On indistinguishability of LRW and XEX2 constructions

Tuan Anh Nguyen

Abstract— **Encryption on a storage device has characteristics that some common block cipher mode of operation such as CBC, CFB, CTR,… are not reach; so the tweakable block cipher notation was introduced. LRW construction was proposed by Liskov, Rivest and Wagner [1], is one of the most popular methods in constructing tweakable block cipher. In this paper, we consider the indistinguishability of LRW and XEX2 constructions. Specifically, we confirm the results in LRW construction's initial proof, and then the indistinguishability of XEX2 is evaluated in detail. Ours results improve the security bound for LRW and XEX2 construction.**

Tóm tắt— **Mã hóa trong môi trường lưu trữ dữ liệu có những đặc thù mà một số chế độ mã khối thông thường như CBC, OFB, CTR,… không đáp ứng được; do đó khái niệm "mã khối tinh chỉnh được" đã ra đời. Cấu trúc LRW, được đề xuất bởi Liskov, Rivest và Wagner [1], là một trong những phương pháp phổ biến để xây dựng mã khối tinh chỉnh được. Trong bài báo này, chúng tôi xem xét về tính không phân biệt được của hai cấu trúc LRW và XEX2. Cụ thể, chúng tôi chính xác hóa lại kết quả trong chứng minh ban đầu của cấu trúc LRW và đưa ra đánh giá chi tiết cho tính không phân biệt được của XEX2. Kết quả của chúng tôi cải tiến cận an toàn cho cấu trúc LRW và XEX2.**

Keywords— **Tweakable block cipher; LRW construction; XEX2 construction.**

Từ khóa— **Mã khối tinh chỉnh được; cấu trúc LRW; cấu trúc XEX2.**

I. 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 et al. presented a new cryptographic primitive, the "tweakable block cipher", in 2002 ([1]). Then, many constructions of tweakable block cipher were proposed such as LRW, XEX, XEX2,… Evaluating the indistinguishability of tweakable block cipher constructions have been attracting research attention in the cryptography community ([1-3]).

Related work. Liskov et al. gave the security proof of LRW ([1]) in 2002. However, the bound can be better and the condition can be expand. A well know case of LRW construction is the XEX2 construction, which is the tweakable block cipher that is used in the XTS mode. This tweakable block cipher is closely based on Rogaway's XEX mode [2]. The security of XEX2 was evaluated by Phillip Rogaway by using the fact that it has LRW construction. However, Phillip Rogaway did not give detail proof.

Our contributions. In this paper, we first confirm the security proof for LRW construction. The received result is better and without the condition $\epsilon \geq 1/2^n$ as ([4]). Then, the detail proof with better indistinguishability advantage of XEX2 construction is given by using above LRW's result.

Outline. This paper organized as follows. In Section 2, we represent some related notions. Section 3 gives the distinguishing advantage of LRW and XEX2 constructions. Finally, some conclusions are given.

II. PRELIMINARIES

A. Notations and definitions

In 2002, the definition "tweakable block cipher" was proposed by Liskov, Rivest and Wagner [1] 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 called "tweak", beside a key and a plaintext. Thus, a tweakable 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 tweakable block cipher under chosen plaintext attack (abbreviate as tcpa). We fix a tweakable block cipher $\tilde{E}: \mathcal{K} \times \mathcal{T} \times \mathcal{X} \to \mathcal{X}$. Consider an adversary that has access to an oracle which is a function $g: \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ was determined by one of the following two cases:

This manuscript is received on February 15, 2018. It is commented on March 25, 2018 and is accepted on April 2, 2018 by the first reviewer. It is commented on February 25, 2017 and is accepted on March 30, 2017 by the second reviewer.

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

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

Definition 1 (see [4]). *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 $\mathbf{Exp}_{\tilde{E}}^{\mathbf{tcpa-1}}(A)$	*Experiment* $\mathbf{Exp}_{\tilde{E}}^{\mathbf{tcpa-0}}(A)$
$k \overset{\$}{\leftarrow} \mathcal{K}$ $b \leftarrow A^{\tilde{E}_K(\cdot,\cdot)}$ *Return b*	$\widetilde{\Pi}(\cdot,\cdot)$ is tweakable random permutation $b \leftarrow A^{\widetilde{\Pi}(\cdot,\cdot)}$ *Return b*

The tcpa advantage of A is defined as

$$\mathrm{Adv}_{\tilde{E}}^{\mathrm{tcpa}}(A) = \Pr\left[\mathrm{Exp}_{\tilde{E}}^{\mathrm{tcpa-1}}(A) = 1\right] - \Pr\left[\mathrm{Exp}_{\tilde{E}}^{\mathrm{tcpa-0}}(A) = 1\right].$$

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

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

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

Next, we consider the security of a tweakable block cipher under chosen ciphertext attack (abbreviate as tcca). We fix a tweakable block cipher $\tilde{E}: \mathcal{K} \times \mathcal{T} \times \mathcal{X} \to \mathcal{X}$. 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 was determined by one of the following two cases:

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

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

Definition 2 (see [4]). *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 $\mathbf{Exp}_{\tilde{E}}^{\mathbf{tcca-1}}(A)$	*Experiment* $\mathbf{Exp}_{\tilde{E}}^{\mathbf{tcca-0}}(A)$
$k \overset{\$}{\leftarrow} \mathcal{K}$ $b \leftarrow A^{\tilde{E}_K(\cdot,\cdot),\tilde{D}_K(\cdot,\cdot)}$ *Return b*	$\widetilde{\Pi}(\cdot,\cdot)$ is a tweakable random permutation $b \leftarrow A^{\widetilde{\Pi}(\cdot,\cdot),\widetilde{\Pi}^{-1}(\cdot,\cdot)}$ *Return b*

The tcca advantage of A is defined as

$$Adv_{\tilde{E}}^{tcca}(A) = Pr\left[Exp_{\tilde{E}}^{tcca-1}(A) = 1\right] - Pr\left[Exp_{\tilde{E}}^{tcca-0}(A) = 1\right].$$

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

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

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

B. LRW construction

LRW construction, which was used to construct a tweakable block cipher from an underlying block cipher, was proposed by Moses Liskov, Ronald L. Rivest and David Wagner [1].

A family $\mathcal{H}$ of functions with signature $\{0,1\}^t \to \{0,1\}^n$ is said to be an ϵ-almost 2-xor-universal hash function family ("ϵ-AXU$_2$ hash function family", for short) if $\Pr[h(x) \oplus h(y) = z] \leq \epsilon$ holds for all x, y, z with $x \neq y$, where the probability is taken over h chosen uniformly at random from $\mathcal{H}$ (see [1]). We have follow definition.

Definition 3 (see [1]). *Let* $\mathcal{H}$ *be an* ϵ-AXU$_2$ *hash function family. The LRW construction uses a key* (K,h) *where* $K \leftarrow \{0,1\}^k$ *and* $h \leftarrow \mathcal{H}$*, and is given by*

$$\tilde{E}_{K,h}(T,M) = E_K\big(M \oplus h(T)\big) \oplus h(T)$$
$$\widetilde{D}_{K,h}(T,C) = D_K\big(C \oplus h(T)\big) \oplus h(T).$$

C. XEX2 construction

XEX2-AES was used in NIST Recommendation SP 300-38E [5] has LRW construction [1] with the underlying block cipher is AES. In this paper, we describe the general definition for the XEX2 construction with an arbitrary block cipher E.

Definition 4. *Let E be an arbitrary block cipher: $\mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$. The* XEX2 *construction: $\{0,1\}^k \times \{0,1\}^n \times [0..2^n - 2] \times \{0,1\}^n \to \{0,1\}^n$ is defined as*

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

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 the finite field $GF(2^n)$, and the operator "$\cdot$" is multiplication in the finite field $GF(2^n)$.

III. THE DISTINGUISHING ADVANTAGE OF LRW AND XEX2 CONSTRUCTION

A. The distinguishing advantage of LRW construction

Consider A be a fix adversary. We let the random variable T_i denote the tweak input on A's i-th oracle call, and we let M_i and C_i denote the plaintext and ciphertext corresponding to this call, so that $\mathcal{O}(T_i, M_i) = C_i$ (the oracle is denoted by $\mathcal{O}$). Moreover, we define the random variables N_i, B_i by $N_i = M_i \oplus h(T_i)$ and $B_i = C_i \oplus h(T_i)$. Note that $E_K(N_i) = B_i$ in the case the adversary has access to the oracle $\mathcal{O} = \tilde{E}_K$.

We observe that if the adversary can create queries such that $N_i = N_j$ or $B_i = B_j$ then he will distinguish LRW construction from a random tweakable permutation. Indeed, if $N_i = N_j$ or $B_i = B_j$ we always have $M_i \oplus M_j = C_i \oplus C_j$ in the case the oracle $\mathcal{O} = \tilde{E}_K$. However, the probability that $N_i = N_j$ or $B_i = B_j$ is neglibible.

We defined Bad_n to be the event that, for some $1 \le i < j \le n$, either $N_i = N_j$ or $B_i = B_j$. Also, we let $\mathrm{Bad} = \mathrm{Bad}_q$. Let $\mathrm{Pr}_1[\cdot]$ is the probability measure in the case where the adversary A interacts with the oracle $\mathcal{O} = \tilde{E}_K$.

Proposition 1. *If $\mathcal{H}$ is ϵ-AXU_2 and if $E_K = \Pi$, then* $\mathrm{Pr}_1[\mathrm{Bad}_q] \le 0.5\epsilon q(q-1)$.

Proof. When $q = 1$, Proposition 1 is correct. Let E denote the event that, for some i, we have $N_i = N_q$, and let $E^{\prime}$ denote the event that, for some i, we have $B_i = B_q$. Note that

$$\begin{aligned}\underset{1}{\mathrm{Pr}}[\mathrm{Bad}_q] &= \underset{1}{\mathrm{Pr}}\big[\mathrm{Bad}_q \big| \mathrm{Bad}_{\mathrm{q-1}}\big] \cdot \underset{1}{\mathrm{Pr}}\big[Bad_{q-1}\big] \\ &\quad + \underset{1}{\mathrm{Pr}}\big[\mathrm{Bad}_q \big| \overline{\mathrm{Bad}}_{\mathrm{q-1}}\big] \cdot \underset{1}{\mathrm{Pr}}[\overline{\mathrm{Bad}}_{\mathrm{q-1}}] \\ &= \underset{1}{\mathrm{Pr}}[\mathrm{Bad}_{q-1}] + \underset{1}{\mathrm{Pr}}\big[\mathrm{Bad}_q \big| \overline{\mathrm{Bad}}_{\mathrm{q-1}}\big] \cdot \underset{1}{\mathrm{Pr}}\big[\overline{\mathrm{Bad}}_{\mathrm{q-1}}\big].\end{aligned}$$

By the inductive hypothesis, $\mathrm{Pr}_1[\mathrm{Bad}_{q-1}] \le 0.5\epsilon(q-1)(q-2)$. Also, $\mathrm{Pr}_1[\overline{\mathrm{Bad}}_{\mathrm{q-1}}] \le 1$. Hence all that remains is to bound the term $\mathrm{Pr}_1\big[\mathrm{Bad}_q \big| \overline{\mathrm{Bad}}_{\mathrm{q-1}}\big]$.

Then, we will evaluate for $\mathrm{Pr}_1\big[\mathrm{Bad}_q \big| \overline{\mathrm{Bad}}_{\mathrm{q-1}}\big]$. We always have $\Pi(N_i) = B_i$ in the case that $E_K = \Pi$. Thus, if the event E occur, the event $E^{\prime}$ will occur, and vice versa. We can bound the term $\mathrm{Pr}_1\big[\mathrm{Bad}_q \big| \overline{\mathrm{Bad}}_{\mathrm{q-1}}\big]$ as follows:

$$\begin{aligned}\underset{1}{\mathrm{Pr}}\big[\mathrm{Bad}_q \big| \overline{\mathrm{Bad}}_{q-1}\big] &= \underset{1}{\mathrm{Pr}}\big[\mathrm{E} \big| \overline{\mathrm{Bad}}_{q-1}\big] \\ = \underset{1}{\mathrm{Pr}}\big[\exists 1 \le i < q, N_q = N_i \big| \overline{\mathrm{Bad}}_{q-1}\big]& \\ \le \sum_{1 \le i < q} \underset{1}{\mathrm{Pr}}\big[N_q = N_i \big| \overline{\mathrm{Bad}}_{q-1}\big]& \\ = \sum_{1 \le i < q} \underset{1}{\mathrm{Pr}}\big[h(T_i) \oplus h(T_q) = M_i \oplus M_q \big| \overline{\mathrm{Bad}}_{q-1}\big]& \\ &\le \epsilon(q-1).\end{aligned}$$

Then, we have:

$$\begin{aligned}\underset{1}{\mathrm{Pr}}[\mathrm{Bad}_q] &\le 0.5\epsilon(q-1)(q-2) + \epsilon(q-1) \\ &= 0.5\epsilon(q-1)q.\end{aligned}$$

Note 1. A similar result was presented in [1] (Lemma 3). However, the constant "0.5" is replaced by "1.5" and it has the condition $\epsilon \ge 1/2^n$.

Replace Lemma 3 ([1]) by our result in the security proof of LRW construction we have the follow proposition.

Proposition 2. *Let $E: \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be an arbitrary block cipher. The LRW construction is defined as $\tilde{E}_{K,h}(T, M) = E_K\big(M \oplus h(T)\big) \oplus h(T)$, with $\mathcal{H}$ be an ϵ-*AXU$_2$ *family. Then*

$$\mathrm{Adv}_{\tilde{E}}^{\mathrm{tcca}}(t, q) \le \mathrm{Adv}_E^{\mathrm{cca}}(t + q, q) + 2.5\epsilon q^2.$$

B. The distinguishing advantage of XEX2

The security of the tweakable block cipher XEX2 was considered by Phillip Rogaway [3]. However, the detail proof was not given. In this section, we will prove the security of the tweakable block cipher XEX2 and give the distinguishing advantage.

Proposition 3. Let $E: \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be an arbitrary block cipher. The XEX2 construction is defined as Definition 4. Then,

$$\mathrm{Adv}_{\mathrm{XEX2}}^{\mathrm{tcca}}(t, q) \le \mathrm{Adv}_{\mathrm{E}}^{\mathrm{cca}}(t, q)$$

$$+\mathrm{Adv}_E^{\mathrm{cpa}}(t, q) + 2.5q^2/(2^n - 1).$$

Proof. The XEX2 construction can be rewritten according to LRW construction as $\tilde{E}_{E_{K_1},h}(X) = E_{K_1}\big(X \oplus h(T)\big) \oplus h(T)$ where $h(T) = h(i,j) = E_{K_2}(i)\cdot\alpha^j$. In order to apply Proposition 2, we first consider E_{K_2} is a random permutation π. Then, we prove that $h(i,j) = \pi(i)\cdot\alpha^j$ is an ϵ-AXU$_2$ function, which means asking to bound

$$\Pr_{\pi}\big[\pi(i_1)\cdot\alpha^{j_1} \oplus \pi(i_2)\cdot\alpha^{j_2} = c\big].$$

We have α is a primitive element of $GF(2^n)$ and $j \in [0..2^n-2]$. Thus,

- If $i_1 \neq i_2$ then $\Pr_{\pi}\big[\pi(i_1)\cdot\alpha^{j_1} = \pi(i_2)\cdot\alpha^{j_2} \oplus c\big] \le 1/(2^n-1)$.
- If $i_1 = i_2$ then $\Pr_{\pi}\big[\pi(i_1)\cdot\big(\alpha^{j_1} \oplus \alpha^{j_2}\big) = c\big] \le 1/2^n$.

This means that h is an $1/(2^n-1)$-AXU$_2$ function. Using Proposition 2 we have the *tcca* advantage in the attack on $\mathrm{XEX2}' = E_{K_1}\big(M \oplus \pi(i)\cdot\alpha^j\big) \oplus \pi(i)\cdot\alpha^j$ is

$$\begin{aligned}\mathrm{Adv}^{\mathrm{tcca}}_{\mathrm{XEX2}'}\ (t,q) \\ &\le \mathrm{Adv}^{\mathrm{cca}}_{\mathrm{E}}(t,q) \\ &+ 2.5q^2/(2^n-1).\end{aligned}$$

Finally, we consider the distinguishing advantage between XEX2 and XEX2′. Note that the decryption in two constructions does not need the operator $E^{-1}_{K_2}$ or π^{-1}. Using the reduction we can prove that $\mathrm{Adv}^{\mathrm{tcca}}_{\mathrm{XEX2}}(t,q) - \mathrm{Adv}^{\mathrm{tcca}}_{\mathrm{XEX2}'}\ (t,q) \le \mathrm{Adv}^{\mathrm{cpa}}_{E}(t,q)$.

From above arguments we have

$$\mathrm{Adv}^{\mathrm{tcca}}_{\mathrm{XEX2}}(t,q) \le \mathrm{Adv}^{\mathrm{cca}}_{\mathrm{E}}(t,q)$$

$$+\mathrm{Adv}^{\mathrm{cpa}}_{E}(t,q) + 2.5q^2/(2^n-1).$$

Note 2. Because the chosen plaintext attack is a chosen ciphertext attack where the number of decryption query is zero, so that $\mathrm{Adv}^{\mathrm{cpa}}_{E}(t,q) \le \mathrm{Adv}^{\mathrm{cca}}_{E}(t,q)$. Thus,

$$\mathrm{Adv}^{\mathrm{tcca}}_{\mathrm{XEX2}}(t,q) \le 2\mathrm{Adv}^{\mathrm{cca}}_{\mathrm{E}}(t,q) + 3q^2/(2^n-1).$$

This is the advantage by Phillip Rogaway's evaluation

IV. CONCLUSION

In conclusion, we can prove that the LRW construction is indistinguishable from a tweakable random permutation without the condition $\epsilon \ge 1/2^n$ and have the better bound. We also give the detail proof for the security of XEX2 construction and give the distinguishing advantage. The theoretic results show that our result is better than the previous results. However, our researches are only for two above constructions, we would like to make evaluations for provable security of tweakable mode of operation such as XTS, which have been attracting research attention in the cryptography community.

REFERENCES

[1]. Liskov, M., R.L. Rivest, and D. Wagner, "Tweakable block ciphers", in Advances in Cryptology—CRYPTO 2002 Springer, pp. 31-46. 2002.

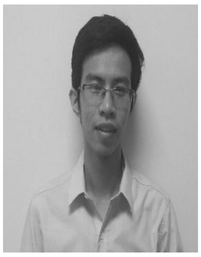
[2]. Rogaway, P., "Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC", in Advances in Cryptology-ASIACRYPT 2004. Springer, pp. 16-31, 2004.

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

[4]. Liskov, M., R.L. Rivest, and D. Wagner, "Tweakable block ciphers". Journal of cryptology, **24**(3): pp. 588-613, 2011.

[5]. 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.

ABOUT THE AUTHOR



BSc. Tuan Anh Nguyen

Workplace: Institute of Cryptography Science and Technology.

Email: tuananhnghixuan@gmail.com

The education process: has received a mathematical bachelor degree in Hanoi Universiy of Science, in 2016.

Research today: secret key cryptography.