (36) \\
&\leq \frac{q^2}{2} \cdot \frac{4}{2^n}, && (37) \\
&\leq \frac{2q^2}{2^n} && (38)
\end{aligned}$$

とわかり，$\epsilon_1 = 2q^2/2^n$ と置くことができる．

次に Good transcript θ に対する $\Pr_{\text{real}}[\Theta = \theta]/\Pr_{\text{ideal}}[\Theta = \theta]$ の評価を行う．

まず，Ideal world では Tweak $\overline{T}$ が等しいクエリが c 個あった場合，オラクルからのレスポンスの確率分布は（暗号化クエリ，復号クエリの順番や個数によらず）

$$\frac{1}{(2^n) \cdot (2^n - 1) \cdot \cdots \cdot (2^n - (c-1))} = \frac{1}{(2^n)_c}$$

となる．より一般的には，Transcript でユニークな $\overline{T}^{(i)}$ が r 個存在するとし，その集合を $\{\bar{t}(1), \ldots, \bar{t}(r)\}$ とする．また，$\bar{t}(i)$ を用いたクエリが c_i 個あったとする．ここで $\sum_{i=1,\ldots,r} c_i = q$ である．

簡単のためすべてのクエリが暗号化クエリであったとする．このとき，Y と V および D から C は一意に定まり，X と V および D が定まれば M は一意であるため，

$$\begin{aligned}
&\Pr_{\text{ideal}}[\Theta = \theta] \\
&= \Pr_{\text{ideal}}[(Y^{(i)} = y^{(i)})_{i=1,\ldots,q} | \\
&\quad (X^{(i)} = x^{(i)})_{i=1,\ldots,q}, (V^{(i)} = v^{(i)})_{i=1,\ldots,q}, (D^{(i)} = d^{(i)})_{i=1,\ldots,q}] && (39) \\
&\cdot \Pr_{\text{ideal}}[(V^{(i)} = v^{(i)})_{i=1,\ldots,q}] && (40)
\end{aligned}$$

となる．Ideal world において $V^{(i)}$ の分布はクエリへのレスポンスと独立であるので，式 (39) の $V^{(i)}$ の条件節は不要となり，式 (39) の確率は

$$\frac{1}{(2^n)_{c_1} \cdot (2^n)_{c_2} \cdot \cdots \cdot (2^n)_{c_r}}$$

と書き換えられる．式 (40) の確率は，r 個のユニークな Tweak $\overline{T}$ が存在することから

$$\frac{1}{(2^n)_r}$$

である．従って

$$\Pr_{\text{ideal}}[\Theta = \theta] = \frac{1}{(2^n)_{c_1} \cdot (2^n)_{c_2} \cdot \cdots \cdot (2^n)_{c_r}} \cdot \frac{1}{(2^n)_r}.$$

なお，暗号化と復号クエリが入り混じる場合での議論も，攻撃者が決定的であるという仮定によって全く同じ式が導出される．

Real world においては，$X^{(i)}$ および $Y^{(i)}$ がすべての $1 \le i \le q$ についてユニークであることが good transcript の条件であることから，

$$\begin{aligned}
&\Pr_{\text{real}}[\Theta = \theta] \\
&= \Pr_{\text{real}}[(Y^{(i)} = y^{(i)})_{i=1,\ldots,q} | \\
&\quad (X^{(i)} = x^{(i)})_{i=1,\ldots,q}, (V^{(i)} = v^{(i)})_{i=1,\ldots,q}, (D^{(i)} = d^{(i)})_{i=1,\ldots,q}] && (41)\\
&\cdot \Pr_{\text{real}}[(V^{(i)} = v^{(i)})_{i=1,\ldots,q}] && (42)\\
&\le \frac{1}{(2^n)_q} \cdot \frac{1}{(2^n)_r} && (43)
\end{aligned}$$

と書くことができる．

ここで任意の正の整数 a および非負の整数 b, c, $b + c \le a$ について $(a)_{b+c} < (a)_b \cdot (a)_c$ であることに注意すると，

$$\begin{aligned}
&\frac{\Pr_{\text{real}}[\Theta = \theta]}{\Pr_{\text{ideal}}[\Theta = \theta]} && (44)\\
&= \frac{1}{(2^n)_q} \cdot \frac{1}{(2^n)_r} \cdot \frac{(2^n)_{c_1} \cdot (2^n)_{c_2} \cdot \cdots \cdot (2^n)_{c_r}}{1} \cdot \frac{(2^n)_r}{1} && (45)\\
&\ge 1. && (46)
\end{aligned}$$

が導かれる．従って $\epsilon_2 = 0$ が導かれる．

最後に $\epsilon_1 = 2q^2/2^n$, $\epsilon_2 = 0$ を補題 4.1 へ代入することで，

$$\mathbf{Adv}^{\mathtt{tsprp}}_{\mathrm{XTSb}_{\mathrm{P}_1,\mathrm{P}_2}}(\mathcal{A}) \le \frac{2q^2}{2^n}$$

が証明された．

■最終的な安全性のバウンド　上記の情報理論的安全性証明と標準的な計算量的安全性への変換 [BDJR97] から，実際のブロック暗号を持ちいた XTSb_K の安全性を導出することができる．XTSb_K に対する q 回のクエリ，計算量 τ の攻撃者 $\mathcal{A}$ に対して，内部のブロック暗号 E_K に対する $2q$ クエリ，計算量 $\tau + O(q)$ の攻撃者 $\mathcal{A}'$ が存在し，

$$\begin{aligned}
&\mathbf{Adv}^{\mathtt{tsprp}}_{\mathrm{XTSb}_K}(\mathcal{A}) \\
&\leq \mathbf{Adv}^{\mathtt{sprp}}_{E_{K_1}}(\mathcal{A}') + \mathbf{Adv}^{\mathtt{sprp}}_{E_{K_2}}(\mathcal{A}') + \mathbf{Adv}^{\mathtt{tsprp}}_{\mathrm{XTSb}_{\mathsf{P}_1,\mathsf{P}_2}}(\mathcal{A}) \qquad (47) \\
&\leq 2\mathbf{Adv}^{\mathtt{sprp}}_{E_K}(\mathcal{A}') + \frac{2q^2}{2^n} \qquad (48)
\end{aligned}$$

が証明される．

5　データ長が n の倍数でない場合の安全性

5.1　理想的な安全性定義

データ長が $n = 128$ の倍数でない場合，すなわち Ciphertext Stealing を組み合わせた場合の安全性の定義および証明については，IEEE, NIST ともに明確な記述はない．原則からいえば NBE を拡張して定義し，その拡張された NBE との判別困難性により定義すべきと思われる．この場合，例えば平文の最終 2 ブロックを M_{m-1}, M_m とし，$|M_{m-1}| = n$ かつ $|M_m| = s < n$ の場合には，この最終 2 ブロックのみ $n + s$ ビットブロック（for $s = 1, \ldots, n$）の可変長ブロックに対応した Tweakable ブロック暗号 $\widetilde{\mathrm{XTSb}}_K$ で暗号化する，というような NBE が考えられる（図 9 ）．この NBE は，直感的には $\widetilde{\mathrm{XTSb}}_K$ と XTSb_K 双方が計算量的に独立とみなせる Tweakable 強疑似ランダム置換であれば安全といえる．このモデルであれば，XTSb_K の（固定長）Tweakable ブロック暗号としての安全性に加えて，$\widetilde{\mathrm{XTSb}}_K$ の（可変長）Tweakable ブロック暗号としての安全性を考慮することで，弱いブロック暗号化としての安全性を自然に定義することが可能である．

具体的な構成方法としても，$\widetilde{\mathrm{XTSb}}_K$ を 4.4 節で述べたいくつかの強いブロック暗号化方式を $n + s$ ビット平文に対して用いることで，効率の劣化は最小限におさえられるうえ，$\widetilde{\mathrm{XTSb}}_K$ の安全性は $O(q^2/2^n)$ を達成することができるため，データ長が n の倍数である場合（式 (47)）と同等の理論的安全性を達成できる．

しかし，Ciphertext Stealing を用いる XTS の仕様が上記の安全性定義を満たすかという観点でみると，明らかに安全ではない．これは，例えば異なる二つの $(M_{m-1}, M_m), (M'_{m-1}, M'_m)$ について，もし $M_{m-1} = M'_{m-1}$，$M_m \neq M'_m$ の場合，対応する暗号文 (C_{m-1}, C_m) と (C'_{m-1}, C'_m) において $C_m = C'_m$ が必ず起きてしまうからである．同様の指摘は 7 章で紹介する CRYPTREC レポートでもみられる．

なお，最後の 2 ブロックをまとめて暗号化せず，通常の n ビットブロック Tweakable ブロック暗号である XTSb_K と，s ビットブロック（for $s = 1, \ldots, n$）の Tweakable ブロック暗号 $\widetilde{\mathrm{XTSb}}'_K$ とで暗号化を行う定義も可能ではあるが，この場合，$\widetilde{\mathrm{XTSb}}'_K$ の実現方法によらず，同一セクタで最終の s ビットブロックについて 2^s 個の平文暗号文対を入手した敵は，それ以降暗号文のみで最終ブロックの復号が可能となる．言い換えれば，$\widetilde{\mathrm{XTSb}}'_K$ が達成できる暗号学的安全性にそもそも s に依存した限界があり，s が小さい場合にはこれは現実的となるため問題である．

また一般的に知られる $\widetilde{\mathrm{XTSb}}'_K$（for $s \in \{1, \ldots, n-1\}$）の構成方法は，現状知られているものでは，非常に効率が悪いものか，あるいは効率がよいが $2^{s/2}$ 程度のクエリ回数で破れる方式のいずれかのケースになっており，これも実現する上での問題となる．

5.2 Ciphertext Stealing の既存研究と XTS との関連

Ciphertext Stealing 自体の既存の安全性評価について概観する．NIST SP 800-38A が定める CTS の方式は最終 2 ブロック以外は CBC モードそのものであり，最終 2 ブロックで，XTSb_K でなくブロック暗号 E_K そのものを用いて図 6 同様の処理を行う．2 ブロックの出力の順序が異なる 3 つの方式が定義されており，それぞれ CBC-CS1, CBC-CS2, CBC-CS3 と呼ばれる．XTS における CTS は CS3 に相当する．

CTS モードの安全性解析については 坂田ら [Sak09] の SCIS 論文と，Rogaway ら [RWZ12] が存在する．

いずれも，暗号文と乱数との判別不能性が CTS モードで満たされることを証明している．具体的には，Rogaway ら [RWZ12] では CS1, CS2, CS3 のいずれも予測不能な IV の下では標準的な安全性（出力の乱数との識別不能性，IND$）を満たすことを示している．さらに [RWZ12] は，暗号化の出力をブロックごとに観測し，ブロックごとに入力できるオンライン攻撃（すなわち C_i を観測

してから M_{i+1} を決定できる）を考えた場合の CTS の安全性を検討している．この攻撃は Blockwise-adaptive 攻撃とも呼ばれる．Blockwise-adaptive/オンライン攻撃は Fouque ら [FJP04] によって考案されており，ベースとなる CBC 自体がオンライン攻撃への耐性がないが，Delayed-CBC [FMP03] と呼ばれるシンプルな変更によって安全となることが知られている．Rogaway らは Delayed-CBC に Ciphertext stealing を加えるとき，CS1，CS2，CS3 のいずれの場合でもオンライン攻撃への安全性が保証できることを示した．

ただし，これらの結果を直接 XTS の Ciphertext Stealing の解析に用いることはできず，別途解析が必要である．大きな違いとして，CTS では予測不能な IV を用いるのに対して，XTS では Tweak を用いることがある．XTS では同一セクタ（すなわち同一の T）の暗号文を継続して観測する攻撃者を考えることができるが，CTS ではこれは複数の平文の同一 IV での暗号化に相当し，そもそも安全性の根拠がなくなった状態に相当する．

Liskov-Minematsu のパブリックコメント [LM06] では，XTS の Ciphertext Stealing におけるおおまかな解析が述べられており，若干ラフであるが，結局 XTS において partial block がある場合の暗号化は，partial block なしのバージョン（すなわち NBE[XTSb$_K$]）の暗号化を 2 回用いて実現可能であることから，安全であると述べている．また，最終 2 ブロック，(C_{m-1}, C_m) の暗号化処理に着目すると，例えば既知平文攻撃，つまり平文がランダムな場合には暗号文も十分ランダムであり，暗号文と乱数との判別のアドバンテージが $O(q^2/2^n)$ であることが分かる．これは，2 回コールされる XTSb$_K$ の入力が常に十分なランダムネスを持つためである．ただしこれは，ECB モードが既知平文攻撃に対して十分な安全性を持つ（例えば [GH09] 参照）ことと同様であり，暗号学的な保証としては十分強いとは言い難い．一方平文の分布が偏っているケースでは，Ciphertext Stealing の有無によらず XTS はブロック間の情報伝搬がないことから，同じセクタ内での暗号文の変化を観測することで平文についての情報が洩れる．Ciphertext Stealing の存在によって，最終 2 ブロック分の情報の平文情報の洩れ方は大きくなっているといえるが，それを定量的に評価することは困難である．

7 章の CRYPTREC レポートでも繰り返し言及されているように，XTS の安全性は認証暗号（AEAD）などと比べて学術的に確立されたものがない．それでも Ciphertext Stealing がない場合であれば，少なくとも 4 章に記載したように形式的な安全性の定義（弱いブロック暗号化）と，それが実用上意味す

るところは比較的イメージしやすい．

しかし，Ciphertext Stealing を用いる場合では，安全性のゴールが何であるかがはっきりと示すことは困難である．

以上を踏まえると，Ciphertext Stealing を用いることについては，例えば，平文の分布によらず暗号文のみ攻撃で情報が漏洩する，といった致命的な問題がある訳ではないものの，もともと安全性定義にあいまいさがある XTS をさらにあいまいにする要素であって，現状その利用を推奨する根拠に乏しいと言わざるを得ない．

なお，実用上は，ハードディスクなどストレージのセクタ単位の暗号化のケースでは，1 セクタのバイトサイズが 16 の倍数となっていることがほとんどであるため，Ciphertext Stealing を用いるケースは稀であると推測される．

6　そのほかの要件に関する考察

6.1　通常のナンスベース暗号化としての利用

XTS を通常のナンスベースの暗号化としてみた場合の安全性を考察する．具体的には，セクタ番号 T をナンスとして用いて，可変長平文（ただし XTS の入力制約から，n ビット以上）を XTS で暗号化するものとする．このときは，カウンターモードや CBC モードなどと同等の安全性が保証される．すなわち，XTS が n ビットブロック暗号をベースとし，攻撃者が合計 σ ブロックの選択平文質問を行った上で，暗号文と乱数の判別を試みる場合，そのアドバンテージは $O(\sigma^2/2^n)$ となる．安全性の証明は，暗号文のブロック $(C_1, C_2, \ldots, C_m)$ ごとに個別の Tweak で暗号化がなされていることと，XEX が Tweak ごとに独立な強疑似ランダム置換を実現することから，ほぼ自明となる．最終 2 ブロックについては CTS がなされている場合とそうでない場合で分ける必要があるが，Tweak のセクタ番号 T がクエリごとに異なることと，CTS がなされる場合でも，C_{m-1} が Tweak (T, m) での XTSb_K 暗号化の出力全部を用いていることと，C_m が Tweak $(T, m-1)$ での XTSb_K 暗号化の出力 $|M_m|$ ビットを用いていることを考えれば，出力暗号文の最終 2 ブロックに $n + |M_m|$ ビット分の（計算量的に安全な）疑似乱数が含まれることが確認できるため，十分である．

なお XTS ではなく XEX をナンスベース暗号化として用いると，認証暗号である OCB，特に OCB2 [Rog04] の暗号化部分と実質的に同じとなる．違

いとしては最終 2 ブロックの暗号化で Ciphertext Stealing を用いることにある．なお認証暗号としての OCB2 には証明に誤りがあり，現実的な攻撃があることが最近報告された（Inoue-Minemastu [IM18], Poettering [Poe18], Iwata [Iwa18]）が，これは認証暗号としての攻撃であり，また最終ブロックの暗号化方式が XEX でないことに起因するものであるため，XTS/XEX には影響はない．

6.2 マスク値漏洩の効果：有効なセクタ番号の場合

ブロック暗号のマスク値として生成される，式 (3) における $E_{K_2}(T)$ がサイドチャネル攻撃や $O(2^{n/2})$ ブロックのデータを用いたバースデー攻撃など何らかの理由で漏洩した場合，攻撃者は容易に XTSb_K と Tweakable ランダム置換との判別が可能となるため，注意が必要である．例えば，あるセクタ T に対するマスクの初期値 $V = E_{K_2}(T)$ を入手した攻撃者は，平文として $V \otimes \alpha^D$ を与えて Tweak $\overline{T} = (T, D)$ で暗号化すると，暗号文が

$$\begin{aligned} &E_{K_2}(T) \otimes \alpha^i \oplus E_{K_1}(E_{K_2}(T) \otimes \alpha^D \oplus E_{K_2}(T) \otimes \alpha^i) \\ &= E_{K_2}(T) \otimes \alpha^D \oplus E_{K_1}(0^n) \end{aligned} \tag{49}$$

となる．次に任意の $D' \neq D$ を用いて，平文として $V \otimes \alpha^{D'}$ を tweak (T, D') で暗号化し，得られた暗号文

$$E_{K_2}(T) \otimes \alpha^{D'} \oplus E_{K_1}(0^n) \tag{50}$$

を得る．二つの暗号文の差分は

$$E_{K_2}(T) \otimes \alpha^D \oplus E_{K_2}(T) \otimes \alpha^{D'} = E_{K_2}(T) \otimes (\alpha^D \oplus \alpha^{D'}) \tag{51}$$

となり，これは V より計算可能な値となる．これにより，XTSb_K と Tweakable ランダム置換の判別が可能となる．

より一般的には，マスク $E_{K_2}(T)$ の漏洩があった場合には，セクタ T に関しての暗号化が，本質的に ECB モードとなるため，暗号文のみから平文に関する情報漏洩が起きると推測される．ECB モードは低エントロピーの平文のときに平文の情報漏洩を起こすことがよく知られている[*5]．ただし，ECB モードとはいっても攻撃者が既知の $E_{K_2} \otimes \alpha^D$ でマスクしたものになるため，単に低エントロピーの平文なら漏洩が起きるとは限らない．バースデー攻撃によりマスクが漏洩した場合の平文回復の可能性については 8 章で詳しく検討する．

[*5] 例えば `https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation`.

6.3 マスク値漏洩の効果：有効でないセクタ番号の場合

上記のマスク漏洩が，もしセクタ番号として有効でない T について起きた場合を考える．この場合，$E_{K_2}(T)$ がある特定の T について漏洩しているとしても，この T が実際の暗号化における tweak として使われないのであれば，XTSb_K は依然として安全である．XEX において，$E_K(T)$ が漏洩した場合でも T を tweak として使わない場合には安全であることが [MM09] により証明されており，二つの鍵を用いる XTS の場合も同様に証明可能である．

しかしながら，実用上のシナリオでマスク値がいかなる T について漏洩するかを制御するのは困難とも想定されるため，漏洩を前提とした運用は実際には避けるべきと考えられる．

6.4 XEX との安全性のギャップ

前述のように，XTS は XEX モードの鍵をマスク生成と ECB 暗号化の部分で二つに分けている．従って，XTS の二つのブロック暗号鍵として同じものを使っていた場合は，XEX モードと同一の処理となる．二つの鍵を一つにできるという点で XEX には明確なメリットがあるが，XEX で tweak $\overline{T} = (T, 0)$ をある $T \in \{0,1\}^n$ で許容すると，ブロック単位の処理 XEXb_K について以下の攻撃が見いだされる [Min06].

1. 復号オラクルへ $C_1 = 0^n$ を tweak $\overline{T} = (T, 0)$ で質問する．
2. 平文 $M_1 = E_K^{-1}(E_K(T)) \oplus E_K(T) = T \oplus E_K(T)$ を得る．ここから $E_K(T) = M_1 \oplus T$ を求める．
3. 次に暗号化オラクルへ $M_2 = \alpha^1 \otimes (M_1 \oplus T) \oplus T$ を tweak $\overline{T}' = (T, 1)$ で質問．
4. 暗号文 C_2 を得る．
5. このとき，C_2 は $C_2 = E_K(T) \oplus \alpha^1 \otimes E_K(T)$ を満たすため，M_1 からオラクルアクセスなしに計算可能となる．

これは，XEXb_K と Tweakable ランダム置換との判別が可能であり，Tweakable ブロック暗号としての安全性が破れることを意味している．従って，単一鍵とする場合には，Tweak $\overline{T} = (T, D)$ において $D = 0$ を排除することが重要である．

6.5 カスケードした場合の安全性について

Triple DES などと同様に，鍵を変えて XTS を複数かけることが考えられる．実際に Veracrypt などのソフトウェアでは複数の異なるブロック暗号を用いて XTS を重ねるモードが選択可能である．Landecker ら [LST12] により，XTSb_K を含むブロック単位の Tweakable ブロック暗号を 2 重化した場合の安全性が証明されており，単一の XTSb_K が $n/2$ ビット安全性であるのに対して，$2n/3$ ビット安全性が達成できることが証明されている．また一般に r 重化した場合の安全性は $rn/(r+1)$ ビットであることが Lampe ら [LS13] で示されている．従って，具体的な適用の仕方によるが，カスケードにより実際に安全性は向上するといえる．

6.6 LRW モード，およびその安全性に関する指摘

LRW モードとは，二つのブロック暗号の鍵 $K = (K_1, K_2)$ を使って，

$$\begin{aligned}
&\mathrm{LRWb}_K(M,T) = S \oplus E_{K_1}(M \oplus S),\\
&\mathrm{LRWb}_K^{-1}(C,T) = S \oplus E_{K_1}^{-1}(Y \oplus S),\\
&S = K_2 \otimes T
\end{aligned} \tag{52}$$

という形でブロックの暗号化を行うものである．ここでは T は n ビット値であり，ストレージのブロックを表すインデックスである．したがって XTS とは異なり，T がセクタ番号とブロックインデックスを合わせた情報となる．ブロックインデックスをインクリメントするたびに乗算が発生するが，実際には $K_2 \otimes T$ から $K_2 \otimes (T+1)$ の計算は容易であるため，計算コストは XTS とほぼ同等といえる．

LRW モードの安全性については，4.6 節と同様の導出によって，計算量的安全性が証明可能であり，その安全性のバウンドについてもほぼ XEX/XTS と同じである．

なおストレージ暗号化の文脈で LRW モードという名前がさす暗号化方式と，一般的に Liskov ら論文で提唱した Tweakable ブロック暗号化の方式とは必ずしも一致するものではない．後者のほうが一般的と言えるが，いずれにせよ LRW モードの定義については広くコンセンサスがあるとはいえない．

LRW モードは XTS の IEEE 標準化に先立って検討が行われた方式である

が，鍵自体の暗号化を行った場合の危険性を指摘された．これは，以下のような攻撃である．

1. $M = K_2$ を Tweak T で暗号化する．
2. $C = E_{K_1}(K_2 \oplus K_2 \otimes T) \oplus K_2 \otimes T$ を得る．
3. $M' = 0^n$ を Tweak $T+1$ で暗号化する．
4. $C' = E_{K_1}(0^n \oplus K_2 \otimes (T+1)) \oplus K_2 \otimes (T+1) = E_{K_1}(K_2 \oplus K_2 \otimes T) \oplus K_2 \otimes (T+1)$ を得る．
5. $C \oplus C' = K_2 \otimes T \oplus K_2 \otimes (T+1) = K_2$ を得る．

したがって攻撃者は暗号文の差分から鍵の一部 K_2 を入手可能となる．

このような攻撃は XEX や XTS には明示的には知られていないが，一方，後述する CRTPTREC レポートでも触れられているように，平文が鍵ないしその一部であった場合の XTS の安全性は示されていない．このように暗号学的な安全性の保証がないことを鑑みると，XTS での暗号化対象に鍵情報そのものが含まれることは避けるべきである．

7 CRYTPTREC 報告書における XTS の評価内容の検討

2012 年の CRYPTREC レポート [Rog11] において，著名な暗号研究者である Rogaway 教授により，暗号利用モードの広範な評価が行われた． XTS も評価対象となっており，その主な主張は以下のとおりである．

- XTS 自体の明確な安全性定義がない．XTS はセクタ単位の暗号化，いわゆる wide-block encryption とみるべき．
- その形式上，XTS は EME2 などと異なり理想的な wide-block encryption = Wide-block 強疑似ランダム置換でない以上，安全性の妥協が必要だが，どのような定義も困難．
- 直感的には安全性を秘匿性と頑健性（non-malleability）で定義すべきだが，
- 上記の困難性は主に最終ブロックが n bit 未満の Ciphertext stealing (CTS) の処理に起因する．それさえなければ，filter function の導入により，ブロックごとの漏洩情報，すなわち同じ平文の繰り返しのみを許容した安全性定義ができる．

- 目指すべきゴールは，n ビットブロックと最終 2 ブロックの $n+b$ ビットブロックとが混在する Tweakable 強疑似ランダム置換によるブロックごとの暗号化（ 5.1 節で述べたものと同様）.
- 最終 2 ブロックが CTS のため，$b \neq 0$ であれば上記の安全性定義は破れてしまう．$b = 1$ の例を提示.
- XTS を改良するために，最終 2 ブロックの処理としていくつかの案を提示.
- ただし上記の ECB-like モード の安全性の定式化は学術的・実用的に意義があるかは疑問である.
- XEX を 2 キー構成にした XEX2 を用いているのは問題ない．LRW を使う場合の鍵依存メッセージ (Key-dependent Message, KDM) 安全性の懸念は正しい．なお XEX2 や XEX での KDM 安全性が証明されているわけではない．結果的にはそれらを理想暗号モデル（Ideal-cipher model）において証明することも可能であろう.
- セクタ単位の WBE も標準化すべき.

これらの評価内容は全体的に同意できるものである．特に CTS 部分の理論的安全性については問題となりうるが，XTS の主要な用途である ディスクフォーマットではセクタサイズが 16-byte の倍数に収まるため，顕在化していないと思われる.

最終 2 ブロックの処理として CRYPTREC レポートでいくつか提案された案のうち，XLS [RR07] については証明の誤りがあり，実際にアタック可能 [Nan14] であるため利用は推奨されない．HEM [Zha12] などの新しい方式も存在する.

8 大量のデータを用いたバースデー攻撃（Birthday attack）による平文回復

8.1 バースデー攻撃

4 章でのべたように，XTS の安全性は暗号化ないし復号を行ったデータの量 σ がひとつの XTS の鍵につき $2^{n/2}$ ブロックよりも十分小さいときに担保される．反対に，σ が $2^{n/2}$ に近いかそれ以上となった場合にどのような攻撃があるかは検討の必要がある.

このような攻撃は大抵，$\sigma \approx 2^{n/2}$ で暗号化処理中の何らかの中間変数で衝突が起きることを利用しており，変数の衝突がバースデーパラドックス（Birthday paradox）と関連している事象であるため，バースデー攻撃とも呼ばれる．また，σ が $2^{n/2}$ より十分小さいならば安全となる（すなわち判別の Advantage が十分小さい）方式を，up-to-birthday-bound (upBB）安全と呼ぶこともある．

XTS-AES においては $n = 128$ であるために，バースデー攻撃を成立させるためには $2^{n/2} = 2^{64}$ ブロック$= 2^{68}$ バイトつまり 256 エクサバイトのデータ処理が必要となる．このデータ量は現在のところは，大規模なクラウドサービスやデータセンターを考えても現実的でなく，またこれらの大量データを扱うケースにおいても単一鍵で処理するデータ量はさらに大幅に小さいことが予想される．しかしながら今後のコンピュータとストレージの発展に伴い，徐々にリスクが高まっていくと見込まれるため，検討が必要である．

そのほか upBB 安全な方式に対してバースデー攻撃の存在の有無，影響などを検討することは以下の観点から重要である．

- 安全性証明がある暗号利用モードの安全性のタイトさを示す．すなわち $O(2^{n/2})$ のデータを用いた攻撃を示すことで，攻撃成功確率の上界と下界の一致を示す．
- 必要な鍵更新の頻度を明らかにする．
- ブロックサイズを小さくした場合の現実的なリスクを明らかにする．

特にストレージ暗号化の場合，鍵の更新を行っても過去に暗号化したデータの復号をサポートする必要があるため，更新は容易ではない．例えば過去に暗号化した全データの復号と再暗号化を行うのは非常に計算コストが高い．

また，実際に XTS，あるいはその前身である LRW は様々な暗号化製品・暗号化ソフトウェアにおいて，64 ビットブロック暗号でも用いられている．例えば古いバージョンの Truecrypt や，BestCrypt [*6]といった暗号化ソフトウェアにおいて，Blowfish や TDES といった 64 ビットブロック暗号での LRW モードに対応している．

XTS に対する攻撃の目的としては，乱数との判別なども考えることが可能であるが，本報告では特に実現したときの影響が大きいと思われる平文回復に対して検討を行うものとする．

[*6] https://www.jetico.com/data-encryption

8.2 攻撃シナリオ

前の章で見てきたように，XTS 全体に対する適切な安全性の定義は容易ではなく，したがって攻撃を考える際には攻撃シナリオを適切に設定するところから始めなければならない．

まず，正規のユーザはセクタ単位で任意データの XTS 暗号化ないし復号が可能であるものとする．攻撃者は XTS で暗号化された HDD, SSD などのストレージの内容を観測することができるものとする．暗号化されたセクタを，攻撃者の観点で以下の 2 種類に分類する．

1. 暗号化されていて平文が未知であるか，あるいは部分的に既知であるセクタ．これは，例えば OS を含めシステムの情報から利用が推定できるプログラムが格納されたセクタなどである．「部分的に既知」という状態は，セクタ内のいくつかのブロックについてのみ既知であるケースや，セクタのいくつかのブロックのさらに一部バイトのみが既知であるケースなど考えられる．
2. 暗号化されているが平文が既知であり，かつ暗号文へ任意の改ざんを行った結果も攻撃者が観測可能なセクタ．例えば文献 [ED08] で指摘されているように，OS のブート画面など特別な権限を要さずに画面から復号結果を視覚的に得る，ということが考えられる．

ただし，攻撃者はどのセクタが上記のカテゴリに属するかは，事前の知識や調査，例えば使用されている OS の推定，改ざんを行った結果の観測など，で既知であるものとする．同様の仮定はそのほかの文献（例えば [KMV17] や [Omo08]）でも見られる．

カテゴリ 2 のセクタをリファレンスセクタ，カテゴリ 1 のセクタをターゲットセクタと呼ぶことにする．どちらのカテゴリのセクタも一般に複数存在するが，ここでは簡単のため，ある特定のリファレンスセクタ $T^{(r)}$ とターゲットセクタ $T^{(t)}$ に対する攻撃を考える．リファレンスセクタの数は一般に極めて少ないものと想定される．また，リファレンスセクタの一部でのみ暗号化と復号が可能である場合も想定される．しかし本報告で示す攻撃は，一部分のブロックにのみ暗号化・復号が適用可能でさえあれば十分である．具体的には，リファレンスセクタ内の 2 ブロックで暗号化と復号ができれば実施可能である．

攻撃の目的は，リファレンスセクタへのバースデー攻撃を用いて，ターゲッ

トセクタの未知の平文ブロックの内容を得ることにある．

■攻撃のアイディア　攻撃の基本的アイディアを説明する．まずリファレンスセクタでの衝突攻撃を用いてマスクを求める．これにより，リファレンスセクタの暗号化は実質的に E_{K_1} による ECB モードと同等となる．リファレンスセクタに対する暗号文はそもそも復号可能としているので，マスクが分かったところでこれ以上の攻撃はほぼ無意味と言ってよい．しかしながら，リファレンスセクタへの暗号化と復号のマスクが既知であることは，E_{K_1} への直接の暗号化・復号クエリが可能，すなわちリファレンスセクタへのアクセスが E_{K_1} オラクルとなることを意味する．いわば，XTS が，ターゲットセクタのマスクを鍵とした 1 ラウンド Even-Mansour（Single-round Even-Mansour, SEM）暗号としてみなせることを意味し，従って既存の SEM への攻撃方法を利用することが可能となる．SEM の内部の鍵なし置換へのクエリをオフラインクエリと呼び，SEM 自体へのクエリをオンラインクエリとも呼ぶ．前者がリファレンスセクタへのクエリ，後者がターゲットセクタへのクエリに相当する．SEM への攻撃に必要なオンライン・オフラインクエリ数はトレードオフが可能であり，例えばリファレンスセクタへの攻撃計算量・メモリ量に比べて，ターゲットセクタへは大幅に少ない計算量・メモリ量で攻撃することも可能である．

この事実を利用してターゲットセクタ $T^{(t)}$ の平文回復を行う．前述のように，ターゲットセクタの平文に対する知識はなにもないか，あっても部分的である．これを，既知平文攻撃よりも弱いクエリしかできないものとしてモデル化する．前述のとおりモデルを単純化し，リファレンスセクタ，ターゲットセクタとも一つとし，攻撃者のクエリはブロック単位，すなわち XTSb_K に対するものとする．このとき，クエリの Tweak は $\overline{T} = (T, D)$ の形をとる．

8.3　リファレンスセクタの衝突攻撃によるマスク回復

まずリファレンスセクタ $T^{(r)}$ のマスク値 $L^{(r)} = E_{K_2}(T^{(r)})$ の回復の方法を示す．XTS の構造から，$2^{n/2}$ 回程度の暗号化オラクルアクセス（すなわちバースデー攻撃）を用いれば内部のブロック暗号への入力での衝突が起きるため，これを用いた $E_{K_2}(T^{(r)})$ の回復が可能であることは容易に推測できる．例えば，リファレンスセクタ内部の特定の 2 ブロック $(T^{(r)}, D)$ と $(T^{(r)}, D')$（D と D' は異なる正整数）で既知平文 M と M' を暗号化し，暗号文 C と C' を観

測したとする．対応するブロック暗号の入出力を

$$X = M \oplus \alpha^{D} L^{(r)} \tag{53}$$
$$X' = M' \oplus \alpha^{D'} L^{(r)} \tag{54}$$
$$Y = C \oplus \alpha^{D} L^{(r)} \tag{55}$$
$$Y' = C' \oplus \alpha^{D'} L^{(r)} \tag{56}$$

と表すとする．このとき

$$M \oplus M' = (\alpha^{D} + \alpha^{D'}) L^{(r)} \oplus X \oplus X' \tag{57}$$
$$C \oplus C' = (\alpha^{D} + \alpha^{D'}) L^{(r)} \oplus Y \oplus Y' \tag{58}$$

である．もし $X = X'$ のときは $Y = Y'$ となるため，

$$M \oplus M' = (\alpha^{D} + \alpha^{D'}) L^{(r)} = C \oplus C' \tag{59}$$

が成立する．したがって M, M', C および C' が $M \oplus M' = C \oplus C'$ を満たすときには，高い確率で $X = X'$ かつ $Y = Y'$ が成立していると推定される．マスク値は $\mathrm{GF}(2^n)$ 上の除算を用いて

$$L^{(r)} = M \oplus M' / (\alpha^{D} + \alpha^{D'}) (= C \oplus C' / (\alpha^{D} + \alpha^{D'}))$$

という計算で求めることが可能である．

よって M_i と M_i' を i ごとに値を変えながら，それぞれ $q = 2^{n/2}$ 回暗号化を行い，暗号文 C_i と C_i' を得たのち，集合 $\mathcal{M} = \{M_i\}_{i=1,\ldots,q}$, $\mathcal{M}' = \{M_i'\}_{i=1,\ldots,q}$, $\mathcal{C} = \{C_i\}_{i=1,\ldots,q}$ および $\mathcal{C}' = \{C_i'\}_{i=1,\ldots,q}$ の中から

$$M_i \oplus M_j' = C_i \oplus C_j'$$

を満たす $(M_i, M_j', C_i, C_j') \in \mathcal{M} \times \mathcal{M}' \times \mathcal{C} \times \mathcal{C}'$ を見つけることでマスク回復が可能である．

このバースデー攻撃のデータ量，メモリ量とクエリ回数は $O(2^{n/2})$ となっている．しかし単純に $M \oplus M'$ と $C \oplus C'$ の一致を求めるためには二つの大きさ $2^{n/2}$ の集合の要素のあらゆる組み合わせについて排他的論理和をとって比較する必要があるため，時間計算量が $2^{n/2} \times 2^{n/2} = 2^{n}$ のオーダとなってしまう．

そこで，中間者一致攻撃のアイディアを利用して，時間計算量も $O(2^{n/2})$ に削減する方法を以下に示す．具体的には $M \oplus C$ と $M' \oplus C'$ の一致をチェックすればよい．

■攻撃の手順

1. $(M_i, \overline{T} = (T^{(r)}, D))$ と $(M'_i, \overline{T}' = (T^{(r)}, D'))$ を i ごとに値を変えつつ $2^{n/2}$ 回暗号化クエリを行う．例えば $i = 1, \ldots, 2^{n/2}$ について i ごとにユニークな n ビット値を d_i とし．$M_i = M'_i = d_i$ とすればよい．
2. M_i および M'_i の暗号化により暗号文 C_i と C'_i を得る．
3. 暗号化の結果のリスト (i, M_i, C_i) に加えて，$(i, M_i \oplus C_i)$ のリスト $\mathcal{S}$ と $(i, M'_i \oplus C'_i)$ のリスト $\mathcal{S}'$ を作成する．
4. $s = (i, z) \in \mathcal{S}$, $s' = (j, z') \in \mathcal{S}'$ について $z = z'$ を満たす $(i, j) \in \{1, \ldots, 2^{n/2}\}^2$，$i \neq j$ を見つけ，すべてリストにする．
5. 上記の (i, j) すべてについて，

   $$(C_i \oplus C'_j)/(\alpha^D + \alpha^{D'})$$

   を $L^{(r)}$ の候補として出力する．

上記の攻撃において，ステップ 3 で発見したペアは $M_i \oplus M'_j = C_i \oplus C'_j$ を満たすため，高い確率で $X_i = X'_j$ および $Y_i = Y'_j$ を満たしており，したがってマスクの予想が高い確率で成功する．予想したマスクが正しいかどうかは追加のクエリを数回行うことで検証可能である．これにより，マスクの回復が高い確率で成功する．ステップ 2 は二つの大きさ $2^{n/2}$ のリスト要素の衝突発見を行うものなので，時間・空間計算量とも $O(2^{n/2})$ となる．より詳細には，

- 時間計算量：$2^{n/2}$ XTS のブロック暗号化
- データ量：$2^{n/2+1}$ 既知平文 / 暗号文対
- メモリ量：$2^{n/2}$ ブロック

となる．例えば 128 ビットブロック暗号であれば時間計算量 2^{64}，データ量 2^{65} 暗号文ペア，メモリ量 2^{64} ブロックとなり，64 ビットブロック暗号では時間計算量 2^{32}，データ量 2^{33} 暗号文ペア，メモリ量 2^{32} ブロックとなる．

8.4 ターゲットセクタへの部分的既知平文攻撃

ターゲットセクタのブロック $(T^{(t)}, D)$ のうち，ある $D \in \mathcal{D}$ については既知平文攻撃可能，またターゲットセクタ全体の暗号文を観測可能とする．この仮定のもと，ブロック $(T^{(t)}, D')$，$D' \notin \mathcal{D}$ について平文回復を行う．

ターゲットセクタのブロック D へのクエリで (M, C) を得たとき，E_{K_1} の入

出力を (X, Y) とすると，

$$E_{K_2}(T^{(t)}) = (\alpha^D)^{-1} \otimes (M \oplus X) = (\alpha^D)^{-1} \otimes (C \oplus Y) \tag{60}$$

が成立し，これはさらに

$$(\alpha^D) \otimes E_{K_2}(T^{(t)}) = M \oplus X = C \oplus Y. \tag{61}$$

を意味する．よって

$$M \oplus C = X \oplus Y \tag{62}$$

である．従って式 (62) を満たす (M, C, X, Y) を求められれば，Dunkelman らの SEM への攻撃 [DKS12] により，マスクは $E_{K_2}(T^{(t)}) = (\alpha^D)^{-1} \otimes (C \oplus Y)$ として求まることを意味する．ブロック $D \in \mathcal{D}$ における $M \oplus C$ の候補は既知平文暗号化クエリにより得られる．X と Y の候補については，リファレンスセクタ内のブロック $(T^{(r)}, D)$ に対するクエリで得られる．具体的には（既知平文攻撃が適当に選択した X について）$\widetilde{M} = X \oplus E_{K_2}(T^{(r)}) \otimes \alpha^D$ をクエリすると，得られる暗号文は $\widetilde{C} = Y \oplus E_{K_2}(T^{(r)}) \otimes \alpha^D$ である．ターゲットセクタへのクエリ q_t 回，リファレンスセクタへのクエリ q_r 回のとき，$q_t \cdot q_r \geq 2^n$ ならば高い確率で式 (62) を満たす (M, C, X, Y) が得られ，ターゲットセクタのマスク $E_{K_2}(T^{(t)})$ が得られる．あとはリファレンスセクタへのクエリを用いることで，ターゲットセクタの平文が未知である $(T^{(t)}, D')$ で $D' \notin \mathcal{D}$ なるブロックの平文回復が可能となる．リファレンスセクタのマスク回復が済んでいるものとし，具体的な攻撃手続きは以下となる．

1. q_r ペアの (X, Y) をリファレンスセクタへの（既知平文ないし復号）クエリで得る．$(Y, X \oplus Y)$ をリスト $\mathcal{S}$ に保持する．
2. q_t 個の既知平文/暗号文対 (M, C) をブロック $(T^{(t)}, D)$ ただし $D \in \mathcal{D}$ から得る．(M, C) を得るごとにリスト $\mathcal{S}$ の右要素と $M \oplus C$ の一致をサーチし，もし一致した場合，リスト要素から (M, C, X, Y) を求める．
3. $(\alpha^D)^{-1} \otimes (C \oplus Y)$ を $E_{K_2}(T^{(t)})$ の候補として出力．
4. $(T^{(t)}, D')$, $D' \notin \mathcal{D}$ の暗号文 C' を，$E_{K_2}(T^{(t)})$ の候補を用いたリファレンスセクタへの復号クエリで復号する．

$q_t \cdot q_r \geq 2^n$ であれば，高い確率で正しい $E_{K_2}(T^{(t)})$ が求まるため，攻撃が成功する．

■計算量の見積もり　リファレンスセクタのマスクリカバリが済んでいるとすると，ターゲットセクタマスクリカバリまでの時間計算量はクエリ回数 $O(q_r + q_t)$ とリスト $\mathcal{S}$ のサーチの計算量であり，後者は 2 分探索を q_t 回行うことにより $O(q_t \log q_r)$ となるため，合計 $O(q_r + q_t \log q_r)$ となる．必要なメモリは $O(q_r)$ となる．ただし q_r と q_t の大小関係に応じてステップ 1 と 2 の順序を変えることで，メモリは $O(\min\{q_r, q_t\})$ とすることが可能である．

この攻撃により，例えば $(q_t, q_r) = (2^{48}, 2^{80})$ とすることで，ターゲットセクタへのクエリ回数は単体のバースデー攻撃を行うのに十分でなくとも，ターゲットセクタの平文を求めることが可能となる．

■複数ターゲットセクタでの攻撃　通常はターゲットセクタは複数あると考えられるが，この場合はステップ 1 は共用でき，リファレンスセクタへのクエリは増やさずに攻撃が可能である．

そのほか，詳細は割愛するが，どのブロックも完全には平文が既知ではない場合（例えばブロックごとに固有の $b < n$ ビットのみ既知）でも， 8.4 節の攻撃から攻撃計算量をわずかに増加させることで攻撃が可能である．さらに，平文情報がまったくなく暗号文のみが入手できる場合でも，2 ラウンド EM 暗号での攻撃 [DDKS16] で用いられた多重衝突を用いるテクニックにより，ランダム推測よりは推測成功確率をわずかながら上げることが可能である [IM].

9　XTS に関するそのほかの既存文献の調査

9.1　サイドチャネル攻撃

Luo et.al [LFD17] では，XTS-AES に対するサイドチャネル攻撃（特に相関電力攻撃（Correlation power analysis, CPA）が示されている．これはサイドチャネル情報を用いた暗号文のみ攻撃であり，平文および Tweak が未知である．マスク計算での乗算処理のサイドチャネルを用いてマスクの初期値（$E_{K_2}(T)$）を求め，これを使ったサイドチャネル攻撃で K_2 を求め，最後に K_1 を求めるものである．また Unterluggauer と Mangard [UM16] により，XEX と XTS について差分電力攻撃（Differential power analysis, DPA）と差分故障解析（Differential fault analysis, DFA）が示されている．

9.2 FDE の安全性評価

Khati et. al [KMV17] はフルディスク暗号化（Full Disk Encryption, FDE）の問題を包括的に捉えることを目的とした研究を行った．具体的には，フルディスク暗号化に適切と思われるいくつかの安全性の定義と，既存の暗号化モードを適用した場合のそれらの充足性を検討している．研究対象の暗号化モードは CBC のように IV 付きのものであればセクタ番号から適切な導出方法を用いたものとし，XTS のように Tweak 付きのモードであれば，XTS 同様にセクタ番号をそのまま Tweak とするとしている．

当該論文の評価では，セクタごとの TSPRP を一番強い安全性としており，これだけみれば CRYPTREC レポート [Rog11] と同様の指摘内容だが，本論文の評価項目はより詳細であり，また評価対象も広い．

10 結論

結論すると，XTS は，AES を含め安全な 128 ビットブロック暗号と組み合わせて使用する場合，安全であるといえる．ただし以下の項目に注意するべきである．

- XTS は認証の機能を持たないため，原理的には暗号文への改ざんを検知することは不可能である．改ざん検知を求める場合には，別途メッセージ認証コードなどを利用するか，認証暗号を用いる必要がある．この場合はタグを格納する場所が別途必要となる．
- XTS のメッセージ全体への処理は，Narrow-block encryption と呼ばれるものであり，保証する安全性に本質的な限界がある．tweak のバリエーションと実際の使い方，平文の分布，データユニット長などから，XTS の利用が適切かを考える．特に，データユニットのブロック長が 2^{20} 以下という，NIST が定めた条件が満たされていることを確認する．
- Ciphertext Stealing（CTS）の利用に関しては，パブリックコメントの評価と，従来研究での CBC での Ciphtertext Stealing の評価を総合すると，単一暗号文から平文が漏洩するといったようなリスクはなく最低限の安全性は確保されている．しかしながら，CTS を使わない場合に可能であった，Tweakable ブロック暗号をベースとしたモダンなストレージ暗号化の安全性モデルから逸脱するため，理論的安全性評価は困難と

考えられる．このため積極的に利用を推奨する根拠に乏しいと言わざるを得ない．

- XTS ではなく XEX を用いる場合，すなわち XTS が用いる二つのブロック暗号の鍵を単一の鍵とする場合には，XTS で許可されていた tweak $\overline{T} = (T, 0)$ は攻撃の危険性があるため，使用しないこと．
- サイドチャネル解析が現実的である環境の場合，何らかの実装手段により，サイドチャネル解析への対策を施すこと．

謝辞

8 章の内容は兵庫県立大学 五十部孝典准教授の協力のもと作成した．

参考文献

[BDJR97] Mihir Bellare, Anand Desai, E. Jokipii, and Phillip Rogaway. A Concrete Security Treatment of Symmetric Encryption. In *38th Annual Symposium on Foundations of Computer Science, FOCS '97, Miami Beach, Florida, USA, October 19-22, 1997*, pages 394–403. IEEE Computer Society, 1997.

[BK09] Alex Biryukov and Dmitry Khovratovich. Related-Key Cryptanalysis of the Full AES-192 and AES-256. In Mitsuru Matsui, editor, *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings*, volume 5912 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2009.

[BLNS18] Christina Boura, Virginie Lallemand, María Naya-Plasencia, and Valentin Suder. Making the Impossible Possible. *J. Cryptology*, 31(1):101–133, 2018.

[CS08] Debrup Chakraborty and Palash Sarkar. HCH: A New Tweakable Enciphering Scheme Using the Hash-Counter-Hash Approach. *IEEE Trans. Information Theory*, 54(4):1683–1699, 2008.

[DDKS16] Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. Key Recovery Attacks on Iterated Even-Mansour Encryption Schemes. *J. Cryptology*, 29(4):697–728, 2016.

[DFJ13] Patrick Derbez, Pierre-Alain Fouque, and Jérémy Jean. Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*, pages 371–387. Springer, 2013.

[DKS12] Orr Dunkelman, Nathan Keller, and Adi Shamir. Minimalism in Cryptography: The Even-Mansour Scheme Revisited. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, volume 7237 of *Lecture Notes in Computer Science*, pages 336–354. Springer, 2012.

[Dwo10] Morris Dworkin. Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices. Standard, National Institute of Standards and Technology., 2010.

[ED08] Mohamed Abo El-Fotouh and Klaus Diepold. A New Narrow Block Mode of Operations for Disk Encryption. In Massimiliano Rak, Ajith Abraham, and Valentina Casola, editors, *Proccedings of the Fourth International Conference on Information Assurance and Security, IAS 2008, September 8-10, 2008, Napoli, Italy*, pages 126–131. IEEE Computer Society, 2008.

[FJP04] Pierre-Alain Fouque, Antoine Joux, and Guillaume Poupard. Blockwise Adversarial Model for On-line Ciphers and Symmetric Encryption Schemes. In Helena Handschuh and M. Anwar Hasan, editors, *Selected Areas in Cryptography, 11th Interna-*

tional Workshop, SAC 2004, Waterloo, Canada, August 9-10, 2004, Revised Selected Papers, volume 3357 of *Lecture Notes in Computer Science*, pages 212–226. Springer, 2004.

[FMP03] Pierre-Alain Fouque, Gwenaëlle Martinet, and Guillaume Poupard. Practical Symmetric On-Line Encryption. In Thomas Johansson, editor, *Fast Software Encryption, 10th International Workshop, FSE 2003, Lund, Sweden, February 24-26, 2003, Revised Papers*, volume 2887 of *Lecture Notes in Computer Science*, pages 362–375. Springer, 2003.

[GH09] Rosario Gennaro and Shai Halevi. More on Key Wrapping. In Michael J. Jacobson Jr., Vincent Rijmen, and Reihaneh Safavi-Naini, editors, *Selected Areas in Cryptography, 16th Annual International Workshop, SAC 2009, Calgary, Alberta, Canada, August 13-14, 2009, Revised Selected Papers*, volume 5867 of *Lecture Notes in Computer Science*, pages 53–70. Springer, 2009.

[HR03] Shai Halevi and Phillip Rogaway. A Tweakable Enciphering Mode. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 482–499. Springer, 2003.

[HR04] Shai Halevi and Phillip Rogaway. A Parallelizable Enciphering Mode. In Tatsuaki Okamoto, editor, *Topics in Cryptology - CT-RSA 2004, The Cryptographers' Track at the RSA Conference 2004, San Francisco, CA, USA, February 23-27, 2004, Proceedings*, volume 2964 of *Lecture Notes in Computer Science*, pages 292–304. Springer, 2004.

[IEE] Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices. Standard, IEEE Security in Storage Working Group.

[IM] Takanori Isobe and Kazuhiko Minematsu. Plaintext Recovery Attacks on XTS. *in preparation.*

[IM18] Akiko Inoue and Kazuhiko Minematsu. Cryptanalysis of OCB2.

IACR Cryptology ePrint Archive, 2018:1040, 2018.

[Iwa18] Tetsu Iwata. Plaintext recovery attack of OCB2. *IACR Cryptology ePrint Archive*, 2018:1090, 2018.

[KMV17] Louiza Khati, Nicky Mouha, and Damien Vergnaud. Full Disk Encryption: Bridging Theory and Practice. In Helena Handschuh, editor, *Topics in Cryptology - CT-RSA 2017 - The Cryptographers' Track at the RSA Conference 2017, San Francisco, CA, USA, February 14-17, 2017, Proceedings*, volume 10159 of *Lecture Notes in Computer Science*, pages 241–257. Springer, 2017.

[LFD17] Chao Luo, Yunsi Fei, and A. Adam Ding. Side-channel power analysis of XTS-AES. In David Atienza and Giorgio Di Natale, editors, *Design, Automation & Test in Europe Conference & Exhibition, DATE 2017, Lausanne, Switzerland, March 27-31, 2017*, pages 1330–1335. IEEE, 2017.

[LM06] Moses Liskov and Kazuhiko Minematsu. Comments on XTS-AES. Technical report, 2006.

[LRW02] Moses Liskov, Ronald L. Rivest, and David A. Wagner. Tweakable Block Ciphers. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*, volume 2442 of *Lecture Notes in Computer Science*, pages 31–46. Springer, 2002.

[LS13] Rodolphe Lampe and Yannick Seurin. Tweakable Blockciphers with Asymptotically Optimal Security. In Shiho Moriai, editor, *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, volume 8424 of *Lecture Notes in Computer Science*, pages 133–151. Springer, 2013.

[LST12] Will Landecker, Thomas Shrimpton, and R. Seth Terashima. Tweakable Blockciphers with Beyond Birthday-Bound Security. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Confer-*

ence, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings, volume 7417 of *Lecture Notes in Computer Science*, pages 14–30. Springer, 2012.

[Mau02] Ueli M. Maurer. Indistinguishability of Random Systems. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*, pages 110–132. Springer, 2002.

[Min06] Kazuhiko Minematsu. Improved Security Analysis of XEX and LRW Modes. In Eli Biham and Amr M. Youssef, editors, *Selected Areas in Cryptography, 13th International Workshop, SAC 2006, Montreal, Canada, August 17-18, 2006 Revised Selected Papers*, volume 4356 of *Lecture Notes in Computer Science*, pages 96–113. Springer, 2006.

[MM07] Kazuhiko Minematsu and Toshiyasu Matsushima. Tweakable Enciphering Schemes from Hash-Sum-Expansion. In K. Srinathan, C. Pandu Rangan, and Moti Yung, editors, *Progress in Cryptology - INDOCRYPT 2007, 8th International Conference on Cryptology in India, Chennai, India, December 9-13, 2007, Proceedings*, volume 4859 of *Lecture Notes in Computer Science*, pages 252–267. Springer, 2007.

[MM09] Kazuhiko Minematsu and Toshiyasu Matsushima. Generalization and Extension of XEX* Mode. *IEICE Transactions*, 92-A(2):517–524, 2009.

[Nan14] Mridul Nandi. XLS is Not a Strong Pseudorandom Permutation. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I*, volume 8873 of *Lecture Notes in Computer Science*, pages 478–490. Springer, 2014.

[NR97] Moni Naor and Omer Reingold. On the Construction of Pseudo-Random Permutations: Luby-Rackoff Revisited (Extended Abstract). In Frank Thomson Leighton and Peter W. Shor, editors, *Proceedings of the Twenty-Ninth Annual ACM Symposium on the Theory of Computing, El Paso, Texas, USA, May 4-6, 1997*, pages 189–199. ACM, 1997.

[Pat08] Jacques Patarin. The "Coefficients H" Technique. In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *Selected Areas in Cryptography, 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, Revised Selected Papers*, volume 5381 of *Lecture Notes in Computer Science*, pages 328–345. Springer, 2008.

[Poe18] Bertram Poettering. Breaking the confidentiality of OCB2. *IACR Cryptology ePrint Archive*, 2018:1087, 2018.

[Rog04] Phillip Rogaway. Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In Pil Joong Lee, editor, *Advances in Cryptology - ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings*, volume 3329 of *Lecture Notes in Computer Science*, pages 16–31. Springer, 2004.

[Rog11] Philip Rogaway. Evaluation of Some Blockcipher Modes of Operation. *CRYPTREC Report*, 2011.

[RR07] Thomas Ristenpart and Phillip Rogaway. How to Enrich the Message Space of a Cipher. In Alex Biryukov, editor, *Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers*, volume 4593 of *Lecture Notes in Computer Science*, pages 101–118. Springer, 2007.

[RWZ12] Phillip Rogaway, Mark Wooding, and Haibin Zhang. The Security of Ciphertext Stealing. In Anne Canteaut, editor, *Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Pa-*

pers, volume 7549 of *Lecture Notes in Computer Science*, pages 180–195. Springer, 2012.

[UM16] Thomas Unterluggauer and Stefan Mangard. Exploiting the Physical Disparity: Side-Channel Attacks on Memory Encryption. In François-Xavier Standaert and Elisabeth Oswald, editors, *Constructive Side-Channel Analysis and Secure Design - 7th International Workshop, COSADE 2016, Graz, Austria, April 14-15, 2016, Revised Selected Papers*, volume 9689 of *Lecture Notes in Computer Science*, pages 3–18. Springer, 2016.

[WFW05] Peng Wang, Dengguo Feng, and Wenling Wu. HCTR: A Variable-Input-Length Enciphering Mode. In Dengguo Feng, Dongdai Lin, and Moti Yung, editors, *Information Security and Cryptology, First SKLOIS Conference, CISC 2005, Beijing, China, December 15-17, 2005, Proceedings*, volume 3822 of *Lecture Notes in Computer Science*, pages 175–188. Springer, 2005.

[Zha12] Haibin Zhang. Length-Doubling Ciphers and Tweakable Ciphers. In Feng Bao, Pierangela Samarati, and Jianying Zhou, editors, *Applied Cryptography and Network Security - 10th International Conference, ACNS 2012, Singapore, June 26-29, 2012. Proceedings*, volume 7341 of *Lecture Notes in Computer Science*, pages 100–116. Springer, 2012.

[Sak09] 坂田 真美 and 岩田 哲. CBC モード，Schneier モード，CTS モード，CTSp モードの安全性解析. **暗号と情報セキュリティシンポジウム** *SCIS 2009*, 2009.

[Omo08] 面 和成. セキュア VM を支える暗号技術. **第** *2* **回セキュア** *VM* **シンポジウム ～仮想化とセキュリティ～**, 2008.

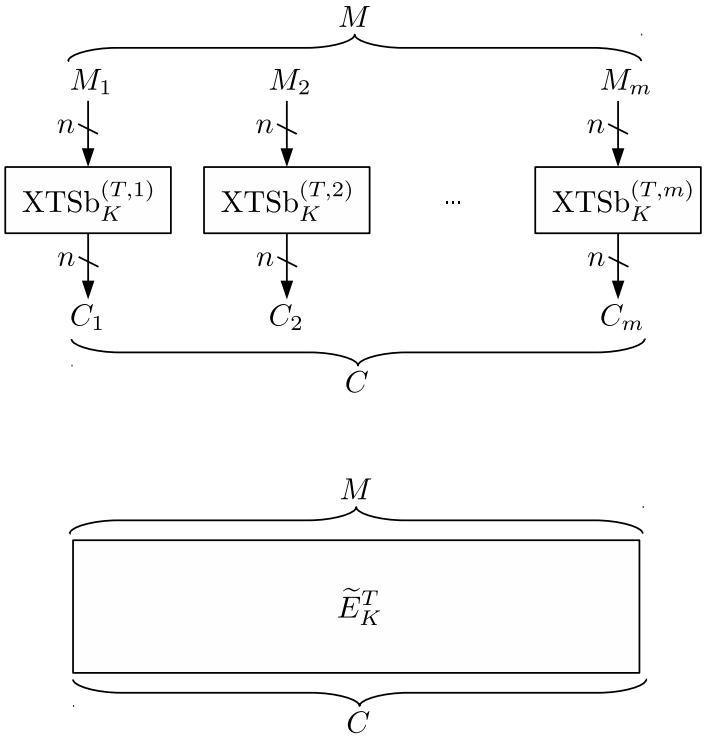

図 8　XTS による弱いブロック暗号化（上）と強いブロック暗号化（下）

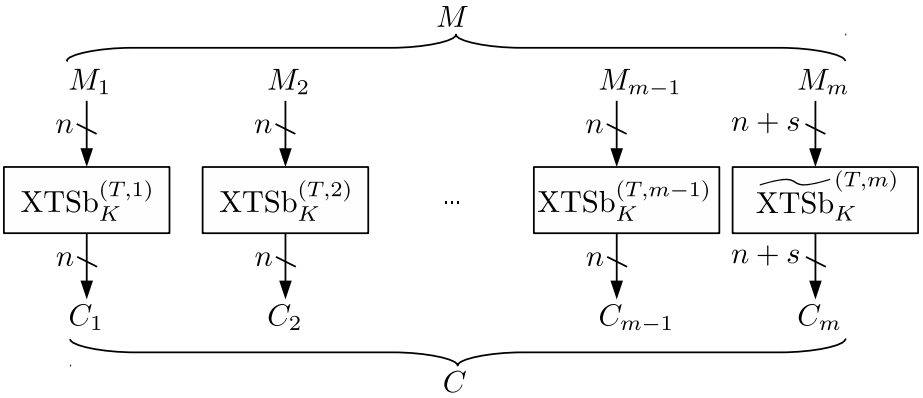

図 9　データ長が n の倍数でない場合の弱いブロック暗号化（NBE）

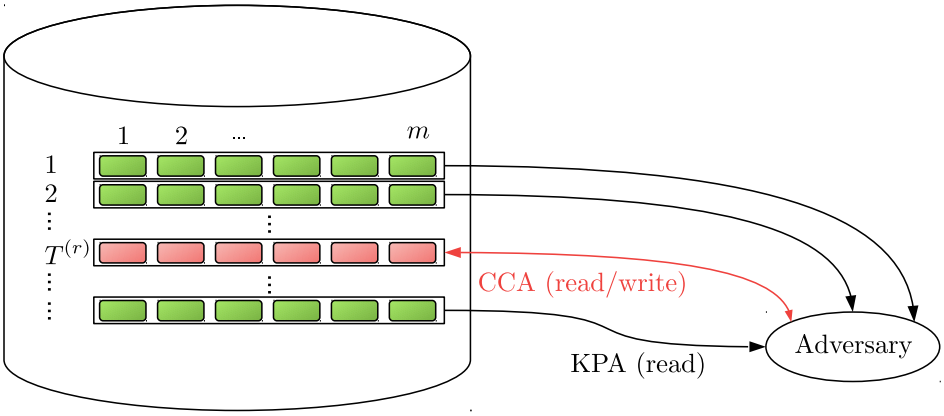

図 10　バースデー攻撃を用いた平文回復攻撃モデル

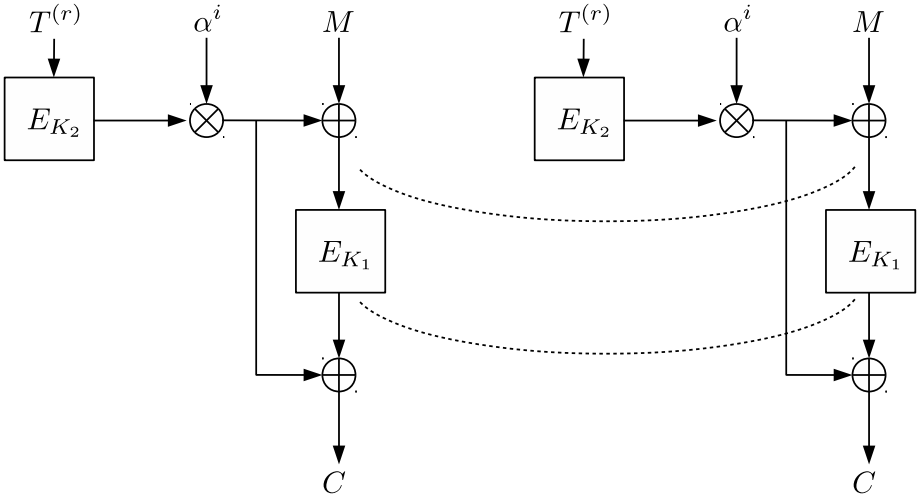

図 11　リファレンスセクタでのマスクリカバリ

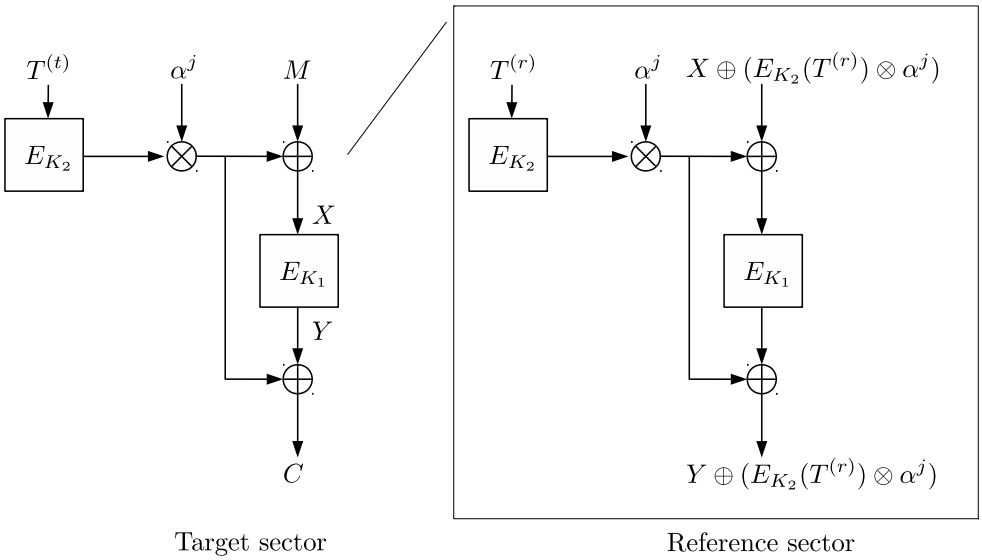

図 12　既知平文攻撃による平文回復