Generalized Tweakable Even-Mansour Cipher with Strong Security Guarantee and Its Application to Authenticated Encryption

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

[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. We present a generalized tweakable blockcipher HPH, which is constructed from a public random permutation P and an almost-XOR-universal (AXU) hash function H 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 the key K is chosen from a key space $\mathcal{K}$, the tweak (t_1, t_2) is chosen from a tweak space $\mathcal{T}$, x is a plaintext, and y is a ciphertext. We prove that HPH is a secure strong tweakable pseudorandom permutation. Then we focus on the security of HPH against multi-key and related-key attacks. We prove that HPH is multi-key-secure and HPH with related-key-AXU hash functions is related-key-secure, and derive a tight bound, respectively. HPH can be extended to wide applications. It is directly applied to authentication and authenticated encryption modes, and makes them provably security in the multi-key and related-key settings.

Keywords: Tweakable Even-Mansour, almost-XOR-universal hash functions, HPH, multi-key attacks, related-key attacks, H-coefficients technique, authenticated encryption.

1 Introduction

A tweakable blockcipher (TBC) is a generalization of a traditional block cipher, which adds a tweak as an extra public input on the basis of the usual inputs (a plaintext and a key). Tweakable blockciphers (TBCs) with distinct tweaks refer to distinct block ciphers, which makes that 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 [19] (Each disk consists of 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 and $\mathcal{E}_K$ is an encryption algorithm with a tweak space $\mathcal{T}$. Moreover, the encryption with distinct sectors is mutual independent). Now TBCs have been extended to all the modes of operation, such as encryption modes [20,1,32], message authentication codes (MACs) [23,22], and authenticated encryption (AE) modes [23,33,34,18].

There exists three approaches to realize a tweakable blockcipher. The first approach is based on a block cipher [23]. The second approach is based on a permutation [14]. The third approach is based on a keyed-function (hash function) [31].

Considering the security in the various applications, Mouha and Luykx [27] described three attack settings: single-key, multi-key, and related-key settings. In the single-key setting, an adversary has access to the encryption and decryption oracles under a fixed key K chosen uniformly and randomly from the key space. Most of previous papers considered the security in the single-key setting. In the multi-key setting, an adversary has access to the encryption and decryption oracles under many keys K_i ($i \geq 2$) chosen independently and randomly from the key space. Multi-key setting has many applications in the real-world implementations. The multi-key setting can be seen as a generalization of the multi-user [8] and broadcast [24] settings. There exists many related researches in the multi-key, multi-user, and broadcast settings, such as [24,8,17,27]. In the related-key attack setting, the key K_i satisfies the relationship $K_i = \phi_i(K)$, where K is a key, and the related-key deriving (RKD) functions ϕ_i are chosen by the adversary. Related-key attack (RKA) was firstly presented by Biham et al. [4,5] for block ciphers [2,6,36] and then extended to other cryptographic algorithms such as stream ciphers [9], permutation-based ciphers [13], hash functions [37], MACs [30,3], AE schemes [16], etc. The above three attack settings have become the important criterion in cipher designs.

The tweakable Even-Mansour cipher (TEM) [11] 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 set $\mathcal{T}$ to $\{0,1\}^n$, and defined as

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

where $K \in \mathcal{K}$ is a key, $t \in \mathcal{T}$ is a tweak, $x \in \{0,1\}^n$ is a plaintext, and $y \in \{0,1\}^n$ is a ciphertext. The security of TEM in the single-key setting was proved secure up to the birthday bound (this construction ensures security up to $2^{n/2}$ adversarial queries, in the random permutation model (RPM) for $P : \{0,1\}^n \rightarrow \{0,1\}^n$).

Follow on, Mennink [25] provided a pure-permutation-based tweakable blockcipher XPX, which is a generalization of tweakable Even-Mansour cipher. 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 $\Delta_1 = t_{11}K \oplus t_{12}P(K)$ and $\Delta_2 = t_{21}K \oplus t_{22}P(K)$, $x \in \{0,1\}^n$ is a plaintext, and $y \in \{0,1\}^n$ is a ciphertext. XPX with a valid tweak space $\mathcal{T}$ was proved secure up to the birthday bound 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 Contribution

In this paper, we are interest in generalizing XPX to the case where the maskings are implemented using universal hash functions. Here we use a common universal hash function H instead of two universal hash functions f and g. As XPX makes two invocations to the underlying permutation 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 random permutation P and an almost-XOR-universal (AXU) family of hash functions $\mathcal{H} = \{H_K\}$ 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 the key K is chosen from a key space $\mathcal{K}$, the tweak (t_1, t_2) is chosen from a tweak space $\mathcal{T}$, x is a plaintext, and y is a ciphertext.

This paper focuses on the security of HPH in the single-key, multi-key, and related-key settings. Due to the weakness of almost-XOR-universal (AXU) hash functions in the related-key setting, we use a family of related-key-almost-XOR-universal (RKA-AXU) hash functions presented by Wang et al. [37]. We prove that HPH is secure up to the birthday bound in the above three attack settings and derive a tight bound, respectively. Our proofs use Patarin's H-coefficients technique [29].

In the single-key setting, we prove that HPH with (ϵ, δ)-AXU-hash functions achieves strong tweakable pseudorandom permutation (STPRP) security up to about $2DT\delta + D(D-1)\epsilon$ queries in the random permutation model, where D is the complexity of construction queries (data complexity) and T is the complexity of internal permutation queries (time complexity).

In the multi-key setting, a small number of plaintexts are encrypted under multiple independent keys. HPH with (ϵ, δ)-AXU-hash functions is secure up to $2DT\delta + (D-l+1)(D-l)\epsilon + D^2(1-1/l)\delta$ queries against multi-key attack, where D is the complexity of construction queries (data complexity), T is the complexity of internal permutation queries (time complexity), and l is the number of keys.

In the related-key setting, a small number of plaintexts are encrypted under multiple related keys. HPH with (ϵ, δ)-RKA-AXU-hash functions is secure up to $2DT\delta + D(D-1)\epsilon$ queries against related-key attack, where D is the complexity of construction queries (data complexity) and T is the complexity of internal permutation queries (time complexity).

HPH is a strongly secure cryptosystem with a lighter key schedule and higher key agility in the single-key, multi-key, and related-key attack settings. Our work is of high practical relevance because of rekey requirements and the inevitability of related keys in real-world implementations. HPH is very useful, not only because of the simplicity of its design and proof, but also because of fast and secure implementations. If the underlying (tweakable) block cipher is replaced with HPH, then encryption, authentication, and authenticated encryption modes may be designed more efficiently and more securely.

1.2 Applications

HPH can be used to improve security guarantee for encryption, authentication, and authenticated encryption modes. Mennink applied XPX to authenticated encryption modes and message authentication code (MAC) in [25]. HPH is a generalization of XPX, therefore HPH can be applied to these modes. In this paper, we cite OPP [18] as an example to illustrate the applications of HPH. On this basis, we improve OPP [18], present a new authenticated encryption mode OPH, and prove that OPH is single-key-AE secure, multi-key-AE secure, and related-key-AE secure.

HPH is directly applied to authenticated encryption mode OPP [18]. We retain the tweak-dependent masking function unchange. It is very easy to prove that OPP [18] is both multi-key secure and related-key secure. As the tweak-based masking function of OPP [18] is based on the underlying primitive, OPP [18] makes extra invocation to the underlying permutation for per-message encryption. Here we utilize a family of universal hash functions, present a new nonce-respecting authenticated encryption mode OPH, and derive provably security bounds in the single-key, multi-key, and related-key settings.

If the underlying permutation is replaced with AES-128, this is similar to OCB [34]. The family of AXU-hash functions can be implemented by four-round AES (AES4 is an excellent choice in certain settings, such as restricted environments or devices with AES-NI).

Organizations of This Paper. Some preliminaries are presented in Section 2. Three security models are presented in Section 3. Three security results of HPH are derived in Section 5. Section 6 present some applications of HPH. Finally, this paper ends up with a conclusion in Section 7.

2 Preliminaries

2.1 Notations

Let n be an integrity and $\{0,1\}^n$ denote the set of all strings whose lengths are n-bit. If X is a finite set, then $x \overset{\$}{\leftarrow} X$ is a value randomly chosen from X, and $|X|$ stands for the number of elements in X.

A tweakable blockcipher with key space $\mathcal{K}$, tweak space $\mathcal{T}$, and plaintext space $\{0,1\}^n$ is a function $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ such that for any key $K \in \mathcal{K}$ and a tweak $t \in \mathcal{T}$, $\widetilde{E}_K(t,\cdot) = \widetilde{E}(K,t,\cdot)$ is a permutation of $\{0,1\}^n$. Similarity, its inverse is denoted by $\widetilde{D}_K = \widetilde{E}_K^{-1}$. Let $Perm(n)$ be the set of all permutations on $\{0,1\}^n$. Let $\widetilde{Perm}(\mathcal{T},n)$ be the set of tweakable permutations, i.e., the set of $Perm(n)$ indexed with $t \in \mathcal{T}$.

An adversary is a probabilistic algorithm with access to certain oracles. Let $\mathcal{A}^O = 1$ be the event that an adversary $\mathcal{A}$ outputs 1 after interacting with the oracle O. Without loss of generality, we assume that the adversary doesn't make redundant queries, that is, i) it doesn't repeat prior queries for each oracle, ii) the adversary does not ask the decryption oracle $\widetilde{D}_K$ after receiving a value in response to an encryption query $\widetilde{E}_K$, and iii) the adversary does not ask the encryption oracle $\widetilde{E}_K$ after receiving a value in response to a decryption query $\widetilde{D}_K$.

A related-key deriving (RKD) function is a map that takes a key $K \in \mathcal{K}$ as an input and returns a related key $\phi(K) \in \mathcal{K}$. A RKD set Φ is a set of RKD functions, which is formalized as $\Phi = \{\phi : \mathcal{K} \to \mathcal{K}\}$. Two typical RKD sets are enumerated as follows:

$$\Phi_{id} = \{\phi : K \to K\};$$
$$\Phi_{\oplus} = \{\phi : K \to K \oplus \triangle \mid \triangle \in \mathcal{K}\},$$

where $K \in \mathcal{K}$. Throughout the paper we assume that membership in RKD sets can be efficiently decided.

2.2 Universal Hash Functions

Definition 1 **((ϵ,δ)-AXU Hash Function Family [21]).** *Let $\mathcal{H} = \{H : \mathcal{K} \times \mathcal{D} \to \mathcal{R}\}$ be a family of hash functions. H is called an (ϵ,δ)-almost XOR universal ((ϵ,δ)-AXU) hash function, if the following two conditions hold:*

1) For any element $X \in \mathcal{D}$ and any element $Y \in \mathcal{R}$,

$$Pr[K \overset{\$}{\leftarrow} \mathcal{K} : H_K(X) = Y] \le \delta;$$

2) For any two distinct elements $X, X' \in \mathcal{D}$ and any element $Y \in \mathcal{R}$,

$$Pr[K \overset{\$}{\leftarrow} \mathcal{K} : H_K(X) \oplus H_K(X') = Y] \le \epsilon.$$

Examples of AXU hash function families are presented as follows.

1) Let $\mathcal{H}_1 = \{H_K(x) = K \cdot x \mid K, x \in GF(2^n)^*\}$. Then $\mathcal{H}_1$ is a $(2^{-n}, 2^{-n})$-AXU hash function family from $\{0,1\}^n \setminus \{0^n\}$ to $\{0,1\}^n$.

2) Let $\mathcal{H}_2 = \{H_K(x_1, x_2, \cdots, x_t) = K \cdot x_1 + K^2 \cdot x_2 + \cdots + K^t \cdot x_t \mid K \in GF(2^n)^*, x_i \in GF(2^n), 1 \le i \le t, (x_1, x_2, \cdots, x_t) \ne (0, 0, \cdots, 0)\}$. Then $\mathcal{H}_2$ is a $(t/2^n, t/2^n)$-AXU hash function family from $\{0,1\}^{tn} \setminus \{0^{tn}\}$ to $\{0,1\}^n$.

3) Let $\mathcal{H}_3 = \{H_{k_1,k_2,\cdots,k_t}(x_1, x_2, \cdots, x_t) = k_1 \cdot x_1 + k_2 \cdot x_2 + \cdots + k_t \cdot x_t \mid k_i \in GF(2^n), x_i \in GF(2^n), 1 \le i \le t, (k_1, k_2, \cdots, k_t) \ne (0, 0, \cdots, 0), (x_1, x_2, \cdots, x_t) \ne (0, 0, \cdots, 0)\}$. Then $\mathcal{H}_3$ is a $(1/2^n, 1/2^n)$-AXU hash function family from $\{0,1\}^{tn} \setminus \{0^{tn}\}$ to $\{0,1\}^n$.

Definition 2 **((ϵ,δ)-RKA-AXU Hash Function Family [37]).** *Let $\mathcal{H} = \{H : \mathcal{K} \times \mathcal{D} \to \mathcal{R}\}$ be a family of hash functions. H is an (ϵ,δ)-related-key-almost-XOR-universal ((ϵ,δ)-RKA-AXU) hash function for the RKD set Φ, if the following two conditions hold:*

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

$$Pr[K \overset{\$}{\leftarrow} \mathcal{K} : H_{\phi(K)}(X) = Y] \le \delta;$$

2) For any $\phi, \phi' \in \Phi, X, X' \in \mathcal{D}, (\phi, X) \ne (\phi', X')$, and $Y \in \mathcal{R}$,

$$Pr[K \overset{\$}{\leftarrow} \mathcal{K} : H_{\phi(K)}(X) \oplus H_{\phi'(K)}(X') = Y] \le \epsilon.$$

For any $\phi, \phi' \in \Phi, \phi \neq \phi'$ means there exists a key $K \in \mathcal{K}$ such that $\phi(K) \neq \phi'(K)$. If the RKD set $\Phi_{id} = \{\phi : K \rightarrow K\}$ is an identity transform, an (ϵ, δ)-RKA-AXU hash function family is an (ϵ, δ)-AXU hash function family.

Restricting RKD Sets [37]. The RKA-AXU-hash function family depends on the choice of RKD sets. For some RKD sets, the RKA-AXU-hash function family may not exist. It is necessary that a RKD set is restricted to both output unpredictable and collision resistant. The restrictions on the RKD set are specifically presented as follows.

1) 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. Let $OU(\Phi) = max_{\phi \in \Phi, S} Pr[K \leftarrow \mathcal{K} : \phi(K) = S]$ be the probability of output predictability. If $OU(\Phi)$ is negligible, we say that Φ is output unpredictable.

2) Collision resistance. Two distinct $\phi, \phi' \in \Phi$ have high collision probability if the probability of $\phi(K) = \phi'(K)$ is hight. Let $CR(\Phi) = max_{\phi \neq \phi' \in \Phi} Pr[K \leftarrow \mathcal{K} : \phi(K) = \phi'(K)]$ be the probability of collision. If $CR(\phi)$ is negligible, we say that ϕ is collision resistant. More strictly, if for any two distinct $\phi, \phi' \in \Phi$ and any key K, we have $\phi(K) \neq \phi'(K)$ or $CR(\Phi) = 0$, we say that Φ is claw-free.

Instances. Wang et al. [37] constructed related-key almost universal hash functions: one fixed-input-length (FIL) UHF named RH1 and two variable-input-length (VIL) UHFs named RH2 and RH3. It is easy to obtain that RH1 and RH2 are both (ϵ, δ)-RKA-AXU hash functions for the RKD set $\Phi^{\oplus}$.

1) RH1: $\{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$, $RH1_K(M) = MK \oplus K^3$ is $(2/2^n, 2/2^n)$-RKA-AXU for the RKD set $\Phi^{\oplus}$.

2) RH2: $\{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$, $pad(M) = M \parallel 0^i \parallel |M|$

$$RH2_K(M) = \begin{cases} K^{l+2} \oplus Poly_K(pad(M)) & l \text{ is odd} \\ K^{l+3} \oplus Poly_K(pad(M))K & l \text{ is even} \end{cases}$$

is $((l_{max} + 3)/2^n, (l_{max} + 3)/2^n)$-RKA-AXU for the RKD set $\Phi^{\oplus}$, where $l = \lceil |M|/n \rceil + 1$ is the number of blocks in $pad(M)$, l_{max} is the maximum block number of messages after padding, and $Poly : \{0,1\}^n \times \{0,1\}^{nm} \rightarrow \{0,1\}^n$ is defined as follows:

$$Poly_K(X) = X_1 K^m \oplus \cdots \oplus X_m K.$$

2.3 The H-Coefficients Technique

Patarin's H-coefficients technique [29] is a vital tool widely used in the encryption modes [14,10,11], authentication modes [12], and authenticated encryption modes [7,15]. We briefly summarize this technique as follows.

Given a real world X and a ideal world Y, considering an information-theoretic adversary $\mathcal{A}$ whose goal is to distinguish X from Y, then the advantage of $\mathcal{A}$ is denoted as

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

Without loss of generality, we can assume $\mathcal{A}$ is a deterministic adversary. The interaction with X or Y is summarized in a transcript τ, which is a list of queries and answers. Denote by D_X the probability distribution of transcripts when interacting with X, and by D_Y the probability distribution of transcripts when interacting with Y.

A transcript τ is attainable if $Pr[D_Y = \tau] > 0$, meaning that it can occur during interaction with Y. Let $\varGamma$ be the set of attainable transcripts. The H-coefficients lemma is presented as follows.

Lemma 1 (H-Coefficients Lemma). *Fix a deterministic adversary $\mathcal{A}$. Let $\varGamma = \varGamma_{good} \bigcup \varGamma_{bad}$ be a partition of the set of attainable transcripts. Assume that there exists ε such that for any $\tau \in \varGamma_{good}$, one has*

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

Then

$$Adv(\mathcal{A}) \leq \varepsilon + Pr[D_Y \in \varGamma_{bad}].$$

3 Three Security Models

3.1 Single-Key Security Model

Let $\widetilde{E}_K : \mathcal{T} \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a tweakable blockcipher based on a random permutation $P \xleftarrow{\$} Perm(n)$, where $K \in \mathcal{K}$. Let $\widetilde{\pi} \xleftarrow{\$} \widetilde{Perm}(\mathcal{T}, n)$ be a random tweakable permutation. The single-key security of $\widetilde{E}$ is formalized with a distinguisher that has adaptive oracle access to 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). In this paper, we consider the adversary that has access to the encryption and decryption queries for X or Y. The definition of single-key security is presented as follows.

Definition 3 (Single-Key Security). *Let $K \xleftarrow{\$} \mathcal{K}$ and $\widetilde{E}_K$ be the tweakable block cipher based on a random permutation $P \xleftarrow{\$} Perm(n)$. Given an adversary $\mathcal{A}$, the single-key strong tweakable pseudorandom permutation (STPRP) advantage of $\mathcal{A}$ is*

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

where $\widetilde{\pi}$ is uniformly drawn from $\widetilde{Perm}(\mathcal{T}, n)$. The adversary $\mathcal{A}$ has access to the encryption and decryption oracles.

3.2 Multi-Key Security Model

Let $\widetilde{E}_K : \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ be a tweakable blockcipher based on a random permutation $P \xleftarrow{\$} Perm(n)$, where $K \in \mathcal{K}$. Let $\widetilde{\pi} \xleftarrow{\$} \widetilde{Perm}(\mathcal{T}, n)$ be a random tweakable permutation. Let l denote the number of keys K_i under which the adversary performs queries, that is, there is at least one query for every key K_i for $1 \leq i \leq l$. The multi-key-security of $\widetilde{E}$ is formalized with a distinguisher that has adaptive oracle access to either $(\widetilde{E}_{K_1}, \widetilde{E}_{K_2}, \cdots, \widetilde{E}_{K_l}; P)$ with $K_i \xleftarrow{\$} \mathcal{K}$ for $i = 1, \cdots, l$, (Real World X), or $(\widetilde{\pi}_1, \widetilde{\pi}_2, \cdots, \widetilde{\pi}_l; P)$ with $\widetilde{\pi}_i \xleftarrow{\$} \widetilde{Perm}(\mathcal{T}, n), i = 1, \cdots, l$ (Ideal World Y). In this paper, we consider the adversary that has access to the encryption and decryption queries for X or Y. The definition of multi-key security is presented as follows.

Definition 4 (Multi-Key Security). *Let $K \xleftarrow{\$} \mathcal{K}$ and $\widetilde{E}_K$ be the tweakable block cipher based on a random permutation $P \xleftarrow{\$} Perm(n)$. Given an adversary $\mathcal{A}$, the multi-key STPRP (MK-STPRP) advantage of $\mathcal{A}$ with respect to l keys is*

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

where the keys $K_1, \cdots, K_l$ are independently and uniformly drawn from $\mathcal{K}$, and $\widetilde{\pi}_1, \widetilde{\pi}_2, \cdots, \widetilde{\pi}_l$ are independently and uniformly drawn from $\widetilde{Perm}(\mathcal{T}, n)$. The adversary $\mathcal{A}$ has access to the encryption and decryption oracles.

3.3 Related-Key Security Model

Let Φ be a set of RKD functions. For a tweakable block cipher $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$, we define a related-key oracle $RK[\widetilde{E}] : \mathcal{K} \times \Phi \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ as

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

where $K \in \mathcal{K}$ is the key, $\phi \in \Phi$ is a RKD function, $t \in \mathcal{T}$ is the tweak, and $x \in \{0,1\}^n$ is the plaintext.

Let $\widetilde{RKPerm}(\Phi, \mathcal{T}, n)$ be the set of tweakable related-key permutations, i.e., the set of all families of permutations on $\{0,1\}^n$ indexed with $(\phi, t) \in \Phi \times \mathcal{T}$.

The security of the tweakable blockcipher in the related-key setting is formalized with a distinguisher which has access to $(RK[\widetilde{E}]_K; P)$ with $K \in \mathcal{K}, \phi \in \Phi$, and $P \xleftarrow{\$} Perm(n)$ (Real World X), or $(RK[\widetilde{\pi}]; P)$ with $RK[\widetilde{\pi}] \xleftarrow{\$} \widetilde{RKPerm}(\Phi, \mathcal{T}, n)$ and $P \xleftarrow{\$} Perm(n)$ (Ideal World Y). In this paper, we consider that an adversary is adaptive and can make encryption and decryption queries to each oracle. We present a definition of related-key security as follows.

Definition 5 (Related-Key Security). *Let Φ be a RKD set, $K \xleftarrow{\$} \mathcal{K}$ be a key, and $\widetilde{E}_K$ be a tweakable blockcipher based on a public random permutation*

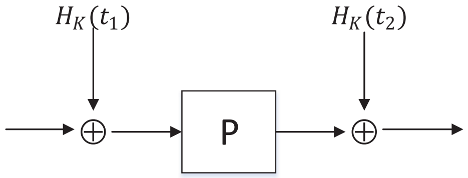

Fig. 1. HPH: Generalized Tweakable Even-Mansour Cipher

$P \xleftarrow{\$} Perm(n)$. Given an adversary $\mathcal{A}$, the related-key STPRP (RK-STPRP) advantage of $\mathcal{A}$ with respect to Φ is

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

where $RK[\widetilde{\pi}] \xleftarrow{\$} \widetilde{RKPerm}(\Phi, \mathcal{T}, n), \phi \xleftarrow{\$} \Phi$, and $P \xleftarrow{\$} Perm(n)$. The adversary $\mathcal{A}$ has access to the encryption and decryption oracles.

4 HPH

Let $\mathcal{K}$ be a key space, $\mathcal{T} = \mathcal{D}^2$ be a 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 almost-XOR-universal (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 universal hash function, $K \in \mathcal{K}$ is a key, $(t_1, t_2) \in \mathcal{T}$ is a tweak, $x \in \{0,1\}^n$ is a plaintext, and $y \in \{0,1\}^n$ is a ciphertext. As H is an universal hash function, therefore $0 \notin \mathcal{T}$. The overview of HPH is depicted in Fig. 1.

HPH is a generalized tweakable Even-Mansour cipher. If $H_K(t_1) = t_{11}K \oplus t_{12}P(K)$ and $H_K(t_2) = t_{21}K \oplus t_{22}P(K)$, where $t_1 = (t_{11}, t_{12})$ and $t_2 = (t_{21}, t_{22})$, HPH meets the construction of XPX and inherits the security of XPX [25]. 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 [11]. We use a non-linear universal hash function family $\mathcal{H}$ in this paper.

If the underlying permutation is replaced with AES-128, HPH is a generalization of the XEX construction [33]. The universal hash function H can be implemented by four-round AES (AES4). AES4 is an excellent choice in certain settings, such as restricted environments or devices with AES-NI.

5 Strong Security of HPH

In this section, we analyze the security of HPH in various security models and prove that HPH achieves STPRP security, MK-STPRP security, and RK-STPRP security.

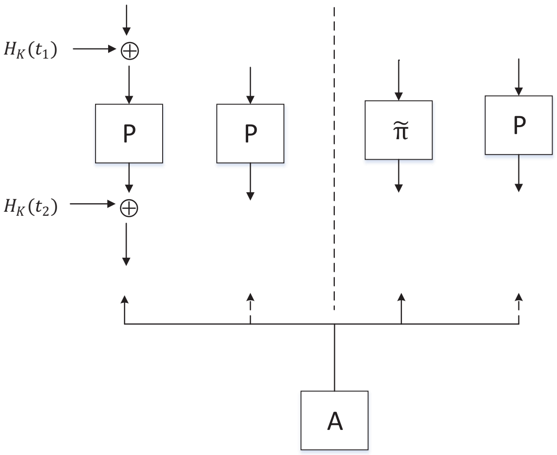

Fig. 2. Single-Key Security of HPH. **Left of dashed line**: Real world $X = (HPH_K^{\pm}; P^{\pm})$ with $K \xleftarrow{\$} \mathcal{K}$ and $P \xleftarrow{\$} Perm(n)$. **Right of dashed line**: Ideal world $Y = (\widetilde{\pi}^{\pm}; P^{\pm})$ with $\widetilde{\pi} \xleftarrow{\$} \widetilde{Perm}(\mathcal{T}, n)$ and $P \xleftarrow{\$} Perm(n)$. The goal of $\mathcal{A}$ is to distinguish the real world X from the ideal world Y. If the distinguishable advantage of $\mathcal{A}$ is negligible, the scheme is STPRP-secure. The number of queries by the adversary $\mathcal{A}$ to any of the first oracle is denoted by D, the number of queries to the last oracle by T.

5.1 Single-Key Security of HPH

Theorem 1 (Single-Key Security of HPH). *Let HPH_K be the tweakable blockcipher with (ϵ, δ)-AXU hash function family, then for all adversaries $\mathcal{A}$ making at most D queries to $HPH_K^{\pm}$ (resp. $\widetilde{\pi}^{\pm}$) and at most T queries to $P^{\pm}$, we have*

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

Our proof is similar to that of the tweakable Even-Mansour cipher in the single-key setting [11]. The result of Theorem 1 is in fact a generalization of [11]. The proof uses Patarin's H-coefficients technique [29].

As shown in Fig. 2, we consider an adversary $\mathcal{A}$ that has access to two oracles (O_1, O_2). In the real world X, these are $(HPH_K^{\pm}; P^{\pm})$ with $K \xleftarrow{\$} \mathcal{K}$ and $P \xleftarrow{\$} Perm(n)$, and in the ideal world Y, these are $(\widetilde{\pi}^{\pm}; P^{\pm})$ with $\widetilde{\pi} \xleftarrow{\$} \widetilde{Perm}(\mathcal{T}, n)$ and $P \xleftarrow{\$} Perm(n)$. Without loss of generality, we assume that $\mathcal{A}$ is a deterministic adversary. It makes D queries to oracle O_1, and T queries to O_2. Let m be the number of distinct tweaks, D_t be the number of queries for the t-th tweak, $1 \leq t \leq m$, using an arbitrary ordering of the tweaks. Then $D = \sum_{t=1}^{m} D_t$.

The interaction of $\mathcal{A}$ with the oracles can be described by a transcript $\tau = (K, \tau_1, \tau_2)$. We assume that the list of queries to O_1 is defined by $\tau_1 = \{(t_1^1, t_2^1, x^1, y^1), \cdots, (t_1^D, t_2^D, x^D, y^D)\}$, where $(t_1^1, t_2^1), \cdots, (t_1^D, t_2^D) \in \mathcal{T}$, and to

O_2 by $\tau_2 = \{(u^1, v^1), \cdots, (u^T, v^T)\}$. We assume that $\mathcal{A}$ never makes duplicate queries, so that $(t_1^i, t_2^i, x^i) \neq (t_1^j, t_2^j, x^j), (t_1^i, t_2^i, y^i) \neq (t_1^j, t_2^j, y^j), u^i \neq u^j$, and $v^i \neq v^j$ for all i and j, where $i \neq j$.

Let D_X denote the probability distribution of transcripts in the real world X, and D_Y denote the probability distribution of transcripts in the ideal world Y. We say that a transcript τ is attainable if it can be obtained from interacting with $(\widetilde{\pi}^{\pm}; P^{\pm})$, that is to say $Pr(D_Y = \tau) > 0$.

Definition 6. *We say that a transcript $\tau = (K, \tau_1, \tau_2)$ is bad if two different queries would result in the same input or output to P, when $\mathcal{A}$ interacting with the real world. Put formally, τ 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 $(t_1^i, t_2^i), (t_1^j, t_2^j) \in \mathcal{T}$ 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 $(t_1^i, t_2^i), (t_1^j, t_2^j) \in \mathcal{T}$ and $1 \leq i \neq j \leq D$.

Otherwise we say that τ is good. We denote Γ_{good} (resp. Γ_{bad}) the set of good (resp. bad) transcripts. Let $\Gamma = \Gamma_{good} \cup \Gamma_{bad}$ be the set of attainable transcripts.

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

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 $\mathcal{K}$. We assume that an adversary $\mathcal{A}$ makes at most D construction queries and at most T primitive queries. Given any $(t_1, t_2, x, y) \in \tau_1$ and $(u, v) \in \tau_2$, where $(t_1, t_2) \in \mathcal{T}$, by the properties of the (ϵ, δ)-AXU hash function H, 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 $(t_1^i, t_2^i), (t_1^j, t_2^j) \in \mathcal{T}$ and $1 \leq i \neq j \leq D$. By the properties of the (ϵ, δ)-AXU hash function H, 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,

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

Therefore,

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

This completes the proof.

We then analyze good transcripts. For a good transcript, in the real world X, all tuples in $\tau = (K, \tau_1, \tau_2)$ uniquely define an input-output pair of P, while in the ideal world it is not.

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

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

Proof. Consider a good transcript $\tau \in \Gamma_{good}$. Denote by Ω_X the set of all possible oracles in the real world X and by Ω_Y the set of all possible oracles in the ideal world Y. Let $comp_X(\tau) \subseteq \Omega_X$ and $comp_Y(\tau) \subseteq \Omega_Y$ be the set of oracles compatible with transcript τ. According to the H-coefficients technique, we have

$Pr(D_X = \tau) = \frac{|comp_X(\tau)|}{|\Omega_X|}$, where $|\Omega_X| = 2^n!|\mathcal{K}|$.

$Pr(D_Y = \tau) = \frac{|comp_Y(\tau)|}{|\Omega_Y|}$, where $|\Omega_Y| = (\prod_t 2^n!) \cdot 2^n!|\mathcal{K}|$ and $t \in \mathcal{T}$.

Firstly, we calculate $|comp_X(\tau)|$. As $\tau \in \Gamma_{good}$, there are no two queries in τ with the same input or output of the underlying permutation. Any query tuple in τ therefore fixes exactly one input-output pair of the underlying oracle. Because τ consists of $D+T$ query tuples, the number of possible oracles in the real world X equals $(2^n - D - T)!$.

By a similar reason, the number of possible oracles in the ideal world Y equals $\prod_{t=1}^{m}(2^n - D_t)!(2^n - T)!$, where $D = \sum_{t=1}^{m} D_t$. It follows that,

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

Therefore, we have $\frac{Pr[D_X = \tau]}{Pr[D_Y = \tau]} \geq 1$.

By Lemmas 1, 2, and 3, we have

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

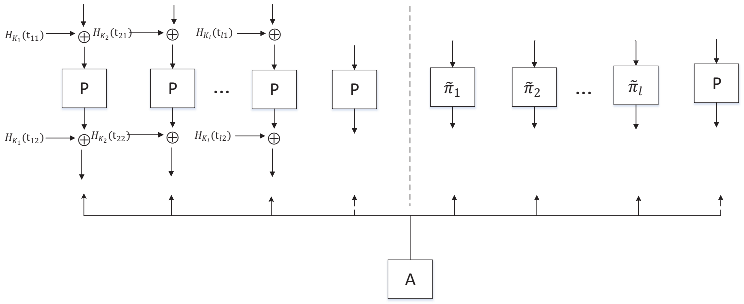

Fig. 3. Multi-Key Security of HPH. **Left of dashed line**: Real world $X = (HPH^{\pm}_{K_1}, HPH^{\pm}_{K_2}, \cdots, HPH^{\pm}_{K_l}; P^{\pm})$ with $K_i \xleftarrow{\$} \mathcal{K}$ for $i = 1, \cdots, l, P \xleftarrow{\$} Perm(n)$. **Right of dashed line**: Ideal world $Y = (\widetilde{\pi}^{\pm}_1, \widetilde{\pi}^{\pm}_2, \cdots, \widetilde{\pi}^{\pm}_l; P^{\pm})$ with $\widetilde{\pi}_i \xleftarrow{\$} \widetilde{Perm}(\mathcal{T}, n), i = 1, \cdots, l$ and $P \xleftarrow{\$} Perm(n)$. The goal of $\mathcal{A}$ is to distinguish the real world X from the ideal world Y. If the distinguishable advantage of $\mathcal{A}$ is negligible, the scheme is multi-key-secure. Although only one direction is shown, inverse oracles can be accessed as well. The number of queries by the adversary $\mathcal{A}$ to any of the first l oracles is denoted by D, the number of queries to the last oracle by T.

5.2 Multi-Key Security of HPH

Theorem 2 (Multi-Key Security of HPH). *Let HPH_K be the tweakable blockcipher with (ϵ, δ)-AXU hash function family, then for all adversaries $\mathcal{A}$ making at most D queries to $HPH^{\pm}_{K_1}, HPH^{\pm}_{K_2}, \cdots, HPH^{\pm}_{K_l}$ (resp. $\widetilde{\pi}^{\pm}_1, \widetilde{\pi}^{\pm}_2, \cdots, \widetilde{\pi}^{\pm}_l$) and at most T queries to $P^{\pm}$, we have*

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

Our proof is similar to that of the Even-Mansour cipher in the multi-key setting [27], except that we need to consider the tweak and the properties of hash functions in the multi-key setting. The result of Theorem 2 is in fact a generalization of [27]. The proof uses Patarin's H-coefficients technique [29]. For a detailed explanation of this technique, you can refer to [10].

As shown in Fig. 3, we consider an adversary $\mathcal{A}$ that has access to $l+1$ oracles $(O_1, \cdots, O_{l+1})$. In the real world, these are $(HPH^{\pm}_{K_1}, HPH^{\pm}_{K_2}, \cdots, HPH^{\pm}_{K_l}; P^{\pm})$ with $K_i \xleftarrow{\$} \mathcal{K}$ for $i = 1, \cdots, l, P \xleftarrow{\$} Perm(n)$, and in the ideal world, these are $(\widetilde{\pi}^{\pm}_1, \widetilde{\pi}^{\pm}_2, \cdots, \widetilde{\pi}^{\pm}_l; P^{\pm})$ with $\widetilde{\pi}_i \xleftarrow{\$} \widetilde{Perm}(\mathcal{T}, n), i = 1, \cdots, l$ and $P \xleftarrow{\$} Perm(n)$. Without loss of generality, we assume that $\mathcal{A}$ is a deterministic adversary. It makes D_i queries to oracle 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, D_t be the number of queries for the t-th tweak, $1 \leq t \leq m$, using an arbitrary ordering of the tweaks. Note that m may depend on the answers received from the oracles, yet one always has $D = \sum_{t=1}^{m} D_t$.)

The interaction of $\mathcal{A}$ with the oracles can be described by a transcript $\tau = (K_1, \cdots, K_l, \tau_1, \cdots, \tau_{l+1})$. We assume that the list of queries to O_i for

$i = 1, \cdots, l$ is defined by $\tau_i = \{(t_{i1}^1, t_{i2}^1, x_i^1, y_i^1), \cdots, (t_{i1}^{D_i}, t_{i2}^{D_i}, x_i^{D_i}, y_i^{D_i})\}$, where $(t_{i1}^1, t_{i2}^1), \cdots, (t_{i1}^{D_i}, t_{i2}^{D_i}) \in \mathcal{T}$, and to O_{l+1} by $\tau_{l+1} = \{(u^1, v^1), \cdots, (u^T, v^T)\}$. We assume that $\mathcal{A}$ never makes redundant queries, so that $(t_{i1}^j, t_{i2}^j, x_i^j) \neq (t_{i1}^{j'}, t_{i2}^{j'}, x_i^{j'}), (t_{i1}^j, t_{i2}^j, y_i^j) \neq (t_{i1}^{j'}, t_{i2}^{j'}, y_i^{j'}), u^j \neq u^{j'}$, and $v^j \neq v^{j'}$ for all i, j, j' where $j \neq j'$.

Let D_X denote the probability distribution of transcripts in the real world X, and D_Y denote the probability distribution of transcripts in the ideal world Y. We say that a transcript τ is attainable if it can be obtained from interacting with $(\widetilde{\pi}_1^{\pm}, \widetilde{\pi}_2^{\pm}, \cdots, \widetilde{\pi}_l^{\pm}; P^{\pm})$, that is to say $Pr(D_Y = \tau) > 0$.

Definition 7. *We say that a transcript τ is bad if two different queries would result in the same input or output to P, when $\mathcal{A}$ interacting with the real world. Put formally, τ is bad if one of the following conditions is satisfied:*

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

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

Bad3: $\exists (t_{i1}^j, t_{i2}^j, x_i^j, y_i^j) \neq (t_{i1}^{j'}, t_{i2}^{j'}, x_i^{j'}, y_i^{j'}) \in \tau_i$ such that $x_i^j \oplus x_i^{j'} = H_{K_i}(t_{i1}^j) \oplus H_{K_i}(t_{i1}^{j'})$, where $(t_{i1}^j, t_{i2}^j), (t_{i1}^{j'}, t_{i2}^{j'}) \in \mathcal{T}$, $1 \leq i \leq l$, and $1 \leq j \neq j' \leq D_i$;

Bad4: $\exists (t_{i1}^j, t_{i2}^j, x_i^j, y_i^j) \neq (t_{i1}^{j'}, t_{i2}^{j'}, x_i^{j'}, y_i^{j'}) \in \tau_i$ such that $y_i^j \oplus y_i^{j'} = H_{K_i}(t_{i2}^j) \oplus H_{K_i}(t_{i2}^{j'})$, where $(t_{i1}^j, t_{i2}^j), (t_{i1}^{j'}, t_{i2}^{j'}) \in \mathcal{T}$, $1 \leq i \leq l$, and $1 \leq j \neq j' \leq D_i$;

Bad5: $\exists (t_{i1}^j, t_{i2}^j, x_i^j, y_i^j) \in \tau_i, (t_{i'1}^{j'}, t_{i'2}^{j'}, x_{i'}^{j'}, y_{i'}^{j'}) \in \tau_{i'}$, and $(t_{i1}^j, t_{i2}^j, x_i^j, y_i^j) \neq (t_{i'1}^{j'}, t_{i'2}^{j'}, x_{i'}^{j'}, y_{i'}^{j'})$ such that $x_i^j \oplus x_{i'}^{j'} = H_{K_i}(t_{i1}^j) \oplus H_{K_{i'}}(t_{i'1}^{j'})$, where $(t_{i1}^j, t_{i2}^j), (t_{i'1}^{j'}, t_{i'2}^{j'}) \in \mathcal{T}$, $1 \leq i \neq i' \leq l, 1 \leq j \leq D_i$, and $1 \leq j' \leq D_{i'}$;

Bad6: $\exists (t_{i1}^j, t_{i2}^j, x_i^j, y_i^j) \in \tau_i, (t_{i'1}^{j'}, t_{i'2}^{j'}, x_{i'}^{j'}, y_{i'}^{j'}) \in \tau_{i'}$, and $(t_{i1}^j, t_{i2}^j, x_i^j, y_i^j) \neq (t_{i'1}^{j'}, t_{i'2}^{j'}, x_{i'}^{j'}, y_{i'}^{j'})$ such that $y_i^j \oplus y_{i'}^{j'} = H_{K_i}(t_{i2}^j) \oplus H_{K_{i'}}(t_{i'2}^{j'})$, where $(t_{i1}^j, t_{i2}^j), (t_{i'1}^{j'}, t_{i'2}^{j'}) \in \mathcal{T}$, $1 \leq i \neq i' \leq l, 1 \leq j \leq D_i$, and $1 \leq j' \leq D_{i'}$.

Otherwise we say that τ is good. We denote Γ_{good} (resp. Γ_{bad}) the set of good (resp. bad) transcripts. Let $\Gamma = \Gamma_{good} \cup \Gamma_{bad}$ be the set of attainable transcripts.

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

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

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

Proof. In the ideal world Y, $\tau = (K_1, \cdots, K_l, \tau_1, \cdots, \tau_l, \tau_{l+1})$ is an attainable transcript generated independently of the dummy key $K_i \in \mathcal{K}$ for $i = 1, \cdots, l$. We assume that an adversary $\mathcal{A}$ makes at most D construction queries and at most T primitive queries. For $(t_{i1}^j, t_{i2}^j, x_i^j, y_i^j) \in \tau_i$ and $(u^{j'}, v^{j'}) \in \tau_{l+1}$, where $(t_{i1}^j, t_{i2}^j) \in \mathcal{T}$, $1 \leq i \leq l, 1 \leq j \leq D_i$, $1 \leq j' \leq T$, and $D = \sum_{i=1}^{l} D_i$, by the properties of the (ϵ, δ)-AXU hash function H, we have

$$Pr[K_i \overset{\$}{\leftarrow} \mathcal{K} : H_{K_i}(t_{i1}^j) = x_i^j \oplus u^{j'} \vee H_{K_i}(t_{i2}^j) = y_i^j \oplus v^{j'}] \leq 2\delta.$$

It follows that,

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

Fix any distinct queries $(t_{i1}^j, t_{i2}^j, x_i^j, y_i^j) \neq (t_{i1}^{j'}, t_{i2}^{j'}, x_i^{j'}, y_i^{j'}) \in \tau_i$, where $(t_{i1}^j, t_{i2}^j), (t_{i1}^{j'}, t_{i2}^{j'}) \in \mathcal{T}$, $1 \leq i \leq l$, and $1 \leq j \neq j' \leq D_i$. By the properties of the (ϵ, δ)-AXU hash function H, we have

$$Pr[K_i \overset{\$}{\leftarrow} \mathcal{K} : H_{K_i}(t_{i1}^j) \oplus H_{K_i}(t_{i1}^{j'}) = C_1 \vee H_{K_i}(t_{i2}^j) \oplus H_{K_i}(t_{i2}^{j'}) = C_2] \leq 2\epsilon,$$

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

It follows that,

$$\begin{aligned} Pr[Bad3 \vee Bad4] &\leq \sum_{i=1}^{l} \sum_{j' \neq j=1}^{D_i} 2\epsilon \\ &\leq 2\sum_{i=1}^{l} \binom{D_i}{2} \epsilon. \end{aligned}$$

As there is at least one query for every key K_i, we consider the maximum case: the adversary makes $(D - l + 1)$ queries for some key, one query per key for another $l - 1$ keys. Therefore, we have

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

Given any distinct queries $(t_{i1}^j, t_{i2}^j, x_i^j, y_i^j) \in \tau_i, (t_{i'1}^{j'}, t_{i'2}^{j'}, x_{i'}^{j'}, y_{i'}^{j'}) \in \tau_{i'}$, and $(t_{i1}^j, t_{i2}^j, x_i^j, y_i^j) \neq (t_{i'1}^{j'}, t_{i'2}^{j'}, x_{i'}^{j'}, y_{i'}^{j'})$ such that $x_i^j \oplus x_{i'}^{j'} = H_{K_i}(t_{i1}^j) \oplus H_{K_{i'}}(t_{i'1}^{j'})$, 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 $D = \sum_{i=1}^{l} D_i = \sum_{i'=1}^{l} D_{i'}$.

As K_i and $K_{i'}$ are independently and randomly chosen from $\mathcal{K}$, we can not directly use the properties of the (ϵ, δ)-AXU hash function H. Therefore, we firstly consider the following probability.

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

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,

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

This completes the proof.

We then analyze good transcripts. For a good transcript, in the real world X, all tuples in $(K_1, \cdots, K_l, \tau_1, \cdots, \tau_{l+1})$ uniquely define an input-output pair of P, while in the ideal world it is not.

Lemma 5. *For any good transcript τ, one has*

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

Proof. Consider a good transcript $\tau \in \Gamma_{good}$. Denote by Ω_X the set of all possible oracles in the real world X and by Ω_Y the set of all possible oracles in the ideal world Y. Let $comp_X(\tau) \subseteq \Omega_X$ and $comp_Y(\tau) \subseteq \Omega_Y$ be the set of oracles compatible with transcript τ. According to the H-coefficients technique, we have

$Pr(D_X = \tau) = \frac{|comp_X(\tau)|}{|\Omega_X|}$, where $|\Omega_X| = 2^n!|\mathcal{K}|^l$.

$Pr(D_Y = \tau) = \frac{|comp_Y(\tau)|}{|\Omega_Y|}$, where $|\Omega_Y| = (\prod_t 2^n!)^l \cdot 2^n!|\mathcal{K}|^l$ and $t \in \mathcal{T}$.

Firstly, we calculate $|comp_X(\tau)|$. As $\tau \in \Gamma_{good}$, there are no two queries in τ with the same input or output of the underlying permutation. Any query tuple in τ therefore fixes exactly one input-output pair of the underlying oracle. Because τ consists of $D+T$ query tuples, the number of possible oracles in the real world X equals $(2^n - D - T)!$.

For the analysis in the ideal world Y, we define

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

By a similar reason, the number of possible oracles in the ideal world Y 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,

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

Therefore, we have $\frac{Pr[D_X=\tau]}{Pr[D_Y=\tau]} \geq 1$.

By Lemmas 1, 4, and 5, we have

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

The single-key security of HPH is a special case of the multi-key security of HPH where $l = 1$. We prove that the security bound of HPH in multi-key setting is a straightforward extension of the single-key setting. Therefore, the bound that we derived for HPH in the multi-key setting is tight. If we replace the public random permutation with an ideal block cipher with the same characteristics (including block-size, AXU-hash functions, etc), we can obtain the similar security.

5.3 Related-Key Security of HPH

Given a restricting RKD set Φ, let $\mathcal{H}$ be an (ϵ, δ)-RKA-AXU hash function family defined in Definition 2, then the related-key oracle of HPH is written as

$$\begin{aligned} RK[HPH]_K(\phi, t_1, t_2, x) &= HPH_{\phi(K)}(t_1, t_2, x) \\ &= P(x \oplus H_{\phi(K)}(t_1)) \oplus H_{\phi(K)}(t_2), \end{aligned}$$

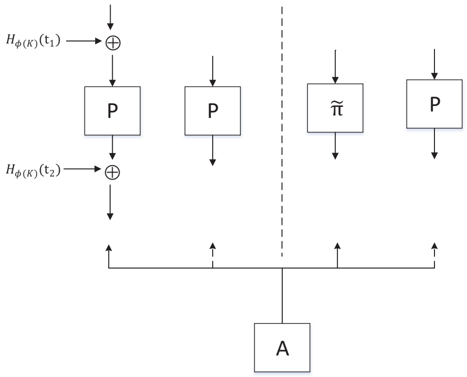

Fig. 4. Related-Key Security of HPH. **Left of dashed line**: Real world $X = (RK[HPH]^{\pm}_{K}; P^{\pm})$ with $K \xleftarrow{\$} \mathcal{K}, \phi \xleftarrow{\$} \Phi$, and $P \xleftarrow{\$} Perm(n)$. **Right of dashed line**: Ideal world $Y = (RK[\widetilde{\pi}]^{\pm}; P^{\pm})$ with $RK[\widetilde{\pi}] \xleftarrow{\$} \widetilde{RKPerm}(\Phi, \mathcal{T}, n)$ and $P \xleftarrow{\$} Perm(n)$. The goal of $\mathcal{A}$ is to distinguish the real world from the ideal world. If the distinguishable advantage of $\mathcal{A}$ is negligible, the scheme is related-key-STPRP secure. Although only one direction is shown, inverse oracles can be accessed as well. The number of queries by the adversary $\mathcal{A}$ to the first oracle is denoted by D, the number of queries to the last oracle by T.

where P is a n-bit public random permutation, $H \xleftarrow{\$} \mathcal{H}$ is a (ϵ, δ)-RKA-AXU hash function, $K \in \mathcal{K}$ is a key, $\phi \in \Phi$ is a RKD function, $(t_1, t_2) \in \mathcal{T}$ is a tweak, and $x \in \{0,1\}^n$ is a plaintext.

In this paper, we assume that an adversary makes two-directional queries to each oracle and never makes redundant queries. The related-key security of HPH is presented as follows.

Theorem 3 (Related-Key Security of HPH). *Let Φ be a restricting RKD set, $\phi \in \Phi, (t_1, t_2) \in \mathcal{T}$, and $HPH_K(t_1, t_2, x) = P(x \oplus H_K(t_1)) \oplus H_K(t_2)$ be the tweakable blockcipher with (ϵ, δ)-RKA-AXU hash function family, then for all adversaries $\mathcal{A}$ making at most D queries to $RK[HPH]^{\pm}_{K}$ (resp. $RK[\widetilde{\pi}]^{\pm}$) and at most T queries to $P^{\pm}$, the RK-STPRP advantage of $\mathcal{A}$ with respect to Φ is*

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

Our proof uses Patarin's H-coefficients technique [29]. As shown in Fig. 4, we consider an adversary $\mathcal{A}$ that has bidirectional access to two oracles (O_1, O_2). In the real world X, these are $(RK[HPH]^{\pm}_{K}; P^{\pm})$ with $K \xleftarrow{\$} \mathcal{K}, \phi \xleftarrow{\$} \Phi$, and $P \xleftarrow{\$} Perm(n)$, and in the ideal world Y, these are $(RK[\widetilde{\pi}]^{\pm}; P^{\pm})$ with $RK[\widetilde{\pi}] \xleftarrow{\$} \widetilde{RKPerm}(\Phi, \mathcal{T}, n)$ and $P \xleftarrow{\$} Perm(n)$. Without loss of generality, we assume that $\mathcal{A}$ is a deterministic adversary.

The interaction of $\mathcal{A}$ with the oracles can be described by a transcript $\tau = (K, \tau_1, \tau_2)$. We assume that the list of queries to O_1 is defined by $\tau_1 =$

$\{(\phi^1, t_1^1, t_2^1, x^1, y^1), \cdots, (\phi^D, t_1^D, t_2^D, x^D, y^D)\}$, where $(\phi^i, (t_1^i, t_2^i)) \in (\Phi, \mathcal{T})$ for $1 \leq i \leq D$, and to O_2 by $\tau_2 = \{(u^1, v^1), \cdots, (u^T, v^T)$. We assume the adversary never makes duplicate queries, so that $(\phi^i, t_1^i, t_2^i, x^i) \neq (\phi^j, t_1^j, t_2^j, x^j), (\phi^i, t_1^i, t_2^i, y^i) \neq (\phi^j, t_1^j, t_2^j, y^j), u^i \neq u^j, v^i \neq v^j$ for all i, j. Let D_X be the probability distribution of transcripts in the real world X and D_Y be the distribution of transcripts in the ideal world Y. A transcript τ is attainable if $Pr[D_Y = \tau] > 0$, meaning that it can occur during interaction with Y.

Definition 8. *We say that a transcript τ is bad if two different queries would result in the same input or output to P, when $\mathcal{A}$ interacting with the real world. Put formally, τ is bad if one of the following conditions is set:*

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 $\phi \in \Phi, (t_1, t_2) \in \mathcal{T}$;

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 $\phi \in \Phi, (t_1, t_2) \in \mathcal{T}$;

Bad3: $\exists(\phi, t_1, t_2, x, y) \neq (\phi', t_1', t_2', x', y') \in \tau_1$ such that $x \oplus x' = H_{\phi(K)}(t_1) \oplus H_{\phi'(K)}(t_1')$, where $\phi, \phi' \in \Phi, (t_1, t_2), (t_1', t_2') \in \mathcal{T}$;

Bad4: $\exists(\phi, t_1, t_2, x, y) \neq (\phi', t_1', t_2', x', y') \in \tau_1$ such that $y \oplus y' = H_{\phi(K)}(t_2) \oplus H_{\phi'(K)}(t_2')$, where $\phi, \phi' \in \Phi, (t_1, t_2), (t_1', t_2') \in \mathcal{T}$.

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

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

Lemma 6. *If H is (ϵ, δ)-RKA-AXU for the RKD set Φ and P is public random permutation, then*

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

Proof. In the ideal world Y, $\tau = (K, \tau_1, \tau_2)$ is an attainable transcript generated independently of the dummy key $K \in \mathcal{K}$. We assume that an adversary $\mathcal{A}$ makes at most D construction queries and at most T primitive queries. For any $(\phi, t_1, t_2, x, y) \in \tau_1$, where $\phi \in \Phi, (t_1, t_2) \in \mathcal{T}$, and $(u, v) \in \tau_2$, by the properties of the (ϵ, δ)-RKA-AXU hash function H, 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,

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

Fix any distinct queries $(\phi, t_1, t_2, x, y) \neq (\phi', t_1', t_2', x', y') \in \tau_1$, where $\phi, \phi' \in \Phi, (t_1, t_2), (t_1', t_2') \in \mathcal{T}$. By the properties of the (ϵ, δ)-RKA-AXU hash function H, we have

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

where $C_1 = x \oplus x'$ and $C_2 = y \oplus y'$.

It follows that,

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

Therefore,

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

We then analyze good transcripts.

Lemma 7. *For any good transcript τ, one has*

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

Proof. Consider a good transcript $\tau \in \Gamma_{good}$. Denote by Ω_X the set of all possible oracles in the real world X and by Ω_Y the set of all possible oracles in the ideal world Y. Let $comp_X(\tau) \subseteq \Omega_X$ and $comp_Y(\tau) \subseteq \Omega_Y$ be the set of oracles compatible with transcript τ. According to the H-coefficients technique, we have

$Pr(D_X = \tau) = \frac{|comp_X(\tau)|}{|\Omega_X|}$, where $|\Omega_X| = 2^n!|\mathcal{K}|$.

$Pr(D_Y = \tau) = \frac{|comp_Y(\tau)|}{|\Omega_Y|}$, where $|\Omega_Y| = \prod_{\phi,t}(2^n!) \cdot 2^n!|\mathcal{K}|$ and $(\phi, t) \in (\Phi, \mathcal{T})$.

Firstly, we calculate $|comp_X(\tau)|$. As $\tau \in \Gamma_{good}$, there are no two queries in τ with the same input or output of the underlying permutation. Any query tuple in τ therefore fixes exactly one input-output pair of the underlying oracle. Because τ consists of $D+T$ query tuples, the number of possible oracles in the real world X equals $(2^n - D - T)!$.

For the analysis in the ideal world Y, we define

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

By a similar reason, the number of possible oracles in Y equals $\prod_{\phi,t}(2^n - D_{\phi,t})!(2^n - T)!$, where $\sum_{\phi,t} D_{\phi,t} = D$. It follows that,

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

Therefore, we have $\frac{Pr[D_X = \tau]}{Pr[D_Y = \tau]} \geq 1$.

By H-coefficients technique, we have

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

The single-key security of HPH is also a special case of the related-key security of HPH if a RKD set $\Phi_{id} = \{\phi : K \to K\}$ is an identity transform. Therefore, the bound that we derived for HPH in the related-key setting is also tight. If we replace the public random permutation with an ideal block cipher with the same characteristics (including block-size, RKA-AXU-hash functions, etc), we can obtain the similar security.

6 Application to Authenticated Encryption

HPH can be used to improve security guarantee for encryption, authentication, and authenticated encryption modes. Mennink applied XPX to authenticated encryption modes (such as COPA [1], Minalper [35], and keyed-Sponge AE [26]) and message authentication code (MAC) Chaskey' (a modified version of Chaskey [28]), and proved that they are all related-key secure in [25]. HPH is a generalization of XPX, therefore HPH can be applied to these modes. In this section, we take OPP [18] as an example to illustrate the applications of HPH. Moreover, we improve OPP, provide a new authenticated encryption mode OPH, and prove its security.

6.1 Three Security Models

Authenticated encryption (AE) is a cryptographic scheme, which provides both privacy and authenticity. An authenticated encryption 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 based on a public random permutation $P \overset{\$}{\leftarrow} Perm(n)$. Let K be a key randomly chosen from $\mathcal{K}$. Let \$ be the randomized version of $\mathcal{E}_K$, which returns fresh and random answers to every query. We define the single-key-AE security of Π as

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

where $\perp$ always returns failure and the probabilities are taken over the random selections of K, P, and \$.

Similarity, we generalize it to multi-key security and related-key security.

The multi-key-AE security of Π is defined as

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

where $\perp$ always returns failure and the probabilities are taken over the random selections of K, P, and $\$_1, \cdots, \$_l$.

The related-key-AE security of Π is defined as

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

where $\perp$ always returns failure and the probabilities are taken over the random selections of K, P, and $RK[\$]$.

For $q, D, T \geq 0$, we define by

$$Adv_{\Pi}(q, D, T) = max_{\mathcal{A}} Adv_{\Pi}(\mathcal{A})$$

the security of Π against any adversary that makes q queries to the construction (D queries complexity) and T queries to the primitive $P^{\pm}$.

6.2 OPP

Offset Public Permutation (OPP) is a permutation-based nonce-respecting authenticated encryption mode presented by Granger et al. [18]. It utilizes a tweak-dependent masking function, which combines the advantages of word-oriented LFSR-based and powering-up-based methods. OPP is fully parallelizable and based on the MEM construction. The single-key-AE security of OPP was presented in [18]. Here we present the multi-key-AE security and related-key-AE security as follows.

Theorem 4. *Let $P \leftarrow Perm(n)$ and l be the number of keys. Then, in the nonce-respecting setting, the multi-key-AE advantage of OPP is*

$$Adv_{OPP}^{mk-ae}(q, D, T) \leq Adv_{MEM}^{mk-sprp} + l2^{n-\tau}/(2^n - 1).$$

Theorem 5. *Let $P \leftarrow Perm(n)$. Then, in the nonce-respecting setting, the related-key-AE advantage of OPP is*

$$Adv_{OPP}^{rk-ae}(q, D, T) \leq Adv_{MEM}^{rk-sprp} + 2^{n-\tau}/(2^n - 1).$$

The proofs of Theorems 4 and 5 are similar to [18].

6.3 OPH

We apply HPH to OPP [18], present a new nonce-respecting authenticated encryption mode, called OPH (Offset public Permutation with universal Hash functions mode), and prove its security. OPH inherits all advantages of OPP.

As the tweak-based masking function of OPP is based on the underlying primitive, OPP makes extra invocation to the underlying permutation for per-message encryption. While the masking function of OPH is generated by a family of universal hash functions. Therefore the efficiency of OPH is better than OPP. If the underlying permutation is replaced with AES-128, OPH is similar to OCB and the family of AXU-hash functions can be efficiently implemented by four-round AES (AES4 is an excellent choice in certain settings, such as restricted environments or devices with AES-NI).

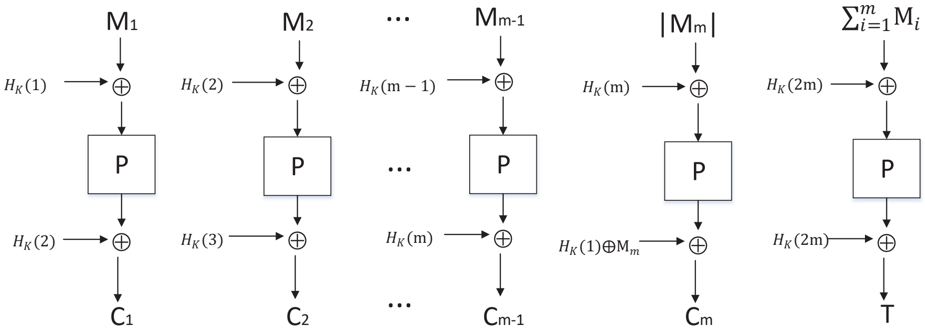

Fig. 5. HPH-based authenticated encryption mode OPH

```
/*Encryption Algorithm*/
Algorithm $OPH.\mathcal{E}_K^N(M)$:
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 $m-1$
    $C_i \leftarrow P(M_i \oplus H_K(i)) \oplus H_K(i+1)$
$C_m \leftarrow P(|M_m| \oplus H_K(m)) \oplus H_K(1) \oplus M_m$
$C \leftarrow C_1C_2\cdots C_m$
$T = P(\sum_{i=1}^{m} M_i \oplus H_K(2m)) \oplus H_K(2m)$
return $C\|T$
```

```
/*Decryption Algorithm*/
Algorithm $OPH.\mathcal{D}_K^N(C\|T)$:
Partition $C$ into $C_1\|\cdots\|C_m$,
$|C_i| = n, 1 \le i \le m-1, 0 < |C_m| \le n$
for $i = 1$ to $m-1$
    $M_i \leftarrow P^{-1}(C_i \oplus H_K(i+1)) \oplus H_K(i)$
$M_m \leftarrow P(|C_m| \oplus H_K(m)) \oplus H_K(1) \oplus C_m$
$M \leftarrow M_1M_2\cdots M_m$
$T' = P(\sum_{i=1}^{m} M_i \oplus H_K(2m)) \oplus H_K(2m)$
if $T' = T$, return $\top$, else return $M$
```

Fig. 6. HPH-based authenticated encryption mode OPH.

The overview of OPH is shown in Fig. 5. The encryption and decryption algorithms of OPH are given in Fig. 6.

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

Theorem 6. *Let $P \leftarrow Perm(n)$. Then, in the nonce-respecting setting, the single-key-AE advantage of OPH is*

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

Theorem 7. *Let $P \leftarrow Perm(n)$ and l be the number of keys. Then, in the nonce-respecting setting, the multi-key-AE advantage of OPH is*

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

Theorem 8. *Let $P \leftarrow Perm(n)$. Then, in the nonce-respecting setting, the related-key-AE advantage of OPH is*

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

7 Conclusion

In this paper, we present a generalized tweakable blockcipher HPH, whose maskings are implemented using universal hash functions. This paper focuses on the security of HPH in the single-key, multi-key, and related-key settings. In the single-key setting, we prove that HPH achieves strong tweakable pseudorandom permutation (STPRP) security in the random permutation model. Multi-key and related-key settings occur frequently in real-world implementations, that is to say, a plaintext may be encrypted under different keys. The adversary can perform chosen-plaintext and chosen-ciphertext attacks under a set of unknown keys. In the multi-key setting, these keys are independently and randomly chosen from the key space. We prove that HPH is MK-STPRP-secure. In the related-key setting, the adversary can observe the operation of a cipher under several different keys whose values are initially unknown, but where some mathematical relationship connecting the keys is known to the adversary. HPH with (ϵ, δ)-RKA-AXU-hash functions is RK-STPRP-secure up to $2DT\delta + D(D-1)\epsilon$ queries, where D is the complexity of construction queries (data complexity) and T is the complexity of internal permutation queries (time complexity).

HPH is a strongly secure cryptosystem with a lighter key schedule and higher key agility in the single-key, multi-key, and related-key attack settings. It is very useful, not only because of the simplicity of its design and proof (Patarin's H-coefficients technique), but also because of fast and secure implementations. If the underlying (tweakable) block cipher is replaced with HPH, then encryption, authentication, and authenticated encryption modes may be implemented more efficiently and may be more secure.

HPH can be used to improve security guarantee for encryption, authentication, and authenticated encryption modes. HPH can be applied to COPA [1], Minalper [35], keyed-Sponge AE [26], and Chaskey' [25]. We apply HPH to OPP [18], present a new OPH mode, and prove that OPH is single-key-AE secure, multi-key-AE secure, and related-key-AE secure.

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. LNCS, vol. 8269, pp. 424–443. Springer, Heidelberg (2013)
2. Bellare, M., Kohno, T.: A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 491–506. Springer, Heidelberg (2003)
3. Bhattacharyya, R., Roy, A.: Secure message authentication against related-key attack. In: Moriai, S. (ed.) FSE 2013. LNCS, vol. 8424, pp. 305–324. Springer, Heidelberg (2013)
4. Biham, E.: New Types of Cryptoanalytic Attacks Using related Keys (Extended Abstract). In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 398–409. Springer, Heidelberg (1993)
5. Biham, E.: New Types of Cryptanalytic Attacks Using Related Keys. J. Cryptology. 7(4), 229–246 (1994)

6. Biryukov, A., Khovratovich, D.: Related-key cryptanalysis of the full AES-192 and AES-256. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 1–18. Springer, Heidelberg (2009)
7. Bossuet, L., Datta, N., Mancillas-L´opez, C., Nandi, M.: ELmD: A Pipelineable Authenticated Encryption and Its Hardware Implementation. IEEE Transactions on Computers. 65(11): 3318–3331 (2016)
8. Chatterjee, S., Menezes, A., Sarkar, P.: Another Look at Tightness. In: Miri, A., Vaudenay, S. (eds.) SAC 2011. LNCS, vol. 7118, pp. 293–319. Springer, Heidelberg (2011)
9. 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. LNCS, vol. 6584, pp. 62–76. Springer, Heidelberg (2010)
10. Chen, S., Steinberger, J.P.: Tight Security Bounds for Key-Alternating Ciphers. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 327–350. Springer, Heidelberg (2014)
11. Cogliati, B., Lampe, R., Seurin, Y.: Tweaking Even-Mansour ciphers. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 189–208. Springer, Heidelberg (2015)
12. Cogliati, B., Seurin, Y.: EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9814, pp. 121–149. Springer, Heidelberg (2016)
13. Cogliati, B., Seurin, Y.: On the provable security of the iterated Even-Mansour cipher against related-key and chosen-key attacks. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 584–613. Springer, Heidelberg (2015)
14. 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. LNCS, vol. 9453, pp. 134–158. Springer, Heidelberg (2015)
15. Datta, N., Nandi, M.: ELmE: A misuse resistant parallel authenticated encryption. In: Susilo, W., Mu, Y. (eds.) ACISP 2014. LNCS, vol. 8544, pp. 306–321. Springer, Heidelberg (2014)
16. Dobraunig, C., Eichlseder, M., Mendel, F.: Related-key forgeries for Prost-OTR. In: Leander, G. (ed.) FSE 2015. LNCS, vol. 9054, pp. 282–296. Springer, Heidelberg (2015)
17. 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. LNCS, vol. 8873, pp. 420–438. Springer, Heidelberg (2014)
18. Granger, R., Jovanovic, P., Mennink, B., Neves, S..: Improved masking for tweakable blockciphers with applications to authenticated encryption. In: Fischlin, M., Coron, J. S. (eds.) EUROCRYPT 2016. LNCS, vol. 9665, pp. 263–293. Springer, Heidelberg (2016)
19. Halevi, S., Rogaway, P.: A tweakable enciphering mode. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 482–499. Springer, Heidelberg (2003)
20. Halevi, S., Rogaway, P.: A parallelizable enciphering mode. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 292–304. Springer, Heidelberg (2004)
21. Kurosawa, K.: Power of a public random permutation and its application to authenticated encryption. IEEE Transactions on Information Theory. 5(10): 5366–5374 (2010)
22. Landecker, W., Shrimpton, T., Terashima, R. S.: Tweakable Blockciphers with Beyond Birthday-Bound Security. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012, LNCS, vol. 7417, pp. 14–30. Springer, Heidelberg (2012)

23. Liskov, M., Rivest, R.L., Wagner, D.: Tweakable block ciphers. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 31–46. Springer, Heidelberg (2002)
24. Mantin, I., Shamir, A.: A Practical Attack on Broadcast RC4. In: Matsui, M. (ed.) FSE 2001. LNCS, vol. 2355, pp. 152–164. Springer, Heidelberg (2001)
25. Mennink, B.: XPX: Generalized Tweakable Even-Mansour with Improved Security Guarantees. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9814, pp. 64–94. Springer, Heidelberg (2016)
26. 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. LNCS, vol. 9453, pp. 465–489. Springer, Heidelberg (2015)
27. Mouha, N., Luykx, A.: Multi-key Security: The Even-Mansour Construction Revisited. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 209–223. Springer, Heidelberg (2015)
28. 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. LNCS, vol. 8781, pp. 306–323. Springer, Heidelberg (2014)
29. Patarin, J.: The "Coefficients H" Technique. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 328–345. Springer, Heidelberg (2008)
30. Peyrin, T., Sasaki, Y., Wang, L.: Generic related-key attacks for HMAC. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 580–597. Springer, Heidelberg (2012)
31. Reyhanitabar, R., Vaudenay, S., Vizr, 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. LNCS, vol. 8782, pp. 55C70. Springer, Heidelberg (2014)
32. Rogaway, P., Zhang, H.: Online ciphers from tweakable blockciphers. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 237–249. Springer, Heidelberg (2011)
33. Rogaway, P.: Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 16–31. Springer, Heidelberg (2004)
34. 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)
35. Sasaki, Y., Todo, Y., Aoki, K., Naito, Y., Sugawara, T., Murakami, Y., Matsui, M., Hirose, S.: Minalpher v1 (2014), submission to CAESAR competition.
36. 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. LNCS, vol. 8873, pp. 158–178. Springer, Heidelberg (2014)
37. Wang, P., Li, Y., Zhang, L., Zheng, K.: Related-Key Almost Universal Hash Functions: Definitions, Constructions and Applications. In: Peyrin, T. (ed.) FSE 2016. LNCS, vol. 9783, pp. 514–532. Springer, Heidelberg (2016)