Related-Key Almost Universal Hash Functions: Definitions, Constructions and Applications

Peng Wang[1] and Yuling Li[1] and Liting Zhang[2] and Kaiyan Zheng[1]

[1] State Key Laboratory of Information Security
Institute of Information Engineering, Chinese Academy of Sciences
[2] Institution of Software, Chinese Academy of Sciences
wp@is.ac.cn, liyuling@iie.ac.cn, zhangliting@tca.iscas.ac.cn, zhengkaiyan@iie.ac.cn

Abstract. Universal hash functions (UHFs) have been extensively used in the design of cryptographic schemes. If we consider the related-key attack against these UHF-based schemes, some of them may not be secure, especially those using the key of UHF as a part of the whole key of scheme, due to the weakness of UHF in the related-key setting. In order to solve the issue, we propose a new concept of related-key almost universal hash function, which is a natural extension to almost universal hash function in the related-key setting. We define related-key almost universal (RK-AU) hash function and related-key almost XOR universal (RK-AXU) hash function. However almost all the existing UHFs do not satisfy the new definitions. We construct fixed-input-length universal hash functions such as RH1 and variable-input-length universal hash functions such as RH2, RH3. We show that RH1 and RH2 are both RK-AXU, and RH3 is RK-AU. Furthermore, RH1, RH2 and RH3 are nearly as efficient as previous similar constructions. RK-AU (RK-AXU) hash functions can be used as components in the related-key secure cryptographic schemes. If we replace the universal hash functions in the schemes with our corresponding constructions, the problems about related-key attack can be solved. More specifically, we give four concrete applications of RK-AU and RK-AXU in related-key secure MACs and TBCs.

Keywords. Almost universal hash function, related-key attack, related-key almost universal hash function, message authentication code, tweakable block cipher.

1 Introduction

Universal hash functions. Since introduced by Carter and Wegman [15,51], *universal hash functions* (UHFs) have become common components in numerous cryptographic constructions, especially in modes of operation, to provide security services as confidentiality, authenticity or both. A universal hash function (UHF) is a family of functions indexed by keys. Unlike other components such as block ciphers, keyed hash functions and permutations, which are often uses as pseudorandom permutations (PRPs), pseudorandom permutations (PRFs) and public random permutations respectively, UHFs have no cryptographic strength such as pseudorandom. So UHFs usually come along with other primitives, such as PRPs, PRFs, etc., to set up cryptographic schemes. The basic property of UHF is that the collision probability of hash values from any two different messages is small when the key is uniformly random.

For example we define a polynomial evaluation hash function [8] in which the variable is the key and the coefficients consist of message blocks: $Poly : \{0,1\}^n \times \{0,1\}^{nm} \to \{0,1\}^n$,

$$Poly_K(M) = M_1 K^m \oplus M_2 K^{m-1} \oplus \cdots \oplus M_m K \tag{1}$$

where $M = M_1 \| M_2 || \cdots \| M_m \in \{0,1\}^{nm}$, $M_i \in \{0,1\}^n$, $i = 1, 2, \cdots, m$ and all the operations are in the finite field $GF(2^n)$. This kind of UHF appears in GCM [37], XCB [29], HCTR [50], HCH [16,17], COBRA [2], Enchilada [27], POET [1] and many other constructions. For any $M \neq M'$, $Poly_K(M) \oplus Poly_K(M')$ is a polynomial in K whose degree is nonzero and no more than m, so there are at most m keys leading to $Poly_K(M) = Poly_K(M')$, that is the collision probability is at most $m/2^n$ when K is uniformly random. We say that this hash function is $m/2^n$-almost-universal (AU). Obviously the probability of $Poly_K(M) \oplus Poly_K(M') = C$ is also at most $m/2^n$ for any $M \neq M'$ and C. That is another commonly used concept: almost XOR universal (AXU) hash functions. $Poly$ is also $m/2^n$-AXU.

A direct application of UHFs is in message authentication codes (MACs) in which the message is hashed by the UHF into a short digest and then encrypted into a tag. MACs of this kind have been standardized in ISO/IEC 9797-3:2011 [31] which includes UMAC [13], Badger [14], Poly1305-AES [6] and GMAC [37]. UHFs are also used in tweakable block ciphers (TBCs) [36] and tweakable enciphering schemes (TESes), e.g. XTS-AES in IEEE Std 1619-2007 [28] and NIST SP 800-38E [40], XCB in IEEE Std 1619.2-2010 [29], HCTR [50] and HCH [16,17], etc. The third application of UHF is in authenticated encryptions (AEs), e.g. the most widely used AE GCM [37] standardized in ISO/IEC-19772:2009 [30] and NIST SP 800-38D [39]. In the recent CAESAR competition, several UHF-based AEs were proposed, e.g. COBRA [2], Enchilada [27] and POET [1], etc. In the security proofs of all these schemes, a crucial point is the collision probability about the inputs to other primitives. The property of UHF guarantees that the collision seldom happens.

Related-key attacks. Related-key attack was firstly introduced by Biham et al. [10] against block ciphers [22,12,48] and then extended to other cryptographic algorithms such as stream ciphers [18], MACs [41], TESes [49], AEs [21], etc. Bellare and Kohno [5] firstly gave a theoretical study of related-key security of block cipher, modeling the concept of related-key pseudorandom permutation (RK-PRP) and related-key pseudorandom function (RK-PRF). Applebaum, Harnik and Ishai [3] gave the related-key security definition of encryption. Bhattacharyya and Roy [9] gave the related-key security definition of MAC. Related-key security has become an important criteria for cryptographic constructions.

In the *related-key* setting, the adversary does not know the secret key as in the usual *invariable-key* setting, but can apply related-key-deriving (RKD) transformations to change the secret key of the algorithm and observe the output under the related keys. Let Φ be a RKD set which consists of transformations on the key space $\mathcal{K} = \{0,1\}^k$. There are two canonical RKD sets: $\Phi^{\oplus} = \{XOR_{\Delta} : K \mapsto K \oplus \Delta, \Delta \in \mathcal{K}\}$ and $\Phi^{+} = \{ADD_{\delta} : K \mapsto K + \delta \mod 2^k, \delta \in \mathcal{K}\}$. In the following, we use $\Phi^{\oplus}$ as the default RKD set unless specified otherwise.

The related-key security requires that the queries under the related keys do not threaten the security under the original key, as the definition of related-key unforgeability in [9]. Or more strictly, for different related keys, the corresponding algorithms are secure independently, as the definitions in [5] and [3]. For completeness, we give related-key security definitions of MAC, TBC, TES and AE in Appendix A.

How to guarantee the related-key security? An intuition is that if the underlying components are related-key secure, the upper constructions are related-key secure. This is true for most of block cipher modes of operation, especially for those one-key modes whose key is also that of the underlying block cipher, including CBC, OFB, CFB, CTR, CMAC, OCB, et al.

Motivations. Although almost all the UHF-based schemes have security proofs in the usual invariable-key setting, some of them can not resist the related-key attack. We show practical attacks against some popular constructions including MAC, TBC, TES and AE which use *Poly* as the UHF component.

1) MAC. A typical UHF-based MAC encrypts the hash value into a tag by one-time-pad encryption. This method was originated from Carter and Wegman [15,51] and dominates the usages of UHF in MACs [31]. Consider a simple example: $MAC_{K,K'}(N,M) = Poly_K(M) \oplus E_{K'}(N)$ where $M = M_1 \| M_2 \in \{0,1\}^{2n}$, $Poly_K(M_1\|M_2) = M_1K^2 \oplus M_2K$, E is a block cipher and N is a nonce. It has been proved that [44,7] if E is a PRF and $Poly$ is almost XOR universal, MAC is secure. But if we query with $A\|A$ under the related key $(K \oplus 0^{n-1}1, K')$, the answer is $T = (A(K \oplus 0^{n-1}1)^2 \oplus A(K \oplus 0^{n-1}1)) \oplus E_{K'}(N) = (AK^2 \oplus AK)) \oplus E_{K'}(N)$. Therefore we can predict that the tag of $A\|A$ under the original key is also T. So $(N, A\|A, T)$ is a successful forgery which breaks the related-key security of the MAC. A similar attack can apply to Poly1305-AES [6] in ISO/IEC 9797-3:2011 [31].

2) TBC. A tweakable block cipher (TBC) is a generalized block cipher with an extra input called tweak. TBCs were first formalized by Liskov, Rivest and

Wanger [36] and found applications largely in modes of operation [42]. In their seminal paper, Liskov et al. gave a construction of TBC from a block cipher: $TBC_{K,K'}(T,M) = E_{K'}(M \oplus H_K(T)) \oplus H_K(T)$ where E is the block cipher, H is a universal hash function and T is the tweak. They proved that when E is a PRP against chosen ciphertext attacks (CCAs) and H is almost XOR universal, TBC is secure against CCA attacks. If we use $Poly_K(T) = TK$ as the underlying UHF, the following is an attack. First we query with (T, M) under the derived key $(K \oplus \Delta, K')$ where $\Delta \neq 0$, then the answer is $C = E_{K'}(M \oplus T(K \oplus \Delta)) \oplus T(K \oplus \Delta) = E_{K'}((M \oplus T\Delta) \oplus TK) \oplus TK \oplus T\Delta$. So we can predict that the ciphertext of $(T, (M \oplus T\Delta))$ under the original key is $C \oplus T\Delta$. Therefore it does not resist related-key attack.

3) TES. A tweakable enciphering scheme is a generalized TBC with large or variable input length, suitable for disk sector encryption. Recently Sun et al. [49] show that HCTR [50], HCHp and HCHfp [16,17] suffer related-key attacks. All these TESes use the polynomial evaluation hash function as the underlying UHF.

4) AE. An authenticated encryption scheme achieves both confidentiality and authenticity. One of AE designs, such as OCB [43,42] following from IAPM [33], encrypts the message blocks using independent PRPs into ciphertext blocks and encrypts the XOR of the message blocks into a tag using another independent PRP. Kurosawa [35] proposed a modified IAPM, the encryption of message blocks is

$$C_i = E_{K'}(M_i \oplus Poly_K(IV\|(2i-1))) \oplus Poly_K(IV\|(2i-1))$$

where M_i is the i-th message block, E is the block cipher and the key of the scheme is (K, K'). Kurosawa proved that this modified IAPM is secure even if the underlying block cipher is publicly accessible. But if we query with (IV, M) under the derived key $(K \oplus 0^{n-1}1, K')$, the first ciphertext block $C_1 = E_{K'}((M_i \oplus IV \oplus 0^{n-1}1) \oplus (Poly_K(IV\|0^{n-1}1)) \oplus Poly_K(IV\|0^{n-1}1) \oplus IV \oplus 0^{n-1}1$. We can predict that the first ciphertext block of (IV, M') under the original key is $C_1 \oplus IV \oplus 0^{n-1}1$, where M' is changed from M by changing the first block into $M_1 \oplus IV \oplus 0^{n-1}1$. If we define the confidentiality as the indistinguishability between ciphertexts and uniformly random bits, this scheme does not resist the related-key attack.

In the above examples, the key of UHF is a part of the key of whole scheme, so that the adversary can derive the related key of UHF and get the input collision to other primitives such as PRPs or PRFs. The collisions in the above attacks are listed as following.

1) $Poly_{K \oplus 0^{n-1}1}(A\|A) = Poly_K(A\|A)$ used in the MAC example;
2) $Poly_{K \oplus \Delta}(T) \oplus Poly_K(T) = \Delta T$ used in the TBC example;
3) $Poly_{K \oplus \Delta}(A\|B) \oplus Poly_K(A\|B) = A\Delta^2 \oplus B\Delta$ used in the TES and AE examples.

We stress that the above attacks only use the properties of UHF in the related-key setting and have nothing to do with the underlying block cipher, whether it is related-key secure or not. *In other words, the related-key weaknesses of UHF alone result in related-key attacks against the upper schemes.*

DEFINITIONS. In order to prevent the above attacks, we propose a new concept of related-key almost universal hash function which can ensure that the above collisions seldom happen. The new concept is a natural extension to almost universal hash function in the related-key setting. We define *related-key almost universal* (RK-AU) hash function and *related-key almost XOR universal* (RK-AXU) hash function. We will show that these definitions solve the above problems. Unfortunately almost all the existing UHFs do not satisfy the new definitions, including *Poly* mentioned in the above, MMH [26], Square Hash [23], NMH [26] and NH [13], etc. See Appendix B for details.

CONSTRUCTIONS. We construct a fixed-input-length universal hash function RH1 and two variable-input-length universal hash functions RH2 and RH3. We prove that RH1 and RH2 are both RK-AXU, and RH3 is RK-AU, over the RKD set $\Phi^{\oplus}$. Furthermore, RH1, RH2 and RH3 are almost as efficient as previous constructions.

APPLICATIONS. If we replace the universal hash functions in the examples of section 1 with our constructions, the problems about related-key attacks can be solved. To be more specifical, we give four concrete examples in MACs and TBCs.

2 Definitions

For a finite set $\mathcal{S}$, $x \stackrel{\$}{\leftarrow} \mathcal{S}$ means selecting an element x uniformly at random from the set X. For a string M, $|M|$ denotes the bit length of M. For $b \in \{0,1\}$. b^m denotes m bits of b. $\mathbb{A}^{\mathcal{O}} \Rightarrow b$ denotes that the algorithm $\mathbb{A}$ with an oracle $\mathcal{O}$ outputs b.

For a function $H : \mathcal{K} \times \mathcal{D} \to \mathcal{R}$, when $K \in \mathcal{K}$ is a key, we write $H(K,M)$ as $H_K(M)$, where $(K,M) \in \mathcal{K} \times \mathcal{D}$. The following are the usual definitions of UHF.

Definition 1 (AU [46]). *H is an ϵ-almost-universal (ϵ-AU) hash function, if for any $M, M' \in \mathcal{D}$, $M \neq M'$,*

$$\Pr[K \stackrel{\$}{\leftarrow} \mathcal{K} : H_K(M) = H_K(M')] \leq \epsilon.$$

When ϵ is negligible we say that H is AU.

Definition 2 (AXU [34]). *Let* $(\mathcal{R}, \oplus)$ *be an abelian group*[3]*. H is an* ϵ*-almost-XOR-universal (*ϵ*-AXU), if for any* $M, M' \in \mathcal{D}$*,* $M \neq M'$*, and* $C \in \mathcal{R}$*,*

$$\Pr[K \xleftarrow{\$} \mathcal{K} : H_K(M) \oplus H_K(M') = C] \leq \epsilon.$$

When ϵ *is negligible we say that H is AXU.*

Clearly, if H is ϵ-AXU, it is also ϵ-AU, for ϵ-AU is a special case of ϵ-AXU when $C = 0$.

RK-AU and RK-AXU. In the following, we extend the above definitions in the related-key setting. Let Φ be a RKD set.

Definition 3 (RK-AU). *H is an* ϵ*-related-key-almost-universal (*ϵ*-RK-AU) hash function over the RKD set* Φ*, if for any* $\phi, \phi' \in \Phi$*,* $M, M' \in \mathcal{D}$*,* $(\phi, M) \neq (\phi', M')$*,*

$$\Pr[K \xleftarrow{\$} \mathcal{K} : H_{\phi(K)}(M) = H_{\phi'(K)}(M')] \leq \epsilon.$$

When ϵ *is negligible we say that H is RK-AU.*

Definition 4 (RK-AXU). *Let* $(\mathcal{R}, \oplus)$ *be an abelian group. H is an* ϵ*-related-key-almost-universal (*ϵ*-RK-AXU) hash function over the RKD set* Φ*, if for any* $\phi, \phi' \in \Phi$*,* $M, M' \in \mathcal{D}$*,* $(\phi, M) \neq (\phi', M')$*, and* $C \in \mathcal{R}$*,*

$$\Pr[K \xleftarrow{\$} \mathcal{K} : H_{\phi(K)}(M) \oplus H_{\phi'(K)}(M') = C] \leq \epsilon.$$

When ϵ *is negligible we say that H is RK-AXU.*

For $\phi, \phi' \in \Phi$, $\phi \neq \phi'$ means there exists a key $K \in \mathcal{K}$ such that $\phi(K) \neq \phi'(K)$.

Restricting RKD sets. As in the discussion of RK-PRP [5], the related-key properties of UHF are relevant to the choice of the RKD set. For some RKD sets the related-key almost universal hash functions may not be available. We must put some restrictions on the RKD set.

One restriction is *output unpredictability.* A $\phi \in \Phi$ that has predictable outputs if there exists a constant S such that the probability of $\phi(K) = S$ is high. If it happens, then probability of $H_{\phi(K)}(M) \oplus H_{\phi(K)}(M') = H_S(M) \oplus H_S(M')$ is also high for any two distinct M and M'. So the RK-AXU function is not available for the RKD set which has predictable transformations.

The other restriction is *claw-freeness.* The RKD set Φ has claws if there exists two distinct $\phi, \phi' \in \Phi$ such that $\phi(K) = \phi'(K)$. If it happens, then for any M we have $H_{\phi(K)}(M) \oplus H_{\phi'(K)}(M) = 0$. So neither the RK-AXU nor RK-AU function is available for the RKD set with claws.

[3] For arbitrary abelian groups a generalized notion is almost Delta universal (AΔU) hash function [47]. In the following when we say AXU we may sometimes refer to AΔU.

Without loss of generality, in the paper we assume that Φ is *output unpredictable* and *claw-free*. We also assume that the identity transformation $id \in \Phi$. We note that $\Phi^{\oplus}$ and Φ^{+} satisfy all these conditions.

The examples in section 1 have shown that $Poly$ is not RK-AXU over the RKD set $\Phi^{\oplus}$. If we choose the message M to be 0^{mn}, $Poly_K(M)$ will always be 0^n. Therefore for any $\phi, \phi' \in \Phi$, we have $Poly_{\phi(K)}(0^{mn}) = Poly_{\phi'(K)}(0^{mn})$. So $Poly$ is not RK-AU either. If we look at the other existing UHFs, unfortunately almost all of them do not satisfy the new definitions, including MMH [26], Square Hash [23], NMH [26] and NH [13], etc. See Appendix B for more details.

3 Constructions

We construct two types of related-key almost universal hash functions: fixed-input-length (FIL) UHFs such as RH1 and variable-input-length (VIL) UHFs such as RH2 and RH3. We prove that RH1 and RH2 are both RK-AXU, and RH3 is RK-AU, over the RKD set $\Phi^{\oplus}$.

For a function $F : \mathcal{K} \times \mathcal{D} \to \mathcal{R}$, in the related-key setting, the RKD transformation can be seen as an extra input to F. We define a new function $F' : \mathcal{K} \times (\mathcal{K} \times \mathcal{D}) \to \mathcal{R}$

$$F'_K(\Delta, M) = F_{K \oplus \Delta}(M).$$

It is easy to see that F is RK-AU (RK-AXU) if and only if F' is AU (AXU). All the constructions are based on the polynomial evaluation function $Poly$. From the above observation, our main idea is to modify $Poly_K(M)$ into $F_K(M)$ such that $F_{K \oplus \Delta}(M)$ is still an ordinary almost (XOR) universal hash function.

FIL Constructions. We first construct a function based on $Poly_K(M) = MK$ by adding a term K^3.

Construction 1 RH1 : $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$,

$$\mathrm{RH1}_K(M) = MK \oplus K^3. \tag{2}$$

Theorem 1. RH1 *is* $2/2^n$*-RK-AXU over the RKD set* $\Phi^{\oplus}$*.*

Proof. We prove that for any $M, M', \Delta_1, \Delta_2 \in \{0,1\}^n$, $(\Delta_1, M) \neq (\Delta_2, M')$, and $C \in GF(2^n)$, $\Pr[K \xleftarrow{\$} \{0,1\}^n : F(K) = C] \leq \epsilon$, where $F(K) = \mathrm{RH1}_{K \oplus \Delta_1}(M) \oplus \mathrm{RH1}_{K \oplus \Delta_2}(M')$. We have

$$F(K) = (\Delta_1 \oplus \Delta_2)K^2 \oplus (\Delta_1^2 \oplus \Delta_2^2 \oplus M \oplus M')K \oplus (\Delta_1^3 \oplus \Delta_2^3 \oplus M\Delta_1 \oplus M'\Delta_2).$$

If $\Delta_2 \neq \Delta_1$, $F(K) = C$ has two roots at most. If $\Delta_1 = \Delta_2$, then $M \neq M'$. The degree of $F(K)$ is 1 and $F(K) = C$ has one root. Therefore RH1 is $2/2^n$-RK-AXU. □

(i,j)	(1,1)	(1,2)	(1,3)	(1,4)	(2,1)	(2,2)	(2,3)	(2,4)	(3,1)	(3,2)	(3,3)	(3,4)	(4,1)	(4,2)	(4,3)	(4,4)
$GF(2^n)$	-	-	1	-	-	-	1	-	0	0	-	0	-	-	1	-
$GF(p)$	-	-	1	1	0	-	0	1	0	1	-	1	0	1	1	-

Table 1. RK-AXU or RK-AU. Here "1" means it is RK-AXU, "0" means it is RK-AU, and "-" means it is neither RK-AU nor RK-AXU.

More generally we consider polynomial $H_K^{i,j}(M) = MK^i + K^j$ over the finite field $GF(2^n)$ or $GF(p)$ where i, j are integers and p is a large prime. We show the results when $1 \le i, j \le 4$ in Table 1.

VIL Constructions. *Poly* does not support variable input length. For any message $M \in \{0,1\}^*$, a general padding method as in [37] is to firstly pad minimum zeroes to make the length multiple of the block length and then pad the bit length of M as the last block:

$$pad(M) = M \| 0^i \| |M|.$$

Then $Poly_K(pad(M))$ is variable-input-length AXU hash function but still is not RK-AU (RK-AXU). Following the above method we add some term K^i in order to get the RK-AXU property.

Construction 2 RH2 : $\{0,1\}^n \times \{0,1\}^* \to \{0,1\}^n$,

$$\mathrm{RH2}_K(M) = \begin{cases} K^{l+2} \oplus Poly_K(pad(M)), & l \text{ is odd} \\ K^{l+3} \oplus Poly_K(pad(M))K, & l \text{ is even} \end{cases} \tag{3}$$

where $l = \lceil |M|/n \rceil + 1$ is the number of blocks in $pad(M)$.

Theorem 2. RH2 *is $(l_{max}+3)/2^n$-RK-AXU over the RKD set $\Phi^{\oplus}$, where l_{max} is the maximum block number of messages after padding.*

Proof. For any message M, suppose $pad(M) = M_1 \| M_2 \| \cdots \| M_l$. When l is odd

$$\mathrm{RH2}_K(M) = K^{l+2} \oplus M_1 K^l \oplus \cdots \oplus M_l K.$$

When l is even

$$\mathrm{RH2}_K(M) = K^{l+3} \oplus M_1 K^{l+1} \oplus \cdots \oplus M_l K^2.$$

We prove that for any $M, M' \in \{0,1\}^*$, $\Delta_1, \Delta_2, C \in \{0,1\}^n$, $(\Delta_1, M) \neq (\Delta_2, M')$, $\Pr[F(K) = C] \le \epsilon$, where $F(K) = \mathrm{RH2}_{K\oplus\Delta_1}(M) \oplus \mathrm{RH2}_{K\oplus\Delta_2}(M')$. We only need to show the degree of $F(K)$ is nonzero. Suppose $pad(M) = M_1 \| M_2 \| \cdots \| M_l$ and $pad(M') = M'_1 \| M'_2 \| \cdots \| M'_{l'}$. Consider $F(K)$ in the following two cases.

Case 1. $\Delta_1 \neq \Delta_2$. Suppose the degrees of $\mathrm{RH2}_{K\oplus\Delta_1}(M)$ and $\mathrm{RH2}_{K\oplus\Delta_2}(M')$ are d and d' respectively, which are both odd.

When $d = d'$, the coefficient of K^{d-1} in $F(K)$ is $\Delta_1 \oplus \Delta_2$ which is nonzero.

When $d \neq d'$, suppose $d > d'$ w.l.o.g. The coefficient of K^d in $F(K)$ is 1.

Case 2. $\Delta_1 = \Delta_2$. We treat $K \oplus \Delta_1$ as a new key, so without loss of generality, we only consider $\Delta_1 = \Delta_2 = 0$ in the following.

When $l = l'$, there exists $1 \leq j \leq l$ s.t. $M_j \neq M'_j$. So the coefficient of K^{l+1-j} (if l is odd) or K^{l+2-j} (if l is even) in $F(K)$ is $M_j \oplus M'_j$ which is nonzero.

When $l' \neq l$ and are both odd, the coefficient of K is $|M| \oplus |M'|$ which is nonzero.

When $l' \neq l$ and are both even, the coefficient of K^2 is $|M| \oplus |M'|$ which is nonzero.

When $l' \neq l$, one is odd and one is even, the coefficient of K is $|M|$ or $|M'|$ which are both nonzero.

Therefore the degree of $F(K)$ is nonzero. □

Since RH2 is RK-AXU, it is also RK-AU. But we can still improve the efficiency of RK-AU construction if replace *Poly* in RH2 with the following *Poly*′:

$$Poly'_K(M) = M_1K^{m-1} \oplus M_2K^{m-2} \oplus \cdots \oplus M_m$$

where $M = M_1\|M_2\|\cdots\|M_m \in \{0,1\}^{nm}$. $Poly'$ is AU but not AXU and more efficient than *Poly*. We have the following construction and the proof is similar to that of theorem 2.

Construction 3 $\mathrm{RH3} : \{0,1\}^n \times \{0,1\}^* \rightarrow \{0,1\}^n$,

$$\mathrm{RH3}_K(M) = \begin{cases} K^{l+2} \oplus Poly'_K(pad(M)), & l \text{ is odd} \\ K^{l+3} \oplus Poly'_K(pad(M))K, & l \text{ is even} \end{cases} \tag{4}$$

where $l = \lceil |M|/n \rceil + 1$ *is the number of blocks in* $pad(M)$.

Theorem 3. RH3 *is* $(l_{max} + 3)/2^n$*-RK-AU over the RKD set* $\Phi^{\oplus}$*, where* l_{max} *is the maximum number of blocks in messages after padding.*

Efficiency of constructions. We analyze the efficiency of RH1, RH2 and RH3 compared with previous similar constructions.

1) RH1. Compared with $Poly_K(M) = MK$, in $\mathrm{RH1}_K(M) = MK \oplus K^3$ the monomial K^3 can be pre-computed. So RH1 need extra one pre-computation and one XOR operation.

2) RH2. The polynomial $T = M_1K^m \oplus M_2K^{m-1} \oplus \cdots \oplus M_mK$ is usually evaluated by Horner's rule: $T \leftarrow 0$, $T \leftarrow (T \oplus M_i)K$ for $1 \leq i \leq m$. Assume that $pad(M) = M_1\|M_2\|\cdots\|M_l$, Table 2 shows the computation processes of $\mathrm{RH2}_K(M)$ and $Poly_K(pad(M))$ by Horner's rule respectively. We can see that

$\mathrm{RH2}_K(M)$:	$Poly_K(pad(M))$:
$T \leftarrow K^2$ **for** $i = 1$ **to** l $T \leftarrow (T \oplus M_i)K$ **if** l is even $T \leftarrow TK$ **return** T	$T \leftarrow 0$ **for** $i = 1$ **to** l $T \leftarrow (T \oplus M_i)K$ **return** T

Table 2. Computation processes of $\mathrm{RH2}_K(M)$ and $Poly_K(pad(M))$.

compared with $Poly_K(pad(M))$, RH2 needs one additional pre-computation of K^2, and one more multiplication if l is even.

3) RH3. Similar to the analysis of RH2, RH3 needs one additional pre-computation of K^2, and one more multiplication if l is even, compared with $Poly'_K(pad(M))$.

In brief, RH1, RH2 and RH3 are almost as efficient as previous similar constructions.

4 Applications

RK-AU (RK-AXU) hash functions can be used as components, along with other primitives such as RK-PRPs and RK-PRFs, in the design of related-key secure cryptographic schemes. If we replace the UHFs in the cryptographic schemes in section 1 with our corresponding constructions, the issues about related-key attacks can be solved. *Informally speaking, if the UHF is RK-AU or RK-AXU over the RKD set Φ_1 and the underlying primitive is RK-PRP or RK-PRF over the RKD set Φ_2, even if the key of UHF is a part of the key of the whole upper scheme, the scheme is related-key secure over the RKD set $\Phi_1 \times \Phi_2$.*

In the following, we give four concrete applications of RK-AU and RK-AXU in related-key secure MACs and TBCs. In the analyses of these schemes, we mainly give intuitive interpretations by establishing the relationship between the invariable-key setting and the related-key setting. Then the remaining proof is similar to that in the invariable-key setting. For simplicity we only consider the *claw-free* RKD set Φ in which for any $\phi_1, \phi_1 \in \Phi$ and any key K we have $\phi_1(K) \neq \phi_2(K)$. Let RK-PRF be PRF against related-key attacks. We define a CCA secure tweakable block cipher as a strongly tweakable pseudorandom permutation (STPRP, SPRP if it has no tweak). If it is also related-key secure we denote it as RK-STPRP (RK-SPRP if it has no tweak). The detailed definitions are in Appendix A.

The relationships are based on three observations on the underlying components when we regard the RKD transformation as an additional input.

Observation 1. For a function $F : \mathcal{K} \times \mathcal{D} \to \mathcal{R}$ and a claw-free RKD set Φ on $\mathcal{K}$. We define a new function $F' : \mathcal{K} \times (\Phi \times \mathcal{D}) \to \mathcal{R}$, $F'_K(\phi, M) = F_{\phi(K)}(M)$. It is directly derived from the definition that F is RK-AU (RK-AXU) if and only if F' is AU (AXU).

Observation 2. Furthermore, we have that F is a RK-PRF if and only if F' is a RPF. That is from the fact that for any ϕ, $F_{\phi(K)}$ is an independent PRF.

Observation 3. For a block cipher $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$, define a tweakable block cipher $E' : \mathcal{K} \times \Phi \times \{0,1\}^n \to \{0,1\}^n$, $E'_K(\phi, M) = E_{\phi(K)}(M)$. Bellare and Kohno observed [5] that if E is a RK-SPRP, then E' is a STPRP.

4.1 Related-key secure MACs

Beside the Carter-Wegman scheme to construct MAC [51]

$$\mathrm{MAC1}_{K,K'}(N, M) = H_K(M) \oplus E_{K'}(N) \tag{5}$$

the other method [45] is

$$\mathrm{MAC2}_{K,K'}(M) = E_{K'}(H_K(M)) \tag{6}$$

where $H : \mathcal{K}_1 \times \mathcal{D} \to \{0,1\}^n$ is a universal hash function, $E : \mathcal{K}_2 \times \{0,1\}^n \to \{0,1\}^n$ is usual a block cipher, M is a message and N is a nonce. We show that the two schemes are all related-key secure by the following two theorems.

Theorem 4. *If H is ϵ-RK-AXU over the RKD set Φ_1 and E is a RK-PRF over the RKD set Φ_2, then* MAC1 *is related-key unforgable (RK-UF) over the RKD set $\Phi_1 \times \Phi_2$. More specifically,*

$$\mathbf{Adv}^{rk-uf}_{\mathrm{MAC1}}(q,t) \le \mathbf{Adv}^{rk-prf}_{E}(q,t') + \epsilon$$

where the adversary makes q queries to $MAC1$ and $t' = t + O(q)$.

From Observation 1, $H'_K(\phi_1, M) = H_{\phi_1(K)}(M)$ is AXU; from Observation 3, $E'_{K'}(\phi_2, N) = E_{\phi_2(K')}(N)$ is a PRF. If we look ϕ_1 as a part of the message and ϕ_2 as a part of the nonce, we only need to prove that $F'_{K,K'}(\phi_2, N, \phi_1, M) = H'_K(\phi_1, M) \oplus E'_{K'}(\phi_2, N)$ is unforgeable in the invariable-key setting. The remaining proof is similar to that in [34].

Theorem 5. *If H is ϵ-RK-AU over the RKD set Φ_1 and E is a RK-PRF over the RKD set Φ_2, then* MAC2 *is a RK-PRF over the RKD set $\Phi_1 \times \Phi_2$. More specifically,*

$$\mathbf{Adv}^{rk-prf}_{\mathrm{MAC2}}(q,t) \le \mathbf{Adv}^{rk-prf}_{E}(q,t') + \epsilon q^2/2$$

where the adversary makes q queries to $MAC2$ and $t' = t + O(q)$.

From Observation 1, $H'_K(\phi_1, M) = H_{\phi_1(K)}(M)$ is AXU; from Observation 2, $E'_{K'}(\phi_2, M) = E_{\phi_2(K')}(M)$ is a PRF. If we look ϕ_1 and ϕ_2 as a part of the message, we only need to prove that $F'_{K,K'}(\phi_1, \phi_2, M) = E'_{K'}(\phi_2, H'_K(\phi_1, M))$ is a PRF in the invariable-key setting. The remaining proof is similar to that in [45].

4.2 Related-key secure TBCs

BLOCK CIPHER BASED SCHEMES. In [36] Liskov et al. gave a construction of tweakable block cipher (TBC) from a block cipher and a universal hash function:

$$\mathrm{TBC1}_{K,K'}(T, M) = E_{K'}(M \oplus H_K(T)) \oplus H_K(T) \tag{7}$$

where $H : \mathcal{K}_1 \times \mathcal{D} \to \{0,1\}^n$ is the universal hash function and $E : \mathcal{K}_2 \times \{0,1\}^n \to \{0,1\}^n$ is the block cipher. In section 1 we have shown that TBC1 is not related-key secure if $H_K(T) = TK$. But if H is RK-AXU, we show that TBC1 is related-key secure in theorem 6.

Theorem 6. *If H is ϵ-RK-AXU over the RKD set Φ_1 and E is RK-SPRP over the RKD set Φ_2, then* TBC1 *is a RK-STPRP over the RKD set $\Phi_1 \times \Phi_2$. More specifically,*

$$\mathbf{Adv}_{\mathrm{TBC1}}^{rk-stprp}(q,t) \leq \mathbf{Adv}_{E}^{rk-sprp}(q,t') + 3\epsilon q^2$$

where the adversary makes q queries to TBC1 *or* $\mathrm{TBC1}^{-1}$ *and $t' = t + O(q)$.*

From Observation 1, $H'_K(\phi_1, M) = H_{\phi_1(K)}(M)$ is AXU; from Observation 3, $E'_{K'}(\phi_2, M) = E_{\phi_2(K')}(M)$ is a STPRP. If we look ϕ_1 and ϕ_2 as a part of the nonce, we only need to prove that $\widetilde{E}_{K,K'}(\phi_1, \phi_2, T, M) = E'_{K'}(\phi_2, M \oplus H'_K(\phi_1, T)) \oplus H'_K(\phi_1, T)$ is a STPRP in the invariable-key setting. The remaining proof is similar to that in [36].

PERMUTATION BASED SCHEMES. If we replace the block cipher in TBC1 as a complex permutation, we get

$$\mathrm{TBC2}_K(T, M) = \pi(M \oplus H_K(T)) \oplus H_K(T) \tag{8}$$

where π is the permutation from $\{0,1\}^m$ to $\{0,1\}^m$, $n \leq m$. For $A \in \{0,1\}^n$, $B \in \{0,1\}^m$, when $n < m$, $A \oplus B$ is defined as $(A \| 0^{m-n}) \oplus B$. We show the related-key security of TBC2 in theorem 7. We need that H is both RK-AXU and related-key almost uniform. H is δ-related-key-almost-uniform means for any $\phi \in \Phi$, $M \in \mathcal{D}$ and $C \in \{0,1\}^n$, $\Pr[K \xleftarrow{\$} \mathcal{K} : H_{\phi(K)}(M) = C] \leq \delta$. When H is also ϵ-RK-AXU, we say that it is (ϵ, δ)-RK-AXU. For example, $\mathrm{RH1} = MK \oplus K^3$ is $(2/2^n, 3/2^n)$-RK-AXU.

TBC2 is a one-round tweakable Even-Mansour cipher. How to add tweak and retain related-key security of the Even-Mansour cipher is a popular topic in recent years [24,20,19,38,25]. Compared with previous constructions in [38] and [25] we only need one permutation invocation (two in [38,25]).

Theorem 7. *If H is (ϵ, δ)-RK-AXU over the RKD set Φ and π is public random permutation, then* TBC2 *is a RK-TSPRP over the RKD set Φ. More specifically,*

$$\mathbf{Adv}^{rk-stprp}_{\mathrm{TBC2}}(q_0, q_1) \leq q_0^2\epsilon + 2q_0q_1\delta + 2^{-m}(q_0^2 + 2q_0q_1)$$

where the adversary makes q_0 queries to TBC2 *or* $\mathrm{TBC2}^{-1}$ *and q_1 queries to π or π^{-1}.*

From Observation 1, $H'_K(\phi, M) = H_{\phi(K)}(M)$ is AXU. If we look ϕ as a part of the nonce, we only need to prove that $\widetilde{E}_K(\phi, T, M) = \pi(M \oplus H'_K(\phi, T)) \oplus H'_K(\phi, T)$ is a STPRP in the invariable-key setting. The remaining proof is similar to that in [35] or [19].

5 Discussions and Conclusions

In this paper we mainly focus on two-key schemes, e.g. one key for the UHF and the other key for the block cipher. In order to resist related-key attacks, we define a new concept of related-key almost universal hash function, which is a natural extension to almost universal hash function in the related-key setting.

Not every UHF-based scheme suffers related-key attacks. GCM [37] is an example. GCM has only one key which is also the key of the underlying block cipher. The key of UHF is derived from the master key K as $E_K(0^{128})$. GCM has been proved to be secure in the invariable-key setting [32] given that E is a PRP. If E is a RK-PRP, for each $\phi \in \Phi$, $E_{\phi(K)}$ is an independent PRP. So GCM is secure independently for each related key, that is GCM is also secure in the related-key setting. In this roughly reasoning, we only require that the UHF is AXU but not RK-AXU. Therefore it is possible that the upper scheme "inherit" the related-key security only from the underlying block cipher. It is also true to some other one-key schemes such as XCB [29], POET [1], etc. We can even modify the vulnerable schemes in this paper into related-key secure ones without the notion of RK-AXU or RK-AU by generating the keys in the schemes as $K_i = E_K(i)$, $i = 1, 2, \cdots$ where K is the master key. So do we still need the new definitions? The answer is yes. Firstly, there are a lot of two-key schemes such as Poly1305-AES [6], HCTR [50], HCHp and HCHfp [16,17]. Secondly, regarding related-key attacks as a class of *side-channel attacks*, the attacker may have the ability to change a stored key via tampering or fault injection [11,4]. The key of UHF stored somewhere, whether it is a part of the master key or derived from the master key, can be changed in this scenario.

We also give several efficient constructions such as RH1, RH2 and RH3 which are nearly as efficient as previous similar ones. RK-AU (RK-AXU) hash functions can be used as components, along with other primitives such as RK-PRPs and RK-PRFs etc., in the design of related-key secure cryptographic schemes.

References

1. Abed, F., Fluhrer, S., Foley, J., Forler, C., List, E., Lucks, S., McGrew, D., , Wenzel, J.: The POET family of on-line authenticated encryption schemes (2014), http://competitions.cr.yp.to/caesar-submissions.html 2, 13
2. Andreeva, E., Bogdanov, A., Lauridsen, M.M., Luykx, A., Mennink, B., Tischhauser, E., Yasuda, K.: AES-COBRA (2014), http://competitions.cr.yp.to/caesar-submissions.html 2
3. Applebaum, B., Harnik, D., Ishai, Y.: Semantic security under related-key attacks and applications. In: Chazelle, B. (ed.) Innovations in Computer Science - ICS 2010. pp. 45–60. Tsinghua University Press (2011), http://conference.itcs.tsinghua.edu.cn/ICS2011/content/papers/30.html 3
4. Bellare, M., Cash, D., Miller, R.: Cryptography secure against related-key attacks and tampering. In: Lee, D.H., Wang, X. (eds.) Advances in Cryptology - ASIACRYPT 2011. Lecture Notes in Computer Science, vol. 7073, pp. 486–503. Springer (2011), http://dx.doi.org/10.1007/978-3-642-25385-0_26 13
5. Bellare, M., Kohno, T.: A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. In: Biham, E. (ed.) EUROCRYPT. Lecture Notes in Computer Science, vol. 2656, pp. 491–506. Springer (2003), http://dx.doi.org/10.1007/3-540-39200-9_31 2, 3, 6, 11
6. Bernstein, D.J.: The poly1305-AES message-authentication code. In: Gilbert, H., Handschuh, H. (eds.) FSE 2005, Revised Selected Papers. Lecture Notes in Computer Science, vol. 3557, pp. 32–49. Springer (2005), http://dx.doi.org/10.1007/11502760_3 2, 3, 13
7. Bernstein, D.J.: Stronger security bounds for wegman-carter-shoup authenticators. In: Cramer, R. (ed.) Advances in Cryptology - EUROCRYPT 2005. Lecture Notes in Computer Science, vol. 3494, pp. 164–180. Springer (2005), http://dx.doi.org/10.1007/11426639_10 3
8. Bernstein, D.J.: Polynomial evaluation and message authentication (2011), http://cr.yp.to/papers.html#pema 2
9. Bhattacharyya, R., Roy, A.: Secure message authentication against related-key attack. In: Moriai, S. (ed.) Fast Software Encryption, FSE 2013. Lecture Notes in Computer Science, vol. 8424, pp. 305–324. Springer (2013), http://dx.doi.org/10.1007/978-3-662-43933-3_16 3
10. Biham, E.: New types of cryptoanalytic attacks using related keys (extended abstract). In: Helleseth, T. (ed.) EUROCRYPT. Lecture Notes in Computer Science, vol. 765, pp. 398–409. Springer (1993) 2
11. Biham, E., Shamir, A.: Differential fault analysis of secret key cryptosystems. In: Jr., B.S.K. (ed.) Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings. Lecture Notes in Computer Science, vol. 1294, pp. 513–525. Springer (1997), http://dx.doi.org/10.1007/BFb0052259 13

12. Biryukov, A., Khovratovich, D.: Related-key cryptanalysis of the full AES-192 and AES-256. In: Matsui, M. (ed.) Advances in Cryptology - ASIACRYPT 2009. Lecture Notes in Computer Science, vol. 5912, pp. 1–18. Springer (2009), http://dx.doi.org/10.1007/978-3-642-10366-7_1 2
13. Black, J., Halevi, S., Krawczyk, H., Krovetz, T., Rogaway, P.: UMAC: fast and secure message authentication. In: Wiener [52], pp. 216–233, http://dx.doi.org/10.1007/3-540-48405-1_14 2, 5, 7, 19
14. Boesgaard, M., Christensen, T., Zenner, E.: Badger - A fast and provably secure MAC. In: Ioannidis, J., Keromytis, A.D., Yung, M. (eds.) Applied Cryptography and Network Security, ACNS 2005. Lecture Notes in Computer Science, vol. 3531, pp. 176–191 (2005), http://dx.doi.org/10.1007/11496137_13 2
15. Carter, L., Wegman, M.N.: Universal classes of hash functions. J. Comput. Syst. Sci. 18(2), 143–154 (1979) 1, 3
16. Chakraborty, D., Sarkar, P.: HCH: A new tweakable enciphering scheme using the hash-encrypt-hash approach. In: Barua, R., Lange, T. (eds.) Progress in Cryptology - INDOCRYPT 2006. Lecture Notes in Computer Science, vol. 4329, pp. 287–302. Springer (2006), http://dx.doi.org/10.1007/11941378_21 2, 4, 13
17. Chakraborty, D., Sarkar, P.: HCH: A new tweakable enciphering scheme using the hash-counter-hash approach. IEEE Transactions on Information Theory 54(4), 1683–1699 (2008), http://dx.doi.org/10.1109/TIT.2008.917623 2, 4, 13
18. Chen, J., Miyaji, A.: A new practical key recovery attack on the stream cipher RC4 under related-key model. In: Lai, X., Yung, M., Lin, D. (eds.) Inscrypt 2010. Lecture Notes in Computer Science, vol. 6584, pp. 62–76. Springer (2010), http://dx.doi.org/10.1007/978-3-642-21518-6_5 2
19. Cogliati, B., Lampe, R., Seurin, Y.: Tweaking Even-Mansour ciphers. In: Gennaro, R., Robshaw, M. (eds.) Advances in Cryptology - CRYPTO 2015, Part I. Lecture Notes in Computer Science, vol. 9215, pp. 189–208. Springer (2015), http://dx.doi.org/10.1007/978-3-662-47989-6_9 13
20. 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.) Advances in Cryptology - EUROCRYPT 2015, Proceedings, Part I. Lecture Notes in Computer Science, vol. 9056, pp. 584–613. Springer (2015), http://dx.doi.org/10.1007/978-3-662-46800-5_23 13
21. Dobraunig, C., Eichlseder, M., Mendel, F.: Related-key forgeries for Prøst-OTR. IACR Cryptology ePrint Archive, to appear in FSE 2015 (2015), http://eprint.iacr.org/2015/091 2
22. Dunkelman, O., Keller, N., Shamir, A.: A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3g telephony. J. Cryptology 27(4), 824–849 (2014), http://dx.doi.org/10.1007/s00145-013-9154-9 2
23. Etzel, M., Patel, S., Ramzan, Z.: SQUARE HASH: fast message authenication via optimized universal hash functions. In: Wiener [52], pp. 234–251, http://dx.doi.org/10.1007/3-540-48405-1_15 5, 7, 19
24. Farshim, P., Procter, G.: The related-key security of iterated Even-Mansour ciphers. In: Leander, G. (ed.) Fast Software Encryption, FSE 2015, Revised Selected Papers. Lecture Notes in Computer Science, vol. 9054, pp. 342–363. Springer (2015), http://dx.doi.org/10.1007/978-3-662-48116-5_17 13

25. Granger, R., Jovanovic, P., Mennink, B., Neves, S.: Improved masking for tweakable blockciphers with applications to authenticated encryption. Cryptology ePrint Archive, Report 2015/999 (2015), http://eprint.iacr.org/ 13
26. Halevi, S., Krawczyk, H.: MMH: software message authentication in the gbit/second rates. In: Biham, E. (ed.) Fast Software Encryption 1997. Lecture Notes in Computer Science, vol. 1267, pp. 172–189. Springer (1997), http://dx.doi.org/10.1007/BFb0052345 5, 7, 19
27. Harris, S.: AES-COBRA (2014), http://competitions.cr.yp.to/caesar-submissions.html 2
28. IEEE Std 1619-2007: IEEE standard for cryptographic protection of data on block-oriented storage devices (2008) 2
29. IEEE Std 1619.2-2010: IEEE standard for wide-block encryption for shared storage media (2011) 2, 13
30. ISO/IEC 19772:2009: Information technology – security techniques – authenticated encryption (2009) 2
31. ISO/IEC9797-3:2011: Information technology – security techniques – message authentication codes (MACs) – part 3: Mechanisms using a universal hash-function (2011) 2, 3
32. Iwata, T., Ohashi, K., Minematsu, K.: Breaking and repairing GCM security proofs. In: Safavi-Naini, R., Canetti, R. (eds.) Advances in Cryptology - CRYPTO 2012. Lecture Notes in Computer Science, vol. 7417, pp. 31–49. Springer (2012), http://dx.doi.org/10.1007/978-3-642-32009-5_3 13
33. Jutla, C.S.: Encryption modes with almost free message integrity. In: Pfitzmann, B. (ed.) EUROCRYPT. Lecture Notes in Computer Science, vol. 2045, pp. 529–544. Springer (2001), http://dx.doi.org/10.1007/3-540-44987-6_32 4
34. Krawczyk, H.: LFSR-based hashing and authentication. In: Desmedt, Y. (ed.) Advances in Cryptology - CRYPTO '94. Lecture Notes in Computer Science, vol. 839, pp. 129–139. Springer (1994), http://dx.doi.org/10.1007/3-540-48658-5_15 6, 11
35. Kurosawa, K.: Power of a public random permutation and its application to authenticated encryption. IEEE Transactions on Information Theory 56(10), 5366–5374 (2010), http://dx.doi.org/10.1109/TIT.2010.2059636 4, 13
36. Liskov, M., Rivest, R.L., Wagner, D.: Tweakable block ciphers. In: Yung, M. (ed.) CRYPTO 2012. Lecture Notes in Computer Science, vol. 2442, pp. 31–46. Springer (2002), http://dx.doi.org/10.1007/3-540-45708-9_3 2, 4, 12
37. McGrew, D.A., Viega, J.: The Galois/Counter mode of operation (GCM) (2004), http://csrc.nist.gov/groups/ST/toolkit/BCM/ 2, 8, 13
38. Mennink, B.: XPX: generalized tweakable Even-Mansour with improved security guarantees. IACR Cryptology ePrint Archive 2015, 476 (2015), http://eprint.iacr.org/2015/476 13
39. NIST SP 800-38D: Recommendations for block cipher modes of operation: Galois/counter mode (GCM) and GMAC (November 2007) 2
40. NIST SP 800-38E: Recommendation for block cipher modes of operation: The XTS-AES mode for confidentiality on storage devices (2010) 2
41. Peyrin, T., Sasaki, Y., Wang, L.: Generic related-key attacks for HMAC. In: Wang, X., Sako, K. (eds.) Advances in Cryptology - ASIACRYPT 2012. Lecture Notes in

Computer Science, vol. 7658, pp. 580–597. Springer (2012), http://dx.doi.org/10.1007/978-3-642-34961-4_35 2

42. Rogaway, P.: Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In: Lee, P.J. (ed.) Advances in Cryptology - ASIACRYPT 2004. Lecture Notes in Computer Science, vol. 3329, pp. 16–31. Springer (2004), http://dx.doi.org/10.1007/978-3-540-30539-2_2 4
43. Rogaway, P., Bellare, M., Black, J., Krovetz, T.: OCB: a block-cipher mode of operation for efficient authenticated encryption. In: Reiter, M.K., Samarati, P. (eds.) ACM Conference on Computer and Communications Security. pp. 196–205. ACM (2001) 4
44. Shoup, V.: On fast and provably secure message authentication based on universal hashing. In: Koblitz, N. (ed.) Advances in Cryptology - CRYPTO '96. Lecture Notes in Computer Science, vol. 1109, pp. 313–328. Springer (1996), http://dx.doi.org/10.1007/3-540-68697-5_24 3
45. Shoup, V.: Sequences of games: a tool for taming complexity in security proofs. IACR Cryptology ePrint Archive 2004, 332 (2004), http://eprint.iacr.org/2004/332 11, 12
46. Stinson, D.R.: Universal hashing and authentication codes. In: Feigenbaum, J. (ed.) Advances in Cryptology - CRYPTO '91. Lecture Notes in Computer Science, vol. 576, pp. 74–85. Springer (1991), http://dx.doi.org/10.1007/3-540-46766-1_5 5
47. Stinson, D.R.: On the connections between universal hashing, combinatorial designs and error-correcting codes. Electronic Colloquium on Computational Complexity (ECCC) 2(52) (1995), http://eccc.hpi-web.de/eccc-reports/1995/TR95-052/index.html 6
48. Sun, S., Hu, L., Wang, P., Qiao, K., Ma, X., Song, L.: Automatic security evaluation and (related-key) differential characteristic search: Application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers. In: Sarkar, P., Iwata, T. (eds.) Advances in Cryptology - ASIACRYPT 2014. Lecture Notes in Computer Science, vol. 8873, pp. 158–178. Springer (2014), http://dx.doi.org/10.1007/978-3-662-45611-8_9 2
49. Sun, Z., Wang, P., Zhang, L.: Weak-key and related-key analysis of hash-counter-hash tweakable enciphering schemes. In: Foo, E., Stebila, D. (eds.) ACISP 2015. Lecture Notes in Computer Science, vol. 9144, pp. 3–19. Springer (2015), http://dx.doi.org/10.1007/978-3-319-19962-7_1 2, 4
50. Wang, P., Feng, D., Wu, W.: HCTR: A variable-input-length enciphering mode. In: Feng, D., Lin, D., Yung, M. (eds.) Information Security and Cryptology, First SKLOIS Conference, CISC 2005, Beijing, China, December 15-17, 2005, Proceedings. Lecture Notes in Computer Science, vol. 3822, pp. 175–188. Springer (2005), http://dx.doi.org/10.1007/11599548_15 2, 4, 13
51. 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) 1, 3, 11
52. Wiener, M.J. (ed.): Advances in Cryptology - CRYPTO '99, Lecture Notes in Computer Science, vol. 1666. Springer (1999) 15

A Related-key security of MAC, TBC, TES and AE

1) RK-PRF. For a function $F : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$, the adversary $\mathbb{A}$ can make related-key oracle queries $(\phi, M) \in \Phi \times \mathcal{D}$ and is responded with $F_{\phi(K)}(M)$ where K is the secret key. Let ρ be a uniformly random function from $\mathcal{K} \times \mathcal{D}$ to $\mathcal{R}$. The advantage of $\mathbb{A}$ is defined as

$$\mathbf{Adv}_{\mathbf{F}}^{rk-prf}(\mathbb{A}) = \Pr[\mathbb{A}^{\mathbf{F}_{\cdot(K)}(\cdot)} \Rightarrow 1] - \Pr[\mathbb{A}^{\rho_{\cdot(K)}(\cdot)} \Rightarrow 1].$$

For all adversaries with computation time at most t, oracle queries at most q, we denote $\mathbf{Adv}_{F}^{rk-prf}(q,t) = max_{\mathbb{A}}\mathbf{Adv}_{F}^{rk-prf}(\mathbb{A})$. When the advantage is negligible, we say that F is a RK-PRF over Φ.

2) RK-UF. A message authentication code (MAC) is a function $F : \mathcal{K} \times \mathcal{N} \times \mathcal{M} \rightarrow \{0,1\}^n$, where $\mathcal{K}$, $\mathcal{N}$, $\mathcal{M}$ and $\{0,1\}^n$ are spaces of key, nonce, message and tag respectively. The nonce space can be an empty set $\mathcal{N} = \emptyset$. For a RKD set Φ, an adversary $\mathbb{A}$ queries the MAC algorithm with $(\phi, N, M) \in \Phi \times \mathcal{N} \times \mathcal{M}$ but never repeats N, and gets $T = F_{\phi(K)}(N, M)$. After several queries $\mathbb{A}$ returns a quadruple (ϕ', N', M', T') which never appear before in the queries. We define the probability of $T' = F_{\phi'(K)}(N', M')$ as the advantage of $\mathbb{A}$ and write it as:

$$\mathbf{Adv}_{F}^{rk-uf}(\mathbb{A}) = \Pr[\mathbb{A}^{F_{\cdot(K)}(\cdot,\cdot)} \text{ forges}].$$

For all adversaries with computation time at most t, oracle queries at most q, we denote $\mathbf{Adv}_{F}^{rk-uf}(q,t) = max_{\mathbb{A}}\mathbf{Adv}_{F}^{rk-uf}(\mathbb{A})$. When the advantage is negligible, we say that F is related-key unforgeable (RK-UF) or related-key unpredictable.

3) RK-STPRP and RK-SPRP. A tweakable block cipher consists of two algorithms $\mathcal{S} = (\mathbf{E}, \mathbf{D})$. The encryption algorithm $\mathbf{E} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \rightarrow \{0,1\}^n$, where $\mathcal{K}$, $\mathcal{T}$ and $\{0,1\}^n$ are spaces of key, tweak, plaintext/ciphertext respectively. For input $(K, T, P) \in \mathcal{K} \times \mathcal{T} \times \{0,1\}^n$, we write the result as $C = \mathbf{E}_K^T(P)$ The decryption algorithm $\mathbf{D} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \rightarrow \{0,1\}^n$. We require that for any $(K,T) \in \mathcal{K} \times \mathcal{T}$, $\mathbf{E}_K^T(\cdot)$ and $\mathbf{D}_K^T(\cdot)$ are permutations, and $\mathbf{D}_K^T(\mathbf{E}_K^T(P)) = P$. For a RKD set Φ, an adversary $\mathbb{A}$ queries $\mathbf{E}$ with $(\phi, T, P) \in \Phi \times \mathcal{T} \times \{0,1\}^n$ or queries $\mathbf{D}$ with $(\phi, T, C) \in \Phi \times \mathcal{T} \times \{0,1\}^n$. $\mathbb{A}$ tries to distinguish $\mathcal{S}$ from an ideal TBC, where for any $(K,T) \in \mathcal{K} \times \mathcal{T}$, π_K^T is an independent uniformly random permutation. Without loss of generality we assume that the adversary never make *pointless* queries that the adversary “knows” the answer. For example, if the adversary query (ϕ, T, P) to the encryption oracle and get the answer C, he will never query (ϕ, T, C) to the decryption oracle. We define the advantage as

$$\mathbf{Adv}_{\mathcal{S}}^{rk-stprp}(\mathbb{A}) = \Pr[\mathbb{A}^{\mathbf{E}^{\cdot}_{\cdot(K)}(\cdot),\mathbf{D}^{\cdot}_{\cdot(K)}(\cdot)} \Rightarrow 1] - \Pr[\mathbb{A}^{\pi^{\cdot}_{\cdot(K)}(\cdot),\pi^{-1\cdot}_{\cdot(K)}(\cdot)} \Rightarrow 1].$$

For all adversaries with computation time at most t, oracle queries at most q, we denote $\mathbf{Adv}_{\mathcal{S}}^{rk-stprp}(q,t) = max_{\mathbb{A}}\mathbf{Adv}_{\mathcal{S}}^{rk-stprp}(\mathbb{A})$. When the advantage is negligible, we say that $\mathcal{S}$ is a relate-key strongly tweakable pseudorandom permutation (RK-STPRP). When the tweak space $\mathcal{T}$ is a empty set $\mathbf{E}$ becomes a block cipher. The corresponding security notion is relate-key strongly pseudorandom permutation (RK-SPRP). A tweakable enciphering schemes are TBCs with large or variable input length. The definition is the same as that of TBC.

4) RK-AE. An authenticated encryptions consists of two algorithms $\mathcal{SE} = (\mathbf{E}, \mathbf{D})$. The encryption $\mathbf{E} : \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{P} \rightarrow \mathcal{C}$, where $\mathcal{K}$, $\mathcal{N}$, $\mathcal{A}$, $\mathcal{P}$ and $\mathcal{C}$ are spaces of key, nonce, associated data, plaintext and ciphertext respectively. For input $(K, N, A, P) \in \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{P}$, we write the result as $C = \mathbf{E}_K(N, A, P)$. The decryption algorithm $\mathbf{D} : \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{C} \rightarrow \mathcal{P} \cup \{\perp\}$. We require that $\mathbf{D}_K(N, A, \mathbf{E}_K(N, A, P)) = P$. For a RKD set Φ, an adversary $\mathbb{A}$ queries the $\mathbf{E}$ with $(\phi, N, A, P) \in \Phi \times \mathcal{N} \times \mathcal{A} \times \mathcal{P}$ but never repeats (ϕ, N), or queries the $\mathbf{D}$ with (ϕ, N, A, C). $\mathbb{A}$ tries to distinguish $\mathcal{SE}$ from an ideal AE $(\$, \perp)$, where for any query \$ returns a random string and $\perp$ always returns $\perp$. We define the advantage as

$$\mathbf{Adv}^{rk-ae}_{\mathcal{SE}}(\mathbb{A}) = \Pr[\mathbb{A}^{\mathbf{E}_{\cdot(K)}(\cdot,\cdot,\cdot), \mathbf{D}_{\cdot(K)}(\cdot,\cdot,\cdot)} \Rightarrow 1] - \Pr[\mathbb{A}^{\$(\cdot,\cdot,\cdot,\cdot), \perp(\cdot,\cdot,\cdot,\cdot)} \Rightarrow 1].$$

For all adversaries with computation time at most t, oracle queries at most q, we denote $\mathbf{Adv}^{rk-ae}_{\mathcal{SE}}(q, t) = max_{\mathbb{A}} \mathbf{Adv}^{rk-ae}_{\mathcal{SE}}(\mathbb{A})$. When the advantage is negligible, we say that $\mathcal{SE}$ is related-key secure.

B Existing UHFs that are not RK-AXU (RK-AU)

The following universal hash functions are proved to be AXU (A$\varDelta$U).

1) MMH [26]: $H_K(M) = (((\sum_{i=1}^{t} M_i K_i) \mod 2^{64}) \mod p) \mod 2^{32}$, $M_i, K_i \in \mathbf{Z}_{2^{32}}$ and $p = 2^{32} + 15$;
2) Square Hash [23]: $H_K(M) = \sum_{i=1}^{t} (M_i + K_i)^2 \mod p$, $M_i, K_i \in \mathbf{Z}_p$;
3) NMH [26]: $H_K(M) = (\sum_{i=1}^{t/2} (M_{2i-1} + K_{2i-1})(M_{2i} + K_{2i})) \mod p$, $M_i, K_i \in \mathbf{Z}_{2^{32}}$, $p = 2^{32} + 15$;
4) NH [13]: $H_K(M) = (\sum_{i=1}^{t/2} ((M_{2i-1} + K_{2i-1}) \mod 2^w)((M_{2i} + K_{2i}) \mod 2^w)) \mod 2^{2w}$, $M_i, K_i \in \mathbf{Z}_{2^w}$.

In 1) we set $t = 1$, then $H_K(M) = (MK \mod 2^{32} + 15) \mod 2^{32}$. If $M = M' = \varDelta' = 1$, $\varDelta = 0$, then $H_K(M) = K$, $H_{K+\varDelta'}(M') = K + 1 \mod 2^{32}$, therefore $H_K(M) + 1 = H_{K+\varDelta'}(M')$, MMH is not RK-A$\varDelta$U. 2), 3) and 4) all have the term $M_1 + K_1$. From $M_1 + K_1 = (M_1 - 1) + (K_1 + 1)$ we know that they are all not RK-AU.