Multi-Key Security: The Even-Mansour Construction Revisited

Nicky Mouha[1,2] and Atul Luykx[1]

[1] Dept. Electrical Engineering-ESAT/COSIC, KU Leuven, Leuven and iMinds, Ghent, Belgium.
[2] Project-team SECRET, Inria, France.
Firstname.Lastname@esat.kuleuven.be

Abstract. At ASIACRYPT 1991, Even and Mansour introduced a block cipher construction based on a single permutation. Their construction has since been lauded for its simplicity, yet also criticized for not providing the same security as other block ciphers against generic attacks. In this paper, we prove that if a small number of plaintexts are encrypted under multiple independent keys, the Even-Mansour construction surprisingly offers similar security as an ideal block cipher with the same block and key size. Note that this *multi-key setting* is of high practical relevance, as real-world implementations often allow frequent rekeying. We hope that the results in this paper will further encourage the use of the Even-Mansour construction, especially when the secure and efficient implementation of a key schedule would result in a significant overhead.

Keywords: Even-Mansour, multi-key setting, broadcast attack, related-key setting.

1 Introduction

Modern block cipher design is based on the concept of iterating a round function [42]. This round function typically consists of a subkey addition followed by an unkeyed invertible function. All commonly-used block ciphers, including the DES [44] and AES [21] standards, follow this design strategy.

As such, the design of an iterated block cipher consists of two parts: the design of a round function, and a key schedule to generate the subkeys for every round. Although round function design seems to be a relatively well-understood problem, this is much less the case for the key schedule. For example, Rijmen and Daemen already stated in the AES design book that: "*There is no consensus on the criteria that a key schedule must satisfy* [21, p. 77]. This fact has been repeated many times since, for example in the SHA-3 finalist Grøstl design document [30, p. 5]. In particular, there seems to be no consensus on whether a "strong" or a "simple" key schedule is required, a choice which appears to depend on the application.

An argument for a "simple" key schedule is that keys should be chosen uniformly at random from the entire key space anyway, in order to avoid a speed-up

of brute-force attacks due to low key entropy. As a result, attacks based on weak keys [23] and known keys [40] are no longer applicable. Similarly, when multiple keys are used, they should be chosen independently, in order to avoid that the compromise of one key may help to recover other keys. This avoids attacks based on related keys [7–9].

Proponents of a "strong" key schedule point out that in practice, keys may not always be chosen independently from a uniformly random distribution. The cause of this could be a weak protocol, a programming error or an insecure implementation.

Complexity, however, always comes at a cost. It makes cryptosystems more difficult to design, to implement and to analyze. Hence, we argue for a block cipher with a simple key schedule, combined with the use of a secure key derivation function (KDF) [18] for secret-key applications.

Although the use of a KDF avoids attacks on weak keys, known keys and related keys, it cannot prevent multi-key attacks [10, 12, 22, 36]: a plaintext may be encrypted under multiple independent keys. Often overlooked by block cipher designers, multi-key attacks are highly relevant in practice (cf. Sect. 2).

This leads us to the following open problem, formulated by Daemen and Rijmen in 2012 [22]. In their paper, they point out: "A scenario where the adversary can query the block cipher under related keys, or even multiple keys, inevitably leads to security erosion". Paraphrased, they ask whether in a multi-key setting: "Can we design a secure block cipher with a lighter key schedule and higher key agility if related-key security is not required?"

In this paper, we give a positive answer to their question. Surprisingly, one of the simplest block ciphers, the single-key Even-Mansour construction[3] [24,27,28], shown in Fig. 1, offers similar security as an ideal block cipher when a small number of plaintexts can be queried under many keys.

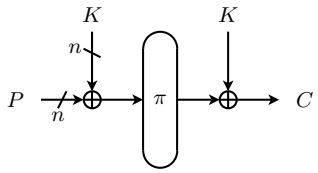

Fig. 1. The Even-Mansour construction.

Outline. The single-key, related-key and multi-key attack settings are discussed in Sect. 2, from a theoretical as well as a practical perspective. In Sect. 3, we prove tight bounds for the security of an Even-Mansour block cipher and of an

[3] Throughout this paper, we will always refer to the single-key variant of the Even-Mansour construction, that is, using only a single n-bit key K.

ideal block cipher in the multi-key setting. The relevance of our observations for the security and efficiency of block cipher implementations is discussed in Sect. 4. We conclude the paper in Sect. 5.

2 Attack Settings

2.1 Three Attack Settings

Single-key setting. One key K is chosen uniformly at random from the key space in the *single-key setting*, also referred to as the *fixed-key setting*. The adversary can then make encryption and decryption queries to block cipher E, all under the same key K.

Related-key setting. In the *related-key setting*, the adversary can perform encryption and decryption queries to block cipher E under keys K_i. Each key i satisfies the relationship $K_i = \Phi_i(K)$, where K is secret, but the functions Φ_i are chosen by the adversary. To avoid that not every block cipher E is vulnerable to a related-key attack, restrictions are necessary on the functions Φ_i as explained in [7].

Security against related-key attacks is often considered in the design of a block cipher. For example, it was a stated design goal for the AES block cipher [21], although it was recently shown that AES is not secure against related-key attacks [13, 14].

Furthermore, it should be noted that certain commonly-used algorithms, including DES and Triple-DES, are trivially insecure against related-key attacks. For DES [44] and Triple-DES [4], this is an immediate result of its complementation property [34]: $\overline{E_K} = E_{\overline{K}}(\overline{P})$, where $\overline{x}$ represents the bitwise complement of x.

It is difficult to say whether related-key security should be a requirement, as this depends on the protocol in which the cryptosystem is used. Nevertheless, it seems fair to point out that protocol designers should not assume related-key security, given that several commonly-used designs are (sometimes trivially) insecure in this setting.

Multi-key setting. In the *multi-key setting*, the adversary can query encryption and decryption queries under keys K_i, where all K_i are independently chosen uniformly at random. The multi-key setting can be seen as a generalization of the *multi-user setting* of Chatterjee et al. [17], where encryption queries of only one plaintext P are allowed under keys K_i.[4] This multi-user setting is then again a

[4] In the model of Chatterjee et al. [17], an adversary can also *corrupt* any user of its choosing, meaning that their key is given to the adversary. The goal of the adversary is then to win the game for any uncorrupted user. Although it is straightforward to take this refinement into account, we decided not to do this for the clarity of our exposition.

further generalization of the *broadcast setting* of Mantin and Shamir [43], where the plaintext P is unknown to the attacker.

Every attack in the broadcast setting also leads to an attack in the multi-user setting, and every multi-user attack is also a multi-key attack. We will therefore use the multi-key setting throughout this paper, in order to evaluate the security against the most powerful adversaries.

2.2 Practical Relevance of the Multi-Key Setting

The terms "broadcast" and "multi-user" imply a setting where one message is sent to many users, encrypted under independent keys. Note, however, that this setting does not actually require a large amount of users, but also applies to one user that rekeys frequently.

Frequent rekeying is often a result of the common implementation practice to use *session keys*. As explained in [46, § 12.2.2], session keys limit the available ciphertext under the same key for cryptanalytic attacks, and limit the exposure in case a session key is compromised.

Furthermore, rekeying is necessary in certain scenarios in order to avoid cryptanalytical attacks or to comply with existing standards. It should be noted that several cryptanalytical attacks have a higher success probability when more plaintext-ciphertext pairs under a specific key are available [6].

For example, NIST limits the amount of plaintext that can be processed under the same key to 2^{32} blocks (32 GB) for three-key Triple-DES, and to 2^{20} blocks (16 MB) for two-key Triple-DES [4]. In the case of MAC functions, NIST not only recommends to limit the number of message blocks under the same key, but also to limit the number of MAC failures before rekeying is required [25,26]. In the case of TLS, rekeying is required after only one MAC failure [32].

AlFardan et al. [2] showed that it is a realistic attack vector in the case of TLS to obtain the encryption of one secret (a cookie or password) under multiple independent keys. They explained that this can be done either by using JavaScript malware to generate multiple sessions, or by causing the session to be terminated, after which some applications automatically reconnect and retransmit the cookie or password. As shown by Paterson et al. [49], the same attack setting also applies to WPA-TKIP because of its use of per-packet keys.

2.3 Security in the Multi-Key Setting

As noted by Biham [10, 11], there exists a faster generic key-recovery attack on any block cipher in the multi-key setting compared to the single-key setting. This can be seen as follows. To keep our explanation simple, let us assume in this section that key size k equals the block size n.

In the single-key setting, an adversary with $D = 1$ plaintext-ciphertext pair will need on average $T = 2^{k-1}$ encryptions to recover the key by exhaustive search with a success probability of about 50%. More plaintext-ciphertext pairs will increase the success probability of the attack, as probability decreases that

a random key will be found instead of the correct key, but will not reduce the time complexity of the attack.

Recovering one key can be done with a lower time complexity in the multi-key setting. To see this, let an attacker have D encryptions

$$E_{K_1}(P), E_{K_2}(P), \ldots, E_{K_D}(P) \tag{1}$$

of the same plaintext P under multiple independent keys $K_1, K_2, \ldots, K_D$. Then, after on average $T = 2^{k-1}/D$ encryptions of the plaintext P, one of the keys $K_1, K_2, \ldots, K_D$ will be recovered with a success probability of about 50%.

Besides this observation, Biham also remarked in [10, 11] that key collisions become likely in this multi-key setting after about $D = 2^{k/2}$ plaintext-ciphertext pairs. Consequently, the key size k should be chosen to be sufficiently by design to avoid key collision attacks.

In Sect. 3, we will prove that the Even-Mansour construction has similar security to an ideal block cipher in the multi-key setting, assuming the number of plaintexts queried per key is small. Or put differently, when multi-key attacks with a small amount of plaintext per key are taken into account, there is little advantage in choosing a block cipher with a more complicated key schedule than the Even-Mansour construction.

2.4 Related Work

The time-memory tradeoff of Hellman [35] is not a concern for block ciphers with a reasonably long key size, because its precomputation time is the same as that of exhaustive key search. This is different from the time-memory-data tradeoffs for stream ciphers of Babbage-Golić [3,31] and Biryukov-Shamir [15], where the time complexity can be far below exhaustive search.

As shown by Hong and Sarkar [36], and independently by Birykov [12], the stream cipher time-memory-data tradeoffs can be applied to the block cipher setting as well, assuming that a plaintext is encrypted under multiple keys. Their work generalizes the findings of Biham that we presented in Sect. 1.

Chatterjee, Koblitz, Menezes and Sarkar critiqued the security proofs of symmetric-key encryption and authentication modes [17, 41, 45], pointing out that security is often reduced when a multi-user setting is considered.

Their findings inspired Fouque et al. [29] to look at collision search algorithms in the multi-user setting. One of their results is the first analysis of the Even-Mansour construction in the multi-user setting. We will use an entirely different approach in this paper, by considering information-theoretic adversaries that are only limited by the number of queries to the Even-Mansour block cipher and to the underlying permutation. As we will show, the attack by Fouque et al. reaches the security bound that we will prove for the Even-Mansour construction in the multi-key setting.

Note that the multi-user setting is not only relevant for symmetric-key cryptography, but also for public-key cryptography. For a theoretical treatment of public-key encryption in the multi-user setting, we refer to Bellare et al. [5].

3 Security Proofs in the Multi-Key Setting

Block cipher security in the multi-key setting is formalized with a distinguisher comparing two worlds, one in which the distinguisher is given access to a block cipher instantiated with ℓ keys, and one in which it is given access to ℓ independent permutations. Our focus is on constructions in the ideal model, meaning they make use of an ideal primitive.

Definition 1. *An ideal primitive is a uniformly distributed random variable over a set of functions F.*

These primitives model basic components from which cryptographic algorithms are constructed. In line with Kerckhoffs's principle, ideal primitives are public and can be accessed by adversaries in security definitions. The adversaries themselves are information-theoretic and are only bounded in the number of queries they make to each oracle.

Let $\mathsf{perm}(n)$ denote the set of all permutations on n bits, and $\mathsf{block}(k, n)$ denote the set of all block ciphers with k-bit key and n-bit block size. Let ℓ denote 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 $1 \leq i \leq \ell$.

Definition 2 (Multi-Key Security). *Let Π be a primitive and E^{Π} a random variable over $\mathsf{block}(k, n)$. Given an adversary $\mathcal{A}$, the multi-key advantage of D with respect to ℓ keys is*

$$\mathbf{Adv}_{E}^{\mathsf{mk}}(\mathcal{A}) = \left| \Pr\left(A^{E^{\Pi}_{K_1}, E^{\Pi}_{K_2}, \ldots, E^{\Pi}_{K_\ell}, \Pi} \to 1\right) - \Pr\left(A^{p_1, p_2, \ldots, p_\ell, \Pi} \to 1\right) \right| \quad , \tag{2}$$

where the keys $K_1, \ldots, K_\ell$ are independently and uniformly drawn from $\{0,1\}^k$, and $p_1, \ldots, p_\ell$ are independently and uniformly drawn from $\mathsf{perm}(n)$. The adversary $\mathcal{A}$ has access to both forward and inverse oracles.

In the case of the Even-Mansour block cipher, the primitive Π is a permutation, whereas for an ideal block cipher, the primitive Π is the block cipher itself.

Theorem 1 (Even-Mansour Multi-Key Security). *Let* EM *be the Even-Mansour block cipher $E_K(P) = \pi(P \oplus K) \oplus K$, then for all $\mathcal{A}$ making at most D queries to $E_{K_1}, \ldots, E_{K_\ell}$ (resp. $p_1, \ldots, p_\ell$) or their inverses and at most T queries to π or π^{-1},*

$$\mathbf{Adv}_{\mathrm{EM}}^{\mathsf{mk}}(\mathcal{A}) \leq \frac{D^2 + 2DT}{2^n} \quad . \tag{3}$$

Our proof is similar to the security proof of the MAC function Chaskey [47]. The proof uses Patarin's H-coefficient technique [48]. For a detailed explanation of this technique, we refer to Chen and Steinberger [19]. The proof can be seen as a generalization of the security analysis of the Even-Mansour block cipher [27,28].

Proof. As shown in Fig. 2, we consider an adversary $\mathcal{A}$ that has bidirectional access to $\ell+1$ oracles $(\mathcal{O}_1, \ldots, \mathcal{O}_{\ell+1})$. In the real world, these are $(E_{K_1}, \ldots, E_{K_\ell}, \pi)$

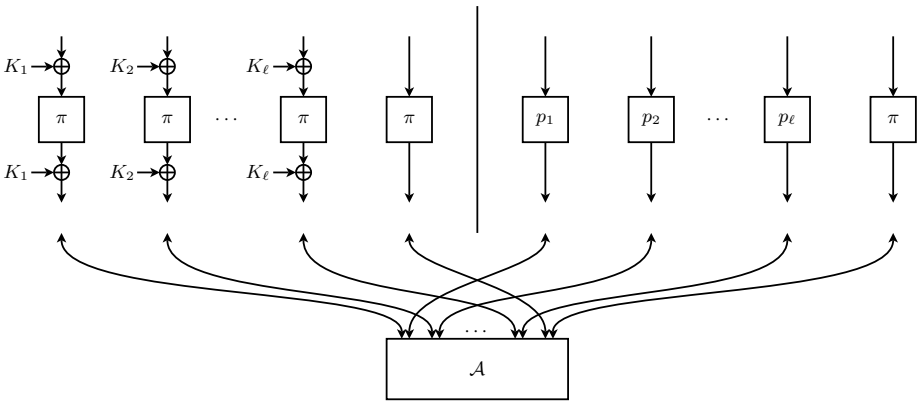

Fig. 2. An Even-Mansour block cipher $E_K(P) = \pi(P \oplus K) \oplus K$ in the multi-key setting. Although only one direction is shown, inverse oracles can be accessed as well. The number of queries by the adversary $\mathcal{A}$ to any of the first ℓ oracles is denoted by D, the number of queries to the last oracle by T.

(where $E_K(P) = \pi(P \oplus K) \oplus K$) with $K_i \xleftarrow{\$} \{0,1\}^n$ for $i = 1, \ldots, \ell$, $\pi \xleftarrow{\$} \mathsf{perm}(n)$, and in the ideal world these are $(p_1, \ldots, p_\ell, \pi) \xleftarrow{\$} \mathsf{perm}(n)^{\ell+1}$. Without loss of generality we assume that $\mathcal{A}$ is deterministic. It makes D_i queries to oracle $\mathcal{O}_i$ for $i = 1, \ldots, \ell$, and T queries to $\mathcal{O}_{\ell+1}$. Let $D = \sum_{i=1}^{\ell} D_i$. To be overly generous to the adversary $\mathcal{A}$, after it has made all of its $D + T$ queries, but before it outputs its decision, we will reveal the keys $K_1, \ldots, K_\ell$ (in the real world) or randomly generated dummy keys $K_1, \ldots, K_\ell$ (in the ideal world).

The interaction of $\mathcal{A}$ with the oracles can be summarized by a transcript $\tau = (K_1, \ldots, K_\ell, \tau_1, \ldots, \tau_{\ell+1})$. Here, the directionless list of queries to $\mathcal{O}_j$ for $i = 1, \ldots, \ell$ is denoted by $\tau_i = \{(P_i^{(1)}, C_i^{(1)}), \ldots, (P_i^{(D_i)}, C_j^{(D_i)})\}$, and to $\mathcal{O}_{\ell+1}$ by $\tau_{\ell+1} = \{(x^{(1)}, y^{(1)}), \ldots, (x^{(T)}, y^{(T)})\}$. We assume the adversary never makes duplicate queries, so that $P_i^{(j)} \neq P_i^{(j')}$, $C_i^{(j)} \neq C_i^{(j')}$, $x^{(j)} \neq x^{(j')}$, and $y^{(j)} \neq y^{(j')}$ for all i, j, j' where $j \neq j'$.

Given the fixed deterministic adversary $\mathcal{A}$, we denote the probability distribution of transcripts in the real world by X, and in the ideal world by Y. We say that a transcript τ is attainable if it can be obtained from interacting with $(p_1, \ldots, p_\ell, \pi)$, hence if $\Pr(Y = \tau) > 0$. According to the H-coefficient technique, we have (see [19] for a proof):

Lemma 1 (H-coefficient Technique). *Let us consider a fixed deterministic adversary $\mathcal{A}$, and let $\mathcal{T} = \mathcal{T}_{\text{good}} \cup \mathcal{T}_{\text{bad}}$ be a partition of the set of attainable transcripts. Let ε be such that for all $\tau \in \mathcal{T}_{\text{good}}$*

$$\frac{\Pr(X = \tau)}{\Pr(Y = \tau)} \geq 1 - \varepsilon \ . \tag{4}$$

Then, $\mathbf{Adv}_{\text{EM}}^{\mathsf{mk}}(\mathcal{A}) \leq \varepsilon + \Pr(Y \in \mathcal{T}_{\text{bad}})$.

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

$$\exists i, i', j, j' : i \neq i' : P_i^{(j)} \oplus P_{i'}^{(j')} = K_i \oplus K_{i'} \vee C_i^{(j)} \oplus C_{i'}^{(j')} = K_i \oplus K_{i'} \ , \quad (5)$$

$$\exists i, j, j' : \qquad P_i^{(j)} \oplus x^{(j')} = K_i \qquad \vee C_i^{(j)} \oplus x^{(j')} = K_i \oplus K_{i'} \ . \quad (6)$$

A transcript that is not a *bad* transcript, is referred to as a *good* transcript.

Upper Bounding $\Pr(Y \in \mathcal{T}_{\mathbf{bad}})$. We want to upper bound the event that a transcript τ in the ideal world satisfies (5)–(6). Note that $K_i \xleftarrow{\$} \{0,1\}^n$ for $i = 1, \ldots, \ell$ are dummy keys generated independently of $\tau_1, \ldots, \tau_\ell$. Therefore, there are at most $2D_iD_{i'}$ possible keys that satisfy (5) for any fixed $i \neq i'$. Analogously, there are at most $2D_iT$ possible keys that satisfy (6) for any fixed i. Therefore,

$$\Pr(Y \in \mathcal{T}_{\text{bad}}) \leq \frac{\sum_i \sum_{i' \neq i} 2D_iD_{i'} + \sum_i 2D_iT}{2^n} \ , \quad (7)$$

$$\leq \frac{D^2 + 2DT}{2^n} \ . \quad (8)$$

Lower Bounding Ratio $\Pr(X = \tau) / \Pr(Y = \tau)$. Let us consider a good and attainable transcript $\tau \in \mathcal{T}_{\text{good}}$. Then denote by $\Omega_X = 2^{n\ell} \cdot 2^n!$ the set of all possible oracles in the real world and by $\mathsf{comp}_X(\tau) \subseteq \Omega_X$ the set of oracles in Ω_X compatible with transcript τ. Define $\Omega_Y = 2^{n\ell} \cdot (2^n!)^{\ell+1}$ and $\mathsf{comp}_Y(\tau)$ similarly. According to the H-coefficient technique:

$$\Pr(X = \tau) = \frac{|\mathsf{comp}_X(\tau)|}{|\Omega_X|} \ , \qquad \text{and} \qquad \Pr(Y = \tau) = \frac{|\mathsf{comp}_Y(\tau)|}{|\Omega_Y|} \ . \quad (9)$$

First, we calculate $|\mathsf{comp}_X(\tau)|$. As $\tau \in \mathcal{T}_{\text{good}}$, there are no two queries in τ with the same input to or output of the underlying permutation. Any query tuple in τ therefore fixes exactly one input-output pair of the underlying oracle. Because τ consists of $D+T$ query tuples, the number of possible oracles in the real world equals $(2^n - D - T)!$. By a similar reasoning, the number of possible oracles in the ideal world equals $\prod_{i=1}^{\ell} (2^n - D_i)! \cdot (2^n - T)!$. Therefore,

$$\Pr(X = \tau) = \frac{(2^n - D - T)!}{2^{n\ell} \cdot 2^n!} \ , \quad (10)$$

$$\Pr(Y = \tau) = \frac{\prod_{i=1}^{\ell} (2^n - D_i)! \cdot (2^n - T)!}{2^{n\ell} \cdot (2^n!)^{\ell+1}} \leq \frac{(2^n - D - T)! \cdot (2^n!)^{\ell}}{2^{n\ell} \cdot (2^n!)^{\ell+1}} \ . \quad (11)$$

It then follows that $\Pr(X = \tau) / \Pr(Y = \tau) \geq 1$. □

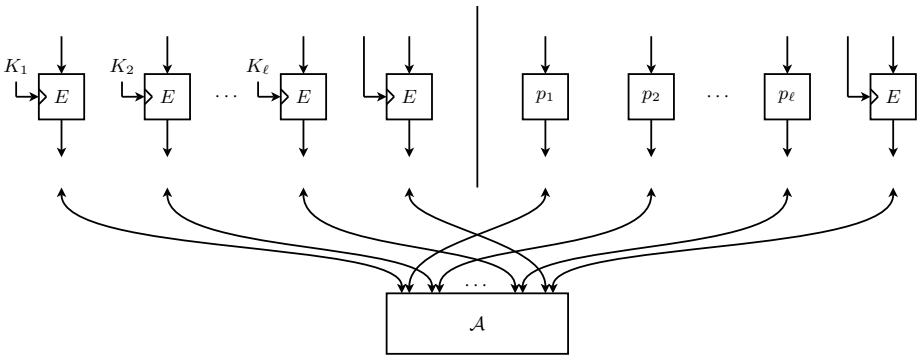

Fig. 3. An ideal block cipher E_K in the multi-key setting. Although only one direction is shown, all oracles are assumed to be bidirectional.

Theorem 2 (Ideal Block Cipher Multi-Key Security). *Let the ideal block cipher* IBC *be uniformly distributed random variable over* $\mathsf{block}(k, n)$*, then for all* $\mathcal{A}$ *making at most* D *queries to* $E_{K_1}, \ldots, E_{K_\ell}$ *(resp.* $p_1, \ldots, p_\ell$*) or their inverses and at most* T *queries to* E_K *or its inverse under adversary-chosen keys,*

$$\mathbf{Adv}^{\mathsf{mk}}_{\mathrm{IBC}}(\mathcal{A}) \leq \frac{\ell^2 + 2\ell T}{2^{k+1}} \quad . \tag{12}$$

Proof. We consider the adversary $\mathcal{A}$ shown in Fig. 3. Define $\mathbf{E}$ to be the event where either

1. there exists $i \neq j$ such that $K_i = K_j$ or
2. there exists a query $E(K, X)$ or $E^{-1}(K, X)$ such that $K = K_i$ for some i.

Given that $\mathbf{E}$ does not happen, $E_{K_1}, \ldots, E_{K_\ell}$ are drawn independently and uniformly at random from $\mathsf{perm}(n)$, and all queries made to E are independent of $E_{K_1}, \ldots, E_{K_\ell}$. Therefore $(E_{K_1}, \ldots, E_{K_\ell}, E)$ and $(p_1, \ldots, p_\ell, E)$ are indistinguishable given the negation of $\mathbf{E}$, and by the fundamental lemma of game playing,

$$\mathbf{Adv}^{\mathsf{mk}}_{\mathrm{IBC}}(\mathcal{A}) \leq \Pr(\mathbf{E}) \quad . \tag{13}$$

The probability that there exists an adversary query $E(K, X)$ or $E^{-1}(K, X)$ such that $K = K_i$ is at most $\frac{T\ell}{2^k}$. The probability that two keys collide is bounded above by $\frac{\ell^2}{2^{k+1}}$, hence

$$\Pr(\mathbf{E}) \leq \frac{\ell^2 + 2\ell T}{2^{k+1}} \quad . \tag{14}$$

□

By our definition, there must be at least one query for every key. Therefore $D \geq \ell$, so that the following corollary can be derived from Theorem 2:

Corollary 1 (Corollary of Theorem 2).

$$\mathbf{Adv}^{\mathsf{mk}}_{\mathrm{IBC}}(\mathcal{A}) \leq \frac{D^2 + 2DT}{2^{k+1}} \quad . \tag{15}$$

Observe that when the amount of plaintext per key is small, this bound is close to that of Theorem 2.

3.1 Tightness of the Security Bounds

Several attacks have been published that match the security bound of the Even-Mansour block cipher in the single-key setting. The first attacks were published by Daemen [20]: a known-plaintext attack for $D = 2$ and a chosen-plaintext attack for any value of D. Biruykov and Wagner [16] presented a known-plaintext attack for $D \geq 2^{n/2}$. A known-plaintext attack for any value of D was given by Dunkelman et al. [24].

The single-key setting is a special case of the multi-key setting where $\ell = 1$. We proved in Sect. 3 (see Theorem 1) that the security bound of Even-Mansour in multi-key setting is a straightforward extension of the single-key setting. Therefore, the bound that we derived for Even-Mansour in the multi-key setting is also tight.

An attack matching our Even-Mansour security bound in the multi-key setting was recently given by Fouque et al. [29] for $\ell = 2^{n/3}$, $D_i = 2^{n/3}$ for $i = 1, \ldots, \ell$ and $T = 2^{n/3}$.

In the case of an ideal block cipher in the multi-key setting with $D = \ell$, the key collision and time-memory trade-off attacks of Biham [10, 11] show that the security bound of Corollary 1 is also tight. For a discussion of these attacks and their subsequent improvements, we refer to Sect. 2.3. Evidently, these attacks are also applicable to the Even-Mansour block cipher in the multi-key setting.

4 Discussion

As we proved in Sect. 3, the Even-Mansour block cipher has similar security in the multi-key setting as an ideal block cipher with the same block and key size, assuming $D \approx \ell$. In Sect. 2.2, we pointed out the relevance of this multi-key setting in practice.

The Even-Mansour block cipher is interesting from a design point of view because of its simplicity. As Dunkelman et al. [24] argued, it also achieves minimalism, in the sense that removing any component (one of the two key additions or the permutation) results in an insecure construction. But the Even-Mansour construction also has many implementation advantages.

From an efficiency point of view, the Even-Mansour block cipher avoids that round keys need to be precalculated and stored in memory, or that they need to be calculated on-the-fly. Avoiding precalculation of the key schedule results in a higher key agility, because of the lower cost to rekey. If round keys do not need to be calculated on-the-fly, the efficiency of every block cipher call increases. For

software implementations, avoiding a key schedule reduces register pressure and decreases RAM requirements. The amount of RAM is very critical on certain microcontrollers, as shown for example in [37].

From a security point of view, the Even-Mansour block cipher avoids the need to store round keys securely. Note that in the case of AES-128, recovery of any round key leads to recovery of the encryption key. In the case of AES with 192-bit or 256-bit keys, any two consecutive round keys can be used to recover the encryption key.

Secure key storage is not only a problem for smart cards and RFID tags, but is also difficult to ensure on general purpose CPUs. The virtual memory system may move cryptographic keys into swap storage, which necessitates error-prone techniques to avoid swapping, or to use swap encryption [52].

But even in the presence of these countermeasures, cold boot attacks [33] may be used to exploit the fact that DRAM retains a large part of its memory for several seconds after removing power. Cooling techniques may be used to increase this time to several hours or even days.

If the round keys that are recovered by a cold boot attack contains errors (due to memory bit decay), it may still be possible to recover the encryption key. For AES, Halderman et al. [33] describe a simple algorithm to recover the encryption key in this case. Improved attacks were later given by Albrecht et al. [1] using integer programming, and by Tsow [53], and Kamal and Youssef [39] using a SAT solver.

The Even-Mansour block cipher avoids all attacks that recover the encryption key from noisy round keys, as it avoids the calculation of round keys altogether. The leakage of encryption keys or round keys cannot be avoided without additional security measures. However, this problem becomes much more manageable for the Even-Mansour construction, as there are no round keys to protect.

5 Conclusion and Future Work

Rekeying occurs frequently in real-world implementations, meaning that a plaintext may be encrypted under different keys. This setting is used, for example, in the attacks by AlFardan et al. [2] on TLS, and by Paterson et al. [49] on WPA-TKIP.

This setting is often referred to as the *broadcast setting* or the *multi-user setting*. In this paper, we introduced the *multi-key setting* to generalize the aforementioned settings. In the multi-key setting, the adversary can perform chosen-plaintext and chosen-ciphertext attacks under a set of unknown keys.

In the multi-key setting, we proved that the Even-Mansour block cipher is secure up to $(D^2 + 2DT)/2^n$ queries. We proved a similar bound for an ideal block cipher with $k = n$, and showed that both bounds are tight. We used our proofs to argue in favor of the Even-Mansour construction: not only because of the simplicity of its design, but also because the lack of a key schedule makes it easier to generate fast and secure implementations.

Modes of operation for encryption and/or authentication may be designed more efficiently, if it is known that the underlying block cipher follows the Even-Mansour construction. It also seems that an Even-Mansour block cipher may still be secure if the underlying permutation is far from ideal, an idea that was pioneered by the design of the Chaskey MAC function [47]. We leave the further exploration of these research questions to future work.

Acknowledgments. The authors would like to thank Bart Mennink for his useful comments and suggestions. This work was supported in part by the Research Council KU Leuven: GOA TENSE (GOA/11/007), by Research Fund KU Leuven, OT/13/071, and by the ANR BLOC project. Nicky Mouha is supported by a Postdoctoral Fellowship from the Flemish Research Foundation (FWO-Vlaanderen). Atul Luykx is supported by a Ph.D. Fellowship from the Institute for the Promotion of Innovation through Science and Technology in Flanders (IWT-Vlaanderen).

References

1. Albrecht, M.R., Cid, C.: Cold Boot Key Recovery by Solving Polynomial Systems with Noise. In: Lopez, J., Tsudik, G. (eds.) Applied Cryptography and Network Security - 9th International Conference, ACNS 2011, Nerja, Spain, June 7-10, 2011. Proceedings. Lecture Notes in Computer Science, vol. 6715, pp. 57–72 (2011), http://dx.doi.org/10.1007/978-3-642-21554-4_4
2. AlFardan, N.J., Bernstein, D.J., Paterson, K.G., Poettering, B., Schuldt, J.C.: On the Security of RC4 in TLS and WPA. In: USENIX Security Symposium (2013)
3. Babbage, S.H.: Improved "Exhaustive Search" Attacks on Stream Ciphers. In: ECOS 95 (European Convention on Security and Detection), Conference publication No. 408. pp. 161–166 (May 1995)
4. Barker, W.C., Barker, E.: SP 800-67 Revision 1: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher (January 2012), http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf
5. Bellare, M., Boldyreva, A., Micali, S.: Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements. In: Preneel [51], pp. 259–274
6. Bellare, M., Desai, A., Jokipii, E., Rogaway, P.: A Concrete Security Treatment of Symmetric Encryption. In: 38th Annual Symposium on Foundations of Computer Science, FOCS '97, Miami Beach, Florida, USA, October 19-22, 1997. pp. 394–403. IEEE Computer Society (1997), http://dx.doi.org/10.1109/SFCS.1997.646128
7. Bellare, M., Kohno, T.: A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications. In: Biham, E. (ed.) EUROCRYPT. LNCS, vol. 2656, pp. 491–506. Springer (2003)
8. Biham, E.: New Types of Cryptoanalytic Attacks Using related Keys (Extended Abstract). In: Helleseth, T. (ed.) EUROCRYPT. LNCS, vol. 765, pp. 398–409. Springer (1993)
9. Biham, E.: New Types of Cryptanalytic Attacks Using Related Keys. J. Cryptology 7(4), 229–246 (1994)
10. Biham, E.: How to Forge DES-Encrypted Messages in 2^{28} Steps. Technical Report CS0884, Technion Computer Science Departement, Israel (1996)

11. Biham, E.: How to decrypt or even substitute DES-encrypted messages in 2^{28} steps. Inf. Process. Lett. 84(3), 117–124 (2002)
12. Biryukov, A.: Some Thoughts on Time-Memory-Data Tradeoffs. Cryptology ePrint Archive, Report 2005/207 (2005), http://eprint.iacr.org/
13. Biryukov, A., Khovratovich, D.: Related-Key Cryptanalysis of the Full AES-192 and AES-256. In: Matsui, M. (ed.) ASIACRYPT. Lecture Notes in Computer Science, vol. 5912, pp. 1–18. Springer (2009)
14. Biryukov, A., Khovratovich, D., Nikolic, I.: Distinguisher and Related-Key Attack on the Full AES-256. In: Halevi, S. (ed.) CRYPTO. Lecture Notes in Computer Science, vol. 5677, pp. 231–249. Springer (2009)
15. Biryukov, A., Shamir, A.: Cryptanalytic Time/Memory/Data Tradeoffs for Stream Ciphers. In: Okamoto, T. (ed.) Advances in Cryptology - ASIACRYPT 2000, 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, December 3-7, 2000, Proceedings. Lecture Notes in Computer Science, vol. 1976, pp. 1–13. Springer (2000)
16. Biryukov, A., Wagner, D.: Advanced Slide Attacks. In: Preneel [51], pp. 589–606, http://dx.doi.org/10.1007/3-540-45539-6_41
17. Chatterjee, S., Menezes, A., Sarkar, P.: Another Look at Tightness. In: Miri, A., Vaudenay, S. (eds.) Selected Areas in Cryptography. Lecture Notes in Computer Science, vol. 7118, pp. 293–319. Springer (2011)
18. Chen, L.: Recommendation for Key Derivation Using Pseudorandom Functions (Revised). NIST special publication 800-108, National Institute of Standards and Technology (NIST) (October 2009), http://csrc.nist.gov/publications/nistpubs/800-108/sp800-108.pdf
19. Chen, S., Steinberger, J.P.: Tight Security Bounds for Key-Alternating Ciphers. In: Nguyen, P.Q., Oswald, E. (eds.) Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings. Lecture Notes in Computer Science, vol. 8441, pp. 327–350. Springer (2014), http://dx.doi.org/10.1007/978-3-642-55220-5_19
20. Daemen, J.: Limitations of the Even-Mansour Construction. In: Imai et al. [38], pp. 495–498
21. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Springer (2002)
22. Daemen, J., Rijmen, V.: On the Related-Key Attacks against AES. Proceedings of the Romanian Academy, Series A 13(4), 395–400 (2012)
23. Davies, D.W.: Some Regular Properties of the 'Data Encryption Standard' Algorithm. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) CRYPTO. pp. 89–96. Plenum Press, New York (1982)
24. Dunkelman, O., Keller, N., Shamir, A.: Minimalism in Cryptography: The Even-Mansour Scheme Revisited. In: Pointcheval and Johansson [50], pp. 336–354
25. Dworkin, M.: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. NIST special publication 800-38b, National Institute of Standards and Technology (NIST) (May 2005), http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf
26. Dworkin, M.: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC (November 2007), http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf
27. Even, S., Mansour, Y.: A Construction of a Cipher From a Single Pseudorandom Permutation. In: Imai et al. [38], pp. 210–224

28. Even, S., Mansour, Y.: A Construction of a Cipher from a Single Pseudorandom Permutation. J. Cryptology 10(3), 151–162 (1997)
29. Fouque, P., Joux, A., Mavromati, C.: Multi-user Collisions: Applications to Discrete Logarithm, Even-Mansour and PRINCE. In: Sarkar, P., Iwata, T. (eds.) Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I. Lecture Notes in Computer Science, vol. 8873, pp. 420–438. Springer (2014), http://dx.doi.org/10.1007/978-3-662-45611-8_22
30. Gauravaram, P., Knudsen, L.R., Matusiewicz, K., Mendel, F., Rechberger, C., Schläffer, M., Thomsen, S.S.: Grøstl – a SHA-3 candidate. Submission to the NIST SHA-3 Competition (Round 3) (2011), http://www.groestl.info/Groestl.pdf
31. Golić, J.D.: Cryptanalysis of Alleged A5 Stream Cipher. In: Fumy, W. (ed.) Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding. Lecture Notes in Computer Science, vol. 1233, pp. 239–255. Springer (1997)
32. Group, I.N.W.: The Transport Layer Security (TLS) Protocol. http://tools.ietf.org/html/rfc4346 (2006)
33. Halderman, J.A., Schoen, S.D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J.A., Feldman, A.J., Appelbaum, J., Felten, E.W.: Lest We Remember: Cold Boot Attacks on Encryption Keys. In: van Oorschot, P.C. (ed.) Proceedings of the 17th USENIX Security Symposium, July 28-August 1, 2008, San Jose, CA, USA. pp. 45–60. USENIX Association (2008), http://www.usenix.org/events/sec08/tech/full_papers/halderman/halderman.pdf
34. Hellman, M.E., Merkle, R., Schroeppel, R., Diffie, W., Pohlig, S., Schweitzer, P.: Results of an Initial Attempt to Cryptanalyze the NBS Data Encryption Standard. Technical Report, Stanford University, USA (1976)
35. Hellman, M.E.: A Cryptanalytic Time-Memory Trade-off. Information Theory, IEEE Transactions on 26(4), 401–406 (1980)
36. Hong, J., Sarkar, P.: New Applications of Time Memory Data Tradeoffs. In: Roy, B.K. (ed.) ASIACRYPT. Lecture Notes in Computer Science, vol. 3788, pp. 353–372. Springer (2005)
37. Ideguchi, K., Owada, T., Yoshida, H.: A Study on RAM Requirements of Various SHA-3 Candidates on Low-cost 8-bit CPUs. Cryptology ePrint Archive, Report 2009/260 (2009), http://eprint.iacr.org/
38. Imai, H., Rivest, R.L., Matsumoto, T. (eds.): Advances in Cryptology - ASIACRYPT '91, International Conference on the Theory and Applications of Cryptology, Fujiyoshida, Japan, November 11-14, 1991, Proceedings, Lecture Notes in Computer Science, vol. 739. Springer (1993)
39. Kamal, A.A., Youssef, A.M.: Applications of SAT Solvers to AES key Recovery from Decayed Key Schedule Images. In: Emerging Security Information Systems and Technologies (SECURWARE), 2010 Fourth International Conference on. pp. 216–220. IEEE (2010)
40. Knudsen, L.R., Rijmen, V.: Known-Key Distinguishers for Some Block Ciphers. In: Kurosawa, K. (ed.) ASIACRYPT. LNCS, vol. 4833, pp. 315–324. Springer (2007)
41. Koblitz, N., Menezes, A.: Another look at HMAC. J. Mathematical Cryptology 7(3), 225–251 (2013)
42. Lai, X., Massey, J.L.: Markov Ciphers and Differential Cryptanalysis. In: Davies, D.W. (ed.) EUROCRYPT. Lecture Notes in Computer Science, vol. 547, pp. 17–38. Springer (1991)

43. Mantin, I., Shamir, A.: A Practical Attack on Broadcast RC4. In: Matsui, M. (ed.) Fast Software Encryption, 8th International Workshop, FSE 2001 Yokohama, Japan, April 2-4, 2001, Revised Papers. Lecture Notes in Computer Science, vol. 2355, pp. 152–164. Springer (2001)
44. Mehuron, W.: Data Encryption Standard (DES) (October 1999), http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
45. Menezes, A.: Another Look at Provable Security. In: Pointcheval and Johansson [50], p. 8
46. Menezes, A., van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press (1997)
47. Mouha, N., Mennink, B., Herrewege, A.V., Watanabe, D., Preneel, B., Verbauwhede, I.: Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers. In: Joux, A., Youssef, A.M. (eds.) Selected Areas in Cryptography - SAC 2014 - 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers. Lecture Notes in Computer Science, vol. 8781, pp. 306–323. Springer (2014), http://dx.doi.org/10.1007/978-3-319-13051-4_19
48. Patarin, J.: The "Coefficients H" Technique. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) Selected Areas in Cryptography, 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, Revised Selected Papers. Lecture Notes in Computer Science, vol. 5381, pp. 328–345. Springer (2008), http://dx.doi.org/10.1007/978-3-642-04159-4_21
49. Paterson, K.G., Schuldt, J.C., Poettering, B.: Plaintext Recovery Attacks Against WPA/TKIP. In: Cid, S., Rechberger, C. (eds.) FSE 2014. Lecture Notes in Computer Science, Springer (2015 (To appear)), Available at: http://eprint.iacr.org/2013/748
50. Pointcheval, D., Johansson, T. (eds.): Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings, Lecture Notes in Computer Science, vol. 7237. Springer (2012)
51. Preneel, B. (ed.): Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding, Lecture Notes in Computer Science, vol. 1807. Springer (2000)
52. Provos, N.: Encrypting Virtual Memory. In: Bellovin, S.M., Rose, G. (eds.) 9th USENIX Security Symposium, Denver, Colorado, USA, August 14-17, 2000. USENIX Association (2000), https://www.usenix.org/conference/9th-usenix-security-symposium/encrypting-virtual-memory
53. Tsow, A.: An Improved Recovery Algorithm for Decayed AES Key Schedule Images. In: Jacobson Jr., M.J., Rijmen, V., Safavi-Naini, R. (eds.) Selected Areas in Cryptography, 16th Annual International Workshop, SAC 2009, Calgary, Alberta, Canada, August 13-14, 2009, Revised Selected Papers. Lecture Notes in Computer Science, vol. 5867, pp. 215–230. Springer (2009), http://dx.doi.org/10.1007/978-3-642-05445-7_14