Evaluating the indistinguishability of the XTS mode in the proposed security model

Nguyen Tuan Anh*, Nguyen Bui Cuong**

*tuananhnghixuan@gmail.com, **nguyenbuicuong@gmail.com

Abstract: In this paper, we consider the indistinguishability of XTS in some security models for both full final block and partial final block cases. Firstly, some evaluations of the indistinguishability up-to-block are presented. Then, we present a new security model in which the adversary can not control sector number, based on an ϵ-collision resistant function. In this model, we give a bound of the distinguishing advantage that the adversary can get when attacks on XTS. The received results is an extension of [6].

Keywords: block cipher, XTS, indistinguishability, ciphertext stealing.

1 Introduction

Encryption on a storage device has characteristics that some common block cipher mode of operations such as CBC, CFB, CTR... are not suitable. Thus, Liskov, Rivest and Wagner proposed the tweakalbe block cipher notion in 2002 (see [7]). Then, many structures of tweakable block cipher were proposed such as LRW, XEX, XEX2... The XTS mode (XEX-based tweaked-codebook mode with ciphertext stealing; XEX is acronymed of XOR-Encryption-XOR) is recommended to use for encrypting data on storage devices by IEEE P1619 Standard and NIST SP 800-38E Recommendation (see [4, 5]). The security in the design of encryption schemes is often considered based on the indistinguishability in some specific models such as real or random indistinguishability, left or right indistinguishability [2].... Evaluating the indistinguishability for XTS have been attracting research attention in the cryptography community [1, 6, 9].

Related worked. In [6], the authors considered the indistinguishability up-to-block, the indistinguishability up-to-prefix, the indistinguishability up-to-repetition of some mode of operations when they are used on a storage device. However, the ciphertext stealing was not considered in that paper. Moreover, in order to avoid the restriction of XTS that encrypts the same plaintext twice in the same sector will always result in an identical ciphertext, Louiza Khati et al. presented the ideal that associates a diversifier to every sector by using SSD (solid state drive) in [6]. Then the combination of the sector number i and the diversifier is used instead of the sector number in XTS construction. This ideal makes that encrypting the same plaintext will result different ciphertexts in the same sector. In other words, this diversifier allows us to encrypt the same plaintext in distinct ways for the same sector number. However, the authors assert that the diversifier must be a rather short value, typically only a few bits [6]. We suppose that this recommendation makes the diversifier easy to repeat so XTS still has the restriction.

Our contributions. In this paper, firstly, we consider the security of XTS with the indistinguisability up-to-block [6] in the case using ciphertext stealing. Then, we generalize the ideal that associates a random variable to every sector in [6] by using an ϵ-collision resistant function. Moreover, we evaluate the distinguished advantage of the adversary that attacks on XTS in two above models.

Outline. This paper is organized as follows. In Section 2, we represent some related notions. In Section 3, we evaluate the indistinguishability up-to-block of the XTS mode. In Section 4, we evaluate the indistinguishability of the XTS mode in the proposed security model. Finally, some conclusions are given.

2 Preliminaries

In 2002, the definition of tweakable block cipher was proposed by Liskov, Rivest and Wagner [7] has the signature: $\tilde{E} : \{0,1\}^k \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$. A tweakable block cipher has the new input, which is called tweak, beside a key and a plaintext. Thus, a tweakalbe block cipher takes three inputs: a key $K \in \{0,1\}^k$, a tweak $T \in \mathcal{T}$, and a plaintext $M \in \{0,1\}^n$ to produce as ouput a ciphertext $C \in \{0,1\}^n$.

Firstly, we consider the security of a tweakalbe block cipher under chosen plaintext attack (abbreviate as tcpa). Let $\tilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ be a fix tweakalbe block cipher. Consider an adversary that has access to an oracle which is a function $g : \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ is determined by one of the following two cases:

World 0: A tweakable random permutation $\tilde{\Pi}(\cdot,\cdot)$ where $\tilde{\Pi}$ is a family of independent random permutation parameterized by T which denotes $\tilde{\Pi}(T,\cdot)$.

World 1: A function is chosen randomly from the family functions $\tilde{E}$ that means a key $K \xleftarrow{\$} \mathcal{K}$ and takes $g(\cdot,\cdot) \leftarrow \tilde{E}_K(\cdot,\cdot)$.

Definition 1 *(see [8]) Let $\tilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ be a tweakable block cipher and A be a probabilistic polynomial-time algorithm takes an oracle for a function $g : \mathcal{T} \times \mathcal{X} \to \mathcal{X}$,and returns a bit. We consider two experiments:*

Experiment$\boldsymbol{Exp}_{\tilde{E}}^{tcpa\text{-}1}(A)$	*Experiment*$\boldsymbol{Exp}_{\tilde{E}}^{tcpa\text{-}0}(A)$
$K \xleftarrow{\$} \mathcal{K}$	$\tilde{\Pi}$ *is a tweakable random permutation*
$b \leftarrow A^{\tilde{E}_K(\cdot,\cdot)}$	$b \leftarrow A^{\tilde{\Pi}(\cdot,\cdot)}$
Return b	*Return b*

The tcpa advantage of A is defined as

$$Adv_{\tilde{E}}^{tcpa}(A) = |Pr[Exp_{\tilde{E}}^{tcpa\text{-}1}(A) = 1] - Pr[Exp_{\tilde{E}}^{tcpa\text{-}0}(A) = 1]|.$$

Then, the tcpa advantage function in the attack on $\tilde{E}$ is defined as

$$Adv_{\tilde{E}}^{tcpa}(t,q) = \max_{A \in \mathcal{A}(t,q)} Adv_{\tilde{E}}^{tcpa}(A),$$

where $\mathcal{A}(t, q)$ is the set of all adversary making at most q oracle queries and running in time at most t.

In order to prove security models, we define a tweakable block cipher $\tilde{E}$ is (t, q, ϵ)-tcpa security if $\mathrm{Adv}^{\mathrm{tcpa}}_{\tilde{E}}(t, q) \leq \epsilon$.

Next, we consider the security of a tweakalbe block cipher under chosen ciphertext attack (abbreviate as tcca). Let $\tilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ be a fix tweakalbe block cipher. Consider an adversary that has access to an oracle which is a function $g : \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ and its inverse is determined by one of the following two cases:

World 0: A tweakable random permutation $\tilde{\Pi}(\cdot, \cdot)$ and $\tilde{\Pi}^{-1}(\cdot, \cdot)$ where $\tilde{\Pi}$ is a family of independent random permutation parameterized by T which denotes $\tilde{\Pi}(T, \cdot)$.

World 1: A function is chosen randomly from the family functions $\tilde{E}$ and the corresponding decryption function, that means a key $K \xleftarrow{\$} \mathcal{K}$ and takes $g(\cdot, \cdot) \leftarrow \tilde{E}_K(\cdot, \cdot), g(\cdot, \cdot)^{-1} \leftarrow \tilde{D}_K^{-1}(\cdot, \cdot)$.

Definition 2 *(see [8]) Let $\tilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ be a tweakable block cipher and A be a probabilistic polynomial-time algorithm takes an oracle for a function $g : \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ and its inverse,and returns a bit. We consider two experiments:*

$Experiment\boldsymbol{Exp}^{tcca\text{-}1}_{\tilde{E}}(A)$	$Experiment\boldsymbol{Exp}^{tcca\text{-}0}_{\tilde{E}}(A)$
$K \xleftarrow{\$} \mathcal{K}$	$\tilde{\Pi}$ *is a tweakable random permutation*
$b \leftarrow A^{\tilde{E}_K(\cdot,\cdot),\tilde{D}_K(\cdot,\cdot)}$	$b \leftarrow A^{\tilde{\Pi}(\cdot,\cdot),\tilde{\Pi}^{-1}(\cdot,\cdot)}$
Return b	*Return b*

The tcca advantage of A is defined as

$$Adv^{tcca}_{\tilde{E}}(A) = |Pr[Exp^{tcca\text{-}1}_{\tilde{E}}(A) = 1] - Pr[Exp^{tcca\text{-}0}_{\tilde{E}}(A) = 1]|.$$

Then, the tcca advantage function in the attack on $\tilde{E}$ is defined as

$$Adv^{tcca}_{\tilde{E}}(t, q) = \max_{A \in \mathcal{A}(t,q)} Adv^{tcca}_{\tilde{E}}(A),$$

where $\mathcal{A}(t, q)$ is the set of all adversary making at most q oracle queries and running in time at most t.

Simillar to Definition 1, we define a tweakable block cipher $\tilde{E}$ is (t, q, ϵ)-tcca security if $\mathrm{Adv}^{\mathrm{tcca}}_{\tilde{E}}(t, q) \leq \epsilon$.

The XEX2-AES block cipher is used in NIST SP 300-38E Recommendation [4] has LRW construction [2] where the underlying block cipher is AES. In this paper, we describe the general definition for the XEX2 block cipher with an arbitrary underlying block cipher E.

Definition 3 *Let E be an arbitrary block cipher: $\mathcal{K} \times \{0, 1\}^n \to \{0, 1\}^n$. The XEX2 tweakable block cipher: $\{0, 1\}^k \times \{0, 1\}^n \times [0..2^n - 2] \times \{0, 1\}^n \to \{0, 1\}^n$ is defined as*

$$XEX2^{i,j}_K(M) = E_{K_1}(M \oplus E_{K_2}(i) \cdot \alpha^j) \oplus E_{K_2}(i) \cdot \alpha^j,$$

where $K = K_1||K_2 \in \{0, 1\}^k$ ($K_i \in \mathcal{K}$ for $i = 1, 2; k = 2|K_1|$), $(i, j) \in \{0, 1\}^n \times [0..2^n - 2]$, α be a primitive element of $GF(2^n)$, and the operator $\cdot$ is the multiplication in $GF(2^n)$.

The security of XEX2 under chosen ciphertext attack is obtained from the fact that it has LRW construction.

Proposition 1 *(see [9]) Let $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a security block cipher under ciphertext attack. Then, the XEX2 tweakable block cipher is security under ciphertext attack. Moreover,*

$$Adv^{tcca}_{XEX2}(t', q) \leq 2Adv^{prp\text{-}cca}_{E}(t, q) + 3q^2/(2^n - 1),$$

where $t' = t + \mathcal{O}(q), Adv^{prp\text{-}cca}_{E}(t, q)$ is the advantage function under chosen ciphertext attack which distinguishes the block cipher E from a random permutation (see Def 4.8 [3]).

The XTS mode can be regarded as an ECB-like mode over XEX2, but something special-ciphertext stealing is employed for any fractional final block and its predecessor. In [4, 5], XTS is described for the underlying block cipher which is AES with the block length $n = 128$ bit. In this paper, we use the previous general definition of XEX2 to propose a general model for the XTS mode for an arbitrary underlying block cipher.

Definition 4 *Let $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be an arbitrary block cipher. The XTS mode constructs a function*

$$XTS^i_K : \mathcal{K}^2 \times \mathcal{T} \times \{0,1\}^N \to \{0,1\}^N,$$

where $i \in \mathcal{T} = \{0,1\}^n, K = K_1||K_2 \in \mathcal{K}^2, n \leq N \leq n \cdot (2^n - 1)$.
With inputs are a key $K \in \mathcal{K}^2$, a tweakable $i \in \mathcal{T}$ and a plaintext $P \in \{0,1\}^N$, the XTS mode operates as the following algorithm:

```
**Algorithm**$XTS^i_k(P)$
$K \in \mathcal{K}^2, i \in \{0,1\}^n, P \in \{0,1\}^N$
$P_0 P_1 \cdot P_m \leftarrow P$ where $m = \lceil |P|/n \rceil - 1$ and $|P_j| = n$ with $0 \leq j < m, 1 \leq |P_m| \leq n$
$b \leftarrow |P_m|$
For $j \leftarrow 0$ to $m - 1$ do $C_j \leftarrow XEX2^{i,j}_K(P_j)$
If $b = n$ then
    $C_m \leftarrow XEX2^{i,m}_K(P_m)$
else
    $C_m||D \leftarrow C_{m-1}$ where $|C_m| = b$
    $C_{m-1} \leftarrow XEX2^{i,m}_K(P_m||D)$
Endif
Return $C_0 \cdots C_m$
```

3 The indistinguishability up-to-block of XTS

The XTS mode is not security tweakable block cipher under chosen plaintext attack: encrypting the same plaintext twice in the same sector will always result in an identical ciphertext. Thus, the XTS mode was considered in some more restrictive model [6]. In this part, we evaluate

XTS with the indistinguishability up-to-block. This security notion is described in [6], however, ciphertext stealing is not considered. Moreover, the authors asserted (not proved) that: XTS is indistinguishable up-to-block. In order to evaluate for two cases, we represent the indistinguishability up-to-block under chosen plaintext attack and chosen ciphertext attack. Note that the adversary has the privilege choosing the sector which he wants to write plaintext.
Firstly, we consider the indistinguishability up-to-block under chosen plaintext attack (abbreviate as ub-cpa). The adversary is allowed to query a plaintext P and a tweak i. The authors [6] presented this definition base on game models, however it has not the distinguishing advantage. In this paper, we represent in detail the definition of indistinguishability up-to-block based on oracle model, we also give the advantage function of the adversary. Now, we describe two oracles which the adversary must distinguish.

World 1. Firstly, a key $K \xleftarrow{\$} \mathcal{K}$ is chosen randomly. Then, the oracle operates as follows. The oracle takes two inputs-a tweak $i \in \{0,1\}^n$ and a plaintext $P \in \mathcal{X}$ and produces as output a ciphert $C \leftarrow \mathrm{XTS}_K^i(P)$ for the adversary. We denote the oracle by $\mathrm{XTS}_K(\cdot)$.

World 0. The oracle takes two inputs: a plaintext $P \in \mathcal{X}$ and a tweak $i \in \{0,1\}^n$. Then, the oracle chooses randomly a permutation $\Pi^{i,j}(\cdot) \in \mathrm{Perm}(n)$ for every pair (i,j) where $0 \leq j \leq m$ (note that this permutations are saved in the query process). When N is a multiple of n, the oracle encrypts $C_j \leftarrow \Pi^{i,j}(P_j)$ where $0 \leq j \leq m$. When N is not a multiple of n or $N = b(\mathrm{mod} n)$. If $0 \leq j \leq m-1$, the oracle encrypts $C_j \leftarrow \Pi^{i,j}(P_j)$, then put $C_m||D \leftarrow C_{m-1}$ with $|C_m| = b$ and then encrypts $C_{m-1} \leftarrow \Pi^{i,j}(P_m||D)$. The oracle outputs $C = C_0|| \cdots ||C_m$. We denote the oracle by $\{\Pi(\cdot)\}$.

Definition 5 *Let the XTS mode is determined by Definition 4 and A is an adversary that has access to an oracle. We consider the two following experiments:*

Experiment$\boldsymbol{Exp}^{\textit{ub-cpa-1}}_{XTS}(A)$	*Experiment*$\boldsymbol{Exp}^{\textit{ub-cpa-0}}_{XTS}(A)$
$K \xleftarrow{\$} \mathcal{K}$	
$d \leftarrow A^{XTS_K(\cdot)}$	$d \leftarrow A^{\{\Pi(\cdot)\}}$
Return d	*Return d*

The ub-cpa advantage of A is defined as

$$Adv^{\textit{ub-cpa}}_{XTS}(A) = |Pr[Exp^{\textit{ub-cpa-1}}_{XTS}(A) = 1] - Pr[Exp^{\textit{ub-cpa-0}}_{XTS}(A) = 1]|.$$

Then, ub-cpa advantage function in the attack on XTS is defined as

$$Adv^{\textit{ub-cpa}}_{XTS}(t,q,\sigma) = \max_{A \in \mathcal{A}(t,q,\sigma)} Adv^{\textit{ub-cpa}}_{XTS}(A),$$

where $\mathcal{A}(t,q,\sigma)$ is the set of all adversary making at most q oracle queries with the total number of blocks at most σ, running in time at most t. We define a tweakable block cipher $\tilde{E}$ is (t,q,σ,ϵ)-ub-cpa security if $Adv^{\textit{ub-cpa}}_{XTS}(t,q,\sigma) \leq \epsilon$.

Next, we consider the indistinguishability up-to-block under chosen ciphertext attack (abbreviate as ub-cca). The adversary is allowed to query a plaintext P and a tweak i or query a ciphertext C and a tweak i. We describe two oracles which the adversary must distinguish similarly to the chosen plaintext attack.

World 0. Firstly, a key $K \xleftarrow{\$} \mathcal{K}$ is chosen randomly. Then, the oracle operates as follows. The oracle takes two inputs-a tweak $i \in \{0,1\}^n$ and a plaintext $P \in \mathcal{X}$ and produces as output a ciphertext $C \leftarrow \mathrm{XTS}^i_K(P)$ for the adversary. The oracle takes two inputs tweak $i \in \{0,1\}^n$ and a plaintext $C \in \mathcal{X}$ and produces as output a ciphertext $P \leftarrow \mathrm{D}^i_K(P)$ for the adversary. We denote the oracle by $\mathrm{XTS}_K(\cdot), \mathrm{XTS}^{-1}_K(\cdot)$.

World 1. If inputs are a tweak i and a plaintext P the oracle operates as the cpa case (note that permutations $\Pi^{i,j}$ is saved). If inputs are a tweak $i \in \{0,1\}^n$ and a ciphertext $C \in \mathcal{X}$ the oracle operates as follows. When N is a multiple of n, the oracle decrypts $P_j \leftarrow (\Pi^{i,j})^{-1}(C_j)$ where $0 \leq j \leq m$. When N is not a multiple of n or $N = b(\mathrm{mod} n)$, the oracle decrypts $P_j \leftarrow (\Pi^{i,j})^{-1}(C_j)$ where $0 \leq j \leq m-2$, then it decrypts $P_m||D \leftarrow (\Pi^{i,m})^{-1}(C_{m-1})$ with $|P_m| = b, P_{m-1} \leftarrow (\Pi^{i,m-1})^{-1}(C_m||D)$. The oracle returns $P = P_0||\cdots||P_m$. We denote the oracle by $\{\Pi(\cdot)\}, \{\Pi^{-1}(\cdot)\}$.

Definition 6 *Let the XTS mode is determined by Definition 4 and A is an adversary that has access to the oracle. We consider the two following experiments:*

$Experiment\boldsymbol{Exp}^{\textit{ub-cca-1}}_{XTS}(A)$	$Experiment\boldsymbol{Exp}^{\textit{ub-cca-0}}_{XTS}(A)$
$K \xleftarrow{\$} \mathcal{K}$	
$d \leftarrow A^{XTS_K(\cdot),XTS^{-1}_K(\cdot)}$	$d \leftarrow A^{\{\Pi(\cdot)\},\{\Pi^{-1}(\cdot)\}}$
Return d	*Return d*

The ub-cca advantage of A is defined as

$$Adv^{\textit{ub-cca}}_{XTS}(A) = |Pr[Exp^{\textit{ub-cca-1}}_{XTS}(A) = 1] - Pr[Exp^{\textit{ub-cca-0}}_{XTS}(A) = 1]|.$$

Then, ub-cca advantage function in the attack on XTS is defined as

$$Adv^{\textit{ub-cca}}_{XTS}(t,q,\sigma) = \max_{A \in \mathcal{A}(t,q,\sigma)} Adv^{\textit{ub-cca}}_{XTS}(A),$$

where $\mathcal{A}(t,q,\sigma)$ is the set of all adversary making at most q oracle queries with the total number of blocks at most σ, running in time at most t. We define a tweakable block cipher $\tilde{E}$ is (t,q,σ,ϵ)-ub-cca security if $Adv^{\textit{ub-cca}}_{XTS}(t,q,\sigma) \leq \epsilon$.

Now, we present and prove Proposition 2 which states that XTS is ub-cca security.

Proposition 2 *Let $E : \{0,1\}^n \times \mathcal{K} \to \{0,1\}^n$ be a family of functions and XTS is determined by Definition 4 using E as an underlying block cipher. We have:*

$$Adv^{\textit{ub-cca}}_{XTS}(t',q,\sigma) \leq Adv^{\textit{prp-cca}}_{E}(t,q) + 3q^2/(2^n-1),$$

where t' is a polynomial of t.

Proof. We only need prove for the case that uses ciphertext stealing. Using Proposition 1 we have

$$\mathrm{Adv}^{\mathrm{tcca}}_{\mathrm{XEX2}}(t'',q) \leq \mathrm{Adv}^{\mathrm{prp\text{-}cca}}_{E}(t,q) + 3q^2/(2^n-1).$$

We will prove that if there is an ub-cca adversary A on XTS, there will be exist a tcca adversary B on XEX2 such that

$$\mathrm{Adv}_{\mathrm{XTS}}^{\text{ub-cca}}(A) \leq \mathrm{Adv}_{\mathrm{XEX2}}^{\mathrm{tcca}}(B)$$

For every ub-cca adversary A on XTS, we will construct a tcca adversary B on XEX2. If A queries a tweak i and a plaintext P, B separates $P = P_0||\cdots||P_m$ where $|P_0| = \cdots = |P_{m-1}| = n$ and $|P_m| = b < n$. The adversary B queries consecutively (P_j, i, j) where $j = 0, \cdots, m-1$ to the oracle of XEX2 and receives $C_0, \cdots, C_{m-1}$. The adversary B put $C_m||D \leftarrow C_{m-1}$ and queries $(P_m||D, i, m)$ to the oracle of XEX2, it receives C'_{m-1}. B returns $C = C_0||\cdots||C_{m-2}||C'_{m-1}||C_m$. If A queries a tweak i and ciphertext C, B separates $C = C_0||\cdots||C_m$ where $|C_0| = \cdots = |C_{m-1}| = n$ and $|C_m| = b < n$. The adversary B queries consecutively (C_{m-1}, i, m) where $j = 0, \cdots, m-2$ and receives $P_0, \cdots, P_{m-2}$. B queries $C_{m-1}, i, m)$ and receives $P_m||D$. Then B queries $(C_m||D, i, m-1)$ and receives P_{m-1}. B returns $P = P_0||\cdots||P_m$. If the adversary A returns a bit d after querying q times, the adversary B returns d.

If B is used the oracle $\mathcal{O} = \mathrm{XEX2}_K$, the view that A runs as a subroutine of B same the view that A runs independently attacks on XTS. Thus, we have:

$$\Pr[\mathrm{Exp}_{\mathrm{XTS}}^{\text{ub-cca-1}}(A) = 1] = \Pr[\mathrm{Exp}_{\mathrm{XEX2}}^{\text{tcca-1}}(B) = 1].$$

B is used the oracle $\mathcal{O} = \tilde{\Pi}(\cdot, \cdot)$. Because of our construction so the probability that B returns 1 is the probability that A returns 1 in that case, we denote $A^{\tilde{\Pi}(\cdot,\cdot)}$. This means that:

$$\Pr[A^{\tilde{\Pi}(\cdot,\cdot)} = 1] = \Pr[\mathrm{Exp}_{\mathrm{XEX2}}^{\text{tcca-0}}(B) = 1].$$

Now, we consider the view that A runs independently attacks on XTS and the view that A runs as a subroutine of B. Then, we present the relationship between two probabilities $\Pr[\mathrm{Exp}_{\mathrm{XTS}}^{\text{ub-cca-0}}(A) = 1]$ and $\Pr[A^{\tilde{\Pi}(\cdot,\cdot)} = 1]$. In the first case, A receives answers from the permutations $\Pi^{i,j}$ or $(\Pi^{i,j})^{-1}$. In the second case, A receives answers from the tweakable random permutations $\tilde{\Pi}(\cdot, \cdot)$ or $\tilde{\Pi}^{-1}(\cdot, \cdot)$. Note that in the construction of $\Pi^{i,j}$ or $(\Pi^{i,j})^{-1}$, values are chosen randomly. Thus, we can state that the view that B creates for A same as the view that A runs independently attacks on XTS. We have

$$\Pr[\mathrm{Exp}_{\mathrm{XTS}}^{\text{ub-cca-0}}(A) = 1] = \Pr[\mathrm{Exp}_{\mathrm{XEX2}}^{\text{tcca-0}}(B) = 1].$$

From above arguments we have

$$\mathrm{Adv}_{\mathrm{XEX2}}^{\mathrm{tcca}}(B) = \mathrm{Adv}_{\mathrm{XTS}}^{\text{ub-cca}}(A).$$

We get the proof for Proposition 2. □

4 The indistinguishability in the proposed security model

4.1 Our security model

Typically, the XTS mode encrypts the same plaintext twice in the same sector number will produce an identical ciphertext. The authors of [6] presented the ideal that transforms the sector number to a random value. This allows us to encrypt the same plaintext in distinct ways for the same sector number. In this paper, we generalize the above ideal and present the detail distinguishing advantage. Instead of using the sector number i, we use a function $\psi : \{0,1\}^s \times \{0,1\}^r \to \{0,1\}^n$ with number sector i and a random value r to generate a new value $\psi(i,r) = i'$; then the plaintext will be encrypted by the index i' but the ciphertext is saved in the sector i. This means that the jth ciphertext block in the sector number i is determined by $E_{K_1}(P \oplus E_{K_2}(i') \cdot \alpha^j) \oplus E_{K_2}(i') \cdot \alpha^j$. Note that the combination $i||R$ in [6] is a special case of our model. In order to present the distinguishing advantage, we consider a family of function ψ which satisfies $\Pr[\psi(i_1,r_1) = \psi(i_2,r_2)] \leq \epsilon$ for every $(i_1,r_1) \neq (i_2,r_2)$, we call such function be an ϵ-collision resistant function.

Next, we will present the security model for this ideal. Let $\tilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ be a fix tweakable block cipher. Consider an adversary that has access to an oracle which is one of two cases as follows:

World 1. Firstly, a key $K \xleftarrow{\$} \mathcal{K}$ is chosen randomly. When the input is (i,P), the oracle chooses $r \xleftarrow{\$} \{0,1\}^r$ and computes $i' \leftarrow \psi(i,r)$ then returns (i',C) where $C = E_K^{i'}(P)$. We denote the oracle by $\tilde{E}_K(\cdot)$

World 0. The input is (i,P). The oracle chooses $r \xleftarrow{\$} \{0,1\}^r$ and computes $i' \leftarrow \psi(i,r)$ then returns (i',C) where $C \leftarrow \tilde{\Pi}(i,P)$ and $\tilde{\Pi}(\cdot,\cdot)$ is a tweakable random permutation ($\tilde{\Pi}(i,\cdot)$ is a permutation which is chosen randomly form $\mathrm{Perm}(N)$. We denote the oracle by $\tilde{\Pi}(\cdot,\cdot)$.

Definition 7 *Let $\tilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ X be a tweakalbe block cipher and A is a probability polynomial-time algorithm that has access the oracle. We consider two experiments:*

Experiment$\boldsymbol{Exp}_{\tilde{E}}^{tcpa\text{-}1}(A)$	*Experiment*$\boldsymbol{Exp}_{\tilde{E}}^{tcpa\text{-}1}(A)$
$K \xleftarrow{\$} \mathcal{K}$	$\tilde{\Pi}(\cdot,\cdot)$ *is a tweakable random permutation*
$r \xleftarrow{\$} \{0,1\}^r$	$r \xleftarrow{\$} \{0,1\}^r$
$b \leftarrow A^{\tilde{E}_K(\cdot)}$	$b \leftarrow A^{\tilde{\Pi}(\cdot,\cdot)}$
Return b	*Return b*

The tcpa advantage of A is defined as

$$Adv_{\tilde{E}}^{tcpa}(A) = |Pr[Exp_{\tilde{E}}^{tcpa\text{-}1}(A) = 1] - Pr[Exp_{\tilde{E}}^{tcpa\text{-}0}(A) = 1]|.$$

Then, tcpa advantage function in the attack on XTS is defined as

$$Adv_{\tilde{E}}^{tcpa}(t,q) = \max_{A \in \mathcal{A}(t,q)} Adv_{\tilde{E}}^{tcpa}(A),$$

where $\mathcal{A}(t,q)$ is the set of all adversary making at most q oracle queries running in time at most t. We define a tweakable block cipher $\tilde{E}$ is (t,q,ϵ)-tcpa security if $Adv_{\tilde{E}}^{tcpa}(t,q) \leq \epsilon$.

4.2 Main result

From above definition, we present and prove for the following proposition.

Proposition 3 *Let $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ is a family of functions and the XTS mode is defined by Definition 4 using E as an underlying block cipher. If ψ is an ϵ-collision resistant function we have*

$$Adv_{XTS}^{tcpa}(t', q) \leq 2Adv_{E}^{prp\text{-}cpa}(t, q) + 3q^2/(2^n - 1) + \epsilon,$$

where t' is a polynomial of t, $Adv_{E}^{prp\text{-}cpa}(t, q)$ is the advantage function under chosen planitext attack which distinguishes the block cipher E from a random permutation (see Def 4.7 [3]).

Proof. Using Proposition 1 we have

$$\mathrm{Adv}_{\mathrm{XEX2}}^{\mathrm{tcpa}}(t'', q) \leq \mathrm{Adv}_{E}^{\mathrm{prp\text{-}cpa}}(t, q) + 3q^2/(2^n - 1).$$

We will prove that if there is a tcpa adversary A on XTS, there will exist a tcpa adversary B on XEX2 such that

$$\mathrm{Adv}_{\mathrm{XTS}}^{\mathrm{tcpa}} \leq \mathrm{Adv}_{\mathrm{XEX2}}^{\mathrm{tcpa}}(B) + \epsilon.$$

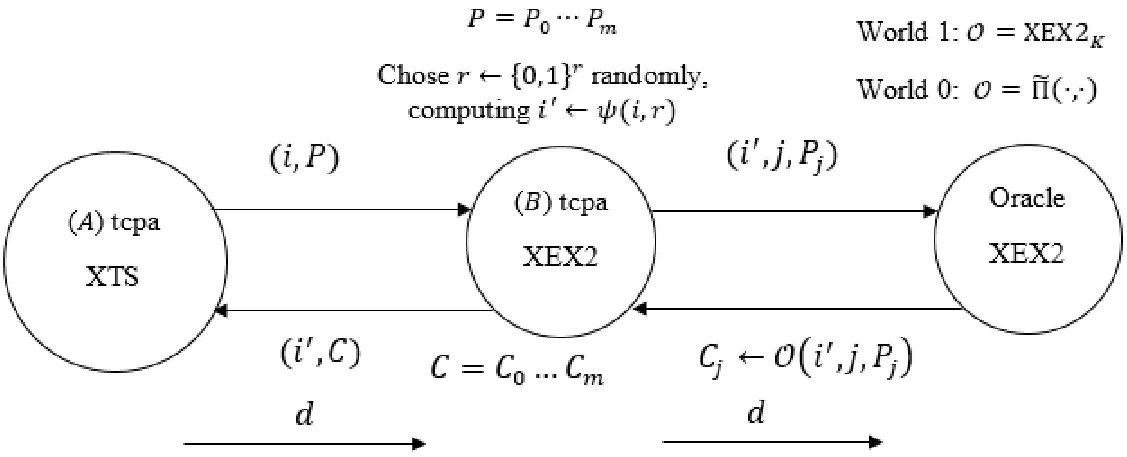
$P = P_0 \cdots P_m$
Chose $r \leftarrow \{0,1\}^r$ randomly,
computing $i' \leftarrow \psi(i, r)$
World 1: $\mathcal{O} = \mathrm{XEX2}_K$
World 0: $\mathcal{O} = \tilde{\Pi}(\cdot,\cdot)$
(i, P)
(i', j, P_j)
(A) tcpa
XTS
(B) tcpa
XEX2
Oracle
XEX2
(i', C)
$C = C_0 \dots C_m$
$C_j \leftarrow \mathcal{O}(i', j, P_j)$
d
d

Figure 1: The diagram builds an adversary B on XEX2 from an adversary A on XTS

For every tcpa adversary A on XTS, we will construct a tcpa adversary B on XEX2. If A queries (i, P) where $|P| = N$, B chooses a random value $r \overset{\$}{\leftarrow} \{0,1\}^r$ and computes $i' \leftarrow \psi(i, r)$, then B separates $P = P_0 || \cdots || P_m$ where $|P_0| = \cdots = |P_{m-1}| = n$ and $|P_m| = b \leq n$. When $b = n$, B queries consecutively (i', j, P_j) to the oracle $\mathcal{O}$ of XEX2 where $0 \leq j \leq m$ and it receives C_j. When $b < n$, B queries consecutively (i', j, P_j) to the oracle $\mathcal{O}$ of XEX2 where $0 \leq j \leq m - 1$ and it receives C_j. Next, B puts $C_m || D \leftarrow C_{m-1}$ where $|C_m| = b$ and queries $(i', m, P_m || D)$ to the oracle. B is returned a value which names C_{m-1}. Finally, B returns (i', C) where $C = C_0 || \cdots || C_m$. If the adversary A returns a bit d after querying q times, the adversary B returns d. Note that, we only need consider for the case that $b < n$.

If B is used the oracle $\mathcal{O} = \mathrm{XEX2}_K$, the view that A runs as a subroutine of B sames the view that A runs independently attacks on XTS. Thus, we have:

$$\Pr[\mathrm{Exp}_{\mathrm{XTS}}^{\mathrm{tcpa\text{-}1}}(A) = 1] = \Pr[\mathrm{Exp}_{\mathrm{XEX2}}^{\mathrm{tcpa\text{-}1}}(B) = 1].$$

If B is used the oracle $\mathcal{O} = \tilde{\Pi}(\cdot,\cdot)$, the ciphertext that A is returned when running as a subroutine of B is (i', C) where $C = C_0||\cdots||C_m$ and $C_j = \Pi^{i',j}(P_j)$ with $0 \leq j \leq m-2, C_m||D = \Pi^{i',m-1}(P_{m-1}), |C_m| = b$ and $C_{m-1} = \Pi^{i',m}(P_m||D)$ where $\Pi^{i',j}(\cdot) = \Pi((i',j),\cdot)$ is a permutation which is chosen randomly in $\mathrm{Perm}(n)$. Thus, C_j are random and independent values so C is a random value. In the case that A runs independently attacks on XTS, the ciphertext that A is returned is $C = \tilde{\Pi}(i', P)$ where $\tilde{\Pi}(i',\cdot)$ is a permutation which is chosen randomly in $\mathrm{Perm}(N)$. We will compare the view of A in both cases. If the tweak i' that is generated by $\psi(i,r)$ in q times is different, then the view that A runs as a subroutine of B same the view that A runs independently attacks on XTS. Indeed, ciphertexts that is returned to A are random and independent values in the both cases. If there is the tweak i' that repeats twice in q times, then the ciphertexts C are not independent so the view of A is different in two cases, however this has probability at most ϵ. Thus, we have

$$\Pr[\mathrm{Exp}^{\text{tcpa-0}}_{\text{XEX2}}(B) = 1] - \Pr[\mathrm{Exp}^{\text{tcpa-0}}_{\text{XTS}}(A) = 1] \leq \epsilon.$$

From above arguments we have

$$\begin{aligned}\mathrm{Adv}^{\text{tcpa}}_{\text{XTS}}(A) =&\Pr[\mathrm{Exp}^{\text{tcpa-1}}_{\text{XTS}}(A) = 1] - \Pr[\mathrm{Exp}^{\text{tcpa-0}}_{\text{XTS}}(A) = 1]\\ \leq&\Pr[\mathrm{Exp}^{\text{tcpa-1}}_{\text{XEX2}}(B) = 1] - \Pr[\mathrm{Exp}^{\text{tcpa-0}}_{\text{XEX2}}(B) = 1] + \epsilon\\ =&\mathrm{Adv}^{\text{tcpa}}_{\text{XEX2}}(B) + \epsilon\end{aligned}$$

We get the proof for Proposition 3.□
The ideal of [6] is a special case of our model where the function $\psi(i,r) = i||r$. It is easy to see that $\epsilon = 1/2^r$. From Proposition 3, the tcpa advantage in the model which was proposed in [6] is:

$$\mathrm{Adv}^{\text{tcpa}}_{\text{XTS}} \leq 2\mathrm{Adv}^{\text{prp-cpa}}_{E} + 3q^2/(2^n - 1) + 1/2^r.$$

Note. In [6] commented that the values of r may be very small, this means that ϵ is non-negligible. By our result, we can state that the XTS mode in this model is distinguishability. Moreover, we can realize that the model in [6] is attacked easily on the indistinguishability when an adversary repeats consecutively queries.

5 Conclusion

In conclusion, the XTS mode is indistinguishability up-to-block even it uses ciphertext stealing. Moreover, we present the evaluation for the indistinguishability of XTS in security model which based on an ϵ-collision resistant function to transform sector number. The theoretic result shows that the indistinguishability of XTS is guaranteed when the random value r is large enough. However, in order to actualise requests in our model there requires some technology problems that solve the storage of the added random value. In the future, we hope that there are another technology solution more effective.

References

[1] BALL, Matthew V., et al, “The XTS-AES disk encryption algorithm and the security of ciphertext stealing”, *Cryptologia, 2012, 36.1:*, 70-79.

[2] Bellare, Mihir and Desai, Anand and Jokipii, Eron and Rogaway, Phillip, “A concrete security treatment of symmetric encryption”, *Foundations of Computer Science, 1997. Proceedings., 38th Annual Symposium on*, 394–403.

[3] Bellare, Mihir, and Phillip Rogaway, “Introduction to modern cryptography”, *Ucsd Cse 207 (2005): 207.*.

[4] Dworkin, M.J., “Recommendation for block cipher modes of operation: The XTS-AES mode for confidentiality on storage devices”, *Special Publication (NIST SP)-800-38E, 2010.*

[5] IEEE Std 1619-2007, “The XTS-AES Tweakable Block Cipher”, *Institute of Electrical and Electronics Engineers, Inc, April 18, 2008.*.

[6] Khati, L., N. Mouha, and D. Vergnaud, “Full Disk Encryption: Bridging Theory and Practice”, *in Cryptographers Track at the RSA Conference. 2017. Springer.*.

[7] Liskov, M., R.L. Rivest, and D. Wagner, “Tweakable block ciphers”, *in Advances in CryptologyCRYPTO 2002. 2002, Springer*, p. 31-46.

[8] Liskov, M., R.L. Rivest, and D. Wagner, “Tweakable block ciphers”, *Journal of cryptology, 2011. 24(3)*, p. 588-613.

[9] Rogaway, P., “Evaluation of some blockcipher modes of operation”, *Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan, 2011.*