Generalized Tweakable Even-Mansour Cipher and Its Applications

Ping Zhang[1], Honggang Hu[1], and Peng Wang[2]

[1] University of Science and Technology of China, Hefei, China, 230027,
zgp@mail.ustc.edu.cn,hghu2005@ustc.edu.cn
[2] Institute of Information Engineering, CAS, Beijing, China, 100049, wp@is.ac.cn

Abstract. This paper describes a generalized tweakable blockcipher HPH, which is based on a public random permutation P and a family of almost-XOR-universal (AXU) hash functions $\mathcal{H} = \{H_K\}_{K\in\mathcal{K}}$ with a key and tweak schedule, and defined as $y = HPH_K((t_1, t_2), x) = P(x \oplus H_K(t_1)) \oplus H_K(t_2)$, where K is a key randomly chosen from a key space $\mathcal{K}$, (t_1, t_2) is a tweak randomly chosen from a valid tweak space $\mathcal{T}$, x is a plaintext, and y is a ciphertext. We prove that HPH is a secure strong tweakable pseudorandom permutation (STPRP) by using H-coefficients technique. Then we focus on the security of HPH against multi-key and related-key attacks. We prove that HPH achieves both multi-key STPRP (MK-STPRP) security and related-key STPRP (RK-STPRP) security. HPH can be extended to wide applications. It can be directly applied to authentication and authenticated encryption modes. We appy HPH to PMAC1 and OPP, provide an improved authentication mode HPMAC and a new authenticated encryption mode OPH, and prove that they achieve single-key security, multi-key security, and related-key security.

Keywords: Tweakable blockcipher, HPH, universal hash function, single-key security, multi-key security, related-key security, H-coefficients technique, authentication, authenticated encryption.

1 Introduction

A tweakable blockcipher (TBC) is a generalized block cipher, which adds a tweak as an extra public input on the basis of the usual inputs (a plaintext and a key). TBCs with distinct tweaks refer to distinct block ciphers. Therefore, the cost of tweaks' update is lower than that of rekeys. The original application scenarios of TBCs focus on storage encryptions, especially the disk sector encryption [24] (Each disk contains fixed-length sectors. The size of a sector is usually 512 bytes. In the disk sector encryption, we need to encrypt a plaintext x under the sector location $t \in \mathcal{T}$ and obtain the corresponding ciphertext $y = \mathcal{E}_K(t, x)$, where K is a key randomly chosen from a key space $\mathcal{K}$ and $\mathcal{E}_K$ is an encryption algorithm with a tweak space $\mathcal{T}$. Moreover, the encryption with distinct sectors is mutual independent. Therefore, the outputs are perfectly uniform). Now TBCs have been extended to all the modes of operation, such as encryption modes

[30,25,42], authentication modes [30,43,29], and authenticated encryption (AE) modes [27,1,22,10,9,37,50]. There exist three approaches to realize a tweakable blockcipher. The first approach is based on a block cipher, such as [30,1,9]. The second approach is based on a permutation, such as [14,17,32,22]. The third approach is based on a keyed compression function (or hash function), such as [39,40].

Considering the security in the various applications, Mouha and Luykx [34] divided attack settings into three categories: single-key setting, multi-key setting, and related-key setting. In the single-key setting, an adversary has access to the encryption and decryption oracles under a fixed key. Most of previous papers considered the single-key security of the schemes, such as [30,43,1,9,10,22,41,37]. In the multi-key setting, an adversary has access to the encryption and decryption oracles under multiple keys, which are independently and randomly chosen from the key space. Multi-key setting has many applications in the real-world implementations. The multi-user [11] and broadcast [31] settings utilize multiple keys, so they belong to the multi-key setting. There exist many related researches in the multi-key, multi-user, and broadcast settings, such as [31,11,21,34,3,26,4]. In the related-key setting, an adversary has access to the encryption and decryption oracles under multiple different keys and each key exists some mathematical relationship (related-key deriving function), which is known and chosen to the adversary. Biham et al. first presented a concept of related-key attack (RKA) in [7] for block ciphers [2,8,48]. Then RKA is extended to other cryptographic algorithms such as stream ciphers [12], permutation-based ciphers [16,32], hash functions [49], MACs [38,5], and AE schemes [20]. The above three attack settings have become the important criterion in cipher designs.

The tweakable Even-Mansour cipher (TEM) [14] is a permutation-based tweakable blockcipher, which is constructed from an n-bit public random permutation P and an almost-XOR-universal (AXU) family of hash functions $\mathcal{H} = (H_K)_{K \in \mathcal{K}}$ from some tweak space $\mathcal{T}$ to $\{0,1\}^n$, and defined as

$$y = TEM_K(t, x) = P(x \oplus H_K(t)) \oplus H_K(t),$$

where K is a key randomly chosen from the key space $\mathcal{K}$, t is a tweak randomly chosen from the tweak space $\mathcal{T}$, x is an n-bit plaintext, and y is an n-bit ciphertext. In the single-key setting, TEM ensures birthday bound security, i.e., up to about $2^{n/2}$ queries, under the random permutation model (RPM).

Follow on, Mennink [32] provided a pure-permutation-based tweakable blockcipher XPX, which is constructed from an n-bit public random permutation P. Assume that K is a key randomly chosen from a key space $\mathcal{K}$ and $(t_{11}, t_{12}, t_{21}, t_{22})$ is a tweak chosen from a valid tweak space $\mathcal{T}$, XPX is defined as

$$y = XPX_K((t_{11}, t_{12}, t_{21}, t_{22}), x) = P(x \oplus \Delta_1) \oplus \Delta_2,$$

where $\Delta_1 = t_{11}K \oplus t_{12}P(K)$, $\Delta_2 = t_{21}K \oplus t_{22}P(K)$, $x \in \{0,1\}^n$ is a plaintext, and $y \in \{0,1\}^n$ is a ciphertext. XPX with a valid tweak space was proven birthday-bound-secure in the single-key and related-key settings.

Let $\Delta_1 = t_{11}K \oplus t_{12}P(K) = f_K(t_1)$ and $\Delta_2 = t_{21}K \oplus t_{22}P(K) = g_K(t_2)$, where $t_1 = (t_{11}, t_{12})$ and $t_2 = (t_{21}, t_{22})$, then we have

$$y = XPX_K((t_1, t_2), x) = P(x \oplus f_K(t_1)) \oplus g_K(t_2).$$

1.1 Our Contributions

In this paper, we are interest in generalizing XPX to the case where the masking functions are implemented by using universal hash functions. Here we use a common universal hash function H instead of two universal hash functions f and g. As the underlying permutation is invoked twice for per-message encryption in XPX (the best efficiency happens when the underlying permutation is invoked only once for per-message encryption) and universal hash functions can be efficiently implemented, here we present a generalized tweakable blockcipher HPH, which is constructed from a public n-bit random permutation P and a family of AXU hash functions $\mathcal{H} = \{H_K\}_{K \in \mathcal{K}}$ with a tweak and key schedule $(t_1, t_2, K) \in \mathcal{T} \times \mathcal{K}$, and defined as

$$y = HPH_K((t_1, t_2), x) = P(x \oplus H_K(t_1)) \oplus H_K(t_2),$$

where $K \in \mathcal{K}$ is a key, $(t_1, t_2) \in \mathcal{T}$ is a valid tweak, $x \in \{0,1\}^n$ is a plaintext, and $y \in \{0,1\}^n$ is a ciphertext. Here we must ensure that both t_1 and t_2 are distinct for all $(t_1, t_2) \in \mathcal{T}$. Otherwise, it is very easy to find the following attack about HPH. We assume that an adversary makes four distinct queries (t_1, t_2, x), (t_1, t_2', x), (t_1', t_2, x'), and (t_1', t_2', x') to HPH and receives the corresponding answers y, y', y'' and y'''. It always holds $y \oplus y' = y'' \oplus y'''$ for HPH. Whereas, for a random tweakable blockcipher, it holds with a probability of 2^{-n}. Therefore, here the tweak space $\mathcal{T}$ is called valid if it satisfies that both t_1 and t_2 are distinct for all $(t_1, t_2) \in \mathcal{T}$.

This paper focuses on the security of HPH with a valid tweak space in the single-key, multi-key, and related-key settings. HPH is proven secure in above three attack settings. Assume that D is the number of the construction queries, T is the number of the underlying permutation queries, and l is the number of keys. In the single-key setting, we prove that HPH with a family of (ϵ, δ)-AXU hash functions achieves single-key strong tweakable pseudorandom permutation (STPRP) security up to about $2DT\delta + D(D-1)\epsilon$ queries in the random permutation model (RPM). In the multi-key setting, we prove that HPH with a family of (ϵ, δ)-AXU hash functions achieves multi-key STPRP (MK-STPRP) security up to $2DT\delta + (D-l+1)(D-l)\epsilon + D^2(1-1/l)\delta$ queries in the RPM. In the related-key setting, we replace a family of AXU hash functions with a family of related-key-AXU (RKA-AXU) hash functions provided by Wang et al. [49] and prove that HPH with a family of (ϵ, δ)-RKA-AXU hash functions achieves related-key STPRP (RK-STPRP) security up to $2DT\delta + D(D-1)\epsilon$ queries in the RPM. Our proofs use Patarin's H-coefficients technique [36].

HPH is a strongly secure cryptography architecture with a higher key agility and fewer key length. Our work has a great significance in practice as rekey

is essential and the relationship between keys exists inevitability in real-world implementations. HPH is very practical as HPH is based on a permutation and can be implemented securely and efficiently. If we utilize HPH to replace the underlying tweakable blockcipher, some cryptography schemes may be designed more securely and more efficiently, such as encryption schemes, authentication schemes, and authenticated encryption schemes.

1.2 Applications

HPH can be used to improve security guarantee for encryption, authentication, and authenticated encryption (AE) modes. In this paper, we apply HPH to PMAC1 [43] and OPP [22], present an improved authentication mode HPMAC and a new AE mode OPH, and prove that they are single-key-secure, multi-key-secure, and related-key-secure.

Firstly, HPH is directly applied to an authentication mode PMAC1 [43]. PMAC1 provided by Rogaway is a TBC-based parallelizable message authentication code (MAC). Rogaway utilized a conventional block cipher to instantiate PMAC1 and proved the security of PMAC1 with a block cipher in [43]. However, the cost of the implementation for block ciphers is higher than permutations. Therefore, we replace the block cipher with a permutation, present a new simpler and faster HPMAC mode, and prove that HPMAC achieves single-key pseudorandom function (PRF) security, multi-key PRF (MK-PRF) security, and related-key PRF (RK-PRF) security.

Secondly, HPH is directly applied to an AE mode OPP [22]. OPP presented by Granger et al. is a permutation-based nonce-respecting AE mode. As Granger et al. utilized a tweak-dependent masking function based on the underlying permutation, OPP makes an extra invocation to the underlying permutation for per-message encryption. Therefore, we utilize a family of universal hash functions to replace tweak-dependent masking functions and present a new permutation-based nonce-respecting parallelizable AE mode OPH. In this paper, we prove that OPH achieves single-key AE security, multi-key AE (MK-AE) security, and related-key AE (RK-AE) security, and derive provably security bounds.

Organizations of This Paper. Some preliminaries are presented in Section 2. Three security models are provided in Section 3. HPH is described in Section 4. Three security results of HPH are derived in Section 5. Section 6 presents a HPH-based and provably secure parallelizable MAC mode HPMAC. Section 7 provides a HPH-based and provably secure AE mode OPH. Finally, we conclude this paper in Section 8.

2 Preliminaries

2.1 Notations

Let $\{0,1\}^*$ be the set containing all finite strings (including an empty string). Let n denote an integer and $\{0,1\}^n$ be the set of strings of bit-length n. For a

finite string x, $|x|$ stands for its bit-length. For two finite strings x and y, let $x\|y$ or xy be the concatenation of them. For a finite set X, let $x \xleftarrow{\$} X$ stand for a value randomly chosen from X and $|X|$ denote the number of elements in X. Let $\lceil\cdot\rceil$ be the operation that rounds up to an integer. Let $\mathcal{A}^O = 1$ be an event that an adversary $\mathcal{A}$ outputs 1 after interacting with the oracle O. Here $\mathcal{A}$ never makes a query for which the response is obviously known.

A tweakable blockcipher $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ is a function that takes a key $K \in \mathcal{K}$, a tweak $t \in \mathcal{T}$, and a plaintext $x \in \{0,1\}^n$ as inputs, and generates a ciphertext $y = \widetilde{E}(K,t,x)$, where $\mathcal{K}$ is a key space and $\mathcal{T}$ is a tweak space. For any $K \in \mathcal{K}$, $t \in \mathcal{T}$, $\widetilde{E}_K(t,\cdot) = \widetilde{E}(K,t,\cdot)$ is a permutation over $\{0,1\}^n$. Let $\widetilde{D}_K = \widetilde{E}_K^{-1}$ denote its inverse. Let $Perm(n)$ be the set of all permutations on n bits. Let $\widetilde{Perm}(\mathcal{T},n)$ be the set of all mappings from $\mathcal{T}$ to permutations on n bits.

A related-key deriving (RKD) function is a mapping that takes a key $K \in \mathcal{K}$ as an input and returns a related key $\phi(K) \in \mathcal{K}$. Let Φ be a RKD set, which consists of all RKD functions, i.e., $\Phi = \{\phi : \mathcal{K} \to \mathcal{K}\}$.

2.2 Universal Hash Functions

Here we refer to [28,49] and introduce two definitions about universal hash functions as follows.

Definition 1 ((ϵ,δ)-AXU Hash Function Family [28]). *Let $\mathcal{H} = \{H : \mathcal{K} \times \mathcal{D} \to \mathcal{R}\}$ be a set of hash functions. We say that $\mathcal{H}$ is an (ϵ,δ)-almost-XOR-universal ((ϵ,δ)-AXU) hash function family, if the following two conditions are satisfied:*

1) For any $x \in \mathcal{D}$ and $y \in \mathcal{R}$,

$$Pr[K \xleftarrow{\$} \mathcal{K} : H_K(x) = y] \leq \delta;$$

2) For any $x, x' \in \mathcal{D}$, $x \neq x'$, and $y \in \mathcal{R}$,

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

Definition 2 ((ϵ,δ)-RKA-AXU Hash Function Family [49]). *Let $\mathcal{H} = \{H : \mathcal{K} \times \mathcal{D} \to \mathcal{R}\}$ be a set of hash functions. We say that $\mathcal{H}$ is an (ϵ,δ)-related-key-almost-XOR-universal ((ϵ,δ)-RKA-AXU) hash function family with respect to a restricting RKD set Φ, if the following two conditions are satisfied:*

1) For any $\phi \in \Phi, x \in \mathcal{D}$, and $y \in \mathcal{R}$,

$$Pr[K \xleftarrow{\$} \mathcal{K} : H_{\phi(K)}(x) = y] \leq \delta;$$

2) For any $\phi, \phi' \in \Phi, x, x' \in \mathcal{D}, (\phi, x) \neq (\phi', x')$, and $y \in \mathcal{R}$,

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

Given any $\phi, \phi' \in \Phi$ and $K \in \mathcal{K}$, if $\phi(K) \neq \phi'(K)$, we say $\phi \neq \phi'$. The (ϵ, δ)-AXU hash function family is a special case of the (ϵ, δ)-RKA-AXU hash function family when the RKD set is an identity transform, i.e., $\Phi_{id} = \{\phi : K \to K\}$.

The RKA-AXU-hash function family provided by Wang et al. [49] depends on the choice of RKD sets. For some RKD sets, the RKA-AXU-hash function family may not exist. Wang et al. pointed the restricting conditions (output unpredictability and collision resistance) of the RKD set in [49]. There exist many instances about AXU (RKA-AXU) hash functions, such as [28,49].

2.3 The H-Coefficients Technique

Patarin's H-coefficients technique [36] is an important method widely used in the encryption modes [17,13,14,32], authentication modes [15], and AE modes [9,18,37]. We briefly summarize this technique as follows.

Given a real world X and an ideal world Y, considering an adversary $\mathcal{A}$ which interacts with X and Y, then the advantage of $\mathcal{A}$ is defined as

$$Adv(\mathcal{A}) = |Pr[\mathcal{A}^X = 1] - Pr[\mathcal{A}^Y = 1]|.$$

We assume without loss of generality that $\mathcal{A}$ is a deterministic adversary. The goal of $\mathcal{A}$ is to distinguish X from Y. The interaction of $\mathcal{A}$ with X or Y can be described by a transcript τ, which consists of a list of queries and responses. Let D_X (resp. D_Y) be the probability distribution on transcripts induced by X (resp. Y). A transcript τ is attainable if it occurs in Y with non-zero probability. We denote Γ the set of all attainable transcripts. The lemma of the H-coefficients technique is described as follows.

Lemma 1 (H-Coefficients Lemma). *Let $\mathcal{A}$ be a deterministic adversary. Let Γ be the set of all attainable transcripts and $\Gamma = \Gamma_{good} \cup \Gamma_{bad}$. If there exists ε_1 such that for any $\tau \in \Gamma_{good}$, one has*

$$\frac{Pr[D_X = \tau]}{Pr[D_Y = \tau]} \geq 1 - \varepsilon_1,$$

and there exists ε_2 such that

$$Pr[D_Y \in \Gamma_{bad}] \leq \varepsilon_2.$$

Then the advantage of $\mathcal{A}$ is

$$Adv(\mathcal{A}) \leq \varepsilon_1 + \varepsilon_2.$$

3 Three Security Models of Encryption

3.1 Single-Key Security Model [32]

Let $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ be a tweakable blockcipher (TBC), which is constructed by a public random permutation $P \xleftarrow{\$} Perm(n)$. Let $\widetilde{\pi}$

be a tweakable permutation randomly chosen from $\widetilde{Perm}(\mathcal{T}, n)$. The single-key security of $\widetilde{E}$ is formalized with a distinguisher that has access to two oracles (O_1, O_2): either $(\widetilde{E}_K; P)$ with $K \xleftarrow{\$} \mathcal{K}$ (Real World X) or $(\widetilde{\pi}; P)$ with $\widetilde{\pi} \xleftarrow{\$} \widetilde{Perm}(\mathcal{T}, n)$ (Ideal World Y). We consider an adversary that has access to the encryption and decryption queries for X or Y in this paper. The single-key security of $\widetilde{E}$ is defined as follows.

Definition 3 (Single-Key Security). *Let $\widetilde{E}$ be a TBC constructed by a permutation P. Let $\mathcal{A}$ be a deterministic adversary, then the (single-key) strong tweakable pseudorandom permutation (STPRP) advantage of $\mathcal{A}$ is*

$$Adv_{\widetilde{E}}^{stprp}(\mathcal{A}) = |Pr[A^{\widetilde{E}_K^{\pm}; P^{\pm}} = 1] - Pr[A^{\widetilde{\pi}^{\pm}; P^{\pm}} = 1]|,$$

where K is uniformly drawn from $\mathcal{K}$, P is uniformly drawn from $Perm(n)$, $\widetilde{\pi}$ is uniformly drawn from $\widetilde{Perm}(\mathcal{T}, n)$, and the probabilities are taken over the random choices of $K, P, \widetilde{\pi}$.

For $D, T \geq 0$, let $Adv_{\widetilde{E}}^{stprp}(D, T) = max_{\mathcal{A}} Adv_{\widetilde{E}}^{stprp}(\mathcal{A})$ denote the (single-key) STPRP security of $\widetilde{E}$ against any adversary that makes D queries to the construction $\widetilde{E}_K^{\pm}$ (data complexity) and T queries to the primitive $P^{\pm}$ (time complexity).

3.2 Multi-Key Security Model [34]

Let $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ be a TBC constructed by a permutation P. Let l be the number of keys. We assume that all adversaries perform at least one query for each key. The multi-key security of $\widetilde{E}$ is seen as a distinguisher that has access to $l+1$ oracles $(O_1, \cdots, O_l, O_{l+1})$: either $(\widetilde{E}_{K_1}, \cdots, \widetilde{E}_{K_l}; P)$ with $K_1, \cdots, K_l \xleftarrow{\$} \mathcal{K}$ (Real World X) or $(\widetilde{\pi}_1, \cdots, \widetilde{\pi}_l; P)$ with $\widetilde{\pi}_1, \cdots, \widetilde{\pi}_l \xleftarrow{\$} \widetilde{Perm}(\mathcal{T}, n)$ (Ideal World Y). We consider an adversary that makes the encryption and decryption queries for X or Y in this paper. The multi-key security of $\widetilde{E}$ is defined as follows.

Definition 4 (Multi-Key Security). *Let $\widetilde{E}$ be a TBC constructed by a permutation P. Let $\mathcal{A}$ be a deterministic adversary, then the multi-key STPRP (MK-STPRP) advantage of $\mathcal{A}$ with respect to l keys is*

$$Adv_{\widetilde{E}}^{mk-stprp}(\mathcal{A}) = |Pr[A^{\widetilde{E}_{K_1}^{\pm}, \widetilde{E}_{K_2}^{\pm}, \cdots, \widetilde{E}_{K_l}^{\pm}; P^{\pm}} = 1] - Pr[A^{\widetilde{\pi}_1^{\pm}, \widetilde{\pi}_2^{\pm}, \cdots, \widetilde{\pi}_l^{\pm}; P^{\pm}} = 1]|,$$

where $K_1, \cdots, K_l$ are independently and randomly chosen from $\mathcal{K}$, P is randomly chosen from $Perm(n)$, tweakable permutations $\widetilde{\pi}_1, \widetilde{\pi}_2, \cdots, \widetilde{\pi}_l$ are independently and randomly chosen from $\widetilde{Perm}(\mathcal{T}, n)$, and the probabilities are taken over the random choices of $K_1, \cdots, K_l$, P, and $\widetilde{\pi}_1, \widetilde{\pi}_2, \cdots, \widetilde{\pi}_l$.

For $D, T \geq 0$, let $Adv_{\widetilde{E}}^{mk-stprp}(D, T) = max_{\mathcal{A}} Adv_{\widetilde{E}}^{mk-stprp}(\mathcal{A})$ denote the MK-STPRP security of $\widetilde{E}$ against any adversary that makes D queries to the construction (data complexity) and T queries to $P^{\pm}$ (time complexity).

3.3 Related-Key Security Model [32]

Given a RKD set Φ and a TBC $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$, the related-key oracle $RK[\widetilde{E}] : \mathcal{K} \times \Phi \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ is defined as

$$RK[\widetilde{E}](K, \phi, t, x) = RK[\widetilde{E}]_K(\phi, t, x) = \widetilde{E}_{\phi(K)}(t, x),$$

where $K \in \mathcal{K}$, $\phi \in \Phi$, $t \in \mathcal{T}$, and $x \in \{0,1\}^n$. Let $\widetilde{RKPerm}(\Phi, \mathcal{T}, n)$ be the set of related-key tweakable permutations, i.e., the set of all mappings from $\Phi \times \mathcal{T}$ to permutations on n bits. The related-key security of $\widetilde{E}$ is seen as a distinguisher that has access to two oracles (O_1, O_2): either $(RK[\widetilde{E}]_K; P)$ with $K \in \mathcal{K}$ and $\phi \in \Phi$ (Real World X) or $(RK[\widetilde{\pi}]; P)$ with $RK[\widetilde{\pi}] \xleftarrow{\$} \widetilde{RKPerm}(\Phi, \mathcal{T}, n)$ (Ideal World Y). We consider an adversary that makes the encryption and decryption queries for X and Y in this paper. The related-key security of $\widetilde{E}$ is defined as follows.

Definition 5 (Related-Key Security). *Let $\widetilde{E}$ be a TBC constructed by a permutation P. Let $\mathcal{A}$ be a deterministic adversary, then the related-key STPRP (RK-STPRP) advantage of $\mathcal{A}$ with respect to a RKD set Φ is*

$$Adv_{\widetilde{E}}^{rk-stprp}(\mathcal{A}) = |Pr[\mathcal{A}^{RK[\widetilde{E}]_K^{\pm}; P^{\pm}} = 1] - Pr[\mathcal{A}^{RK[\widetilde{\pi}]^{\pm}; P^{\pm}} = 1]|,$$

where K is uniformly drawn from $\mathcal{K}$, P is uniformly drawn from $Perm(n)$, $RK[\widetilde{\pi}]$ is uniformly drawn from $\widetilde{RKPerm}(\Phi, \mathcal{T}, n)$, ϕ is uniformly drawn from Φ, and the probabilities are taken over the random choices of $\phi, K, P, RK[\widetilde{\pi}]$.

For $D, T \geq 0$, let $Adv_{\widetilde{E}}^{rk-stprp}(D, T) = max_{\mathcal{A}} Adv_{\widetilde{E}}^{rk-stprp}(\mathcal{A})$ denote the RK-STPRP security of $\widetilde{E}$ against any adversary that makes D queries to the construction (data complexity) and T queries to $P^{\pm}$ (time complexity).

4 HPH

Let $\mathcal{K}$ be a key space, $\mathcal{T} = \mathcal{D} \times \mathcal{D} = \mathcal{D}^2$ be a valid tweak space, and P be an n-bit public random permutation. Let $\mathcal{H} = \{H : \mathcal{K} \times \mathcal{D} \to \{0,1\}^n\}$ be a family of AXU hash functions. Then we present a tweakable blockcipher HPH: $\mathcal{K} \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$, which is defined as

$$y = HPH_K((t_1, t_2), x) = P(x \oplus H_K(t_1)) \oplus H_K(t_2),$$

where $H \xleftarrow{\$} \mathcal{H}$ is an AXU hash function, $K \in \mathcal{K}$ is a key, $(t_1, t_2) \in \mathcal{T}$ is a valid tweak ($t_1, t_2 \in \mathcal{D}$), $x \in \{0,1\}^n$ is a plaintext, and $y \in \{0,1\}^n$ is a ciphertext. The overview of HPH is depicted in Figure 1.

What is a valid tweak space? Here we must ensure that both t_1 and t_2 are distinct for all $(t_1, t_2) \in \mathcal{T}$. Otherwise, it is very easy to find the following attack about HPH. We assume that an adversary makes four distinct queries (t_1, t_2, x),

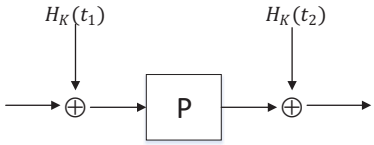


Fig. 1. HPH: Generalized Tweakable Even-Mansour Cipher

(t_1, t_2', x), (t_1', t_2, x'), and (t_1', t_2', x') to HPH and receives the corresponding answers y, y', y'' and y'''. For HPH, the equation $y \oplus y' = y'' \oplus y'''$ always holds. Whereas, for a random tweakable blockcipher, it holds with a probability of 2^{-n}. Therefore, here the tweak space $\mathcal{T}$ is called valid if it satisfies that both t_1 and t_2 are distinct for all $(t_1, t_2) \in \mathcal{T}$.

HPH is a generalized tweakable Even-Mansour cipher. 1) If $H_K(t_1) = t_{11}K \oplus t_{12}P(K)$ and $H_K(t_2) = t_{21}K \oplus t_{22}P(K)$, HPH meets the construction of XPX and inherits the security of XPX [32], where $t_1 = (t_{11}, t_{12})$, $t_2 = (t_{21}, t_{22})$, and $(t_1, t_2) \in \mathcal{T}$ is a valid tweak ($\mathcal{T}$ is a valid tweak set). 2) If $H_K(t_1) = H_K(t_2) = H_K(t)$, where $t_1 = t_2 = t$, HPH degrades into TEM and inherits the security of TEM [14]. Furthermore, if $H_K(t) = \varphi_{u-1}^{i_{u-1}} \circ \cdots \circ \varphi_0^{i_0}(P(X||K))$, HPH matches the MEM [22] construction and inherits the security of MEM, where $u \geq 1$, $\varphi_j : \{0,1\}^n \to \{0,1\}^n$, $t = (X, i_0, \cdots, i_{u-1})$ $(X \in \{0,1\}^{n-k}, i_j \geq 0)$, $K \in \{0,1\}^k$, and $0 \leq j \leq u-1$.

If the underlying permutation P is replaced with AES-128, HPH is a generalization of the XEX construction [43]. The universal hash function H can be implemented by four-round AES (AES4). Assuming round keys are mutually independent, Daemen et al. showed that AES4 is a 2^{-113}-AXU hash function in [19]. We recommend using a non-linear universal hash function family $\mathcal{H}$ to ensure the security.

5 Strong Security of HPH

In this section, we focus on the security of HPH in various attack settings and prove that HPH achieves STPRP security, MK-STPRP security, and RK-STPRP security.

5.1 Single-Key Security of HPH

Theorem 1 (Single-Key Security of HPH). *Let* $K \xleftarrow{\$} \mathcal{K}, \widetilde{\pi} \xleftarrow{\$} \widetilde{Perm}(\mathcal{T}, n)$, *and* $P \xleftarrow{\$} Perm(n)$. *Let* $\mathcal{A}$ *be an adversary that makes at most* D *queries to* $HPH_K^{\pm}$ *(resp.* $\widetilde{\pi}^{\pm}$*) and at most* T *queries to* $P^{\pm}$. *For HPH with a family of* (ϵ, δ)*-AXU hash functions, the single-key STPRP security is*

$$Adv_{HPH}^{stprp}(\mathcal{A}) \leq 2DT\delta + D(D-1)\epsilon.$$

Our proof is similar to [14]. The result of Theorem 1 is in fact a generalization of the single-key security of TEM [14].

Let $\mathcal{A}$ be an adversary, which interacts with two oracles (O_1, O_2). Here (O_1, O_2) stand for $(HPH_K^{\pm}; P^{\pm})$ in the real world X and stand for $(\widetilde{\pi}^{\pm}; P^{\pm})$ in the ideal world Y (See Figure 2).

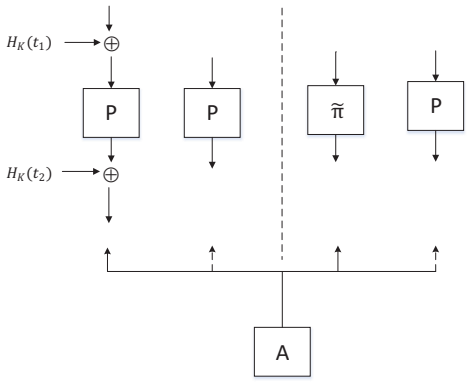


Fig. 2. Single-Key Security Model of HPH. **Left of Dashed Line**: $(O_1, O_2) = (HPH_K^{\pm}; P^{\pm})$ (Real World X). **Right of Dashed Line**: $(O_1, O_2) = (\widetilde{\pi}^{\pm}; P^{\pm})$ (Ideal World Y). Let $\mathcal{A}$ be an adversary, whose goal is to distinguish X from Y. If $Adv_{HPH}^{stprp}(\mathcal{A})$ is negligible, HPH achieves STPRP security.

Without loss of generality, we assume that $\mathcal{A}$ is a deterministic adversary. It makes D queries to O_1, and T queries to O_2. Let m be the number of distinct tweaks and D_t be the number of queries for the t-th tweak, where $1 \leq t \leq m$. Then $D = \sum_{t=1}^{m} D_t$.

The interaction of $\mathcal{A}$ with (O_1, O_2) is described by a transcript $\tau = (K, \tau_1, \tau_2)$, where $K \in \mathcal{K}$ is a key, $\tau_1 = \{(t_1^1, t_2^1, x^1, y^1), \cdots, (t_1^D, t_2^D, x^D, y^D)\}$ is the list of queries to O_1, $(t_1^1, t_2^1), \cdots, (t_1^D, t_2^D) \in \mathcal{T}$, and $\tau_2 = \{(u^1, v^1), \cdots, (u^T, v^T)\}$ is the list of queries to O_2. We assume that $\mathcal{A}$ never makes repeated queries, i.e., $(t_1^i, t_2^i, x^i) \neq (t_1^j, t_2^j, x^j), (t_1^i, t_2^i, y^i) \neq (t_1^j, t_2^j, y^j), u^i \neq u^j$, and $v^i \neq v^j$ for all i and j, where $t_1^i \neq t_1^j, t_2^i \neq t_2^j$, and $i \neq j$.

Definition 6. *We say that a transcript $\tau = (K, \tau_1, \tau_2)$ is bad if one of the following conditions is satisfied:*

Bad1: $\exists (t_1, t_2, x, y) \in \tau_1$ and $(u, v) \in \tau_2$ such that $x \oplus u = H_K(t_1)$, where $(t_1, t_2) \in \mathcal{T}$;

Bad2: $\exists (t_1, t_2, x, y) \in \tau_1$ and $(u, v) \in \tau_2$ such that $y \oplus v = H_K(t_2)$, where $(t_1, t_2) \in \mathcal{T}$;

Bad3: $\exists (t_1^i, t_2^i, x^i, y^i) \neq (t_1^j, t_2^j, x^j, y^j) \in \tau_1$ such that $x^i \oplus x^j = H_K(t_1^i) \oplus H_K(t_1^j)$, where $(t_1^i, t_2^i), (t_1^j, t_2^j) \in \mathcal{T}$, $t_1^i \neq t_1^j, t_2^i \neq t_2^j$, and $1 \leq i \neq j \leq D$;

Bad4: $\exists (t_1^i, t_2^i, x^i, y^i) \neq (t_1^j, t_2^j, x^j, y^j) \in \tau_1$ such that $y^i \oplus y^j = H_K(t_2^i) \oplus H_K(t_2^j)$, where $(t_1^i, t_2^i), (t_1^j, t_2^j) \in \mathcal{T}$, $t_1^i \neq t_1^j, t_2^i \neq t_2^j$, and $1 \leq i \neq j \leq D$.

Let Γ_{bad} be the set of bad transcripts. Let Γ be the set of attainable transcripts. Let $\Gamma_{good} = \Gamma \setminus \Gamma_{bad}$ be the set of good transcripts.

By the H-coefficients technique, we first upper bound the probability to get a bad transcript in Y.

Lemma 2. *Let H be an (ϵ, δ)-AXU hash function, then*

$$Pr[D_Y \in \Gamma_{bad}] \leq 2DT\delta + D(D-1)\epsilon.$$

Proof. Let $\tau = (K, \tau_1, \tau_2)$ be any attainable transcript. In the ideal world Y, the dummy key K is randomly chosen from $\mathcal{K}$. Let $\mathcal{A}$ be an adversary, which never makes repeated queries. Given any $(t_1, t_2, x, y) \in \tau_1$ and $(u, v) \in \tau_2$, where $(t_1, t_2) \in \mathcal{T}$, according to Definition 1, we have

$$Pr[K \xleftarrow{\$} \mathcal{K} : H_K(t_1) = x \oplus u \vee H_K(t_2) = y \oplus v] \leq 2\delta.$$

It follows that,

$$Pr[Bad1 \vee Bad2] \leq 2DT\delta.$$

Fix any distinct queries $(t_1^i, t_2^i, x^i, y^i) \neq (t_1^j, t_2^j, x^j, y^j) \in \tau_1$, where $(t_1^i, t_2^i), (t_1^j, t_2^j) \in \mathcal{T}$, $t_1^i \neq t_1^j, t_2^i \neq t_2^j$, and $1 \leq i \neq j \leq D$. By Definition 1, we have

$$Pr[K \xleftarrow{\$} \mathcal{K} : H_K(t_1^i) \oplus H_K(t_1^j) = x^i \oplus x^j \vee H_K(t_2^i) \oplus H_K(t_2^j) = y^i \oplus y^j] \leq 2\epsilon.$$

It follows that,

$$Pr[Bad3 \vee Bad4] \leq \binom{D}{2} 2\epsilon = D(D-1)\epsilon.$$

Therefore, by the formula for the union of any number of sets, we have

$$\begin{aligned} Pr[D_Y \in \Gamma_{bad}] &= Pr[\bigcup_{i=1}^{4} Badi] \\ &\leq 2DT\delta + D(D-1)\epsilon. \end{aligned}$$

This completes the proof.

We then lower bound the ratio $Pr[D_X = \tau]/Pr[D_Y = \tau]$. For a good transcript, any tuple in $\tau = (K, \tau_1, \tau_2)$ uniquely defines an input-output pair of the underlying oracle in the real world X.

Lemma 3. *Let $\tau = (K, \tau_1, \tau_2)$ be a good transcript, then*

$$\frac{Pr[D_X = \tau]}{Pr[D_Y = \tau]} \geq 1.$$

Proof. Let Ω_X (resp. Ω_Y) be the sample space in X (resp. Y). Let $\omega_X \in \Omega_X$ (resp. $\omega_Y \in \Omega_Y$) be an oracle for an adversary $\mathcal{A}$ to interact with X (resp. Y). Let $comp_X(\tau) \subseteq \Omega_X$ (resp. $comp_Y(\tau) \subseteq \Omega_Y$) be the set of ω_X (resp. ω_Y) compatible with a transcript τ.

First, we calculate $Pr[D_X = \tau] = \frac{|comp_X(\tau)|}{|\Omega_X|}$, where $|\Omega_X| = 2^n!|\mathcal{K}|$. As $\tau = (K, \tau_1, \tau_2) \in \Gamma_{good}$, the inputs or outputs of the underlying permutation are distinct for any two queries in τ and any query tuple in τ uniquely defines an input-output pair of the underlying permutation in the real world X. Because τ_1 is made up of D query tuples and τ_2 includes T query tuples, the number of $comp_X(\tau)$ equals $(2^n - D - T)!$. It follows that,

$$Pr[D_X = \tau] = \frac{(2^n - D - T)!}{2^n!|\mathcal{K}|}.$$

Second, we evaluate $Pr[D_Y = \tau] = \frac{|comp_Y(\tau)|}{|\Omega_Y|}$, where $|\Omega_Y| = (\prod_t 2^n!) \cdot 2^n!|\mathcal{K}|$ and $t \in \mathcal{T}$. By a similar reason, the number of $comp_Y(\tau)$ equals $\prod_{t=1}^{m}(2^n - D_t)!(2^n - T)!$, where $D = \sum_{t=1}^{m} D_t$. It follows that,

$$\begin{aligned} Pr[D_Y = \tau] &= \frac{\prod_{t=1}^{m}(2^n - D_t)!(2^n - T)!}{(\prod_t 2^n!) \cdot 2^n!|\mathcal{K}|} \\ &\leq \frac{(2^n - D - T)!}{2^n!|\mathcal{K}|}. \end{aligned}$$

Therefore, we lower bound the ratio $\frac{Pr[D_X=\tau]}{Pr[D_Y=\tau]} \geq 1$.

By Lemmas 1, 2, and 3, we have

$$Adv_{HPH}^{stprp}(\mathcal{A}) \leq 2DT\delta + D(D-1)\epsilon.$$

5.2 Multi-Key Security of HPH

Theorem 2 (Multi-Key Security of HPH). *Let* $K_i \xleftarrow{\$} \mathcal{K}$ *and* $\widetilde{\pi}_i \xleftarrow{\$} \widetilde{Perm}(\mathcal{T}, n)$ *for* $i = 1, \cdots, l$. *Let* $P \xleftarrow{\$} Perm(n)$. *Let* $\mathcal{A}$ *be an adversary that makes at most* D *queries to* $HPH_{K_1}^{\pm}, HPH_{K_2}^{\pm}, \cdots, HPH_{K_l}^{\pm}$ *(resp.* $\widetilde{\pi}_1^{\pm}, \widetilde{\pi}_2^{\pm}, \cdots, \widetilde{\pi}_l^{\pm}$*) and at most* T *queries to* $P^{\pm}$. *For HPH with a family of* (ϵ, δ)*-AXU hash functions, the MK-STPRP security is*

$$Adv_{HPH}^{mk-stprp}(\mathcal{A}) \leq 2DT\delta + (D - l + 1)(D - l)\epsilon + D^2(1 - 1/l)\delta.$$

The result of Theorem 2 is a generalization of the multi-key security of the Even-Mansour cipher [34]. Unlike the proof of the Even-Mansour cipher, our proof needs to consider the properties of a tweak and a family of AXU hash functions.

Let $\mathcal{A}$ be an adversary, which interacts with $l + 1$ oracles $(O_1, \cdots, O_{l+1})$. Here $(O_1, \cdots, O_{l+1})$ stand for $(HPH_{K_1}^{\pm}, \cdots, HPH_{K_l}^{\pm}; P^{\pm})$ in the real world X and stand for $(\widetilde{\pi}_1^{\pm}, \cdots, \widetilde{\pi}_l^{\pm}; P^{\pm})$ in the ideal world Y (See Figure 3).

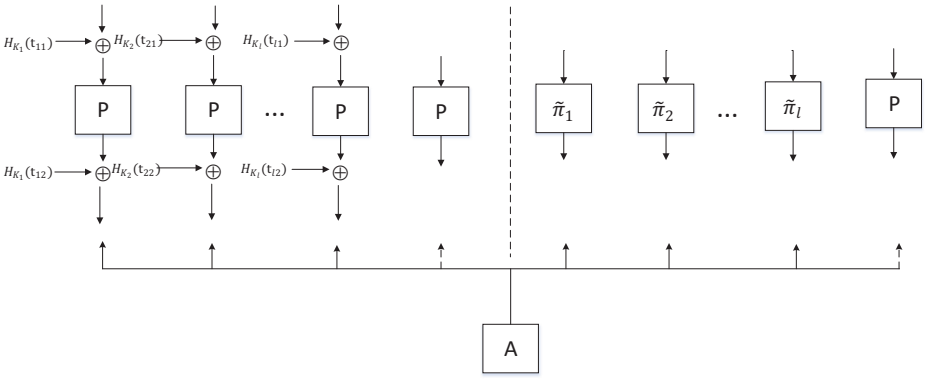


Fig. 3. Multi-Key Security Model of HPH. **Left of Dashed Line**: $(O_1, \cdots, O_{l+1}) = (HPH^{\pm}_{K_1}, \cdots, HPH^{\pm}_{K_l}; P^{\pm})$ (Real World X). **Right of Dashed Line**: $(O_1, \cdots, O_{l+1}) = (\widetilde{\pi}^{\pm}_1, \cdots, \widetilde{\pi}^{\pm}_l; P^{\pm})$ (Ideal World Y). Let $\mathcal{A}$ be an adversary, whose goal is to distinguish X from Y. If $Adv^{mk-stprp}_{HPH}(\mathcal{A})$ is negligible, HPH achieves MK-STPRP security.

Without loss of generality, we assume that $\mathcal{A}$ is a deterministic adversary. It makes D_i queries to O_i for $i = 1, \cdots, l$, and T queries to O_{l+1}. Let $D = \sum_{i=1}^{l} D_i$ (Let m be the number of distinct tweaks and D_t be the number of queries for the t-th tweak, where $1 \leq t \leq m$. Then $D = \sum_{t=1}^{m} D_t$).

The interaction of $\mathcal{A}$ with $(O_1, \cdots, O_{l+1})$ is described by a transcript $\tau = (K_1, \cdots, K_l, \tau_1, \cdots, \tau_{l+1})$. Here the list of queries to O_i is defined by $\tau_i = \{(t^1_{i1}, t^1_{i2}, x^1_i, y^1_i), \cdots, (t^{D_i}_{i1}, t^{D_i}_{i2}, x^{D_i}_i, y^{D_i}_i)\}$, where $(t^1_{i1}, t^1_{i2}), \cdots, (t^{D_i}_{i1}, t^{D_i}_{i2}) \in \mathcal{T}$ and $i = 1, \cdots, l$, and the list of queries to O_{l+1} is denoted by $\tau_{l+1} = \{(u^1, v^1), \cdots, (u^T, v^T)\}$. In this paper, $\mathcal{A}$ doesn't make redundant queries, i.e., $(t^j_{i1}, t^j_{i2}, x^j_i) \neq (t^{j'}_{i1}, t^{j'}_{i2}, x^{j'}_i), (t^j_{i1}, t^j_{i2}, y^j_i) \neq (t^{j'}_{i1}, t^{j'}_{i2}, y^{j'}_i), u^j \neq u^{j'}$, and $v^j \neq v^{j'}$ for all i, j, j', where $t^j_{i1} \neq t^{j'}_{i1}, t^j_{i2} \neq t^{j'}_{i2}$, and $j \neq j'$.

Definition 7. *We say that a transcript $\tau = (K_1, \cdots, K_l, \tau_1, \cdots, \tau_{l+1})$ is bad if one of the following conditions is satisfied:*

Bad1: $\exists (t^j_{i1}, t^j_{i2}, x^j_i, y^j_i) \in \tau_i$ and $(u^{j'}, v^{j'}) \in \tau_{l+1}$ such that $x^j_i \oplus u^{j'} = H_{K_i}(t^j_{i1})$, where $(t^j_{i1}, t^j_{i2}) \in \mathcal{T}$, $1 \leq i \leq l, 1 \leq j \leq D_i$, and $1 \leq j' \leq T$;

Bad2: $\exists (t^j_{i1}, t^j_{i2}, x^j_i, y^j_i) \in \tau_i$ and $(u^{j'}, v^{j'}) \in \tau_{l+1}$ such that $y^j_i \oplus v^{j'} = H_{K_i}(t^j_{i2})$, where $(t^j_{i1}, t^j_{i2}) \in \mathcal{T}$, $1 \leq i \leq l, 1 \leq j \leq D_i$, and $1 \leq j' \leq T$;

Bad3: $\exists (t^j_{i1}, t^j_{i2}, x^j_i, y^j_i) \neq (t^{j'}_{i1}, t^{j'}_{i2}, x^{j'}_i, y^{j'}_i) \in \tau_i$ such that $x^j_i \oplus x^{j'}_i = H_{K_i}(t^j_{i1}) \oplus H_{K_i}(t^{j'}_{i1})$, where $(t^j_{i1}, t^j_{i2}), (t^{j'}_{i1}, t^{j'}_{i2}) \in \mathcal{T}$, $t^j_{i1} \neq t^{j'}_{i1}, t^j_{i2} \neq t^{j'}_{i2}$, $1 \leq i \leq l$, and $1 \leq j \neq j' \leq D_i$;

Bad4: $\exists (t^j_{i1}, t^j_{i2}, x^j_i, y^j_i) \neq (t^{j'}_{i1}, t^{j'}_{i2}, x^{j'}_i, y^{j'}_i) \in \tau_i$ such that $y^j_i \oplus y^{j'}_i = H_{K_i}(t^j_{i2}) \oplus H_{K_i}(t^{j'}_{i2})$, where $(t^j_{i1}, t^j_{i2}), (t^{j'}_{i1}, t^{j'}_{i2}) \in \mathcal{T}$, $t^j_{i1} \neq t^{j'}_{i1}, t^j_{i2} \neq t^{j'}_{i2}$, $1 \leq i \leq l$, and $1 \leq j \neq j' \leq D_i$;

Bad5: $\exists(t^j_{i1}, t^j_{i2}, x^j_i, y^j_i) \in \tau_i$ *and* $(t^{j'}_{i'1}, t^{j'}_{i'2}, x^{j'}_{i'}, y^{j'}_{i'}) \in \tau_{i'}$ *such that* $x^j_i \oplus x^{j'}_{i'} = H_{K_i}(t^j_{i1}) \oplus H_{K_{i'}}(t^{j'}_{i'1})$, *where* $(t^j_{i1}, t^j_{i2}), (t^{j'}_{i'1}, t^{j'}_{i'2}) \in \mathcal{T}$, $1 \le i \ne i' \le l, 1 \le j \le D_i$, *and* $1 \le j' \le D_{i'}$;

Bad6: $\exists(t^j_{i1}, t^j_{i2}, x^j_i, y^j_i) \in \tau_i$ *and* $(t^{j'}_{i'1}, t^{j'}_{i'2}, x^{j'}_{i'}, y^{j'}_{i'}) \in \tau_{i'}$ *such that* $y^j_i \oplus y^{j'}_{i'} = H_{K_i}(t^j_{i2}) \oplus H_{K_{i'}}(t^{j'}_{i'2})$, *where* $(t^j_{i1}, t^j_{i2}), (t^{j'}_{i'1}, t^{j'}_{i'2}) \in \mathcal{T}$, $1 \le i \ne i' \le l, 1 \le j \le D_i$, *and* $1 \le j' \le D_{i'}$.

Let Γ_{bad} *be the set of bad transcripts. Let* Γ *be the set of attainable transcripts. Let* $\Gamma_{good} = \Gamma \setminus \Gamma_{bad}$ *be the set of good transcripts.*

By the H-coefficients technique, we first upper bound $Pr[D_Y \in \Gamma_{bad}]$.

Lemma 4. *Let* H *be an* (ϵ, δ)*-AXU hash function and* l *be the number of keys, then*

$$Pr[D_Y \in \Gamma_{bad}] \le 2DT\delta + (D - l + 1)(D - l)\epsilon + D^2(1 - 1/l)\delta.$$

Proof. In the ideal world Y, $\tau = (K_1, \cdots, K_l, \tau_1, \cdots, \tau_l, \tau_{l+1})$ is an attainable transcript with the dummy keys $K_i \in \mathcal{K}$ for $i = 1, \cdots, l$. Let $\mathcal{A}$ be an adversary, which makes at most D construction queries and at most T primitive queries and never makes repeated queries. For $(t^j_{i1}, t^j_{i2}, x^j_i, y^j_i) \in \tau_i$ and $(u^{j'}, v^{j'}) \in \tau_{l+1}$, where $(t^j_{i1}, t^j_{i2}) \in \mathcal{T}$, $1 \le i \le l, 1 \le j \le D_i$, $1 \le j' \le T$, and $D = \sum_{i=1}^{l} D_i$, by Definition 1, we have

$$Pr[K_i \xleftarrow{\$} \mathcal{K} : H_{K_i}(t^j_{i1}) = x^j_i \oplus u^{j'} \vee H_{K_i}(t^j_{i2}) = y^j_i \oplus v^{j'}] \le 2\delta.$$

It follows that,

$$\begin{aligned} Pr[Bad1 \vee Bad2] &\le \sum_{i=1}^{l} \sum_{j=1}^{D_i} \sum_{j'=1}^{T} 2\delta \\ &= \sum_{i=1}^{l} 2D_i T\delta = 2DT\delta. \end{aligned}$$

Fix any distinct queries $(t^j_{i1}, t^j_{i2}, x^j_i, y^j_i) \ne (t^{j'}_{i1}, t^{j'}_{i2}, x^{j'}_i, y^{j'}_i) \in \tau_i$, where (t^j_{i1}, t^j_{i2}), $(t^{j'}_{i1}, t^{j'}_{i2}) \in \mathcal{T}$, $t^j_{i1} \ne t^{j'}_{i1}, t^j_{i2} \ne t^{j'}_{i2}$, $1 \le i \le l$, and $1 \le j \ne j' \le D_i$. By Definition 1, we have

$$Pr[K_i \xleftarrow{\$} \mathcal{K} : H_{K_i}(t^j_{i1}) \oplus H_{K_i}(t^{j'}_{i1}) = C_1 \vee H_{K_i}(t^j_{i2}) \oplus H_{K_i}(t^{j'}_{i2}) = C_2] \le 2\epsilon,$$

where $C_1 = x^j_i \oplus x^{j'}_i$ and $C_2 = y^j_i \oplus y^{j'}_i$.

It follows that,

$$Pr[Bad3 \vee Bad4] \le 2 \sum_{i=1}^{l} \binom{D_i}{2} \epsilon.$$

As the adversary $\mathcal{A}$ makes at least one query for every key, here we consider the maximum case: $\mathcal{A}$ makes $(D-l+1)$ queries for some key and $l-1$ queries for another $l-1$ keys. Thus

$$\begin{aligned} Pr[Bad3 \vee Bad4] &\leq 2\sum_{i=1}^{l}\binom{D_i}{2}\epsilon \\ &\leq 2\binom{D-l+1}{2}\epsilon \\ &= (D-l+1)(D-l)\epsilon. \end{aligned}$$

Given any two queries $(t_{i1}^j, t_{i2}^j, x_i^j, y_i^j) \in \tau_i$ and $(t_{i'1}^{j'}, t_{i'2}^{j'}, x_{i'}^{j'}, y_{i'}^{j'}) \in \tau_{i'}$, where $(t_{i1}^j, t_{i2}^j), (t_{i'1}^{j'}, t_{i'2}^{j'}) \in \mathcal{T}$, $1 \leq i \neq i' \leq l, 1 \leq j \leq D_i$, $1 \leq j' \leq D_{i'}$, and $D = \sum_{i=1}^{l} D_i = \sum_{i'=1}^{l} D_{i'}$, we upper bound the probabilities of Bad5 and Bad6 conditions.

As K_i and $K_{i'}$ are independently and randomly chosen from $\mathcal{K}$, we can not directly utilize Definition 1. Therefore, we firstly consider the following probability.

$$\begin{aligned} &Pr[K_i, K_{i'} \xleftarrow{\$} \mathcal{K} : H_{K_i}(t_i^j) \oplus H_{K_{i'}}(t_{i'}^{j'}) = C] \\ =& \sum_{a_i, b_i \in \{0,1\}^n} Pr[K_i, K_{i'} \xleftarrow{\$} \mathcal{K} : a_i \oplus b_i = C | H_{K_i}(t_i^j) = a_i, H_{K_{i'}}(t_{i'}^{j'}) = b_i] \times \\ & \qquad Pr[K_i, K_{i'} \xleftarrow{\$} \mathcal{K} : H_{K_i}(t_i^j) = a_i, H_{K_{i'}}(t_{i'}^{j'}) = b_i] \\ \leq& \sum_{a_i \in \{0,1\}^n} Pr[K_i, K_{i'} \xleftarrow{\$} \mathcal{K} : H_{K_i}(t_i^j) = a_i, H_{K_{i'}}(t_{i'}^{j'}) = C - a_i] \quad (keys' \ independence) \\ \leq& \sum_{a_i \in \{0,1\}^n} Pr[K_i \xleftarrow{\$} \mathcal{K} : H_{K_i}(t_i^j) = a_i] \times Pr[K_{i'} \xleftarrow{\$} \mathcal{K} : H_{K_{i'}}(t_{i'}^{j'}) = C - a_i] \\ \leq& 2^n \delta^2 \leq \delta, \end{aligned}$$

where $C \in \{0,1\}^n$ is a constant and $\delta \leq 2^{-n}$.

Then we have

$$Pr[K_i, K_{i'} \xleftarrow{\$} \mathcal{K}^2 : H_{K_i}(t_{i1}^j) \oplus H_{K_{i'}}(t_{i'1}^{j'}) = C_1 \vee H_{K_i}(t_{i2}^j) \oplus H_{K_{i'}}(t_{i'2}^{j'}) = C_2] \leq 2\delta,$$

where $C_1 = x_i^j \oplus x_{i'}^{j'}$ and $C_2 = y_i^j \oplus y_{i'}^{j'}$.

It follow that,

$$\begin{aligned}Pr[Bad5 \vee Bad6] \leq & 2(\binom{D}{2} - \sum_{i=1}^{l}\binom{D_i}{2})\delta \\ = & (D^2 - D - \sum_{i=1}^{l} D_i^2 + \sum_{i=1}^{l} D_i)\delta \qquad (\sum_{i=1}^{l} D_i = D) \\ = & (D^2 - \sum_{i=1}^{l} D_i^2)\delta \qquad (Cauchy\ Inequality : \sum_{i=1}^{l} D_i^2 \geq D^2/l) \\ \leq & D^2(1 - 1/l)\delta.\end{aligned}$$

Therefore, by the formula for the union of any number of sets, we have

$$\begin{aligned}Pr[D_Y \in \Gamma_{bad}] = & Pr[\bigcup_{i=1}^{6} Badi] \\ & \leq 2DT\delta + (D - l + 1)(D - l)\epsilon + D^2(1 - 1/l)\delta.\end{aligned}$$

This completes the proof.

We then lower bound the ratio $Pr[D_X = \tau]/Pr[D_Y = \tau]$. For a good transcript, in the real world X, any tuple in $(K_1, \cdots, K_l, \tau_1, \cdots, \tau_{l+1})$ uniquely defines an input-output pair of the underlying permutation, while, in the ideal world, it is not.

Lemma 5. *Let $\tau = (K_1, \cdots, K_l, \tau_1, \cdots, \tau_{l+1})$ be a good transcript, then*

$$\frac{Pr[D_X = \tau]}{Pr[D_Y = \tau]} \geq 1.$$

Proof. Let Ω_X (resp. Ω_Y) be the sample space in X (resp. Y). Let $\omega_X \in \Omega_X$ (resp. $\omega_Y \in \Omega_Y$) be an oracle for an adversary $\mathcal{A}$ to interact with X (resp. Y). Let $comp_X(\tau) \subseteq \Omega_X$ (resp. $comp_Y(\tau) \subseteq \Omega_Y$) be the set of ω_X (resp. ω_Y) compatible with a transcript τ.

First, we compute $Pr[D_X = \tau] = \frac{|comp_X(\tau)|}{|\Omega_X|}$, where $|\Omega_X| = 2^n!|\mathcal{K}|^l$. As $\tau = (K_1, \cdots, K_l, \tau_1, \cdots, \tau_{l+1}) \in \Gamma_{good}$, the inputs or outputs of the underlying permutation are distinct for any two queries in τ and any query tuple in τ uniquely defines an input-output pair of the underlying permutation in the real world X. Because $(\tau_1, \cdots, \tau_l)$ are made up of D query tuples and τ_{l+1} includes T query tuples, the number of $comp_X(\tau)$ equals $(2^n - D - T)!$. It follows that,

$$Pr[D_X = \tau] = \frac{(2^n - D - T)!}{2^n!|\mathcal{K}|^l}.$$

Second, we evaluate $Pr[D_Y = \tau] = \frac{|comp_Y(\tau)|}{|\Omega_Y|}$, where $|\Omega_Y| = (\prod_t 2^n!)^l \cdot 2^n!|\mathcal{K}|^l$ and $t \in \mathcal{T}$. For the sake of the convenient calculation, we define

$$D_{t,i} = |\{(t_{i1}, t_{i2}, x_i, y_i) \in \tau_i | t = (t_{i1}, t_{i2}) \in \mathcal{T}, x_i, y_i \in \{0,1\}^n, 1 \leq i \leq l\}|.$$

By a similar reason, the number of $comp_Y(\tau)$ equals $\prod_t \prod_{i=1}^{l}(2^n - D_{t,i})!(2^n - T)!$, where $D = \sum_t \sum_{i=1}^{l} D_{t,i}$. It follows that,

$$\begin{aligned} Pr[D_Y = \tau] &= \frac{\prod_t \prod_{i=1}^{l}(2^n - D_{t,i})!(2^n - T)!}{(\prod_t 2^n!)^l \cdot 2^n!|\mathcal{K}|^l} \\ &\leq \frac{(2^n - D - T)!}{2^n!|\mathcal{K}|^l}. \end{aligned}$$

Therefore, we lower bound the ratio $\frac{Pr[D_X=\tau]}{Pr[D_Y=\tau]} \geq 1$.

By Lemmas 1, 4, and 5, we have

$$Adv_{HPH}^{mk-stprp}(\mathcal{A}) \leq 2DT\delta + (D - l + 1)(D - l)\epsilon + D^2(1 - 1/l)\delta.$$

Remark 1. The single-key security of HPH is a particular case of the multi-key security when $l = 1$. We prove that the multi-key security of HPH is a straightforward generalization of the single-key security. Therefore, the bound of HPH that we derive in the multi-key setting is tight. Meanwhile, we present a positive answer for the problem whether TEM is multi-key secure up to the birthday bound in [23].

5.3 Related-Key Security of HPH

Theorem 3 (Related-Key Security of HPH). *Let* $K \xleftarrow{\$} \mathcal{K}, RK[\widetilde{\pi}] \xleftarrow{\$} \widetilde{RKPerm}(\Phi, \mathcal{T}, n)$, *and* $P \xleftarrow{\$} Perm(n)$. *Let* $\mathcal{A}$ *be an adversary that makes at most* D *queries to* $RK[HPH]_K^{\pm}$ *(resp.* $RK[\widetilde{\pi}]^{\pm}$*) and at most* T *queries to* $P^{\pm}$. *For HPH with a family of* (ϵ, δ)*-RKA-AXU hash functions, the RK-STPRP security of HPH with respect to a RKD set* Φ *is*

$$Adv_{HPH}^{rk-stprp}(\mathcal{A}) \leq 2DT\delta + D(D - 1)\epsilon.$$

The proof is similar to that of Theorem 1. Let $\mathcal{A}$ be an adversary, which interacts with two oracles (O_1, O_2). Here (O_1, O_2) stand for $(RK[HPH]_K^{\pm}; P^{\pm})$ in the real world X and stand for $(RK[\widetilde{\pi}]^{\pm}; P^{\pm})$ in the ideal world Y (See Figure 4). Without loss of generality, we assume that $\mathcal{A}$ is a deterministic adversary.

The interaction of $\mathcal{A}$ with (O_1, O_2) is described by a transcript $\tau = (K, \tau_1, \tau_2)$, where $K \in \mathcal{K}$ is a key, $\tau_1 = \{(\phi^1, t_1^1, t_2^1, x^1, y^1), \cdots, (\phi^D, t_1^D, t_2^D, x^D, y^D)\}$ is the list of queries to O_1, $(\phi^i, (t_1^i, t_2^i)) \in (\Phi, \mathcal{T})$ for $1 \leq i \leq D$, and $\tau_2 = \{(u^1, v^1), \cdots, (u^T, v^T)\}$ is the list of queries to O_2. We assume that $\mathcal{A}$ never makes duplicate queries, i.e., $(\phi^i, t_1^i, t_2^i, x^i) \neq (\phi^j, t_1^j, t_2^j, x^j), (\phi^i, t_1^i, t_2^i, y^i) \neq (\phi^j, t_1^j, t_2^j, y^j), u^i \neq u^j, v^i \neq v^j$ for all i, j, where $t_1^i \neq t_1^j, t_2^i \neq t_2^j$, and $i \neq j$.

Definition 8. *We say that a transcript* $\tau = (K, \tau_1, \tau_2)$ *is bad if one of the following conditions holds:*

Bad1: $\exists(\phi, t_1, t_2, x, y) \in \tau_1$ *and* $(u, v) \in \tau_2$ *such that* $x \oplus u = H_{\phi(K)}(t_1)$, *where* $\phi \in \Phi$ *and* $(t_1, t_2) \in \mathcal{T}$;

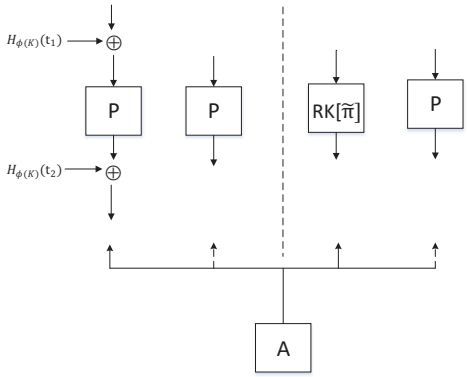


Fig. 4. Related-Key Security Model of HPH. **Left of Dashed Line**: $(O_1, O_2) = (RK[HPH]_K^{\pm}; P^{\pm})$ (Real World X). **Right of Dashed Line**: $(O_1, O_2) = (RK[\tilde{\pi}]^{\pm}; P^{\pm})$ (Ideal World Y). Let $\mathcal{A}$ be an adversary, whose goal is to distinguish X from Y. If $Adv_{HPH}^{rk-stprp}(\mathcal{A})$ is negligible, HPH achieves RK-STPRP security.

Bad2: $\exists(\phi, t_1, t_2, x, y) \in \tau_1$ *and* $(u, v) \in \tau_2$ *such that* $y \oplus v = H_{\phi(K)}(t_2)$*, where* $\phi \in \Phi$ *and* $(t_1, t_2) \in \mathcal{T}$*;*

Bad3: $\exists(\phi^i, t_1^i, t_2^i, x^i, y^i) \neq (\phi^j, t_1^j, t_2^j, x^j, y^j) \in \tau_1$ *such that* $x^i \oplus x^j = H_{\phi^i(K)}(t_1^i) \oplus H_{\phi^j(K)}(t_1^j)$*, where* $\phi^i, \phi^j \in \Phi, (t_1^i, t_2^i), (t_1^j, t_2^j) \in \mathcal{T}$*,* $t_1^i \neq t_1^j, t_2^i \neq t_2^j$*, and* $1 \leq i \neq j \leq D$*;*

Bad4: $\exists(\phi^i, t_1^i, t_2^i, x^i, y^i) \neq (\phi^j, t_1^j, t_2^j, x^j, y^j) \in \tau_1$ *such that* $y^i \oplus y^j = H_{\phi^i(K)}(t_2^i) \oplus H_{\phi^j(K)}(t_2^j)$*, where* $\phi^i, \phi^j \in \Phi, (t_1^i, t_2^i), (t_1^j, t_2^j) \in \mathcal{T}$*,* $t_1^i \neq t_1^j, t_2^i \neq t_2^j$*, and* $1 \leq i \neq j \leq D$*.*

Let Γ_{bad} *be the set of bad transcripts. Let* Γ *be the set of attainable transcripts. Let* $\Gamma_{good} = \Gamma \setminus \Gamma_{bad}$ *be the set of good transcripts.*

By the H-coefficients technique, we first upper bound the probability to get a bad transcript in Y.

Lemma 6. *Let* H *be an* (ϵ, δ)*-RKA-AXU hash function with respect to a RKD set* Φ*, then*

$$Pr[D_Y \in \Gamma_{bad}] \leq 2DT\delta + D(D-1)\epsilon.$$

Proof. Let $\tau = (K, \tau_1, \tau_2)$ be any attainable transcript. In the ideal world Y, the dummy key K is randomly chosen from $\mathcal{K}$. Let $\mathcal{A}$ be an adversary, which never makes repeated queries. For any $(\phi, t_1, t_2, x, y) \in \tau_1$, where $\phi \in \Phi$ and $(t_1, t_2) \in \mathcal{T}$, and $(u, v) \in \tau_2$, by Definition 2, we have

$$Pr[K \xleftarrow{\$} \mathcal{K} : H_{\phi(K)}(t_1) = x \oplus u \vee H_{\phi(K)}(t_2) = y \oplus v] \leq 2\delta.$$

It follows that,

$$Pr[Bad1 \vee Bad2] \leq 2DT\delta.$$

For any distinct queries $(\phi^i, t_1^i, t_2^i, x^i, y^i) \neq (\phi^j, t_1^j, t_2^j, x^j, y^j) \in \tau_1$, where $\phi^i, \phi^j \in \Phi, (t_1^i, t_2^i), (t_1^j, t_2^j) \in \mathcal{T}$, $t_1^i \neq t_1^j, t_2^i \neq t_2^j$, and $1 \leq i \neq j \leq D$, by Definition 2, we have

$$Pr[K \xleftarrow{\$} \mathcal{K} : H_{\phi^i(K)}(t_1^i) \oplus H_{\phi^j(K)}(t_1^j) = C_1 \vee H_{\phi^i(K)}(t_2^i) \oplus H_{\phi^j(K)}(t_2^j) = C_2] \leq 2\epsilon,$$

where $C_1 = x^i \oplus x^j$ and $C_2 = y^i \oplus y^j$.

It follows that,

$$Pr[Bad3 \vee Bad4] \leq \binom{D}{2} 2\epsilon = D(D-1)\epsilon.$$

Therefore, by the formula for the union of any number of sets, we have

$$\begin{aligned} Pr[D_Y \in \Gamma_{bad}] &= Pr[\bigcup_{i=1}^{4} Badi] \\ &\leq 2DT\delta + D(D-1)\epsilon. \end{aligned}$$

This completes the proof.

We then lower bound the ratio $Pr[D_X = \tau]/Pr[D_Y = \tau]$.

Lemma 7. *Let $\tau = (K, \tau_1, \tau_2)$ be a good transcript, then*

$$\frac{Pr[D_X = \tau]}{Pr[D_Y = \tau]} \geq 1.$$

Proof. Let Ω_X (resp. Ω_Y) be the sample space in X (resp. Y). Let $\omega_X \in \Omega_X$ (resp. $\omega_Y \in \Omega_Y$) be an oracle for an adversary $\mathcal{A}$ to interact with X (resp. Y). Let $comp_X(\tau) \subseteq \Omega_X$ (resp. $comp_Y(\tau) \subseteq \Omega_Y$) be the set of ω_X (resp. ω_Y) compatible with a transcript τ.

First, we compute $Pr[D_X = \tau] = \frac{|comp_X(\tau)|}{|\Omega_X|}$, where $|\Omega_X| = 2^n!|\mathcal{K}|$. As $\tau = (K, \tau_1, \tau_2) \in \Gamma_{good}$, the inputs or outputs of the underlying permutation are distinct for any two queries in τ and any query tuple in τ uniquely defines an input-output pair of the underlying permutation in the real world X. Because τ_1 is made up of D query tuples and τ_2 includes T query tuples, the number of $comp_X(\tau)$ equals $(2^n - D - T)!$. It follows that,

$$Pr[D_X = \tau] = \frac{(2^n - D - T)!}{2^n!|\mathcal{K}|}.$$

Second, we evaluate $Pr[D_Y = \tau] = \frac{|comp_Y(\tau)|}{|\Omega_Y|}$, where $|\Omega_Y| = \prod_{\phi,t}(2^n!) \cdot 2^n!|\mathcal{K}|$ and $(\phi, t) \in (\Phi, \mathcal{T})$. For the sake of the convenient calculation, we define

$$D_{\phi,t} = |\{(\phi, (t_1, t_2), x, y) \in \tau_1 | (\phi, (t_1, t_2)) \in (\Phi, \mathcal{T}), x, y \in \{0,1\}^n\}|.$$

By similar analyses, the number of $comp_Y(\tau)$ equals $\prod_{\phi,t}(2^n - D_{\phi,t})!(2^n - T)!$, where $\sum_{\phi,t} D_{\phi,t} = D$. Therefore, we have

$$\begin{aligned} Pr[D_Y = \tau] &= \frac{\prod_{\phi,t}(2^n - D_{\phi,t})!(2^n - T)!}{\prod_{\phi,t}(2^n!) \cdot 2^n!|\mathcal{K}|} \\ &\leq \frac{(2^n - D - T)!}{2^n!|\mathcal{K}|}. \end{aligned}$$

Therefore, we lower bound the ratio $\frac{Pr[D_X=\tau]}{Pr[D_Y=\tau]} \geq 1$.

By Lemmas 1, 6, and 7, we have

$$Adv_{HPH}^{rk-stprp}(\mathcal{A}) \leq 2DT\delta + D(D-1)\epsilon.$$

Remark 2. The single-key security of HPH is also a particular case of the related-key security if the RKD set is an identity transform, i.e., $\Phi_{id} = \{\phi : K \to K\}$. Furthermore, the bound of HPH that we derive in the related-key setting is also tight.

6 Application to Authentication

HPH can be used to improve security guarantee for authentication modes. Mennink applied XPX to Chaskey' (a modified version of Chaskey [35]) and proved its security in [32]. HPH is a generalization of XPX, therefore HPH can be applied to Chaskey'. In this section, we apply HPH to PMAC1, provide a new improved authentication mode HPMAC, and prove its security in the single-key, multi-key, and related-key attack settings.

6.1 Three Security Models of Authentication

Authentication mode is a cryptographic scheme, which guarantees message authenticity or integrity, such as [43,11,38,5,35,15,3]. Message authentication codes (MACs) are the most typical authentication modes. In this part, we consider a pseudorandom function (PRF) security model for MACs.

Let $F : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$ be a MAC function constructed by a public random permutation $P \xleftarrow{\$} Perm(n)$, which inputs a key $K \in \mathcal{K}$ and a message $M \in \mathcal{M}$, and outputs a tag $T \in \mathcal{T}$. Let \$ $(\$_1, \cdots, \$_l)$ be the randomized version of F_K $(F_{K_1}, \cdots, F_{K_l})$, which always returns a fresh and random response for each query. Let $\mathcal{A}$ be an adversary, which never makes repeated queries. Then the (single-key) PRF security of F is denoted as

$$Adv_F^{prf}(\mathcal{A}) = |Pr[\mathcal{A}^{F_K;P^{\pm}} = 1] - Pr[\mathcal{A}^{\$;P^{\pm}} = 1]|,$$

where the probabilities are taken over the random coins of K, P, and \$.

Similarity, we generalize it to multi-key PRF (MK-PRF) security and related-key PRF (RK-PRF) security of F.

The MK-PRF security of F with respect to l keys is denoted as

$$Adv_F^{mk-prf}(\mathcal{A}) = |Pr[\mathcal{A}^{F_{K_1},\cdots,F_{K_l};P^{\pm}} = 1] - Pr[\mathcal{A}^{\$_1,\cdots,\$_l;P^{\pm}} = 1]|,$$

where the probabilities are taken over the random coins of $K_1 \cdots, K_l, P$, and $\$_1, \cdots, \$_l$.

The RK-PRF security of F with respect to a RKD set Φ is denoted as

$$Adv_F^{rk-prf}(\mathcal{A}) = |Pr[\mathcal{A}^{RK[F]_K;P^{\pm}} = 1] - Pr[\mathcal{A}^{RK[\$];P^{\pm}} = 1]|,$$

where the probabilities are taken over the random coins of $RK[\$] : \Phi \times \mathcal{M} \to \mathcal{T}$, $\phi \in \Phi, K$, and P.

For $q, D, T \geq 0$, let $Adv_F^{(sk)/mk/rk-prf}(q, D, T) = max_{\mathcal{A}} Adv_F^{(sk)/mk/rk-prf}(\mathcal{A})$ be the (single-key) PRF (resp. MK-PRF, RK-PRF) security of F against any adversary that makes q queries to the construction (D queries complexity) and T queries to the primitive $P^{\pm}$ (time complexity).

6.2 HPMAC: HPH-based Parallelizable MAC

We apply HPH to PMAC1 [43] and present a new permutation-based parallelizable MAC, called HPMAC. HPMAC inherits all advantages of PMAC1.

PMAC1 provided by Rogaway is a TBC-based parallelizable message authentication code. Rogaway utilized a conventional block cipher to instantiate PMAC1 and proved the security of PMAC1 with a block cipher. However, the cost of the implementation for block ciphers is higher than permutations. Therefore, we replace the block cipher with a permutation, present a new simpler and faster HPMAC mode, and prove that HPMAC achieves single-key PRF security, MK-PRF security, and RK-PRF security.

Let $\mathcal{H}$ be a family of (ϵ, δ)-AXU hash functions, $K \in \mathcal{K}$ be a key, and $M = M_1 \cdots M_m \in \mathcal{M}$ be a message, where $m = \lceil |M|/n \rceil$. Let $T \in \mathcal{T}$ be the authentication tag. The overview of HPMAC: $\mathcal{K} \times \mathcal{M} \to \mathcal{T}$ is shown in Figure 5. The authentication algorithm of HPMAC is given in Figure 6.

Next, we derive the single-key PRF security, MK-PRF security, and RK-PRF security of HPMAC as follows.

Theorem 4. *Let H be (ϵ, δ)-(RKA)-AXU and l be the number of keys. Then we have*

$$Adv_{HPMAC}^{prf}(q, D, T) \leq 2DT\delta + D(D-1)\epsilon + D^2/2^n,$$
$$Adv_{HPMAC}^{mk-prf}(q, D, T) \leq 2DT\delta + (D-l+1)(D-l)\epsilon + D^2(1-\frac{1}{l})\delta + D^2/2^n,$$
$$Adv_{HPMAC}^{rk-prf}(q, D, T) \leq 2DT\delta + D(D-1)\epsilon + D^2/2^n.$$

Proof. The provable security of HPMAC is similar to PMAC1 [43]. First, we consider the single-key PRF security of HPMAC and replace all HPH

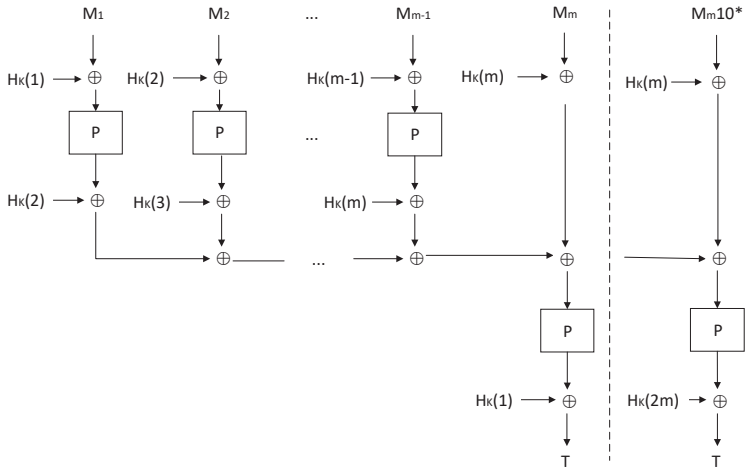


Fig. 5. HPH-based Parallelizable MAC: HPMAC

Algorithm $\mathrm{HPMAC}_K(M)$:
Partition M into $M_1 \| \cdots \| M_m$
$|M_i| = n, 1 \le i \le m-1, 0 < |M_m| \le n$
for $i = 1$ to $m-1$
  $Y_i \leftarrow P(M_i \oplus H_K(i)) \oplus H_K(i+1)$
If $|M_m| = n$, then $\Sigma = P(M_m \oplus H_K(m) \oplus Y_1 \oplus \cdots \oplus Y_{m-1}) \oplus H_K(1)$
  else $\Sigma = P(M_m 10^* \oplus H_K(m) \oplus Y_1 \oplus \cdots \oplus Y_{m-1}) \oplus H_K(2m)$
$T = \Sigma$[first τ bits]
return T

Fig. 6. HPH-based Parallelizable MAC Algorithm: HPMAC

constructions in HPMAC with random tweakable permutations. By a hybrid argument, we have

$$Adv^{prf}_{HPMAC}(q, D, T) \le Adv^{stprp}_{HPH}(D, T) + Adv^{tprf}_{HPMAC[\widetilde{Perm}(\mathcal{T},n)]}(q, D, T).$$

According to Theorem 15 of the full version of PMAC1 [43], we have

$$Adv^{tprf}_{HPMAC[\widetilde{Perm}(\mathcal{T},n)]}(q, D, T) = Adv^{tprf}_{PMAC1[\widetilde{Perm}(\mathcal{T},n)]}(q, D, T) \le D^2/2^n.$$

It follows that, by Theorem 1, the single-key PRF security of HPMAC is

$$\begin{aligned} Adv^{prf}_{HPMAC}(q, D, T) &\le Adv^{stprp}_{HPH}(D, T) + D^2/2^n \\ &\le 2DT\delta + D(D-1)\epsilon + D^2/2^n. \end{aligned}$$

Then, we consider the MK-PRF security and RK-PRF security of HPMAC. As their proof is similar to that of the single-key PRF security, according to the above process, we can easily bound their security. Here we omit the details of their proof.

7 Application to Authenticated Encryption (AE)

HPH can be used to improve security guarantee for AE modes. Mennink applied XPX to AE modes (such as COPA [1], Minalper [45], and keyed-Sponge AE [33]) and proved that they are all related-key-secure in [32]. HPH is a generalization of XPX, therefore HPH can be applied to these modes. In this section, we apply HPH to OPP [22], provide a new permutation-based nonce-respecting parallelizable AE mode OPH, and prove its security against single-key, multi-key, and related-key attacks.

7.1 Three Security Models of AE

AE mode is a cryptographic scheme, which provides both privacy and authenticity. Some examples include [44,30,43,18,27,1,47,22,10,9,37,41,46]. An AE scheme Π consists of an encryption algorithm $\mathcal{E} : \mathcal{K} \times \mathcal{N} \times \mathcal{M} \to \mathcal{C} \times \mathcal{T}$ and a decryption algorithm $\mathcal{D}$: $\mathcal{K} \times \mathcal{N} \times \mathcal{C} \times \mathcal{T} \to \mathcal{M} \cup \perp$.

Let $\Pi = (\mathcal{E}, \mathcal{D})$ be an AE scheme, which is constructed by a public random permutation $P \xleftarrow{\$} Perm(n)$. Let K be a key randomly chosen from the key space $\mathcal{K}$. Let \$ be the randomized version of $\mathcal{E}_K$, which always returns a fresh and random response for each query. The symbol $\perp$ indicates the failure of the decryption oracle. Let $\mathcal{A}$ be an adversary, which never makes repeated queries. We define the (single-key) AE security of Π as

$$Adv^{ae}_{\Pi}(\mathcal{A}) = |Pr[\mathcal{A}^{\mathcal{E}_K, \mathcal{D}_K; P^{\pm}} = 1] - Pr[\mathcal{A}^{\$, \perp; P^{\pm}} = 1]|,$$

where the probabilities are taken over the random choices of K, P, and \$.

Similarity, we generalize it to multi-key AE (MK-AE) security and related-key AE (RK-AE) security.

The MK-AE security of Π with respect to l keys is denoted as

$$Adv^{mk-ae}_{\Pi}(\mathcal{A}) = |Pr[\mathcal{A}^{\mathcal{E}_{K_1}, \mathcal{D}_{K_1}, \cdots, \mathcal{E}_{K_l}, \mathcal{D}_{K_l}; P^{\pm}} = 1] - Pr[\mathcal{A}^{\$_1, \perp, \cdots, \$_l, \perp; P^{\pm}} = 1]|,$$

where the probabilities are taken over the random choices of $K_1, \cdots, K_l, P$, and $\$_1, \cdots, \$_l$.

The RK-AE security of Π with respect to a RKD set Φ is denoted as

$$Adv^{rk-ae}_{\Pi}(\mathcal{A}) = |Pr[\mathcal{A}^{RK[\mathcal{E}]_K, RK[\mathcal{D}]_K; P^{\pm}} = 1] - Pr[\mathcal{A}^{RK[\$], \perp; P^{\pm}} = 1]|,$$

where the probabilities are taken over the random choices of $RK[\$] : \Phi \times \mathcal{N} \times \mathcal{M} \to \mathcal{C} \times \mathcal{T}$, K, and P.

For $q, D, T \geq 0$, let $Adv^{(sk)/mk/rk-ae}_{\Pi}(q, D, T) = max_{\mathcal{A}} Adv^{(sk)/mk/rk-ae}_{\Pi}(\mathcal{A})$ be the (single-key) AE (resp. MK-AE, RK-AE) security of Π against any adversary that makes q queries to the construction (the query complexity D) and T queries to the primitive $P^{\pm}$ (time complexity).

7.2 OPH

We apply HPH to OPP [22], present a new nonce-respecting parallelizable AE mode, called OPH (Offset public Permutation with universal Hash functions), and prove that OPH achieves single-key AE security, MK-AE security, and RK-AE security.

Offset Public Permutation (OPP) is a permutation-based nonce-respecting parallelizable AE mode presented by Granger et al. [22]. It utilizes a tweak-dependent masking function, which combines the word-oriented LFSR method and the powering-up technique. As the tweak-dependent masking function of OPP is based on the underlying primitive, OPP makes an extra invocation to the underlying permutation for per-message encryption. While the masking sequence of OPH is generated by a family of universal hash functions. Therefore, the efficiency of OPH may be better than OPP.

Let $\mathcal{H}$ be an (ϵ, δ)-AXU hash function family, $N \in \mathcal{N}$ be a nonce, $K \in \mathcal{K}$ be a key, and $M = M_1 \cdots M_m \in \mathcal{M}$ be a message, where $m = \lceil |M|/n \rceil$. Let $C = C_1 \cdots C_m \in \mathcal{C}$ be a ciphertext and $T \in \mathcal{T}$ be the authentication tag. To improve the efficiency of OPH, the masking sequence is defined by $\{(X_1, Y_1), \cdots, (X_{m+1}, Y_{m+1})\}$, where $X_i = H_K(N, i)$ for $1 \le i \le m$, $Y_i = X_{i+1}$ for $1 \le i \le m-1$, $Y_m = X_1$, and $Y_{m+1} = X_{m+1} = H_K(N, 2m)$. The overview of OPH: $\mathcal{K} \times \mathcal{N} \times \mathcal{M} \to \mathcal{C} \times \mathcal{T}$ is shown in Figure 7. The encryption and decryption algorithms of OPH are given in Figure 8.

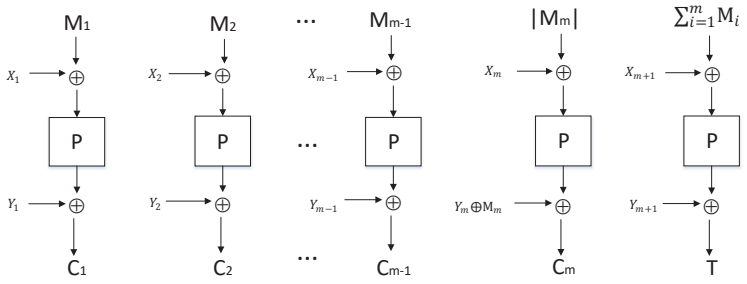


Fig. 7. HPH-based Authenticated Encryption Mode OPH

Next, we derive the single-key AE security, MK-AE security, and RK-AE security of OPH as follows.

Theorem 5. *Let $P \leftarrow Perm(n)$ be an n-bit public permutation, $\mathcal{H}$ be a family of (ϵ, δ)-(RKA)-AXU hash functions, l be the number of keys, and τ be the bit-*

/*Encryption Algorithm*/	/*Decryption Algorithm*/
Algorithm $OPH.\mathcal{E}_K^N(M)$:	**Algorithm** $OPH.\mathcal{D}_K^N(C\|\|T)$:
Partition M into $M_1\|\cdots\|M_m$,	Partition C into $C_1\|\cdots\|C_m$,
$\|M_i\| = n, 1 \le i \le m-1, 0 < \|M_m\| \le n$	$\|C_i\| = n, 1 \le i \le m-1, 0 < \|C_m\| \le n$
for $i = 1$ to m: $X_i \leftarrow H_K(N, i)$	for $i = 1$ to m: $X_i \leftarrow H_K(N, i)$
$X_{m+1} \leftarrow H_K(N, 2m)$	$X_{m+1} \leftarrow H_K(N, 2m)$
for $i = 1$ to $m-1$: $Y_i \leftarrow X_{i+1}$	for $i = 1$ to $m-1$: $Y_i \leftarrow X_{i+1}$
$Y_m \leftarrow X_1$, $Y_{m+1} \leftarrow X_{m+1}$	$Y_m \leftarrow X_1$, $Y_{m+1} \leftarrow X_{m+1}$
for $i = 1$ to $m-1$	for $i = 1$ to $m-1$
$\quad C_i \leftarrow P(M_i \oplus X_i) \oplus Y_i$	$\quad M_i \leftarrow P^{-1}(C_i \oplus Y_i) \oplus X_i$
$S \leftarrow P(\|M_m\| \oplus X_m) \oplus Y_m$	$S \leftarrow P(\|C_m\| \oplus X_m) \oplus Y_m$
$C_m \leftarrow S$[first $\|M_m\|$ bits]$\oplus M_m$	$M_m \leftarrow S$[first $\|C_m\|$ bits]$\oplus C_m$
$C \leftarrow C_1 C_2 \cdots C_m$	$M \leftarrow M_1 M_2 \cdots M_m$
$C_{m+1} = P(\sum_{i=1}^m M_i \oplus X_{m+1}) \oplus Y_{m+1}$	$C_{m+1} = P(\sum_{i=1}^m M_i \oplus X_{m+1}) \oplus Y_{m+1}$
$T = C_{m+1}$[first τ bits]	$T' = C_{m+1}$[first τ bits]
return $C\|\|T$	If $T' = T$, return M, else return $\perp$

Fig. 8. HPH-based Authenticated Encryption Algorithm OPH

length of the authentication tag. Then, in the nonce-respecting setting, we have

$$Adv_{OPH}^{ae}(q, D, T) \le 2DT\delta + D(D-1)\epsilon + 2^{n-\tau}/(2^n - 1),$$

$$Adv_{OPH}^{mk-ae}(q, D, T) \le 2DT\delta + (D-l+1)(D-l)\epsilon + D^2(1 - \frac{1}{l})\delta + l2^{n-\tau}/(2^n - 1),$$

$$Adv_{OPH}^{rk-ae}(q, D, T) \le 2DT\delta + D(D-1)\epsilon + 2^{n-\tau}/(2^n - 1).$$

Proof. The provable security of OPH is similar to OPP [22]. First, we consider the single-key AE security of OPH and replace all HPH constructions in OPH with random tweakable permutations. Using a hybrid argument, we have

$$Adv_{OPH}^{ae}(q, D, T) \le Adv_{HPH}^{stprp}(D, T) + Adv_{OPH[\widetilde{Perm}(\mathcal{T},n)]}^{ae}(q, D, T).$$

According to the AE security of OCB3 of Krovetz and Rogaway [27] (or the AE security of OPP of Granger et al. [22]), we have

$$Adv_{OPH[\widetilde{Perm}(\mathcal{T},n)]}^{ae}(q, D, T) \le 2^{n-\tau}/(2^n - 1).$$

It follows that, by Theorem 1, the single-key AE security of OPH is

$$Adv_{OPH}^{ae}(q, D, T) \le 2DT\delta + D(D-1)\epsilon + 2^{n-\tau}/(2^n - 1).$$

For the MK-AE security and RK-AE security of OPH, their proof is similar to that of the single-key AE security. Therefore, we omit it.

Remark 3. To design an authenticated encryption with associated data (AEAD) mode, we can combine HPMAC for handling an associated data A and OPH for processing a message M: $\text{HPMAC}_K(A) \oplus OPH_K^N(M)$, where $\oplus$ XORs

into the end. To design a misuse resistant AE mode, we replace MEM with HPH in MRO [22]. Then the authentication tag is generated by HPMAC, i.e., T=HPMAC$_K(A||M)$. The ciphertext is generated by CTR-like mode with HPH, i.e., C=CTR-like$_K(T, M)$.

Remark 4. If the underlying permutation is replaced with AES-128, OPH is a generalization of OCB [43,27] and the family of AXU-hash functions can be efficiently implemented by four-round AES.

8 Conclusion

In this paper, we present a generalized tweakable blockcipher HPH, whose masking functions are implemented by using universal hash functions. We prove that HPH achieves strong tweakable pseudorandom permutation (STPRP) security in the random permutation model. In the real world, a message can be encrypted under multiple keys. This paper focuses on the security of HPH against multi-key and related-key attacks. In the multi-key setting, these keys are mutually independent and random. However, in the related-key setting, these keys exist some mathematical relationship known by the adversary. We prove that HPH is both MK-STPRP-secure and RK-STPRP-secure.

HPH is a strongly secure cryptography architecture with a higher key agility and fewer key length. HPH can be used to improve security guarantee for encryption, authentication, and AE modes. In this paper, we apply HPH to PMAC1 [43], present a new improved authentication mode HPMAC, and prove that HPMAC achieves PRF security, MK-PRF security, and RK-PRF security. Furthermore, we apply HPH to OPP [22], present a new authenticated encryption mode OPH, and prove that OPH enjoys AE security, MK-AE security, and RK-AE security.

References

1. 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. Lecture Notes in Computer Science, vol. 8269, pp. 424–443. Springer, Heidelberg (2013) 2, 23
2. Bellare, M., Kohno, T.: A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. In: Biham, E. (ed.) EUROCRYPT 2003. Lecture Notes in Computer Science, vol. 2656, pp. 491–506. Springer, Heidelberg (2003) 2
3. Bellare, M., Bernstein, D. J., Tessaro, S.: Hash-function based PRFs: AMAC and its multi-user security. In: Fischlin, M., Coron, JS. (eds.) EUROCRYPT 2016. Lecture Notes in Computer Science, vol. 9665, pp. 566–595. Springer, Heidelberg (2016) 2, 20
4. Bellare, M., Tackmann, B.: The Multi-user Security of Authenticated Encryption: AES-GCM in TLS 1.3. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. Lecture Notes in Computer Science, vol. 9814, pp. 247–276. Springer, Heidelberg (2016) 2

5. Bhattacharyya, R., Roy, A.: Secure message authentication against related-key attack. In: Moriai, S. (ed.) FSE 2013. Lecture Notes in Computer Science, vol. 8424, pp. 305–324. Springer, Heidelberg (2013) 2, 20
6. Biham, E.: New types of cryptoanalytic attacks using related keys (extended abstract). In: Helleseth, T. (ed.) EUROCRYPT 1993. Lecture Notes in Computer Science, vol. 765, pp. 398–409. Springer, Heidelberg (1993)
7. Biham, E.: New types of cryptanalytic attacks using related keys. J. Cryptology. 7(4), 229–246 (1994) 2
8. Biryukov, A., Khovratovich, D.: Related-key cryptanalysis of the full AES-192 and AES-256. In: Matsui, M. (ed.) ASIACRYPT 2009. Lecture Notes in Computer Science, vol. 5912, pp. 1–18. Springer, Heidelberg (2009) 2
9. Bossuet, L., Datta, N., Mancillas-López, C., Nandi, M.: ELmD: A Pipelineable Authenticated Encryption and Its Hardware Implementation. IEEE Transactions on Computers. 65(11), 3318–3331 (2016) 2, 6, 23
10. Chakraborty, D., Sarkar, P.: On modes of operations of a block cipher for authentication and authenticated encryption. Cryptogr. Commun. 8(4), 455–511 (2016) 2, 23
11. Chatterjee, S., Menezes, A., Sarkar, P.: Another Look at Tightness. In: Miri, A., Vaudenay, S. (eds.) SAC 2011. Lecture Notes in Computer Science, vol. 7118, pp. 293–319. Springer, Heidelberg (2011) 2, 20
12. 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, Heidelberg (2010) 2
13. Chen, S., Steinberger, J. P.: Tight Security Bounds for Key-Alternating Ciphers. In: Nguyen, P. Q., Oswald, E. (eds.) EUROCRYPT 2014. Lecture Notes in Computer Science, vol. 8441, pp. 327–350. Springer, Heidelberg (2014) 6
14. Cogliati, B., Lampe, R., Seurin, Y.: Tweaking Even-Mansour ciphers. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. Lecture Notes in Computer Science, vol. 9215, pp. 189–208. Springer, Heidelberg (2015) 2, 6, 9, 10
15. Cogliati, B., Seurin, Y.: EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. Lecture Notes in Computer Science, vol. 9814, pp. 121–149. Springer, Heidelberg (2016) 6, 20
16. 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. Lecture Notes in Computer Science, vol. 9056, pp. 584–613. Springer, Heidelberg (2015) 2
17. Cogliati, B., Seurin, Y.: Beyond-Birthday-Bound Security for Tweakable Even-Mansour Ciphers with Linear Tweak and Key Mixing. In: Iwata, T., Cheon, H. (eds.) ASIACRYPT 2015. Lecture Notes in Computer Science, vol. 9453, pp. 134–158. Springer, Heidelberg (2015) 2, 6
18. Datta, N., Nandi, M.: ELmE: A misuse resistant parallel authenticated encryption. In: Susilo, W., Mu, Y. (eds.) ACISP 2014. Lecture Notes in Computer Science, vol. 8544, pp. 306–321. Springer, Heidelberg (2014) 6, 23
19. Daemen, J., Lamberger, M., Pramstaller, N., Rijmen, V., Vercauteren, F.: Computational aspects of the expected differential probability of 4-round AES and AES-like ciphers. Computing. 85(1), 85–104 (2009) 9
20. Dobraunig, C., Eichlseder, M., Mendel, F.: Related-key forgeries for Prost-OTR. In: Leander, G. (ed.) FSE 2015. Lecture Notes in Computer Science, vol. 9054, pp. 282–296. Springer, Heidelberg (2015) 2

21. Fouque, P., Joux, A., Mavromati, C.: Multi-user Collisions: Applications to Discrete Logarithm, Even-Mansour and PRINCE. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. Lecture Notes in Computer Science, vol. 8873, pp. 420–438. Springer, Heidelberg (2014) 2
22. 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. Lecture Notes in Computer Science, vol. 9665, pp. 263–293. Springer, Heidelberg (2016) 2, 4, 9, 23, 24, 25, 26
23. Guo, Z., Wu, W., Liu, R., Zhang, L.: Multi-key Analysis of Tweakable Even-Mansour with Applications to Minalpher and OPP. IACR Transactions on Symmetric Cryptology. 2016(2), 288–306 (2016) 17
24. Halevi, S., Rogaway, P.: A tweakable enciphering mode. In: Boneh, D. (ed.) CRYPTO 2003. Lecture Notes in Computer Science, vol. 2729, pp. 482–499. Springer, Heidelberg (2003) 1
25. Halevi, S., Rogaway, P.: A parallelizable enciphering mode. In: Okamoto, T. (ed.) CT-RSA 2004. Lecture Notes in Computer Science, vol. 2964, pp. 292–304. Springer, Heidelberg (2004) 2
26. 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. Lecture Notes in Computer Science, vol. 9814, pp. 3–32. Springer, Heidelberg (2016) 2
27. Krovetz, T., Rogaway, P.: The software performance of authenticated-encryption modes. In: Joux, A. (ed.) FSE 2011. Lecture Notes in Computer Science, vol. 6733, pp. 306–327. Springer, Heidelberg (2011) 2, 23, 25, 26
28. Kurosawa, K.: Power of a public random permutation and its application to authenticated encryption. IEEE Trans. Inform. Theory. 5(10), 5366–5374 (2010) 5, 6
29. Landecker, W., Shrimpton, T., Terashima, R. S.: Tweakable Blockciphers with Beyond Birthday-Bound Security. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012, Lecture Notes in Computer Science, vol. 7417, pp. 14–30. Springer, Heidelberg (2012) 2
30. Liskov, M., Rivest, R.L., Wagner, D.: Tweakable block ciphers. In: Yung, M. (ed.) CRYPTO 2002. Lecture Notes in Computer Science, vol. 2442, pp. 31–46. Springer, Heidelberg (2002) 2, 23
31. Mantin, I., Shamir, A.: A Practical Attack on Broadcast RC4. In: Matsui, M. (ed.) FSE 2001. Lecture Notes in Computer Science, vol. 2355, pp. 152–164. Springer, Heidelberg (2001) 2
32. Mennink, B.: XPX: Generalized Tweakable Even-Mansour with Improved Security Guarantees. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. Lecture Notes in Computer Science, vol. 9814, pp. 64–94. Springer, Heidelberg (2016) 2, 6, 8, 9, 20, 23
33. Mennink, B., Reyhanitabar, R., Vizár, D.: Security of full-state keyed sponge and duplex: Applications to authenticated encryption. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. Lecture Notes in Computer Science, vol. 9453, pp. 465–489. Springer, Heidelberg (2015) 23
34. Mouha, N., Luykx, A.: Multi-key Security: The Even-Mansour Construction Revisited. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. Lecture Notes in Computer Science, vol. 9215, pp. 209–223. Springer, Heidelberg (2015) 2, 7, 12
35. Mouha, N., Mennink, B., Van Herrewege, A., Watanabe, D., Preneel, B., Verbauwhede, I.: Chaskey: An efficient MAC algorithm for 32-bit microcontrollers.

In: Joux, A., Youssef, A. (eds). SAC 2014. Lecture Notes in Computer Science, vol. 8781, pp. 306–323. Springer, Heidelberg (2014) 20
36. Patarin, J.: The "Coefficients H" Technique. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. Lecture Notes in Computer Science, vol. 5381, pp. 328–345. Springer, Heidelberg (2008) 3, 6
37. Peyrin, T., Seurin, Y.: Counter-in-Tweak: Authenticated Encryption Modes for Tweakable Block Ciphers. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. Lecture Notes in Computer Science, vol. 9814, pp. 33–63. Springer, Heidelberg (2016) 2, 6, 23
38. Peyrin, T., Sasaki, Y., Wang, L.: Generic related-key attacks for HMAC. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. Lecture Notes in Computer Science, vol. 7658, pp. 580–597. Springer, Heidelberg (2012) 2, 20
39. Reyhanitabar, R., Vaudenay, S., Vizár, D.: Misuse-Resistant Variants of the OMD Authenticated Encryption Mode. In: Chow, S.S.M., Liu, J.K., Hui, L.C.K., Yiu, S. (eds.) ProvSec 2014. Lecture Notes in Computer Science, vol. 8782, pp. 55–70. Springer, Heidelberg (2014) 2
40. Reyhanitabar, R., Vaudenay, S., Vizár, D.: Boosting OMD for Almost Free Authentication of Associated Data. In: Leander, G. (ed.) FSE 2015. Lecture Notes in Computer Science, vol. 9054, pp. 411–427. Springer, Heidelberg (2015) 2
41. Reyhanitabar, R., Vaudenay, S., Vizár, D.: Authenticated Encryption with Variable Stretch. In: Cheon, J., Takagi, T. (eds.) ASIACRYPT 2016. Lecture Notes in Computer Science, vol. 10031, pp. 396–425. Springer, Heidelberg (2016) 2, 23
42. Rogaway, P., Zhang, H.: Online ciphers from tweakable blockciphers. In: Kiayias, A. (ed.) CT-RSA 2011. Lecture Notes in Computer Science, vol. 6558, pp. 237–249. Springer, Heidelberg (2011) 2
43. Rogaway, P.: Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In: Lee, P.J. (ed.) ASIACRYPT 2004. Lecture Notes in Computer Science, vol. 3329, pp. 16–31. Springer, Heidelberg (2004) 2, 4, 9, 20, 21, 22, 23, 26
44. Rogaway, P., Bellare, M., Black, J.: OCB: a block-cipher mode of operation for efficient authenticated encryption. ACM Trans. Inf. Syst. Secur. 6(3), 365–403 (2003) 23
45. Sasaki, Y., Todo, Y., Aoki, K., Naito, Y., Sugawara, T., Murakami, Y., Matsui, M., Hirose, S.: Minalpher v1 (2014), submission to CAESAR competition (2014) 23
46. Sasaki, Y., Yasuda, K.: A New Mode of Operation for Incremental Authenticated Encryption with Associated Data. In: Dunkelman, O., Keliher, L. (eds.) SAC 2015. Lecture Notes in Computer Science, vol. 9566, pp. 397–416. Springer, Heidelberg (2016) 23
47. Sarkar, P.: Modes of operations for encryption and authentication using stream ciphers supporting an initialisation vector. Cryptogr. Commun. 6(3), 189–231 (2014) 23
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.) ASIACRYPT 2014. Lecture Notes in Computer Science, vol. 8873, pp. 158–178. Springer, Heidelberg (2014) 2
49. Wang, P., Li, Y., Zhang, L., Zheng, K.: Related-Key Almost Universal Hash Functions: Definitions, Constructions and Applications. In: Peyrin, T. (ed.) FSE

2016. Lecture Notes in Computer Science, vol. 9783, pp. 514–532. Springer, Heidelberg (2016) 2, 3, 5, 6

50. Wang, L., Guo, J., Zhang, G., Zhao, J., Gu, D.: How to Build Fully Secure Tweakable Blockciphers from Classical Blockciphers. In: Cheon, J., Takagi, T. (eds.) ASIACRYPT 2016. Lecture Notes in Computer Science, vol. 10031, pp. 455-483. Springer, Heidelberg (2016) 2