Hindawi
Security and Communication Networks
Volume 2020, Article ID 4180139, 6 pages
https://doi.org/10.1155/2020/4180139

Research Article

Minimizing Key Materials: The Even–Mansour Cipher Revisited and Its Application to Lightweight Authenticated Encryption

Ping Zhang[1] **and Qian Yuan**[2]

[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*

Correspondence should be addressed to Ping Zhang; zhgp@njupt.edu.cn

Received 12 December 2019; Accepted 7 February 2020; Published 10 March 2020

Guest Editor: Andrea Visconti

The Even–Mansour cipher has been widely used in block ciphers and lightweight symmetric-key ciphers because of its simple structure and strict provable security. Its research has been a hot topic in cryptography. This paper focuses on the problem to minimize the key material of the Even–Mansour cipher while its security bound remains essentially the same. We introduce four structures of the Even–Mansour cipher with a short key and derive their security by Patarin's H-coefficients technique. These four structures are proven secure up to $\widetilde{O}(2^k/\mu)$ adversarial queries, where k is the bit length of the key material and μ is the maximal multiplicity. Then, we apply them to lightweight authenticated encryption modes and prove their security up to about $\min\{b/2, c, k - \log \mu\}$-bit adversarial queries, where b is the size of the permutation and c is the capacity of the permutation. Finally, we leave it as an open problem to settle the security of the t-round iterated Even–Mansour cipher with short keys.

1. Introduction

In recent years, more and more attention has been paid to lightweight cryptography as smart home, Internet of things (IoT), smart transportation, and 5G/B5G networks are proposed. These new technologies brought convenience to our lives but have introduced a powerful security threat, such as the leakage of the private data in our smart phone. Lightweight cryptography is an effective countermeasure against the security threats in order to achieve the privacy and integrity protections of the sensitive data. Lightweight cryptography is mainly used in resource-constrained devices. The block cipher has become a very vital lightweight symmetric-key cryptography, due to its fast speed, easy implementation, and easy standardization on these devices. It is often used to implement sensitive data encryption, digital signature, message authentication, and key encapsulation schemes in the field of information security and network communication security.

The t-round iterated Even–Mansour cipher is simply described as a pure permutation-based block cipher:

$$y = P_t\left(P_{t-1}\left(\cdots\left(P_1\left(x \oplus K_1\right) \oplus K_2\right)\cdots \oplus K_t\right) \oplus K_{t+1}, \quad (1)$$

where $(K_1, K_2, \ldots, K_t, K_{t+1})$ is a sequence of n-bit round keys which are usually derived from some master key and $(P_1, P_2, \ldots, P_t)$ is a sequence of t public random permutations. This iterated Even–Mansour cipher, also known as key-alternating ciphers, is of great significance in the design of block ciphers and is also favored in the design of lightweight cryptography. The security of the iterated Even–Mansour ciphers is based on the random permutation model (RPM). In RPM, all permutations are modeled as public random permutation oracles, in other words, anyone can query these permutations and obtain the corresponding responses. The related research includes [1–9].

This paper focuses on the case $t = 1$. Even and Mansour [10] did pioneering work in 1997 and proved that it is birthday-bound secure. That is where the name "Even–Mansour cipher" comes from. The Even–Mansour cipher has some very nice properties, such as simplest structure and strict provable security. Although the research of the Even–Mansour cipher went unnoticed for years, Gold

will always shine. Fortunately, it has been a very hot topic in cryptography. In 2012, Dunkelman et al. [11] pointed out that the Even–Mansour cipher is minimal, i.e., any component (either one of the keys or the permutation) is removed; the Even–Mansour cipher becomes trivially breakable. In 2015, Cogliati et al. [12] introduced the tweakable Even–Mansour (TEM) cipher combined by the Even–Mansour cipher and a tweak, and proved its security. Meanwhile, Mouha and Luykx [13] revisited the Even–Mansour cipher and analyzed the multikey security. do Nascimento and Xexeo [14] applied the Even–Mansour cipher to the Internet of Things (IoT) environments and presented a flexible lightweight authenticated encryption mode in 2017. It follows that Cho et al. [15] presented a new family of white-box block ciphers based on the Even–Mansour cipher WEM which achieves balances between performance and security. Farshim et al. [16] analyzed the security of the Even–Mansour cipher under key-dependent messages. In 2018, we described a generalized tweakable Even–Mansour cipher and applied it to authentication and authenticated encryption modes [17].

In the lightweight devices, the storage resources are limited. Therefore, a vital issue is the minimalism and agility of the key material in the design of lightweight ciphers. In this paper, we revisit the Even–Mansour cipher and consider as problem whether we can use the least key material to achieve the same security bound. The Even–Mansour cipher is proven security up to approximately $2^{k/2}$ adversarial queries, where k is the bit-length of the key material. Can we decrease the key material and achieve the same security bound (this bound must be beyond-birthday-bound)?

We answer positively to the question in this paper. We introduce four structures of the Even–Mansour cipher with a short key and present the provable security results. More concretely, we derive their security up to $\widetilde{O}(2^k/\mu)$ adversarial queries using Patarin's H-coefficients technique, where k is the bit-length of the reducing key material and μ is the maximal multiplicity. The Even–Mansour cipher with a short key has many good advantages, such as calculating on-the-fly, avoiding the key schedule, and minimizing the key material. Therefore, it can be widely applied to resource-constrained lightweight devices. Then, we apply its four structures to lightweight authenticated encryption (AE) modes and prove their security up to about $\min\{b/2, c, k - \log\mu\}$-bit adversarial queries, where $b = r + c$ is the size of the permutation and c (resp. r) is the capacity (resp. rate) of the permutation. Finally, we leave it as an open problem to settle the security of the t-round iterated Even–Mansour cipher with short keys.

The rest of this paper is organized as follows. In Section 2, we introduce some preliminaries. In Section 3, we prove the security of the Even–Mansour cipher with a short key. Section 4 describes lightweight AE modes based on four structures of the Even–Mansour cipher with a short key. Section 5 ends up with this paper.

2. Preliminaries

Let $\{0,1\}^b$ be the set of binary strings of length b and $N = 2^b$. For two strings X and Y, let $X\|Y$ or XY be the concatenation of X and Y. Given a string X, we utilize $|X|$ to denote the length in bits of X. Given a nonempty set X, let $x \leftarrow X$ denote an element x drawing from X uniformly at random and $\#X$ be the cardinality of X. Let $\mathrm{Perm}(b)$ stand for the set of permutations on $\{0,1\}^b$. Let $\mathscr{A}^O = 1$ be an event that an adversary $\mathscr{A}$ outputs 1 after interacting with the oracle O. Here, $\mathscr{A}$ never makes a query for which the response is obviously known. Let $\Pr[\mathbf{E}]$ be the probability that the event $\mathbf{E}$ occurs.

2.1. Multiplicity. Let $\{(x_i, y_i)\}_{i=1}^N$ be a set of N evaluations of a permutation P, where $x_i = \overline{x}_i\|\widehat{x}_i$, $y_i = \overline{y}_i\|\widehat{y}_i$. We introduce the total maximal multiplicity as $\mu = \mu_{\mathrm{fwd}} + \mu_{\mathrm{bwd}}$ inspired by [18], where

$$\mu_{\mathrm{fwd}} = \max_a \#\{i = 1, \ldots, N : \overline{x}_i = a \text{ or } \widehat{x}_i = a\}, \tag{2}$$

$$\mu_{\mathrm{bwd}} = \max_a \#\{i = 1, \ldots, N : \overline{y}_i = a \text{ or } \widehat{y}_i = a\}. \tag{3}$$

2.2. H-Coefficients Technique. H-coefficients technique introduced by Patarin [19] is a very important analytical method in the symmetric-key cryptography. We briefly summarize this technique as follows. Consider an information-theoretic adversary $\mathscr{A}$, whose goal is to distinguish a real world X and an ideal world Y and denote the distinguishing advantage of $\mathscr{A}$ as

$$\mathrm{Adv}(\mathscr{A}) = \left|\Pr\left[\mathscr{A}^X = 1\right] - \Pr\left[\mathscr{A}^Y = 1\right]\right|. \tag{4}$$

Without loss of generality, we can assume that $\mathscr{A}$ is a deterministic adversary. The interaction with any of the two worlds X or Y is summarized in a transcript τ. Denote by D_X the probability distribution of transcripts when interacting with X, and similarly, D_Y the distribution of transcripts when interacting with Y. A transcript τ is attainable if $\Pr[D_Y = \tau] > 0$, meaning that it can occur during interaction with Y. Let Γ be the set of attainable transcripts. We denote Γ_1 as a set of good transcripts when interacting with X (Y). Let Γ_2 be a set of bad transcripts such that the probability to obtain any $\tau \in \Gamma_2$ is small in the ideal world $\Gamma = \Gamma_1 \cup \Gamma_2$.

Lemma 1 (H-coefficients lemma [19]). *Fix a deterministic adversary $\mathscr{A}$. Let $\Gamma = \Gamma_1 \cup \Gamma_2$ be a partition of the set of attainable transcripts. Assume that there exists ϵ_1 such that for any $\tau \in \Gamma_1$, one has*

$$\frac{\Pr[D_X = \tau]}{\Pr[D_Y = \tau]} \geq 1 - \epsilon_1, \tag{5}$$

and that there exists ϵ_2 such that

$$\Pr[D_Y \in \Gamma_2] \leq \epsilon_2. \tag{6}$$

Then, the advantage of the adversary $\mathscr{A}$ is

$$\mathrm{Adv}(\mathscr{A}) \leq \epsilon_1 + \epsilon_2. \tag{7}$$

3. The Even–Mansour Cipher with a Short Key

Fix a public permutation P: $\{0,1\}^b \longrightarrow \{0,1\}^b$ and integers r, c, and k, such that $b = r + c$ and $k \leq \min\{r, c\}$. Let

$\mathcal{K} = \{0,1\}^k$. The Even–Mansour cipher with a short key, called EM for short, is described in Figure 1. EM takes a uniform random key $K \in \{0,1\}^k$ and a plaintext $x \in \{0,1\}^b$ as inputs and outputs the ciphertext $y = \mathrm{EM}_K^P(x) \in \{0,1\}^b$. Let $\mathrm{pad}_1(K) = 0^{r-k}\|K$ and $\mathrm{pad}_2(K) = 0^{c-k}\|K$. The four structures of EM are, respectively, shown as follows:

$$\begin{aligned}
&(a):\ y = \mathrm{EM}_K^P(x) = P\left(x \oplus \mathrm{pad}_1(K)\|0^c\right) \oplus \mathrm{pad}_1(K)\|0^c,\\
&(b):\ y = \mathrm{EM}_K^P(x) = P\left(x \oplus \mathrm{pad}_1(K)\|0^c\right) \oplus 0^r\|\mathrm{pad}_2(K),\\
&(c):\ y = \mathrm{EM}_K^P(x) = P\left(x \oplus 0^r\|\mathrm{pad}_2(K)\right) \oplus 0^r\|\mathrm{pad}_2(K),\\
&(d):\ y = \mathrm{EM}_K^P(x) = P\left(x \oplus 0^r\|\mathrm{pad}_2(K)\right) \oplus \mathrm{pad}_1(K)\|0^c.
\end{aligned} \tag{8}$$

We consider the security of the Even–Mansour cipher with a short key and obtain the following theorem.

Theorem 1. *For EM_K^P with $K \in \{0,1\}^k$ and $P \leftarrow Perm(b)$, we have*

$$\mathrm{Adv}_{\mathrm{EM}}\left(q_e, q_p\right) \le \frac{\mu q_p}{2^k}. \tag{9}$$

The proof of Theorem 1 utilizes the H-coefficients technique. We consider an adversary $\mathcal{A}$ which can interact with $X = (\mathrm{EM}_K^P, P)$ in the real world or $Y = (Q, P)$ in the ideal world, where P and Q are uniform random and independent permutations and K is a (dummy) key. We assume that the adversary $\mathcal{A}$ makes at most q_e construction queries and at most q_p primitive queries. The transcripts can be expressed as this form $\tau = (\mathcal{Q}_e, \mathcal{Q}_p, K)$, where $\mathcal{Q}_e = \{(x_i, y_i)\}_{i=1}^{q_e}$ and $\mathcal{Q}_p = \left\{(u_j, v_j)\right\}_{j=1}^{q_p}$. We start by defining bad transcripts.

Definition 1. We define an attainable transcript $\tau = (\mathcal{Q}_e, \mathcal{Q}_p, K) \in \Gamma$ as bad if one of the two following conditions is fulfilled.

$\mathrm{Bad}_1 : \exists (x,y) \in \mathcal{Q}_e$ and $(u,v) \in \mathcal{Q}_p$, such that

$$\begin{aligned}
&(a)\,\&\,(b):\ x \oplus u = \mathrm{pad}_1(K)\|0^c,\\
&(c)\,\&\,(d):\ x \oplus u = 0^r\|\mathrm{pad}_2(K),
\end{aligned} \tag{10}$$

$\mathrm{Bad}_2 : \exists (x,y) \in \mathcal{Q}_e$ and $(u,v) \in \mathcal{Q}_p$, such that

$$\begin{aligned}
&(a)\,\&\,(d):\ y \oplus v = \mathrm{pad}_1(K)\|0^c,\\
&(b)\,\&\,(c):\ y \oplus v = 0^r\|\mathrm{pad}_2(K).
\end{aligned} \tag{11}$$

Otherwise we say that τ is good. We denote Γ_{good}, resp. Γ_{bad} the set of good, resp. bad transcripts, and $\Gamma = \Gamma_{\mathrm{good}} \sqcup \Gamma_{\mathrm{bad}}$.

In the real world X, a bad transcript implies that two invocations to P exist with the same input: one directly from querying the primitive oracle P and another one indirectly from querying the construction oracle EM_K^P, while all tuples in $(\mathcal{Q}_e, \mathcal{Q}_p)$ uniquely determine an input-output pair of P for a good transcript. In the ideal world Y, the abovementioned result is clearly established for a bad transcript, while it is not for a good transcript.

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

Lemma 2

$$\Pr\left(D_Y \in \Gamma_{\mathrm{bad}}\right) \le \frac{\mu q_p}{2^k}. \tag{12}$$

Proof. In the ideal world Y, $(\mathcal{Q}_e, \mathcal{Q}_p)$ is an attainable transcript with a dummy uniform random key $K \in \{0,1\}^k$.

Here, we assume that an adversary $\mathcal{A}$ makes at most q_e construction queries and at most q_p primitive queries. For each $(x,y) \in \mathcal{Q}_e$ and each $(u,v) \in \mathcal{Q}_p$, we obtain at most μ_{fwd} (resp. μ_{bwd}) tuples (x,y) such that $\overline{x} = \overline{u}$ for structures (a) and (b) or $\widehat{x} = \widehat{u}$ for structures (c) and (d) (resp. $\overline{y} = \overline{v}$ for structures (a) and (d) or $\widehat{y} = \widehat{v}$ for structures (b) and (c)) from the property of multiplicity.

It follows that $\Pr(\mathrm{Bad}_1) \le \mu_{\mathrm{fwd}} q_p / 2^k$ and $\Pr(\mathrm{Bad}_2) \le \mu_{\mathrm{bwd}} q_p / 2^k$. Hence, the probability of bad transcripts in the ideal world Y is at most $\mu q_p / 2^k$, where $\mu = \mu_{\mathrm{fwd}} + \mu_{\mathrm{bwd}}$.

We then analyze good transcripts and lower bound the ratio $(\Pr[D_X = \tau])/\Pr[D_Y = \tau]$. □

Lemma 3. *For any good transcript τ, one has*

$$\frac{\Pr\left[D_X = \tau\right]}{\Pr\left[D_Y = \tau\right]} \ge 1. \tag{13}$$

Proof. Consider a good transcript $\tau \in \Gamma_{\mathrm{good}}$. Let Ω_X be a nonempty set of all possible oracles in the real world X and Ω_Y be a nonempty set of all possible oracles in the ideal world Y. Therefore, the cardinalities of sets Ω_X and Ω_Y are, respectively, $\#\Omega_X = (2^b)! \cdot 2^k$ and $\#\Omega_Y = (2^b!)^2 \cdot 2^k$. Let $\mathrm{comp}_X(\tau) \subseteq \Omega_X$ and $\mathrm{comp}_Y(\tau) \subseteq \Omega_Y$ be the two sets of oracles compatible with transcript τ. The probabilities appearing in Lemma 1 can be evaluated as follows:

$$\Pr\left(D_X = \tau\right) = \frac{\#\mathrm{comp}_X(\tau)}{\#\Omega_X}, \tag{14}$$

$$\Pr\left(D_Y = \tau\right) = \frac{\#\mathrm{comp}_Y(\tau)}{\#\Omega_Y}. \tag{15}$$

First, we calculate $\#\mathrm{comp}_X(\tau)$. As $\tau \in \Gamma_{\mathrm{good}}$ consists of $q_e + q_p$ query tuples and any query tuple in τ fixes exactly one input-output pair of the underlying permutation oracle, the number of possible oracles in the real world X equals $(2^b - q_e - q_p)!$.

Second, we calculate $\#\mathrm{comp}_Y(\tau)$. The number of possible oracles in the ideal world Y equals $(2^b - q_p)!(2^b - q_e)!$, as P and Q are uniform random and independent permutations.

It follows that

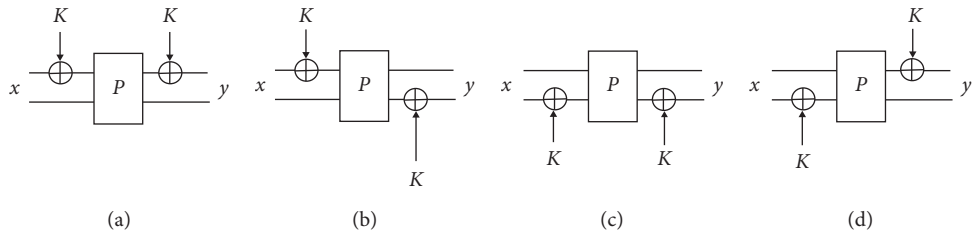

Figure 1: Four structures of EM.

$$\Pr(D_X = \tau) = \frac{\#\mathrm{comp}_X(\tau)}{\#\Omega_X} = \frac{(2^b - q_e - q_p)!}{(2^b!)\cdot 2^k} = \frac{(2^b - q_e - q_p)!2^b!}{(2^b!)^2 \cdot 2^k} \geq \frac{(2^b - q_p)!(2^b - q_e)!}{(2^b!)^2 \cdot 2^k} = \Pr(D_Y = \tau). \quad (16)$$

Therefore, we have $(\Pr[D_X = \tau]/\Pr[D_Y = \tau]) \geq 1$.

Combining Lemmas 1–3, we can obtain the result of Theorem 1. □

4. Application to Lightweight Authenticated Encryption

With the rises of the smart home, IoT, and 5G/B5G networks, lightweight authenticated encryption (AE) modes are attracting more and more attentions [20–22]. A lightweight AE mode is a lightweight symmetric-key cipher which supports the services of privacy and authenticity of the sensitive data in the devices.

The Even–Mansour cipher with a short key can be directly applied to a lightweight AE mode, which is shown in Figure 2. It consists of an encryption algorithm E and a decryption algorithm D. The encryption algorithm E takes a plaintext M and a key K as inputs and returns a ciphertext C and an authentication tag T, i.e., $C\|T = \mathrm{EM}_K^P(M\|0^c) = E(K, M)$. The decryption algorithm D takes a key K, a ciphertext C, and an authentication tag T as inputs and returns a plaintext M or a reject symbol $\perp$, i.e., $M/\perp = D(K, C, T)$. If the last c-bit of the EM decryption is 0, then the decryption algorithm D returns M. Otherwise, the decryption algorithm D returns $\perp$.

Let $\Pi = (E, D)$ stand for our lightweight AE modes. We introduce the AE-security model as follows.

Definition 2. (AE security). Let P be a public random permutation. Let $\Pi = (E, D)$ be a P-based AE scheme. Let $\mathscr{A}$ be an adversary which interacts with $X = (E, D, P^{\pm})$ in the real world or $Y = (\$, \perp, P^{\pm})$ in the ideal world. Let $q, p > 0$. Then, the AE-security of $\Pi = (E, D)$ is defined as follows:

$$\mathrm{Adv}_{\Pi}^{ae}(\mathscr{A}) = \left|\Pr\left[\mathscr{A}^{E,D,P^{\pm}} = 1\right] - \Pr\left[\mathscr{A}^{\$,\perp,P^{\pm}} = 1\right]\right|, \quad \mathrm{Adv}_{\Pi}^{ae}(q, p) = \max_{\mathscr{A}} \mathrm{Adv}_{\Pi}^{ae}(\mathscr{A}), \quad (17)$$

where q is the number of queries to the encryption oracle E or the decryption oracle D, p is the number of queries to the random permutation P or its inverse P^{-1}, is a random function which always returns a fresh and random response for each query, and $\perp$ is a symbol which stands for the failure of the decryption oracles.

Theorem 2. *Let $P \leftarrow Perm(b)$ and $b = r + c$. Then,*

$$\mathrm{Adv}_{\Pi}^{ae}(q, p) \leq \frac{\mu p}{2^k} + \frac{q^2}{2^b} + \frac{q}{2^c}. \quad (18)$$

Proof Sketch. Let $\mathscr{A}$ be an adversary with access to the encryption oracle E, the decryption oracle D, and the random permutation P or its inverse P^{-1}. Π can be represented as an EM scheme. We replace the EM modular structure to the random permutation Q. According to Theorem 1, we have

$$\begin{aligned}\mathrm{Adv}_{\Pi}^{ae}(\mathscr{A}) &= |Pr\left[\mathscr{A}^{E,D,P^{\pm}} = 1\right] - \Pr\left[\mathscr{A}^{\$,\perp,P^{\pm}} = 1\right]| \\ &\leq \left|\Pr\left[\mathscr{A}^{E,D,P^{\pm}} = 1\right] - \Pr\left[\mathscr{A}^{Q,Q^{-1},P^{\pm}} = 1\right]\right| \\ &\quad + \left|\Pr\left[\mathscr{A}^{Q,Q^{-1},P^{\pm}} = 1\right] - \Pr\left[\mathscr{A}^{\$,\perp,P^{\pm}} = 1\right]\right| \\ &= \frac{\mu p}{2^k} + \left|\Pr\left[\mathscr{A}^{Q,Q^{-1},P^{\pm}} = 1\right] - \Pr\left[\mathscr{A}^{\$,\perp,P^{\pm}} = 1\right]\right|.\end{aligned} \quad (19)$$

It follows that

$$\begin{aligned}&\left|\Pr\left[\mathscr{A}^{Q,Q^{-1},P^{\pm}} = 1\right] - \Pr\left[\mathscr{A}^{\$,\perp,P^{\pm}} = 1\right]\right| \\ &\leq \left|\Pr\left[\mathscr{A}^{Q,Q^{-1},P^{\pm}} = 1\right] - \Pr\left[\mathscr{A}^{Q,\perp,P^{\pm}} = 1\right]\right| \\ &\quad + \left|\Pr\left[\mathscr{A}^{Q,\perp,P^{\pm}} = 1\right] - \Pr\left[\mathscr{A}^{\$,\perp,P^{\pm}} = 1\right]\right| \\ &\leq \frac{q}{2^c} + \frac{q^2}{2^b},\end{aligned} \quad (20)$$

where $q^2/2^b$ obtained by the PRP-PRF Switch Lemma [23] and $q/2^c$ is from the fact that the successful probability of the adversary is $1/2^c$ for each forgery attempt.

Combining equations (19) and (20), it is easy to draw the result of Theorem 2.

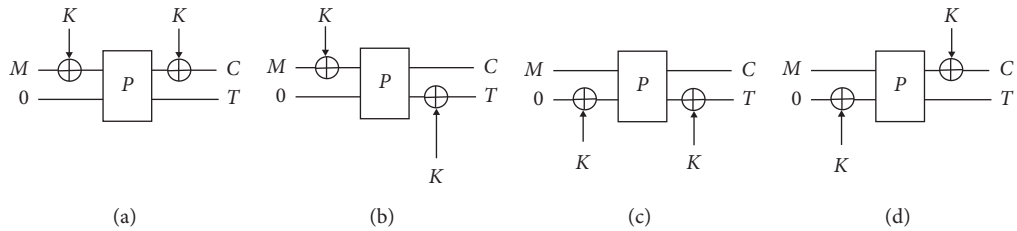

Figure 2: Lightweight authenticated encryption modes.

According to Theorem 2, we can find that these lightweight AE modes ensure about $\min\{b/2, c, k - \log \mu\}$-bit AE-security.

5. Conclusions

The key material is crucial for the secure implementation of cryptographic schemes. Most of devices widely used in smart home, smart transportation, and Internet of Things (IoT) environments are resource constrained. Therefore, in the design of lightweight ciphers, a vital issue is the minimalism and agility of the key material.

In this paper, we revisit the Even–Mansour cipher and discuss this problem whether we can use the least key material to achieve the same (even beyond conventional) security bound in the Even–Mansour cipher. We introduce four structures of the Even–Mansour cipher with a short key and derive security up to $\widetilde{O}(2^k/\mu)$ adversarial queries, where k is the bits of the key material and μ is the maximal multiplicity, using Patarin's H-coefficients technique. Then, we apply them to lightweight authenticated encryption modes and prove their security up to about $\min\{b/2, c, k - \log \mu\}$-bit adversarial queries, where $b = r + c$ is the size of the permutation and c is the capacity of the permutation. Finally, we leave it as an open problem to settle the security of the t-round iterated Even–Mansour cipher with short keys. The Even–Mansour cipher with a short key is proven $(k - \log \mu)$-bit security. It is natural to consider whether our result can be generalized to the t-round iterated Even–Mansour cipher. But the situation of the t-round iterated Even–Mansour cipher with short keys is more complicated. Therefore, it is regarded as an open problem to attract scholars to discuss and analyze it in detail. The Even–Mansour cipher with a short key has many good advantages, such as calculating on-the-fly, avoiding the key schedule, and minimizing the area of the hardware implementation and the key material. Therefore, it can be widely applied to the data security of smart home, Internet of Things, and some lightweight devices.

Data Availability

The data used to support the findings of the study are available within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Research Fund of International Young Scientists (Grant no. 61902195), Natural Science Fund for Colleges and Universities in Jiangsu Province (General Program, Grant no. 19KJB520045), and NUPTSF (Grant no. NY219131).

References

[1] E. Andreeva, A. Bogdanov, Y. Dodis, B. Mennink, and J. P. Steinberger, "On the indifferentiability of key-alternating ciphers," in *Advances in Cryptology–CRYPTO 2013, Lecture Notes in Computer Science*, R. Canetti and J. A. Garay, Eds., vol. 8042, pp. 531–550, Springer, Berlin, Germany, 2013.

[2] A. Bogdanov, L. R. Knudsen, G. Leander, FX. Standaert, J. Steinberger, and E. Tischhauser, "Key-alternating ciphers in a provable setting: encryption using a small number of public permutations," in *Advances in Cryptology–EUROCRYPT 2012, Lecture Notes in Computer Science*, D. Pointcheval and T. Johansson, Eds., vol. 7237, pp. 45–62, Springer, Berlin, Germany, 2012.

[3] S. Chen, R. Lampe, J. Lee, Y. Seurin, and J. Steinberger, "Minimizing the two-round Even-Mansour cipher," *Journal of Cryptology*, vol. 31, no. 4, pp. 1064–1119, 2018.

[4] S. Chen and J. Steinberger, "Tight security bounds for key-alternating ciphers," in *Advances in Cryptology–EUROCRYPT 2014, Lecture Notes in Computer Science*, P. Q. Nguyen and E. Oswald, Eds., vol. 8441, pp. 327–350, Springer, Berlin, Germany, 2014.

[5] B. Cogliati and Y. Seurin, "On the provable security of the iterated Even-Mansour cipher against related-key and chosen-key attacks," in *Advances in Cryptology–EUROCRYPT 2015, Lecture Notes in Computer Science*, E. Oswald and M. Fischlin, Eds., vol. 9056, pp. 584–613, Springer, Berlin, Germany, 2015.

[6] P. Farshim and G. Procter, "The related-key security of iterated Even-Mansour ciphers," in *Fast Software Encryption–FSE 2015, Lecture Notes in Computer Science*, G. Leander, Ed., vol. 9054, pp. 342–363, Springer, Berlin, Germany, 2015.

[7] A. Hosoyamada and K. Aoki, "On quantum related-key attacks on iterated Even-Mansour ciphers," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E102.A, no. 1, pp. 27–34, 2019.

[8] T. Isobe and K. Shibutani, "Meet-in-the-middle key recovery attacks on a single-key two-round Even-Mansour cipher," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E102.A, no. 1, pp. 17–26, 2019.

[9] R. Lampe, J. Patarin, and Y. Seurin, "An asymptotically tight security analysis of the iterated Even-Mansour cipher," in *Advances in Cryptology–ASIACRYPT 2012, Lecture Notes in*

Computer Science, X. Wang and K. Sako, Eds., vol. 7658, pp. 278–295, Springer, Berlin, Germany, 2012.

[10] S. Even and Y. Mansour, "A construction of a cipher from a single pseudorandom permutation," *Journal of Cryptology*, vol. 10, no. 3, pp. 151–161, 1997.

[11] O. Dunkelman, N. Keller, and A. Shamir, "Minimalism in cryptography: the Even-Mansour scheme revisited," in *Advances in Cryptology–EUROCRYPT 2012, Lecture Notes in Computer Science*, D. Pointcheval and T. Johansson, Eds., vol. 7237, pp. 336–354, Springer, Berlin, Germany, 2012.

[12] B. Cogliati, R. Lampe, and Y. Seurin, "Tweaking even-mansour ciphers," in *Advances in Cryptology–CRYPTO 2015, Lecture Notes in Computer Science*, R. Gennaro and M. Robshaw, Eds., vol. 9215, pp. 189–208, Springer, Berlin, Germany, 2015.

[13] N. Mouha and A. Luykx, "Multi-key security: the Even-Mansour construction revisited," in *Advances in Cryptology–CRYPTO 2015, Lecture Notes in Computer Science*, R. Gennaro and M. Robshaw, Eds., vol. 9215, pp. 209–223, Springer, Berlin, Germany, 2015.

[14] E. M. do Nascimento and J. A. M. Xexeo, "A flexible authenticated lightweight cipher using Even-Mansour construction," in *Proceedings of the IEEE International Conference on Communications–ICC 2017*, pp. 1–6, IEEE, Paris, France, May 2017.

[15] J. Cho, K. Y. Choi, I. Dinur et al., "WEM: a new family of white-box block ciphers based on the Even-Mansour construction," in *Cryptographers' Track at the RSA Conference–CT-RSA 2017, Lecture Notes in Computer Science*, H. Handschuh, Ed., vol. 10159, pp. 293–308, Springer, Berlin, Germany, 2017.

[16] P. Farshim, L. Khati, and D. Vergnaud, "Security of Even-Mansour ciphers under key-dependent messages," *The IACR Transactions on Symmetric Cryptology*, vol. 2017, no. 2, pp. 84–104, 2017.

[17] P. Zhang and H.-G. Hu, "Generalized tweakable Even-Mansour cipher and its applications," *Journal of Computer Science and Technology*, vol. 33, no. 6, pp. 1261–1277, 2018.

[18] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Sponge-based pseudo-random number generators," in *Cryptographic Hardware and Embedded Systems–CHES 2010, Lecture Notes in Computer Science*, S. Mangard and FX. Standaert, Eds., vol. 6225, pp. 33–47, Springer, Berlin, Germany, 2010.

[19] J. Patarin, "The "coefficients H" technique," in *Selected Areas in Cryptography–SAC 2008, Lecture Notes in Computer Science*, R. M. Avanzi, L. Keliher, and F. Sica, Eds., vol. 5381, pp. 328–345, Springer, Berlin, Germany, 2008.

[20] A. Chakraborti, N. Datta, M. Nandi, and K. Yasuda, "Beetle family of lightweight and secure authenticated encryption ciphers," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2018, no. 2, pp. 218–241, 2018.

[21] G. Hatzivasilis, G. Floros, I. Papaefstathiou, and C. Manifavas, "Lightweight authenticated encryption for embedded on-chip systems," *Information Security Journal: A Global Perspective*, vol. 25, no. 4–6, pp. 151–161, 2016.

[22] Y. Sasaki and K. Yasuda, "Optimizing online permutation-based AE schemes for lightweight applications," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E102.A, no. 1, pp. 35–47, 2019.

[23] M. Bellare and P. Rogaway, "The security of triple encryption and a framework for code-based game-playing proofs," in *Advances in Cryptology–EUROCRYPT 2006, Lecture Notes in Computer Science*, S. Vaudenay, Ed., vol. 4004, pp. 409–426, Springer, Berlin, Germany, 2006.