SCIENCE CHINA
Information Sciences

• LETTER •

March 2021, Vol. 64 139102:1–139102:3
https://doi.org/10.1007/s11432-018-9757-4

Multi-user security of the tweakable Even-Mansour cipher

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

[1]*School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing* 210023*, China;*
[2]*School of Economics and Management, Southeast University, Nanjing* 211189*, China;*
[3]*School of Information Science and Technology, University of Science and Technology of China, Hefei* 230027*, China;*
[4]*Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100049*, China*

Received 30 August 2018/Accepted 14 January 2019/Published online December 3 2020

Citation Zhang P, Yuan Q, Hu H G, et al. Multi-user security of the tweakable Even-Mansour cipher. Sci China Inf Sci, 2021, 64(3): 139102, https://doi.org/10.1007/s11432-018-9757-4

Dear editor,

Data security, including data privacy security and data integrity security, are usually achieved by a cryptographic algorithm. Block ciphers are widely used to design the cryptographic scheme. However, in some special environments, block ciphers are no longer applicable. A tweakable blockcipher (TBC) is an improved version of a conventional block cipher, which adds an extra input, called tweak, on the basis of a key and a plaintext. The tweakable Even-Mansour (TEM) cipher first presented by Cogliati et al. [1] is a permutation-based TBC, which is constructed from an r-tuple of n-bit permutations and a uniform almost-XOR-universal (AXU) hash function family from some tweak space $\mathcal{T}$ to $\{0,1\}^n$. In classical security models, all cryptography schemes considered the single-user (single-key) security, which means that there exists only a fixed key. This study focuses on the multi-user (multi-key) security. Guo et al. [2] presented a multi-key analysis for one-round TEM cipher (TEM-1) with linear tweak and key mixing in their paper. They provided known-plaintext attacks against TEM-1, utilized detecting collisions to obtain an adaptive chosen-plaintext attack against TEM-1, and left an interesting open problem that whether TEM-1 achieves security up to the birthday bound.

We present a positive response for the above problem. This study focuses on the multi-user security of the TEM cipher. Firstly, we prove that the TEM-1 is multi-user strong tweakable pseudorandom permutation (MU-STPRP) secure in the random permutation model by using the expectation method. Compared with the bounds of the multi-user security obtained by the naive hybrid argument and the pointwise proximity property, the bound directly derived by the expectation method is the best, the tightest, and closest to the single-user bound. Then, we consider the multi-user security of an ideal TBC. The ideal TBC is proven MU-STPRP secure up to very close-to-optimal birthday-bound in the ideal cipher model. Furthermore, by comparison, the bound of TEM-1 we derive is close to the bound of the ideal TBC. Finally, we extend TEM-1 to the r-round TEM cipher, illustrate some loose bounds, and analyze the security of the r-round TEM cipher.

Theorem 1 (Multi-user security of TEM-1)**.** Let H be a uniform ϵ-AXU hash function from $\mathcal{T}$ to $\{0,1\}^n$ and u be the number of users. For $\frac{1}{2^n} \leqslant \epsilon \leqslant \frac{2}{2^n}$, the MU-STPRP security of TEM-1 is

$$\begin{aligned}&\mathrm{Adv}^{\text{MU-STPRP}}_{\text{TEM-1}}(p,q)\\ &\leqslant \frac{2qp}{2^n} + \frac{2q^2(1-\frac{1}{u})}{2^n} + q\left(\frac{q}{u}-1\right)\epsilon.\end{aligned}$$

The bound $\frac{2qp}{2^n} + \frac{2q^2(1-\frac{1}{u})}{2^n} + q(\frac{q}{u}-1)\epsilon$ includes three terms. The first term $2qp/2^n$ means the probability of the collisions between queries of the users and inputs of the random permutation. It is a constant function which has nothing to do with the number of users. The second term $2q^2(1-1/u)/2^n$ means the probability of the collisions for distinct users. It is a monotone increasing function for u over a closed interval $[1,q]$. The third term $q(q/u-1)\epsilon$ means the probability of the collisions for distinct queries of the same users. It is a monotone decreasing function for $u \in [1,q]$. In other words, given enough queries, with the increase of the number of users, the number of the average queries for each user is monotonically decreasing, the collision between the users and the random permutation is a constant, the collision generated by distinct users is monotonically increasing, and the inner collision of each user gradually decreases.

From an overall perspective, our MU-STPRP bound of TEM-1 depends on the randomness of the uniform ϵ-AXU-hash function. (1) If $1/2^n \leqslant \epsilon < 2/2^n$, the MU-STPRP advantage of TEM-1 is monotonically increasing for $u \in [1,q]$. In this case, given enough queries, with the increase of the number of users, the rate of increase for the collision of distinct users is faster than the rate of decrease for the inner collision of the same users.

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

(2) If $\epsilon = 2/2^n$, the MU-STPRP advantage of TEM-1 is a constant $2q(p+q-1)/2^n$ for any $u \in [1, q]$. In this case, given enough queries, with the increase of the number of users, the rate of increase for the collision of distinct users is always equal to the rate of decrease for the inner collision of the same users.

In particular, we consider the following two extreme cases: the worst case and the average case. (1) In the worst case, an adversary makes all q queries to some single user among u users. In this case, the collision only occurs in distinct queries of the single user. Therefore, the multi-user security of TEM-1 directly degrades into the single-user security of TEM-1 which is upper bounded by $2qp/2^n + q(q-1)\epsilon$. (2) In the average case, an adversary just makes q/u queries to each user among u users. If the adversary only makes one query to each user among u users, i.e., $q = u$, then the collision only occurs in queries of the distinct users. Therefore, the multi-user security of TEM-1 is upper bounded by $2q(p+q-1)/2^n$.

By comparison, the bound of TEM-1 we derive is the best and the tightest. Let $n = 128$, $p = q = u$, and $\epsilon = 2^{-n}$. Our MU-STPRP result in Theorem 1 provides 63-bit security. While the result obtained by the naive hybrid argument just provides close-to 42-bit security, which is far way from the birthday security (64-bit), and the result obtained by point-wise proximity slightly larger than 62-bit security. Furthermore, the bound of the multi-user security we derive is very close to the single-user security (see Figure 1).

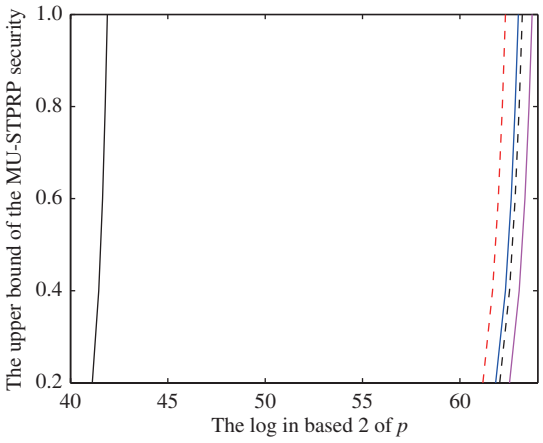

Figure 1 (Color online) Comparison of various security. From left to right: the naive bound of TEM-1 by using the hybrid argument, the bound of TEM-1 by point-wise proximity, the bound of TEM-1 that we derive in Theorem 1, the bound of the single-user security of TEM-1, and the bound of ideal TBC that we derive in Theorem 2. Let $n = 128$, $p = q = u$, and $\epsilon = 2^{-n}$, where u is the number of users.

Theorem 2 (Multi-user security of ideal TBCs)**.** Let ITBC be an ideal TBC randomly chosen from $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$, k be the size of keys, l be the size of tweaks, and u be the number of users. Let $n = k + l$, then for all adversaries $\mathcal{A}$ making at most q queries to $\widetilde{E}^{\pm}_{K_1}, \ldots, \widetilde{E}^{\pm}_{K_u}$ (resp. $\widetilde{\pi}^{\pm}_1, \ldots, \widetilde{\pi}^{\pm}_u$) and at most p queries to $\widetilde{E}^{\pm}$ under adversary-chosen keys,

$$\mathrm{Adv}^{\text{MU-STPRP}}_{\text{ITBC}}(\mathcal{A}) \leqslant \frac{u^2 + 2up}{2^{n+1}} \leqslant \frac{q^2 + 2pq}{2^{n+1}}.$$

Let $n = 128$ and $p = q = u$, an ideal TBC enjoys the MU-STPRP security and is up to close-to 64-bit security. Compared Theorem 1 with Theorem 2, the MU-STPRP security of TEM-1 is close to that of the ideal TBC (see Figure 1). For the security proof of Theorems 1 and 2, please refer to Appendixes A and B.

TEM-1 provides birthday-bound security in the multi-user setting. It's not far-fetched to consider whether we can find a better beyond-birthday-bound (BBB) in the multi-user setting for the r-round TEM cipher, where $r \geqslant 2$. Cogliati et al. [1] proved that the r-round TEM cipher achieves single-user STPRP security and provided a non-tight beyond-birthday-bound. Let r be an even integer, $r' = r/2$, and $N = 2^n$. Let n be an integer and H be a uniform ϵ-AXU hash function. Then the single-user STPRP security of the r-round TEM cipher is

$$\mathrm{Adv}^{\text{STPRP}}_{\text{TEM}[n,r,H]}(p,q) \leqslant \sqrt{2^{r'+4} q(N\epsilon q + p)^{r'}/N^{r'}}.$$

For odd $r \geqslant 3$, we have $\mathrm{Adv}^{\text{STPRP}}_{\text{TEM}[n,r,H]}(p,q) \leqslant \mathrm{Adv}^{\text{STPRP}}_{\text{TEM}[n,r-1,H]}(p,q)$.

We can evaluate the multi-user security from the single-user security. Let $\epsilon'(p,q) = \sqrt{2^{r'+4} q(N\epsilon q + p)^{r'}/N^{r'}}$. Let u be the number of users. Take an even r as an example.

Given the single-user security of the r-round TEM cipher, where $r = 2r'$, if we utilize the naive hybrid argument for lifting single-user STPRP result to the MU-STPRP security, then we would obtain an inferior bound as follows:

$$\mathrm{Adv}^{\text{MU-STPRP}}_{\text{TEM}[n,r,H]}(p,q) \leqslant u\sqrt{2^{r'+4} \frac{q(N\epsilon q + p + qr)^{r'}}{N^{r'}}}.$$

To improve the multi-user security of the r-round TEM cipher, we verify that $\epsilon'(p,q)$ is both super-additive and monotonic increasing. Therefore, we can utilize the point-wise proximity property presented by Hoang and Tessaro [3] to derive the MU-STPRP security, where $r = 2r'$. The better bound of the multi-user security for the r-round TEM cipher is presented as follows:

$$\mathrm{Adv}^{\text{MU-STPRP}}_{\text{TEM}[n,r,H]}(p,q) \leqslant 2\sqrt{2^{r'+4} \frac{q(N\epsilon q + p + qr)^{r'}}{N^{r'}}}.$$

Let $\epsilon = 2^{-n}$, then the r-round TEM cipher derived by the property of point-wise proximity enjoys the MU-STPRP security up to roughly $2^{\frac{r}{r+2}n}$ adversarial queries and it has nothing to do with the number of users. Similarity, for an odd r, the r-round TEM cipher derived by the property of point-wise proximity enjoys the MU-STPRP security up to roughly $2^{\frac{r-1}{r+1}n}$ adversarial queries.

Finally, we utilize the experimental data to analyze the security of the r-round TEM cipher in various settings and obtain the following results.

(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.

(2) 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). For detailed results of the experiment, please refer to Appendix C.

Conclusion. This study focuses on the multi-user security of the tweakable Even-Mansour cipher. Firstly, we prove that TEM-1 enjoys MU-STPRP security in the random permutation model. Compared with the multi-user security obtained by naive hybrid argument and point-wise proximity, the multi-user security directly derived by the expectation method is the best and closest to the single-user security. Then, we prove that the ideal TBC is MU-STPRP secure up to close-to-optimal birthday-bound in the ideal cipher model. By comparison, the bound of TEM-1 we derive is also very close to that of the ideal TBC. Finally, we extend TEM-1 to the r-round TEM cipher, analyze the multi-user security of the r-round TEM cipher in various settings, and call more attentions on the study of the r-round TEM cipher.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61522210, 61632013).

Supporting information Appendixes A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Cogliati B, Lampe R, Seurin Y. Tweaking Even-Mansour ciphers. In: Proceedings of the 35th Annual Cryptology Conference, Santa Barbara, 2015. 189–208
2 Guo Z Y, Wu W L, Liu R, et al. Multi-key analysis of tweakable Even-Mansour with applications to Minalpher and OPP. IACR Trans Symmetric Cryptol, 2017, 2016: 288–306
3 Hoang V T, Tessaro S. Key-alternating ciphers and key-length extension: exact bounds and multi-user security. In: Proceedings of the 36th Annual International Cryptology Conference, Santa Barbara, 2016