# On the Provable Security of the Tweakable Even-Mansour Cipher Against Multi-Key and Related-Key Attacks

Ping Zhang and Honggang Hu

Key Laboratory of Electromagnetic Space information, CAS
University of Science and Technology of China, Hefei, China, 230027
hghu2005@ustc.edu.cn,996602767@qq.com

**Abstract.** Cogliati et al. introduced the tweakable Even-Mansour cipher constructed from a single permutation and an almost-XOR-universal (AXU) family of hash functions with tweak and key schedule. Most of previous papers considered the security of the (iterated) tweakable Even-Mansour cipher in the single-key setting. In this paper, we focus on the security of the tweakable Even-Mansour cipher in the multi-key and related-key settings. We prove that the tweakable Even-Mansour cipher with related-key-AXU hash functions is secure against multi-key and related-key attacks, and derive a tight bound using H-coefficients technique, respectively. Our work is of high practical relevance because of rekey requirements and the inevitability of related keys in real-world implementations.

**Keywords:** Tweakable Even-Mansour, almost-XOR-universal hash functions, multi-key attack, related-key attack, H-coefficient technique.

## 1 Introduction

A tweakable blockcipher (TBC) is a generalization of a traditional block cipher, which adds a tweak as an extra public input on the basis of the usual inputs (a plaintext and a key). Tweakable blockciphers (TBCs) with distinct tweaks refer to distinct block ciphers, which makes that the cost of tweaks' update is lower than that of rekeys. The original application scenarios of TBCs focus on storage encryptions, especially the disk sector encryption [17] (Each disk consists of fixed-length sectors. The size of a sector is usually 512 bytes. In the disk sector encryption, we need to encrypt a plaintext $x$ under the sector location $t \in \mathcal{T}$ and obtain the corresponding ciphertext $y = \mathcal{E}_K(t, x)$, where $K$ is a key and $\mathcal{E}_K$ is an encryption algorithm with a tweak space $\mathcal{T}$. Moreover, the encryption with distinct sectors is mutual independent). Now TBCs have been extended to all the modes of operation, such as encryption modes [18,1,28], message authentication codes (MACs) [22,21], and authenticated encryption (AE) modes [22,29,30,16,7].

There exists three approaches to realize a tweakable blockcipher. The first approach is based on a block cipher [22]. The second approach is based on a permutation [13]. The third approach is based on a keyed-function (hash function) [27]. The tweakable Even-Mansour cipher [11] is a permutation-based tweakable blockcipher, which is constructed from an $n$-bit public random permutation $P$ and an almost XOR-universal (AXU) family of hash functions $\mathcal{H} = (H_K)_{K\in\mathcal{K}}$ from some set $\mathcal{T}$ to $\{0,1\}^n$, and defined as

$$y = TEM_K^P(t,x) = P(x \oplus H_K(t)) \oplus H_K(t),$$

where $K \in \mathcal{K}$ is a key, $t \in \mathcal{T}$ is a tweak, $x \in \{0,1\}^n$ is a plaintext, and $y \in \{0,1\}^n$ is a ciphertext.

According to the different key settings in the applications, Mouha and Luykx [24] described three attack settings: single-key, multi-key, and related-key settings. In the single-key setting, an adversary has access to the encryption and decryption oracles under a fixed key $K$ chosen uniformly and randomly from the key space. Most of previous papers considered the security in the single-key setting. The tweakable Even-Mansour cipher is no exception. The security of the tweakable Even-Mansour cipher in the single-key setting was studied by Cogliati, Lampe, and Seurin [11], and was proved secure up to the birthday bound (this construction ensures security up to $2^{n/2}$ adversarial queries, in the random permutation model (RPM) for $P : \{0,1\}^n \to \{0,1\}^n$).

In the multi-key setting, an adversary has access to the encryption and decryption oracles under many keys $K_i$ $(i \geq 2)$ chosen independently and randomly from the key space. Multi-key setting has many applications in the real-world implementations. The multi-key setting can be seen as a generalization of the multi-user [8] and broadcast [23] settings. There exists many related researches in the multi-key, multi-user, and broadcast settings, such as [23,8,15,24]. In the related-key attack setting, the key $K_i$ satisfies the relationship $K_i = \phi_i(K)$, where $K$ is a key, and the related-key deriving (RKD) functions $\phi_i$ are chosen by the adversary. Related-key attack (RKA) was firstly presented by Biham et al. [4,5] for block ciphers [6,31] and then extended to other cryptographic algorithms such as stream ciphers [9], permutation-based ciphers [12], hash functions [32], MACs [26,3], AE schemes [14], etc. Multi-key security and related-key security have become the important criterion in cipher designs. The security of the tweakable Even-Mansour cipher in the multi-key and related-key settings are still an open problem.

**Our Contributions.** This paper focuses on the security of the tweakable Even-Mansour cipher in the multi-key and related-key settings. Due to the weakness of almost-XOR-universal (AXU) hash functions in the related-key setting, the tweakable Even-Mansour cipher in here is reconstructed by related-key-almost-XOR-universal (RKA-AXU) hash functions presented by Wang et al. [32]. We prove that the tweakable Even-Mansour cipher is secure against multi-key and related-key attacks.

In the multi-key setting, a small number of plaintexts are encrypted under multiple independent keys. The tweakable Even-Mansour cipher with $(\epsilon,\delta)$-AXU-hash functions is secure up to $2D(T + D(1-1/l))\delta + (D-l+1)(D-l)\epsilon$ queries against multi-key attack, where $D$ is the complexity of construction queries (data complexity), $T$ is the complexity of internal permutation queries (time complexity), and $l$ is the number of keys.

In the related-key setting, a small number of plaintexts are encrypted under multiple related keys. The tweakable Even-Mansour cipher with $(\epsilon, \delta)$-RKA-AXU-hash functions is secure up to $D(D-1)\epsilon + 2DT\delta$ queries against related-key attack, where $D$ is the complexity of construction queries (data complexity) and $T$ is the complexity of internal permutation queries (time complexity).

The tweakable Even-Mansour cipher is a secure cryptosystem with a lighter key schedule and higher key agility in the multi-key and related-key attack settings. It is very useful, not only because of the simplicity of its design and proof (Patarin's H-coefficients technique), but also because of fast and secure implementations. If the underlying block cipher is replaced with the tweakable Even-Mansour cipher, then encryption, authentication, and authenticated encryption modes may be designed more efficiently.

We leave it as an interesting open problem to settle the security of two-round iterated tweakable Even-Mansour cipher in the multi-key and related-key settings. Does further extend it for any $r$-round iterated tweakable Even-Mansour cipher?

**Organizations of This Paper.** Notations and H-coefficients technique are presented in Section 2. The multi-key security of the tweakable Even-Mansour cipher is derived in Section 3. The related-key security of the tweakable Even-Mansour cipher is derived in Section 4. Finally, this paper ends up with a conclusion in Section 5.

## 2 Preliminaries

### 2.1 Notations

Let $n$ be an integrity and $\{0,1\}^n$ denote the set of all strings whose lengths are $n$-bit. If $X$ is a finite set, then $x \overset{\$}{\leftarrow} X$ is a value randomly chosen from $X$, and $|X|$ stands for the number of elements in $X$.

A tweakable blockcipher with key space $\mathcal{K}$, tweak space $\mathcal{T}$, and plaintext space $\{0,1\}^n$ is a function $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ such that for any key $K \in \mathcal{K}$ and a tweak $t \in \mathcal{T}$, $\widetilde{E}_K(t, \cdot) = \widetilde{E}(K, t, \cdot)$ is a permutation of $\{0,1\}^n$. Similarity, its inverse is denoted by $\widetilde{D}_K = \widetilde{E}_K^{-1}$. Let $Perm(n)$ be the set of all permutations on $\{0,1\}^n$. Let $\widetilde{Perm}(\mathcal{T}, n)$ be the set of tweakable permutations, i.e., the set of $Perm(n)$ indexed with $t \in \mathcal{T}$. In this work, we focus on a tweakable blockcipher $\widetilde{E}_K^P$ based on a public random permutation $P \overset{\$}{\leftarrow} Perm(n)$.

An adversary is a probabilistic algorithm with access to certain oracles. Let $\mathcal{A}^O = 1$ be the event that an adversary $\mathcal{A}$ outputs 1 after interacting with the oracle $O$. Without loss of generality, we assume that the adversary doesn't make redundant queries, that is, i) it doesn't repeat prior queries for each oracle, ii) the adversary does not ask the decryption oracle $\widetilde{D}_K$ after receiving a value in response to an encryption query $\widetilde{E}_K$, and iii) the adversary does not ask the encryption oracle $\widetilde{E}_K$ after receiving a value in response to a decryption query $\widetilde{D}_K$.

A related-key deriving (RKD) function is a map that takes a key $K \in \mathcal{K}$ as an input and returns a related key $\phi(K) \in \mathcal{K}$. A RKD set $\Phi$ is a set of RKD functions, which is formalized as $\Phi = \{\phi : \mathcal{K} \to \mathcal{K}\}$. Two typical RKD sets are enumerated as follows:

$$\Phi_{id} = \{\phi : K \to K\};$$
$$\Phi_{\oplus} = \{\phi : K \to K \oplus \triangle \mid \triangle \in \mathcal{K}\},$$

where $K \in \mathcal{K}$. Throughout the paper we assume that membership in RKD sets can be efficiently decided.

### 2.2 The H-Coefficients Technique

Patarin's H-coefficients technique [25] is a vital tool widely used in the field of provable security. We briefly summarize this technique as follows.

Consider an information-theoretic adversary $\mathcal{A}$ whose goal is to distinguish a real world $X$ and a ideal world $Y$, then the advantage of $\mathcal{A}$ is denoted as

$$Adv(\mathcal{A}) = |Pr[\mathcal{A}^X = 1] - Pr[\mathcal{A}^Y = 1]|.$$

Without loss of generality, we can assume $\mathcal{A}$ is a deterministic adversary. The interaction with $X$ or $Y$ is summarized in a transcript $\tau$, which is a list of queries and answers. Denote by $D_X$ the probability distribution of transcripts when interacting with $X$, and by $D_Y$ the probability distribution of transcripts when interacting with $Y$.

A transcript $\tau$ is attainable if $Pr[D_Y = \tau] > 0$, meaning that it can occur during interaction with $Y$. Let $\Gamma$ be the set of attainable transcripts. The H-coefficients lemma is presented as follows.

**Lemma 1 (H-Coefficients Lemma).** *Fix a deterministic adversary $\mathcal{A}$. Let $\Gamma = \Gamma_{good} \bigcup \Gamma_{bad}$ be a partition of the set of attainable transcripts. Assume that there exists $\varepsilon$ such that for any $\tau \in \Gamma_{good}$, one has*

$$\frac{Pr[D_X = \tau]}{Pr[D_Y = \tau]} \geq 1 - \varepsilon.$$

*Then*

$$Adv(\mathcal{A}) \leq \varepsilon + Pr[D_Y \in \Gamma_{bad}].$$

## 3 Multi-Key-Security of the Tweakable Even-Mansour Cipher

### 3.1 $(\epsilon, \delta)$-Almost XOR Universal (AXU) Hash Functions [20]

**Definition 1 ($(\epsilon, \delta)$-AXU Hash Function Family [20]).** *Let $\mathcal{H} = \{H : \mathcal{K} \times \mathcal{D} \to \mathcal{R}\}$ be a family of hash functions. $H$ is called an $(\epsilon, \delta)$-almost XOR universal ($(\epsilon, \delta)$-AXU) hash function, if the following two conditions hold:*

*1) For any element $X \in \mathcal{D}$ and any element $Y \in \mathcal{R}$,*

$$Pr[K \xleftarrow{\$} \mathcal{K} : H_K(X) = Y] \leq \delta;$$

*2) For any two distinct elements $X, X' \in \mathcal{D}$ and any element $Y \in \mathcal{R}$,*

$$Pr[K \xleftarrow{\$} \mathcal{K} : H_K(X) \oplus H_K(X') = Y] \leq \epsilon.$$

Examples of AXU hash function families are presented as follows.

1) Let $\mathcal{H}_1 = \{H_K(x) = K \cdot x \mid K, x \in GF(2^n)^*\}$. Then $\mathcal{H}_1$ is a $(2^{-n}, 2^{-n})$-AXU hash function family from $\{0,1\}^n \setminus \{0^n\}$ to $\{0,1\}^n$.

2) Let $\mathcal{H}_2 = \{H_K(x_1, x_2, \cdots, x_t) = K \cdot x_1 + K^2 \cdot x_2 + \cdots + K^t \cdot x_t \mid K \in GF(2^n)^*, x_i \in GF(2^n), 1 \leq i \leq t, (x_1, x_2, \cdots, x_t) \neq (0, 0, \cdots, 0)\}$. Then $\mathcal{H}_2$ is a $(t/2^n, t/2^n)$-AXU hash function family from $\{0,1\}^{tn} \setminus \{0^{tn}\}$ to $\{0,1\}^n$.

3) Let $\mathcal{H}_3 = \{H_{k_1, k_2, \cdots, k_t}(x_1, x_2, \cdots, x_t) = k_1 \cdot x_1 + k_2 \cdot x_2 + \cdots + k_t \cdot x_t \mid k_i \in GF(2^n), x_i \in GF(2^n), 1 \leq i \leq t, (k_1, k_2, \cdots, k_t) \neq (0, 0, \cdots, 0), (x_1, x_2, \cdots, x_t) \neq (0, 0, \cdots, 0)\}$. Then $\mathcal{H}_3$ is a $(1/2^n, 1/2^n)$-AXU hash function family from $\{0,1\}^{tn} \setminus \{0^{tn}\}$ to $\{0,1\}^n$.

### 3.2 Multi-Key-Security Model

Let $\widetilde{E}_K^P : \mathcal{T} \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a tweakable blockcipher based on a random permutation $P \xleftarrow{\$} Perm(n)$, where $K \in \mathcal{K}$. Let $\widetilde{\pi} \xleftarrow{\$} \widetilde{Perm}(\mathcal{T}, n)$ be a random tweakable permutation. Let $l$ denote the number of keys $K_i$ under which the adversary performs queries, that is, there is at least one query for every key $K_i$ for $1 \leq i \leq l$. The multi-key-security of $\widetilde{E}$ is formalized with a distinguisher that has adaptive oracle access to either $(\widetilde{E}_{K_1}^P, \widetilde{E}_{K_2}^P, \cdots, \widetilde{E}_{K_l}^P; P)$ with $K_i \xleftarrow{\$} \mathcal{K}$ for $i = 1, \cdots, l$, (Real World $X$), or $(\widetilde{\pi}_1, \widetilde{\pi}_2, \cdots, \widetilde{\pi}_l; P)$ with $\widetilde{\pi}_i \xleftarrow{\$} \widetilde{Perm}(\mathcal{T}, n), i = 1, \cdots, l$ (Ideal World $Y$). In this paper, we consider the adversary that has access to the encryption and decryption queries for $X$ or $Y$. The definition of multi-key security is presented as follows.

**Definition 2 (Multi-Key Security).** *Let $K \xleftarrow{\$} \mathcal{K}$ and $\widetilde{E}_K^P$ be the tweakable block cipher based on a random permutation $P \xleftarrow{\$} Perm(n)$. Given an adversary $\mathcal{A}$, the multi-key advantage of $\mathcal{A}$ with respect to $l$ keys is*

$$Adv_{\widetilde{E}_K^P}^{mk}(\mathcal{A}) = |Pr[A^{\widetilde{E}_{K_1}^P, \widetilde{E}_{K_2}^P, \cdots, \widetilde{E}_{K_l}^P; P} = 1] - Pr[A^{\widetilde{\pi}_1, \widetilde{\pi}_2, \cdots, \widetilde{\pi}_l; P} = 1]|,$$

*where the keys $K_1, \cdots, K_l$ are independently and uniformly drawn from $\mathcal{K}$, and $\widetilde{\pi}_1, \widetilde{\pi}_2, \cdots, \widetilde{\pi}_l$ are independently and uniformly drawn from $\widetilde{Perm}(\mathcal{T}, n)$. The adversary $\mathcal{A}$ has access to the encryption and decryption oracles.*

### 3.3 Security Proofs of the Tweakable Even-Mansour Cipher in the Multi-Key Setting

Let $\mathcal{H}$ be an $(\epsilon, \delta)$-AXU hash function family defined in Definition 1, then the tweakable Even-Mansour cipher with key space $\mathcal{K}$ and tweak space $\mathcal{T}$ is written

$$TEM_K^P(t, x) = P(x \oplus H_K(t)) \oplus H_K(t),$$

where $P$ is an $n$-bit public random permutation, $H_K \xleftarrow{\$} \mathcal{H}$, $K \in \mathcal{K}$ is the key, $t \in \mathcal{T}$ is the tweak, and $x \in \{0,1\}^n$ is the plaintext.

The multi-key security of the tweakable Even-Mansour cipher is presented as follows.

**Theorem 1 (Multi-Key Security of the Tweakable Even-Mansour Cipher).** *Let $TEM_K^P$ be the tweakable Even-Mansour cipher with $(\epsilon, \delta)$-AXU hash function family, then for all adversaries $\mathcal{A}$ making at most $D$ queries to $TEM_{K_1}^P, TEM_{K_2}^P, \cdots, TEM_{K_l}^P$ (resp. $\widetilde{\pi}_1, \widetilde{\pi}_2, \cdots, \widetilde{\pi}_l$) or their inverses and at most $T$ queries to $P$ or $P^{-1}$, we have*

$$Adv_{TEM}^{mk}(\mathcal{A}) \leq 2D(T + D(1 - \frac{1}{l}))\delta + (D - l + 1)(D - l)\epsilon.$$

Our proof is similar to that of the Even-Mansour cipher in the multi-key setting [24], except that we need to consider the tweak of TEM and the properties of hash functions in the multi-key setting. The result of Theorem 1 is in fact a generalization of [24]. The proof uses Patarin's H-coefficients technique [25]. For a detailed explanation of this technique, you can refer to [10].

As shown in Fig. 1, we consider an adversary $\mathcal{A}$ that has bidirectional access to $l+1$ oracles $(O_1, \cdots, O_{l+1})$. In the real world $X$, these are $(TEM_{K_1}^P, TEM_{K_2}^P, \cdots, TEM_{K_l}^P; P)$ with $K_i \xleftarrow{\$} \mathcal{K}$ for $i = 1, \cdots, l, P \xleftarrow{\$} Perm(n)$, and in the ideal world $Y$, these are $(\widetilde{\pi}_1, \widetilde{\pi}_2, \cdots, \widetilde{\pi}_l; P)$ with $\widetilde{\pi}_i \xleftarrow{\$} \widetilde{Perm}(\mathcal{T}, n), i = 1, \cdots, l$ and $P \xleftarrow{\$} Perm(n)$. Without loss of generality, we assume that $\mathcal{A}$ is a deterministic adversary. It makes $D_i$ queries to oracle $O_i$ for $i = 1, \cdots, l$, and $T$ queries to $O_{l+1}$. Let $D = \sum_{i=1}^{l} D_i$. (Let $m$ be the number of distinct tweaks, $D_t$ be the number of queries for the $t$-th tweak, $1 \leq t \leq m$, using an arbitrary ordering of the tweaks. Note that $m$ may depend on the answers received from the oracles, yet one always has $D = \sum_{t=1}^{m} D_t$.)

The interaction of $\mathcal{A}$ with the oracles can be described by a transcript $\tau = (K_1, \cdots, K_l, \tau_1, \cdots, \tau_{l+1})$. We assume that the list of queries to $O_i$ for $i = 1, \cdots, l$ is defined by $\tau_i = \{(t_i^1, x_i^1, y_i^1), \cdots, (t_i^{D_i}, x_i^{D_i}, y_i^{D_i})\}$, where $t_i^1, \cdots, t_i^{D_i} \in \mathcal{T}$, and to $O_{l+1}$ by $\tau_{l+1} = \{(u^1, v^1), \cdots, (u^T, v^T)\}$. We assume that $\mathcal{A}$ never makes duplicate queries, so that $(t_i^j, x_i^j) \neq (t_i^{j'}, x_i^{j'}), (t_i^j, y_i^j) \neq (t_i^{j'}, y_i^{j'}), u^j \neq u^{j'}$, and $v^j \neq v^{j'}$ for all $i, j, j'$ where $j \neq j'$.

Let $D_X$ denote the probability distribution of transcripts in the real world $X$, and $D_Y$ denote the probability distribution of transcripts in the ideal world $Y$. We say that a transcript $\tau$ is attainable if it can be obtained from interacting with $(\widetilde{\pi}_1, \widetilde{\pi}_2, \cdots, \widetilde{\pi}_l, P)$, that is to say $Pr(D_Y = \tau) > 0$.

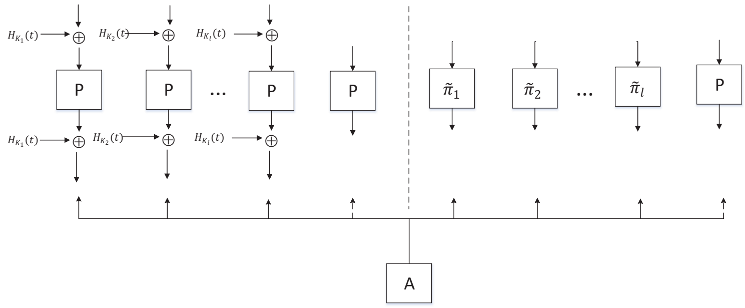

**Fig. 1.** Multi-Key Security of the Tweakable Even-Mansour Cipher. **Left of dashed line**: Real world $X = (TEM^P_{K_1}, TEM^P_{K_2}, \cdots, TEM^P_{K_l}; P)$ with $K_i \xleftarrow{\$} \mathcal{K}$ for $i = 1, \cdots, l, P \xleftarrow{\$} Perm(n)$. **Right of dashed line**: Ideal world $Y = (\widetilde{\pi}_1, \widetilde{\pi}_2, \cdots, \widetilde{\pi}_l; P)$ with $\widetilde{\pi}_i \xleftarrow{\$} \widetilde{Perm}(\mathcal{T}, n), i = 1, \cdots, l$ and $P \xleftarrow{\$} Perm(n)$. The goal of $\mathcal{A}$ is to distinguish the real world $X$ from the ideal world $Y$. If the distinguishable advantage of $\mathcal{A}$ is negligible, the scheme is multi-key-secure. Although only one direction is shown, inverse oracles can be accessed as well. The number of queries by the adversary $\mathcal{A}$ to any of the first $l$ oracles is denoted by $D$, the number of queries to the last oracle by $T$.

**Definition 3.** *We say that a transcript $\tau$ is bad if two different queries would result in the same input or output to $P$, when $\mathcal{A}$ interacting with the real world. Put formally, $\tau$ is bad if one of the following conditions is set:*

*Bad1: $\exists (t_i^j, x_i^j, y_i^j) \in \tau_i$, $t_i^j \in \mathcal{T}$, and $(u^{j'}, v^{j'}) \in \tau_{l+1}$, such that $x_i^j \oplus u^{j'} = H_{K_i}(t_i^j)$, where $1 \leq i \leq l, 1 \leq j \leq D_i, 1 \leq j' \leq T$;*

*Bad2: $\exists (t_i^j, x_i^j, y_i^j) \in \tau_i$, $t_i^j \in \mathcal{T}$, and $(u^{j'}, v^{j'}) \in \tau_{l+1}$, such that $y_i^j \oplus v^{j'} = H_{K_i}(t_i^j)$, where $1 \leq i \leq l, 1 \leq j \leq D_i, 1 \leq j' \leq T$;*

*Bad3: $\exists (t_i^j, x_i^j, y_i^j) \neq (t_i^{j'}, x_i^{j'}, y_i^{j'}) \in \tau_i$, and $t_i^j, t_i^{j'} \in \mathcal{T}$, such that $x_i^j \oplus x_i^{j'} = H_{K_i}(t_i^j) \oplus H_{K_i}(t_i^{j'})$, where $1 \leq i \leq l, 1 \leq j \neq j' \leq D_i$;*

*Bad4: $\exists (t_i^j, x_i^j, y_i^j) \neq (t_i^{j'}, x_i^{j'}, y_i^{j'}) \in \tau_i$, and $t_i^j, t_i^{j'} \in \mathcal{T}$, such that $y_i^j \oplus y_i^{j'} = H_{K_i}(t_i^j) \oplus H_{K_i}(t_i^{j'})$, where $1 \leq i \leq l, 1 \leq j \neq j' \leq D_i$;*

*Bad5: $\exists (t_i^j, x_i^j, y_i^j) \in \tau_i, (t_{i'}^{j'}, x_{i'}^{j'}, y_{i'}^{j'}) \in \tau_{i'}, (t_i^j, x_i^j, y_i^j) \neq (t_{i'}^{j'}, x_{i'}^{j'}, y_{i'}^{j'})$, and $t_i^j, t_{i'}^{j'} \in \mathcal{T}$, such that $x_i^j \oplus x_{i'}^{j'} = H_{K_i}(t_i^j) \oplus H_{K_{i'}}(t_{i'}^{j'})$, where $1 \leq i \neq i' \leq l, 1 \leq j \leq D_i, 1 \leq j' \leq D_{i'}$;*

*Bad6: $\exists (t_i^j, x_i^j, y_i^j) \in \tau_i, (t_{i'}^{j'}, x_{i'}^{j'}, y_{i'}^{j'}) \in \tau_{i'}, (t_i^j, x_i^j, y_i^j) \neq (t_{i'}^{j'}, x_{i'}^{j'}, y_{i'}^{j'})$, and $t_i^j, t_{i'}^{j'} \in \mathcal{T}$, such that $y_i^j \oplus y_{i'}^{j'} = H_{K_i}(t_i^j) \oplus H_{K_{i'}}(t_{i'}^{j'})$, where $1 \leq i \neq i' \leq l, 1 \leq j \leq D_i, 1 \leq j' \leq D_{i'}$.*

*Otherwise we say that $\tau$ is good. We denote $\Gamma_{good}$ (resp. $\Gamma_{bad}$) the set of good (resp. bad) transcripts. Let $\Gamma = \Gamma_{good} \cup \Gamma_{bad}$ be the set of attainable transcripts.*

We firstly upper bound the probability of bad transcripts in the ideal world $Y$ by the following lemma.

**Lemma 2.** *Let $H$ be an $(\epsilon, \delta)$-AXU hash function, $l$ be the number of keys $K_i$, and $TEM_K^P$ be the tweakable Even-Mansour construction, then*

$$Pr(D_Y \in \Gamma_{bad}) \leq 2D(T + D(1 - \frac{1}{l}))\delta + (D - l + 1)(D - l)\epsilon.$$

*Proof.* In the ideal world $Y$, $\tau$ is an attainable transcript generated independently of the dummy key $K_i \in \mathcal{K}$ for $i = 1, \cdots, l$. Assume an adversary $\mathcal{A}$ makes at most $D$ construction queries and at most $T$ primitive queries. For $(t_i^j, x_i^j, y_i^j) \in \tau_i, t_i^j \in \mathcal{T}$, $(u^{j'}, v^{j'}) \in \tau_{l+1}$, where $1 \leq i \leq l, 1 \leq j \leq D_i, 1 \leq j' \leq T$, and $D = \sum_{i=1}^{l} D_i$, by the properties of the $(\epsilon, \delta)$-AXU hash function $H$, we have

$$\begin{aligned} Pr[Bad1] &= Pr[Bad2] \\ &= Pr[K_i \xleftarrow{\$} \mathcal{K} : H_{K_i}(t_i^j) = C] \\ &\leq \sum_{i=1}^{l} D_i T \delta = DT\delta, \end{aligned}$$

where $C = x_i^j \oplus u^{j'}$ in Bad1 or $C = y_i^j \oplus v^{j'}$ in Bad2.

Fix any distinct queries $(t_i^j, x_i^j, y_i^j) \neq (t_i^{j'}, x_i^{j'}, y_i^{j'}) \in \tau_i, t_i^j, t_i^{j'} \in \mathcal{T}$, where $1 \leq i \leq l, 1 \leq j \neq j' \leq D_i$. By the properties of the $(\epsilon, \delta)$-AXU hash function $H$, we have

$$\begin{aligned} Pr[Bad3] &= Pr[Bad4] \\ &= Pr[K_i \xleftarrow{\$} \mathcal{K} : H_{K_i}(t_i^j) \oplus H_{K_i}(t_i^{j'}) = C] \\ &\leq \sum_{i=1}^{l} \binom{D_i}{2} \epsilon, \end{aligned}$$

where $C = x_i^j \oplus x_i^{j'}$ in Bad3 or $C = y_i^j \oplus y_i^{j'}$ in Bad4.

As there is at least one query for every key $K_i$, we consider the maximum case: the adversary makes $(D - l + 1)$ queries for some key, one query per key for another $l - 1$ keys. Therefore, we have

$$\begin{aligned} Pr[Bad3] = Pr[Bad4] &\leq \sum_{i=1}^{l} \binom{D_i}{2} \epsilon \\ &\leq \binom{D - l + 1}{2} \epsilon \\ &= \frac{(D - l + 1)(D - l)\epsilon}{2}. \end{aligned}$$

For any distinct queries $(t_i^j, x_i^j, y_i^j) \in \tau_i, (t_{i'}^{j'}, x_{i'}^{j'}, y_{i'}^{j'}) \in \tau_{i'}, (t_i^j, x_i^j, y_i^j) \neq (t_{i'}^{j'}, x_{i'}^{j'}, y_{i'}^{j'})$, $t_i^j, t_{i'}^{j'} \in \mathcal{T}$, where $1 \leq i \neq i' \leq l, 1 \leq j \leq D_i, 1 \leq j' \leq D_{i'}$, and

$D = \sum_{i=1}^{l} D_i = \sum_{i'=1}^{l} D_{i'}$, by the properties of the $(\epsilon, \delta)$-AXU hash function $H$, we have

$$\begin{aligned}
&Pr[Bad5] = Pr[Bad6] \\
=&Pr[K_i, K_{i'} \xleftarrow{\$} \mathcal{K}^2 : H_{K_i}(t_i^j) \oplus H_{K_{i'}}(t_{i'}^{j'}) = C] \\
=&\sum_{a_i, b_i \in \mathcal{R}^2} Pr[a_i \oplus b_i = C | H_{K_i}(t_i^j) = a_i, H_{K_{i'}}(t_{i'}^{j'}) = b_i] \cdot \\
&Pr[K_i, K_{i'} \xleftarrow{\$} \mathcal{K}^2 : H_{K_i}(t_i^j) = a_i, H_{K_{i'}}(t_{i'}^{j'}) = b_i] \\
\leq&\sum_{a_i \in \mathcal{R}} Pr[K_i, K_{i'} \xleftarrow{\$} \mathcal{K}^2 : H_{K_i}(t_i^j) = a_i, H_{K_{i'}}(t_{i'}^{j'}) = C - a_i] \\
\leq&\sum_{a_i \in \mathcal{R}} Pr[K_i \xleftarrow{\$} \mathcal{K} : H_{K_i}(t_i^j) = a_i] \cdot \\
&Pr[K_{i'} \xleftarrow{\$} \mathcal{K} : H_{K_{i'}}(t_{i'}^{j'}) = C - a_i] \quad (Key\ Independence) \\
\leq&2^n(\binom{D}{2} - \sum_{i=1}^{l} \binom{D_i}{2})\delta^2 \qquad (Cauchy\ Inequality) \\
\leq&D^2(1 - 1/l)\delta,
\end{aligned}$$

where $C = x_i^j \oplus x_{i'}^{j'}$ in Bad5 or $C = y_i^j \oplus y_{i'}^{j'}$ in Bad6, $\delta \in [2^{-n}, 2^{-(n-1)}]$.

Therefore,

$$\begin{aligned}
Pr[D_Y \in \Gamma_{bad}] &= Pr[\bigcup_{i=1}^{6} Badi] \leq \sum_{i=1}^{6} Pr[Badi] \\
&\leq 2D(T + D(1 - \frac{1}{l}))\delta + (D - l + 1)(D - l)\epsilon.
\end{aligned}$$

This completes the proof.

We then analyze good transcripts. For a good transcript, in the real world $X$, all tuples in $(K_1, \cdots, K_l, \tau_1, \cdots, \tau_{l+1})$ uniquely define an input-output pair of $P$, while in the ideal world it is not.

**Lemma 3.** *For any good transcript $\tau$, one has*

$$\frac{Pr[D_X = \tau]}{Pr[D_Y = \tau]} \geq 1.$$

*Proof.* Consider a good transcript $\tau \in \Gamma_{good}$. Denote by $\Omega_X$ the set of all possible oracles in the real world $X$ and by $\Omega_Y$ the set of all possible oracles in the ideal world $Y$. Let $comp_X(\tau) \subseteq \Omega_X$ and $comp_Y(\tau) \subseteq \Omega_Y$ be the set of oracles compatible with transcript $\tau$. According to the H-coefficients technique, we have

$Pr(D_X = \tau) = \frac{|comp_X(\tau)|}{|\Omega_X|}$, where $|\Omega_X| = 2^n!|\mathcal{K}|^l$.

$Pr(D_Y = \tau) = \frac{|comp_Y(\tau)|}{|\Omega_Y|}$, where $|\Omega_Y| = (\prod_t 2^n!)^l \cdot 2^n!|\mathcal{K}|^l$ and $t \in \mathcal{T}$.

Firstly, we calculate $|comp_X(\tau)|$. As $\tau \in \Gamma_{good}$, there are no two queries in $\tau$ with the same input or output of the underlying permutation. Any query tuple in $\tau$ therefore fixes exactly one input-output pair of the underlying oracle. Because $\tau$ consists of $D+T$ query tuples, the number of possible oracles in the real world $X$ equals $(2^n - D - T)!$.

For the analysis in the ideal world $Y$, we define

$$D_{t_i} = |\{(t_i, x_i, y_i) \in \tau_i | t_i \in \mathcal{T}, x_i, y_i \in \{0,1\}^n, 1 \leq i \leq l\}|.$$

By a similar reason, the number of possible oracles in the ideal world $Y$ equals $\prod_{i=1}^{l} \prod_t (2^n - D_{t_i})!(2^n - T)!$, where $D = \sum_{i=1}^{l} \sum_t D_{t_i}$. It follows that,

$$\begin{aligned} Pr(D_X = \tau) &= \frac{(2^n - D - T)!}{2^n!|\mathcal{K}|^l} \\ Pr(D_Y = \tau) &= \frac{\prod_{i=1}^{l} \prod_t (2^n - D_{t_i})!(2^n - T)!}{(\prod_t 2^n!)^l \cdot 2^n!|\mathcal{K}|^l} \\ &\leq \frac{(2^n - D - T)!}{2^n!|\mathcal{K}|^l}. \end{aligned}$$

Therefore, we have $\frac{Pr[D_X=\tau]}{Pr[D_Y=\tau]} \geq 1$.

By Lemmas 1, 2, and 3, we have

$$Adv_{TEM}^{mk}(\mathcal{A}) \leq 2D(T + D(1 - \frac{1}{l}))\delta + (D - l + 1)(D - l)\epsilon.$$

The tweakable Even-Mansour cipher in the single-key setting is a special case of it in the multi-key setting where $l = 1$. We prove that the security bound of the tweakable Even-Mansour cipher in multi-key setting is a straightforward extension of the single-key setting. Therefore, the bound that we derived for the tweakable Even-Mansour cipher in the multi-key setting is tight. If we replace the public random permutation with an ideal block cipher with the same characteristics (including block-size, AXU-hash functions, etc), we can obtain the similar security.

## 4 Related-Key-Security of the Tweakable Even-Mansour Cipher

Wang et al. [32] pointed out: “If we consider the related-key attack (RKA) against these universal-hash-function-based (UHF-based) schemes, some of them may not be secure, especially those using the key of UHF as a part of the whole key of scheme, due to the weakness of UHF in the RKA setting”. In order to ensure the security of UHF-based schemes, Wang et al. provided a related-key almost universal hash function which is a natural extension to almost universal hash function in the RKA setting. In this paper, we introduce a concept of $(\epsilon, \delta)$-related-key almost universal hash function to guarantee the related-key security of the tweakable Even-Mansour cipher.

### 4.1 $(\epsilon, \delta)$-Related-Key Almost XOR Universal Hash Functions

**Definition 4** **($(\epsilon, \delta)$-RKA-AXU Hash Function Family).** *Let $\mathcal{H} = \{H : \mathcal{K} \times \mathcal{D} \to \mathcal{R}\}$ be a family of hash functions. $H$ is an $(\epsilon, \delta)$-related-key-almost-XOR-universal ($(\epsilon, \delta)$-RKA-AXU) hash function for the RKD set $\Phi$, if the following two conditions hold:*

*1) For any $\phi \in \Phi, X \in \mathcal{D}$, and $Y \in \mathcal{R}$,*

$$Pr[K \xleftarrow{\$} \mathcal{K} : H_{\phi(K)}(X) = Y] \leq \delta;$$

*2) For any $\phi, \phi' \in \Phi, X, X' \in \mathcal{D}, (\phi, X) \neq (\phi', X')$, and $Y \in \mathcal{R}$,*

$$Pr[K \xleftarrow{\$} \mathcal{K} : H_{\phi(K)}(X) \oplus H_{\phi'(K)}(X') = Y] \leq \epsilon.$$

For any $\phi, \phi' \in \Phi, \phi \neq \phi'$ means there exists a key $K \in \mathcal{K}$ such that $\phi(K) \neq \phi'(K)$. If the RKD set $\Phi_{id} = \{\phi : K \to K\}$ is an identity transform, an $(\epsilon, \delta)$-RKA-AXU hash function family is an $(\epsilon, \delta)$-AXU hash function family.

**Restricting RKD Sets [32].** The RKA-AXU-hash function family depends on the choice of RKD sets. For some RKD sets, the RKA-AXU-hash function family may not exist. It is necessary that a RKD set is restricted to both output unpredictable and collision resistant. The restrictions on the RKD set are specifically presented as follows.

1) Output unpredictability. A $\phi \in \Phi$ that has predictable outputs if there exists a constant $S$ such that the probability of $\phi(K) = S$ is high. Let $OU(\Phi) = max_{\phi \in \Phi, S} Pr[K \leftarrow \mathcal{K} : \phi(K) = S]$ be the probability of output predictability. If $OU(\Phi)$ is negligible, we say that $\Phi$ is output unpredictable.

2) Collision resistance. Two distinct $\phi, \phi' \in \Phi$ have high collision probability if the probability of $\phi(K) = \phi'(K)$ is hight. Let $CR(\Phi) = max_{\phi \neq \phi' \in \Phi} Pr[K \leftarrow \mathcal{K} : \phi(K) = \phi'(K)]$ be the probability of collision. If $CR(\phi)$ is negligible, we say that $\phi$ is collision resistant. More strictly, if for any two distinct $\phi, \phi' \in \Phi$ and any key $K$, we have $\phi(K) \neq \phi'(K)$ or $CR(\Phi) = 0$, we say that $\Phi$ is claw-free.

**Instances.** Wang et al. [32] constructed related-key almost universal hash functions: one fixed-input-length (FIL) UHF named RH1 and two variable-input-length (VIL) UHFs named RH2 and RH3. It is easy to obtain that RH1 and RH2 are both $(\epsilon, \delta)$-RKA-AXU hash functions for the RKD set $\Phi^{\oplus}$.

1) RH1: $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, $RH1_K(M) = MK \oplus K^3$ is $(2/2^n, 2/2^n)$-RKA-AXU for the RKD set $\Phi^{\oplus}$.

2) RH2: $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, $pad(M) = M \parallel 0^i \parallel |M|$

$$RH2_K(M) = \begin{cases} K^{l+2} \oplus Poly_K(pad(M)) & l \text{ is odd} \\ K^{l+3} \oplus Poly_K(pad(M))K & l \text{ is even} \end{cases}$$

is $((l_{max} + 3)/2^n, (l_{max} + 3)/2^n)$-RKA-AXU for the RKD set $\Phi^{\oplus}$, where $l = \lceil |M|/n \rceil + 1$ is the number of blocks in $pad(M)$, $l_{max}$ is the maximum block number of messages after padding, and $Poly : \{0,1\}^n \times \{0,1\}^{nm} \to \{0,1\}^n$ is defined as follows:

$$Poly_K(X) = X_1 K^m \oplus \cdots \oplus X_m K.$$

### 4.2 Related-Key-Security Model

Let $\varPhi$ be a set of RKD functions. For a tweakable block cipher $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ based on a public random permutation $P \xleftarrow{\$} Perm(n)$, we define a related-key oracle $RK[\widetilde{E}] : \mathcal{K} \times \varPhi \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ as

$$RK[\widetilde{E}]^P(K, \phi, t, x) = RK[\widetilde{E}]^P_K(\phi, t, x) = \widetilde{E}^P_{\phi(K)}(t, x),$$

where $K \in \mathcal{K}$ is the key, $\phi \in \varPhi$ is a RKD function, $t \in \mathcal{T}$ is the tweak, and $x \in \{0,1\}^n$ is the plaintext.

Let $\widetilde{RKPerm}(\varPhi, \mathcal{T}, n)$ be the set of tweakable related-key permutations, i.e., the set of all families of permutations on $\{0,1\}^n$ indexed with $(\phi, t) \in \varPhi \times \mathcal{T}$.

The security of the tweakable block cipher in the related-key setting is formalized with a distinguisher which has access to $(\widetilde{E}^P_{\phi(K)}; P)$ with $K \in \mathcal{K}, \phi \in \varPhi$, and $P \xleftarrow{\$} Perm(n)$ (Real World $X$), or $(RK[\widetilde{\pi}]; P)$ with $RK[\widetilde{\pi}] \xleftarrow{\$} \widetilde{RKPerm}(\varPhi, \mathcal{T}, n)$ and $P \xleftarrow{\$} Perm(n)$ (Ideal World $Y$). In this paper, we consider that an adversary is adaptive and can make encryption and decryption queries to each oracle. We present a definition of related-key security as follows.

**Definition 5 (Related-Key Security).** *Let $\varPhi$ be a RKD set, $K \xleftarrow{\$} \mathcal{K}$ be a key, and $\widetilde{E}^P_K$ be a tweakable block cipher based on a public random permutation $P \xleftarrow{\$} Perm(n)$. Given an adversary $\mathcal{A}$, the related-key advantage of $\mathcal{A}$ with respect to $\varPhi$ is*

$$Adv^{rk}_{\widetilde{E}^P_K}(\mathcal{A}) = |Pr[\mathcal{A}^{\widetilde{E}^P_{\phi(K)};P} = 1] - Pr[\mathcal{A}^{RK[\widetilde{\pi}];P} = 1]|,$$

*where $RK[\widetilde{\pi}] \xleftarrow{\$} \widetilde{RKPerm}(\varPhi, \mathcal{T}, n), \phi \xleftarrow{\$} \varPhi$, and $P \xleftarrow{\$} Perm(n)$. The adversary $\mathcal{A}$ has access to the encryption and decryption oracles.*

### 4.3 Security Proofs of the Tweakable Even-Mansour Cipher in the Related-Key Setting

Given a restricting RKD set $\varPhi$, let $\mathcal{H}$ be an $(\epsilon, \delta)$-RKA-AXU hash function family defined in Definition 4, then the construction of tweakable Even-Mansour in the related-key setting is written as

$$TEM^P_{\phi(K)}(t, x) = P(x \oplus H_{\phi(K)}(t)) \oplus H_{\phi(K)}(t),$$

where $P$ is a public random permutation, $H \xleftarrow{\$} \mathcal{H}$, $K \in \mathcal{K}$ is the key, $\phi \in \varPhi$ is a RKD function, $t \in \mathcal{T}$ is the tweak, and $x \in \{0,1\}^n$ is the plaintext.

In this paper, we assume that an adversary makes two-directional queries to each oracle and never makes redundant queries. The related-key security of the tweakable Even-Mansour cipher is presented as follows.

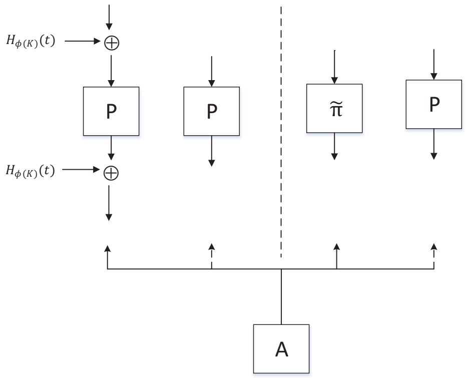

**Fig. 2.** Related-Key Security of the tweakable Even-Mansour Cipher. **Left of dashed line**: Real world $X = (TEM^P_{\phi(K)}; P)$ with $K \xleftarrow{\$} \mathcal{K}, \phi \xleftarrow{\$} \Phi$, and $P \xleftarrow{\$} Perm(n)$. **Right of dashed line**: Ideal world $Y = (RK[\widetilde{\pi}]; P)$ with $RK[\widetilde{\pi}] \xleftarrow{\$} \widetilde{RKPerm}(\Phi, \mathcal{T}, n)$ and $P \xleftarrow{\$} Perm(n)$. The goal of $\mathcal{A}$ is to distinguish the real world from the ideal world. If the distinguishable advantage of $\mathcal{A}$ is negligible, the scheme is related-key-secure. Although only one direction is shown, inverse oracles can be accessed as well. The number of queries by the adversary $\mathcal{A}$ to the first oracle is denoted by $D$, the number of queries to the last oracle by $T$.

**Theorem 2 (Related-Key Security of the Tweakable Even-Mansour Cipher).** *Let $\Phi$ be a restricting RKD set, $\phi \in \Phi, t \in \mathcal{T}$, and $TEM^P_K(t,x) = P(x \oplus H_K(t)) \oplus H_K(t)$ be the tweakable Even-Mansour cipher with $(\epsilon, \delta)$-RKA-AXU hash function family, then for all adversaries $\mathcal{A}$ making at most $D$ queries to $TEM^P_{\phi(K)}$ (resp. $RK[\widetilde{\pi}]$) or their inverses and at most $T$ queries to $P$ or $P^{-1}$, the related-key advantage of $\mathcal{A}$ with respect to $\Phi$ is*

$$Adv^{rk}_{TEM}(\mathcal{A}) \leq D(D-1)\epsilon + 2DT\delta.$$

Our proof uses Patarin's H-coefficients technique [25]. For a detailed explanation of this technique, we refer to [10].

As shown in Fig. 2, we consider an adversary $\mathcal{A}$ that has bidirectional access to two oracles $(O_1, O_2)$. In the real world $X$, these are $(TEM^P_{\phi(K)}; P)$ with $K \xleftarrow{\$} \mathcal{K}, \phi \xleftarrow{\$} \Phi$, and $P \xleftarrow{\$} Perm(n)$, and in the ideal world $Y$, these are $(RK[\widetilde{\pi}]; P)$ with $RK[\widetilde{\pi}] \xleftarrow{\$} \widetilde{RKPerm}(\Phi, \mathcal{T}, n)$ and $P \xleftarrow{\$} Perm(n)$. Without loss of generality, we assume that $\mathcal{A}$ is a deterministic adversary.

The interaction of $\mathcal{A}$ with the oracles can be described by a transcript $\tau = (K, \tau_1, \tau_2)$. We assume that the list of queries to $O_1$ is defined by $\tau_1 = \{(\phi^1, t^1, x^1, y^1), \cdots, (\phi^D, t^D, x^D, y^D)\}$, where $(\phi^1, t^1), \cdots, (\phi^D, t^D) \in (\Phi, \mathcal{T})$, and to $O_2$ by $\tau_2 = \{(u^1, v^1), \cdots, (u^T, v^T)$. We assume the adversary never makes duplicate queries, so that $(\phi^i, t^i, x^i) \neq (\phi^j, t^j, x^j), (\phi^i, t^i, y^i) \neq (\phi^j, t^j, y^j), u^i \neq u^j, v^i \neq v^j$ for all $i, j$. Let $D_X$ be the probability distribution of transcripts in the real world $X$ and $D_Y$ be the distribution of transcripts in the ideal world

$Y$. A transcript $\tau$ is attainable if $Pr[D_Y = \tau] > 0$, meaning that it can occur during interaction with $Y$.

**Definition 6.** *We say that a transcript $\tau$ is bad if two different queries would result in the same input or output to $P$, when $\mathcal{A}$ interacting with the real world. Put formally, $\tau$ is bad if one of the following conditions is set:*

*Bad1: $\exists(\phi, t, x, y) \in \tau_1, \phi \in \Phi, t \in \mathcal{T}$, and $(u, v) \in \tau_2$, such that $x \oplus u = H_{\phi(K)}(t)$;*

*Bad2: $\exists(\phi, t, x, y) \in \tau_1, \phi \in \Phi, t \in \mathcal{T}$, and $(u, v) \in \tau_2$, such that $y \oplus v = H_{\phi(K)}(t)$;*

*Bad3: $\exists(\phi, t, x, y) \neq (\phi', t', x', y') \in \tau_1, \phi, \phi' \in \Phi, t, t' \in \mathcal{T}$, such that $x \oplus x' = H_{\phi(K)}(t) \oplus H_{\phi'(K)}(t')$;*

*Bad4: $\exists(\phi, t, x, y) \neq (\phi', t', x', y') \in \tau_1, \phi, \phi' \in \Phi, t, t' \in \mathcal{T}$, such that $y \oplus y' = H_{\phi(K)}(t) \oplus H_{\phi'(K)}(t')$.*

*Otherwise we say that $\tau$ is good. We denote $\Gamma_{good}$, resp. $\Gamma_{bad}$ the set of good, resp. bad transcripts, $\Gamma = \Gamma_{good} \cup \Gamma_{bad}$.*

We firstly upper bound the probability of bad transcripts in the ideal world $Y$ by the following lemma.

**Lemma 4.** *If $H$ is $(\epsilon, \delta)$-RKA-AXU for the RKD set $\Phi$ and $P$ is public random permutation, then*

$$Pr(D_Y \in \Gamma_{bad}) \leq D(D-1)\epsilon + 2DT\delta.$$

*Proof.* In the ideal world $Y$, $\tau$ is an attainable transcript generated independently of the dummy key $K \in \mathcal{K}$. Assume an adversary $\mathcal{A}$ makes at most $D$ construction queries and at most $T$ primitive queries. For $(\phi, t, x, y) \in \tau_1, \phi \in \Phi, t \in \mathcal{T}$, and $(u, v) \in \tau_2$, by the properties of the $(\epsilon, \delta)$-RKA-AXU hash function $H$, we have

$$\begin{aligned} Pr[Bad1] &= Pr[Bad2] \\ &= Pr[K \xleftarrow{\$} \mathcal{K} : H_{\phi(K)}(t) = C] \leq DT\delta, \end{aligned}$$

where $C = x \oplus u$ in Bad1 or $C = y \oplus v$ in Bad2.

Fix any distinct queries $(\phi, t, x, y) \neq (\phi', t', x', y') \in \tau_1, \phi, \phi' \in \Phi, t, t' \in \mathcal{T}$. By the properties of the $(\epsilon, \delta)$-RKA-AXU hash function $H$, we have

$$\begin{aligned} Pr[Bad3] &= Pr[Bad4] \\ &= Pr[K \xleftarrow{\$} \mathcal{K} : H_{\phi(K)}(t) \oplus H_{\phi'(K)}(t') = C] \\ &\leq \binom{D}{2}\epsilon, \end{aligned}$$

where $C = x \oplus x'$ in Bad3 or $C = y \oplus y'$ in Bad4.

Therefore,

$$
\begin{aligned}
Pr[D_Y \in \Gamma_{bad}] = Pr[\bigcup_{i=1}^{4} Badi] &\leq \sum_{i=1}^{4} Pr[Badi] \\
&\leq D(D-1)\epsilon + 2DT\delta.
\end{aligned}
$$

We then analyze good transcripts.

**Lemma 5.** *For any good transcript $\tau$, one has*

$$\frac{Pr[D_X = \tau]}{Pr[D_Y = \tau]} \geq 1.$$

*Proof.* Consider a good transcript $\tau \in \Gamma_{good}$. Denote by $\Omega_X$ the set of all possible oracles in the real world $X$ and by $\Omega_Y$ the set of all possible oracles in the ideal world $Y$. Let $comp_X(\tau) \subseteq \Omega_X$ and $comp_Y(\tau) \subseteq \Omega_Y$ be the set of oracles compatible with transcript $\tau$. According to the H-coefficients technique, we have

$Pr(D_X = \tau) = \frac{|comp_X(\tau)|}{|\Omega_X|}$, where $|\Omega_X| = 2^n!|\mathcal{K}|$.

$Pr(D_Y = \tau) = \frac{|comp_Y(\tau)|}{|\Omega_Y|}$, where $|\Omega_Y| = \prod_{\phi,t}(2^n!) \cdot 2^n!|\mathcal{K}|$ and $(\phi, t) \in (\Phi, \mathcal{T})$.

Firstly, we calculate $|comp_X(\tau)|$. As $\tau \in \Gamma_{good}$, there are no two queries in $\tau$ with the same input or output of the underlying permutation. Any query tuple in $\tau$ therefore fixes exactly one input-output pair of the underlying oracle. Because $\tau$ consists of $D+T$ query tuples, the number of possible oracles in the real world $X$ equals $(2^n - D - T)!$.

For the analysis in the ideal world $Y$, we define

$$D_{\phi,t} = |\{(\phi, t, x, y) \in \tau_1 | (\phi, t) \in (\Phi, \mathcal{T}), x, y \in \{0,1\}^n\}|.$$

By a similar reason, the number of possible oracles in $Y$ equals $\prod_{\phi,t}(2^n - D_{\phi,t})!(2^n - T)!$, where $\sum_{\phi,t} D_{\phi,t} = D$. It follows that,

$$
\begin{aligned}
Pr(D_X = \tau) &= \frac{(2^n - D - T)!}{2^n!|\mathcal{K}|} \\
Pr(D_Y = \tau) &= \frac{\prod_{\phi,t}(2^n - D_{\phi,t})!(2^n - T)!}{\prod_{\phi,t}(2^n!) \cdot 2^n!|\mathcal{K}|} \\
&\leq \frac{(2^n - D - T)!}{2^n!|\mathcal{K}|}.
\end{aligned}
$$

Therefore, we have $\frac{Pr[D_X = \tau]}{Pr[D_Y = \tau]} \geq 1$.

By H-coefficients technique, we have

$$Adv_{TEM}^{rka}(\mathcal{A}) \leq D(D-1)\epsilon + 2DT\delta.$$

The tweakable Even-Mansour cipher in the single-key setting is a special case of it in the related-key setting if a RKD set $\Phi_{id} = \{\phi : K \to K\}$ is an identity transform. Therefore, the bound that we derived for the tweakable Even-Mansour cipher in the related-key setting is also tight. If we replace the public random permutation with an ideal block cipher with the same characteristics (including block-size, RKA-AXU-hash functions, etc), we can obtain the similar security.

## 5 Conclusion

This paper focuses on the tweakable Even-Mansour cipher in the multi-key and related-key settings. Multi-key and related-key settings occur frequently in real-world implementations, that is to say, a plaintext may be encrypted under different keys. The adversary can perform chosen-plaintext and chosen-ciphertext attacks under a set of unknown keys.

In the multi-key setting, these keys are independently and randomly chosen from the key space. We prove that the tweakable Even-Mansour cipher with $(\epsilon, \delta)$-AXU-hash functions is multi-key-secure up to $2D(T + D(1 - 1/l))\delta + (D - l + 1)(D - l)\epsilon$ queries, where $D$ is the complexity of construction queries (data complexity), $T$ is the complexity of internal permutation queries (time complexity), and $l$ is the number of keys.

In the related-key setting, the adversary can observe the operation of a cipher under several different keys whose values are initially unknown, but where some mathematical relationship connecting the keys is known to the adversary. We prove that the tweakable Even-Mansour cipher with $(\epsilon, \delta)$-RKA-AXU-hash functions is related-key-secure up to $D(D-1)\epsilon + 2DT\delta$ queries, where $D$ is the complexity of construction queries (data complexity) and $T$ is the complexity of internal permutation queries (time complexity).

The tweakable Even-Mansour cipher with RKA-AXU-hash function is secure in the single-key, multi-key, and related-key settings. The tweakable Even-Mansour cipher not only has a simple structure, but also it is based on a permutation, which makes it easier to generate fast and secure implementations. If we use the tweakable Even-Mansour cipher instead of the underlying block cipher, encryption modes, authentication modes, and authenticated encryption modes may be implemented more efficiently and may be more secure.

We leave it as an interesting open problem to settle the security of two-round iterated tweakable Even-Mansour cipher in the multi-key and related-key settings. Does further extend it for any $r$-round iterated tweakable Even-Mansour cipher?

**Acknowledgments.** The heading should be treated as a subsubsection heading and should not be assigned a number.

## References

1. Andreeva, E., Bogdanov, A., Luykx, A., Mennink, B., Tischhauser, E., Yasuda, K.: Parallelizable and authenticated online ciphers. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013. LNCS, vol. 8269, pp. 424–443. Springer, Heidelberg (2013)
2. Bellare, M., Kohno, T.: A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 491–506. Springer, Heidelberg (2003)
3. Bhattacharyya, R., Roy, A.: Secure message authentication against related-key attack. In: Moriai, S. (ed.) FSE 2013. LNCS, vol. 8424, pp. 305–324. Springer, Heidelberg (2013)

4. Biham, E.: New Types of Cryptoanalytic Attacks Using related Keys (Extended Abstract). In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 398–409. Springer, Heidelberg (1993)
5. Biham, E.: New Types of Cryptanalytic Attacks Using Related Keys. J. Cryptology. 7(4), 229–246 (1994)
6. Biryukov, A., Khovratovich, D.: Related-key cryptanalysis of the full AES-192 and AES-256. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 1–18. Springer, Heidelberg (2009)
7. Chakraborty, D., Sarkar, P.: On modes of operations of a block cipher for authentication and authenticated encryption. Cryptography and Communications. 8(4): 455-511 (2016)
8. Chatterjee, S., Menezes, A., Sarkar, P.: Another Look at Tightness. In: Miri, A., Vaudenay, S. (eds.) SAC 2011. LNCS, vol. 7118, pp. 293–319. Springer, Heidelberg (2011)
9. Chen, J., Miyaji, A.: A new practical key recovery attack on the stream cipher RC4 under related-key model. In: Lai, X., Yung, M., Lin, D. (eds.) Inscrypt 2010. LNCS, vol. 6584, pp. 62–76. Springer, Heidelberg (2010)
10. Chen, S., Steinberger, J.P.: Tight Security Bounds for Key-Alternating Ciphers. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 327–350. Springer, Heidelberg (2014)
11. Cogliati, B., Lampe, R., Seurin, Y.: Tweaking Even-Mansour ciphers. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 189–208. Springer, Heidelberg (2015)
12. Cogliati, B., Seurin, Y.: On the provable security of the iterated Even-Mansour cipher against related-key and chosen-key attacks. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 584–613. Springer, Heidelberg (2015)
13. Cogliati, B., Seurin, Y.: Beyond-Birthday-Bound Security for Tweakable Even-Mansour Ciphers with Linear Tweak and Key Mixing. In: Iwata, T., Cheon, H. (eds.) ASIACRYPT 2015. LNCS, vol. 9453, pp. 134–158. Springer, Heidelberg (2015)
14. Dobraunig, C., Eichlseder, M., Mendel, F.: Related-key forgeries for Prost-OTR. In: Leander, G. (ed.) FSE 2015. LNCS, vol. 9054, pp. 282–296. Springer, Heidelberg (2015)
15. Fouque, P., Joux, A., Mavromati, C.: Multi-user Collisions: Applications to Discrete Logarithm, Even-Mansour and PRINCE. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 420–438. Springer, Heidelberg (2014)
16. Granger, R., Jovanovic, P., Mennink, B., Neves, S..: Improved masking for tweakable blockciphers with applications to authenticated encryption. In: Fischlin, M., Coron, J. S. (eds.) EUROCRYPT 2016. LNCS, vol. 9665, pp. 263–293. Springer, Heidelberg (2016)
17. Halevi, S., Rogaway, P.: A tweakable enciphering mode. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 482–499. Springer, Heidelberg (2003)
18. Halevi, S., Rogaway, P.: A parallelizable enciphering mode. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 292–304. Springer, Heidelberg (2004)
19. Hellman, M.E.: A Cryptanalytic Time-Memory Trade-off. IEEE Transactions on Information Theory. 26(4), 401–406 (1980)
20. Kurosawa, K.: Power of a public random permutation and its application to authenticated encryption. IEEE Transactions on Information Theory. 5(10): 5366–5374 (2010)
21. Landecker, W., Shrimpton, T., Terashima, R. S.: Tweakable Blockciphers with Beyond Birthday-Bound Security. In Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012, LNCS, vol. 7417, pp. 14–30. Springer, Heidelberg (2012)

22. Liskov, M., Rivest, R.L., Wagner, D.: Tweakable block ciphers. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 31–46. Springer, Heidelberg (2002)
23. Mantin, I., Shamir, A.: A Practical Attack on Broadcast RC4. In: Matsui, M. (ed.) FSE 2001. LNCS, vol. 2355, pp. 152–164. Springer, Heidelberg (2001)
24. Mouha, N., Luykx, A.: Multi-key Security: The Even-Mansour Construction Revisited. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 209–223. Springer, Heidelberg (2015)
25. Patarin, J.: The "Coefficients H" Technique. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 328–345. Springer, Heidelberg (2008)
26. Peyrin, T., Sasaki, Y., Wang, L.: Generic related-key attacks for HMAC. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 580–597. Springer, Heidelberg (2012)
27. Reyhanitabar, R., Vaudenay, S., Vizr, D.: Misuse-Resistant Variants of the OMD Authenticated Encryption Mode. In: Chow, S.S.M., Liu, J.K., Hui, L.C.K., Yiu, S. (eds.) ProvSec 2014. LNCS, vol. 8782, pp. 55C70. Springer, Heidelberg (2014)
28. Rogaway, P., Zhang, H.: Online ciphers from tweakable blockciphers. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 237–249. Springer, Heidelberg (2011)
29. Rogaway, P.: Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 16–31. Springer, Heidelberg (2004)
30. Rogaway, P., Bellare, M., Black, J.: OCB: a block-cipher mode of operation for efficient authenticated encryption. ACM Trans. Inf. Syst. Secur. 6(3), 365–403 (2003)
31. Sun, S., Hu, L., Wang, P., Qiao, K., Ma, X., Song, L.: Automatic security evaluation and (related-key) differential characteristic search: Application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 158–178. Springer, Heidelberg (2014)
32. Wang, P., Li, Y., Zhang, L., Zheng, K.: Related-Key Almost Universal Hash Functions: Definitions, Constructions and Applications. IACR Cryptology ePrint Archive 2015, 766 (2015), https://eprint.iacr.org/2015/766.pdf