Des. Codes Cryptogr. (2018) 86:623–640
https://doi.org/10.1007/s10623-017-0347-3

Connecting tweakable and multi-key blockcipher security

Jooyoung Lee[1] · **Atul Luykx**[2,3,4] · **Bart Mennink**[5] · **Kazuhiko Minematsu**[6]

Received: 8 November 2016 / Revised: 19 February 2017 / Accepted: 21 February 2017 /
Published online: 4 March 2017

Abstract The significance of understanding blockcipher security in the multi-key setting is highlighted by the extensive literature on attacks, and how effective key size can be significantly reduced. Nevertheless, little attention has been paid in formally understanding the design of multi-key secure blockciphers. In this work, we formalize the multi-key security of tweakable blockciphers in case of general key derivation functions. We show an equivalence between blockcipher multi-key security and tweakable blockcipher security. Our equivalence connects two objects of study, the iterated Even–Mansour (EUROCRYPT 2012) and the iterated Tweakable Even–Mansour (CRYPTO 2015), which establishes that results in both areas are, to a certain extent, transferable. Using our novel equivalence relation, we derive new bounds for both constructions, pave the path towards the solution of two well-studied conjectures, and show that, contrary to common knowledge, key derivation functions need not necessarily be pseudorandom functions in order to provide security: for the iterated Even–Mansour universal hash functions suffice.

Communicated by L. R. Knudsen.

✉ Bart Mennink
b.mennink@cs.ru.nl

Jooyoung Lee
hicalf@kaist.ac.kr

Atul Luykx
atul.luykx@kuleuven.be

Kazuhiko Minematsu
k-minematsu@ah.jp.nec.com

1 School of Computing, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon, Korea

2 Department of Electrical Engineering, ESAT/COSIC, KU Leuven, Leuven, Belgium

3 Department of Computer Science, University of California, Davis, CA, USA

4 imec, Ghent, Belgium

5 Digital Security Group, Radboud University, Nijmegen, The Netherlands

6 NEC Corporation, 1753 Shimonumabe, Nakahara-Ku, Kawasaki, Japan

Keywords Even–Mansour · Tweakable Even–Mansour · Cascaded LRW · Multi-key · Conjectures

Mathematics Subject Classification 94A60

1 Introduction

A necessity for any cryptographic system is the ability to support communication among many users, for potentially long periods of time. Enabling security in such scenarios requires distributing many keys, not only per user, but also per unit of time. As a result, understanding the multi-key security of cryptographic algorithms is important.

In applications where symmetric-key algorithms are used for the bulk of communication, the difficulty in maintaining security in multi-key settings involves not only initially distributing and managing keys for each pair of communicating parties, but also ensuring that keys are not used beyond recommended data and time limits. How long a key can be used and how much data it can process is determined via cryptanalysis and security bounds estimating adversarial success probability. However, until recently, most analysis has been performed in the single-key setting, even though analyzing cryptographic algorithms in the multi-key setting has more practical significance.

Nevertheless, the limitations of the multi-key setting are well-understood for a large variety of cryptographic algorithms, such as public key encryption [5], key establishment protocols [9,13], signatures [65], and message authentication codes [6,17]. Blockciphers are no exception, and have been the subject of many attacks taking advantage of the availability of multiple keys. For example, Biham [7] showed that the effective key size of blockciphers can halve in the multi-key setting, provided sufficiently many keys are employed in the encryption of a known plaintext. Subsequent attacks used time-memory-key tradeoffs [12,29,34,41] for improvements.

Despite the multitude of attacks, little exploration has been done concerning the design of blockciphers in the multi-key setting. This is most likely due to the result stating that the multi-key security of a blockcipher can be reduced to its single-key security with a security loss proportional to the number of keys used, a fact which has been formally proven for public key encryption schemes [5] and message authentication codes [17], among others. This reduction relies on the fact that all keys are independent and uniformly distributed. In practice, however, generating keys is often done via the use of key derivation functions (KDFs), which use a master key to output many different keys. Therefore, to be able to rely on single-key security, such a KDF must behave like a pseudorandom function, so that its outputs are computationally indistinguishable from independent, uniformly distributed values.

1.1 Linking multi-key security with tweakable blockciphers

Our main contribution is drawing a powerful connection between the multi-key security of blockciphers and the security of *tweakable* blockciphers. As a first step towards the connection, we present a generalized definition of multi-key security of (tweakable) blockciphers in Sect. 3. While earlier definitions, including Mouha and Luykx [64], only considered independent, uniformly generated keys, we introduce KDFs in the definition of multi-key security, and say that the combination of a blockcipher with KDF is secure if it is indistinguishable from uniform random permutations.

By explicitly including KDFs into blockcipher security, and viewing key schedules as a type of KDF, one can put weak, known, and related key attacks in perspective with multi-key security. More importantly, due to the explicit inclusion of KDFs, the connection between multi-key and tweakable blockcipher security (Sect. 4) is immediate. This connection allows one to use the large body of work on tweakable blockciphers (see Sect. 5) to understand the multi-key security of blockciphers, and vice versa.

Finally, via the connection with tweakable blockciphers, *related-key* security of blockciphers [10] can also be linked to multi-key security. In more detail, in related-key security, an attacker may transform the master key via a related-key-deriving function, which could also be interpreted as deriving a new subkey in the multi-key setting.

1.2 Application to even–mansour and tweakable even–mansour

By identifying KDFs with key schedules, or rather TWEAKEY schedules [48], which process both tweak and key input to generate subkeys for use in blockciphers, significant performance gains can be made depending upon the application. KDFs are usually designed to behave like pseudorandom functions, which is the optimal choice when blockciphers are treated like black boxes. However, in order to improve performance blockciphers cannot be treated as black boxes, and KDFs must be designed with specific blockciphers in mind, which is what a TWEAKEY schedule is.

Instead of looking at one specific blockcipher, or treating them as black boxes, we take an intermediate approach and apply our observations to the iterated Even–Mansour construction EM[r] [11,30,31] and the Tweakable Even–Mansour construction TEM[r] [21], which can be viewed as generic versions of key alternating ciphers [27,28], the design approach to the AES [28]. As depicted in Fig. 1, both constructions process their input using $r \geq 1$ consecutive, independent permutations interleaved with maskings derived from the key; the main difference between the constructions is that in TEM[r] the maskings are derived from the key and the tweak via a universal hash function. See Sect. 5 for a detailed explanation of the constructions.

Chen and Steinberger [19] proved that EM[r] achieves asymptotically $2^{rn/(r+1)}$ single-key security for arbitrary $r \geq 1$. Hoang and Tessaro [42] recently simplified their bound and improved it by a constant factor. They additionally demonstrated how the results directly generalize to the multi-key setting based on uniformly random KDF. For TEM[r], Cogliati et al. [16] proved $2^{n/2}$ single-key security for $r = 1$, $2^{2n/3}$ for $r = 2$, and $2^{rn/(r+2)}$ for any *even* r, and conjectured that it achieves (tight) $2^{rn/(r+1)}$ single-key security for any $r \geq 1$. These results are summarized in Table 1, with further related work in Sect. 5.

First, we use our new equivalence result as a tool to transfer the EM[r] multi-key bound to TEM[r] in Sect. 5.4, establishing a $2^{rn/(r+1)}$ bound for *any* r, as long as the universal hash function is replaced by a uniform random function, and the adversaries use a limited number of tweaks. In applications where the number of tweaks can be limited to a small number, as might, for example, be the case in certain authenticated encryption schemes [2,26,68], our newly obtained bound on TEM[r] improves over the state of the art, and even solves the conjecture by Cogliati et al. in 2015 [21] for the specific case of uniformly random masking. The replacement of the universal hash function by a uniform random function may in certain settings by a burden, but this condition allows us to make a first step towards solving this conjecture for general masking. The new bounds are summarized in Table 1.

As a bonus, the new TEM[r] bound carries over to its blockcipher-based sibling LRW[r] [53,55,56,67]; see Fig. 1 for its depiction, and Sect. 5 for a detailed explanation of the construction. Our bounds therefore also partially solve the related conjecture by Landecker

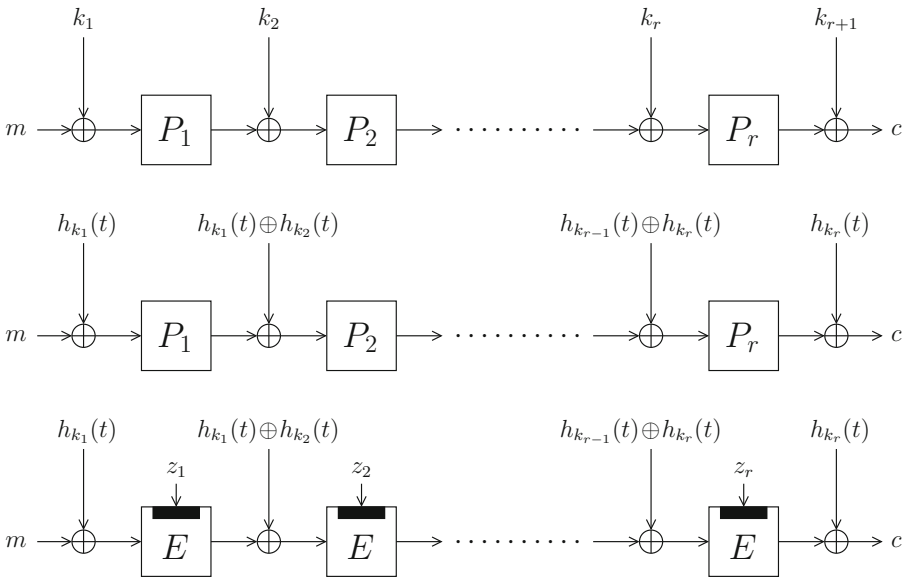

Fig. 1 From *top* to *bottom*: r rounds of iterated Even–Mansour, Tweakable Even–Mansour, and Cascaded LRW. Here, k_i and z_i are key material, P_i are permutations, E is a blockcipher, and h_{k_i} are universal hash functions. All schemes reveal strong similarity, with one caveat: LRW[r] and TEM[r] explicitly have r-wise independent masking, while EM[r] uses $r+1$ keys. However, the state of the art security analysis on EM[r] also covers r-wise independent keying [19]

Table 1 State of the art and new results on EM[r], TEM[r], and LRW[r], with n the size of the permutation or blockcipher, μ the number of users, and ℓ the number of tweaks used

Scheme	Model	# Rounds			Note
		1	2	r	
EM	Single-key	$2^{n/2}$	$2^{2n/3}$	$2^{\frac{rn}{r+1}}$	[19,42]
EM	UAXU-multi-key	$2^{n/2}$	$2^{2n/3}$	$2^{\frac{rn}{r+2}}$	New
EM	Random-multi-key	$2^{n/2}$	$2^{2n/3}$	$2^{\frac{rn}{r+1}}$	[3,42,64]
TEM (UAXU mask)	Single-key	$2^{n/2}$	$2^{2n/3}$	$2^{\frac{rn}{r+2}}$	[16]
TEM (random mask)	Single-key	$2^{n/2}$	$2^{2n/3}$	$2^{\frac{rn}{r+1}}$	New
LRW (AXU mask)	Single-key	$2^{n/2}$	$2^{2n/3}$	$2^{\frac{rn}{r+2}}$	[53,55,56,67]
LRW (random mask)	Single-key	$2^{n/2}$	$2^{2n/3}$	$2^{\frac{rn}{r+1}}$	New

et al. [56] and Lampe and Seurin [55] on LRW[r], provided the maximum number of tweaks can be bounded and the masking is random.

Finally, we also consider multi-key security of EM[r] with a KDF that is not necessarily random. Using aforementioned equivalence in reverse direction, in Sect. 5.4 we transfer the results from Cogliati et al. [16] on TEM[r] to multi-key security bounds of EM[r] which do not degrade relative to the number of users, but with the same limitations on r as with the TEM[r] bounds (see Table 1). The bound is identical to that of [16]. Interestingly, we are

able to conclude that a pseudorandom KDF is *not* necessary to achieve multi-key security with the EM[r] construction. Since the tweaks for TEM[r] are generated using universal hash functions, such functions suffice as KDF for EM[r].

1.3 Performance gains

Besides the necessity of using pseudorandom KDFs when the blockcipher is treated as a black box, it is also important if the application scenario contains malicious users: it should be infeasible for one pair of communicating users to guess the keys of other users. Therefore, weakening the KDF must be done with care. However, there are applications where the users are known not to be malicious.

Consider wireless sensor networks for example, which consist of small autonomous sensors used to monitor environmental conditions. Using our connection between multi-key security and tweakable blockciphers, it is clear that in those settings one could replace the combination of a KDF and blockcipher with a single tweakable blockcipher, where the "keys" for each of the sensors would correspond to different tweaks for the tweakable blockcipher. Even though each of the sensors could easily compute the "key" of any other sensor, the main security threat in this scenario are external attackers, not the sensors themselves. This approach is formalized in Sect. 6.

The only issue would be key compromise of a sensor, which would immediately leak the key, and therefore security of the entire system would be lost. Even if it is difficult to ensure that no sensor will leak its key, one can still avoid using pseudorandom KDFs. For example, an intermediate solution is to group together sensors, and to distribute an independent key to each group, while communication within the group is performed by changing tweaks. In Sect. 3.2 we describe another solution, which uses universal hash functions which are secure against collusion of a group of users, meaning a certain number of sensors could be compromised without the entire system loosing security.

2 Preliminaries

The set of bit strings of length $n \geq 0$ is denoted $\{0,1\}^n$. For two sets $\mathcal{X}, \mathcal{Y}$, the set of all functions from $\mathcal{X} \to \mathcal{Y}$ is denoted $\mathsf{Func}(\mathcal{X}, \mathcal{Y})$, the case of $\mathcal{X} = \mathcal{Y}$ being abbreviated to $\mathsf{Func}(\mathcal{X})$. The set of permutations on $\mathcal{X}$ is denoted $\mathsf{Perm}(\mathcal{X})$. Uniform random drawing of an element x from $\mathcal{X}$ is denoted $x \xleftarrow{\$} \mathcal{X}$.

2.1 Blockciphers and tweakable blockciphers

A blockcipher is a mapping $E : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$ where for every key $k \in \mathcal{K}$, the function $E(k, \cdot)$ is a permutation on $\mathcal{M}$. Its inverse is denoted $E^{-1}(k, \cdot)$. A tweakable blockcipher is a mapping $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$ where for every key $k \in \mathcal{K}$ and every tweak $t \in \mathcal{T}$, the function $\widetilde{E}(k, t, \cdot)$ is a permutation on $\mathcal{M}$. Its inverse is denoted $\widetilde{E}^{-1}(k, t, \cdot)$. Denote by $\mathsf{TPerm}(\mathcal{T}, \mathcal{M})$ the set of all functions $\widetilde{\pi} : \mathcal{T} \times \mathcal{M} \to \mathcal{M}$ such that $\widetilde{\pi}(t, \cdot) \in \mathsf{Perm}(\mathcal{M})$ for all $t \in \mathcal{T}$.

Note that a conventional blockcipher is a tweakable blockcipher with tweak space of size 1, meaning that tweakable blockcipher security definitions can be applied to blockciphers. Therefore, we will only discuss the security of tweakable ciphers, which will be denoted explicitly with the use of 'T' and '$\sim$'. The corresponding notation for conventional blockciphers follows by removing the 'T's and '$\sim$'s.

Let $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$ be a tweakable blockcipher that is internally based on $r \geq 1$ primitives $\Pi_1, \ldots, \Pi_r \in \mathsf{Prims}$, where Prims is some set of primitives. Examples include $\mathsf{Prims} = \mathsf{Perm}(\mathcal{M})$, which is used in the Even–Mansour constructions, and $\mathsf{Prims} = \mathsf{Func}(\mathcal{M}')$, which is used in Feistel networks where $\mathcal{M}'$ is of size smaller than $\mathcal{M}$.

In the following definition we consider a distinguisher $\mathcal{D}$ that either interacts in a "real world", where it has query access to $\widetilde{E}_k$ with secret $k \xleftarrow{\$} \mathcal{K}$, or an "ideal world", where $\mathcal{D}$ interacts with an ideal tweakable permutation $\widetilde{\pi} \xleftarrow{\$} \mathsf{TPerm}(\mathcal{T}, \mathcal{M})$. In both worlds $\mathcal{D}$ gets access to the idealized primitives $\Pi = (\Pi_1, \ldots, \Pi_r) \xleftarrow{\$} \mathsf{Prims}^r$. The goal of $\mathcal{D}$ is to distinguish the real from the ideal world.

Definition 1 (*STPRP security*) Consider $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$ based on $r \geq 1$ primitives $\Pi_1, \ldots, \Pi_r \in \mathsf{Prims}$. The STPRP (strong tweakable pseudorandom permutation) advantage of a distinguisher $\mathcal{D}$ is

$$\mathbf{Adv}^{\mathsf{stprp}}_{\widetilde{E}}(\mathcal{D}) = \Delta_{\mathcal{D}}(\widetilde{E}_k, \Pi \; ; \; \widetilde{\pi}, \Pi) = \left| \mathbf{Pr}\left(\mathcal{D}^{\widetilde{E}_k, \Pi} = 1\right) - \mathbf{Pr}\left(\mathcal{D}^{\widetilde{\pi}, \Pi} = 1\right) \right| ,$$

where the probabilities are taken over the random choices of $k \xleftarrow{\$} \mathcal{K}$, $\Pi \xleftarrow{\$} \mathsf{Prims}^r$, and $\widetilde{\pi} \xleftarrow{\$} \mathsf{TPerm}(\mathcal{T}, \mathcal{M})$. The distinguisher has two-sided query access to each of its oracles. For any $q, \ell, p \geq 0$ with $\ell \leq |\mathcal{T}|$, we define $\mathbf{Adv}^{\mathsf{stprp}}_{\widetilde{E}}(q, \ell, p)$ to be the maximum advantage over any distinguisher $\mathcal{D}$ that makes at most q queries to the construction for at most ℓ different tweaks, and p queries to each of the primitives.

Inclusion of the parameter ℓ might seem artificial, but it can be set arbitrarily large and therefore does not limit applicability of the definition. Although it is included to describe distinguishers more accurately, it has a meaningful connection to the security bounds of MAC functions and authenticated encryption schemes based on blockciphers. In more detail, consider an authenticated encryption scheme based on a tweakable blockcipher, denote by ℓ' the maximal message length, and ℓ the number of different tweaks employed in the authenticated encryption schemes. On the one hand, the parameter ℓ' often plays a significant role in the security bounds, while on the other hand, the values ℓ and ℓ' are often close to each other, and differ at most by a multiplicative constant. For example, for COPA [2], ELmE [26], and SCT [68], we have $\ell \approx 2\ell'$.

2.2 Universal hash functions

Let $(\mathcal{Y}, \oplus)$ be an abelian group. Let $H = \{h_k : \mathcal{X} \to \mathcal{Y} \mid k \in \mathcal{K}\}$ be a family of functions indexed by a key $k \in \mathcal{K}$. We say that H is *uniform* if for any $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, we have

$$\mathbf{Pr}\left(k \xleftarrow{\$} \mathcal{K} \; : \; h_k(x) = y\right) = 1/|\mathcal{Y}| \, .$$

We say that H is ε-*almost-XOR-universal* (ε-*AXU*)[1] if for any distinct $x, x' \in \mathcal{X}$ and $y \in \mathcal{Y}$, we have

$$\mathbf{Pr}\left(k \xleftarrow{\$} \mathcal{K} \; : \; h_k(x) \oplus h_k(x') = y\right) \leq \varepsilon.$$

We say that H is ε-*UAXU* if it is uniform and ε-AXU.

A result that we will use later is that a uniform random function is also uniform and AXU. More formally, define

[1] The "almost" is in fact implicit in the term ε, but we will maintain it conform general convention.

$$\mathsf{F}^{\mathcal{X}}_{\mathcal{Y}} : \mathsf{Func}(\mathcal{X}, \mathcal{Y}) \times \mathcal{X} \to \mathcal{Y} \tag{1}$$

as a family of functions defined as $\mathsf{F}^{\mathcal{X}}_{\mathcal{Y}}(f, x) = f(x)$.

Lemma 1 *$\mathsf{F}^{\mathcal{X}}_{\mathcal{Y}}$ is uniform and $|\mathcal{Y}|^{-1}$-AXU.*

Throughout, we will simply write $\mathsf{F}^{\mathcal{X}}_{n}$ for $\mathsf{F}^{\mathcal{X}}_{\{0,1\}^n}$. Our interest in uniform random functions is purely in connecting our definition of multi-key security to the conventional definitions.

3 Multi-key security

Mouha and Luykx [64] formalized the notion of multi-key security of blockciphers, and applied it to one round of Even–Mansour (cf. Sect. 5.1). We introduce the generalization of this model to (i) tweakable blockcipher constructions and (ii) arbitrary key derivation functions. The model shows similarity with that of Hoang and Tessaro [42]. As in Sect. 2.1 we will discuss the multi-key security model for tweakable blockciphers, including 'T's and '$\sim$'s. The multi-key security for conventional blockciphers follows by removing the 'T's and '$\sim$'s.

In the definition below, μ represents the number of instantiations with which the adversary interacts. A master key $k \xleftarrow{\$} \mathcal{K}'$ is generated for use in the key derivation function (KDF) $F : \mathcal{K}' \times \mathcal{X} \to \mathcal{K}$, which maps the master key along with what we call an ID in $x \in \mathcal{X}$, to a key in $\mathcal{K}$. Here, the different IDs correspond to the different instances in the multi-key setting. The adversary can adaptively choose IDs via the oracle $\widetilde{E}_{F(k,\cdot)}$, where the ID is input via $F(k, \cdot)$. The adversary can instantiate at most μ IDs. The ideal functionality corresponding to $\widetilde{E}_{F(k,\cdot)}$ is $\widetilde{\pi}_{(\cdot)}$, which is formalized as a tweakable permutation with tweak space $\mathcal{T} \times \mathcal{X}$: the subscript input $(\cdot)$ can be viewed as a tweak input from $\mathcal{X}$ which specifies the selected user, which in turn specifies a particular tweakable permutation to use. Figure 2 depicts the oracles with which distinguisher $\mathcal{D}$ interacts.

Definition 2 (*TMK security*) Let $\mu \geq 1$. Consider tweakable blockcipher $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$ based on $r \geq 1$ primitives $\Pi_1, \ldots, \Pi_r \in \mathsf{Prims}$, and let $F : \mathcal{K}' \times \mathcal{X} \to \mathcal{K}$ with $|\mathcal{X}| \geq \mu$ be a KDF. The TMK advantage of a distinguisher $\mathcal{D}$ is

$$\begin{aligned}\mathbf{Adv}^{\mathsf{tmk}}_{\widetilde{E},F}(\mathcal{D}) &= \Delta_{\mathcal{D}}\left(\widetilde{E}_{F(k,\cdot)}, \Pi \;;\; \widetilde{\pi}_{(\cdot)}, \Pi\right) \\ &= \left|\mathbf{Pr}\left(\mathcal{D}^{\widetilde{E}_{F(k,\cdot)},\Pi} = 1\right) - \mathbf{Pr}\left(\mathcal{D}^{\widetilde{\pi}_{(\cdot)},\Pi} = 1\right)\right| ,\end{aligned}$$

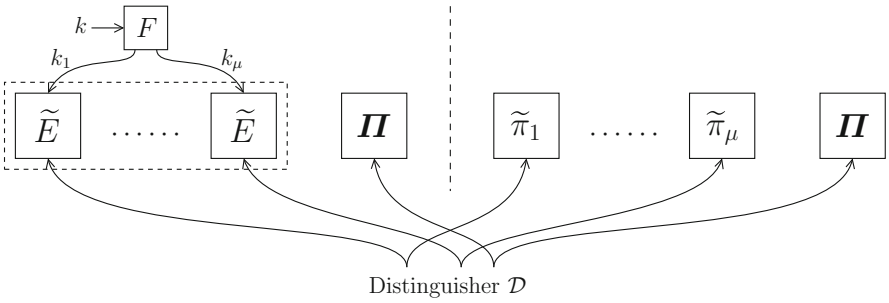

Fig. 2 Multi-key security model (Definition 2). $k_1, \ldots, k_\mu$ are the μ derived keys

where the probabilities are taken over the random choices of $k \xleftarrow{\$} \mathcal{K}'$, $\Pi \xleftarrow{\$} \mathsf{Prims}^r$, and $\widetilde{\pi}_{(\cdot)} \xleftarrow{\$} \mathsf{TPerm}(\mathcal{T} \times \mathcal{X}, \mathcal{M})$. The distinguisher has two-sided query access to each of its oracles. For any $\mu, q, \ell, p \geq 0$, we define $\mathbf{Adv}^{\mathsf{tmk}}_{\widetilde{E},F}(\mu, q, \ell, p)$ to be the maximum advantage over any distinguisher $\mathcal{D}$ that makes at most q queries to the μ constructions (in whatever distribution), for at most ℓ different tweaks per construction, and p queries to each of the primitives.

3.1 Compatibility with prior definitions

The original multi-key definition of Mouha and Luykx [64] can be viewed as a special case of Definition 2, by considering non-tweakable blockciphers with keys generated using a uniformly random KDF, that is, $\mathsf{F}^{\mathcal{X}}_{\mathcal{K}}$ of (1). Definition 1, conventional STPRP security, is a special case of Definition 2 as well, seen by putting $\mu = 1$ and taking the KDF to be $\mathsf{F}^{\mathcal{X}}_{\mathcal{K}}$ again:

$$\mathbf{Adv}^{\mathsf{tmk}}_{\widetilde{E},\mathsf{F}^{\mathcal{X}}_{\mathcal{K}}}(\mathcal{D}) = \mathbf{Adv}^{\mathsf{stprp}}_{\widetilde{E}}(\mathcal{D})\,.$$

Note that, as with our definition of STPRP security, we explicitly include primitives with which the adversary can interact. This is in order to capture ideal model definitions and proofs, but standard model definitions are also included by only considering adversaries which make zero queries to the primitives.

Due to the generalized nature of our definition, it is in fact *equivalent* to the definition of related-key security of (tweakable) blockciphers [10,21,32], although the applications structurally differ in the types of key derivation functions considered. Particularly, related-key security targets simple KDFs, often as simple as bitwise XOR or bitwise addition, while for multi-key security the KDFs are usually stronger primitives, and in most cases are pseudorandom. Nevertheless, the obvious equivalence between related-key security and our generalized multi-key security definition hints at the existence of more applications of our work in the context of related-key security, although this direction is beyond the scope of our work.

3.2 On multi-key-derivation functions

Taking a uniformly random KDF is, naturally, the most secure way of multi-key derivation, but it requires a lot of randomness. Definition 2 allows us to consider more general KDFs, including universal hash functions and pseudorandom number generators.

When choosing a KDF which is not pseudorandom, caution is needed to prevent related-key attacks when users are malicious. Particularly, if too many multi-keys are derived with the master key, the application may be prone to attacks. For example, taking a counter as KDF, $F(k, x) = k \oplus x$, allows for users to derive each others' keys without knowledge of the master key, as for any x, x' we have $F(k, x') = F(k, x) \oplus x \oplus x'$. More generally, it is desirable that F generates multi-keys that have enough entropy, even conditioned on a small set of other multi-keys. In other words, it should not be possible for a small set of malicious users to collude and compute the keys of the honest users. One solution to this issue is via γ-strongly universal hash functions, as introduced by Wegman and Carter [78]. In more detail, let $1 \leq \gamma \leq \mu$, and consider KDF $F : \mathcal{K}^{\gamma} \times \mathcal{X} \to \mathcal{K}$ defined as

$$F(k^{(1)} \| k^{(2)} \| \cdots \| k^{(\gamma)}, x) = \bigoplus_{i=1}^{\gamma} x^i \cdot k^{(i)}\,.$$

It is impossible for any set of $\gamma - 1$ colluding users to obtain the keys of the remaining honest users. On the other hand, any γ colluding users $\{x_1, \ldots, x_\gamma\}$ can recover the master key $k^{(1)} \| \cdots \| k^{(\gamma)}$ by invertibility of the Vandermonde matrix:

$$\begin{pmatrix} k^{(1)} \\ k^{(2)} \\ \vdots \\ k^{(\gamma)} \end{pmatrix} = \begin{pmatrix} x_1^1 & x_1^2 & \cdots & x_1^\gamma \\ x_2^1 & x_2^2 & \cdots & x_2^\gamma \\ \vdots & \vdots & \ddots & \vdots \\ x_\gamma^1 & x_\gamma^2 & \cdots & x_\gamma^\gamma \end{pmatrix}^{-1} \begin{pmatrix} k_{x_1} \\ k_{x_2} \\ \vdots \\ k_{x_\gamma} \end{pmatrix} .$$

Other examples of γ-universal hash functions for general γ include tabulation hashing and extensions [72,79]. For the specific case of $\gamma = 2$, examples abound [8,23,24,40,50,76].

On a more general note, we remark that typically stand-alone key derivation functions are multi-purpose, with main application the key derivation from passwords and salts. We refer to Yao and Yin [35], Krawczyk [43,49], and ISO-18033-3 [47] for various designs and analyses.

4 Tweakable blockciphers versus multi-key security

By introducing KDF's in the definition of multi-key security of blockciphers, the connection between multi-key security and tweakable security of blockciphers is nearly immediate: an ID can be viewed as a tweak, and a tweak can be viewed as an ID. Hence, taking a blockcipher $E : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$ and a KDF $F : \mathcal{K}' \times \mathcal{T} \to \mathcal{K}$, we can define the tweakable blockcipher $\widetilde{E} : \mathcal{K}' \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$ which identifies tweaks in $\mathcal{T}$ with IDs in $\mathcal{X}$, that is

$$\widetilde{E}_k(t, m) = E_{F(k,t)}(m) . \tag{2}$$

This construction can be seen as a generalization of Minematsu's tweakable blockcipher [63], but it has many more applications. In fact, extracting a blockcipher E from a tweakable blockcipher $\widetilde{E}$ by reversing the above construction is sometimes possible as well. For example, if E is the Even–Mansour construction of Sect. 5.1, and F is a UAXU family of hash functions, then $\widetilde{E}$ corresponds to the Tweakable Even–Mansour construction of Sect. 5.2.

A distinguisher $\mathcal{D}_1$ attacking the MK security of E with respect to F can be converted into a distinguisher $\mathcal{D}_2$ attacking the STPRP security of $\widetilde{E}$, by mapping each ID queried by $\mathcal{D}_1$ into a tweak queried by $\mathcal{D}_2$. Conversely, any STPRP distinguisher $\mathcal{D}_2$ can be converted into a MK distinguisher $\mathcal{D}_1$ by using the reverse transformation, namely, map each tweak into a different ID. Formally, we achieve the following theorem.

Theorem 1 *Let $E : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$ be a blockcipher, $F : \mathcal{K}' \times \mathcal{T} \to \mathcal{K}$ a KDF, and $\widetilde{E}$ the construction from (2). Let $\mu \geq 1$ and $q, \ell, p \geq 0$. If $\mu \leq \ell$, then,*

$$\mathbf{Adv}^{\mathsf{mk}}_{E,F}(\mu, q, p) \leq \mathbf{Adv}^{\mathsf{stprp}}_{\widetilde{E}}(q, \ell, p) .$$

If $\ell \leq \mu$, then,

$$\mathbf{Adv}^{\mathsf{stprp}}_{\widetilde{E}}(q, \ell, p) \leq \mathbf{Adv}^{\mathsf{mk}}_{E,F}(\mu, q, p) .$$

Proof Let $\mathcal{D}_1$ be a MK distinguisher against E with respect to F, and let $\mathcal{D}_2$ be described as above, namely, each input m made to ID $t \in \mathcal{T}$ is converted into a $\widetilde{E}$-query (t, m) with tweak t and input m. All primitive queries and $\mathcal{D}_1$'s final decision are forwarded by $\mathcal{D}_2$. Note

that $E_{F(k,\cdot)} = \widetilde{E}_k^{(\cdot)}$, where the ID input of E is changed to tweak input for $\widetilde{E}$. Similarly, a permutation $\pi_{(\cdot)}$ with ID input, is equivalent to a tweakable permutation $\widetilde{\pi}$ where the IDs are mapped to tweaks. This means we have,

$$\begin{aligned}\mathbf{Adv}^{\mathsf{mk}}_{E,F}(\mathcal{D}_1) &= \Delta_{\mathcal{D}_1}(E_{F(k,\cdot)}, \Pi \;;\; \pi_{(\cdot)}, \Pi) \\ &= \Delta_{\mathcal{D}_2}(\widetilde{E}_k, \Pi \;;\; \widetilde{\pi}, \Pi) = \mathbf{Adv}^{\mathsf{stprp}}_{\widetilde{E}}(\mathcal{D}_2)\,,\end{aligned}$$

and since $\mu \le \ell$, we establish

$$\mathbf{Adv}^{\mathsf{mk}}_{E,F}(\mu, q, p) \le \mathbf{Adv}^{\mathsf{stprp}}_{\widetilde{E}}(q, \ell, p)\,.$$

The reverse inequality can be obtained similarly. □

5 Application of equivalence of Sect. 4

We briefly summarize the state of the art on iterated Even–Mansour (Sect. 5.1), Tweakable Even–Mansour (Sect. 5.2), and LRW (Sect. 5.3). Then, we consider the application of the equivalence of Sect. 4 to these constructions in Sect. 5.4.

5.1 Iterated Even–Mansour

For $r \ge 1$, we define the r-round iterated Even–Mansour construction $\mathrm{EM}[r] : \{0,1\}^{(r+1)n} \times \{0,1\}^n \to \{0,1\}^n$ as (see also Fig. 1)

$$\mathrm{EM}[r]_{k_1,\ldots,k_{r+1}}(m) = P_r(\cdots P_1(m \oplus k_1) \cdots \oplus k_r) \oplus k_{r+1}\,, \tag{3}$$

where $\mathbf{P} = (P_1, \ldots, P_r) \in \mathsf{Perm}(\{0,1\}^n)^r$ are n-bit permutations. The first formal presentation of this construction is by Even and Mansour at ASIACRYPT '91 [30,31], who introduced it for $r = 1$ and proved that it achieves $2^{n/2}$ security. Daemen proved tightness of this bound [22]. The general construction was introduced by Bogdanov et al. [11]. Following a line of research set, among others, by Dunkelman et al. [25], Lampe et al. [52], and Steinberger [74], Chen and Steinberger [19] proved that $\mathrm{EM}[r]$ tightly achieves $\mathcal{O}(2^{rn/(r+1)})$ single-key blockcipher security in the model of Sect. 2.1. This bound is, however, asymptotic, and Hoang and Tessaro [42] recently improved their bound on $\mathrm{EM}[r]$.

Proposition 1 (Single-Key Security of EM $[r]$ [19,42]) *Let $r \ge 1$ and $q, p \ge 0$. Then,*

$$\mathbf{Adv}^{\mathsf{sprp}}_{\mathrm{EM}[r]}(q, p) \le \frac{q(4p)^r}{(2^n)^r}\,. \tag{4}$$

Their bound is in fact a bit more fine-grained, having p separated over all r primitives. It is important that the results on $\mathrm{EM}[r]$ [19,42] effectively require r-wise independency of the key, i.e., for any $i \in \{1, \ldots, r+1\}$, $(k_1, \ldots, k_{i-1}, k_{i+1}, \ldots, k_{r+1})$ has a uniform distribution on $\{0,1\}^{rn}$ [19, p. 329].

Andreeva et al. [3] and Mouha and Luykx [64] considered one round of Even–Mansour in the multi-key setting, and showed that similar results are achieved.

Proposition 2 (Multi-Key Security of EM[1] [64]) *Consider $F = \mathsf{F}_n^{\mathcal{X}}$ of (1). Let $\mu \ge 1$ and $q, p \ge 0$. Then,*

$$\mathbf{Adv}^{\mathsf{mk}}_{\mathrm{EM}[1],\mathsf{F}_n^{\mathcal{X}}}(\mu, q, p) \le \frac{q^2 + 2qp}{2^n}\,.$$

Hoang and Tessaro [42] derived a strong generic reduction from multi-key to single-key security and transferred their result (Proposition 1) to the multi-key setting.

Proposition 3 (Multi-Key Security of EM[r] [42]) *Consider* $F = \mathsf{F}_n^{\mathcal{X}}$ *of* (1). *Let* $\mu \geq 1$, $r \geq 1$, *and* q, $p \geq 0$. *Then,*

$$\mathbf{Adv}^{\mathsf{mk}}_{\mathrm{EM}[r],\mathsf{F}_n^{\mathcal{X}}}(\mu, q, p) \leq \frac{2q(4(p+rq))^r}{(2^n)^r} .$$

Beyond single-key and multi-key security, further works on EM[r] cover the related-key security [21,32], chosen-key security [1,38,54], and security of minimized EM[2] [15].

5.2 Iterated tweakable Even–Mansour

At CRYPTO 2015, Cogliati et al. [16] introduced the generic Tweakable Even–Mansour construction based on universal hash functions. For a permutation $P \in \mathsf{Perm}(\{0,1\}^n)$ and a universal hash function $h_k : \mathcal{T} \to \{0,1\}^n$, define

$$\Psi[P](k, t, m) = h_k(t) \oplus P(m \oplus h_k(t)) .$$

For $r \geq 1$, we define the r-round iterated Tweakable Even–Mansour construction $\mathrm{TEM}[r] : \mathcal{K}^r \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ as (see also Fig. 1)

$$\begin{aligned} \mathrm{TEM}[r]_{k_1,\ldots,k_r}(t, m) &= \Psi[P_r](k_r, t, \cdots \Psi[P_1](k_1, t, m) \cdots) \\ &= P_r(\cdots P_1(m \oplus h_{k_1}(t)) \oplus h_{k_1}(t) \cdots \oplus h_{k_r}(t)) \oplus h_{k_r}(t), \end{aligned} \quad (5)$$

where $\mathbf{P} = (P_1, \ldots, P_r) \in \mathsf{Perm}(\{0,1\}^n)^r$ are n-bit permutations, and $H = \{h_k : \mathcal{T} \to \{0,1\}^n \mid k \in \mathcal{K}\}$ is a uniform almost-XOR-universal hash function family. Cogliati et al. [16] derived the following security results for TEM[r].

Proposition 4 (Single-Key Security of TEM[r] [16]) *Let* $H = \{h_k : \mathcal{T} \to \{0,1\}^n \mid k \in \mathcal{K}\}$ *be an* ε*-UAXU family of hash functions. Let* $r \geq 1$ *and* $q, \ell, p \geq 0$. *Then,*

$$\begin{aligned} \mathbf{Adv}^{\mathsf{stprp}}_{\mathrm{TEM}[1]}(q, \ell, p) &\leq q^2\varepsilon + \frac{2qp}{2^n} , \\ \mathbf{Adv}^{\mathsf{stprp}}_{\mathrm{TEM}[2]}(q, \ell, p) &\leq \frac{29q^{1/2}p}{2^n} + q^{1/2}p\varepsilon + 4q^{3/2}\varepsilon + \frac{30q^{3/2}}{2^n} , \\ \mathbf{Adv}^{\mathsf{stprp}}_{\mathrm{TEM}[2r]}(q, \ell, p) &\leq 4q^{1/2}\left(2q\varepsilon + \frac{2p}{2^n}\right)^{r/2} . \end{aligned}$$

Note that TEM[r] is in fact the EM[r] construction where the keys $(k_1, \ldots, k_{r+1})$ are replaced with

$$h_{k_1}(t) , \; h_{k_1}(t) \oplus h_{k_2}(t) , \; \ldots , \; h_{k_{r-1}}(t) \oplus h_{k_r}(t) , \; h_{k_r}(t) . \quad (6)$$

In particular, TEM[r] also has r-wise independent masking, be it of a specific form.

Further constructions related to TEM[r], and to which our findings can be applied as well, are XPX [59], MEM [37], and a variant of TEM[4] with linear mixing [20].

5.3 Iterated LRW

The Tweakable Even–Mansour construction is closely related to the iterated LRW construction [53]. In more detail, the r-round LRW[r] construction is based on r blockcipher calls instead of r permutations. It is defined identically as in (5), with $P_1, \ldots, P_r$ instantiated as

$E_{z_1}, \ldots, E_{z_r}$ for independent keys $z_1, \ldots, z_r$.We can likewise use the definition of STPRP security of Definition 1 where, now, p bounds the total number of evaluations of E a distinguisher can make. A security analysis for $r = 1$ was performed by Liskov et al. [53], $r = 2$ by Landecker et al. [56] and Procter [67], and for a general number of even rounds by Lampe and Seurin [55]. These results on LRW[r] are comparable to the bounds of Proposition 4, which should not be surprising as

$$\mathbf{Adv}^{\mathsf{stprp}}_{\mathrm{LRW}[r]}(q, \ell, p) \le \mathbf{Adv}^{\mathsf{stprp}}_{\mathrm{TEM}[r]}(q, \ell, 0) + r \cdot \mathbf{Adv}^{\mathsf{sprp}}_{E}(q, p)\,. \tag{7}$$

The derivation of this bound is fairly straightforward: first, replace the blockcipher calls $E_{z_1}, \ldots, E_{z_r}$ by r independent *secret* permutations $P_1, \ldots, P_r$. This step costs at most $r \cdot \mathbf{Adv}^{\mathsf{sprp}}_{E}(q, p)$. What remains is the TEM[r] construction with the difference that the adversary has no access to the secret underlying permutations, hence we have $p = 0$: $\mathbf{Adv}^{\mathsf{stprp}}_{\mathrm{TEM}[r]}(q, \ell, 0)$. See also [16, Remark 1].

Further constructions related to LRW[1] include the XEX construction [71] and its generalizations [18,37,62], tweakable Feistel schemes [36,60], and tweakable blockciphers with tweak-dependent rekeying [58,61,63].

5.4 Application of equivalence of Sect. 4

Theorem 1 along with Proposition 4 implies multi-key security of EM[r] with KDF $F : (\mathcal{K})^r \times \mathcal{X} \to \{0,1\}^{(r+1)n}$ defined as (see also (6))

$$F(k_1, \ldots, k_r, x) = \big(h_{k_1}(x), h_{k_1}(x) \oplus h_{k_2}(x), \ldots, h_{k_{r-1}}(x) \oplus h_{k_r}(x), h_{k_r}(x)\big), \tag{8}$$

where $H = \{h_k : \mathcal{X} \to \{0,1\}^n \mid k \in \mathcal{K}\}$ is an ε-UAXU family of hash functions. Note that F is not UAXU itself, but it is still sufficiently strong to achieve multi-key security of EM[r]. Although F's outputs admit a specific type of r-wise independence, it is clear to see that the result immediately generalizes to any F which outputs r-wise independent keys with the same joint distribution.

Corollary 1 *Consider F of (8). Let $\mu \ge 1$, $r \ge 1$, and $q, p \ge 0$. Then,*

$$\mathbf{Adv}^{\mathsf{mk}}_{\mathrm{EM}[1],F}(\mu, q, p) \le q^2\varepsilon + \frac{2qp}{2^n}\,,$$

$$\mathbf{Adv}^{\mathsf{mk}}_{\mathrm{EM}[2],F}(\mu, q, p) \le \frac{29q^{1/2}p}{2^n} + q^{1/2}p\varepsilon + 4q^{3/2}\varepsilon + \frac{30q^{3/2}}{2^n}\,,$$

$$\mathbf{Adv}^{\mathsf{mk}}_{\mathrm{EM}[2r],F}(\mu, q, p) \le 4q^{1/2}\left(2q\varepsilon + \frac{2p}{2^n}\right)^{r/2}\,.$$

Note that the result of Proposition 3 is better than that of Corollary 1, but it explicitly requires random key-derivation while Corollary 1 allows for a more flexible key-derivation.

By using the equivalence reduction of Theorem 1 in reverse direction, we can transfer Proposition 3 to the security of Tweakable Even–Mansour TEM[r].

Corollary 2 *Consider the 2^{-n}-UAXU family of hash functions $\mathsf{F}^{\mathcal{T}}_n$ of (1). Let $r \ge 1$ and $q, \ell, p \ge 0$. Then,*

$$\mathbf{Adv}^{\mathsf{stprp}}_{\mathrm{TEM}[r]}(q, \ell, p) \le \frac{2q(4(p + rq))^r}{(2^n)^r}\,.$$

Similarly, for LRW[r], we can find via (7) the following corollary.

Corollary 3 *Let $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a blockcipher, and consider the 2^{-n}-UAXU family of hash functions $\mathsf{F}_n^{\mathcal{T}}$ of (1). Let $r \geq 1$ and $q, \ell, p \geq 0$ such that $q + p \leq 2^n/3$. Then,*

$$\mathbf{Adv}^{\mathsf{stprp}}_{\mathrm{LRW}[r]}(q, \ell, p) \leq \frac{2q(4(p+rq))^r}{(2^n)^r} + r \cdot \mathbf{Adv}^{\mathsf{sprp}}_{E}(q, p)\,.$$

As a matter of fact, the two corollaries apply to TEM[r] and LRW[r] *for any form of r-wise independence keying* (not just (6)). Clearly, for $r = 1$ and $r = 2$, above corollaries do not improve over the state of the art for LRW[r] [53,55,56] and TEM[r] [21]. On the other hand, for $r \geq 3$, the corollaries solve the conjectures on the two schemes for a specific scenario: the UAXU family of hash functions is $\mathsf{F}_n^{\mathcal{T}}$ of (1).

6 Tweakable blockciphers versus related-key security

The first formalization of related-key security was by Bellare and Kohno [10]. Cogliati and Seurin [21] generalized the model to blockciphers and applied it to cascaded Even–Mansour (cf. Sect. 5.1). Mennink [59] provided a formalism for the case of tweakable blockcipher constructions.

The definition of related-key security is in fact strongly related to that of multi-key security of Sect. 3. In related-key attacks, a set of related-key-deriving functions Φ is defined prior to the experiment. The adversary can adaptively choose related-key functions φ from Φ that transform the key under which the query is made: $\widetilde{E}_{\varphi(k)}$. As such, one can specifically see related-key security as multi-key security using key derivation function $F : \mathcal{K} \times \Phi \to \mathcal{K}$ defined as $F(k, \varphi) = \varphi(k)$. The ideal functionality corresponding to $\widetilde{E}_{F(k,\cdot)}$ is $\widetilde{\pi}_{(\cdot)}$, which is formalized as a tweakable permutation with tweak space $\mathcal{T} \times \Phi$: the subscript input $(\cdot)$ can be viewed as a tweak input from Φ which specifies the selected user, which in turn specifies a particular tweakable permutation to use.

Definition 3 (*TRK security*) Let Φ be a set of related-key-deriving functions. Consider tweakable blockcipher $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$ based on $r \geq 1$ primitives $\Pi_1, \ldots, \Pi_r \in \mathsf{Prims}$, and let $F : \mathcal{K} \times \Phi \to \mathcal{K}$ be defined as $F(k, \varphi) = \varphi(k)$. The TRK advantage of a distinguisher $\mathcal{D}$ is

$$\begin{aligned}\mathbf{Adv}^{\mathsf{trk}}_{\widetilde{E},\Phi}(\mathcal{D}) &= \Delta_{\mathcal{D}}\left(\widetilde{E}_{F(k,\cdot)}, \Pi \;;\; \widetilde{\pi}_{(\cdot)}, \Pi\right) \\ &= \left|\mathbf{Pr}\left(\mathcal{D}^{\widetilde{E}_{F(k,\cdot)},\Pi} = 1\right) - \mathbf{Pr}\left(\mathcal{D}^{\widetilde{\pi}_{(\cdot)},\Pi} = 1\right)\right|\,,\end{aligned}$$

where the probabilities are taken over the random choices of $k \xleftarrow{\$} \mathcal{K}$, $\Pi \xleftarrow{\$} \mathsf{Prims}^r$, and $\widetilde{\pi}_{(\cdot)} \xleftarrow{\$} \mathsf{TPerm}(\mathcal{T} \times \Phi, \mathcal{M})$. The distinguisher has two-sided query access to each of its oracles. For any $q, \ell, p \geq 0$, we define $\mathbf{Adv}^{\mathsf{trk}}_{\widetilde{E},\Phi}(q, \ell, p)$ to be the maximum advantage over any distinguisher $\mathcal{D}$ that makes at most q queries to the construction for at most ℓ different related-key-deriving functions per construction, and p queries to each of the primitives.

6.1 On related-key-derivation functions

If Φ simply consists of the identity function, $\Phi = \{\varphi : k \mapsto k\}$, Definition 3 boils down to conventional STPRP security, Definition 1:

$$\mathbf{Adv}^{\mathsf{trk}}_{\widetilde{E},\{\varphi:k\mapsto k\}}(\mathcal{D}) = \mathbf{Adv}^{\mathsf{stprp}}_{\widetilde{E}}(\mathcal{D})\,.$$

Two well-known sets of related-key-deriving functions [10,45] are the XOR and additive differences on the keys:

$$\Phi_{\oplus} = \{\varphi_\delta : k \mapsto k \oplus \delta \mid \delta \in \mathcal{K}\},$$
$$\Phi_{+} = \{\varphi_\delta : k \mapsto k + \delta \mid \delta \in \mathcal{K}\},$$

where $+$ denotes modular addition. More involved sets of related-key-deriving functions where the functions may depend on the cryptographic primitives are discussed in [4,59].

6.2 Relation

The relation between tweakable blockciphers and the related-key security of conventional blockciphers was already pointed out by Cogliati et al. [16,20,21]. At a high level, they suggest that if a blockcipher $E : \mathcal{K} \times \mathcal{M} \to \mathcal{M}$ is related-key secure for related-key-deriving functions Φ, then the tweakable blockcipher $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$ with $\mathcal{T} = \Phi$, that is defined as

$$\widetilde{E}_k(\phi, m) = E_{\phi(k)}(m), \tag{9}$$

is an equally secure tweakable blockcipher:

$$\mathbf{Adv}^{\mathsf{stprp}}_{\widetilde{E}}(q, \ell, p) = \mathbf{Adv}^{\mathsf{rk}}_{E,\Phi}(q, \ell, p),$$

for any q, ℓ, p. As a matter of fact, Cogliati et al. restrict their observation to XOR-induced related-key-deriving functions $\Phi_{\oplus}$ of Sect. 6.1, but their observation straightforwardly generalizes. Lucks [57] and Tessaro [77] considered constructions comparable to (9), albeit not in the context of tweakable blockciphers.

However, the reverse direction appears to be underexposed, despite its seemingly broad spectrum of potential applications. Assume we have a tweakable blockcipher $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$, and define a blockcipher $E : (\mathcal{K} \times \mathcal{T}) \times \mathcal{M} \to \mathcal{M}$ as

$$E_{k\|t}(m) = \widetilde{E}_k(t, m). \tag{10}$$

Then, for the set of related-key-deriving functions

$$\Phi_{\mathrm{id}\|\oplus} = \{\varphi_\delta : k\|t \mapsto k\|(t \oplus \delta) \mid \delta \in \mathcal{T}\},$$

which can be seen as a set of partially-transforming related-key-deriving functions in the terminology of Lucks [57], we can derive the following result.

Theorem 2 *Let $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$ be a tweakable blockcipher, and E the construction from (10). Let $q, \ell, p \geq 0$. Then,*

$$\mathbf{Adv}^{\mathsf{rk}}_{E,\Phi_{\mathrm{id}\|\oplus}}(q, \ell, p) \leq \mathbf{Adv}^{\mathsf{stprp}}_{\widetilde{E}}(q, \ell, p).$$

Proof Let $\mathcal{D}_1$ be a RK distinguisher against E with respect to $\Phi_{\mathrm{id}\|\oplus}$. Let $\mathcal{D}_2$ be as follows: first, it selects a random tweak t. Then, each query (δ, m) made by $\mathcal{D}_1$ (we can without loss of generality describe an element $\varphi_\delta \in \Phi_{\mathrm{id}\|\oplus}$ by δ) is transformed into a query $(t \oplus \delta, m)$ to $\widetilde{E}$, and the response is relayed. $\mathcal{D}_1$'s final decision is forwarded by $\mathcal{D}_1$. By design,

$$\mathbf{Adv}^{\mathsf{rk}}_{E,\Phi_{\mathrm{id}\|\oplus}}(\mathcal{D}_1) = \mathbf{Adv}^{\mathsf{stprp}}_{\widetilde{E}}(\mathcal{D}_2)\,,$$

and the result is established by maximizing over all distinguishers with complexity (q, ℓ, p). □

We can use this construction to allow for multiple instances of blockcipher E under related keys, by keeping the master key k the same, and changing t for all users. For instance, if μ instances of E are required, these could be generated via the following offsets:

$$E_{k\|t}\,,\ E_{k\|t\oplus 1}\,,\ \ldots\,,\ E_{k\|t\oplus\mu-1}\,.$$

7 Conclusion

Our research illustrates how placing existing security definitions in a different context can lead to fruitful insights. After extending the definition of blockcipher multi-key security to include KDFs, the connection with tweakable blockcipher security immediately follows, and with it the connections to related-key security and the security of blockcipher key schedules. We applied these connections to illustrate how results on the iterated Even–Mansour and the iterated Tweakable Even–Mansour can be transferred between each other, resulting in new theoretical results. Furthermore, our definitions and results pave the way to understanding the design of KDFs, in particular, ones which are not necessarily PRFs. We saw how the KDFs can be implemented as universal hash functions, which could result in efficiency improvements in practice.

Acknowledgements This work was supported in part by the Research Council KU Leuven: GOA TENSE (GOA/11/007). Jooyoung Lee is supported by a Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2013R1A1A2007488). Atul Luykx is supported by a Fellowship from the Institute for the Promotion of Innovation through Science and Technology in Flanders (IWT-Vlaanderen). Bart Mennink is supported by a postdoctoral fellowship from the Netherlands Organisation for Scientific Research (NWO) under Veni grant 016.Veni.173.017. Core ideas of this work have been developed during the Asian Workshop on Symmetric Key Cryptography 2015.

References

1. Andreeva E., Bogdanov A., Dodis Y., Mennink B., Steinberger J.P.: On the indifferentiability of key-alternating ciphers. In: Canetti R., Garay J.A. (eds.) CRYPTO 2013. LNCS, Part I, vol. 8042, pp. 531–550. Springer, Heidelberg (2013).
2. Andreeva E., Bogdanov A., Luykx A., Mennink B., Tischhauser E., Yasuda K.: Parallelizable and authenticated online ciphers. In: Sako K., Sarkar P. (eds.) ASIACRYPT 2013. LNCS, Part I, vol. 8269, pp. 424–443. Springer, Heidelberg (2013).
3. Andreeva E., Daemen J., Mennink B., Van Assche G.: Security of keyed sponge constructions using a modular proof approach. In: Leander G. (ed.) FSE 2015. LNCS, vol. 9054, pp. 364–384. Springer, Heidelberg (2015).
4. Albrecht M.R., Farshim P., Paterson K.G., Watson G.J.: On cipher-dependent related-key attacks in the ideal-cipher model. In: Joux A. (ed.) FSE 2011. LNCS, vol. 6733, pp. 128–145. Springer, Heidelberg (2011).

5. Bellare M., Boldyreva A., Micali S.: Public-key encryption in a multi-user setting: security proofs and improvements. In: Preneel B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 259–274. Springer, Heidelberg (2000).
6. Bellare M., Bernstein D.J., Tessaro S.: Hash-function based PRFs: AMAC and its multi-user security. In: Fischlin M., Coron J.-S. (eds.) EUROCRYPT 2016. LNCS, Part I, vol. 9665, pp. 566–595. Springer, Heidelberg (2016).
7. Biham E.: How to decrypt or even substitute DES-encrypted messages in 2^{28} steps. Inf. Process. Lett. **84**(3), 117–124 (2002).
8. Bierbrauer J., Johansson T., Kabatianskii G., Smeets B.J.M.: On families of hash functions via geometric codes and concatenation. In: Stinson D.R. (ed.) CRYPTO'93. LNCS, vol. 773, pp. 331–342. Springer, Heidelberg (1994).
9. Blake-Wilson S., Johnson D., Menezes A.: Key agreement protocols and their security analysis. In: Darnell M. (ed.) Cryptography and Coding 1997. LNCS, vol. 1355, pp. 30–45. Springer, Heidelberg (1997).
10. Bellare M., Kohno T.: A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. In: Biham E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 491–506. Springer, Heidelberg (2003).
11. Bogdanov A., Knudsen L.R., Leander G., Standaert F.-X., Steinberger J.P., Tischhauser E.: Key-alternating ciphers in a provable setting: encryption using a small number of public permutations—(extended abstract). In: Pointcheval D., Johansson T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 45–62. Springer, Heidelberg (2012).
12. Biryukov A., Mukhopadhyay S., Sarkar P.: Improved time-memory trade-offs with multiple data. In: Preneel B., Tavares S.E. (eds.) SAC 2005. LNCS, vol. 3897, pp. 110–127. Springer, Heidelberg (2005).
13. Bellare M., Rogaway P.: Entity authentication and key distribution. In: CRYPTO'93. LNCS, vol. 773, pp. 232–249. Springer, Heidelberg (1994).
14. Biham E., Youssef A.M. (eds.): SAC 2006. LNCS, vol. 4356. Springer, Heidelberg (2007).
15. Chen S., Lampe R., Lee J., Seurin Y., Steinberger J.P.: Minimizing the two-round Even-Mansour cipher. In: Garay J.A., Gennaro R. (eds.) CRYPTO 2014. LNCS Part I, vol. 8616, pp. 39–56. Springer, Heidelberg (2014).
16. Cogliati B., Lampe R., Seurin Y.: Tweaking Even-Mansour ciphers. In: Gennaro R., Robshaw M. (eds.) CRYPTO 2015, Part I, vol. 9215, pp. 189–208. Springer, Heidelberg, (2015).
17. Chatterjee S., Menezes A., Sarkar P.: Another look at tightness. In: Miri A., Vaudenay S. (eds.) SAC 2011. LNCS, vol. 7118, pp. 293–319. Springer, Heidelberg (2011).
18. Chakraborty D., Sarkar P.: A general construction of tweakable block ciphers and different modes of operations. In: Lipmaa H., Yung M., Lin D. (eds.) Inscrypt 2006. LNCS, vol. 4318, pp. 88–102. Springer, Heidelberg (2006).
19. Chen S., Steinberger J.P.: Tight security bounds for key-alternating ciphers. In: Nguyen P.Q., Oswald E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 327–350. Springer, Heidelberg (2014).
20. Cogliati B., Seurin Y.: Beyond-birthday-bound security for tweakable Even-Mansour ciphers with linear tweak and key mixing. In: Iwata T., Cheon J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9453, pp. 134–158. Springer, Heidelberg (2015).
21. Cogliati B., Seurin Y.: On the provable security of the iterated Even-Mansour cipher against related-key and chosen-key attacks. In: Oswald E., Fischlin M. (eds.) EUROCRYPT 2015. LNCS, Part I, vol. 9056, pp. 584–613. Springer, Heidelberg (2015).
22. Daemen J.: Limitations of the Even-Mansour construction. In: Imai H., Rivest R.L., Matsumoto T. (eds.) ASIACRYPT'91. LNCS, vol. 739, pp. 495–498. Springer, Heidelberg (1993).
23. den Boer B.: A simple and key-economical unconditional authentication scheme. J. Comput. Secur. **2**, 65–72 (1993).
24. Daniel J.: Bernstein. The Poly1305-AES message-authentication code. In: Gilbert H., Handschuh H. (eds.) FSE 2005. LNCS, vol. 3557, pp. 32–49. Springer, Heidelberg (2005).
25. Dunkelman O., Keller N., Shamir A.: Minimalism in cryptography: the Even-Mansour scheme revisited. In: Pointcheval D., Johansson T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 336–354. Springer, Heidelberg (2012).
26. Datta N., Nandi M.: ELmE: A misuse resistant parallel authenticated encryption. In: Susilo W., Yi M. (eds.) ACISP 2014. LNCS, vol. 8544, pp. 306–321. Springer, Heidelberg (2014).
27. Daemen J., Rijmen V.: The wide trail design strategy. In: Bahram H. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 222–238. Springer, Heidelberg (2001).
28. Daemen J., Rijmen V.: The Design of Rijndael: AES—The Advanced Encryption Standard. Springer, Heidelberg (2002).
29. Daemen J., Rijmen V.: On the related-key attacks against aes. Proc. Rom. Acad. Ser. A **13**(4), 395–400 (2012).

30. Even S., Mansour Y.: A construction of a cipher from a single pseudorandom permutation. In: Imai H.,Rivest R.L., Matsumoto T. (eds.) ASIACRYPT'91. LNCS, vol. 739, pp. 210–224. Springer, Heidelberg (1993).
31. Even S., Mansour Y.: A construction of a cipher from a single pseudorandom permutation. J. Cryptol. **10**(3), 151–162 (1997).
32. Farshim P., Procter G.: The related-key security of iterated Even-Mansour ciphers. In: Leander G. (ed.) FSE 2015. LNCS, vol. 9054, pp. 342–363. Springer, Heidelberg (2015).
33. Fischlin M., Coron J.-S. (eds.): EUROCRYPT 2016. LNCS, Part I, vol. 9665. Springer, Heidelberg (2016).
34. Fouque P.-A., Joux A., Mavromati C.: Multi-user collisions: Applications to discrete logarithm, Even-Mansour and PRINCE. In: Sarkar P., Iwata T. (eds.) ASIACRYPT 2014. LNCS, Part I, vol. 8873, pp. 420–438. Springer, Heidelberg (2014).
35. Frances F.: Yao and Yiqun Lisa Yin. Design and analysis of password-based key derivation functions. In: Menezes A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 245–261. Springer, Heidelberg (2005).
36. Goldenberg D., Hohenberger S., Liskov M.: Elizabeth Crump Schwartz, and Hakan Seyalioglu. On tweaking Luby-Rackoff blockciphers. In: Kurosawa K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 342–356. Springer, Heidelberg (2007).
37. Granger R., Jovanovic P., Mennink B., Neves S.: Improved masking for tweakable blockciphers with applications to authenticated encryption. In: Fischlin M., Coron J.-S. (eds.) EUROCRYPT 2016. LNCS, Part I, vol. 9665, pp. 263–293. Springer, Heidelberg (2016).
38. Guo C., Lin D.: A synthetic indifferentiability analysis of interleaved double-key Even-Mansour ciphers. In: Iwata T., Cheon J.H. (eds.) ASIACRYPT 2015. LNCS, Part II, vol. 9453, pp. 389–410. Springer, Heidelberg (2015).
39. Gennaro R., Robshaw M. (eds.): CRYPTO 2015. LNCS, Part I, vol. 9215. Springer, Heidelberg (2015).
40. Halevi S., Krawczyk H.: MMH: software message authentication in the Gbit/second rates. In: Biham E. (ed.) FSE '97. LNCS, vol. 1267, pp. 172–189. Springer, Heidelberg (1997).
41. Hong J., Sarkar P.: New applications of time memory data tradeoffs. In: Roy B.K. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 353–372. Springer, Heidelberg (2005).
42. Hoang V.T., Tessaro S.: Key-alternating ciphers and key-length extension: exact bounds and multi-user security. In: Robshaw M., Katz J. (eds.) CRYPTO 2016. LNCS, Part I, vol. 9814, pp. 3–32. Springer, Heidelberg (2016).
43. Hugo K. HMAC-based extract-and-expand key derivation function (HKDF). Request for Comments (RFC) 5869, May (2010). https://tools.ietf.org/html/rfc5869.
44. Iwata T., Cheon J.H. (eds.): ASIACRYPT 2015. LNCS, Part II, vol. 9453. Springer, Heidelberg (2015).
45. Iwata T., Kohno T.: New security proofs for the 3GPP confidentiality and integrity algorithms. In: Roy B.K., Meier W. (eds.) FSE 2004. LNCS, vol. 3017, pp. 427–445. Springer, Heidelberg (2004).
46. Imai H., Rivest R.L., Matsumoto T. (eds.): ASIACRYPT '91. LNCS, vol. 739. Springer, Heidelberg (1993).
47. ISO/IEC 18033-3:2010. Information technology—security techniques—encryption algorithms—Part 3: Block ciphers, December (2010).
48. Jean J., Nikolić I., Peyrin T.: Tweaks and keys for block ciphers: The TWEAKEY framework. In: Sarkar P., Iwata T. (eds.) ASIACRYPT 2014. LNCS, Part II, vol. 8874, pp. 274–288. Springer, Heidelberg (2014).
49. Krawczyk H.: Cryptographic extraction and key derivation: the HKDF scheme. In: Rabin T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 631–648. Springer, Heidelberg (2010).
50. Krovetz, T.: Message authentication on 64-bit architectures. In: Biham E., Youssef A.M. (eds.) SAC 2006. LNCS, vol. 4356, pp. 327–341. Springer, Heidelberg (2007).
51. Leander G. (ed.): FSE 2015. LNCS, vol. 9054. Springer, Heidelberg (2015).
52. Lampe R., Patarin J., Seurin Y.: An asymptotically tight security analysis of the iterated Even-Mansour cipher. In: Wang X., Sako K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 278–295. Springer, Heidelberg (2012).
53. Liskov M., Rivest R.L., Wagner D.: Tweakable block ciphers. In: Yung M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 31–46. Springer, Heidelberg (2002).
54. Lampe R., Seurin Y.: How to construct an ideal cipher from a small set of public permutations. In Sako K., Sarkar P. (eds.) ASIACRYPT 2013. LNCS, Part I, vol. 8269, pp. 444–463. Springer, Heidelberg (2013).
55. Lampe R., Seurin Y.: Tweakable blockciphers with asymptotically optimal security. In: Moriai S. (ed.) FSE 2013. LNCS, vol. 8424, pp. 133–151. Springer, Heidelberg (2013).
56. Landecker W., Shrimpton T.: and R. Seth Terashima. Tweakable blockciphers with beyond birthday-bound security. In: Safavi-Naini R., Canetti R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 14–30. Springer, Heidelberg (2012).
57. Lucks S.: Ciphers secure against related-key attacks. In Roy B.K., Meier W. (eds.) FSE 2004. LNCS, vol. 3017, pp. 359–370. Springer, Heidelberg (2004).

58. Mennink B.: Optimally secure tweakable blockciphers. In: Leander G. (ed.) FSE 2015. LNCS, vol. 9054, pp. 428–448. Springer, Heidelberg (2015).
59. Mennink, B.: XPX: generalized tweakable Even-Mansour with improved security guarantees. In Robshaw M., Katz J. (eds.) CRYPTO 2016. LNCS, vol. 9814, pp. 64–94. Springer, Heidelberg (2016).
60. Mitsuda A., Iwata T.: Tweakable pseudorandom permutation from generalized Feistel structure. In: Baek J., Bao F., Chen K., Lai X. (eds.) Provable Security 2008. LNCS, vol. 5324, pp. 22–37. Springer, Heidelberg (2008).
61. Minematsu K., Iwata T.: Tweak-length extension for tweakable blockciphers. In: Groth J. (ed.) Cryptography and Coding 2015. LNCS, vol. 9496, pp. 77–93. Springer, Heidelberg (2015).
62. Minematsu, K..: Improved security analysis of XEX and LRW modes. In Biham E., Youssef A.M. (eds.) SAC 2006. LNCS, vol. 4356, pp. 96–113. Springer, Heidelberg (2007).
63. Minematsu K.: Beyond-birthday-bound security based on tweakable block cipher. In: Dunkelman O. (ed.) FSE 2009. LNCS, vol. 5665, pp. 308–326. Springer, Heidelberg (2009).
64. Mouha N., Luykx A.: Multi-key security: the Even-Mansour construction revisited. In Gennaro R., Robshaw M. (eds.) CRYPTO 2015. LNCS, Part I, vol. 9215, pp. 209–223. Springer, Heidelberg (2015)
65. Menezes A., Smart N.P.: Security of signature schemes in a multi-user setting. Des. Codes Cryptogr. **33**(3), 261–274 (2004).
66. Pointcheval D., Johansson T. (eds.): EUROCRYPT 2012. LNCS, vol. 7237. Springer, Heidelberg (2012).
67. Procter G.: A note on the CLRW2 tweakable block cipher construction. Cryptology ePrint Archive, Report 2014/111 (2014).
68. Peyrin T., Seurin Y.: Counter-in-Tweak: authenticated encryption modes for tweakable block ciphers. In: Robshaw M., Katz J. (eds.) CRYPTO 2016. LNCS, Part I, vol. 9814, pp. 33–63. Springer, Heidelberg (2016).
69. Robshaw M., Katz J. (eds.) CRYPTO 2016. LNCS, Part I, vol. 9814. Springer, Heidelberg (2016).
70. Roy B.K., Meier W. (eds):FSE 2004. LNCS, vol. 3017. Springer, Heidelberg (2004).
71. Rogaway P.: Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In: Pil J.L. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 16–31. Springer, Heidelberg (2004).
72. Siegel A.: On universal classes of extremely random constant-time hash functions. SIAM J. Comput. **33**(3), 505–543 (2004).
73. Sako K., Sarkar P. (eds.): ASIACRYPT 2013. LNCS, Part I, vol. 8269. Springer, Heidelberg (2013).
74. Steinberger J.: Improved security bounds for key-alternating ciphers via Hellinger distance. Cryptology ePrint Archive, Report 2012/481 (2012).
75. Stinson D.R. (ed.): CRYPTO'93. LNCS, vol. 773. Springer, Heidelberg (1994).
76. Taylor, R.: An integrity check value algorithm for stream ciphers. In: Stinson D.R. (ed.) CRYPTO'93. LNCS, vol. 773, pp. 40–48. Springer, Heidelberg (1994).
77. Tessaro S.: Optimally secure block ciphers from ideal primitives. In: Iwata T., Cheon J.H. (eds.) ASIACRYPT 2015. LNCS, Part II, vol. 9453, pp. 437–462. Springer, Heidelberg (2015).
78. Wegman M.N., Carter L.: New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci. **22**(3), 265–279 (1981).
79. Zobrist A.: A new hashing method with application for game playing. Technical Report 88 Computer Sciences Department, University of Wisconsin (1970).