SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Multi-user security of the tweakable Even-Mansour cipher

Ping ZHANG[1*], Qian YUAN[2], Honggang HU[3] & Peng WANG[4]

[1]*Nanjing University of Posts and Telecommunications, Nanjing* 210023*, China;*
[2]*Southeast University, Nanjing* 211189*, China;*
[3]*University of Science and Technology of China, Hefei* 230027*, China;*
[4]*Institute of Information Engineering, CAS, Beijing* 100049*, China*

Appendix A The security proof of Theorem 1

Appendix A.1 Preliminaries

Notations. Let $\mathbb{N}$ be a set of natural number. Given a finite set X, let $x \xleftarrow{\$} X$ be a value uniformly sampling from X. Let $Pr[\mathcal{A}^O = 1]$ be a probability of an event that an adversary $\mathcal{A}$ outputs 1 after interacting with the oracle O. Here we require $\mathcal{A}$ never makes a query whose response is obviously known.

Tweakable Blockcipher (TBC). A TBC $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ is a mapping, which inputs a key $K \in \mathcal{K}$, a tweak $t \in \mathcal{T}$, and a message $x \in \{0,1\}^n$, and outputs a ciphertext $y = \widetilde{E}(K,t,x)$, where the nonempty set $\mathcal{K}$ is a key space and the nonempty set $\mathcal{T}$ is a tweak space. Fix any $K \in \mathcal{K}$ and $t \in \mathcal{T}$, $\widetilde{E}_K(t,\cdot) = \widetilde{E}(K,t,\cdot)$ is a permutation over $\{0,1\}^n$ and $\widetilde{D}_K(t,\cdot) = \widetilde{E}_K^{-1}(t,\cdot)$ stands for its inverse. Let $Perm(n)$ be the set of all permutations over $\{0,1\}^n$. Let $\widetilde{Perm}(\mathcal{T},n)$ be the set of all mappings $\widetilde{Perm} : \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ such that $\widetilde{Perm}(t,\cdot)$ is a permutation over $\{0,1\}^n$ for each $t \in \mathcal{T}$.

Tweakable Even-Mansour (TEM) Cipher. Let $n, r \geqslant 1$ be two integers and $\mathcal{K}, \mathcal{T}$ be two nonempty sets. Given an r-tuple of n-bit permutations $P = (P_1, \cdots, P_r)$ and a universal hash function $H : \mathcal{K} \times \mathcal{T} \to \{0,1\}^n$, let $K = (K_1, \cdots, K_r) \in \mathcal{K}^r$ be a key, $t \in \mathcal{T}$ be a tweak, and x be an n-bit plaintext, then the r-round TEM cipher (TEM$[n, r, H]$) is defined as

$$TEM^P(K,t,x) = \Pi^{P_r}_{K_r,t} \circ \cdots \circ \Pi^{P_1}_{K_1,t}(x),$$

where $\Pi^P_{K,t}$ is defined as (corresponding to the one-round TEM cipher)

$$\Pi^P_{K,t}(x) = P(x \oplus H_K(t)) \oplus H_K(t).$$

Universal Hash Function Family. Let $\mathcal{K}$ be a nonempty key set and $\mathcal{T}$ be a nonempty input set. Let $\mathcal{H} = \{H_K : \mathcal{T} \to \{0,1\}^n\}$ be a set of functions, where $K \in \mathcal{K}$. If for any $t \in \mathcal{T}$ and $y \in \{0,1\}^n$,

$$Pr[K \xleftarrow{\$} \mathcal{K} : H_K(t) = y] = 2^{-n},$$

then $\mathcal{H}$ is called a uniform hash function family.

If for any $t, t' \in \mathcal{T}$, $t \neq t'$, and $y \in \{0,1\}^n$,

$$Pr[K \xleftarrow{\$} \mathcal{K} : H_K(t) \oplus H_K(t') = y] \leqslant \epsilon,$$

then $\mathcal{H}$ is called an ϵ-almost-XOR-universal (ϵ-AXU) hash function family.

If $\mathcal{H}$ is both uniform and ϵ-AXU, then $\mathcal{H}$ is called a uniform ϵ-AXU-hash function family.

Appendix A.2 Multi-user security of tweakable blockciphers

Let $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ be a permutation-based tweakable blockcipher. Let $P \xleftarrow{\$} Perm(n)$ be a public random permutation. Let u denote the number of users. Let $\mathcal{A}$ be an adversary that always has two-directional access to the underlying permutation and has (two-)directional access to the construction.

* Corresponding author (email: zhgp@njupt.edu.cn)

1. If $\mathcal{A}$ only makes the encryption queries to the construction, then the multi-user tweakable pseudorandom permutation (MU-TPRP) advantage of $\mathcal{A}$ with respect to u users is defined as

$$Adv_{\widetilde{E}}^{mu-tprp}(\mathcal{A}) = |Pr[A^{\widetilde{E}_{K_1},\widetilde{E}_{K_2},\cdots,\widetilde{E}_{K_u};P^{\pm}} = 1] - Pr[A^{\widetilde{\pi}_1,\widetilde{\pi}_2,\cdots,\widetilde{\pi}_u;P^{\pm}} = 1]|,$$

where $K_i \xleftarrow{\$} \mathcal{K}$ is the key of the i-th user, $1 \leqslant i \leqslant u$, and $\widetilde{\pi}_1, \widetilde{\pi}_2, \cdots, \widetilde{\pi}_u$ are independently and uniformly drawn from $\widetilde{Perm}(\mathcal{T}, n)$.

2. If $\mathcal{A}$ makes the encryption and decryption queries to the construction, then the multi-user strong tweakable pseudorandom permutation (MU-STPRP) advantage of $\mathcal{A}$ with respect to u users is defined as

$$Adv_{\widetilde{E}}^{mu-stprp}(\mathcal{A}) = |Pr[A^{\widetilde{E}^{\pm}_{K_1},\widetilde{E}^{\pm}_{K_2},\cdots,\widetilde{E}^{\pm}_{K_u};P^{\pm}} = 1] - Pr[A^{\widetilde{\pi}^{\pm}_1,\widetilde{\pi}^{\pm}_2,\cdots,\widetilde{\pi}^{\pm}_u;P^{\pm}} = 1]|,$$

where $K_i \xleftarrow{\$} \mathcal{K}$ is the key of the i-th user, $1 \leqslant i \leqslant u$, and $\widetilde{\pi}_1, \widetilde{\pi}_2, \cdots, \widetilde{\pi}_u$ are independently and uniformly drawn from $\widetilde{Perm}(\mathcal{T}, n)$.

For $p, q \geqslant 0$, let

$$Adv_{\widetilde{E}}^{mu-(s)tprp}(p, q) = max_{\mathcal{A}} Adv_{\widetilde{E}}^{mu-(s)tprp}(\mathcal{A})$$

be the MU-(S)TPRP security of $\widetilde{E}$ against any adversary that makes p queries to the primitive and q queries to the construction, where p and q are respectively the total number of queries for the primitive and the construction.

For some special cases, we make some discussions as follows: If $u = 1$, we denote $Adv_{\widetilde{E}}^{tprp}$ and $Adv_{\widetilde{E}}^{stprp}$ as the single-user TPRP and STPRP advantages, respectively. If the tweak space $\mathcal{T}$ is an empty set, we denote Adv_{E}^{mu-prp} and $Adv_{E}^{mu-sprp}$ as the MU-PRP and MU-SPRP advantages against a block cipher E, respectively. Especially, if $u = 1$, we denote Adv_{E}^{prp} and Adv_{E}^{sprp} as the single-user PRP and SPRP advantages, respectively.

Appendix A.3 The expectation method

The property of point-wise proximity first presented by Hoang and Tessaro [1] is a stronger property than indistinguishability. We describe simply this property as follows. Given a real system X and an ideal system Y, let $\mathcal{A}$ be an adversary, which interacts with X or Y. The interaction between $\mathcal{A}$ and X or Y is seen as a transcript τ, which contains a list of query-response pairs. Let $p_X(\tau)$ (resp. $p_Y(\tau)$) be the real (resp. ideal) interpolation probability, which denotes the probability of the transcript τ induced by X (resp. Y). Let V_X (resp. V_Y) be the random variable representing the transcript induced by X (resp. Y). Then $p_X(\tau) = Pr[V_X = \tau]$ and $p_Y(\tau) = Pr[V_Y = \tau]$.

Definition 1 (Point-wise proximity [1])**.** We say that X and Y satisfy ϵ-point-wise proximity if, for every possible transcript τ,

$$\Delta(\tau) = p_Y(\tau) - p_X(\tau) \leqslant p_Y(\tau) \cdot \epsilon.$$

Let $\mathcal{A}$ be a deterministic adversary, whose goal is to distinguish X from Y. Then the advantage of $\mathcal{A}$ is bounded by ϵ, i.e.,

$$\begin{aligned} Adv(\mathcal{A}) &= |Pr[\mathcal{A}^X = 1] - Pr[\mathcal{A}^Y = 1]| \\ &\leqslant SD(X, Y) = \frac{1}{2}\sum_{\tau} |p_X(\tau) - p_Y(\tau)| \\ &= \sum_{\tau} \Delta(\tau) \leqslant \sum_{\tau} p_Y(\tau) \cdot \epsilon \leqslant \epsilon. \end{aligned}$$

In this paper, we present the expectation method introduced by Hoang and Tessaro [1] to bound the gap $\Delta(\tau)$ for a multi-user transcript τ such that $p_Y(\tau) > 0$. We briefly introduce this method as follows.

The expectation method is an improved version of Patarin's H-coefficients technique [2]. This method can be utilized to process a complex transcript with a random variable S (e.g., a secret key). Let X be a real system that depends on S. Let $p_X(\tau, s)$ be the real probability that X answers queries according to τ and that S equals to s. Let Y be an ideal system, which includes the random variable S with the same marginal distribution as X but independent of the behavior of Y. Let $p_Y(\tau, s) = p_Y(\tau) \cdot Pr[S = s]$.

Lemma 1 (The expectation method [1])**.** Fix a transcript τ for which $p_Y(\tau) > 0$. Assume that there exists a partition Γ_{good} and Γ_{bad} of the range U of S, and a function $g : U \to [0, \infty)$ such that $Pr[S \in \Gamma_{bad}] \leqslant \delta$, and for all $s \in \Gamma_{good}$,

$$1 - \frac{p_X(\tau, s)}{p_Y(\tau, s)} \leqslant g(s).$$

Then

$$\Delta(\tau) \leqslant p_Y(\tau) \cdot (\delta + E[g(S)]).$$

Let $\mathcal{A}$ be an adversary, according to Definition 1, then the advantage of $\mathcal{A}$ is bounded by $\delta + E[g(S)]$.

The partitioning into Γ_{good} and Γ_{bad}, the function g, and the random variable S are all allowed to depend on τ.

When s is reduced to τ (i.e., $s = \tau$) and $g(s) = \varepsilon$ is a constant, the expectation method degrades to Patarin's H-coefficients technique [2].

Appendix A.4 The security proof of Theorem 1

Let $\widetilde{E}_K = TEM[n,1,H]$ stand for the encryption algorithm of TEM-1. Let $X = (\widetilde{E}^{\pm}_{K_1}, \cdots, \widetilde{E}^{\pm}_{K_u}; P^{\pm})$, where $K_1, \cdots, K_u$ are the keys of u users, (resp. $Y = (\widetilde{\pi}^{\pm}_1, \cdots, \widetilde{\pi}^{\pm}_u; P^{\pm})$, where $\widetilde{\pi}_1, \cdots, \widetilde{\pi}_u$ are randomly sampling from $\widetilde{Perm}(\mathcal{T}, n)$) be the real (resp. ideal) world. Let $\mathcal{A}$ be an adversary, which makes at most p queries to $P^{\pm}$ and q queries to $(\widetilde{E}^{\pm}_{K_1}, \cdots, \widetilde{E}^{\pm}_{K_u})$ or $(\widetilde{\pi}^{\pm}_1, \cdots, \widetilde{\pi}^{\pm}_u)$ (See Figure A1).

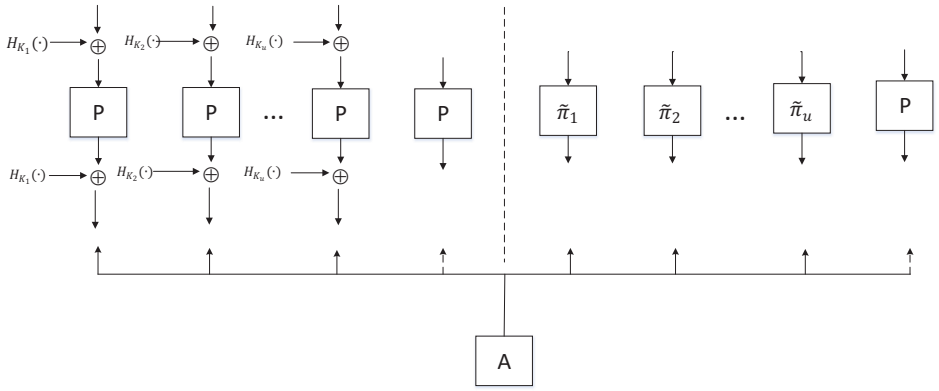

Figure A1 Multi-user security model of TEM-1. Let $\mathcal{A}$ be an adversary, which makes the encryption and decryption queries to TEM-1.

We assume that the adversary $\mathcal{A}$ makes at most q queries in total, adaptively chooses q_i queries to $\widetilde{E}^{\pm}_{K_i}$ or $\widetilde{\pi}^{\pm}_i$ for user i, where $q_i = 0, \cdots, q$ for $i = 1, \cdots, u$ and $q = \sum_{i=1}^{u} q_i$, and interacts with X and Y. This interaction generates a tuple of transcripts $\tau = (K_1, \cdots, K_u, \tau_1, \cdots, \tau_u, \tau_{u+1})$, where K_i is the key of the i-th user and $\tau_i = \{(t_i^1, x_i^1, y_i^1), \cdots, (t_i^{q_i}, x_i^{q_i}, y_i^{q_i})\}$ with $t_i^1, \cdots, t_i^{q_i} \in \mathcal{T}$ is the transcript of all queries to the i-th user for $i = 1, \cdots, u$, and $\tau_{u+1} = \{(u^1, v^1), \cdots, (u^p, v^p)\}$ is the transcript of all queries to $P^{\pm}$. Assuming that $\mathcal{A}$ never makes useless queries, we have $(t_i^j, x_i^j) \neq (t_i^{j'}, x_i^{j'}), (t_i^j, y_i^j) \neq (t_i^{j'}, y_i^{j'}), u^j \neq u^{j'}$, and $v^l \neq v^{l'}$ for all i, j, j', l, and l', where $1 \leqslant i \leqslant u$, $1 \leqslant j \neq j' \leqslant q_i$, and $1 \leqslant l \neq l' \leqslant p$.

Let $p_X(\tau)$ (resp. $p_Y(\tau)$) denote the interpolation probability of the transcript τ induced by X (resp. Y). Let V_X (resp. V_Y) be the random variable representing the transcript induced by X (resp. Y). Then $p_X(\tau) = Pr[V_X = \tau]$ and $p_Y(\tau) = Pr[V_Y = \tau]$. By the expectation method (H-coefficients technique), we start with the definition of bad transcripts.

Definition 2. A transcript $\tau = (K_1, \cdots, K_u, \tau_1, \cdots, \tau_u, \tau_{u+1})$ is called bad if any two distinct queries in X or Y would lead to the same input or output to P. In other words, τ is bad if one of the following events happens:

Event E_1: There exist $(t_i^j, x_i^j, y_i^j) \in \tau_i$ and $(u^{j'}, v^{j'}) \in \tau_{u+1}$ such that $x_i^j \oplus u^{j'} = H_{K_i}(t_i^j)$, where $t_i^j \in \mathcal{T}$, $1 \leqslant i \leqslant u, 1 \leqslant j \leqslant q_i$, and $1 \leqslant j' \leqslant p$;

Event E_2: There exist $(t_i^j, x_i^j, y_i^j) \in \tau_i$ and $(u^{j'}, v^{j'}) \in \tau_{u+1}$ such that $y_i^j \oplus v^{j'} = H_{K_i}(t_i^j)$, where $t_i^j \in \mathcal{T}$, $1 \leqslant i \leqslant u, 1 \leqslant j \leqslant q_i$, and $1 \leqslant j' \leqslant p$;

Event E_3: There exist $(t_i^j, x_i^j, y_i^j) \neq (t_i^{j'}, x_i^{j'}, y_i^{j'}) \in \tau_i$ such that $x_i^j \oplus x_i^{j'} = H_{K_i}(t_i^j) \oplus H_{K_i}(t_i^{j'})$, where $t_i^j, t_i^{j'} \in \mathcal{T}$, $1 \leqslant i \leqslant u$, and $1 \leqslant j \neq j' \leqslant q_i$;

Event E_4: There exist $(t_i^j, x_i^j, y_i^j) \neq (t_i^{j'}, x_i^{j'}, y_i^{j'}) \in \tau_i$ such that $y_i^j \oplus y_i^{j'} = H_{K_i}(t_i^j) \oplus H_{K_i}(t_i^{j'})$, where $t_i^j, t_i^{j'} \in \mathcal{T}$, $1 \leqslant i \leqslant u$, and $1 \leqslant j \neq j' \leqslant q_i$;

Event E_5: There exist $(t_i^j, x_i^j, y_i^j) \in \tau_i$ and $(t_{i'}^{j'}, x_{i'}^{j'}, y_{i'}^{j'}) \in \tau_{i'}$ such that $x_i^j \oplus x_{i'}^{j'} = H_{K_i}(t_i^j) \oplus H_{K_{i'}}(t_{i'}^{j'})$, where $t_i^j, t_{i'}^{j'} \in \mathcal{T}$, $1 \leqslant i \neq i' \leqslant u, 1 \leqslant j \leqslant q_i$, and $1 \leqslant j' \leqslant q_{i'}$;

Event E_6: There exist $(t_i^j, x_i^j, y_i^j) \in \tau_i$ and $(t_{i'}^{j'}, x_{i'}^{j'}, y_{i'}^{j'}) \in \tau_{i'}$ such that $y_i^j \oplus y_{i'}^{j'} = H_{K_i}(t_i^j) \oplus H_{K_{i'}}(t_{i'}^{j'})$, where $t_i^j, t_{i'}^{j'} \in \mathcal{T}$, $1 \leqslant i \neq i' \leqslant u, 1 \leqslant j \leqslant q_i$, and $1 \leqslant j' \leqslant q_{i'}$.

If a transcript τ is not bad, we say τ is a good transcript. Let Γ_{good} (resp. Γ_{bad}) be the set of good (resp. bad) transcripts. Let $\Gamma = \Gamma_{good} \cup \Gamma_{bad}$.

We first upper bound $Pr[V_Y \in \Gamma_{bad}]$ in the ideal world Y.

Lemma 2. Let H be a uniform ϵ-AXU hash function from a tweak space $\mathcal{T}$ to $\{0,1\}^n$ and u be the number of users. For $\frac{1}{2^n} \leqslant \epsilon \leqslant \frac{2}{2^n}$, then

$$Pr[V_Y \in \Gamma_{bad}] \leqslant \frac{2qp}{2^n} + \frac{2q^2(1-\frac{1}{u})}{2^n} + q(\frac{q}{u} - 1)\epsilon.$$

Proof. Let $\tau = (\tau_1, \cdots, \tau_u, \tau_{u+1})$ be any tuple of transcripts. In the ideal world Y, $K_i \in \mathcal{K}$ is the dummy key of the i-th user, where $i = 1, \cdots, u$. Let $\mathcal{A}$ be a deterministic adversary, which makes p queries to $P^{\pm}$ and q_i queries to $\widetilde{E}^{\pm}_{K_i}$ or $\widetilde{\pi}^{\pm}_i$, where $1 \leqslant i \leqslant u$ and $q = \sum_{i=1}^{u} q_i$.

For events E_1 and E_2, according to the properties of H, we have

$$\begin{aligned} Pr[E_1 \vee E_2] &= Pr[K_i \xleftarrow{\$} \mathcal{K} : H_{K_i}(t_i^j) = x_i^j \oplus u^{j'} \vee H_{K_i}(t_i^j) = y_i^j \oplus v^{j'}] \\ &\leqslant 2\sum_{i=1}^{u} q_i p/2^n = 2qp/2^n. \end{aligned}$$

For events E_3 and E_4, according to the properties of H, we have

$$\begin{aligned} Pr[E_3 \vee E_4] &= Pr[K_i \xleftarrow{\$} \mathcal{K} : H_{K_i}(t_i^j) \oplus H_{K_i}(t_i^{j'}) = C] \\ &\leqslant 2\sum_{i=1}^{u} \binom{q_i}{2}\epsilon = (\sum_{i=1}^{u} q_i^2 - q)\epsilon, \end{aligned}$$

where $C = x_i^j \oplus x_i^{j'}$ in **Event** E_3 or $C = y_i^j \oplus y_i^{j'}$ in **Event** E_4.

For events E_5 and E_6, according to the properties of H, we have

$$\begin{aligned} &Pr[E_5 \vee E_6] \\ =&Pr[K_i, K_{i'} \xleftarrow{\$} \mathcal{K} : H_{K_i}(t_i^j) \oplus H_{K_{i'}}(t_{i'}^{j'}) = C] \\ =&\sum_{a_i, b_i \in \{0,1\}^n} Pr[K_i, K_{i'} \xleftarrow{\$} \mathcal{K} : a_i \oplus b_i = C | H_{K_i}(t_i^j) = a_i, H_{K_{i'}}(t_{i'}^{j'}) = b_i] \cdot \\ &Pr[K_i, K_{i'} \xleftarrow{\$} \mathcal{K} : H_{K_i}(t_i^j) = a_i, H_{K_{i'}}(t_{i'}^{j'}) = b_i] \\ \leqslant&\sum_{a_i \in \{0,1\}^n} Pr[K_i, K_{i'} \xleftarrow{\$} \mathcal{K} : H_{K_i}(t_i^j) = a_i, H_{K_{i'}}(t_{i'}^{j'}) = C - a_i] \\ \leqslant&\sum_{a_i \in \{0,1\}^n} Pr[K_i \xleftarrow{\$} \mathcal{K} : H_{K_i}(t_i^j) = a_i] \cdot \\ &Pr[K_{i'} \xleftarrow{\$} \mathcal{K} : H_{K_{i'}}(t_{i'}^{j'}) = C - a_i] \ \ (Key\ Independence) \\ \leqslant&2 \times 2^n \times (q^2 - \sum_{i=1}^{u} q_i^2) \times 2^{-n} \times 2^{-n} \\ \leqslant&2q^2/2^n - 2\sum_{i=1}^{u} q_i^2/2^n, \end{aligned}$$

where $C = x_i^j \oplus x_{i'}^{j'}$ in **Event** E_5 or $C = y_i^j \oplus y_{i'}^{j'}$ in **Event** E_6.

To summarise, we have

$$\begin{aligned} Pr[V_Y \in \Gamma_{bad}] &= Pr[\bigcup_{i=1}^{6} E_i] \\ &\leqslant Pr[E_1 \vee E_2] + Pr[E_3 \vee E_4] + Pr[E_5 \vee E_6] \\ &\leqslant 2pq/2^n + (\sum_{i=1}^{u} q_i^2 - q)\epsilon + 2q^2/2^n - 2\sum_{i=1}^{u} q_i^2/2^n \\ &\leqslant 2q(p+q)/2^n + \sum_{i=1}^{u} q_i^2(\epsilon - 2/2^n) - q\epsilon. \end{aligned}$$

1) If $1/2^n \leqslant \epsilon \leqslant 2/2^n$, by Cauchy Inequality $\sum_{i=1}^{u} q_i^2 \geqslant q^2/u$, where the minimum value q^2/u is obtained by the average case that an adversary makes q/u queries to each user, we have

$$\begin{aligned} Pr[V_Y \in \Gamma_{bad}] &= Pr[\bigcup_{i=1}^{6} E_i] \\ &\leqslant 2q(p+q)/2^n - \sum_{i=1}^{u} q_i^2(2/2^n - \epsilon) - q\epsilon \\ &\leqslant 2q(p+q)/2^n - q^2/u \cdot (2/2^n - \epsilon) - q\epsilon \\ &= \frac{2qp}{2^n} + \frac{2q^2(1-\frac{1}{u})}{2^n} + q(\frac{q}{u} - 1)\epsilon. \end{aligned}$$

2) If $\epsilon > 2/2^n$, by the inequality $q^2/u \leqslant \sum_{i=1}^{u} q_i^2 \leqslant q^2$, where the minimum value q^2/u is obtained by the average case that an adversary makes q/u queries to each user and the maximum value q^2 is obtained by the worst case that an adversary makes all q queries to some single user and no queries to others (single-user case), we have

$$Pr[V_Y \in \Gamma_{bad}] = Pr[\bigcup_{i=1}^{6} E_i]$$

$$\leqslant 2q(p+q)/2^n + \sum_{i=1}^{u} q_i^2(\epsilon - 2/2^n) - q\epsilon$$
$$\leqslant 2q(p+q)/2^n + q^2(\epsilon - 2/2^n) - q\epsilon$$
$$= 2qp/2^n + q(q-1)\epsilon.$$

Summarizing the above two cases, we have

$$Pr[V_Y \in \Gamma_{bad}] \leqslant \begin{cases} \frac{2qp}{2^n} + \frac{2q^2(1-\frac{1}{u})}{2^n} + q(\frac{q}{u} - 1)\epsilon & \epsilon \leqslant 2/2^n, \\ 2qp/2^n + q(q-1)\epsilon & \epsilon > 2/2^n. \end{cases}$$

Note that here ϵ stands for the randomness of uniform AXU-hash functions. In general, each uniform ϵ-AXU-hash function we choose should be close to a uniform distribution, i.e., $\epsilon \simeq 2^{-n}$. Therefore, for a good uniform ϵ-AXU-hash function, i.e., $1/2^n \leqslant \epsilon \leqslant 2/2^n$, we have

$$Pr[V_Y \in \Gamma_{bad}] \leqslant \frac{2qp}{2^n} + \frac{2q^2(1-\frac{1}{u})}{2^n} + q(\frac{q}{u} - 1)\epsilon.$$

This completes the proof.

According to the expectation method (H-coefficients technique), for a good transcript, we have the following lemma.

Lemma 3. Let τ be any good transcript, then

$$1 - \frac{p_X(\tau)}{p_Y(\tau)} \leqslant 0.$$

Proof. For a permutation queries transcript τ_{u+1} and a primitive permutation P, if $P(x) = y$ for all $(x, y) \in \tau_{u+1}$, we say P extends τ_{u+1}, i.e., $P \vdash \tau_{u+1}$. As τ_{u+1} includes p query tuples, we have

$$Pr[P \xleftarrow{\$} Perm(n) : P \vdash \tau_{u+1}] = \frac{(2^n - p)!}{2^n!}.$$

Similarity, for a tweakable permutation transcript τ_i and a tweakable permutation $\widetilde{\pi}_i$, if $\widetilde{\pi}_i(t, x) = y$ for all $(t, x, y) \in \tau_i$, we say $\widetilde{\pi}_i$ extends τ_i, i.e., $\widetilde{\pi}_i \vdash \tau_i$, for $i = 1, \cdots, u$.

As τ_i includes q_i query tuples, the number of tweaks is m, and the adversary makes $q_{t,i}$ queries to the t-th tweak in τ_i, where $\sum_{t=1}^{m} q_{t,i} = q_i$ and $\sum_{i=1}^{u} q_i = q$, we have

$$Pr[\widetilde{\pi}_i \xleftarrow{\$} \widetilde{Perm}(\mathcal{T}, n) : \widetilde{\pi}_i \vdash \tau_i] = \prod_{t=1}^{m} \frac{(2^n - q_{t,i})!}{2^n!}.$$

In the ideal world Y, the keys $\{K_i\}_{i=1}^{u}$, the permutations P, and the tweakable permutations $\{\widetilde{\pi}_i\}_{i=1}^{u}$ are random and independent, therefore the probability to obtain τ is

$$p_Y(\tau) = \frac{1}{|\mathcal{K}|^u} \times \frac{(2^n - p)!}{2^n!} \prod_{i=1}^{u} \prod_{t=1}^{m} \frac{(2^n - q_{t,i})!}{2^n!}.$$

In the real world X, the keys $\{K_i\}_{i=1}^{u}$ are randomly and independently drawn from the key space $\mathcal{K}$ and any query tuple in τ uniquely defines an input-output pair of the underlying permutation P, therefore the probability to obtain τ is

$$p_X(\tau) = \frac{1}{|\mathcal{K}|^u} \times \frac{(2^n - q - p)!}{2^n!}.$$

According to the inequality $(2^n - a)!(2^n - b)! \leqslant 2^n!(2^n - a - b)!$ for any $a, b \geqslant 0$, therefore we have

$$1 - \frac{p_X(\tau)}{p_Y(\tau)} \leqslant 0.$$

Therefore, the proof is finished and the expectation of a constant 0 is 0.

By Lemmas **??**, 2, and 3, for $1/2^n \leqslant \epsilon \leqslant 2/2^n$, we have

$$Adv_{TEM-1}^{mu-stprp}(p, q) \leqslant \frac{2qp}{2^n} + \frac{2q^2(1-\frac{1}{u})}{2^n} + q(\frac{q}{u} - 1)\epsilon.$$

Appendix B The security proof of Theorem 2

The proof is similar to Theorem 2 in [3]. Let $\mathcal{K}$ be the key space and $\mathcal{T}$ be the tweak space. Let $X = (\widetilde{E}_{K_1}^{\pm}, \cdots, \widetilde{E}_{K_u}^{\pm}; \widetilde{E}^{\pm})$ be the real world, where $K_1, \cdots, K_u$ are the keys of u users. Let $Y = (\widetilde{\pi}_1^{\pm}, \cdots, \widetilde{\pi}_u^{\pm}; \widetilde{E}^{\pm})$ be the ideal world, where $\widetilde{\pi}_1, \cdots, \widetilde{\pi}_u$ are randomly sampling from $\widetilde{Perm}(\mathcal{T}, n)$. Let $\mathcal{A}$ be an adversary, which makes at most p queries to $\widetilde{E}^{\pm}$ and q queries to $(\widetilde{E}_{K_1}^{\pm}, \cdots, \widetilde{E}_{K_u}^{\pm})$ or $(\widetilde{\pi}_1^{\pm}, \cdots, \widetilde{\pi}_u^{\pm})$ (See Figure B1).

Let $\mathbf{E}_1$ be an event that there exists $i \neq j$ such that $(t_i, K_i) = (t_j, K_j)$, where $t_i, t_j \in \mathcal{T}$ and $K_i, K_j \in \mathcal{K}$. Let $\mathbf{E}_2$ be an event that there exists a query $\widetilde{E}^{\pm}(K, t, \cdot)$ such that $(t, K) = (t_i, K_i)$ for some i, where $t_i, t \in \mathcal{T}$ and $K_i, K \in \mathcal{K}$. Let $\mathbf{E} = \mathbf{E}_1 \vee \mathbf{E}_2$.

Assuming that the event $\mathbf{E}$ does not happen, $\widetilde{E}_{K_1}, \cdots, \widetilde{E}_{K_u}$ are chosen independently and randomly from $\widetilde{Perm}(\mathcal{T}, n)$, and all queries made to $\widetilde{E}^{\pm}$ are independent of $\widetilde{E}_{K_1}^{\pm}, \cdots, \widetilde{E}_{K_u}^{\pm}$, i.e., $X = (\widetilde{E}_{K_1}^{\pm}, \cdots, \widetilde{E}_{K_u}^{\pm}; \widetilde{E}^{\pm})$ and $Y = (\widetilde{\pi}_1^{\pm}, \cdots, \widetilde{\pi}_u^{\pm}; \widetilde{E}^{\pm})$ are indistinguishable. Therefore, the distinguishing advantage of $\mathcal{A}$ is bounded by

$$Adv_{ITBC}^{mu-stprp}(\mathcal{A}) \leqslant Pr[\mathbf{E}].$$

Let $n = k + l$, where k is the size of keys and l is the size of tweaks, we can easily evaluate

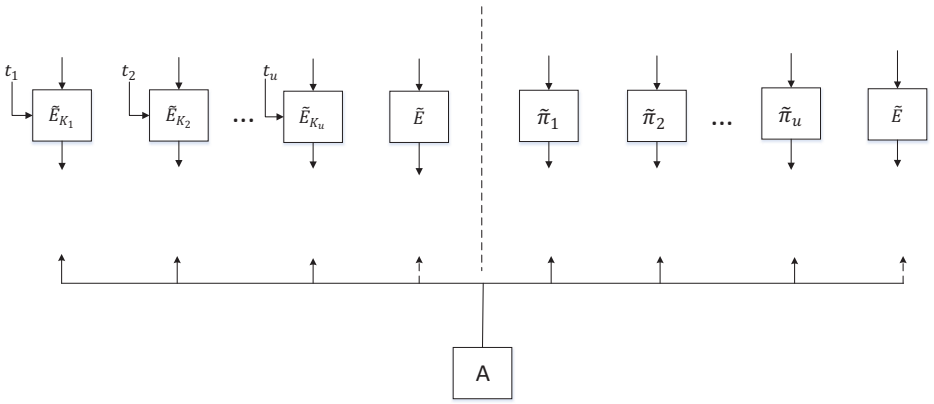

Figure B1 Multi-user security model of ideal TBCs. Let $\mathcal{A}$ be an adversary, which makes the encryption and decryption queries to ideal TBCs.

$$Pr[\mathbf{E}_1] \leqslant u(u-1)/2^{n+1} \leqslant u^2/2^{n+1} \text{ and } Pr[\mathbf{E}_2] \leqslant pu/2^n.$$

Therefore, by the addition theorem of probability, we have

$$\begin{aligned} Pr[\mathbf{E}] &= Pr[\mathbf{E}_1 \vee \mathbf{E}_2] \leqslant Pr[\mathbf{E}_1] + Pr[\mathbf{E}_2] \leqslant pu/2^n + u^2/2^{n+1} \\ &\leqslant \frac{u^2+2pu}{2^{n+1}} \leqslant \frac{q^2+2pq}{2^{n+1}}. \end{aligned}$$

To summarize, we have

$$Adv_{ITBC}^{mu-stprp}(\mathcal{A}) \leqslant Pr[\mathbf{E}] \leqslant \frac{q^2+2pq}{2^{n+1}}.$$

Appendix C Multi-user security of the r-round tweakable Even-Mansour cipher

Appendix C.1 From single-user security to multi-user security

Given a single-user security, the multi-user security can be directly obtained by the naive hybrid argument. But this bound is inferior and loose in reality. For lifting the single-user security to the multi-user security and obtaining a better bound of the multi-user security, Hoang and Tessaro presented the following results in their papers [1, 4].

Let $\mathcal{A}$ be an adversary, which makes at most p primitive queries and q construction queries. In the single-user case, the construction is $\epsilon(p,q)$-point-wise proximity, i.e., for i-th user, the advantage of $\mathcal{A}$ is bounded by

$$Adv^{su}(A) \leqslant \epsilon(p,q).$$

Let m be the number of invocations to the underlying primitive in the case of a single invocation to the construction. Take the r-round TEM cipher as an example, here $m = r$. Let $\epsilon(p+qm,q) \leqslant 1/2$. Hoang and Tessaro considered the following two cases.

Case 1. Assume that $\epsilon(p,q)$ satisfies the following conditions:

1) super-additive: $\epsilon(x,y) + \epsilon(x,z) \leqslant \epsilon(x,y+z)$ for every $x,y,z \in \mathbb{N}$.

2) monotonic increasing: $\epsilon(\cdot,z)$ is an increasing function on $\mathbb{N}$, for every $z \in \mathbb{N}$.

Hoang and Tessaro [1] showed that the multi-user security lifted from the single-user security via point-wise proximity is presented as follows.

Lemma 4 (From the single-user security to the multi-user security via point-wise proximity [1])**.** Assume that $\epsilon(p,q)$ satisfies the above two conditions. Let $\mathcal{A}$ be an adversary, which makes at most p primitive queries and q construction queries (for arbitrary users). Then

$$Adv^{mu}(A) \leqslant 2\epsilon(p+qm,q).$$

Case 2. Assume that $\epsilon(p,q)$ doesn't satisfy both super-additive and monotonic increasing, for lifting the single-user security to the multi-user security, Hoang and Tessaro generalized the property of point-wise proximity and provided another property of almost proximity to establish the multi-user security in [4]. As this paper is irrelevant to this property, we omit the details of this method.

Appendix C.2 Analysis of experimental data

Let $n = 128$, $p = q = u$, and $\epsilon = 2^{-n}$. We utilize the experimental data to analyze the security of the r-round TEM cipher in various settings (See Table C1).

Table C1 Results in Various Settings for the r-Round TEM Cipher, where $r \geqslant 2$. mu-naive: the multi-user security obtained by naive hybrid argument. mu-pwp: the multi-user security obtained by point-wise proximity. su: the single-user security. proximate: proximate (beyond-)birthday-bound security ($\frac{r}{r+2} \cdot n$-bit security for an even r or $\frac{r-1}{r+1} \cdot n$-bit security for an odd r). optimal: the asymptotically optimal beyond-birthday-bound security ($\frac{r}{r+1} \cdot n$-bit security for any r). Let $n = 128$, $p = q = u$, and $\epsilon = 2^{-n}$. The values in the table denote the log in base 2 of the minimal number of queries.

r	$2^{1)}$	3	4	5	6	7	8	9	10
mu-naive	30.25	30.25	48.97	48.97	61.33	61.33	70.10	70.10	76.63
mu-pwp	59.5	59.5	80.94	80.94	91.5	91.5	97.74	97.74	101.85
su	61	61	82.67	82.67	93.5	93.5	100	100	104.33
proximate	64	64	85.33	85.33	96	96	102.4	102.4	106.67
optimal	85.33	96	102.4	106.67	109.71	112	113.78	115.2	116.36

Table C1 shows that:

1) Compared with the single-user security, the multi-user security (derived by naive hybrid argument and point-wise proximity) is lower than it. This meets the fact that an adversary can obtain a bigger advantage by multiple (multi-user) queries. Furthermore, the multi-user security via point-wise proximity is better than the multi-user security via naive hybrid argument and the multi-user security via naive hybrid argument even doesn't reach the birthday-bound security (64-bit) in the case of small rounds.

2) For $r = 2, 3$, the bounds of the single-user security and the multi-user security via point-wise proximity are birthday bounds. For $r \geqslant 4$, the bounds of the single-user security and the multi-user security via point-wise proximity are loose (non-tight) beyond-birthday-bounds and far away from the optimal bound. Furthermore, for $r = 2, 3$, the bounds of the single-user security and the multi-user security via point-wise proximity can be improved to beyond-birthday-bounds. This reflects that there exist new techniques to obtain a better beyond-birthday-bound of the two-round TEM cipher.

3) For an even r or an odd r, their security is monotonically increasing, but for any integer r, their security is not monotonically increasing. This reflects that there exists a gap between the security of an odd round TEM cipher and the security of an even round TEM cipher, and meanwhile verifies that the security of the r-round TEM cipher is loose (non-tight).

Open Problem. For $r = 2$, Cogliati et al. presented a tight beyond-birthday-bound in the single-user setting [5]. However, for $r \geqslant 3$, the single-user security of the r-round TEM cipher is still an open problem. Therefore, we call more attentions on the study of the r-round TEM cipher and leave it as another interesting open problem of this paper to find a tight beyond-birthday-bound (and even close-to-optimal bound) for the multi-user security of the r-round TEM cipher, where $r \geqslant 2$. We have known that for TEM-1, the bound of the multi-user security directly derived by the expectation method (H-coefficients technique) is better than the bounds derived by naive hybrid argument and point-wise proximity. For the r-round TEM cipher, where $r \geqslant 2$, whether can we find a better (and tight) beyond-birthday-bound of the multi-user security directly using the expectation method (H-coefficients technique) or new techniques?

References

1 Hoang V T, Tessaro S. Key-alternating ciphers and key-length extension: exact bounds and multi-user security. In: Robshaw M, Katz J, eds. Proceedings of the 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, 2016. 3–32

2 Patarin J. The "Coefficients H" technique. In: Avanzi R M, Keliher L, Sica F, eds. Proceedings of the 15th International Workshop on Selected Areas in Cryptography, Sackville, New Brunswick, Canada, 2008. 328–345

3 Mouha N, Luykx A. Multi-key security: the Even-Mansour construction revisited. In: Gennaro R, Robshaw M, eds. Proceedings of the 35th Annual Cryptology Conference, Santa Barbara, CA, USA, 2015. 209–223

4 Hoang V T, Tessaro S. The multi-user security of double encryption. In: Coron J S, Nielsen J, eds. Proceedings of the 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, 2017. 381–411

5 Cogliati B, Lampe R, Seurin Y. Tweaking Even-Mansour ciphers. In: Gennaro R, Robshaw M, eds. Proceedings of the 35th Annual Cryptology Conference, Santa Barbara, CA, USA, 2015. 189–208

1) The cases $r = 2, 3$ can be improved to better beyond-birthday-bounds, according to the single-user security of the 2-round TEM cipher presented by Cogliati et al. [5]. From top to bottom: 30.25, 59.5, 61, and 64 are replaced with 48.42, 80.03, 81.33, and 85.33, respectively.