IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2017, No. 2, pp. 1–26. DOI:10.13154/tosc.v2017.i2.1-26

Tweakable Blockciphers for Efficient Authenticated Encryptions with Beyond the Birthday-Bound Security

Yusuke Naito

Mitsubishi Electric Corporation, Kanagawa, Japan
Naito.Yusuke@ce.MitsubishiElectric.co.jp

Abstract. Modular design via a tweakable blockcipher (TBC) offers efficient authenticated encryption (AE) schemes (with associated data) that call a blockcipher once for each data block (of associated data or a plaintext). However, the existing efficient blockcipher-based TBCs are secure up to the birthday bound, where the underlying keyed blockcipher is a secure strong pseudorandom permutation. Existing blockcipher-based AE schemes with beyond-birthday-bound (BBB) security are not efficient, that is, a blockcipher is called twice or more for each data block.

In this paper, we present a TBC, XKX, that offers efficient blockcipher-based AE schemes with BBB security, by combining with efficient TBC-based AE schemes such as ΘCB3 and $\mathbb{OTR}$. XKX is a combination of two TBCs, Minematsu's TBC and Liskov et al.'s TBC. In the XKX-based AE schemes, a nonce and a counter are taken as tweak; a nonce-dependent blockcipher's key is generated by using a pseudo-random function F (from Minematsu); a counter is inputted to an almost xor universal hash function, and the hash value is xor-ed with the input and output blocks of a blockcipher with the nonce-dependent key (from Liskov et al.). For each query to the AE scheme, after the nonce-dependent key is generated, it can be reused, thereby a blockcipher is called once for each data block. We prove that the security bounds of the XKX-based AE schemes become roughly $\ell^2 q/2^n$, where q is the number of queries to the AE scheme, n is the blockcipher size, and ℓ is the number of blockcipher calls in one AE evaluation. Regarding the function F, we present two blockcipher-based instantiations, the concatenation of blockcipher calls, $F^{(1)}$, and the xor of blockcipher calls, $F^{(2)}$, where $F^{(i)}$ calls a blockcipher $i+1$ times. By the PRF/PRP switch, the security bounds of the XKX-based AE schemes with $F^{(1)}$ become roughly $\ell^2 q/2^n + q^2/2^n$, thus if $\ell \ll 2^{n/2}$ and $q \ll 2^{n/2}$, these achieve BBB security. By the xor construction, the security bounds of the XKX-based AE schemes with $F^{(2)}$ become roughly $\ell^2 q/2^n + q/2^n$, thus if $\ell \ll 2^{n/2}$, these achieve BBB security.

Keywords: Blockcipher · tweakable blockcipher · efficient authenticated encryption · beyond-birthday-bound security

1 Introduction

Confidentiality and authenticity of data are the most important properties to securely communicate over an insecure channel. In the symmetric-key setting, an authenticated encryption (AE) scheme (with associated data) ensures jointly these properties. AE schemes have been mainly designed from a blockcipher, and designing an efficient AE scheme is a main theme in AE research. In efficient schemes such as OCB3 [KR11] and OTR [Min14], a blockcipher is called once for each data block[1] (for associated data or a

[1] The size of the data block is equal to the block size of the blockcipher.

Received: 2017-03-01, Accepted: 2017-05-01, Published: 2017-06-19

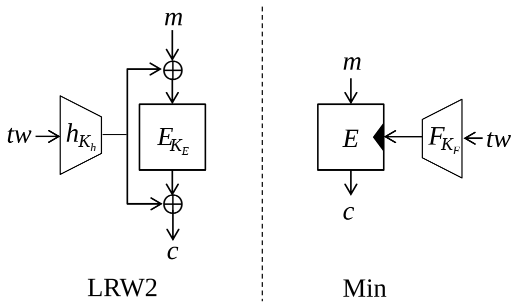

Figure 1: LRW2 (left) and Min (right).

plaintext). Such AE schemes that we call *efficient* AE schemes[2] have been designed via a *tweakable blockcipher*.

Tweakable blockcipher (TBC) whose concept was introduced by Liskov et al. [LRW02] is a generalization of classical blockcipher. An encryption by a TBC takes an input called tweak in addition to a key and a plaintext. Tweak is a public parameter, where retweaking (changing the tweak value) offers the same functionality as changing its secret key but should be less costly. An efficient blockcipher-based AE scheme is obtained by (1) designing an efficient TBC, that is, a blockcipher is called once; (2) designing an efficient TBC-based AE scheme, that is, a TBC is called once for each data block; (3) combining (1) and (2).

Regarding security, existing efficient blockcipher-based AE schemes are secure up to the *birthday bound*. However, birthday-bound security sometimes becomes unreliable, for example, when a lightweight blockcipher is used, when large amounts of data are processed, or when a large number of connections need to be kept secure. In (2) efficient TBC-based AE schemes with *beyond-birthday-bound* (BBB) security have been proposed such as ΘCB3 [KR11] and $\mathbb{OTR}$ [Min14], whereas in (1) existing efficient TBCs are secure up to the birthday bound. In order to obtain efficient BBB-secure AE schemes in (3), one needs to design a BBB-secure TBC in (1). Note that in (1), a keyed blockcipher is assumed to be a secure strong-pseudo-random permutation (SPRP),[3] and in (2), a keyed TBC is assumed to be a secure tweakable SPRP (TSPRP).[4] Hereafter, E_{K_E} denotes a blockcipher with n-bit block having a k-bit key K_E.

1.1 Existing Efficient TBCs with Birthday-Bound Security

Liskov et al. [LRW02] proposed an efficient blockcipher-based TBC called LRW2 that has an Even-Mansour-style structure [EM97], where a tweak is taken by an almost xor universal (AXU) hash function, and a plaintext and a ciphertext of the underlying blockcipher are xor-ed with the hash value. The encryption of LRW2 is illustrated in Figure 1 (Left), where tw is a tweak, m is a plaintext block, c is a ciphertext block, and h_{K_h} is an AXU hash function with a key K_h that accepts tw and returns an n-bit value. Regarding AXU hash functions, several efficient instantiations have been proposed such as powering-up scheme [Rog04], gray-code-based scheme [KR11, RBBK01] and LFSR-based scheme [CS08, GJMN16]. It was proven that LRW2 is a secure TSPRP up to the birthday bound ($2^{n/2}$ queries) [LRW02].

[2] The efficiency of AE schemes is often measured by "rate" that takes all blockcipher calls including a precomputation phase into consideration. For example, the most efficient AE scheme is rate-1, where the number of blockcipher calls in one AE procedure is the number of data blocks plus 2 (the number of blockcipher calls for a tag and for a nonce in a precomputation phase). On the other hand, the term "efficient" considered in this paper does not take the precomputation phase into account.

[3] A blockcipher with a random key is indistinguishable from a random permutation (RP).

[4] A TBC with a random key is indistinguishable from a tweakable RP.

1.2 BBB-Secure TBCs

So far, several BBB-secure TBCs have been proposed. Minematsu [Min09] designed a TBC denoted by Min. In Min, a tweak-dependent key is defined by using a pseudo-random function (PRF), and a plaintext is encrypted by a blockcipher with the tweak-dependent key. The encryption of Min is illustrated in Figure 1 (right), where F_{K_F} is a secure PRF with a key K_F. He gave a blockcipher-based instantiation: $F_{K_E}(tw) = E_{K_E}(tw)$, where $k = n$. He proved that Min is a secure TSPRP up to $\max\{2^{n/2}, 2^n/N_{tw}\}$ queries, where N_{tw} is the number of distinct tweaks in the queries. Thus if $N_{tw} < 2^{n/2}$, Min achieves BBB security. Landecker et al. [LST12] proposed a TBC called Chained LRW2 (CLRW2), where LRW2 is iterated twice. They proved that CLRW2 is a secure TSPRP up to $2^{2n/3}$ queries. Lampe and Seurin [LS13] considered a more general scheme called r-CLRW where LRW2 is iterated r times. They proved that r-CLRW is a secure TSPRP up to $2^{rn/(r+2)}$ queries.

1.3 Open Problem

In ΘCB3 and $\mathbb{OTR}$ that are efficient nonce-based and TBC-based AE schemes, a plaintext block is encrypted by a TBC that takes a nonce and a counter as tweak, where a nonce is changed for each query, and a counter is changed for each data block. Hence, a tweak is changed for every TBC call. Incorporating Min into these AE schemes, for each data block, the resultant schemes call a blockcipher twice, and perform the key scheduling once. Since the same tweak is not repeated, $N_{tw} = 2^{n/2}$ after $2^{n/2}$ TBC calls, and thus the security bound falls into the birthday one (security up to $2^{n/2}$ queries). Incorporating CLRW2 into these AE schemes, the resultant schemes achieve BBB security (security up to $2^{2n/3}$ queries) but call a blockcipher twice for each data block. Similarly, incorporating r-CLRW into these AE schemes, the resultant schemes achieve BBB security (security up to $2^{rn/(r+2)}$ queries) but call a blockcipher r times for each data block.

Several blockcipher-based AE schemes have been proposed, which are either efficient or BBB-secure but not both. Existing efficient blockcipher-based AE schemes [RBBK01, Rog04, KR11, Min14] are secure up to the birthday bound. Iwata [Iwa08] proposed an AE scheme that is secure up to $2^{2n/3}$ blockcipher calls. In the default setting of the AE scheme, for each 4 data blocks, it requires 6 blockcipher calls, and for each data block, it requires one multiplication. Iwata and Yasuda [IY09a, IY09b] pointed out that a combination of the xor of keyed blockciphers [Luc00] and the Feistel network with six rounds [Pat04] becomes a BBB-secure SPRP, thus offers BBB-secure AE schemes. However, the resultant AE schemes require 6 blockcipher calls for each data block. Iwata and Minematsu [IM16] proposed AE schemes that are secure up to $2^{rn/(r+1)}$ blockcipher calls for a parameter r. In the encryption procedure, for each data block, a blockcipher is called r times. A tag is generated by using r AXU-hash functions.

As mentioned above, there is no efficient blockcipher-based AE scheme with BBB security. Therefore, the following question arises: *Can we design a TBC that offers efficient blockcipher-based AE schemes with BBB security?*

1.4 Our Results

We present TBCs that offer efficient AE schemes with BBB security.

1.4.1 Basic Construction

Our TBCs are based on Minematsu's TBC Min. In order to avoid the frequent key scheduling, we separate counters from the tweak function F_{K_F}, and instead use the tweak function of LRW2 h_{K_h} to take counters. The basic construction of our TBCs that we call XKX is illustrated in Figure 2 (left), where (N, ctr) is a pair of tweaks such that the first

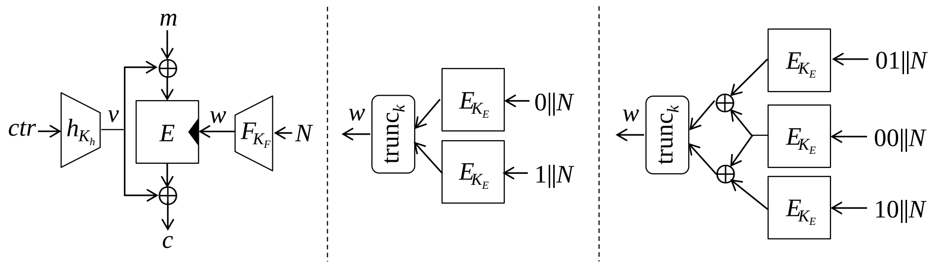

Figure 2: XKX (left), $F^{(1)}$ (center), $F^{(2)}$ (right).

tweak N becomes a nonce and the second one *ctr* becomes a counter. We prove that XKX is a secure TSPRP as long as the keyed blockcipher is a secure SPRP, the keyed function is a secure PRF, and the keyed hash function is AXU. The security bound is roughly $\ell^2 q/2^n$ + $q\times$(the SPRP-security advantage for E) + (the PRF-security advantage for F), where q is the number of distinct first tweaks (nonces in AE schemes), and ℓ is the number of queries with the same first tweak (the number of blockcipher calls in one AE evaluation). If the SPRP-security advantage becomes roughly $\ell q/2^k$ (an adversary conducts a naive brute-force attack, see [BKR98]), the security bound becomes $\ell^2 q/2^n + \ell q^2/2^k$ + (the PRF-security advantage for F).

1.4.2 Blockcipher-Based Instantiations

We give two blockcipher-based instantiations of F, where a blockcipher with $n \leq k \leq 2n$ is used.

- The first instantiation $F^{(1)}$, which is based on Minematsu's instantiation, is illustrated in Figure 2 (center), where $\mathsf{trunc}_k(x)$ outputs the first k bits of a $2n$-bit string x, and N is an (n-1)-bit tweak. By the PRF/PRP switch, the PRF-security advantage of $F^{(1)}$ is upper-bounded by $q^2/2^n$. Hence, incorporating $F^{(1)}$ into XKX, the security bound of the TBC becomes roughly $\ell^2 q/2^n + \ell q^2/2^k + q^2/2^n$. XKX with $F^{(1)}$ is denoted by XKX$^{(1)}$.

- The second instantiation $F^{(2)}$, in order to remove the PRF/PRP-switch term $q^2/2^n$, uses an xor function of a blockcipher shown in Figure 2 (right), where N is an (n-2)-bit tweak, and K_E is a k-bit key. The PRF-security of the xor function was analyzed in [Pat10, IMV16], where the PRF-bound is roughly $q/2^n$. Hence, incorporating $F^{(2)}$ into XKX, the security bound of the TBC becomes roughly $\ell^2 q/2^n + \ell q^2/2^k + q/2^n$. XKX with $F^{(2)}$ is denoted by XKX$^{(2)}$.

1.4.3 Applications

Incorporating XKX into AE schemes ΘCB3 and $\mathbb{OTR}$, the resultant schemes are efficient ones, since for a query to the AE scheme, after a nonce-dependent key w is defined, it can be reused. In order to generate the nonce-dependent key, for each query to the AE scheme, the XKX$^{(1)}$-based AE schemes call a blockcipher once ($k = n$); twice ($n < k \leq 2n$), and the XKX$^{(2)}$-based AE schemes call it twice ($k = n$); three times ($n < k \leq 2n$). In addition to the blockcipher calls, these schemes perform a key scheduling once. For an input to the AXU hash function, the XKX-based schemes take a counter, whereas AE schemes with other BBB-secure TBCs take a counter and a nonce. In efficient AXU hash functions [Rog04, KR11, RBBK01, CS08, GJMN16], if a counter and a nonce are inputted, a nonce is inputted to a blockcipher, then the output L is updated by counters, e.g., the powering-up scheme [Rog04] updates L as $2 \cdot L, 2^2 \cdot L, 2^3 \cdot L$ etc., where the counters are

Table 1: Comparison of security and efficiency of BBB-secure TBCs. This table considers ΘCB3-based and $\mathbb{OTR}$-based schemes whose underlying TBCs are given in the left most column. In these bounds, it is assumed that the influences of the decryption queries and associated data are sufficiently small. "BC" shows the number of blockcipher calls per one data block. In "Rekey," "1/TBC" means that a key scheduling is performed for each TBC call, and "1/AE" meas that a key scheduling is performed for each AE query. "Hash" shows the number of keyed hash function evaluations in one TBC call, and in the parentheses, the inputs are given. In "Precomp.," i-E means that a blockcipher is called i times in a precomputation phase.

TBC [Ref.]	Security Bound	BC	Rekey	Hash (Input)	Precomp.
Min [Min09]	$(\ell q)^2/2^n$	2	1/TBC	—	—
CLRW2 [LST12]	$(\ell q)^3/2^{2n}$	2	—	2 (N, ctr)	—
r-CLRW [LS13]	$(\ell q)^{r+2}/2^{rn}$	r	—	r (N, ctr)	—
$\mathrm{XKX}^{(1)}$ [Ours]	$(\ell^2 q + q^2)/2^n + \ell q^2/2^k$	1	1/AE	1 (ctr)	1-E or 2-E
$\mathrm{XKX}^{(2)}$ [Ours]	$\ell^2 q/2^n + \ell q^2/2^k$	1	1/AE	1 (ctr)	2-E or 3-E

$1, 2, 3$ etc., and the multiplication is done in $GF(2^n)$. In the XKX-based schemes, a nonce is not inputted to the AXU hash function, thus the blockcipher call with the nonce can be removed.[5]

From the security bounds of XKX, those of the XKX-based AE schemes are $\ell^2 q/2^n + \ell q^2/2^k + q^2/2^n$ ($\mathrm{XKX}^{(1)}$) and $\ell^2 q/2^n + \ell q^2/2^k$ ($\mathrm{XKX}^{(2)}$), where ℓ is the number of blockcipher calls in one AE evaluation and q is the number of queries to the AE scheme. Thus, if $q \ll 2^{n/2}$ and $\ell \ll 2^{n/2}$, the $\mathrm{XKX}^{(1)}$-based AE schemes achieve BBB security, and if $\ell \ll 2^{n/2}$, the $\mathrm{XKX}^{(2)}$-based AE schemes achieve BBB security. The security and the efficiency of the XKX-based AE schemes and other TBC-based AE schemes are summarized in Table 1, which are based on TBC-based AE schemes ΘCB3 and $\mathbb{OTR}$. Note that since ΘCB3 and $\mathbb{OTR}$ are one-pass, online and parallelizable, so are the XKX-based schemes.

1.4.4 Impact in the Practical Setting

Finally, we study the security bounds of the XKX-based AE schemes. We consider the example given in [BL16] which is the HTTP connection where an adversary can make 2900 queries of length 4 Kbyte per second. We use a blockcipher with $n = 64$ (e.g., PRESENT [BKL+07] and many other lightweight blockciphers). In this setting, the birthday bound is roughly 2^{32} blockcipher calls, and after one hour, the number of blockcipher calls reaches the bound. Next, XKX-based schemes are considered. For the sake of simplicity, we assume that the term $\ell q^2/2^k$ is negligible compared with other terms which can be achieved by using a blockcipher with long-size keys (e.g., $k = 128$). In this setting, the number of blockcipher calls ℓ is roughly 2^9. Then the term $\ell^2 q/2^n$ becomes $q/2^{46}$ $(= (2^9)^2 q/2^{64})$, thus the term reaches $1/2$ if $q = 2^{45}$. The 2^{45} AE queries spend $2^{45}/2900$ seconds ≈ 3847 years. The term $q^2/2^n$ becomes $q^2/2^{64}$, thus the term reaches $1/2$ if $q = 2^{31.5}$. The $2^{31.5}$ AE queries spend $2^{31.5}/2900$ seconds ≈ 121 days. Hence, the security bounds of the AE schemes with $\mathrm{XKX}^{(1)}$ (resp., $\mathrm{XKX}^{(2)}$) reach $1/2$ after 121 days (resp., 3847 years), and in this setting, it seems hard to break the security of the $\mathrm{XKX}^{(2)}$-based schemes. Note that the birthday term $q^2/2^n$ comes from the PRF/PRP switch for the tweak function F. If the underlying blockcipher is not influenced by the PRF/PRP difference, that is, the birthday term can be ignored, then $\mathrm{XKX}^{(1)}$-based schemes have the

[5] In the XKX-based schemes, L can be randomly generated or can be generated by using a blockcipher with a constant input, e.g., $L = E_{K_E}(0^n)$. (In this case, L can be precomputed.)

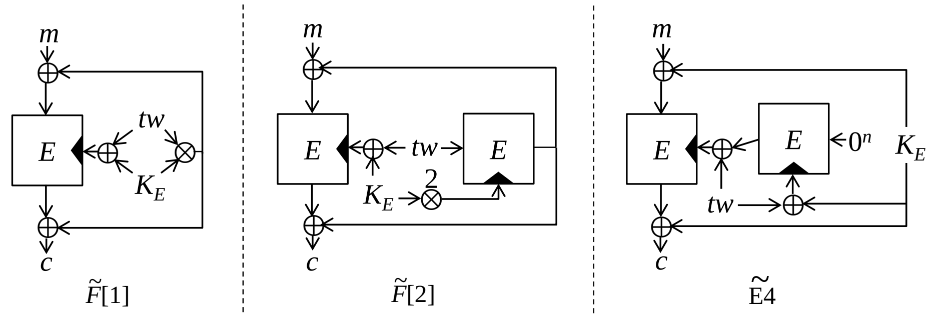

Figure 3: $\widetilde{F}[1]$ (left), $\widetilde{F}[2]$ (center), Wang et al.'s TBC $\widetilde{\text{E4}}$ (right). m is a plaintext block, c is a ciphertext block, tw is a tweak, and K_E is a key. $\otimes$ is the multiplication in $GF(2^n)$.

same level of security as $\text{XKX}^{(2)}$-based ones.

1.5 Related Works

Mennink [Men15] proposed two blockcipher-based TBCs called $\widetilde{F}[1]$ and $\widetilde{F}[2]$. $\widetilde{F}[1]$ calls a blockcipher once and a multiplication once, and is a secure TSPRP up to $2^{2n/3}$ queries. $\widetilde{F}[2]$ calls a blockcipher twice, and is fully secure (secure up to 2^n queries).[6] Note that the security proofs were given in the ideal cipher model. Wang et al. [WGZ+16] extended the result of Mennink, and proposed 32 fully secure TBCs in the ideal-cipher model. Mennink's TBCs and one of Wang et al.'s TBCs $\widetilde{\text{E4}}$ are illustrated in Figure 3. These TBCs offer AE schemes with BBB security in the ideal-cipher model. Note that the security of our TBCs is given in the standard model (the SPRP assumption).

So far, several TBC-based AE schemes have been proposed. Minematsu [Min09] and Coron et al. [CDMS10] proposed $2n$-bit blockcipher constructions from a TBC with n-bit block that is a fully secure SPRP. Combining these with birthday-bound AE schemes, the resultant schemes become fully secure AE schemes. Peyrin and Seurin [PS16] proposed an AE scheme that is fully secure against nonce-respecting adversaries and is birthday-bound secure against nonce-misuse adversaries. The AE scheme calls a blockcipher twice, and is not online. List and Nandi [LN17] proposed a fully secure deterministic AE scheme. The AE scheme calls a blockcipher twice and is not online. Again, these AE schemes are TBC-based.

Forler et al. [FLLW16] proposed a BBB-secure deterministic AE scheme that requires a $2n$-bit blockcipher, an AXU-hash function, and an encryption scheme accepting variable length plaintexts.

Cogliati and Seurin [CLS15, CS15] proposed tweakable-Even-Mansour-type TBCs with BBB security. These schemes are permutation-based, and the security proofs were given in the random-permutation model. Many permutation-based AE schemes including CAESAR candidates [DEMS, BDP+a, BDP+b, AJN] have the sponge-style structures [BDPA08, BDPA11, JLM14, ADMA15, MRV15], where a permutation is iterated, and data blocks are handled by using several bits of the internal state. The security proofs were given in the random-permutation model, and the security bound is the birthday one.

1.6 Organization

We start by giving notations and security definitions in Section 2. In Section 3, we give the specification of XKX, the security bound, and the security proof. In Section 4, we give

[6] Wang et al. [WGZ+16] showed that the primary version of $\widetilde{F}[2]$ is not a fully secure TBC. After that, Mennink repaired the TBC to become a fully secure one.

blockcipher-based instantiations of F. In Section 5, we apply XKX to efficient TBC-based AE schemes ΘCB3 and $\mathbb{OTR}$, and give the security bounds of the resultant AE schemes. Finally, in Section 6, we study the security bounds of the AE schemes.

2 Preliminaries

2.1 Notations

Let $\{0,1\}^*$ be the set of all bit strings, $\{0,1\}^n$ the set of n-bit strings, and 0^n the bit string of n-bit zeroes for an integer $n \geq 0$. Let $[i] := \{1, 2, \ldots, i\}$ for a positive integer i. For a finite set $\mathcal{X}$, $x \xleftarrow{\$} \mathcal{X}$ means that an element is randomly drawn from $\mathcal{X}$ and is assigned to x. For a bit string x and a set $\mathcal{X}$, we denote by $|x|$ and $|\mathcal{X}|$ the bit length of x and the number of elements in $\mathcal{X}$, respectively. Let $\mathsf{trunc}_i(x)$ be the first i-bit string of a bit string x, where $i \leq |x|$. Let $\mathsf{Perm}(\mathcal{B})$ be the set of all permutations over a non-empty set $\mathcal{B}$. A random permutation over $\mathcal{B}$ is defined as $P \xleftarrow{\$} \mathsf{Perm}(\mathcal{B})$. The inverse is denoted by P^{-1}. An adversary $\mathbf{A}$ with oracle access to $\mathcal{O}$ is denoted by $\mathbf{A}^{\mathcal{O}}$. An event that $\mathbf{A}^{\mathcal{O}}$ outputs a result y is denoted by $\mathbf{A}^{\mathcal{O}} \Rightarrow y$. In this paper, an adversary is a computationally bounded algorithm and the resource is measured in terms of time and query complexities.

2.2 Definitions of (Tweakable) Blockciphers

2.2.1 Definition of Classical Blockcipher

Let $\mathsf{BC}(\mathcal{K}, \mathcal{B})$ be the set of all encryptions of blockciphers with the set of keys $\mathcal{K}$ and the set of (plain/ciphertext) blocks $\mathcal{B}$. Fixing a blockcipher $E \in \mathsf{BC}(\mathcal{K}, \mathcal{B})$, E having a key $K \in \mathcal{K}$, denoted by $E(K, \cdot)$ or $E_K(\cdot)$, becomes a permutation over $\mathcal{B}$. The decryption function is denoted by E^{-1}, and E_K^{-1} becomes the inverse permutation of E_K. An ideal cipher is defined as $E \xleftarrow{\$} \mathsf{BC}(\mathcal{K}, \mathcal{B})$, and for each $K \in \mathcal{K}$, E_K becomes a random permutation.

We consider Strong-Pseudo-Random Permutation (SPRP) security that is indistinguishability between a (keyed) blockcipher and a random permutation. Let $E \in \mathsf{BC}(\mathcal{K}, \mathcal{B})$ be a blockcipher with the sets of keys $\mathcal{K}$ and blocks $\mathcal{B}$. The advantage function of an sprp-adversary $\mathbf{A}$ that outputs a bit are defined as

$$\mathbf{Adv}_E^{\mathsf{sprp}}(\mathbf{A}) = \Pr[K \xleftarrow{\$} \mathcal{K}; \mathbf{A}^{E_K, E_K^{-1}} \Rightarrow 1] - \Pr[P \xleftarrow{\$} \mathsf{Perm}(\mathcal{B}); \mathbf{A}^{P, P^{-1}} \Rightarrow 1] \enspace ,$$

where the probabilities are taken over $\mathbf{A}$, K and P. We say $\mathbf{A}$ is a (q,t)-sprp-adversary if $\mathbf{A}$ makes q queries and runs in time t. Pseudo-Random Permutation (PRP) security is a weaker security notion than SPRP security, where an adversary has access to only E_K/P. The advantage function of a prp-adversary $\mathbf{A}$ is denoted by $\mathbf{Adv}_E^{\mathsf{prp}}(\mathbf{A})$. We say $\mathbf{A}$ is a (q,t)-prp-adversary if $\mathbf{A}$ makes q queries and runs in time t.

2.2.2 Definition of Tweakable Blockcipher

Let $\widetilde{\mathsf{BC}}(\mathcal{K}, \mathcal{TW}, \mathcal{B})$ be the set of all encryptions of tweakable blockciphers (TBCs) with the set of keys $\mathcal{K}$, the set of tweaks $\mathcal{TW}$ and the set of (plain/ciphertext) blocks $\mathcal{B}$. Fixing a TBC $\widetilde{E} \in \mathsf{BC}(\mathcal{K}, \mathcal{TW}, \mathcal{B})$, $\widetilde{E}$ having a key $K \in \mathcal{K}$ and tweak $tw \in \mathcal{TW}$, denoted by $\widetilde{E}(K, tw, \cdot)$ or $\widetilde{E}_K(tw, \cdot)$, becomes a permutation over $\mathcal{B}$. The decryption function is denoted by $\widetilde{E}^{-1}$, and $\widetilde{E}_K^{-1}(tw, \cdot)$ is the inverse permutation of $\widetilde{E}_K(tw, \cdot)$.

We consider Tweakable-Strong-Pseudo-Random Permutation (TSPRP) security that is indistinguishability between a TBC and a (keyed) tweakable random permutation. Let $\widetilde{\mathsf{Perm}}(\mathcal{TW}, \mathcal{B})$ be the set of all tweakable permutations with the sets of tweaks $\mathcal{TW}$ and of blocks $\mathcal{B}$, where fixing $\widetilde{P} \in \widetilde{\mathsf{Perm}}(\mathcal{TW}, \mathcal{B})$, $\widetilde{P}$ having a tweak $tw \in \mathcal{TW}$ denoted by $\widetilde{P}(tw, \cdot)$

becomes a permutation over $\mathcal{B}$. The inverse is denoted by $\widetilde{P}^{-1}$. The advantage function of a tsprp-adversary $\mathbf{A}$ that outputs a bit is defined as

$$\mathbf{Adv}^{\widetilde{\mathsf{sprp}}}_{\widetilde{E}}(\mathbf{A}) = \Pr\left[K \xleftarrow{\$} \mathcal{K}; \mathbf{A}^{\widetilde{E}_K, \widetilde{E}_K^{-1}} \Rightarrow 1\right] - \Pr\left[\widetilde{P} \xleftarrow{\$} \widetilde{\mathsf{Perm}}(\mathcal{TW}, \mathcal{B}); \mathbf{A}^{\widetilde{P}, \widetilde{P}^{-1}} \Rightarrow 1\right] ,$$

where the probabilities are taken over $\mathbf{A}$, K and $\widetilde{P}$. We say $\mathbf{A}$ is a (q,t)-tsprp-adversary if $\mathbf{A}$ makes at most q queries and runs in time t. Tweakable-Pseudo-Random-Permutation (TPRP) security is a weaker security notion than TSPRP security, where an adversary has access to only $\widetilde{E}_K/\widetilde{P}$. The advantage function of a tprp-adversary $\mathbf{A}$ is denoted by $\mathbf{Adv}^{\widetilde{\mathsf{prp}}}_{\widetilde{F}}(\mathbf{A})$. We say $\mathbf{A}$ is a (q,t)-tprp-adversary if $\mathbf{A}$ makes at most q queries and runs in time t.

2.3 Definition of Pseudo-Random Function

Let $\mathsf{Func}(\mathcal{X}, \mathcal{Y})$ be the set of all functions from a set $\mathcal{X}$ to a set $\mathcal{Y}$. Let $\{F_K\}_{K \in \mathcal{K}}$ be a family of keyed functions indexed by the set of keys $\mathcal{K}$ that maps $\mathcal{X}$ to $\mathcal{Y}$. We consider Pseudo-Random-Function (PRF) security that is indistinguishability from a random function (RF), where an RF is defined as $f \xleftarrow{\$} \mathsf{Func}(\mathcal{X}, \mathcal{Y})$. The advantage function of a prf-adversary $\mathbf{A}$ that outputs a bit is defined as

$$\mathbf{Adv}^{\mathsf{prf}}_{F}(\mathbf{A}) = \Pr[K \xleftarrow{\$} \mathcal{K}; \mathbf{A}^{F_K} \Rightarrow 1] - \Pr[f \xleftarrow{\$} \mathsf{Func}(\mathcal{X}, \mathcal{Y}); \mathbf{A}^{f} \Rightarrow 1] ,$$

where the probabilities are taken over $\mathbf{A}$, K and f. We say $\mathbf{A}$ is a (q,t)-prf-adversary if $\mathbf{A}$ makes at most q queries and runs in time t.

2.4 Definition of Nonce-Based Authenticated Encryption

In this paper, we apply our TBC to nonce-based Authenticated Encryption (nAE) schemes (with associated data). The syntax and the definition of nAE schemes are given in the following.

An nAE scheme is a pair of encryption and decryption algorithms $\Pi = (\mathsf{Enc}, \mathsf{Dec})$. $\mathcal{K}, \mathcal{N}, \mathcal{M}, \mathcal{C}, \mathcal{A}$ and $\mathcal{T}$ are the sets of keys, nonces, messages, ciphertexts, associated data and tags of the nAE scheme. The encryption algorithm with a key $K \in \mathcal{K}$, Enc_K, takes a nonce $N \in \mathcal{N}$, associated data $A \in \mathcal{A}$, and a plaintext $M \in \mathcal{M}$. $\mathsf{Enc}_K(N, A, M)$ returns, deterministically, a pair of a ciphertext $C \in \mathcal{C}$ and a tag $tag \in \mathcal{T}$. The decryption algorithm with a key $K \in \mathcal{K}$, Dec_K, takes a tuple $(N, A, C, tag) \in \mathcal{N} \times \mathcal{A} \times \mathcal{C} \times \mathcal{T}$. $\mathsf{Dec}_K(N, A, C, tag)$ returns, deterministically, either the distinguished invalid symbol $\perp$ or a plaintext $M \in \mathcal{M}$. We require $|\mathsf{Enc}_K(N, A, M)| = |\mathsf{Enc}_K(N, A, M')|$ when the encryption are strings and $|M| = |M'|$.

We follow the security definition in [BN08, Rog02] that considers privacy and authenticity of an nAE scheme Π. The privacy advantage of an adversary $\mathbf{A}$ is defined as

$$\mathbf{Adv}^{\mathsf{priv}}_{\Pi}(\mathbf{A}) = \Pr[K \xleftarrow{\$} \mathcal{K}; \mathbf{A}^{\mathsf{Enc}_K} \Rightarrow 1] - \Pr[\mathbf{A}^{\$} \Rightarrow 1] ,$$

where a random-bits oracle \$ has the same interface as Enc_K, and for query (N, A, M) returns a random bit string of length $|\mathsf{Enc}_K(N, A, M)|$. The authenticity advantage of an adversary $\mathbf{A}$ is defined as

$$\mathbf{Adv}^{\mathsf{auth}}_{\Pi}(\mathbf{A}) = \Pr[K \xleftarrow{\$} \mathcal{K}; \mathbf{A}^{\mathsf{Enc}_K, \mathsf{Dec}_K} \text{ forges}] ,$$

where "$\mathbf{A}^{\mathsf{Enc}_K, \mathsf{Dec}_K}$ forges" means that $\mathbf{A}$ makes a query to Dec_K whose response is not $\perp$. We demand that $\mathbf{A}$ is nonce-respecting, namely, never asks two encryption queries with the same nonce, that $\mathbf{A}$ never asks a decryption query (N, A, C, tag) such that there is no prior encryption query with $(C, tag) = \mathsf{Enc}_K(N, A, M)$, and that $\mathbf{A}$ never repeats a query.

Algorithm 1 XKX

Procedure $\text{XKX}[F, E]_{K_F, K_h}((N, ctr), m)$

1: $v \leftarrow h_{K_h}(ctr)$; $x \leftarrow v \oplus m$
2: $w \leftarrow F_{K_F}(N)$; $y \leftarrow E_w(x)$ ▷ Minematsu's TBC
3: $c \leftarrow y \oplus v$
4: **return** c

2.5 Definition of Almost XOR Universal Hash Function

We will need a class of non-cryptographic functions called universal hash functions [CW79] defined as follows.

Definition 1. Let $\mathcal{H} = \{h_K\}_{K \in \mathcal{K}}$ be a family of functions from (some set) $\mathcal{TW}_N$ to $\{0,1\}^n$ indexed by the set of keys $\mathcal{K}$. $\mathcal{H}$ is said to be (ϵ, δ)-almost XOR universal ((ϵ, δ)-AXU) if

1. for any distinct $N, N' \in \mathcal{TW}_N$ and any $c \in \{0,1\}^n$,

$$\Pr[K \xleftarrow{\$} \mathcal{K} : h_K(N) \oplus h_K(N') = c] \le \epsilon \ ,$$

2. for any $N \in \mathcal{TW}_N$ and any $c \in \{0,1\}^n$,

$$\Pr[K \xleftarrow{\$} \mathcal{K} : h_K(N) = c] \le \delta \ .$$

3 XKX

3.1 Specification

XKX is constructed from a blockcipher and two tweak functions. Using XKX in nAE schemes, one of the tweak function is used to take nonces, and the other is used to take counters. These definitions are given in the following.

- The blockcipher is defined as $E \in \mathsf{BC}(\{0,1\}^k, \{0,1\}^n)$, where positive integers n and k are the block size and the key size, respectively.
- The first tweak function is a keyed function from a set of (first) tweaks $\mathcal{TW}_N$ to $\{0,1\}^k$ whose family is defined as $\mathcal{F} := \{F_{K_F}\}_{K_F \in \mathcal{K}_F}$ indexed by a set of keys $\mathcal{K}_F$.
- The second tweak function is a keyed hash function from a set of (second) tweaks $\mathcal{TW}_{ctr}$ to $\{0,1\}^n$ whose family is defined as $\mathcal{H} := \{h_{K_h}\}_{K_h \in \mathcal{K}_h}$ indexed by a set of keys $\mathcal{K}_h$.

$\text{XKX}[F, E]_{K_F, K_h}$ denotes XKX using underlying primitives F, E, h and keys K_F, K_h. $\text{XKX} \in \widetilde{\mathsf{BC}}(\mathcal{K}_F \times \mathcal{K}_h, \mathcal{TW}_N \times \mathcal{TW}_{ctr}, \{0,1\}^n)$ is defined in Algorithm 1 and is illustrated in Figure 2. A tweak taken by the first (resp., second) tweak function is called a first (resp., second) tweak.

3.2 Security of XKX

The upper-bound of the tsprp-advantage for XKX given in the following theorem, assuming the keyed blockcipher is a secure SPRP, the first tweak function is a secure PRF and the family of second tweak functions is AXU.

Theorem 1. *Assume that $\mathcal{H}$ is (ϵ,δ)-AXU. Let $\mathbf{A}$ be a (σ,t)-tsprp-adversary. Here, q is the number of distinct first tweaks, and ℓ_N is the number of queries with first tweak $N \in \mathcal{TW}_N$. Then, there exist a $(\sigma, t+O(\sigma))$-sprp-adversary $\mathbf{A}_E$ and $(q, t+O(\sigma))$-prf-adversary $\mathbf{A}_F$ such that*

$$\mathbf{Adv}^{\widetilde{\mathsf{sprp}}}_{\mathrm{XKX}}(\mathbf{A}) \le q \cdot \mathbf{Adv}^{\mathsf{sprp}}_{E}(\mathbf{A}_E) + \mathbf{Adv}^{\mathsf{prf}}_{F}(\mathbf{A}_F) + \sum_{N \in \mathcal{N}} \ell_N^2 \cdot \epsilon \ .$$

3.3 Proof of Theorem 1

Without loss of generality, assume that an adversary $\mathbf{A}$ never repeats a query.

3.3.1 Replacing Minematsu's TBC with TPRP

XKX is based on Minematsu's TBC [Min09] whose encryption denoted by $\mathrm{Min} \in \widetilde{\mathsf{BC}}(\mathcal{K}_F, \mathcal{TW}_N, \{0,1\}^n)$ is defined as follows:

$$\mathrm{Min}[F,E]_{K_F}(N,m) = E_w(m) \text{ where } w = F_{K_F}(N).$$

In Algorithm 1, Step 2 uses the TBC. Minematsu [Min09] gave the following upper-bound of the tsprp-advantage.

Lemma 1. *Let $\mathbf{A}$ be a (σ,t)-tsprp-adversary whose queries include q distinct tweaks. Then there exist a $(\sigma, t+O(\sigma))$-prp-adversary $\mathbf{A}_E$ and a $(q, t+O(\sigma))$-prf-adversary $\mathbf{A}_F$ such that*

$$\mathbf{Adv}^{\widetilde{\mathsf{sprp}}}_{\mathrm{Min}}(\mathbf{A}) \le q \cdot \mathbf{Adv}^{\mathsf{sprp}}_{E}(\mathbf{A}_E) + \mathbf{Adv}^{\mathsf{prf}}_{F}(\mathbf{A}_F) \ .$$

The term $q \cdot \mathbf{Adv}^{\mathsf{sprp}}_{E}(\mathbf{A}_E)$ comes from the SPRP security of E with q-blockcipher's keys, and the term $\mathbf{Adv}^{\mathsf{prf}}_{F}(\mathbf{A}_F)$ comes from the PRF security of F.

By the above lemma, Min can be replaced with a tweakable random permutation $\widetilde{P}_R \xleftarrow{\$} \widetilde{\mathsf{Perm}}(\mathcal{TW}_N, \{0,1\}^n)$ with the above security loss. Hereafter, XKX using $\widetilde{P}_R$ is denoted by $\widetilde{F}[\widetilde{P}_R]$.

3.3.2 TSPRP Security of $\widetilde{F}[\widetilde{P}_R]$

The remaining work is to upper-bound the tsprp-advantage which is defined as

$$\begin{aligned}\mathbf{Adv}^{\widetilde{\mathsf{sprp}}}_{\widetilde{F}}(\mathbf{A}) =& \Pr[\widetilde{P}_R \xleftarrow{\$} \widetilde{\mathsf{Perm}}(\mathcal{TW}_N, \{0,1\}^n); K_h \xleftarrow{\$} \mathcal{K}_h; \mathbf{A}^{\widetilde{F}[\widetilde{P}_R]_{K_h}, \widetilde{F}[\widetilde{P}_R]^{-1}_{K_h}} \Rightarrow 1] - \\ & \Pr[\widetilde{P}_I \xleftarrow{\$} \widetilde{\mathsf{Perm}}(\mathcal{TW}_N \times \mathcal{TW}_{ctr}, \{0,1\}^n); \mathbf{A}^{\widetilde{P}_I, \widetilde{P}_I^{-1}} \Rightarrow 1] \ .\end{aligned}$$

This case can be seen as the multi-key setting of LRW2, where an adversary has oracle access to either q LRW2 oracles with distinct random permutations or q tweakable random permutation. Roughly speaking, since the random permutations of q LRW2 oracles are independently defined, the above difference is upper-bounded by $q\times$(the tsprp-advantage of LRW2 in the single-key setting). The upper-bound of the tsprp-advantage of LRW2 is given in [LRW02] (or [CLS15] for the more general case), which is $\ell^2 \cdot \epsilon$ for an adversary making at most ℓ queries. Hence, the above difference is upper-bounded by $\ell^2 q \cdot \epsilon$.

In the following, the full analysis is given. In this analysis, the values defined at the α-th query are denoted by using the superscript character of α. The world with $\widetilde{F}[\widetilde{P}_R]_{K_h}$ is called the real world, and the world with $\widetilde{P}_I$ is called the ideal world.

Transcript. This proof permits for $\mathbf{A}$ to obtain the key K_h after its interaction but before outputting a decision bit. In the ideal world, a dummy key is defined as $K_h \xleftarrow{\$} \mathcal{K}_{K_h}$. After $\mathbf{A}$'s interaction, it obtains the following transcript.

$$\tau = \left(K_h, \bigcup_{\alpha=1}^{\sigma} \{((N^\alpha, ctr^\alpha), m^\alpha, c^\alpha)\} \right)$$

Let T_R be the transcript in the real world obtained by sampling $\widetilde{P}_R \xleftarrow{\$} \widetilde{\mathsf{Perm}}(\mathcal{TW}_N, \{0,1\}^n)$ and $K_h \xleftarrow{\$} \mathcal{K}_h$. Let T_I be the transcript in the ideal world obtained by sampling $\widetilde{P}_I \xleftarrow{\$} \widetilde{\mathsf{Perm}}(\mathcal{TW}_N \times \mathcal{TW}_{ctr}, \{0,1\}^n)$ and $K_h \xleftarrow{\$} \mathcal{K}_h$. We call a transcript τ *valid* if an interaction with their oracles could render this transcript, namely, $\Pr[\mathsf{T}_i = \tau] > 0$ for $i \in \{R, I\}$. Then the tsprp-advantage is upper-bounded by the statistical distance of transcripts, i.e.,

$$\mathbf{Adv}_{\widetilde{F}}^{\widetilde{\mathsf{sprp}}}(\mathbf{A}) \leq \mathsf{SD}(\mathsf{T}_R, \mathsf{T}_I) = \frac{1}{2} \sum_{\tau} |\Pr[\mathsf{T}_R = \tau] - \Pr[\mathsf{T}_I = \tau]| \ ,$$

where the sum is over all valid transcripts.

Coefficient H Technique. The statistical distance $\mathsf{SD}(\mathsf{T}_R, \mathsf{T}_I)$ can be upper-bounded by the coefficient H technique [CS14, Pat08]. Let $\mathcal{T}$ be valid transcripts. In this technique, $\mathcal{T}$ is partitioned into two transcripts: good transcripts $\mathcal{T}_{\mathsf{good}}$ and bad transcripts $\mathcal{T}_{\mathsf{bad}}$. Then $\mathsf{SD}(\mathsf{T}_R, \mathsf{T}_I)$ is upper-bound by the following lemma.

Lemma 2. *Let* $0 \leq \varepsilon \leq 1$ *be such that for all* $\tau \in \mathcal{T}_{\mathsf{good}}$, $\frac{\Pr[\mathsf{T}_R = \tau]}{\Pr[\mathsf{T}_I = \tau]} \geq 1 - \varepsilon$. *Then,* $\mathsf{SD}(\mathsf{T}_R, \mathsf{T}_I) \leq \Pr[\mathsf{T}_I \in \mathcal{T}_{\mathsf{bad}}] + \varepsilon$.

Hereafter, first good and bad transcripts are defined. Then ε and $\Pr[\mathsf{T}_I \in \mathcal{T}_{\mathsf{bad}}]$ are upper-bounded. Finally, by the above lemma, the upper-bound of the tsprp-advantage is obtained.

Good and Bad Transcripts. Bad transcripts $\mathcal{T}_{\mathsf{bad}}$ are defined such that the following condition is satisfied, and good transcripts $\mathcal{T}_{\mathsf{good}}$ are defined such that this condition is not satisfied.

- $\mathsf{coll} \Leftrightarrow \exists \alpha, \beta \in [\sigma]$ with $\alpha \neq \beta$ s.t. $(N^\alpha = N^\beta)$ and $(x^\alpha = x^\beta$ or $y^\alpha = y^\beta)$.

Note that in the ideal world, x^α is defined as $x^\alpha = h_{K_h}(ctr^\alpha) \oplus m^\alpha$, and y^α is defined as $y^\alpha = h_{K_h}(ctr^\alpha) \oplus c^\alpha$.

Upper-Bound of $\Pr[\mathsf{T}_I \in \mathcal{T}_{\mathsf{bad}}]$. Since $\Pr[\mathsf{T}_I \in \mathcal{T}_{\mathsf{bad}}] = \Pr[\mathsf{coll}]$, in the following $\Pr[\mathsf{coll}]$ is upper-bounded.

Consider the condition in coll: $N^\alpha = N^\beta$ and $x^\alpha = x^\beta$. The equation $x^\alpha = x^\beta$ implies

$$h_{K_h}(ctr^\alpha) \oplus h_{K_h}(ctr^\beta) = m^\alpha \oplus m^\beta \ .$$

Hence, fixing α, β with $N^\alpha = N^\beta$, since $\mathcal{H}$ is (ϵ, δ)-AXU, the probability that $x^\alpha = x^\beta$ is at most ϵ. Similarly, fixing α, β with $N^\alpha = N^\beta$, the probability that $y^\alpha = y^\beta$ is at most ϵ.

Since the number of queries with the first tweak N is ℓ_N, we have

$$\Pr[\mathsf{T}_I \in \mathcal{T}_{\mathsf{bad}}] = \Pr[\mathsf{coll}] \leq \sum_{N \in \mathcal{TW}_N} \binom{\ell_N}{2} \cdot 2\epsilon \leq \sum_{N \in \mathcal{TW}_N} \ell_N^2 \cdot \epsilon \ .$$

Upper-Bound of ε. Let τ be a good transcript. Let all_R (resp. all_I) be the set of all oracles in the real (resp. ideal) world. Let $\mathrm{comp}_R(\tau)$ (resp. $\mathrm{comp}_I(\tau)$) be the set of oracles compatible with τ in the real (resp. ideal) world. Then

$$\Pr[\mathsf{T}_R = \tau] = \frac{|\mathrm{comp}_R(\tau)|}{|\mathrm{all}_R|} \text{ and } \Pr[\mathsf{T}_I = \tau] = \frac{|\mathrm{comp}_I(\tau)|}{|\mathrm{all}_I|} \ .$$

Firstly, $|\mathrm{all}_R|$ is counted. Since $K_h \in \mathcal{K}_h$ and $\widetilde{P}_R \in \widetilde{\mathsf{Perm}}(\mathcal{TW}_N, \{0,1\}^n)$, we have

$$|\mathrm{all}_R| = |\mathcal{K}_h| \cdot (2^n!)^{|\mathcal{TW}_N|} \ .$$

Secondly, $|\mathrm{all}_I|$ is counted. Since $K_h \in \mathcal{K}_h$ and $\widetilde{P}_I \in \widetilde{\mathsf{Perm}}(\mathcal{TW}_N \times \mathcal{TW}_{ctr}, \{0,1\}^n)$, we have

$$|\mathrm{all}_I| = |\mathcal{K}_h| \cdot (2^n!)^{|\mathcal{TW}_N| \times |\mathcal{TW}_{ctr}|} \ .$$

Thirdly, $|\mathrm{comp}_R(\tau)|$ is counted. By $\neg\mathsf{coll}$, all $\widetilde{P}_R$-evaluations with the same first tweak don't overlap with each other. K is uniquely determined. Hence, we have

$$|\mathrm{comp}_R(\tau)| = \prod_{N \in \mathcal{TW}_N} (2^n - \ell_N)! \ .$$

Fourthly, $|\mathrm{comp}_I(\tau)|$ is counted. Let $\ell_{N,ctr}$ be the number of queries with the first tweak N and the second tweak ctr. Note that $\ell_N = \sum_{ctr \in \mathcal{TW}_{ctr}} \ell_{N,ctr}$. Then,

$$\begin{aligned}|\mathrm{comp}_I(\tau)| &= \prod_{N \in \mathcal{TW}_N, ctr \in \mathcal{TW}_{ctr}} (2^n - \ell_{N,ctr})! \\ &\le (2^n!)^{|\mathcal{TW}_{ctr}|} \cdot \prod_{N \in \mathcal{TW}_N} (2^n - \ell_N)! \ ,\end{aligned}$$

using $(2^n - a)! \cdot (2^n - b)! \le 2^n! \cdot (2^n - a - b)!$ for any $0 \le a, b \le 2^n$.

Finally,

$$\frac{\Pr[\mathsf{T}_R = \tau]}{\Pr[\mathsf{T}_M = \tau]} \ge \frac{\prod_{N \in \mathcal{TW}_N} (2^n - \ell_N)!}{|\mathcal{K}_h| \cdot (2^n!)^{|\mathcal{TW}_N|}} \times \frac{|\mathcal{K}_h| \cdot (2^n!)^{|\mathcal{TW}_N| \times |\mathcal{TW}_{ctr}|}}{(2^n!)^{|\mathcal{TW}_{ctr}|} \cdot \prod_{N \in \mathcal{TW}_N} (2^n - \ell_N)!} = 1 \ .$$

Thus we have $\varepsilon = 0$.

Upper-Bound of $\mathbf{Adv}^{\widetilde{\mathsf{sprp}}}_{\widetilde{F}}(\mathbf{A})$. Putting the above upper-bounds in Lemma 2 gives

$$\mathbf{Adv}^{\widetilde{\mathsf{sprp}}}_{\widetilde{F}}(\mathbf{A}) \le \sum_{N \in \mathcal{TW}_N} \ell_N^2 \cdot \epsilon \ .$$

3.3.3 Conclusion of the Proof

Finally, combining Lemma 1 and the upper-bound of $\mathbf{Adv}^{\widetilde{\mathsf{sprp}}}_{\widetilde{F}}(\mathbf{A})$ gives

$$\mathbf{Adv}^{\widetilde{\mathsf{sprp}}}_{\mathrm{XKX}}(\mathbf{A}) \le q \cdot \mathbf{Adv}^{\mathsf{sprp}}_{E}(\mathbf{A}_E) + \mathbf{Adv}^{\mathsf{prf}}_{F}(\mathbf{A}_F) + \sum_{N \in \mathcal{TW}_N} \ell_N^2 \cdot \epsilon \ ,$$

where $\mathbf{A}_E$ is a $(\sigma, t + O(\sigma))$-sprp-adversary and $\mathbf{A}_F$ is a $(q, t + O(\sigma))$-prf-adversary. $\square$

3.4 Removing the Output Masking of XKX

In Theorem 1, the upper-bound of the tsprp-advantage of XKX is given, where an adversary has oracle access to both of the encryption function and the decryption function. In XKX, in order to avoid a collision attack in inputs to the underlying blockcipher from the encryption oracle, the input masking is introduced, and in order to avoid a collision in outputs to the underlying blockcipher from the decryption oracle, the output masking is introduced. Since the decryption oracle is absent in the TPRP-setting, the output masking of XKX can be removed, i.e., the resultant TBC that we call XK is a secure TPRP. The tprp-advantage of XK can be upper-bounded by the proof similar to Theorem 1, where the condition $y^\alpha = y^\beta$ in the event coll (in Subsubsection 3.3.2) is not required, and other analyses are the same. Concretely, the upper-bound of the tprp-advantage is given below. Assume that $\mathcal{H}$ is (ϵ, δ)-AXU. Let $\mathbf{A}$ be a (σ, t)-tprp-adversary. Here, q is the number of distinct first tweaks, and ℓ_N is the number of queries with first tweak $N \in \mathcal{TW}_N$. Then, there exist a $(\sigma, t + O(\sigma))$-prp-adversary $\mathbf{A}_E$ and $(q, t + O(\sigma))$-prf-adversary $\mathbf{A}_F$ such that

$$\mathbf{Adv}^{\widetilde{\mathsf{prp}}}_{\mathrm{XK}}(\mathbf{A}) \le q \cdot \mathbf{Adv}^{\mathsf{prp}}_{E}(\mathbf{A}_E) + \mathbf{Adv}^{\mathsf{prf}}_{F}(\mathbf{A}_F) + \sum_{N \in \mathcal{N}} 0.5\ell_N^2 \cdot \epsilon \ .$$

4 Instantiations of F

We show how to construct the first tweak function F_{K_F} from a blockcipher. The blockcipher is defined as $E \in \mathsf{BC}(\{0,1\}^k, \{0,1\}^n)$. We deal with blockciphers with $n \le k \le 2n$, since almost all of blockciphers satisfy the condition.

We define a first tweak function that uses blockcipher outputs.

- $F^{(1)}_{K_F}(N) = \mathsf{trunc}_k(E_{K_E}(0\|N)\|E_{K_E}(1\|N))$ where $K_F = K_E$, $\mathcal{K}_F := \{0,1\}^k$, and $\mathcal{TW}_N := \{0,1\}^{n-1}$.

By the PRF/PRP switch, the prf-advantage is upper-bounded the prp-advantage of the blockcipher plus the birthday bound $O(q^2/2^n)$.

Next, we define a first tweak functions so that the birthday bound is removed. In order to remove the birthday bound, the xor function is used.

- $F^{(2)}_{K_F}(N) = \mathsf{trunc}_k\Big(\big(E_{K_E}(00\|N) \oplus E_{K_E}(01\|N)\big)\|\big(E_{K_E}(00\|N) \oplus E_{K_E}(10\|N)\big)\Big)$ where $K_F = K_E$, $\mathcal{K}_F := \{0,1\}^k$, and $\mathcal{TW}_N := \{0,1\}^{n-2}$.

In [Pat10], it was proven that the xor function achieves optimal PRF security, thus the prf-advantage is upper-bounded by the prp-advantage of the blockcipher plus the optimal PRF-security bound $O(q/2^n)$.

These concrete bounds are given in the following, where the upper-bound of $F^{(1)}$ is obtained by the PRF/PRP switch, and the upper-bound of $F^{(2)}$ is obtained by using Theorem 2 in [IMV16] (the original analysis is given in Theorem 6 of [Pat10]).

Lemma 3 (PRF Security of $F^{(1)}$)**.** *For any (q, t)-prf-adversary $\mathbf{A}$, there exists a $(2q, t + O(q))$-prp-adversary $\mathbf{A}_E$ such that*

$$\mathbf{Adv}^{\mathsf{prf}}_{F^{(1)}}(\mathbf{A}) \le \mathbf{Adv}^{\mathsf{prp}}_{E}(\mathbf{A}_E) + \frac{q^2}{2^n} \ .$$

Lemma 4 (PRF Security of $F^{(2)}$)**.** *For any (q, t)-prf-adversary $\mathbf{A}$, there exists a $(3q, t + O(q))$-prp-adversary $\mathbf{A}_E$ such that*

$$\mathbf{Adv}^{\mathsf{prf}}_{F^{(2)}}(\mathbf{A}) \le \mathbf{Adv}^{\mathsf{prp}}_{E}(\mathbf{A}_E) + \frac{4q}{2^n} \ .$$

Remark 1. When $n = k$, $F^{(1)}$ (resp., $F^{(2)}$) calls a blockcipher once (resp., twice), and the domain separation bit(s) perpended to N can be removed (resp., shortened). When $2n < k$, the first tweak functions can be defined by making the bit length longer.

5 Applications

We apply XKX to nAE schemes ΘCB [KR11] and $\mathbb{OTR}$ [Min14]. As shown below, the XKX-based schemes achieve BBB security, and become efficient, one-pass, online and parallelizable.

5.1 ΘCB3 with XKX

5.1.1 ΘCB3 [KR11]

ΘCB3 is a TBC generalization of OCB3 [KR11], and is efficient, one-pass, online and parallelizable. In ΘCB3, a plaintext is encrypted by the ECB-like construction (but a tweak is varied for each block), and a tag is generated by encrypting the checksum of plaintext blocks. In the decryption, a ciphertext is decrypted by the decryption of the ECB-like construction, then a tag is generated by encrypting the checksum of the decrypted plaintext blocks (thus a tag is generated by the PMAC-like structure [Rog04]).

We briefly give the construction of ΘCB3, following the notations in [KR11]. Here, a TBC is defined as $\widetilde{E} \in \widetilde{\mathsf{BC}}(\{0,1\}^k, \mathcal{TW}, \{0,1\}^n)$, where k is the key size in bits, $\mathcal{TW}$ is the set of tweaks, and n is the block size. The set of tweaks is defined as follows.

$$\begin{aligned}\mathcal{TW} := &(\mathcal{N} \times \mathbb{N}_1) \cup (\mathcal{N} \times \mathbb{N}_0 \times \{*\}) \cup (\mathcal{N} \times \mathbb{N}_0 \times \{\$\}) \cup (\mathcal{N} \times \mathbb{N}_0 \times \{*\$\})\\ &\cup \mathbb{N}_1 \cup (\mathbb{N}_0 \times \{*\})\end{aligned}$$

where $\mathcal{N}$ is the set of nonces, $\mathbb{N}_1$ and $\mathbb{N}_0$ are positive and nonnegative integers, respectively. Hence, ΘCB3 uses six types of permutations: $\widetilde{E}_K((N,i),\cdot)$, $\widetilde{E}_K((N,i,*),\cdot)$, $\widetilde{E}_K((N,i,\$),\cdot)$, $\widetilde{E}_K((N,i,*\$),\cdot)$, $\widetilde{E}_K(i,\cdot)$, and $\widetilde{E}_K((i,*),\cdot)$. The first two permutations are used to encrypt plaintext blocks. The next two permutations are used to generate a tag. The last two permutations are used to handle associated data. In each procedure, the latter permutation is used to avoid an additional permutation call by the padding. In the encryption of ΘCB3, for a nonce N and n-bit plaintext blocks $M_1, \ldots, M_l$, the i-th ciphertext block is defined as $C_i \leftarrow \widetilde{E}_K((N,i), M_i)$. Regarding associated data $A_1, \ldots, A_a$, the i-th block A_i is inputted to the TBC as $B_i \leftarrow \widetilde{E}_K(i, A_i)$. Then the tag is defined as $tag \leftarrow \mathsf{trunc}_\tau(\widetilde{E}_K((N,i,\$), \mathrm{Checksum}) \oplus B_1 \oplus \cdots \oplus B_a)$, where Checksum is the checksum of the plaintext blocks. Note that if the length of the message is not multiple of n, then permutations with tweaks including "$*$" are used to encrypt the last block and generate a tag. Similarly, if the length of associated data is not multiple of n, then $\widetilde{E}_K((i,*),\cdot)$ is used to process the last block of associated data. The encryption of ΘCB3 is illustrated in Figure 4. In the decryption of ΘCB3, the inverse procedure of the encryption is performed. Please see Subsection 4.2 in [KR11] for the concrete construction of ΘCB3.

In [KR11], the security of ΘCB3 was analyzed in the information-theoretic model, that is, the keyed TBC is replaced with a tweakable random permutation. Regarding the privacy, for each TBC call, a distinct tweak is used, thus each ciphertext block is randomly drawn from $\{0,1\}^n$. Hence, for any adversary $\mathbf{A}$,

$$\mathbf{Adv}^{\mathsf{priv}}_{\Theta\mathrm{CB3}}(\mathbf{A}) = 0 \ .$$

Regarding the authenticity, two cases are considered: an adversary $\mathbf{A}$ makes a decryption query such that (1) the nonce appeared in the previous encryption queries; (2) the nonce has not appeared in the previous encryption queries. In order to forge a tag, in (1), $\mathbf{A}$

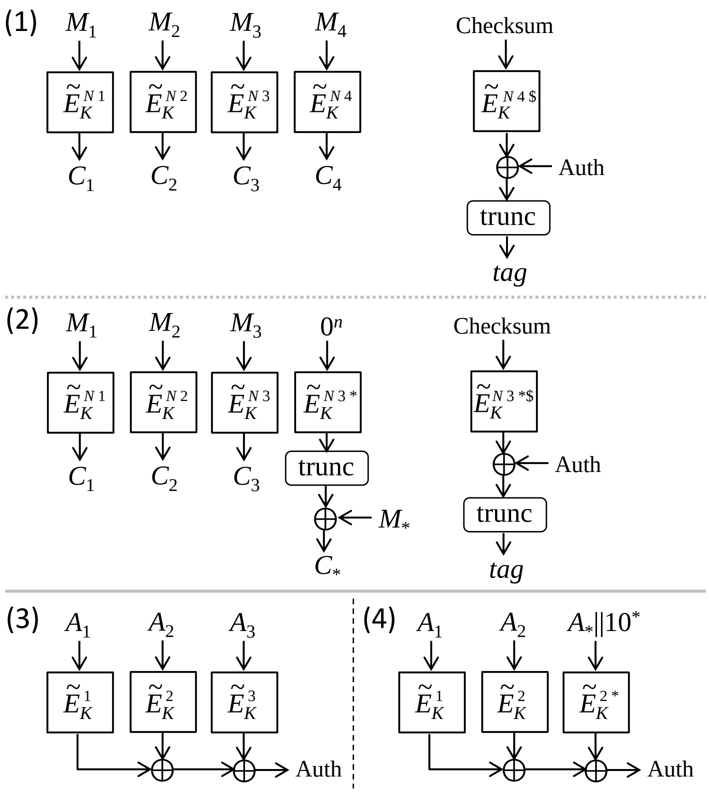

Figure 4: Encryption of ΘCB3. The procedure (1) encrypts four n-bit plaintext blocks M_1, M_2, M_3, M_4, and returns a tag. The procedure (2) encrypts three n-bit plaintext blocks M_1, M_2, M_3 and a plaintext block of length less than n bits M_*, and returns a tag. The procedure (3) handles three n-bit associated data blocks A_1, A_2, A_3. The procedure (4) handles two n-bit associated data blocks A_1, A_2 and an associated data block A_* of length less than n bits ($A_*\|10^*$ is an n-bit string, where 1 is appended to A_* and an appropriate number of bits 0 is appended so that the bit length becomes n).

should occur a collision of the checksum values with the same nonces (yielding the same tags), and then makes a query with the same tag; in (2), **A** should hit a tag that is randomly drawn. In [KR11], it was proven that these probabilities are at most $2^{n-\tau}/(2^n-1)$. Hence, for any adversary **A** making at most $q_{\mathcal{D}}$ decryption queries,

$$\mathbf{Adv}^{\mathsf{priv}}_{\Theta\mathrm{CB3}}(\mathbf{A}) \leq \frac{q_{\mathcal{D}} 2^{n-\tau}}{2^n - 1} \enspace .$$

5.1.2 ΘCB3 with XKX

We apply XKX to ΘCB3. The resultant scheme is denoted by ΘCB3[XKX]. The set of first tweaks is defined as $\mathcal{TW}_N := \mathcal{N} \cup \{0\}$ such that $0 \notin \mathcal{N}$. "0" is used to define a blockcipher's key to handle associated data. The set of second tweaks is defined as $\mathcal{TW}_{ctr} := \mathbb{N}_1 \cup (\mathbb{N}_0 \times \{*\}) \cup (\mathbb{N}_0 \times \{\$\}) \cup (\mathbb{N}_0 \times \{*\$\}) \cup \mathbb{N}_1 \cup (\mathbb{N}_0 \times \{*\})$. In XKX, for each encryption or decryption query, a blockcipher's key is defined by the first tweak function F_{K_F} whose input is a nonce N and is fixed, thus F_{K_F} is called once for each encryption or decryption query. Namely, for each data block, ΘCB3[XKX] calls a blockcipher once (and calls an AXU hash function once). Hence, ΘCB3[XKX] is efficient, one-pass, online and parallelizable. Since inputs of the AXU hash function do not include nonces, the hash values can be precomputed. If there is a storage that keeps the hash values, then the hash computations can be removed.

Regarding the security of ΘCB3[XKX], since XKX can be used as a tweakable random permutation up to the security bound given in Theorem 1, the security bounds of ΘCB3[XKX] are obtained by summing the security bound given in Theorem 1 and the security bounds of ΘCB3. The details are given in following. Here, $\mathcal{H}$ is assumed to be (ϵ, δ)-AXU.

First, the privacy of ΘCB3[XKX] is considered. Let $\mathbf{A}$ be an adversary that makes $q_{\mathcal{E}}$ encryption queries and runs in time t such that σ_A is the number of blockcipher calls by associated data and ℓ_N is the total number of blockcipher calls by queries with the nonce $N \in \mathcal{N}$. Let $\sigma_{\mathcal{E}} = \sigma_A + \sum_{N\in\mathcal{N}} \ell_N$. In this setting, at most $q_{\mathcal{E}}$ "nonce-dependent" blockcipher's keys are defined, which are used to encrypt plaintexts and generate tags, and another key is used to handle associated data. Hence, at most $q_{\mathcal{E}} + 1$ blockcipher's keys are defined. Combining Theorem 1 and the privacy bound of ΘCB3, the following result is obtained: There exist a $(\sigma_{\mathcal{E}}, t + O(\sigma_{\mathcal{E}}))$-sprp-adversary $\mathbf{A}_E$ and a $(q_{\mathcal{E}} + 1, t + O(\sigma_{\mathcal{E}}))$-prf-adversary $\mathbf{A}_F$ such that

$$\mathbf{Adv}^{\mathsf{priv}}_{\Theta\mathrm{CB3[XKX]}}(\mathbf{A}) \le (q_{\mathcal{E}} + 1) \cdot \mathbf{Adv}^{\mathsf{sprp}}_{E}(\mathbf{A}_E) + \mathbf{Adv}^{\mathsf{prf}}_{F}(\mathbf{A}_F) + \left(\sigma_A^2 + \sum_{N\in\mathcal{N}} \ell_N^2\right) \cdot \epsilon \ .$$

Next, the authenticity of ΘCB3[XKX] is considered. Let $\mathbf{A}$ be an adversary that makes $q_{\mathcal{E}}$ encryption/$q_{\mathcal{D}}$ decryption queries and runs in time t such that the number of blockcipher calls by associated data is σ_A and the number of blockcipher calls by queries with the nonce $N \in \mathcal{N}$ is ℓ_N. Let $q = q_{\mathcal{E}} + q_{\mathcal{D}}$ and $\sigma = \sigma_{\mathcal{E}} + \sum_{N\in\mathcal{N}} \ell_N$. In this setting, at most q nonce-dependent blockcipher's keys are defined to encrypt plaintexts, decrypt ciphertexts and generate tags, and another key is defined to handle associated data. Hence, at most $q + 1$ blockcipher's keys are defined. Combining Theorem 1 and the authenticity bound of ΘCB3, the following result is obtained: There exist a $(\sigma, t + O(\sigma))$-sprp-adversary $\mathbf{A}_E$ and a $(q + 1, t + O(\sigma))$-prf-adversary $\mathbf{A}_F$ such that

$$\begin{aligned}
&\mathbf{Adv}^{\mathsf{auth}}_{\Theta\mathrm{CB3[XKX]}}(\mathbf{A}) \\
&\le (q + 1) \cdot \mathbf{Adv}^{\mathsf{sprp}}_{E}(\mathbf{A}_E) + \mathbf{Adv}^{\mathsf{prf}}_{F}(\mathbf{A}_F) + \left(\sigma_A^2 + \sum_{N\in\mathcal{N}} \ell_N^2\right) \cdot \epsilon + \frac{q_{\mathcal{D}} 2^{n-\tau}}{2^n - 1} \ .
\end{aligned}$$

5.2 $\mathbb{OTR}$ with XKX

$\mathbb{OTR}$ [Min14] is a variant of ΘCB3, which is also efficient, one-pass, online and parallelizable (under two-block partition). $\mathbb{OTR}$ encrypts two plaintext blocks by two-round Feistel permutation, where in each round a TBC (or a function) is called once. By the Feistel permutation, $\mathbb{OTR}$ does not require the decryption function of the underlying TBC. Hence, adopting XKX to $\mathbb{OTR}$, the resultant scheme is efficient, one-pass, and parallelizable without a decryption function of a blockcipher.

$\mathbb{OTR}$ has the same level of security as ΘCB (the constant factors in the authenticity bounds are distinct). Hence, $\mathbb{OTR}$ with XKX also achieves the same level of security as ΘCB[XKX]. Since $\mathbb{OTR}$ does not require a decryption function of a blockcipher, the security proofs of the $\mathbb{OTR}$-based AE scheme do not require the SPRP assumption but require the PRP one.

5.3 Remark

Since $\mathbb{OTR}$ does not require the decryption function of a TBC, XKX can be replaced with XK. In ΘCB3, the decryption function is not required for handling associated data and generating a tag. Hence, for the TBC calls, XKX can be replaced with XK.

6 Discussions

6.1 Study of Security Bounds of XKX-based Schemes

We study the security bounds of ΘCB3[XKX] given in Subsection 5.1. Note that this study is applicable to $\mathbb{OTR}$ with XKX. For the sake of simplicity, we assume that for each encryption query, the number of blockcipher calls except for those handling associated data is ℓ. We use an optimal parameter $\epsilon = 1/2^n$.

6.1.1 Security Bounds of ΘCB3[XKX]

The privacy bound becomes roughly

$$q_{\mathcal{E}} \cdot \mathbf{Adv}_E^{\mathsf{sprp}}(\mathbf{A}_E) + \mathbf{Adv}_F^{\mathsf{prf}}(\mathbf{A}_F) + \frac{\sigma_A^2 + \ell^2 q_{\mathcal{E}}}{2^n} \ \text{(privacy)} \ .$$

Regarding the authenticity bound, $\sum_{N \in \mathcal{N}} \ell_N^2 \cdot \epsilon$ becomes maximum if an adversary makes decryption queries whose nonces are the same and appear in some encryption query, thus this term is at most $(\ell^2(q-1) + (\ell + \sigma_{\mathcal{D}})^2)/2^n$. Hence, the authenticity bound becomes roughly

$$q \cdot \mathbf{Adv}_E^{\mathsf{sprp}}(\mathbf{A}_E) + \mathbf{Adv}_F^{\mathsf{prf}}(\mathbf{A}_F) + \frac{\sigma_A^2 + \ell^2 q + \sigma_{\mathcal{D}}^2}{2^n} \ \text{(authenticity)} \ .$$

Next, we assume that $\mathbf{Adv}_E^{\mathsf{sprp}}(\mathbf{A}_E) \approx \ell q_{\mathcal{E}}/2^k$ or $\mathbf{Adv}_E^{\mathsf{sprp}}(\mathbf{A}_E) \approx \ell q/2^k$ (achieved by the exhaustive key search, see [BKR98]), and terms with σ_A and $\sigma_{\mathcal{D}}$ are sufficiently small (e.g., associated data is fixed and the number of fails in decryption queries is limited). Then the privacy and authenticity bounds become roughly

$$\frac{\ell q_{\mathcal{E}}^2}{2^k} + \mathbf{Adv}_F^{\mathsf{prf}}(\mathbf{A}_F) + \frac{\ell^2 q_{\mathcal{E}}}{2^n} \ \text{(privacy)} \qquad \frac{\ell q^2}{2^k} + \mathbf{Adv}_F^{\mathsf{prf}}(\mathbf{A}_F) + \frac{\ell^2 q}{2^n} \ \text{(authenticity)} \ .$$

These bounds ensure that if the key terms $\ell q^2/2^k$ and $\mathbf{Adv}_F^{\mathsf{prf}}(\mathbf{A}_F)$ can be negligible, then the security bounds of the XKX-based schemes become $O(\ell^2 q/2^n)$.

6.1.2 Blockcipher-based Instantiations

We adopt instantiations given in Section 4 to XKX. Here, XKX using function $F^{(i)}$ is denoted by $\mathrm{XKX}^{(i)}$. By Lemma 3 and 4, the privacy and authenticity bounds become roughly

- $\Theta\mathrm{CB3}[\mathrm{XKX}^{(1)}]$:

$$\frac{\ell q_{\mathcal{E}}^2}{2^k} + \frac{q_{\mathcal{E}}^2}{2^n} + \frac{\ell^2 q_{\mathcal{E}}}{2^n} \ \text{(privacy)} \qquad \frac{\ell q^2}{2^k} + \frac{q^2}{2^n} + \frac{\ell^2 q}{2^n} \ \text{(authenticity)} \tag{1}$$

- $\Theta\mathrm{CB3}[\mathrm{XKX}^{(2)}]$:

$$\frac{\ell q_{\mathcal{E}}^2}{2^k} + \frac{\ell^2 q_{\mathcal{E}}}{2^n} \ \text{(privacy)} \qquad \frac{\ell q^2}{2^k} + \frac{\ell^2 q}{2^n} \ \text{(authenticity)} \tag{2}$$

Hence, these bounds are beyond the birthday ones (The birthday bound is $(\ell q)^2/2^n$). The term $\ell q^2/2^k$ depends on the key size k, thus using a blockcipher with long-size keys, these terms can be negligible, e.g., $k = 2n$. AES and many lightweight blockciphers support this parameter (AES: $n = 128$ and $k = 256$, PRESENT: $n = 64$ and $k = 128$, etc.). If this term can be negligible, then the above bounds become $O(q^2/2^n + \ell^2 q/2^n)$ ($\Theta\mathrm{CB3}[\mathrm{XKX}^{(1)}]$) and $O(\ell^2 q/2^n)$ ($\Theta\mathrm{CB3}[\mathrm{XKX}^{(2)}]$).

6.2 Study of the Key Terms $q \cdot \mathbf{Adv}_{E}^{\mathsf{sprp}}(\mathbf{A}_E)$ and $\mathbf{Adv}_{F}^{\mathsf{prf}}(\mathbf{A}_F)$

The security bounds of XKX-based schemes have the term $q \cdot \mathbf{Adv}_{E}^{\mathsf{sprp}}(\mathbf{A}_E)$. This term comes from the construction of XKX, where q-blockcipher's keys are defined via the first tweak function. As mentioned in [ST16], the hybrid factor is not real, but rather an artifact of the proof technique, and this term might be improved by analyzing the term in the ideal cipher model (ICM). On the other hand, the ICM analysis provides only a security heuristic, and seems particularly inappropriate when the underlying blockcipher is know to have obvious non-ideal behavior for certain weak-key class matters, or to suffer from related-key attack. However, in the XKX-based schemes the blockcipher's keys are randomly drawn, thereby the presence of weak keys is unlikely to be a real issue in the XKX-based schemes. In this paper, we study the security of XKX-based schemes in the ICM, and show that this term can be improved.

Recall the proof of Theorem 1. The terms $q \cdot \mathbf{Adv}_{E}^{\mathsf{sprp}}(\mathbf{A}_E)$ and $\mathbf{Adv}_{F}^{\mathsf{prf}}(\mathbf{A}_F)$ are introduced in Subsubsection 3.3.1, where Min is replaced with a tweakable random permutation. The following lemma analyzes this replacement in the ICM, where the underlying blockcipher is replaced with an ideal cipher, and the first tweak function is replaced with a random function. Here, direct queries to the ideal cipher are called offline queries, and queries to XKX are called online queries. XKX using an ideal cipher E, a random function f and a key of the second tweak function K_h is denoted by $\mathrm{XKX}[f,E]_{K_h}$. Let $\mathrm{XKX}[f,E]_{K_h}^{\pm} = (\mathrm{XKX}[f,E]_{K_h}, \mathrm{XKX}[f,E]_{K_h}^{-1})$ and $E^{\pm} = (E, E^{-1})$.

Lemma 5. *Assume that $\mathcal{H}$ is (ϵ,δ)-AXU. Let $\mathbf{A}$ be a computationally unbounded adversary trying to distinguish* $\mathsf{World1}$ *from* $\mathsf{World2}$*. Here, $\mathbf{A}$ makes σ online queries with q first tweaks and Q offline queries. Then we have*

$$\Pr[\mathsf{World1}] - \Pr[\mathsf{World2}] \le \frac{2\sigma Q\delta}{2^k} + \frac{q^2}{2^{k+1}} \ ,$$

where

$$\mathsf{World1} :=$$
$$\left(E \xleftarrow{\$} \mathsf{BC}(\{0,1\}^k, \{0,1\}^n); f \xleftarrow{\$} \mathsf{Func}(\mathcal{TW}_N, \{0,1\}^k); K_h \xleftarrow{\$} \mathcal{K}_h; \mathbf{A}^{\mathrm{XKX}[f,E]_{K_h}^{\pm}, E^{\pm}} \Rightarrow 1\right)$$
$$\mathsf{World2} :=$$
$$\left(E \xleftarrow{\$} \mathsf{BC}(\{0,1\}^k, \{0,1\}^n); \widetilde{P}_R \xleftarrow{\$} \widetilde{\mathsf{Perm}}(\mathcal{TW}_N, \{0,1\}^n); K_h \xleftarrow{\$} \mathcal{K}_h; \mathbf{A}^{\widetilde{F}[\widetilde{P}_R]_{K_h}^{\pm}, E^{\pm}} \Rightarrow 1\right) \ .$$

proof sketch. In this part, a sketch of the security proof is given, and the full proof is given in Subsection 6.3.

From $\mathsf{World1}$ to $\mathsf{World2}$, Min is replaced with a tweakable random permutation. Hence, we need to evaluate the distinguishing probability coming from the structural differences. There are two differences given in the following.

- **Difference 1:** The difference comes from the (in)dependence between online and offline queries. In $\mathsf{World1}$, responses of online and offline queries are defined by using an ideal cipher. On the other hand, in $\mathsf{World2}$, responses of online queries are defined independently of an ideal cipher.

- **Difference 2:** The difference comes from the (in)dependence between online queries with distinct first tweaks. In $\mathsf{World1}$, for two online queries with distinct first tweaks, if the blockcipher's keys are the same (that is, a collision occurs in outputs of f), the responses are defined by the same permutation (or a blockcipher with the same key). On the other hand, in $\mathsf{World2}$, for two online queries with distinct first tweaks, the responses are defined by the distinct permutations.

Regarding Difference 1, in $\mathsf{World1}$, the independence between online and offline queries might not be ensured, if blockcipher's inputs (or outputs) by online queries and by offline ones overlap with each other. This means that one of pairs for (w, x) (or (w, y)) appears in offline queries, where x is the input block of the blockcipher, w is the blockcipher's key, and y is the output of the blockcipher, defined in XKX. Since w is randomly drawn from $\{0,1\}^n$ by a random function f, and x and y are defined by the AXU hash function, the collision (or overlapping) probability is at most $2\sigma Q \cdot \delta/2^k$. The factor "2" comes from collisions for input blocks and for output blocks.

Regarding Difference 2, in $\mathsf{World1}$, the independence between online queries with distinct first tweaks might not be ensured if a collision occurs in outputs of f. Since there are at most q inputs to f, the collision probability is, by the birthday analysis, at most $q^2/2^{k+1}$.

By summing these probabilities, the upper-bound of the lemma is obtained. □

Using the optimal parameters $\epsilon = \delta = 1/2^n$ and assuming $Q \approx \ell q$, the above bound becomes roughly $(\ell q)^2/2^{n+k} + q^2/2^k$. This bound offers the upper-bounds of the ICM-security of ΘCB3[XKX$^{(1)}$] and ΘCB3[XKX$^{(2)}$] given in the following.

- ΘCB3[XKX$^{(1)}$]:

$$\frac{q_{\mathcal{E}}^2}{2^n} + \frac{\ell^2 q_{\mathcal{E}}}{2^n} \text{ (privacy)} \qquad \frac{q^2}{2^n} + \frac{\ell^2 q}{2^n} \text{ (authenticity)} \tag{3}$$

- ΘCB3[XKX$^{(2)}$]:

$$\frac{q_{\mathcal{E}}^2}{2^k} + \frac{\ell^2 q_{\mathcal{E}}}{2^n} \text{ (privacy)} \qquad \frac{q^2}{2^k} + \frac{\ell^2 q}{2^n} \text{ (authenticity)} \tag{4}$$

In the security bounds of XKX-based schemes, the term in the standard model, $\ell q^2/2^k$, is improved to $q^2/2^k$ in the ICM. Note that $(\ell q)^2/2^{n+k}$ can be negligible compared with $\ell^2 q/2^n$. Hence, query length ℓ becomes independent from the key size in the ICM. Finally, the term $q^2/2^n$ comes from the PRF/PRP switch for the first tweak function F. If the underlying blockcipher is not influenced by the switch, that is, the term $q^2/2^n$ can be eliminated, then the XKX$^{(1)}$-based schemes achieve the same level of security as the XKX$^{(2)}$-based ones. Indeed, from $\mathsf{World1}$ to $\mathsf{World2}$, the term $q^2/2^n$ is introduced by Difference 2 that considers a collision in outputs of f. Using $F^{(1)}$ instead of f, since such collision does not occur due to the use of blockcipher's outputs, one does not have to consider Difference 2 and the term $q^2/2^n$ is eliminated.

6.3 Proof of Lemma 5

In this proof, the upper-bound of the difference $\Pr[\mathsf{World1}] - \Pr[\mathsf{World2}]$ is given, where

$$\begin{aligned}
\mathsf{World1} := \Big(& E \xleftarrow{\$} \mathsf{BC}(\{0,1\}^k, \{0,1\}^n); f \xleftarrow{\$} \mathsf{Func}(\mathcal{TW}_N, \{0,1\}^k); \\
& \qquad K_h \xleftarrow{\$} \mathcal{K}_h; \mathbf{A}^{\mathrm{XKX}[f,E]^{\pm}_{K_h}, E^{\pm}} \Rightarrow 1 \Big) \\
\mathsf{World2} := \Big(& E \xleftarrow{\$} \mathsf{BC}(\{0,1\}^k, \{0,1\}^n); \widetilde{P}_R \xleftarrow{\$} \widetilde{\mathsf{Perm}}(\mathcal{TW}_N, \{0,1\}^n); \\
& \qquad \underline{f \xleftarrow{\$} \mathsf{Func}(\mathcal{TW}_N, \{0,1\}^k);} K_h \xleftarrow{\$} \mathcal{K}_h; \mathbf{A}^{\widetilde{F}[\widetilde{P}_R]^{\pm}_{K_h}, E^{\pm}} \Rightarrow 1 \Big) .
\end{aligned}$$

Note that in $\mathsf{World2}$, a random function f (on the underlined statement) is introduced. It is used in this proof but is not used to define responses of $\mathbf{A}$'s queries. Thus this modification does not change $\mathbf{A}$'s behavior. In this proof, the query-response triple at the α-th online query are denoted by $(tw^\alpha, m^\alpha, c^\alpha)$, and the corresponding values such as v, w, x, y are denoted by using the superscript character of α. The query-response triple at the β-th offline query are denoted by $(W^\beta, X^\beta, Y^\beta)$, where $Y^\beta = E(W^\beta, X^\beta)$ if the β-th offline query is a query to E and $X^\beta = E^{-1}(W^\beta, Y^\beta)$ if the β-th offline query is a query to E^{-1}.

Transcript. After **A**'s interaction, it obtains the following list:

$$\left(\bigcup_{\alpha=1}^{q} \{(tw^\alpha, m^\alpha, c^\alpha)\}, \bigcup_{\beta=1}^{Q} \{(W^\beta, X^\beta, Y^\beta)\} \right) \ .$$

The list is referred as transcript. Let T_1 be the transcript in $\mathsf{World1}$ obtained by sampling $E \xleftarrow{\$} \mathsf{BC}(\{0,1\}^k, \{0,1\}^n)$, $f \xleftarrow{\$} \mathsf{Func}(\mathcal{TW}_N, \{0,1\}^k)$ and $K_h \xleftarrow{\$} \mathcal{K}_h$. Let T_2 be the transcript in $\mathsf{World2}$ obtained by sampling $E \xleftarrow{\$} \mathsf{BC}(\{0,1\}^k, \{0,1\}^n)$, $\widetilde{P}_R \xleftarrow{\$} \widetilde{\mathsf{Perm}}(\mathcal{TW}_N, \{0,1\}^n)$, $f \xleftarrow{\$} \mathsf{Func}(\mathcal{TW}_N, \{0,1\}^k)$ and $K_h \xleftarrow{\$} \mathcal{K}_h$. We call a transcript τ *valid* if an interaction with their oracles could render this transcript, namely, $\Pr[\mathsf{T}_i = \tau] > 0$ for $i \in \{1, 2\}$. Then $\Pr[\mathsf{World1}] - \Pr[\mathsf{World2}]$ is upper-bounded by the statistical distance of transcripts, i.e.,

$$\Pr[\mathsf{World1}] - \Pr[\mathsf{World2}] \leq \mathsf{SD}(\mathsf{T}_1, \mathsf{T}_2) = \frac{1}{2} \sum_{\tau} |\Pr[\mathsf{T}_1 = \tau] - \Pr[\mathsf{T}_2 = \tau]| \ ,$$

where the sum is over all valid transcripts.

Coefficient H Technique. In this proof, the coefficient H technique [CS14, Pat08] is used, where valid transcripts $\mathcal{T}$ are partitioned into good transcripts $\mathcal{T}_{\mathsf{good}}$ and bad transcripts $\mathcal{T}_{\mathsf{bad}}$. Then $\mathsf{SD}(\mathsf{T}_1, \mathsf{T}_2)$ can be upper-bounded by the following lemma.

Lemma 6. *Let $0 \leq \varepsilon \leq 1$ be such that for all $\tau \in \mathcal{T}_{\mathsf{good}}$, $\frac{\Pr[\mathsf{T}_1=\tau]}{\Pr[\mathsf{T}_2=\tau]} \geq 1 - \varepsilon$. Then, $\mathsf{SD}(\mathsf{T}_1, \mathsf{T}_2) \leq \Pr[\mathsf{T}_2 \in \mathcal{T}_{\mathsf{bad}}] + \varepsilon$.*

Hereafter, good and bad transcripts are defined. Then ε and $\Pr[\mathsf{T}_2 \in \mathcal{T}_{\mathsf{bad}}]$ are upper-bounded. Finally, the upper-bound of the difference $\Pr[\mathsf{World1}] - \Pr[\mathsf{World2}]$ is obtained by putting these upper-bounds into the above lemma.

Good and Bad Transcripts. Bad transcripts $\mathcal{T}_{\mathsf{bad}}$ are defined so that one of the following conditions is satisfied, and good transcripts $\mathcal{T}_{\mathsf{good}}$ are defined so that these conditions are not satisfied.

- $\mathsf{hit} \Leftrightarrow \exists \alpha \in [q], \beta \in [Q]$ s.t. $(w^\alpha, x^\alpha) = (W^\beta, X^\beta)$ or $(w^\alpha, y^\alpha) = (W^\beta, Y^\beta)$.
- $\mathsf{coll} \Leftrightarrow \exists \alpha, \beta \in [q]$ with $N^\alpha \neq N^\beta$ s.t. $w^\alpha = w^\beta$.

In $\mathsf{World2}$, w^α is defined as $w^\alpha \leftarrow f(N^\alpha)$. The first condition considers a collision in query-response triples among online and offline queries. The second condition considers a collision in query-response triples by online queries (more precisely, a collision in blockcipher's keys).

Upper-Bound of $\Pr[\mathsf{T}_2 \in \mathcal{T}_{\mathsf{bad}}]$. By the definition of bad transcripts,

$$\Pr[\mathsf{T}_2 \in \mathcal{T}_{\mathsf{bad}}] = \Pr[\mathsf{hit} \vee \mathsf{coll}] \leq \Pr[\mathsf{hit}] + \Pr[\mathsf{coll}] \ .$$

Note that these probabilities are considered in $\mathsf{World2}$. Hereafter, $\Pr[\mathsf{hit}]$ and $\Pr[\mathsf{coll}]$ are upper-bounded.

First, $\Pr[\mathsf{hit}]$ is upper-bounded. Fix $\alpha \in [q]$ and $\beta \in [Q]$. Then $(w^\alpha, x^\alpha) = (W^\beta, X^\beta)$ implies

$$\left(w^\alpha = f(N^\alpha) = W^\beta\right) \wedge \left(m^\alpha \oplus h_{K_h}(ctr^\alpha) = X^\beta\right) \ .$$

Since w^α is randomly drawn from $\{0,1\}^k$, the probability that $w^\alpha = W^\beta$ is at most $1/2^k$. By the AXU hash function, the probability that $m^\alpha \oplus h_{K_h}(ctr^\alpha) = X^\beta$ is at most δ. Similarly, the probability that $(w^\alpha, y^\alpha) = (W^\beta, Y^\beta)$ is at most $\delta/2^k$. By $\alpha \in [q]$ and $\beta \in [Q]$, we have $\Pr[\mathsf{hit}] \leq 2qQ\delta/2^k$.

Next, $\Pr[\mathsf{coll}]$ is upper-bounded. Since there are q distinct first tweaks, we have $\Pr[\mathsf{coll}] \leq \binom{q}{2}/2^k \leq q^2/2^{k+1}$.

Combining these upper-bounds gives

$$\Pr[\mathsf{T}_2 \in \mathcal{T}_{\mathsf{bad}}] \leq \frac{2qQ\delta}{2^k} + \frac{q^2}{2^{k+1}} \ .$$

Upper-Bound of ε. Let $\tau \in \mathcal{T}_{\mathsf{good}}$ be a good transcript that does not satisfy hit and coll. Let $N_{\mathrm{on}}(w)$ be the number of online queries such that the corresponding f's outputs equal w (in $\mathsf{World1}$ w is a blockcipher's key defined by an online query), $N_{\mathrm{off}}(W)$ the number of offline queries whose keys equal W.

Let all_1 (resp. all_2) be the set of all oracles in $\mathsf{World1}$ (resp. $\mathsf{World2}$). Let $\mathrm{comp}_1(\tau)$ (resp. $\mathrm{comp}_2(\tau)$) be the set of oracles compatible with τ in $\mathsf{World1}$ (resp., $\mathsf{World2}$). Then

$$\Pr[\mathsf{T}_1 = \tau] = \frac{|\mathrm{comp}_1(\tau)|}{|\mathrm{all}_1|} \text{ and } \Pr[\mathsf{T}_2 = \tau] = \frac{|\mathrm{comp}_2(\tau)|}{|\mathrm{all}_2|} \ .$$

By $E \in \mathsf{BC}(\{0,1\}^k, \{0,1\}^n)$ and $f \in \mathsf{Func}(\mathcal{TW}_N, \{0,1\}^k)$, we have

$$|\mathrm{all}_1| = (2^n!)^{2^k} \cdot |\mathsf{Func}(\mathcal{TW}_N, \{0,1\}^k)| \ .$$

By $\widetilde{P}_R \in \widetilde{\mathsf{Perm}}(\mathcal{TW}_N, \{0,1\}^n)$, $E \in \mathsf{BC}(\{0,1\}^k, \{0,1\}^n)$ and $f \in \mathsf{Func}(\mathcal{TW}_N, \{0,1\}^k)$, we have

$$|\mathrm{all}_2| = (2^n!)^{|\mathcal{TW}_N|} \cdot (2^n!)^{2^k} \cdot |\mathsf{Func}(\mathcal{TW}_N, \{0,1\}^k)| \ .$$

$|\mathrm{comp}_1(\tau)|$ is counted. Let $N_{f,\tau}$ be the number of functions in $\mathsf{Func}(\mathcal{TW}_N, \{0,1\}^k)$ compatible with τ. By $\neg\mathsf{hit}$, blockcipher evaluations by online and offline queries don't overlap with each other, thereby for each $w \in \{0,1\}^k$, the number of elements whose keys equal w is $N_{\mathrm{on}}(w) + N_{\mathrm{off}}(w)$. K_h is uniquely determined. Hence, we have

$$|\mathrm{comp}_1(\tau)| = N_{f,\tau} \cdot \prod_{w \in \{0,1\}^k} (2^n - N_{\mathrm{on}}(w) - N_{\mathrm{off}}(w))! \ .$$

Next, $|\mathrm{comp}_2(\tau)|$ is counted. Let $N_{\widetilde{E},\mathrm{on}}(tw)$ be the number of online queries whose first tweaks equal tw.

$$\begin{aligned}
&|\mathrm{comp}_2(\tau)| \\
&= N_{f,\tau} \cdot \prod_{tw \in \mathcal{TW}_N} (2^n - N_{\widetilde{E},\mathrm{on}}(tw))! \cdot \prod_{w \in \{0,1\}^k} (2^n - N_{\mathrm{off}}(w)) && (5) \\
&= N_{f,\tau} \cdot (2^n!)^{|\mathcal{TW}_N| - 2^k} \cdot \prod_{w \in \{0,1\}^k} (2^n - N_{\mathrm{on}}(w))! \cdot \prod_{w \in \{0,1\}^k} (2^n - N_{\mathrm{off}}(w))! && (6) \\
&\leq N_{f,\tau} \cdot (2^n!)^{|\mathcal{TW}_N|} \cdot \prod_{w \in \{0,1\}^k} (2^n - N_{\mathrm{on}}(w) - N_{\mathrm{off}}(w))! \ . && (7)
\end{aligned}$$

Regarding (5) = (6), since $tw^\alpha = tw^\beta \Rightarrow w^\alpha = w^\beta$ and $tw^\alpha \neq tw^\beta \Rightarrow w^\alpha \neq w^\beta$ (by $\neg\mathsf{coll}$), the equality is satisfied. Regarding (6) $\leq$ (7), using $(2^n - a)! \cdot (2^n - b)! \leq 2^n! \cdot (2^n - a - b)!$ for any $0 \leq a, b \leq 2^n$, the inequality is satisfied.

Finally,

$$\frac{\Pr[\mathsf{T}_R = \tau]}{\Pr[\mathsf{T}_I = \tau]} \geq \frac{N_{f,\tau} \cdot \prod_{w \in \{0,1\}^k} (2^n - N_{\mathrm{on}}(w) - N_{\mathrm{off}}(w))!}{(2^n!)^{2^k} \times |\mathsf{Func}(\mathcal{TW}_N, \{0,1\}^k)|} \times \frac{(2^n!)^{|\mathcal{TW}_N|} \cdot (2^n!)^{2^k} \cdot |\mathsf{Func}(\mathcal{TW}_N, \{0,1\}^k)|}{N_{f,\tau} \cdot (2^n!)^{|\mathcal{TW}_N|} \cdot \prod_{w \in \{0,1\}^k} (2^n - N_{\mathrm{on}}(w) - N_{\mathrm{off}}(w))!} = 1 \ .$$

Thus we have $\varepsilon = 0$.

Conclusion of the Proof. Putting the above bounds to Lemma 6 gives

$$\Pr[\mathsf{World1}] - \Pr[\mathsf{World2}] \leq \frac{2qQ\delta}{2^k} + \frac{q^2}{2^{k+1}} \ .$$

$\square$

Acknowledgements

We would like to thank Jérémy Jean and the anonymous reviewers for their comments and suggestions.

References

[ADMA15] Elena Andreeva, Joan Daemen, Bart Mennink, and Gilles Van Assche. Security of keyed sponge constructions using a modular proof approach. In Leander [Lea15], pages 364–384.

[AJN] Jean-Philippe Aumasson, Philipp Jovanovic, and Samuel Neves. NORX v3.0, Third-Round Candidates in CAESAR Competition.

[BDP+a] Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche, and Ronny Van Keer. CAESAR submission: Keyak v2, Third-Round Candidates in CAESAR Competition.

[BDP+b] Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche, and Ronny Van Keer. CAESAR submission: Keyak v2, Third-Round Candidates in CAESAR Competition.

[BDPA08] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. On the indifferentiability of the sponge construction. In Nigel P. Smart, editor, *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, volume 4965 of *Lecture Notes in Computer Science*, pages 181–197. Springer, 2008.

[BDPA11] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Duplexing the sponge: Single-pass authenticated encryption and other applications. In Ali Miri and Serge Vaudenay, editors, *Selected Areas in Cryptography - 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers*, volume 7118 of *Lecture Notes in Computer Science*, pages 320–337. Springer, 2011.

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: an ultra-lightweight block cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*, volume 4727 of *Lecture Notes in Computer Science*, pages 450–466. Springer, 2007.

[BKR98] Mihir Bellare, Ted Krovetz, and Phillip Rogaway. Luby-rackoff backwards: Increasing security by making block ciphers non-invertible. In Kaisa Nyberg, editor, *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*, pages 266–280. Springer, 1998.

[BL16] Karthikeyan Bhargavan and Gaëtan Leurent. On the practical (in-)security of 64-bit block ciphers: Collision attacks on HTTP over TLS and openvpn. In Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, pages 456–467. ACM, 2016.

[BN08] Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. *J. Cryptology*, 21(4):469–491, 2008.

[CDMS10] Jean-Sébastien Coron, Yevgeniy Dodis, Avradip Mandal, and Yannick Seurin. A domain extender for the ideal cipher. In Daniele Micciancio, editor, *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*, pages 273–289. Springer, 2010.

[CLS15] Benoit Cogliati, Rodolphe Lampe, and Yannick Seurin. Tweaking even-mansour ciphers. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, volume 9215 of *Lecture Notes in Computer Science*, pages 189–208. Springer, 2015.

[CS08] Debrup Chakraborty and Palash Sarkar. A general construction of tweakable block ciphers and different modes of operations. *IEEE Trans. Information Theory*, 54(5):1991–2006, 2008.

[CS14] Shan Chen and John P. Steinberger. Tight security bounds for key-alternating ciphers. In Nguyen and Oswald [NO14], pages 327–350.

[CS15] Benoît Cogliati and Yannick Seurin. Beyond-birthday-bound security for tweakable even-mansour ciphers with linear tweak and key mixing. In Iwata and Cheon [IC15], pages 134–158.

[CT16] Jung Hee Cheon and Tsuyoshi Takagi, editors. *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I*, volume 10031 of *Lecture Notes in Computer Science*, 2016.

[CW79] Larry Carter and Mark N. Wegman. Universal classes of hash functions. *J. Comput. Syst. Sci.*, 18(2):143–154, 1979.

[DEMS] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ason v1.2, Third-Round Candidates in CAESAR Competition.

[Dun09] Orr Dunkelman, editor. *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.

[EM97] Shimon Even and Yishay Mansour. A construction of a cipher from a single pseudorandom permutation. *J. Cryptology*, 10(3):151–162, 1997.

[FLLW16] Christian Forler, Eik List, Stefan Lucks, and Jakob Wenzel. Efficient beyond-birthday-bound-secure deterministic authenticated encryption with minimal stretch. In Joseph K. Liu and Ron Steinfeld, editors, *Information Security and Privacy - 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part II*, volume 9723 of *Lecture Notes in Computer Science*, pages 317–332. Springer, 2016.

[GJMN16] Robert Granger, Philipp Jovanovic, Bart Mennink, and Samuel Neves. Improved masking for tweakable blockciphers with applications to authenticated encryption. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I*, volume 9665 of *Lecture Notes in Computer Science*, pages 263–293. Springer, 2016.

[IC15] Tetsu Iwata and Jung Hee Cheon, editors. *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, volume 9453 of *Lecture Notes in Computer Science*. Springer, 2015.

[IM16] Tetsu Iwata and Kazuhiko Minematsu. Stronger security variants of GCM-SIV. *IACR Trans. Symmetric Cryptol.*, 2016(1):134–157, 2016.

[IMV16] Tetsu Iwata, Bart Mennink, and Damian Vizár. CENC is optimally secure. *IACR Cryptology ePrint Archive*, 2016:1087, 2016.

[Iwa08] Tetsu Iwata. Authenticated encryption mode for beyond the birthday bound security. In Serge Vaudenay, editor, *Progress in Cryptology - AFRICACRYPT 2008, First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008. Proceedings*, volume 5023 of *Lecture Notes in Computer Science*, pages 125–142. Springer, 2008.

[IY09a] Tetsu Iwata and Kan Yasuda. BTM: A single-key, inverse-cipher-free mode for deterministic authenticated encryption. In Michael J. Jacobson Jr., Vincent Rijmen, and Reihaneh Safavi-Naini, editors, *Selected Areas in Cryptography, 16th Annual International Workshop, SAC 2009, Calgary, Alberta, Canada, August 13-14, 2009, Revised Selected Papers*, volume 5867 of *Lecture Notes in Computer Science*, pages 313–330. Springer, 2009.

[IY09b] Tetsu Iwata and Kan Yasuda. HBS: A single-key mode of operation for deterministic authenticated encryption. In Dunkelman [Dun09], pages 394–415.

[JLM14] Philipp Jovanovic, Atul Luykx, and Bart Mennink. Beyond 2 c/2 security in sponge-based authenticated encryption modes. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 - 20th International*

Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I, volume 8873 of *Lecture Notes in Computer Science*, pages 85–104. Springer, 2014.

[KR11] Ted Krovetz and Phillip Rogaway. The software performance of authenticated-encryption modes. In Antoine Joux, editor, *Fast Software Encryption - 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, 2011, Revised Selected Papers*, volume 6733 of *Lecture Notes in Computer Science*, pages 306–327. Springer, 2011.

[Lea15] Gregor Leander, editor. *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.

[LN17] Eik List and Mridul Nandi. Revisiting full-prf-secure PMAC and using it for beyond-birthday authenticated encryption. In Helena Handschuh, editor, *Topics in Cryptology - CT-RSA 2017 - The Cryptographers' Track at the RSA Conference 2017, San Francisco, CA, USA, February 14-17, 2017, Proceedings*, volume 10159 of *Lecture Notes in Computer Science*, pages 258–274. Springer, 2017.

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

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

[LST12] Will Landecker, Thomas Shrimpton, and R. Seth Terashima. Tweakable blockciphers with beyond birthday-bound security. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, volume 7417 of *Lecture Notes in Computer Science*, pages 14–30. Springer, 2012.

[Luc00] Stefan Lucks. The sum of prps is a secure PRF. In Bart Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, volume 1807 of *Lecture Notes in Computer Science*, pages 470–484. Springer, 2000.

[Men15] Bart Mennink. Optimally secure tweakable blockciphers. In Leander [Lea15], pages 428–448.

[Min09] Kazuhiko Minematsu. Beyond-birthday-bound security based on tweakable block cipher. In Dunkelman [Dun09], pages 308–326.

[Min14] Kazuhiko Minematsu. Parallelizable rate-1 authenticated encryption from pseudorandom functions. In Nguyen and Oswald [NO14], pages 275–292.

[MRV15] Bart Mennink, Reza Reyhanitabar, and Damian Vizár. Security of full-state keyed sponge and duplex: Applications to authenticated encryption. In Iwata and Cheon [IC15], pages 465–489.

[NO14] Phong Q. Nguyen and Elisabeth Oswald, editors. *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*. Springer, 2014.

[Pat04] Jacques Patarin. Security of random feistel schemes with 5 or more rounds. In Matthew K. Franklin, editor, *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, volume 3152 of *Lecture Notes in Computer Science*, pages 106–122. Springer, 2004.

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

[Pat10] Jacques Patarin. Introduction to mirror theory: Analysis of systems of linear equalities and linear non equalities for cryptography. *IACR Cryptology ePrint Archive*, 2010:287, 2010.

[PS16] Thomas Peyrin and Yannick Seurin. Counter-in-tweak: Authenticated encryption modes for tweakable block ciphers. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I*, volume 9814 of *Lecture Notes in Computer Science*, pages 33–63. Springer, 2016.

[RBBK01] Phillip Rogaway, Mihir Bellare, John Black, and Ted Krovetz. OCB: a block-cipher mode of operation for efficient authenticated encryption. In Michael K. Reiter and Pierangela Samarati, editors, *CCS 2001, Proceedings of the 8th ACM Conference on Computer and Communications Security, Philadelphia, Pennsylvania, USA, November 6-8, 2001.*, pages 196–205. ACM, 2001.

[Rog02] Phillip Rogaway. Authenticated-encryption with associated-data. In Vijayalakshmi Atluri, editor, *Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS 2002, Washington, DC, USA, November 18-22, 2002*, pages 98–107. ACM, 2002.

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

[ST16] Thomas Shrimpton and R. Seth Terashima. Salvaging weak security bounds for blockcipher-based constructions. In Cheon and Takagi [CT16], pages 429–454.

[WGZ+16] Lei Wang, Jian Guo, Guoyan Zhang, Jingyuan Zhao, and Dawu Gu. How to build fully secure tweakable blockciphers from classical blockciphers. In Cheon and Takagi [CT16], pages 455–483.