Tweak-Length Extension for Tweakable Blockciphers[⋆]

Kazuhiko Minematsu[1] and Tetsu Iwata[2]

[1] NEC Corporation, Japan, k-minematsu@ah.jp.nec.com
[2] Nagoya University, Japan, iwata@cse.nagoya-u.ac.jp

Abstract. Tweakable blockcipher (TBC) is an extension of standard blockcipher introduced by Liskov, Rivest and Wagner in 2002. TBC is a versatile building block for efficient symmetric-key cryptographic functions, such as authenticated encryption.

In this paper we study the problem of extending tweak of a given TBC of fixed-length tweak, which is a variant of popular problem of converting a blockcipher into a TBC, i.e., blockcipher mode of operation. The problem is particularly important for known dedicated TBCs since they have relatively short tweak. We propose a simple and efficient solution, called XTX, for this problem. XTX converts a TBC of fixed-length tweak into another TBC of arbitrarily long tweak, by extending the scheme of Liskov, Rivest and Wagner that converts a blockcipher into a TBC. Given a TBC of n-bit block and m-bit tweak, XTX provides $(n+m)/2$-bit security while conventional methods provide $n/2$ or $m/2$-bit security. We also show that XTX is even useful when combined with some blockcipher modes for building TBC having security beyond the birthday bound.

Keywords: Tweakable blockcipher, Tweak extension, Mode of operation, LRW

1 Introduction

Tweakable blockcipher. Tweakable blockcipher (TBC) is an extension of standard blockcipher introduced by Liskov, Rivest and Wagner in 2002 [17]. An encryption of TBC takes a parameter called tweak, in addition to key and plaintext. Tweak is public and can be arbitrarily chosen. Due to its versatility, TBC is getting more and more popularity. Known constructions of TBCs are generally classified into two categories: dedicated design and blockcipher mode of operation, i.e. using a blockcipher as a black box.

For the first category, Hasty pudding cipher [30] and Mercy [10] are examples of early designs. More recently Skein hash function uses a dedicated TBC called Threefish [2]. Jean, Nikolić and Peyrin [13] developed several dedicated TBCs as components of their proposals to CAESAR [1], a competition of authenticated encryption (AE).

[⋆] A preliminary version of this paper appears in the proceedings of IMA international conference on cryptography and coding (IMACC) 2015. This is the full version.

For the second category, Liskov et al. [17] provided two blockcipher modes to build TBC, and their second mode is known as LRW[3]. Rogaway [28] refined LRW and proposed XE and XEX modes, and Minematsu [22] proposed a generalization of LRW and XEX. These schemes have provable security up to so-called "birthday bound", i.e. they can be broken if adversary performs around $2^{n/2}$ queries, where n is the block length of TBC. The first scheme to break this barrier was shown by Minematsu [23], though it was limited to short tweak and rekeyed for every tweak. Landecker, Shrimpton and Terashima [16] showed that a chain of two LRWs has security beyond the birthday bound, which is the first scheme with this property which does not use rekeying. Lampe and Seurin [15] extended the work of [16] for longer chains. Tweakable variants of Even-Mansour cipher [11] are studied by Cogliati, Lampe and Seurin [8] and Mennink [21]. A concrete example is seen in a CAESAR proposal, called Minalpher [29].

Tweak extension. In this paper, we study tweak extension of a given TBC. More formally, let $\widetilde{E}$ be a TBC of n-bit block and m-bit tweak, and we want to arbitrarily extend m-bit tweak of $\widetilde{E}$ keeping n-bit block. Here m is considered to be fixed. At first sight the problem looks trivial since most of previous studies in the second category already cover the case of arbitrarily long tweak when combined with a universal hash (UH) function of variable-length input, and a TBC with any fixed tweak is also a blockcipher. Coron et al. (Theorem 6, [9]) pointed out another simple solution by applying a UH function H to tweak and then use the hash value $H(T)$ as the tweak of $\widetilde{E}$. However, the problem is security. For TBC $\widetilde{E}$ of n-bit block and m-bit tweak, applying LRW or XEX to (fixed-tweak) $\widetilde{E}$ the security is up to $O(2^{n/2})$ queries. Coron et al.'s solution is also secure up to $O(2^{m/2})$ queries. We would get a better security bound by using the chained LRW [16, 15], but it would significantly increase the computation cost from $\widetilde{E}$.

In this paper we provide an alternative solution, called XTX, which can be explained as an intuitive yet non-trivial combination of LRW and Coron et al.'s method mentioned above, applicable to any black-box TBC. Specifically, XTX converts a TBC $\widetilde{E}$ of n-bit block and m-bit tweak into another TBC of n-bit block and t-bit tweak for any $t > m$, using H which is a (variant of) UH function of t-bit input and $(n+m)$-bit output. See Fig. 1 for XTX. We proved the security bound of $q^2\epsilon$ where ϵ denotes the bias of UH function. This implies security up to $O(2^{(n+m)/2})$ queries if ϵ is ideally small. As well as LRW, XTX needs one calls of $\widetilde{E}$ and H, hence the computation cost is only slightly increased, and H is called only once for multiple encryptions sharing the same tweak, by caching the output of H.

We observe that tweak length of existing dedicated TBCs are relatively short, at least not much longer than the block length. For instance, KIASU-BC [13] has 128-bit block and 64-bit tweak, and Threefish has 256 or 512 or 1024-bit block

[3] The two schemes shown by [17] are also called LRW1 and LRW2, and we refer to LRW2 throughout this paper.

with 128-bit tweak for all block sizes. One apparent reason for having fixed, short tweak is that it is enough for their primary applications, however, if tweak can be effectively extended it would expand their application areas. For another reason, we think the complexity of security analysis for dedicated TBC is expected to be dependent on the size of tweak space, since we have to make sure that for each tweak the instance should behave as an independently-keyed blockcipher. The TWEAKEY framework of Jean, et al. [13] provided a systematic way to build TBCs by incorporating tweak in the key schedule, and it shows that building efficient TBCs from scratch is far from trivial, in particular when we want to have long tweaks. Our XTX can efficiently extend tweak of dedicated TBCs with reasonably small security degradation in terms of the maximum number of allowable queries. In addition, XTX is even useful when applied to some modes of operations when the baseline TBC from a (non-tweakable) blockcipher has beyond-birthday-bound security. We summarize these results in Section 4.

Applications of tweak extension. We remark that a TBC with long tweak is useful. In general, a tweak of a TBC can be used to contain various additional information associated with plaintext block, hence it would be desirable to make tweak substantially longer than the block length (say 128 bits). For concrete examples, a large-block TBC of Shrimpton and Terashima [31] used a TBC with variable-length tweak, which was instantiated by a combination of techniques from [9, 16]. Hirose, Sasaki and Yasuda [12] presented an AE scheme using TBC with tweak something longer than the unit block.

2 Preliminaries

Notation. Let $\{0,1\}^*$ be the set of all finite bit strings. For an integer $\ell \geq 0$, let $\{0,1\}^\ell$ be the set of all bit strings of ℓ bits. For $X \in \{0,1\}^*$, $|X|$ is its length in bits, and for $\ell \geq 1$, $|X|_\ell = \lceil |X|/\ell \rceil$ is the length in ℓ-bit blocks. When ℓ denotes the length of a binary string we also write ℓ_n to mean $\lceil \ell/n \rceil$. A sequence of a zeros is denoted by 0^a. For set $\mathcal{S} \subseteq \{0,1\}^n$ and $x \in \{0,1\}^n$, $\mathcal{S} \oplus x$ denotes the set $\{s \oplus x : s \in \mathcal{S}\}$. If random variable X is uniformly distributed over $\mathcal{X}$ we write $X \in_{\mathrm{U}} \mathcal{X}$.

Cryptographic functions. For any keyed function we assume that its first argument denotes the key. For keyed function $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$, we write $F_K(x)$ to denote $F(K, x)$ for the evaluation of input $x \in \mathcal{X}$ with key $K \in_{\mathrm{U}} \mathcal{K}$.

A blockcipher $E : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$ is a keyed permutation over the message space $\mathcal{M}$. We write encryption of M using K as $C = E_K(M)$ and its inverse as $M = E_K^{-1}(C)$. Similarly, a tweakable blockcipher (TBC) is a family of n-bit blockcipher indexed by tweak $T \in \mathcal{T}$. It is written as $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$. If $\mathcal{M} = \{0,1\}^n$ and $\mathcal{T} = \{0,1\}^t$, we say $\widetilde{E}$ is an (n,t)-bit TBC. An encryption of message M with tweak T is written as $\widetilde{E}_K^T(M)$, and if we have $C = \widetilde{E}_K^T(M)$

then $M = \widetilde{E}_K^{T,-1}(C)$ holds for any (T, M). Let $\mathrm{Perm}(n)$ be the set of all n-bit permutations. For a finite set $\mathcal{X}$, let $\mathrm{Perm}^{\mathcal{X}}(n)$ be the set of all functions $: \mathcal{X} \times \{0,1\}^n \to \{0,1\}^n$ such that, for any $f \in \mathrm{Perm}^{\mathcal{X}}(n)$ and $x \in \mathcal{X}$, $f(x, *)$ is a permutation. An n-bit uniform random permutation (URP) is a keyed permutation with uniform key distribution over $\mathrm{Perm}(n)$ (where a key directly represents a permutation). Note that implementation of n-bit URP is impractical when n is a block size of conventional blockciphers (say, 64 or 128). We also define an n-bit tweakable URP (TURP) with tweak space $\mathcal{T}$ as a keyed tweakable permutation with uniform key distribution over $\mathrm{Perm}^{\mathcal{T}}(n)$.

Let $\mathcal{A}$ be the adversary trying to distinguish two oracles, $\mathcal{O}_1$ and $\mathcal{O}_2$, by possibly adaptive queries (which we call chosen-plaintext attack, CPA for short). We denote the event that the final binary decision of $\mathcal{A}$ after querying oracle $\mathcal{O}$ is 1 by $\mathcal{A}^{\mathcal{O}} \Rightarrow 1$. We write

$$\mathtt{Adv}^{\mathtt{cpa}}_{\mathcal{O}_1,\mathcal{O}_2}(\mathcal{A}) \overset{\mathrm{def}}{=} \Pr[\mathcal{A}^{\mathcal{O}_1} \Rightarrow 1] - \Pr[\mathcal{A}^{\mathcal{O}_2} \Rightarrow 1], \tag{1}$$

where the probabilities are defined over the internal randomness of $\mathcal{O}_i$ and $\mathcal{A}$. In particular if $\mathcal{O}_1 = E_K$ and $\mathcal{O}_2 = G_{K'}$ for two keyed permutations, E_K and $G_{K'}$, we assume $\mathcal{A}$ performs a chosen-ciphertext attack (CCA), i.e., has encryption and decryption queries and define

$$\mathtt{Adv}^{\mathtt{cca}}_{E,G}(\mathcal{A}) \overset{\mathrm{def}}{=} \Pr[\mathcal{A}^{(E_K, E_K^{-1})} \Rightarrow 1] - \Pr[\mathcal{A}^{(G_{K'}, G_{K'}^{-1})} \Rightarrow 1], \tag{2}$$

where $\mathcal{A}^{(E_K, E_K^{-1})}$ denotes that $\mathcal{A}$ can choose one of E_K or E_K^{-1} for each query. In the same manner we define $\mathtt{Adv}^{\mathtt{cca}}_{\widetilde{E}_K,\widetilde{G}_{K'}}(\mathcal{A})$ for two keyed tweakable permutations, where tweaks in queries are arbitrarily chosen.

For n-bit blockcipher E_K and (n,t)-bit TBC $\widetilde{E}_K$, we define SPRP (for strong pseudorandom permutation) and TSPRP (for tweakable SPRP) advantages for $\mathcal{A}$ as

$$\mathtt{Adv}^{\mathtt{sprp}}_{E}(\mathcal{A}) \overset{\mathrm{def}}{=} \mathtt{Adv}^{\mathtt{cca}}_{E,\mathsf{P}}(\mathcal{A}), \text{ and } \mathtt{Adv}^{\mathtt{tsprp}}_{\widetilde{E}}(\mathcal{A}) \overset{\mathrm{def}}{=} \mathtt{Adv}^{\mathtt{cca}}_{\widetilde{E},\widetilde{\mathsf{P}}}(\mathcal{A}), \tag{3}$$

where P is n-bit URP and $\widetilde{\mathsf{P}}$ is (n,t)-bit TURP.

If $\mathcal{A}$ is information-theoretic, it is only limited in the numbers and lengths of queries. If $\mathcal{A}$ is computational, it also has a limitation on computation time in some fixed model, which is required to define computationally-secure objects, e.g. pseudorandom function (PRF). In this paper most security proofs are information-theoretic, i.e. the target schemes are built upon URP or TURP. When their components are substituted with conventional blockcipher or TBC, a computational security bound is obtained using a standard technique [4].

2.1 Universal hash function and polynomial hash function

We will need a class of non-cryptographic functions called universal hash function [7] defined as follows.

Definition 1. *For function $H : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ being keyed by $K \in_{\mathrm{U}} \mathcal{K}$, we say it is ϵ-almost uniform (ϵ-AU) if*

$$\max_{x \neq x'} \Pr_K[H_K(x) = H_K(x')] \le \epsilon \tag{4}$$

holds. Moreover if $\mathcal{Y} = \{0,1\}^n$ for some n, we say it is ϵ-almost XOR uniform (ϵ-AXU) if

$$\max_{x \neq x', \Delta \in \{0,1\}^n} \Pr_K[H_K(x) \oplus H_K(x') = \Delta] \le \epsilon \tag{5}$$

holds.

From the definition if H is ϵ-AXU then it is also ϵ-AU.

Next we introduce polynomial hash function as a popular class of AU and AXU functions. Let $\mathsf{Poly}[a] : \mathcal{L} \times \{0,1\}^* \to \{0,1\}^a$ for key space $\mathcal{L} = \mathrm{GF}(2^a)$ be the polynomial hash function defined over $\mathrm{GF}(2^a)$. Formally, we have

$$\mathsf{Poly}[a]_L(X) = \sum_{i=1,\dots,|X|_a} L^{|X|_a - i + 1} \cdot X[i], \tag{6}$$

where multiplications and additions are over $\mathrm{GF}(2^a)$, and $(X[1], \dots, X[|X|_a])$ denotes an a-bit partition of $X \in \{0,1\}^*$ with a mapping between $\{0,1\}^a$ and $\mathrm{GF}(2^a)$ and a padding for partial message. Here, padding must have the property that the original message is uniquely recovered from the padded message. For example we can pad the non-empty sequence with $v = 100\dots0$ so that $|X\|v|$ is a multiple of a. Moreover, we write $\mathsf{Poly}[a,b] : \mathcal{L} \times \{0,1\}^* \to \{0,1\}^a \times \{0,1\}^b$ for $\mathcal{L} = \mathrm{GF}(2^a) \times \mathrm{GF}(2^b)$ to denote the function $\mathsf{Poly}[a,b]_{(L_1,L_2)}(X) = (\mathsf{Poly}[a]_{L_1}(X), \mathsf{Poly}[b]_{L_2}(X))$, where L_1 and L_2 are independent. Further extensions, such as $\mathsf{Poly}[a,b,c]$, are similarly defined.

If we limit the input space of Poly to $\{0,1\}^\ell$ for some predetermined ℓ, we have the following.

Proposition 1. *A polynomial hash function $\mathsf{Poly}[n] : \mathcal{L} \times \{0,1\}^\ell \to \{0,1\}^n$ is ϵ-AXU with $\epsilon = \ell_n/2^n$. Moreover, $\mathsf{Poly}[n_1, n_2, \dots, n_c] : \mathcal{L} \times \{0,1\}^\ell \to \mathcal{Y}$ for $\mathcal{L} = \mathrm{GF}(2^{n_1}) \times \cdots \times \mathrm{GF}(2^{n_c})$ and $\mathcal{Y} = \{0,1\}^{n_1} \times \cdots \times \{0,1\}^{n_c}$ is ϵ-AXU for $\epsilon = \prod_i (\ell_{n_i}/2^{n_i})$.*

Polynomial hash function can work over inputs of different lengths if combined with appropriate encoding. However, for simplicity this paper mainly discusses the case where Poly has a fixed input length, and in this respect we treat tweak length (in block or bit) appeared in the security bound as a constant, which is usually denoted by ℓ. Recall that we use ℓ_n to denote $\lceil \ell/n \rceil$.

3 Main construction

3.1 Previous schemes

We start with a description of one of the most popular TBC schemes based on blockcipher. It is the second construction of Liskov et al. [17] and is called LRW.

Using blockcipher $E : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$ with $\mathcal{M} = \{0,1\}^n$ and a keyed function $H : \mathcal{L} \times \mathcal{T} \to \mathcal{M}$, LRW is described as

$$\mathrm{LRW}^T_{K,L}(M) = H_L(T) \oplus E_K(M \oplus H_L(T)), \tag{7}$$

where $T \in \mathcal{T}$ is a tweak and $K \in_{\mathrm{U}} \mathcal{K}$ and $L \in_{\mathrm{U}} \mathcal{L}$ are independent keys. Let $\mathrm{LRW}_{\mathsf{P},L}$ denote LRW using n-bit URP, P, as a blockcipher and H with independent key $L \in_{\mathrm{U}} \mathcal{L}$. Its TSPRP-advantage is bounded as[4]

$$\mathtt{Adv}^{\mathtt{tsprp}}_{\mathrm{LRW}_{\mathsf{P},L}}(\mathcal{A}) \le \epsilon \cdot q^2, \tag{8}$$

for any CCA-adversary $\mathcal{A}$ using q queries, if H is ϵ-AXU. Since $\epsilon \ge 1/2^n$ this implies provable security up to the birthday bound. The bound is tight in that there is an attack matching the bound. Rogaway's XEX [28] and Minematsu's scheme [22] reduce the two keys of LRW to one blockcipher key.

For tweak extension of given (n,m)-bit TBC, $\widetilde{E}$, we have two previous solutions: the first one is to use LRW with blockcipher instantiated by $\widetilde{E}$ taking a fixed tweak. This has security bound of (8), hence $n/2$-bit security when H is (e.g.) $\mathsf{Poly}[n]$. The second one, proposed by Coron et.al. [9] as mentioned earlier, is to use $H : \mathcal{L} \times \mathcal{T} \to \mathcal{V}$ and combine $\widetilde{E}$ and H as $C = \widetilde{E}^V_K(M)$ for $V = H_L(T)$. If H is ϵ-AU, this clearly has security bound of $O(\epsilon q^2)$ which implies $m/2$-bit security at best. Then, what will happen if we use both solutions all together? In the next section we show that in fact this combination gives a better result.

3.2 XTX

We describe our proposal. Let $\widetilde{E} : \mathcal{K} \times \mathcal{V} \times \mathcal{M} \to \mathcal{M}$ be a TBC of message space $\mathcal{M} = \{0,1\}^n$ and tweak space $\mathcal{V} = \{0,1\}^m$. Let $\mathcal{T}$ be another (larger) tweak space. Let $H : \mathcal{L} \times \mathcal{T} \to \mathcal{M} \times \mathcal{V}$ be a function keyed by $L \in_{\mathrm{U}} \mathcal{L}$. We define $\mathrm{XTX} : (\mathcal{K} \times \mathcal{L}) \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$ be a TBC of message space $\mathcal{M}$ and tweak space $\mathcal{T}$ and key space $(\mathcal{K} \times \mathcal{L})$, using $\widetilde{E}$ and H, such that

$$\mathrm{XTX}^T_{K,L}(M) = \widetilde{E}^V_K(M \oplus W) \oplus W, \text{ where } (W,V) = H_L(T). \tag{9}$$

Fig. 1 shows the scheme. For security we need that H is a variant of ϵ-AXU function defined as follows.

Definition 2. *Let H be a keyed function $H : \mathcal{L} \times \mathcal{T} \to \{0,1\}^n \times \{0,1\}^m$. We say H is (n,m,ϵ)-partial AXU ((n,m,ϵ)-pAXU) if it satisfies*

$$\max_{\substack{x,x' \in \mathcal{T}, x \ne x' \\ \Delta \in \{0,1\}^n}} \Pr_L[H_L(x) \oplus H_L(x') = (\Delta, 0^m)] \le \epsilon. \tag{10}$$

Clearly an ϵ-AXU function of $(n+m)$-bit output is also (n,m,ϵ)-pAXU.

A change of a tweak in XTX affects to both block and tweak of inner TBC, whereas in LRW or XEX it affects only to input block, and in Coron et al.'s

[4] Originally proved by [17] with a slightly larger constant, then improved by [22].

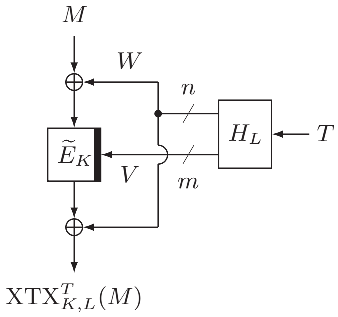

Fig. 1. XTX. A thick black line in $\widetilde{E}$ denotes tweak input.

method it affects only to inner tweak. XTX's structure is somewhat similar to a construction of (n, n)-bit TBC presented by Mennink [20], though [20] was based on ideal-cipher model, while XTX works on standard model and has no limitation on the outer tweak length. As well as LRW, XTX needs two keys. However it can be easily reduced to one by reserving one tweak bit for key generation. For instance, when $\mathcal{L} = \{0,1\}^n$, we let $L = \widetilde{E}^{(0^m)}(0^n)$ and use $(n, m-1)$-bit TBC defined as $\widetilde{E}^{(*\|1)}(*)$.

3.3 Security

We prove the security of XTX when underlying TBC is perfect, i.e. a TURP.

Theorem 1. *Let* $\mathrm{XTX}_{\widetilde{\mathsf{P}},L}$ *be* XTX *using* (n, m)*-bit tweakable URP,* $\widetilde{\mathsf{P}}$*, and* $H : \mathcal{L} \times \mathcal{T} \to \{0,1\}^n \times \{0,1\}^m$ *for tweak space* $\mathcal{T}$ *with independent key* $L \in_{\mathrm{U}} \mathcal{L}$*. Then we have*

$$\mathtt{Adv}^{\mathtt{tsprp}}_{\mathrm{XTX}_{\widetilde{\mathsf{P}},L}}(\mathcal{A}) \le \epsilon \cdot q^2, \tag{11}$$

for any CCA-adversary $\mathcal{A}$ *using* q *queries if* H *is* (n, m, ϵ)*-pAXU.*

In particular, when $\mathcal{T} = \{0,1\}^\ell$ for some ℓ and H is $\mathsf{Poly}[n+m]$, we have $\mathtt{Adv}^{\mathtt{tsprp}}_{\mathrm{XTX}_{\widetilde{\mathsf{P}},L}}(\mathcal{A}) \le \ell_{n+m} q^2/2^{n+m}$ from Theorem 1 and Proposition 1.

3.4 Proof of Theorem 1

Overview. Following the proof of LRW [22], our proof is based on the method developed by Maurer [18][5], though other methods such as game-playing proof [6]

[5] In some special cases the result obtained by the method of [18] cannot be converted into computational counterparts [25, 19]. However the proof presented here does not have such difficulty. A bug in a theorem of [18] was pointed out by Jetchev, Özen and Stam [14], however we did not use it.

or Coefficient-H technique [24] can be used as well. Basically, the proof is an extension of LRW proofs [17, 22], which shows that the advantage is bounded by the probability of "bad" event, defined as a non-trivial input collision in the underlying blockcipher of LRW. Intuitively, the security bound of XTX is obtained by extending this observation, and we can set "bad" event as non-trivial, simultaneous collisions of input *and* tweak in the underlying TBC.

Proof. We start with basic explanations on Maurer's method. They are mostly the same as those of [18], with minor notational changes. Consider the game that an adversary tries to distinguish two keyed functions, F and G, with queries. The game we consider is information-theoretic, that is, adversary has no computational limitation and F and G have no computational assumption, say, they are URF or URP. There may be some conditions of valid adversaries, e.g. no repeating queries etc. Let α_i denote an event defined at time i, i.e. when adversary performs i-th query and receives a response from oracle. Let $\overline{\alpha_i}$ be the negation of α_i. We assume α_i is monotone, i.e., α_i never occurs if $\overline{\alpha_{i-1}}$ occurs. For instance, α_i is monotone if it indicates that all i outputs are distinct. An infinite sequence of monotone events $\alpha = \alpha_0\alpha_1\dots$ is called a *monotone event sequence* (MES). Here, α_0 denotes some tautological event. Note that $\alpha \wedge \beta = (\alpha_0 \wedge \beta_0)(\alpha_1 \wedge \beta_1)\dots$ is a MES if $\alpha = \alpha_0\alpha_1\dots$ and $\beta = \beta_0\beta_1\dots$ are both MESs. Here we may abbreviate $\alpha \wedge \beta$ as $\alpha\beta$. For any sequence of random variables, $X_1, X_2, \dots$, let X^i denote $(X_1, \dots, X_i)$. We use $\mathrm{dist}(X^i)$ to denote that $X_1, X_2, \dots, X_i$ are distinct. We also write $\mathrm{dist}((X, Y)^i)$ to denote that $(X_1, Y_1), \dots, (X_i, Y_i)$ are distinct. Let MESs α and β be defined for two keyed functions, $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ and $G : \mathcal{K}' \times \mathcal{X} \to \mathcal{Y}$, respectively. For simplicity, we omit the description of keys in this explanation. Let $X_i \in \mathcal{X}$ and $Y_i \in \mathcal{Y}$ be the i-th input and output. Let P^F be the probability space defined by F. For example, $P^F_{Y_i|X^iY^{i-1}}(y^i, x^i)$ means $\Pr[Y_i = y_i|X^i = x^i, Y^{i-1} = y^{i-1}]$ where $Y_j = F(X_j)$ for $j \geq 1$. If $P^F_{Y_i|X^iY^{i-1}}(y^i, x^i) = P^G_{Y_i|X^iY^{i-1}}(y^i, x^i)$ for all possible (y^i, x^i), i.e. all assignments for which probabilities are defined, then we write $P^F_{Y_i|X^iY^{i-1}} = P^G_{Y_i|X^iY^{i-1}}$. Inequalities such as $P^F_{Y_i|X^iY^{i-1}} \leq P^G_{Y_i|X^iY^{i-1}}$ are similarly defined. Using MES $\alpha = \alpha_0\alpha_1, \dots$ and $\beta = \beta_0\beta_1, \dots$ defined for F and G we define the following notations, which will be used in our proof.

Definition 3. *We write $F^\alpha \equiv G^\beta$ if $P^F_{Y_i\alpha_i|X^iY^{i-1}\alpha_{i-1}} = P^G_{Y_i\beta_i|X^iY^{i-1}\beta_{i-1}}$ holds for all $i \geq 1$, which means $P^F_{Y_i\alpha_i|X^iY^{i-1}\alpha_{i-1}}(y^i, x^i) = P^G_{Y_i\beta_i|X^iY^{i-1}\beta_{i-1}}(y^i, x^i)$ holds for all possible (y^i, x^i) such that both $P^F_{\alpha_{i-1}|X^{i-1}Y^{i-1}}(y^{i-1}, x^{i-1})$ and $P^G_{\beta_{i-1}|X^{i-1}Y^{i-1}}(y^{i-1}, x^{i-1})$ are positive.*

Definition 4. *We write $F|\alpha \equiv G|\beta$ if $P^F_{Y_i|X^iY^{i-1}\alpha_i} = P^G_{Y_i|X^iY^{i-1}\beta_i}$ holds for all $i \geq 1$.*

In general if $F^\alpha \equiv G^\beta$, then $F|\alpha \equiv G|\beta$ holds, but not vice versa.

Definition 5. *We define $\nu(F, \overline{\alpha_q})$ as the maximal probability of $\overline{\alpha_q}$ for any adversary using q queries to F, considered as valid in the definition of game, which we assume clear in the context.*

Theorem 2. *(Theorem* 1 (i) *of [18]) If $F^{\alpha} \equiv G^{\beta}$ or $F|\alpha \equiv G$ holds, we have $\mathtt{Adv}^{\mathtt{cpa}}_{F,G}(\mathcal{A}) \le \nu(F, \overline{\alpha_q})$ for any adversary using q queries.*

We also use the following two lemmas of [18].

Lemma 1. *(Lemma* 1 (iv) *of [18]) Let MESs α and β be defined for F and G. Moreover, let X_i and Y_i denote the i-th input and output of F (or G), respectively. Assume $F|\alpha \equiv G|\beta$. If $P^F_{\alpha_i|X^iY^{i-1}\alpha_{i-1}} \le P^G_{\beta_i|X^iY^{i-1}\beta_{i-1}}$ for $i \ge 1$, which means $P^F_{\alpha_i|X^iY^{i-1}\alpha_{i-1}}(x^i, y^{i-1}) \le P^G_{\beta_i|X^iY^{i-1}\beta_{i-1}}(x^i, y^{i-1})$ holds for all (x^i, y^{i-1}) such that $P^F_{\alpha_{i-1}|X^{i-1}Y^{i-1}}(x^{i-1}, y^{i-1})$ and $P^G_{\beta_{i-1}|X^{i-1}Y^{i-1}}(x^{i-1}, y^{i-1})$ are positive. Then there exists an MES γ defined for G such that $F^{\alpha} \equiv G^{\beta\gamma}$.*

Lemma 2. *(Lemma* 6 (iii) *of [18]) $\nu(F, \overline{\alpha_q \wedge \beta_q}) \le \nu(F, \overline{\alpha_q}) + \nu(F, \overline{\beta_q})$.*

Analysis of XTX. We abbreviate $\mathrm{XTX}_{\widetilde{\mathsf{P}},L}$ to XTX_1. We define XTX_2 be TURP with tweak space $\mathcal{T}$. What is needed is the indistinguishability of XTX_1 and XTX_2 for CCA adversary.

We write the adversary's query as $\mathbf{X}_i = (X_i, T_i, B_i) \in \{0,1\}^n \times \mathcal{T} \times \{0,1\}$. Here $B_i = 0$ ($B_i = 1$) indicates that i-th query is an encryption (a decryption) query. Let $Y_i \in \{0,1\}^n$ be the corresponding response and we write $H_L(T_i) = (W_i, V_i)$ following (9). We also assume XTX_2 has computation of $H_L(T_i) = (W_i, V_i)$ as dummy, using independent and uniform sampling of L. In XTX_2, W_i and V_i are not used in the computation of Y_i. We write the set of scripts for all $i = 1, \dots, j$-th queries as $Z^j = (\mathbf{X}_1, \dots, \mathbf{X}_j, Y_1, \dots, Y_j)$. We may use M_i to denote X_i when $B_i = 0$ or Y_i when $B_i = 1$, and use C_i to denote Y_i when $B_i = 0$ or X_i when $B_i = 1$. We say Z^j is valid if $T_i = T_j$ and $M_i \ne M_j$ ($C_i \ne C_j$) then $C_i \ne C_j$ ($M_i \ne M_j$) holds. We note that a transcript which is not valid is one that cannot be obtained from a TBC.

We define $S_i = M_i \oplus W_i$ and $U_i = C_i \oplus W_i$ for both XTX_1 and XTX_2. They correspond to the input and output of $\widetilde{\mathsf{P}}$ in XTX_1, and dummy variables in XTX_2. MESs are defined as $\alpha_q = \mathrm{dist}((S, V)^q)$ and $\beta_q = \mathrm{dist}((U, V)^q)$. We observe that in XTX_1, α_q and β_q are equivalent, however not equivalent in XTX_2. Let us define $D(V_q) \overset{\mathrm{def}}{=} \{1 \le i < q : V_i = V_q\}$ and for n-bit variable $A \in \{X, Y, W, S, U\}$ define $A[D(V_q)] \overset{\mathrm{def}}{=} \{A_i : i \in D(V_q)\}$. Here $A[D(V_q)]^c = \{0,1\}^n \setminus A[D(V_q)]$. Fig. 2 shows XTX_1 with the labels mentioned above.

We investigate the distribution $P^G_{Y_q|Z^{q-1}\mathbf{X}_q\alpha_q\beta_q}$ for $G \in \{\mathrm{XTX}_1, \mathrm{XTX}_2\}$. We have

$$P^G_{Y_q|Z^{q-1}\mathbf{X}_q\alpha_q\beta_q} = \sum_{L} P^G_{Y_q|Z^{q-1}\mathbf{X}_q\alpha_q\beta_q L} \cdot P^G_{L|Z^{q-1}\mathbf{X}_q\alpha_q\beta_q}, \tag{12}$$

where the summation is taken for all values of $L = l$. We first focus on the term $P^G_{L|Z^{q-1}\mathbf{X}_q\alpha_q\beta_q}$. Let us assume $B_q = 0$. For both $G = \mathrm{XTX}_1$ and XTX_2,

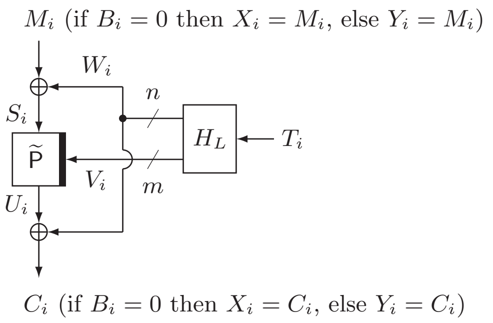
M_i (if $B_i = 0$ then $X_i = M_i$, else $Y_i = M_i$)
W_i
n
S_i
$\widetilde{\mathsf{P}}$
H_L
T_i
V_i
m
U_i
C_i (if $B_i = 0$ then $X_i = C_i$, else $Y_i = C_i$)

Fig. 2. XTX_1 with labels used in the proof of Theorem 1.

L is uniform over all values consistent with the conditional clause (note that L defines W^q, V^q, S^q and U^{q-1}, thus α_q and β_{q-1} are deterministic events given L). Hence we have

$$P^{\mathrm{XTX}_1}_{L|Z^{q-1}\mathbf{X}_q\alpha_q\beta_q} = P^{\mathrm{XTX}_2}_{L|Z^{q-1}\mathbf{X}_q\alpha_q\beta_q}. \tag{13}$$

For $P^G_{Y_q|Z^{q-1}\mathbf{X}_q\alpha_q\beta_q L}$, if $B_q = 0$ and $G = \mathrm{XTX}_1$, U_q is uniform over $\mathcal{U} \stackrel{\mathrm{def}}{=} U[D(V_q)]^c$, thus $Y_q = C_q = U_q \oplus W_q$ is uniform over $\mathcal{U} \oplus W_q$. If $B_q = 0$ and $G = \mathrm{XTX}_2$ and there is no conditional clause $\alpha_q\beta_q$, $Y_q(= C_q)$ is uniform over $\mathcal{C} \stackrel{\mathrm{def}}{=} C[D(T_q)]^c$. Here U_q is uniform over

$$\{C_i \oplus W_q : i \in D(T_q)\}^c = \{C_i \oplus W_i : i \in D(T_q)\}^c = \{U_i : i \in D(T_q)\}^c. \tag{14}$$

With condition $\alpha_q\beta_q$ (here only β_q is relevant since α_q is deterministic given L), U_i for $i \in D(V_q)$ (but $T_i \neq T_q$) is further removed from possible values for U_q, hence U_q is uniform over $\mathcal{U} = U[D(V_q)]^c$ and Y_q is uniform over $\mathcal{U} \oplus W_q$. Therefore C_q's distributions are identical for both XTX_1 and XTX_2. The same analysis holds for the case $B_q = 1$, and we have

$$P^{\mathrm{XTX}_1}_{Y_q|Z^{q-1}\mathbf{X}_q\alpha_q\beta_q L} = P^{\mathrm{XTX}_2}_{Y_q|Z^{q-1}\mathbf{X}_q\alpha_q\beta_q L}. \tag{15}$$

Thus Y_q's distributions are identical for both XTX_1 and XTX_2 if conditioned by $\alpha_q\beta_q$ and $L = l$ for any l. Therefore from (13) and (15) we have

$$P^{\mathrm{XTX}_1}_{Y_q|Z^{q-1}\mathbf{X}_q\alpha_q\beta_q} = P^{\mathrm{XTX}_2}_{Y_q|Z^{q-1}\mathbf{X}_q\alpha_q\beta_q}, \text{ that is, } \mathrm{XTX}_1|\alpha\beta \equiv \mathrm{XTX}_2|\alpha\beta. \tag{16}$$

Let us assume $B_q = 0$, and we focus on $p(G) = P^G_{\alpha_q\beta_q|Z^{q-1}\mathbf{X}_q\alpha_{q-1}\beta_{q-1}L}$. Note that the conditional clause uniquely determines whether α_q holds or not. If α_q does not hold, $p(G) = 0$ for both $G = \mathrm{XTX}_1$ or XTX_2. If α_q holds, $p(\mathrm{XTX}_1) = 1$ as $\beta_q \equiv \alpha_q$ in XTX_1, however $p(\mathrm{XTX}_2) < 1$ since β_q depends on U_q which is not determined by the conditional clause. This shows that

$$P^{\mathrm{XTX}_2}_{\alpha_q\beta_q|Z^{q-1}\mathbf{X}_q\alpha_{q-1}\beta_{q-1}L} \leq P^{\mathrm{XTX}_1}_{\alpha_q\beta_q|Z^{q-1}\mathbf{X}_q\alpha_{q-1}\beta_{q-1}L}. \tag{17}$$

Moreover using similar argument as (12), we have

$$P^{\mathrm{XTX}_1}_{L|Z^{q-1}\mathbf{X}_q\alpha_{q-1}\beta_{q-1}} = P^{\mathrm{XTX}_2}_{L|Z^{q-1}\mathbf{X}_q\alpha_{q-1}\beta_{q-1}}. \tag{18}$$

Thus, from (17) and (18), we have

$$P^{\mathrm{XTX}_2}_{\alpha_q\beta_q|Z^{q-1}\mathbf{X}_q\alpha_{q-1}\beta_{q-1}} \leq P^{\mathrm{XTX}_1}_{\alpha_q\beta_q|Z^{q-1}\mathbf{X}_q\alpha_{q-1}\beta_{q-1}}. \tag{19}$$

From (16) and (19) and Lemma 1, we observe that $\mathrm{XTX}_1^{\alpha\beta\gamma} \equiv \mathrm{XTX}_2^{\alpha\beta}$ holds true for some MES γ. With this equivalence, Theorem 2 and Lemma 2, we have

$$\mathtt{Adv}^{\mathtt{cca}}_{\mathrm{XTX}_1,\mathrm{XTX}_2}(\mathcal{A}) \leq \nu(\mathrm{XTX}_2, \overline{\alpha_q \wedge \beta_q}) \leq \nu(\mathrm{XTX}_2, \overline{\alpha_q}) + \nu(\mathrm{XTX}_2, \overline{\beta_q}) \tag{20}$$

for any CCA adversary $\mathcal{A}$ using q queries.

Let $\mathrm{XTX}_2[\widetilde{p}]$ be XTX_2 using a fixed tweakable permutation $\widetilde{p} \in \mathrm{Perm}^{\mathcal{T}}(n)$. We observe that the last two terms of (20) are bounded as

$$\nu(\mathrm{XTX}_2, \overline{\alpha_q}) \leq \max_{\widetilde{p} \in \mathrm{Perm}^{\mathcal{T}}(n)} \nu(\mathrm{XTX}_2[\widetilde{p}], \overline{\alpha_q}) \tag{21}$$

$$\nu(\mathrm{XTX}_2, \overline{\beta_q}) \leq \max_{\widetilde{p} \in \mathrm{Perm}^{\mathcal{T}}(n)} \nu(\mathrm{XTX}_2[\widetilde{p}], \overline{\beta_q}). \tag{22}$$

As $\widetilde{p}$ is fixed, the adversary can evaluate it without oracle access, hence the right hand side terms of (21) are obtained by considering the maximum of possible and valid (M^q, T^q, C^q). For fixed (M^q, T^q, C^q), the probabilities of $\overline{\alpha_q}$ and $\overline{\beta_q}$ are determined by W^q and V^q. Thus, for any $\widetilde{p}$ we have

$$\begin{aligned}
&\nu(\mathrm{XTX}_2[\widetilde{p}], \overline{\alpha_q}) \\
&\leq \max_{\substack{(M^q,T^q,C^q)\\ \text{valid}}} \Pr_{\substack{(W^q,V^q)\\ (W_i,V_i)=H_L(T_i)}} \left[{}^{\exists} i,j, \text{ s.t. } (W_i \oplus W_j = M_i \oplus M_j) \wedge (V_i = V_j)\right] \\
&\leq \binom{q}{2} \cdot \epsilon, \text{ and} \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (23)\\
&\nu(\mathrm{XTX}_2[\widetilde{p}], \overline{\beta_q}) \\
&\leq \max_{\substack{(M^q,T^q,C^q)\\ \text{valid}}} \Pr_{\substack{(W^q,V^q)\\ (W_i,V_i)=H_L(T_i)}} \left[{}^{\exists} i,j, \text{ s.t. } (W_i \oplus W_j = C_i \oplus C_j) \wedge (V_i = V_j)\right] \\
&\leq \binom{q}{2} \cdot \epsilon, \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (24)
\end{aligned}$$

since H is (n, m, ϵ)-pAXU. From (20) and (23) and (24), we conclude the proof. □

Tightness of our bound. We note that the bound is tight in the sense that we have an attack with about $q = O(2^{(n+m)/2})$ queries. The attack is simple, and let $M = 0^n$. The adversary makes q encryption queries $(M, T_1), \ldots, (M, T_q)$, where $T_1, \ldots, T_q$ are distinct tweaks. With a high probability, we have i and j such that $C_i = C_j$, where C_i is the ciphertext for (M, T_i) and C_j is that for (M, T_j). Now, the adversary can make two more encryption queries (M', T_j) and (M', T_j) for any $M' \neq M$, and see if the corresponding ciphertexts collide, in which case, with a high probability, the oracle is the tweakable blockcipher.

The attack works since in the ideal case, there exit i and j such that $C_i = C_j$ with a non-negligible probability, but we have the collision between ciphertexts of (M', T_i) and (M', T_j) with only a negligible probability.

4 Applications

Suppose we have an (n, m)-bit TBC $\widetilde{E}$ and want to extend tweak by applying XTX. We first remark if $\widetilde{E}$ is obtained by LRW this is almost pointless because $\widetilde{E}$ itself has only security up to the birthday bound. In this case a simple solution would be to extend the input domain of UH function used in LRW. However if $\widetilde{E}$ is a dedicated TBC, or a mode of operation having security beyond the birthday bound, application of XTX to $\widetilde{E}$ can have practical merits.

4.1 Dedicated TBC

Let us assume $\widetilde{E}$ is an (n, m)-bit dedicated TBC. As mentioned, using $\widetilde{E}$ with fixed tweak then applying LRW with some UH function only provides $n/2$-bit security, and Coron's method only provides $m/2$-bit security, while XTX provides $(n+m)/2$-bit security. For example, KIASU-BC [13] is a $(128, 64)$-bit TBC based on AES. By combining XTX using H as $\mathsf{Poly}[192]$ or $\mathsf{Poly}[64, 64, 64]$ we obtain a TBC of longer tweak with 96-bit security with respect to the number of queries, while previous methods provide 64 or 32-bit security. Similarly, a $(256, 128)$-bit TBC version of Threefish can be conveted into a TBC of longer tweak having 192-bit security, using XTX with H being $\mathsf{Poly}[384]$ or $\mathsf{Poly}[128, 128, 128]$.

We remark that the use of $\mathsf{Poly}[m, m, m]$ for $m = n/3$ instead of $\mathsf{Poly}[n + m]$ can reduce the implementation size and gain efficiency. For example Aoki and Yasuda [3] proposed to use $\mathsf{Poly}[n/2, n/2]$ instead of $\mathsf{Poly}[n]$ used in GCM authenticated encryption. A drawback is that it will increase the advantage with respect to tweak length, from linear to cubic in our case (though we assumed it as a constant in Section 2.1). Therefore, the use of a polynomial hash function with a small field is not desirable if the impact of such increase is not negligible. In addition we have to be careful with the existence of weak keys in polynomial hash function pointed out by Procter and Cid [27].

4.2 Rekeying construction

Minematsu's rekeying construction for TBC [23] is described as follows. Using a blockcipher $E : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{M}$ with $\mathcal{K} = \mathcal{M} = \{0, 1\}^n$, [23] builds a (n, m)-bit TBC for $m < n$ such that

$$\mathsf{Min}_K^T(M) = E_{K'_T}(M) \text{ where } K'_T = E_K(T \| 0^{n-m}). \tag{25}$$

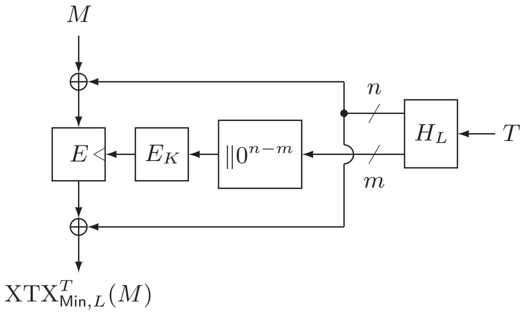

Fig. 3. XTX applied to Minematsu's TBC.

The security bound of this construction is as follows. For any $\mathcal{A}$ using q queries with τ time, we have another adversary $\mathcal{B}$ using q queries with $\tau' = \tau + O(q)$ time such that $\mathtt{Adv}^{\mathtt{tsprp}}_{\mathsf{Min}}(\mathcal{A}) \leq (\eta+1)\mathtt{Adv}^{\mathtt{sprp}}_{E}(\mathcal{B}) + \frac{\eta^2}{2^{n+1}}$, where $\eta = \min\{q, 2^m\}$. As analyzed by [23] this can provide a TBC with beyond-birthday security when $m < n/2$. In particular [23] suggested $m = n/3$ which provides security against $2^{n-m} = 2^{2n/3}$ queries. Despite the simple construction, one big shortcoming is its short tweak length, as mentioned by (e.g.) [20, 15, 16]. This is, however, recovered if (25) is combined with XTX. Let $\mathrm{XTX}_{\mathsf{Min},L}$ be XTX with internal TBC being Min having n-bit block, m-bit tweak using n-bit blockcipher E. Here we assume that tweak space of $\mathrm{XTX}_{\mathsf{Min},L}$ is $\mathcal{T} = \{0,1\}^{\ell}$, and underlying $H : \mathcal{L} \times \mathcal{T} \to \{0,1\}^{n+m}$ is $\mathsf{Poly}[n+m]$. Then for any adversary $\mathcal{A}$ using q queries and τ time, from (25) and Proposition 1 and Theorem 1, we have

$$\mathtt{Adv}^{\mathtt{tsprp}}_{\mathrm{XTX}_{\mathsf{Min},L}}(\mathcal{A}) \leq (\eta+1)\mathtt{Adv}^{\mathtt{sprp}}_{E}(\mathcal{B}) + \frac{\eta^2}{2^{n+1}} + \frac{\ell_{n+m}q^2}{2^{n+m}}, \tag{26}$$

for some adversary $\mathcal{B}$ using q queries with $\tau + O(q)$ time, where $\eta = \min\{q, 2^m\}$ as above. For choosing m, we can assume that $\mathtt{Adv}^{\mathtt{sprp}}_{E}(\mathcal{B})$ is at least $q/2^n$ for adversary $\mathcal{B}$ using q queries and τ time when q is about τ (since E has n-bit key and $\mathcal{B}$ can perform exhaustive key search, as observed by Bellare et al. [5]). Ignoring ℓ_{n+m} and substituting η with 2^m in the bound, the first and last terms are about $q/2^{n-m}$ and $q^2/2^{n+m}$. Then $m = n/3$ is a reasonable choice which makes these terms $(q/2^{2n/3})^i$ for $i = 1$ and $i = 2$. This shows that we can extend tweak keeping the original security of rekeying construction. The resulting scheme is shown in Fig. 3, where a triangle in E denotes key input, and H_L denotes $\mathsf{Poly}[n+m]$. Still, we need rekeying for each tweak and this can be another drawback for performance.

4.3 Chained LRW

A provably-secure TBC construction which does not rely on rekeying construction [23] was first proposed by Landecker et al. [16]. It is an independently-keyed chain of LRW, and is called[6] CLRW2. Assuming LRW shown as (7) using $H : \mathcal{L} \times \mathcal{T} \to \mathcal{M}$ and $E : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$ for $\mathcal{M} = \{0,1\}^n$ and $\mathcal{T} = \{0,1\}^\ell$ as underlying components, they proposed the construction described as

$$\mathrm{CLRW2}^T_{K_1,K_2,L_1,L_2}(M) = \mathrm{LRW}^T_{K_2,L_2}(\mathrm{LRW}^T_{K_1,L_1}(M)). \tag{27}$$

The authors proved[7] that its TSPRP-advantage is $O(q^3\epsilon^2)$ when H is ϵ-AXU. More formally, TSPRP-advantage is at most $8q^3\hat{\epsilon}^2/(1-q^3\hat{\epsilon}^2)$ where $\hat{\epsilon}$ is defined as $\max\{\epsilon, 1/(2^n - 2q)\}$. Thus, assuming $\hat{\epsilon} = \epsilon$ and the denominator being larger than 1/2, the bound is at most

$$16q^3\epsilon^2. \tag{28}$$

If H is $\mathsf{Poly}[n]$, we have $\epsilon = \ell_n/2^n$, then the bound is $16q^3\ell_n^2/2^{2n}$. In this case CLRW2 needs $2\ell_n$ GF(2^n) multiplications for each ℓ-bit tweak.

A natural extension of CLRW2, i.e. a longer chain more than two, was proposed by Lampe and Seurin [15]. The construction for r chains is simply described as r-$\mathrm{CLRW}^T_{K_1,\ldots,K_r,L_1,\ldots,L_r}(M)$ in the same manner to (27), where 2-CLRW is equivalent to CLRW2. If r blockciphers are independent URPs, they proved that r-CLRW for any even r has TSPRP-advantage of

$$c_r q^{\frac{(r+2)}{4}} \epsilon^{\frac{r}{4}}, \text{ where } c_r = \frac{4\sqrt{2}}{\sqrt{r+2}} \cdot 2^{\frac{r}{4}}, \tag{29}$$

when the underlying $H : \mathcal{L} \times \mathcal{T} \to \mathcal{M}$ is ϵ-AXU. If $\mathcal{T}$ is $\{0,1\}^\ell$ and H is $\mathsf{Poly}[n]$, the bound is

$$\frac{c_r q^{\frac{(r+2)}{4}} \ell_n^{\frac{r}{4}}}{2^{\frac{nr}{4}}}. \tag{30}$$

Let r-CLRW(m) be the r-CLRW with n-bit blockcipher E_K and m-bit tweak (for some fixed $m > 0$) processed by independently-keyed r instances of $\mathsf{Poly}[n]$. We note that r-CLRW(ℓ) needs $r\ell_n$ multiplications over GF(2^n).

r-CLRW combined with XTX. Let $r > 2$ be an even integer. We apply XTX with H being $\mathsf{Poly}[n,n]$ using two keys in GF(2^n) to r-CLRW(n), to build an (n,ℓ)-bit TBC. The resulting scheme uses $r + 2\ell_n$ GF(2^n) multiplications, hence uses fewer multiplications than r-CLRW(ℓ) if $\ell_n > 1$ and $r \geq 4$. See Fig. 4 for the combined scheme. From Theorem 1, Proposition 1 and (30), TSPRP-advantage of the resulting scheme is

$$\frac{c_r q^{\frac{(r+2)}{4}}}{2^{\frac{nr}{4}}} + \frac{\ell_n^2 q^2}{2^{2n}}. \tag{31}$$

[6] The name CLRW2 means it is a chain of the second construction of [17], which we simply call LRW.

[7] Originally the constant was 6, however an error in the proof was pointed out by Procter [26]. He fixed the proof with an increased constant, 8.

This provides the same level of security as (30), unless ℓ_n is huge.

In case $r = 2$ the above combination gives no efficiency improvement. Still, by combining CLRW2(m) for some $m < n$ with XTX a slight improvement is possible. This is because CLRW2 needs two n-bit UH functions and the product of their biases is multiplied by q^3, while the bias of $(n + m)$-bit UH function in XTX is multiplied by q^2. For example, assuming n is divisible by 3, we set $m = n/3$, and consider CLRW2(m) using two $\mathsf{Poly}[n]$ (with padding of tweak), combined with XTX using $\mathsf{Poly}[n, m]$ to process ℓ-bit tweak. This requires ℓ_n GF(2^n) multiplications and $3\ell_n$ GF(2^m) multiplications. It is not straightforward to compare the complexity of one multiplication over GF(2^n) and three multiplications over GF(2^m), however, in most cases the latter is considered to be lighter than the former, though the gain will be depending on whether the underlying computing platform operates well over m-bit words. If this is the case our scheme will have a better complexity than the plain use of CLRW2.

As a more concrete example, let us consider CLRW2 using two instances of $\mathsf{Poly}[m, m, m]$ with $m = n/3$ (See the top of Fig. 5). For ℓ-bit tweak, this CLRW2 requires $2 \cdot 3 \cdot 3\ell_n = 18\ell_n$ multiplications over GF(2^m) and its TSPRP-advantage is, based on (28), at most

$$16 \cdot q^3 \left(\frac{(3\ell_n)^3}{(2^{\frac{n}{3}})^3} \right)^2 = \frac{11664 \cdot q^3 \cdot \ell_n^6}{2^{2n}}. \tag{32}$$

If we combine this instance of CLRW2(m) with XTX using $\mathsf{Poly}[m, m, m, m]$, then the advantage is at most

$$\frac{16 \cdot 729 q^3}{2^{2n}} + q^2 \frac{(3\ell_n)^4}{(2^{\frac{n}{3}})^4} = \frac{11664 q^3}{2^{2n}} + \frac{81 \ell_n^4 q^2}{2^{\frac{4n}{3}}}. \tag{33}$$

See the bottom of Fig. 5 for the resulting scheme. As shown by (32) and (33), for a moderate tweak length both bounds indicate the security against about $2^{2n/3}$ queries, while the combined scheme uses fewer GF(2^m) multiplications, i.e. $6 + 4 \cdot 3\ell_n = 6 + 12\ell_n$. For comparison of these two bounds, Fig. 6 shows the case of $n = 128$ and $\ell_n = 16$. In Fig. 6 both bounds are close but CLRW2 combined with XTX is slightly better.

5 Conclusion

In this paper, we have studied the problem of tweak extension for a tweakable blockcipher having fixed-length tweak. We proposed XTX as an effective solution to this problem, by extending the work of Liskov et al. XTX uses one call of a given tweakable blockcipher, $\widetilde{E}$, and a variant of universal hash function, H, for processing global tweak. When $\widetilde{E}$ has n-bit block and m-bit tweak, XTX provides $(n + m)/2$-bit security, which is better than the conventional methods known as Liskov et al.'s LRW or Corol et al.'s solution. The proposed method is useful in extending tweak of dedicated tweakable blockciphers, which typically have relatively short, fixed-length tweak. Moreover, XTX is even useful when

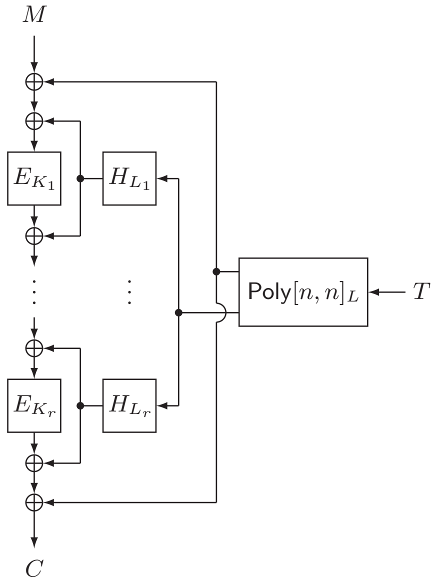

Fig. 4. r-CLRW with XTX, using $\mathsf{Poly}[n,n]$ as outer universal hash function.

applied to some blockcipher modes for tweakable blockcipher which have beyond-birthday-bound security. A natural open problem here is to find tweak extension schemes that have better security bounds than that of XTX.

Acknowledgments. The authors would like to thank the anonymous reviewers for highly constructive and insightful comments. The work by Tetsu Iwata was supported in part by JSPS KAKENHI, Grant-in-Aid for Scientific Research (B), Grant Number 26280045.

References

1. : CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness `http://competitions.cr.yp.to/caesar.html/`.
2. : Skein Hash Function. SHA-3 Submission (2008) `http://www.skein-hash.info/`.
3. Aoki, K., Yasuda, K.: The Security and Performance of "GCM" when Short Multiplications Are Used Instead. In Kutylowski, M., Yung, M., eds.: Information Security and Cryptology - 8th International Conference, Inscrypt 2012, Beijing, China, November 28-30, 2012, Revised Selected Papers. Volume 7763 of Lecture Notes in Computer Science., Springer (2012) 225–245
4. Bellare, M., Desai, A., Jokipii, E., Rogaway, P.: 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, IEEE Computer Society (1997) 394–403

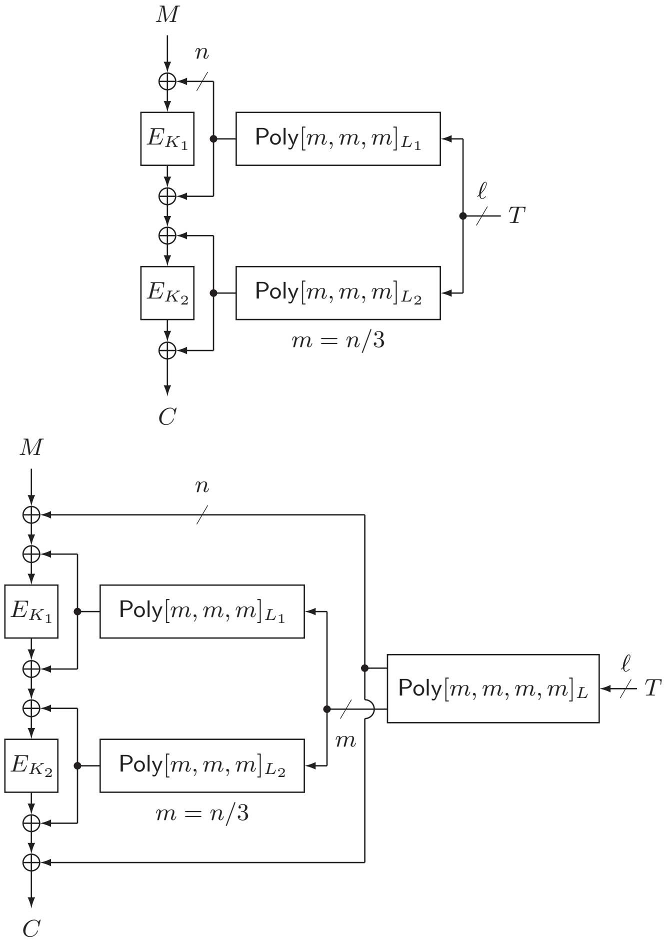
M
n
E_{K_1}
$\mathsf{Poly}[m,m,m]_{L_1}$
ℓ
T
E_{K_2}
$\mathsf{Poly}[m,m,m]_{L_2}$
$m = n/3$
C
M
n
E_{K_1}
$\mathsf{Poly}[m,m,m]_{L_1}$
$\mathsf{Poly}[m,m,m,m]_L$
ℓ
T
m
E_{K_2}
$\mathsf{Poly}[m,m,m]_{L_2}$
$m = n/3$
C

Fig. 5. (Top) CLRW2 using $\mathsf{Poly}[m,m,m]$. (Bottom) CLRW2 combined with XTX, where CLRW2 takes m-bit tweak using $\mathsf{Poly}[m,m,m]$, and XTX uses $\mathsf{Poly}[m,m,m,m]$ as outer universal hash function.

5. Bellare, M., Krovetz, T., Rogaway, P.: Luby-rackoff backwards: Increasing security by making block ciphers non-invertible. In Nyberg, K., ed.: Advances in Cryptology - EUROCRYPT '98, International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland, May 31 - June 4, 1998, Proceeding. Volume 1403 of Lecture Notes in Computer Science., Springer (1998) 266–280

6. Bellare, M., Rogaway, P.: The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs. In Vaudenay, S., ed.: Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings. Volume 4004 of Lecture Notes in Computer Science., Springer (2006) 409–426

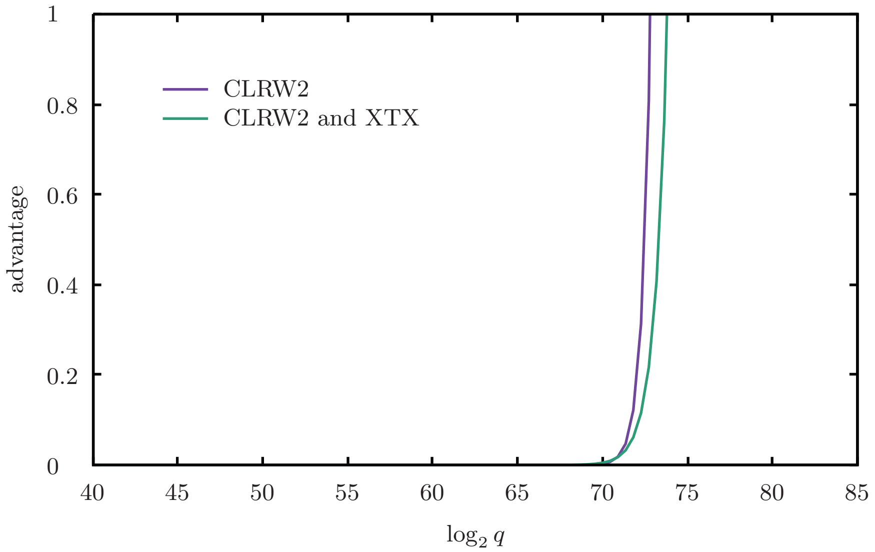

Fig. 6. Security bounds for CLRW2 and CLRW2 combined with XTX, shown in (32) and (33). Here, $n = 128$ and $\ell_n = 16$.

7. Carter, L., Wegman, M.N.: Universal Classes of Hash Functions. J. Comput. Syst. Sci. **18**(2) (1979) 143–154
8. Cogliati, B., Lampe, R., Seurin, Y.: Tweaking Even-Mansour Ciphers. CRYPTO 2015, to appear. Full version in Cryptology ePrint Archive, Report 2015/539 (2015) `http://eprint.iacr.org/`.
9. Coron, J., Dodis, Y., Mandal, A., Seurin, Y.: A Domain Extender for the Ideal Cipher. In Micciancio, D., ed.: Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010. Proceedings. Volume 5978 of Lecture Notes in Computer Science., Springer (2010) 273–289
10. Crowley, P.: Mercy: A Fast Large Block Cipher for Disk Sector Encryption. In Schneier, B., ed.: Fast Software Encryption, 7th International Workshop, FSE 2000, New York, NY, USA, April 10-12, 2000, Proceedings. Volume 1978 of Lecture Notes in Computer Science., Springer (2000) 49–63
11. Even, S., Mansour, Y.: A Construction of a Cipher from a Single Pseudorandom Permutation. J. Cryptology **10**(3) (1997) 151–162
12. Hirose, S., Sasaki, Y., Yasuda, K.: IV-FV Authenticated Encryption and Triplet-Robust Decryption. Early Symetric Crypto, ESC 2015 (2015)
13. Jean, J., Nikolic, I., Peyrin, T.: Tweaks and Keys for Block Ciphers: The TWEAKEY Framework. In Sarkar, P., Iwata, T., eds.: 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 II. Volume 8874 of Lecture Notes in Computer Science., Springer (2014) 274–288
14. Jetchev, D., Özen, O., Stam, M.: Understanding Adaptivity: Random Systems Revisited. In Wang, X., Sako, K., eds.: Advances in Cryptology - ASIACRYPT

2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings. Volume 7658 of Lecture Notes in Computer Science., Springer (2012) 313–330

15. Lampe, R., Seurin, Y.: Tweakable Blockciphers with Asymptotically Optimal Security. In Moriai, S., ed.: Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers. Volume 8424 of Lecture Notes in Computer Science., Springer (2013) 133–151
16. Landecker, W., Shrimpton, T., Terashima, R.S.: Tweakable Blockciphers with Beyond Birthday-Bound Security. In Safavi-Naini, R., Canetti, R., eds.: Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings. Volume 7417 of Lecture Notes in Computer Science., Springer (2012) 14–30
17. Liskov, M., Rivest, R.L., Wagner, D.: Tweakable Block Ciphers. In Yung, M., ed.: 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., Springer (2002) 31–46
18. Maurer, U.M.: Indistinguishability of Random Systems. In Knudsen, L.R., ed.: 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., Springer (2002) 110–132
19. Maurer, U.M., Pietrzak, K.: Composition of Random Systems: When Two Weak Make One Strong. In Naor, M., ed.: Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings. Volume 2951 of Lecture Notes in Computer Science., Springer (2004) 410–427
20. Mennink, B.: Optimally secure tweakable blockciphers. In Leander, G., ed.: Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers. Volume 9054 of Lecture Notes in Computer Science., Springer (2015) 428–448
21. Mennink, B.: XPX: generalized tweakable even-mansour with improved security guarantees. IACR Cryptology ePrint Archive **2015** (2015) 476
22. Minematsu, K.: Improved Security Analysis of XEX and LRW Modes. In Biham, E., Youssef, A.M., eds.: 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., Springer (2006) 96–113
23. Minematsu, K.: Beyond-Birthday-Bound Security Based on Tweakable Block Cipher. In Dunkelman, O., ed.: Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, February 22-25, 2009, Revised Selected Papers. Volume 5665 of Lecture Notes in Computer Science., Springer (2009) 308–326
24. Patarin, J.: The ”Coefficients H” Technique. In Avanzi, R.M., Keliher, L., Sica, F., eds.: 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., Springer (2008) 328–345
25. Pietrzak, K.: Composition Does Not Imply Adaptive Security. In Shoup, V., ed.: Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings. Volume 3621 of Lecture Notes in Computer Science., Springer (2005) 55–65
26. Procter, G.: A Note on the CLRW2 Tweakable Block Cipher Construction. IACR Cryptology ePrint Archive **2014** (2014) 111

27. Procter, G., Cid, C.: On Weak Keys and Forgery Attacks Against Polynomial-Based MAC Schemes. In Moriai, S., ed.: Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers. Volume 8424 of Lecture Notes in Computer Science., Springer (2013) 287–304
28. Rogaway, P.: Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In Lee, P.J., ed.: 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., Springer (2004) 16–31
29. Sasaki, Y., Todo, Y., Aoki, K., Naito, Y., Sugawara, T., Murakami, Y., Matsui, M., Hirose, S.: Minalpher. A submission to CAESAR competition.
30. Schroeppel, R.: Hasty Pudding Cipher. AES Submission (1998) `http://www.cs.arizona.edu/rcs/hpc/`.
31. Shrimpton, T., Terashima, R.S.: A Modular Framework for Building Variable-Input-Length Tweakable Ciphers. In Sako, K., Sarkar, P., eds.: Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I. Volume 8269 of Lecture Notes in Computer Science., Springer (2013) 405–423