

Designing Tweakable Enciphering Schemes Using Public Permutations

Debrup Chakraborty¹, Avijit Dutta², and Samir Kundu¹

¹ Indian Statistical Institute
203 B.T. Road, Kolkata-700108
E-mail: debrup@isical.ac.in, samirkundu3@gmail.com
² Institute for Advancing Intelligence, TCG-CREST
Salt Lake, Kolkata-700091
E-mail: avirocks.dutta13@gmail.com

Abstract. A tweakable enciphering scheme (TES) is a length preserving (tweakable) encryption scheme that provides (tweakable) strong pseudorandom permutation security on arbitrarily long messages. TES is traditionally built using block ciphers and the security of the mode depends on the strong pseudorandom permutation security of the underlying block cipher. In this paper, we construct TESs using public random permutations. Public random permutations are being considered as a replacement of block cipher in several cryptographic schemes including AEs, MACs, etc. However, to our knowledge, a systematic study of constructing TES using public random permutations is missing. In this paper, we give a generic construction of a TES which uses a public random permutation, a length expanding public permutation based PRF and a hash function which is both almost xor universal and almost regular. Further, we propose a concrete length expanding public permutation based PRF construction. We also propose a single keyed TES using a public random permutation and an AXU and almost regular hash function.

1 Introduction

Permutation Based Cryptography. A cryptographic permutation is a key-less public permutation that is designed to behave as a random permutation. In recent years cryptographic permutations have started to evolve as a useful primitive in parallel to the block ciphers. The primary feature of a cryptographic permutation is that it does not use any key and hence separate processing of the key and the data input is not required as in a block cipher. This makes cryptographic permutations a more efficient primitive compared to block ciphers in certain scenarios. The use of cryptographic permutation gained popularity during the SHA-3 competition [1], as several submitted candidates in the competition were based on this type of primitive. Furthermore, the selection of the permutation-based Keccak sponge function as the SHA-3 standard has generated ample confidence within the community for using this primitive [49]. In 2007, Bertoni et al. defined the cryptographic permutation based sponge function [7], which was initially aimed for hashing. Soon after, several efficient modes for encryption, authentication and authenticated encryption were developed [45, 5, 6]. Today, permutation based sponge-based

38 constructions have become a successful and a full-fledged alternative to the block cipher-
 39 based modes. In fact, in the first round of the ongoing NIST lightweight competition [47],
 40 24 out of 57 submitted constructions are based on cryptographic permutations, and out
 41 of 24, 16 permutation based proposals have qualified for round 2. These statistics, beyond
 42 any doubt, clearly depict the wide adoption of permutation based schemes [3, 4, 9, 15, 26,
 43 32] in parallel to the block cipher based designs. Apart from the modes, several cryp-
 44 tographic permutations have also been designed which are claimed to be efficient than
 45 standard block ciphers [8, 13, 4].

46
 47 Besides the permutation based designs of encryption/authentication schemes, a long line
 48 of research has been carried out in the study of designing block cipher and tweakable
 49 block cipher out of public random permutations. Even Mansour (EM) [36] and Iter-
 50 ated Even Mansour (IEM) ciphers are notable approaches in this direction. EM cipher
 51 is defined as $EM(x) \triangleq \pi(x \oplus k_1) \oplus k_2$, where π is a public random permutation and
 52 k_1, k_2 are two independent keys. Iterating EM cipher for $r \geq 2$ times with r indepen-
 53 dent permutations and $r + 1$ independent round keys defines the r -round IEM cipher, i.e.
 54 $EM^r(x) \triangleq k_{r+1} \oplus \pi_r(k_r \oplus \pi_{r-1}(\dots(\pi_2(k_2 \oplus \pi_1(k_1 \oplus x))\dots)))$. A long line of research has
 55 studied the security of r -round IEM [14, 25, 31, 27]. Recently, Chen et al. have designed
 56 two public permutation based PRFs [24] which have been proven to be secure beyond the
 57 birthday bound.

58
 59 **Tweakable Enciphering Schemes.** A *Tweakable Enciphering Scheme* or in short TES
 60 is a deterministic length preserving encryption scheme which provides security against
 61 adaptive chosen plaintext and ciphertext attacks, i.e., no efficient adversary should be
 62 able to distinguish ciphertexts from random strings and should not be able to tamper a ci-
 63 phertext so that it gets decrypted to something meaningful. The security requirement of a
 64 TES is very similar to that of a deterministic authenticated encryption (DAE) scheme [2].
 65 However, DAE schemes are not length preserving; the ciphertext resulting from the DAE
 66 is always expanded by the expansion factor defined by a specific DAE scheme. It is thus
 67 the length preserving property that makes TES a separate cryptographic primitive from
 68 DAE. The length preserving feature of TES makes it a suitable candidate for low level
 69 disk encryption [20, 16]. One can see a tweakable enciphering scheme as a tweakable block
 70 cipher [43] with arbitrary block lengths and are thus sometimes called wide block modes.

71
 72 Over the years, there have been several proposals of TES constructions and most of them
 73 are build on top of block ciphers. Constructions like CMC [38], EME [39], EME* [37],
 74 FMix [11], AEZ [40] are build only using block ciphers whereas XCB [44, 17], HCTR [51],
 75 HCH [20] uses both block ciphers and universal hash functions. There are few construc-
 76 tions of TES using stream ciphers [18, 50].

77 Most block cipher based schemes have been proven to be secure assuming the block
 78 cipher to be a strong pseudorandom permutation, as these constructions require the
 79 decryption functionality of the block cipher for deciphering the ciphertext. However, there
 80 are some constructions such as FMix [11], AEZ [40] and FAST [16], which do not require
 81 the decryption functionality of the block cipher and hence their security can be proved
 82 under the assumption that the underlying block cipher is a pseudorandom function. Such
 83 schemes are called *inverse free* TESs. Moreover, the security of all these constructions
 84 caps at birthday bound ¹. Dutta and Nandi [34] proposed a tweakable block cipher based
 85 TES and proved its security beyond the birthday bound ² assuming the underlying block
 86 cipher to be a tweakable strong pseudorandom permutation.

87
 88 **Our Contributions.** Although several modes for authentication, hash function, and au-
 89 thenticated encryption, have been developed using public permutations till date, **to our**
 90 **knowledge**, the only work which describes a TES built using a public random permuta-
 91 tion is [5]. The construction in [5] uses four round Luby Rackoff construction using two
 92 pseudorandom functions and the pseudorandom functions are constructed using public
 93 permutations. Concrete security bounds and formal security proofs for the TES scheme
 94 **are** not provided in [5] and to the best of our knowledge, there is no provably secure
 95 public permutation based TES scheme. We initiate a study of such a construction in this
 96 paper. Our concrete contributions are the following.

- 97 1. First, we propose a generic construction of a public permutation based TES, called
 98 **ppTES**. Our proposal closely resembles the HCTR construction. **ppTES** is designed
 99 using a public permutation π , a length expanding public permutation based pseudo-
 100 random function³ $F_k^{\pi'}$, where π and π' are two independent public random permu-
 101 tations over the same space. **Additionally**, **ppTES** uses a keyed hash function H_{k_h} ,
 102 which is required to be both almost xor universal (AXU) and almost regular (AR)
 103 (we further call such functions as AXUAR functions). We prove that if $F_k^{\pi'}$ is a se-
 104 cure length expanding public permutation based PRF and the hash function is a
 105 secure AXUAR function, then **ppTES** is secure against adaptive chosen plaintext and
 106 ciphertext adversaries.
- 107 2. As our second contribution, we construct a length expanding public permutation
 108 based PRF which we call **ppCTR**. **ppCTR** essentially is a counter mode of encryption

¹ A cryptographic construction is said to be birthday bound secure if its security retains as long as the number of queries is upto $2^{n/2}$, where n is the block size of the underlying primitive. In literature, there are plenty of constructions which are birthday bound secure [19, 21, 16, 22].

² A cryptographic construction is said to be beyond birthday bound secure if its security retains even if the number of queries exceeds $2^{n/2}$, where n is the block size of the underlying primitive. Examples of beyond birthday bound secure construction includes [28, 46, 29, 30, 35, 33].

³ Informally, a length expanding PRF takes an input x and the number of blocks b and outputs b many blocks, where block refers to an element of $\{0, 1\}^n$, for some fixed n .

109 where the block ciphers are replaced by the single round Even Mansour [36] construc-
 110 tion. We show that ppCTR offers a tight $n/2$ bit security. We use ppCTR and the
 111 PolyHash [52] function in ppTES construction to realize a concrete TES **which** we call
 112 ppHCTR. ppHCTR requires two keys and two independent public permutations.

113 3. Finally, we propose ppHCTR+, a public permutation based TES which uses a single
 114 key and a single public permutation. Along with the permutation, ppHCTR+ also
 115 requires an AXUAR hash function and the only key required in ppHCTR+ is the
 116 hash key of the AXUAR hash function. We prove that ppHCTR+ is a birthday bound
 117 secure public permutation based TES.

118 We would like to mention that any block-cipher based TES can be converted to a public
 119 permutation based scheme by replacing the block ciphers with a single round EM con-
 120 struction. But such direct replacement of block cipher by the EM scheme will require
 121 multiple keys, for example a direct replacement of the block cipher with the single round
 122 EM construction in HCTR mode results in a three keyed (along with the hash key)
 123 construction with two independent permutations. Whereas our proposed construction
 124 ppHCTR+ requires only the hash key and a single random permutation. Additionally,
 125 ppHCTR+ saves a few XOR counts compared to the direct replacement of the block ci-
 126 pher with single round EM construction. Also, ppHCTR+ **provides** comparable security
 127 to the existing block cipher based TES schemes.

128 2 Preliminaries

129 BASIC NOTATIONS. For a finite set \mathcal{X} , $X \leftarrow_{\$} \mathcal{X}$ denotes that X is sampled uniformly at
 130 random from \mathcal{X} . For a sequence of r random variables (X_1, \dots, X_r) , $X_1, \dots, X_r \leftarrow_{\$} \mathcal{X}$
 131 denotes that X_i 's are independently and uniformly sampled from \mathcal{X} . For $q \in \mathbb{N}$, we write
 132 $[q]$ to refer to the set $\{1, \dots, q\}$. For $n \in \mathbb{N}$, $\{0, 1\}^n$ denotes the set of all binary strings of
 133 length n and $\{0, 1\}^{\geq n}$ denotes the set of all binary strings of length at least n . Therefore,
 134 $\{0, 1\}^{\geq 0}$ is the set of all binary strings of arbitrary length (including the empty string
 135 ε) and denoted by $\{0, 1\}^*$. An element of $\{0, 1\}^n$ is called a *block*. For $x \in \{0, 1\}^*$, $|x|$
 136 denotes the length of x in bits. For $s \in \mathbb{N}$, $\text{first}(s, x)$ denotes the first s bits of a binary
 137 string x whose length is at least s . For $x, y \in \{0, 1\}^*$, $x||y$ denotes the concatenation of
 138 x followed by y . For $x, y \in \{0, 1\}^n$, we write $x \oplus y$ to denote their bitwise xor. For any
 139 $x \in \{0, 1\}^*$, $\text{parse}_n(x)$ parses x as $x_1||x_2||\dots||x_\ell$ where each x_i , for $i \in [\ell - 1]$, is a block
 140 and $0 \leq |x_\ell| \leq n$. For a sequence of elements $x^1, x^2, \dots, x^s \in \{0, 1\}^*$, we write x_a^i to
 141 denote the a -th block of the i -th element x^i . $\langle j \rangle$ denotes the n -bit binary representation
 142 of a non negative integer $j < 2^n$. For integers $1 \leq b \leq a$, we write $\mathbf{P}(a, b)$ to denote
 143 $a(a-1)\dots(a-b+1)$, where $\mathbf{P}(a, 0) = 1$ by convention.

144 The set of all functions from \mathcal{X} to \mathcal{Y} is denoted by $\text{Func}(\mathcal{X}, \mathcal{Y})$. When $\mathcal{Y} = \{0, 1\}^n$,
 145 then we denote $\text{Func}(\mathcal{X}, \{0, 1\}^n)$ simply as $\text{Func}_{\mathcal{X}}(n)$ and sometimes we write $\text{Func}(n)$ by

146 omitting \mathcal{X} when the domain of the function is understood from the context. We denote
 147 the set of all n bit permutations by $\text{Perm}(n)$.

148 2.1 Security Definitions

149 In this paper, we adapt the definitions of PRF and TES in the random permutation
 150 model.

PRF BASED ON PUBLIC RANDOM PERMUTATION. Let $F : \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{Y}$ be a keyed function from \mathcal{X} to \mathcal{Y} constructed using d many n -bit permutations $\boldsymbol{\pi} \triangleq (\pi_1, \dots, \pi_d)$, where \mathcal{K} is called the key space, \mathcal{X} is called the input space and \mathcal{Y} is called the output space. We consider the Pseudo Random Function (PRF) security of F under public permutation model where we assume that $\pi_1, \dots, \pi_d \leftarrow_{\$} \text{Perm}(n)$ and the distinguisher D is given access to either $(F_K^{\boldsymbol{\pi}}; \pi_1^{\pm}, \dots, \pi_d^{\pm})$ for a random key $K \leftarrow_{\$} \mathcal{K}$ or $(\text{RF}; \pi_1^{\pm}, \dots, \pi_d^{\pm})$ for $\text{RF} \leftarrow_{\$} \text{Func}(\mathcal{X}, \mathcal{Y})$. The superscript \pm for the π_i 's denotes that the distinguisher can query π_i in both the forward and reverse directions. Query of the distinguisher to π_i is called the *primitive query* and query to $F_K^{\boldsymbol{\pi}}$ or RF is called the *construction query*. We define the PRF advantage of F in public permutation model with respect to the distinguisher D that makes q construction queries and total q_p primitive queries as

$$\mathbf{Adv}_F^{\text{PRF}}(D) \triangleq | \Pr[D^{F_K^{\boldsymbol{\pi}}; \pi_1^{\pm}, \dots, \pi_d^{\pm}} \rightarrow 1] - \Pr[D^{\text{RF}; \pi_1^{\pm}, \dots, \pi_d^{\pm}} \rightarrow 1] |,$$

151 where $K \leftarrow_{\$} \mathcal{K}, \pi_1, \dots, \pi_d \leftarrow_{\$} \text{Perm}(n)$ and $\text{RF} \leftarrow_{\$} \text{Func}(\mathcal{X}, \mathcal{Y})$. F is said to be a (q, q_p, t) -
 152 secure PRF if $\mathbf{Adv}_F^{\text{PRF}}(q, q_p, t) \triangleq \max_D \mathbf{Adv}_F^{\text{PRF}}(D) \leq \epsilon$, where the maximum is taken
 153 over all distinguishers D that makes q construction queries, total q_p primitive queries and
 154 runs for time at most t .

155 TES BASED ON PUBLIC RANDOM PERMUTATION. Let \mathcal{K}, \mathcal{T} and \mathcal{M} be three non-empty
 156 finite sets. A *tweakable enciphering scheme* (TES) \mathfrak{T} is defined by a pair of efficient
 157 algorithms $\mathfrak{T} = (\text{Enc}, \text{Dec})$, where $\text{Enc} : \mathcal{K} \times \mathcal{T} \times \mathcal{M} \rightarrow \mathcal{M}$ and $\text{Dec} : \mathcal{K} \times \mathcal{T} \times \mathcal{M} \rightarrow$
 158 \mathcal{M} . Let Enc and Dec be constructed by d many n -bit permutations $\boldsymbol{\pi} \triangleq (\pi_1, \dots, \pi_d)$,
 159 then we call them by $\text{Enc}^{\boldsymbol{\pi}}$ and $\text{Dec}^{\boldsymbol{\pi}}$. For all $k \in \mathcal{K}$ and all $T \in \mathcal{T}$, $\text{Enc}_k^{\boldsymbol{\pi}}(T, \cdot)$ is a
 160 length preserving permutation over \mathcal{M} , i.e., $|\text{Enc}_k^{\boldsymbol{\pi}}(T, M)| = |M|$ for all $M \in \mathcal{M}$. For
 161 the correctness, one requires that for all $k \in \mathcal{K}$, for all $T \in \mathcal{T}$, and for all $M \in \mathcal{M}$,
 162 $\text{Dec}_k^{\boldsymbol{\pi}}(T, \text{Enc}_k^{\boldsymbol{\pi}}(T, M)) = M$. A *tweakable permutation* with tweak space \mathcal{T} and domain
 163 \mathcal{M} is a mapping $\tilde{\Pi} : \mathcal{T} \times \mathcal{M} \rightarrow \mathcal{M}$ such that for all tweak $T \in \mathcal{T}$, $M \mapsto \tilde{\Pi}(T, M)$ is a
 164 permutation of \mathcal{M} . We often write $\tilde{\Pi}^T(M)$ for $\tilde{\Pi}(T, M)$. $\text{TP}(\mathcal{T}, \mathcal{M})$ denotes the set of all
 165 such tweakable permutations.

We consider the tweakable Strong Pseudo Random Permutation (tSPRP) security of \mathfrak{T} in public permutation model where we assume that $\pi_1, \dots, \pi_d \leftarrow_{\$} \text{Perm}(n)$ and the distinguisher D is given access to either the oracles $(\mathfrak{T}.\text{Enc}_K^{\boldsymbol{\pi}}; \mathfrak{T}.\text{Dec}_K^{\boldsymbol{\pi}}; \pi_1^{\pm}, \dots, \pi_d^{\pm})$ for a

random key $K \leftarrow_s \mathcal{K}$ or the oracles $(\tilde{\Pi}; \tilde{\Pi}^{-1}; \pi_1^\pm, \dots, \pi_d^\pm)$ for $\tilde{\Pi} \leftarrow_s \text{TP}(\mathcal{T}, \mathcal{M})$. We call such a distinguisher as Chosen Ciphertext Attack (CCA) distinguisher. We define the tSPRP advantage of \mathfrak{D} in public permutation model with respect to the CCA distinguisher D that makes q_e encryption queries to the first oracle, q_d decryption queries to the second oracle and altogether q_p primitive queries as

$$\mathbf{Adv}_{\mathfrak{D}}^{\text{tSPRP}}(D) \triangleq | \Pr[D^{\mathfrak{S}. \text{Enc}_K^{\tilde{\Pi}}; \mathfrak{S}. \text{Dec}_K^{\tilde{\Pi}}; \pi_1^\pm, \dots, \pi_d^\pm} \rightarrow 1] - \Pr[D^{\tilde{\Pi}; \tilde{\Pi}^{-1}; \pi_1^\pm, \dots, \pi_d^\pm} \rightarrow 1] |,$$

where $K \leftarrow_s \mathcal{K}$, $\pi_1, \dots, \pi_d \leftarrow_s \text{Perm}(n)$ and $\tilde{\Pi} \leftarrow_s \text{TP}(\mathcal{T}, \mathcal{M})$. \mathfrak{D} is said to be a $(q_e, q_d, q_p, \ell, \sigma, t)$ -secure tSPRP if

$$\mathbf{Adv}_{\mathfrak{D}}^{\text{tSPRP}}(q_e, q_d, q_p, \ell, \sigma, t) \triangleq \max_D \mathbf{Adv}_{\mathfrak{D}}^{\text{tSPRP}}(D) \leq \epsilon,$$

166 where the maximum is taken over all CCA distinguishers D that run at most time t and
 167 make q_e encryption, q_d decryption and altogether q_p primitive queries with a maximum
 168 of ℓ data blocks present in a single encryption or decryption queried message and total
 169 σ many data blocks queried throughout all the encryption and decryption queries.

170 In all of the above definitions of security advantage, we omit the time parameter t for
 171 information-theoretic distinguisher ⁴. In the rest of the paper, we assume information-
 172 theoretic *non-trivial* distinguishers, i.e., they do not ask duplicate queries or queries
 173 to which they already can compute the answers by themselves from the earlier query-
 174 response. Since, we assume the distinguishers are computationally unbounded, without
 175 loss of generality, we limit the distinguishers to be deterministic.

176 **ALMOST (XOR) UNIVERSAL AND ALMOST REGULAR HASH FUNCTION.** Let $\mathcal{K}_h, \mathcal{X}$ be
 177 two non-empty finite sets and H be an n -bit keyed function $H : \mathcal{K}_h \times \mathcal{X} \rightarrow \{0, 1\}^n$.
 178 Then, H is said to be an ϵ -Almost Xor Universal (AXU) hash function if for any distinct
 179 $X, X' \in \mathcal{X}$ and for any $\delta \in \{0, 1\}^n$,

$$\Pr[K_h \leftarrow_s \mathcal{K}_h : H_{K_h}(X) \oplus H_{K_h}(X') = \delta] \leq \epsilon. \quad (1)$$

180 Moreover, H is said to be an ϵ -Almost Regular (AR) hash function if for any $X \in \mathcal{X}$ and
 181 for any $\delta \in \{0, 1\}^n$,

$$\Pr[K_h \leftarrow_s \mathcal{K}_h : H_{K_h}(X) = \delta] \leq \epsilon. \quad (2)$$

182 A keyed hash function is said to be an $(\epsilon_{\text{axu}}, \epsilon_{\text{reg}})$ -AXUAR hash function if it is ϵ_{axu} -AXU
 183 and ϵ_{reg} -AR hash function.

184 **POLYHASH FUNCTION.** PolyHash [52] is one of the popular examples of algebraic hash
 185 function, defined as follows: for a fixed key $k_h \in \{0, 1\}^n$ and for a message $M \in \{0, 1\}^*$,
 186 we first apply a padding rule 0^* i.e., pad the minimum number of zeros to the end of M ,

⁴ An information-theoretic distinguisher is the one who is computationally unbounded but can make a limited number of queries to its available oracles.

187 so that the total number of bits in the padded message becomes a multiple of n . Let the
 188 padded message be $M^* = M_1 \| M_2 \| \dots \| M_l$ where $l = \lceil |M|/n \rceil$ and for each i , $|M_i| = n$.
 189 Then,

$$\text{Poly}_{k_h}(M) = M_1 \cdot k_h^{l+1} \oplus M_2 \cdot k_h^l \oplus \dots \oplus M_l \cdot k_h^2 \oplus \langle |M| \rangle \cdot k_h, \quad (3)$$

190 where l is the number of blocks of M^* and the multiplications in Eqn. (3) are in the
 191 field $\text{GF}(2^n)$. If $M = \varepsilon$, the empty string, we define $\text{Poly}_{k_h}(\varepsilon) = k_h^2 \oplus k_h$. Note that
 192 the use of the non-injective padding rule (i.e., appending 0^* at the end of the message)
 193 does not make the hash function insecure as the definition includes the message length
 194 information which is the safeguard against the xor universal attack. The following result
 195 says that the PolyHash defined in Eqn. (3) with an n -bit key, is an $(\ell/2^n, \ell/2^n)$ -AXUAR
 196 hash function, where ℓ is the maximum number of message blocks. Proof of the lemma
 197 is straightforward and hence omitted.

198 **Lemma 1.** *PolyHash as defined in Eqn. (3) is $(\ell/2^n, \ell/2^n)$ -AXUAR hash function.*

199 2.2 An Useful Result

200 Let \mathfrak{T} be a public permutation based tweakable enciphering scheme over the message
 201 space \mathcal{M} and the tweak space \mathcal{T} . Let us assume that \mathfrak{T} is based on d many permuta-
 202 tions π_1, \dots, π_d . Let \mathbb{S}_0 and \mathbb{S}_1 are two functions sampled uniformly and independently
 203 from $\text{Func}(\mathcal{M}, \mathcal{M})$ and π_1, \dots, π_d are d many n -bit random permutations sampled uni-
 204 formly and independently from $\text{Perm}(n)$. Then, the following result says that a uniform
 205 length-preserving random permutation is very close to a uniform length-preserving ran-
 206 dom function. More formally,

207 **Theorem 1.** *Let \mathfrak{T} be a public permutation based TES over a message space $\mathcal{M} \subseteq \{0, 1\}^*$
 208 which is based on d many n -bit independent random permutations π_1, \dots, π_d . Let \mathbb{S}_0
 209 and \mathbb{S}_1 are two functions sampled uniformly and independently from $\text{Func}(\mathcal{M}, \mathcal{M})$ and
 210 π_1, \dots, π_d are d many n -bit random permutations sampled independently to \mathbb{S}_0 and \mathbb{S}_1 .
 211 Then, for any information theoretic non-trivial CCA distinguisher D , making altogether
 212 q encryption and decryption queries and total q_p primitive queries, we have,*

$$\begin{aligned} \text{Adv}_{\mathfrak{T}}^{\text{tSPRP}}(\mathsf{D}) &\leq \underbrace{|\Pr[\mathsf{D}^{\mathfrak{T}. \text{Enc}_K^{\pi}; \mathfrak{T}. \text{Dec}_K^{\pi}; \pi_1^{\pm}, \dots, \pi_d^{\pm}} \rightarrow 1] - \Pr[\mathsf{D}^{\mathbb{S}_0; \mathbb{S}_1; \pi_1^{\pm}, \dots, \pi_d^{\pm}} \rightarrow 1]|}_{\text{Adv}_{\mathfrak{T}}^{\pm \text{rnd}}(\mathsf{D})} \\ &\quad + \frac{q(q-1)}{2^{m+1}}, \quad \text{where } m = \min\{\ell : \mathcal{M} \cap \{0, 1\}^{\ell} \neq \emptyset\}. \end{aligned} \quad (4)$$

213 The above result has been already been used in the standard model in several places
 214 including in [12, 42]. The proof of Theorem 1 is very similar to the proof given in [42] and
 215 hence we omit it here.

2.3 H-Coefficient Technqie

In this section, we briefly discuss the H-Coefficient Technique, which was introduced by Patarin [48] and regained attention since the work of Chen and Steinberger [23] to analyze the security of iterated Even-Mansour [36] cipher. Since then, it has been successfully used as a tool to upper bound the statistical distance between the responses of two interactive systems and is typically used to prove the pseudo randomness of several constructions against information theoretic distinguishers. We consider a information theoretic deterministic distinguisher D with access to either the real oracle, i.e., the construction of our interest, or the ideal oracle which is usually considered to be a uniform random function or permutation. The collection of all the queries made by D to the oracle and the responses received by D from the oracle, is called the *attack transcript* of D , denoted as τ . Sometimes, we allow the oracle to release more internal information to D only after it completes all its queries, but before it outputs the decision bit. In this case, the transcript of D includes the additional information about the oracle and clearly the maximum distinguishing advantage of D in this setting can not be less than that of without additional information. The transcript τ is a random variable and the randomness of the distribution of τ comes only from the randomness of the oracle with which D interacts.

Let T_{re} and T_{id} denote the random variable that takes the transcript τ resulting from the interaction between D and the real world or between D and the ideal world respectively. The probability of realizing a transcript τ in the real (resp. ideal) world is called the *real (resp. ideal) interpolation probability*. A transcript τ is said to be *attainable* with respect to D if its ideal interpolation probability is non-zero (i.e., $\Pr[T_{\text{id}} = \tau] > 0$). We denote the set of all attainable transcripts by \mathcal{V} . Following these notations, we state the main theorem of H-Coefficient Technique [48, 23] as follows:

Theorem 2 (H-Coefficient Technique). *Let D be a fixed deterministic distinguisher that has access to either the real oracle \mathcal{O}_{re} or the ideal oracle \mathcal{O}_{id} . Let $\mathcal{V} = \mathcal{V}_{\text{g}} \cup \mathcal{V}_{\text{b}}$, $\mathcal{V}_{\text{g}} \cap \mathcal{V}_{\text{b}} = \emptyset$, be some partition of the set of all attainable transcripts of D . Suppose there exists $\epsilon_{\text{ratio}} \geq 0$ such that for any $\tau \in \mathcal{V}_{\text{g}}$,*

$$\frac{\Pr[T_{\text{re}} = \tau]}{\Pr[T_{\text{id}} = \tau]} \geq 1 - \epsilon_{\text{ratio}},$$

and there exists $\epsilon_{\text{bad}} \geq 0$ such that $\Pr[T_{\text{id}} \in \mathcal{V}_{\text{b}}] \leq \epsilon_{\text{bad}}$. Then,

$$\mathbf{Adv}_{\mathcal{O}_{\text{re}}}^{\mathcal{O}_{\text{id}}}(D) \triangleq |\Pr[D^{\mathcal{O}_{\text{re}}} \rightarrow 1] - \Pr[D^{\mathcal{O}_{\text{id}}} \rightarrow 1]| \leq \epsilon_{\text{ratio}} + \epsilon_{\text{bad}}. \quad (5)$$

3 HCTR Construction

HCTR is one of the popular tweakable enciphering modes, proposed by Wang et al. [51], that turns an n -bit strong pseudorandom permutation into a variable length tweakable

HCTR.Enc $_{k,k_h}(T, M)$	HCTR.Dec $_{k,k_h}(T, C)$
1. $M_1 \parallel \dots \parallel M_l \leftarrow \text{parse}_n(M)$;	1. $C_1 \parallel \dots \parallel C_l \leftarrow \text{parse}_n(C)$;
2. $\mathbf{M}_L \leftarrow M_1; \mathbf{M}_R \leftarrow (M_2 \parallel \dots \parallel M_l)$;	2. $\mathbf{C}_L \leftarrow C_1; \mathbf{C}_R \leftarrow (C_2 \parallel \dots \parallel C_l)$;
3. $U \leftarrow \mathbf{M}_L \oplus \text{Poly}_{k_h}(\mathbf{M}_R \parallel T)$;	3. $V \leftarrow \mathbf{C}_L \oplus \text{Poly}_{k_h}(\mathbf{C}_R \parallel T)$;
4. $V \leftarrow \mathbf{E}_k(U); Z \leftarrow U \oplus V$;	4. $U \leftarrow \mathbf{E}_k^{-1}(V); Z \leftarrow U \oplus V$;
5. for $i = 1$ to l	5. for $i = 1$ to l
6. $S_i \leftarrow \mathbf{E}_k(Z \oplus i)$;	6. $S_i \leftarrow \mathbf{E}_k(Z \oplus i)$;
7. $\mathbf{S} \triangleq S_1 \parallel \dots \parallel S_l$;	7. $\mathbf{S} \triangleq S_1 \parallel \dots \parallel S_l$;
8. $\mathbf{C}_R \leftarrow \text{first}(\mathbf{M}_R , \mathbf{S}) \oplus \mathbf{M}_R$;	8. $\mathbf{M}_R \leftarrow \text{first}(\mathbf{C}_R , \mathbf{S}) \oplus \mathbf{C}_R$;
9. $\mathbf{C}_L \leftarrow V \oplus \text{Poly}_{k_h}(\mathbf{C}_R \parallel T)$;	9. $\mathbf{M}_L \leftarrow U \oplus \text{Poly}_{k_h}(\mathbf{M}_R \parallel T)$;
10. return $(\mathbf{C}_L \parallel \mathbf{C}_R)$;	10. return $(\mathbf{M}_L \parallel \mathbf{M}_R)$;

Fig. 3.1. HCTR construction based on an n -bit block cipher \mathbf{E}_k and an n -bit Polyhash function. Left part of the algorithm is the encryption function and right part is the decryption function.

244 strong pseudorandom permutation. The encryption and decryption algorithm of HCTR
 245 is shown in Fig. 3.1 and its pictorial representation is shown in Fig. 3.2.

246 We explain the encryption algorithm of HCTR using an example. The decryption
 247 algorithm can be understood in a similar way. Suppose the input message $M = (M_1 \parallel M_2)$
 248 and for the sake of simplicity, we assume that $|M_1| = |M_2| = n$, i.e., M consists of two
 249 full blocks. Therefore, in step (2) of the algorithm, the variable \mathbf{M}_L is assigned to M_1
 250 and \mathbf{M}_R is assigned to M_2 . In step (3) of the algorithm, we evaluate the poly hash Poly_{k_h}
 251 on $(M_2 \parallel T)$ which results to $M_2 \cdot k_h^3 \oplus T \cdot k_h^2 \oplus (|M_2| + |T|) \cdot k_h$ which is xored with
 252 the n -bit value M_1 to produce U . In step (4), we take the xor of U and its encryption
 253 $V = \mathbf{E}_k(U)$ to produce Z . In step (6), we compute the key stream $\mathbf{S} = S_1 \parallel S_2$ where each
 254 $|S_1| = |S_2| = n$. Since, $|\mathbf{M}_R| = n$, \mathbf{C}_R will be $M_2 \oplus S_1$, which becomes the input along
 255 with tweak T to the poly hash function Poly_{k_h} . Evaluation of the poly hash on input
 256 $\mathbf{C}_R \parallel T$ results to $\mathbf{C}_R \cdot k_h^3 \oplus T \cdot k_h^2 \oplus (|\mathbf{C}_R| + |T|) \cdot k_h$. Then the result is xored with V to
 257 produce \mathbf{C}_L , which is returned along with \mathbf{C}_R as the encryption of $M = M_1 \parallel M_2$.

258 Wang et al. [51] have shown that HCTR is a secure TES against all adaptive chosen plain-
 259 text and chosen ciphertext adversaries that make roughly $2^{n/3}$ encryption and decryption
 260 queries. Later Chakraborty and Nandi [19] improved its security bound to $O(\sigma^2/2^n)$,
 261 where σ is the total number of message blocks among all q queries. Recently, Dutta and
 262 Nandi [34] proposed a **tweakable** block cipher based HCTR, called *tweakable* HCTR, and
 263 showed its security beyond the birthday bound.

264 *Remark 1.* In [51], authors defined the output of the PolyHash to be the hash key k_h for
 265 ε . But that definition of the PolyHash function leads to an attack on the construction

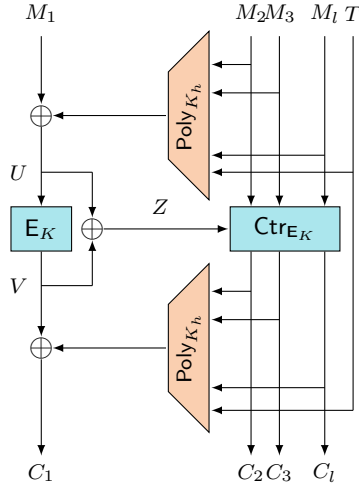


Fig. 3.2. HCTR construction with tweak T and message $M_1 \| M_2 \| \dots \| M_i$ and the corresponding ciphertext $C_1 \| C_2 \| \dots \| C_i$. Poly_{K_h} is the polynomial hash function with hash key K_h . Ctr_{E_K} is the block cipher based counter mode of encryption.

266 as reported in [41]. This attack does not work if the message space contains messages of
 267 length at least $n + 1$. We redefine the output of the PolyHash for an empty input string
 268 to be $k_h^2 \oplus k_h$, which eliminates the message length restriction.

269 Motivated by HCTR, we first replace the block cipher based counter mode part of HCTR
 270 with a public permutation based length expanding PRF, and the block cipher E_K (see
 271 Fig. 3.2) with a public permutation π . We show that such combination yields a secure
 272 public permutation based TES, which we call ppTES as described in section 4. In section
 273 6, we construct a public permutation based length expanding PRF, which we call ppCTR.
 274 Using ppCTR along with the the PolyHash function, we instantiate ppTES to realize a
 275 public permutation based TES, which we call ppHCTR. However, ppHCTR requires two
 276 independent public permutations, a key for the ppCTR and another independent hash
 277 key for the PolyHash function. Next, we go one step further to reduce the number of
 278 keys and permutations used in ppHCTR and come up with a single keyed (for the Poly-
 279 Hash function) and single permutation based TES construction, ppHCTR+. We describe
 280 ppHCTR+ in section 7.

281 4 ppTES : A Generic Public Permutation Based TES

282 ppTES is based on three cryptographic components: (i) an n -bit public random permuta-
 283 tion π_1 , (ii) an AXUAR hash function H_{k_h} which maps $\{0, 1\}^*$ to $\{0, 1\}^n$, and (iii) a public
 284 permutation based length expanding PRF $F_k^{\pi_2}$, where π_2 is a n -bit independent public

285 random permutation independent of π_1 . The message space of **ppTES** is $\{0, 1\}^{\geq n}$ and the
 286 tweak space is $\{0, 1\}^{\text{tw}}$. The working principle of **ppTES** is exactly same as HCTR where
 287 the block cipher is replaced by a public permutation π_1 and the counter mode encryption
 288 is replaced by a public permutation based length expanding PRF $F_k^{\pi_2}$. The algorithmic
 289 description of encryption and decryption function of **ppTES** is shown in Fig. 4.1. The
 290 description in Fig. 4.1 mentions $F_k^{\pi_2}$, which is a length expanding PRF. We describe this
 291 primitive next.

ppTES.Enc $_{k,k_h}^{\pi_1,\pi_2}(T, M)$	ppTES.Dec $_{k,k_h}^{\pi_1,\pi_2}(T, C)$
<ol style="list-style-type: none"> 1. $M_1 \parallel \dots \parallel M_\ell \leftarrow \text{parse}_n(M)$; 2. $\mathbf{M}_L \leftarrow M_1; \mathbf{M}_R \leftarrow (M_2 \parallel \dots \parallel M_\ell)$; 3. $U \leftarrow \mathbf{M}_L \oplus H_{k_h}(\mathbf{M}_R \parallel T)$; 4. $V \leftarrow \pi_1(U); Z \leftarrow U \oplus V$; 5. $\mathbf{S} \triangleq S_1 \parallel \dots \parallel S_{\ell-1} \leftarrow F_k^{\pi_2}(Z, \ell)$; 6. $\mathbf{C}_R \leftarrow \text{first}(\mathbf{M}_R , \mathbf{S}) \oplus \mathbf{M}_R$; 7. $\mathbf{C}_L \leftarrow V \oplus H_{k_h}(\mathbf{C}_R \parallel T)$; 8. return $(\mathbf{C}_L \parallel \mathbf{C}_R)$; 	<ol style="list-style-type: none"> 1. $C_1 \parallel \dots \parallel C_\ell \leftarrow \text{parse}_n(C)$; 2. $\mathbf{C}_L \leftarrow C_1; \mathbf{C}_R \leftarrow (C_2 \parallel \dots \parallel C_\ell)$; 3. $V \leftarrow \mathbf{C}_L \oplus H_{k_h}(\mathbf{C}_R \parallel T)$; 4. $U \leftarrow \pi_1^{-1}(V); Z \leftarrow U \oplus V$; 5. $\mathbf{S} \triangleq S_1 \parallel \dots \parallel S_{\ell-1} \leftarrow F_k^{\pi_2}(Z, \ell)$; 6. $\mathbf{M}_R \leftarrow \text{first}(\mathbf{C}_R , \mathbf{S}) \oplus \mathbf{C}_R$; 7. $\mathbf{M}_L \leftarrow U \oplus H_{k_h}(\mathbf{M}_R \parallel T)$; 8. return $(\mathbf{M}_L \parallel \mathbf{M}_R)$;

Fig. 4.1. **ppTES** based on an n -bit public random permutations π_1 , an AXUAR hash function H_{k_h} and a public permutation based length expanding PRF $F_k^{\pi_2}$. $M \in \{0, 1\}^{\geq n}$ is the input message and $T \in \{0, 1\}^{\text{tw}}$ is the tweak. Left part of the algorithm is the encryption function and right part is the decryption function.

292 As in case of HCTR to explain the encryption algorithm we use a two block message
 293 $M = (M_1 \parallel M_2)$, where $|M_1| = |M_2| = n$. On input M , in step (2) of the algorithm, the
 294 variable \mathbf{M}_L is assigned to M_1 and \mathbf{M}_R is assigned to M_2 . In step (3) of the algorithm,
 295 we evaluate the hash value H_{k_h} on $(M_2 \parallel T)$ which is xored with the n -bit value M_1 to
 296 produce U . In step (4), we take the xor of U and its permuted value $V = \pi_1(U)$ to
 297 produce Z . In step (5), we compute the key stream $\mathbf{S} = S_1$ using length expanding PRF
 298 $F_k^{\pi_2}$ where $|S_1| = n$. Since, $|\mathbf{M}_R| = n$, \mathbf{C}_R will be $M_2 \oplus S_1$, which becomes the input
 299 along with tweak T to the hash function H_{k_h} . Then the resulting hash value is xored with
 300 V to produce \mathbf{C}_L , which is returned along with \mathbf{C}_R as the encryption of $M = M_1 \parallel M_2$.

301 4.1 Length Expanding Pseudorandom Function

302 For an arbitrary large positive integer L , Let $\mathcal{F} \subseteq \text{Func}(\{0, 1\}^n \times \mathbb{N}, \cup_{0 < i \leq L} \{0, 1\}^{ni})$, such
 303 that $F \in \mathcal{F}$ if and only if the following two conditions are satisfied:

- 304 1. For every $x \in \{0, 1\}^n$ and every $b \in [L]$, $|F(x, b)| = nb$.
 305 2. For every $x \in \{0, 1\}^n$ and every $b, b' \in [L]$, $b \geq b'$, $\text{first}(nb', F(x, b)) = F(x, b')$.

306 We call a uniform random element of \mathcal{F} a *length expanding random function*.

307 In Fig. 4.2 we give an algorithmic description of a length expanding random function
 308 ρ . The algorithm depicts ρ as a lazy sampler which gives as output $\rho(x, b)$ upon receiving
 309 a query (x, b) . For any input (x, b) , it first checks whether x is a fresh element or not.
 310 If it is fresh, then it samples b many blocks uniformly at random from $\{0, 1\}^{nb}$. If it is
 311 not fresh, then it first checks whether the number of requested blocks b' in the earlier
 312 query for input x is less than the number of requested blocks in the current query for the
 313 same input. In that case, it first fetches b' many blocks which are already stored at $\mathbb{T}[x]$,
 314 and then samples the remaining blocks, i.e., $b - b'$ blocks independently and uniformly
 315 at random from $\{0, 1\}^{n(b-b')}$ which is appended with the first b' many fetched blocks and
 316 finally updates the entry $\mathbb{T}[x]$ with the output of the current query. The final case is if
 317 the number of requested blocks in the current query for input x is less than the number
 318 of requested blocks in the earlier query with the same input. Then it fetches the first b
 319 many blocks out of b' many blocks which are already stored at $\mathbb{T}[x]$ and returns it.

320 Informally, length expanding pseudorandom function is a function which is indistin-
 321 guishable from a length expanding random function by any efficient distinguisher. For
 322 the sake of our **construction**, we require a public permutation based length expanding
 323 PRF which we formally define next.

Definition 1. Public Permutation Based Length Expanding PRF . Let L be an arbitrary large positive integer and let $F : \mathcal{K} \times \{0, 1\}^n \times [L] \rightarrow \cup_{1 \leq i \leq L} \{0, 1\}^{ni}$ be a keyed function based on d many n -bit permutations $\pi \triangleq (\pi_1, \dots, \pi_d)$ such that for any input $(x, b) \in \{0, 1\}^n \times [L]$, $F_K^\pi(x, b)$ returns (y_1, \dots, y_b) where each $y_i \in \{0, 1\}^n$. We consider the length expanding PRF security of F under public permutation model where we assume that $\pi_1, \dots, \pi_d \leftarrow_{\$} \text{Perm}(n)$ and the distinguisher D is given access to either of the world $(F_K^\pi, \pi_1^\pm, \dots, \pi_d^\pm)$ for a random key $K \leftarrow_{\$} \mathcal{K}$ or $(\rho, \pi_1^\pm, \dots, \pi_d^\pm)$, where ρ works as shown in Fig 4.2. We define the LENPRF advantage of F in public permutation model with respect to the distinguisher D that makes q construction queries and total q_p primitive queries as

$$\mathbf{Adv}_F^{\text{LENPRF}}(D) \triangleq | \Pr[D^{F_K^\pi, \pi_1^\pm, \dots, \pi_d^\pm} \rightarrow 1] - \Pr[D^{\rho, \pi_1^\pm, \dots, \pi_d^\pm} \rightarrow 1] |,$$

324 where $K \leftarrow_{\$} \mathcal{K}$, $\pi_1, \dots, \pi_d \leftarrow_{\$} \text{Perm}(n)$. F is said to be a (q, q_p, σ, t) -secure LENPRF if
 325 $\mathbf{Adv}_F^{\text{LENPRF}}(q, q_p, \sigma, t) \triangleq \max_D \mathbf{Adv}_F^{\text{LENPRF}}(D) \leq \epsilon$, where the maximum is taken over
 326 all distinguishers D that makes q construction queries with total $\sigma = (b_1 + \dots + b_q)$ blocks,
 327 where b_i is the number of blocks requested at i -th construction query. It also makes total
 328 q_p primitive queries and runs for time at most t . As before, for information theoretic
 329 distinguisher, we omit the time parameter t and in the rest of the paper, we assume the
 330 distinguisher is information theoretic.

Algorithm for ρ

```

1. initialize:
2. for all  $x \in \{0, 1\}^n$ 
3.    $\mathbb{T}[x] \leftarrow \perp; \mathbb{L}[x] \leftarrow \perp;$ 
4. end for;
5. on input  $(x, b) \neq (x', b')$ ;
6.   if  $x = x'$ 
7.     if  $b > b'$ , then
8.        $Y \triangleq (y_{b'+1}, y_{b'+2}, \dots, y_b) \leftarrow_{\$} \{0, 1\}^{n(b-b')}$ ;
9.        $\mathbb{T}[x] \leftarrow \mathbb{T}[x] || Y; \mathbb{L}[x] \leftarrow b;$  return  $\mathbb{T}[x];$ 
10.    else return  $\mathbb{T}[x']_{1, \dots, b};$ 
11.    end if;
12.  else
13.     $Y \triangleq (y_1, \dots, y_b) \leftarrow_{\$} \{0, 1\}^{nb};$ 
14.     $\mathbb{T}[x] \leftarrow Y; \mathbb{L}[x] \leftarrow b;$ 
15.    return  $\mathbb{T}[x];$ 
16.  end if;
```

Fig. 4.2. Algorithm corresponding to a length expanding random function. $\mathbb{T}[x]_{1, \dots, b}$ denotes the first b many blocks stored at the x -th entry of table \mathbb{T} .

331 *Remark 2.* The length expanding PRF is a weaker notion than the notion of variable
 332 output length PRF [10]. For a length expanding PRF, if two queries have the same input
 333 with different number of requesting blocks, then one output is a prefix of other. In case
 334 of variable output length PRF, outputs for two queries are completely random even if
 335 they have the same input with different number of requesting blocks.

336 4.2 Security of ppTES

337 In this section, we show that if $\pi_1, \pi_2 \leftarrow_{\$} \text{Perm}(n)$ are two independently sampled n -bit
 338 public random permutations, $K \leftarrow_{\$} \{0, 1\}^n$ be a uniformly sampled n -bit key, H is an
 339 $(\epsilon_{\text{axu}}, \epsilon_{\text{reg}})$ -AXUAR n -bit keyed hash function and $\mathsf{F}_K^{\pi_2}$ is a secure public permutation
 340 based length expanding PRF, then ppTES is a public permutation based secure TES
 341 against all $(q_e, q_d, q_{p_1} + q_{p_2}, \ell, \sigma)$ information theoretic adaptive CCA distinguishers that
 342 make q_e many encryption, q_d many decryption queries with total σ many blocks queried
 343 among all $q \triangleq q_e + q_d$ queries and ℓ is the maximum number of message blocks present
 344 in a single encryption or decryption query. Moreover, it also makes q_{p_1} primitive queries
 345 to π_1 and q_{p_2} primitive queries to π_2 . Formally, the following result bounds the tSPRP
 346 advantage of ppTES in public permutation model.

347 **Theorem 3.** Let \mathcal{K}_h be a finite and non-empty set, $\pi_1, \pi_2 \leftarrow_{\$} \text{Perm}(n)$ be two indepen-
 348 dently sampled n -bit public random permutations and $K \leftarrow_{\$} \{0, 1\}^n$ be an n -bit random
 349 key. Let $\mathbf{H} : \mathcal{K}_h \times \{0, 1\}^* \rightarrow \{0, 1\}^n$ be an $(\epsilon_{\text{axu}}, \epsilon_{\text{reg}})$ -AXUAR n -bit keyed hash function.
 350 Let $\mathbf{F}_K^{\pi_2}$ be a secure LENPRF. Then, for any $(q_e, q_d, q_{p_1} + q_{p_2}, \ell, \sigma)$ information theoretic
 351 adaptive CCA distinguisher \mathbf{D} against the tSPRP security of $\text{ppTES}[\pi_1, \pi_2, K, \mathbf{H}]$ in the
 352 public permutation model, there exists a LENPRF adversary \mathbf{B} against the length expand-
 353 ing PRF security of $\mathbf{F}_K^{\pi_2}$ in the public permutation model, where σ is the total number of
 354 message blocks queried, such that

$$\text{Adv}_{\text{ppTES}}^{\text{tSPRP}}(\mathbf{D}) \leq \text{Adv}_{\mathbf{F}}^{\text{LENPRF}}(\mathbf{B}) + q^2 \epsilon_{\text{axu}} + 2qq_{p_1} \epsilon_{\text{reg}} + \frac{q^2}{2^{n+1}} + \frac{q(q-1)}{2^{n+1}}.$$

355 The proof of this result is given in section 5.

356 5 Proof of Theorem 3

357 As a matter of convenience, we refer to the construction $\text{ppTES}[\pi_1, \pi_2, K, \mathbf{H}]$ as simply
 358 ppTES when the underlying primitives are assumed to be understood.

359 5.1 Initial Set Up

360 By Theorem 1, we have

$$\text{Adv}_{\text{ppTES}}^{\text{tSPRP}}(\mathbf{D}) \leq \text{Adv}_{\text{ppTES}}^{\pm\text{rnd}}(\mathbf{D}) + \frac{q(q-1)}{2^{n+1}}, \quad (6)$$

361 where recall that n is the minimum message length allowed for ppTES . Therefore, we
 362 bound the $\pm\text{rnd}$ advantage of ppTES . Let \mathbf{D} be any information theoretic non-trivial adap-
 363 tive deterministic CCA distinguisher with access to the oracles in either of the following
 364 two worlds: in the real world it interacts with $\mathcal{O}_{\text{re}} = (\text{ppTES}.\text{Enc}_{K, K_h}^{\pi_1, \pi_2}, \text{ppTES}.\text{Dec}_{K, K_h}^{\pi_1, \pi_2}, \pi_1^{\pm}, \pi_2^{\pm})$
 365 for an n -bit random key K , a random hash key K_h and two independent n -bit random
 366 permutations π_1 and π_2 or in the ideal world it interacts with $\mathcal{O}_{\text{id}} = (\$0, \$1, \pi_1^{\pm}, \pi_2^{\pm})$,
 367 where $\$0$ and $\$1$ are two independent random functions that **output** uniform random
 368 strings for every distinct input. Now, our goal is to upper bound the maximum advan-
 369 tage in distinguishing the real world from the ideal one.

For doing this, as the first step of the proof, we replace $\mathbf{F}_K^{\pi_1, \pi_2}$ with the function ρ as
 described in Fig. 4.2. We call the resulting construction as ppTES^* . This replacement
 comes at the cost of the length expanding PRF security of $\mathbf{F}_K^{\pi_1, \pi_2}$ in the random permutation
 model, where the PRF adversary \mathbf{B} simulates \mathbf{D} as follows: it first samples a hash key
 $K_h \leftarrow_{\$} \mathcal{K}_h$ and an n -bit random permutation $\pi \leftarrow_{\$} \text{Perm}(n)$. Then, for any input (M, T) ,
 it computes

$$Z \leftarrow \pi_1(\mathbf{H}_{K_h}(\mathbf{M}_{\mathbf{R}} \| T) \oplus \mathbf{M}_{\mathbf{L}}) \oplus \mathbf{H}_{K_h}(\mathbf{M}_{\mathbf{R}} \| T) \oplus \mathbf{M}_{\mathbf{L}}.$$

370 Then it calls its own oracle with $(Z, \lceil \frac{|M|}{n} \rceil)$ as input and receives the $n \lceil \frac{|M|}{n} \rceil$ bit **output** \mathbf{S} .
 371 Then it masks the first $|M_{\mathbf{R}}|$ bits of \mathbf{S} with $M_{\mathbf{R}}$ and produces the ciphertext blocks $\mathbf{C}_{\mathbf{R}}$
 372 which is hashed along with T and the hash output is masked with $\pi_1(\mathbf{H}_{K_h}((M_{\mathbf{R}}\|T)\oplus M_{\mathbf{L}}))$
 373 to generate the first ciphertext block $\mathbf{C}_{\mathbf{L}}$. For any primitive query x made by \mathbf{D} to π_1 , \mathbf{B}
 374 accordingly returns the value $\pi_1(x)$. Similarly, it returns the response for backward query
 375 to π_1 . For any primitive query x made by \mathbf{D} to π_2 , \mathbf{B} forwards the query to its own oracle
 376 and returns the received response. Similarly, it returns the response for backward query
 377 to π_2 . Finally \mathbf{B} outputs the same bit as returned by \mathbf{D} . Therefore, we have

$$\mathbf{Adv}_{\text{ppTES}}^{\pm\text{rnd}}(\mathbf{D}) \leq \mathbf{Adv}_{\mathbf{F}}^{\text{LENPRF}}(\mathbf{B}) + \underbrace{\mathbf{Adv}_{\text{ppTES}^*}^{\pm\text{rnd}}(\mathbf{D})}_{\delta^*}. \quad (7)$$

378 5.2 Attack Transcript

379 Our main goal is to bound δ^* , i.e., we need to distinguish the two worlds: the real
 380 world $\mathcal{O}_{\text{re}} = (\text{ppTES}^*. \text{Enc}_{K, K_h}^{\pi_1, \pi_2}, \text{ppTES}^*. \text{Dec}_{K, K_h}^{\pi_1, \pi_2}, \pi_1^{\pm}, \pi_2^{\pm})$ from the ideal world $\mathcal{O}_{\text{id}} =$
 381 $(\$_0, \$_1, \pi_1^{\pm}, \pi_2^{\pm})$, where K is an n -bit random key, K_h is a random hash key and π_1, π_2
 382 are two independent n -bit random permutations. Since, we consider the maximum distin-
 383 guishing advantage, let us assume that \mathbf{D} be the information theoretic non-trivial adaptive
 384 CCA distinguisher for which the distinguishing advantage is maximum. Let \mathbf{D} makes q_e
 385 (resp. q_d) encryption (resp. decryption) queries and q_{p_1} primitive queries to π_1 and q_{p_2}
 386 primitive queries to π_2 . Since, our proof is in random permutation model, \mathbf{D} can query
 387 the primitive in forward and reverse direction. After the interaction is over, the real world
 388 returns the hash key K_h and the ideal world samples a dummy hash key $K_h \leftarrow \$\mathcal{K}_h$ and
 389 returns it to \mathbf{D} . Finally, \mathbf{D} outputs a single bit. Let $\tau \triangleq \{(T^1, M^1, C^1), (T^2, M^2, C^2),$
 390 $\dots, (T^q, M^q, C^q)\}$ be the list of construction queries and responses (i.e., including en-
 391 cryption and decryption queries), $\tau_{p_1} \triangleq \{(x_1, y_1), (x_2, y_2), \dots, (x_{q_{p_1}}, y_{q_{p_1}})\}$ and $\tau_{p_2} \triangleq$
 392 $\{(u_1, v_1), (u_2, v_2), \dots, (u_{q_{p_2}}, v_{q_{p_2}})\}$ be the two list of primitive queries and responses to
 393 π_1 and π_2 respectively made by \mathbf{D} . The triplet $\tau' = (\tau, \tau_{p_1}, \tau_{p_2}, K_h)$ constitutes the query
 394 transcript of the attack.

395 5.3 Definition and Probability of Bad Transcripts

396 In this section, we define bad transcripts and bound their probability in the ideal world.
 397 From transcript τ' , we derive the following notation: for $i \in q$, $U_i = M_1^i \oplus \mathbf{H}_{K_h}(M_2^i \| \dots \| M_{l_i}^i \| T^i)$,
 398 $V_i = C_1^i \oplus \mathbf{H}_{K_h}(C_2^i \| \dots \| C_{l_i}^i \| T^i)$ and $Z_i = U_i \oplus V_i$. Having set up the notation, we identify
 399 an event to be bad if for any two construction queries there is a collision in the Z_i values
 400 or there is a non-trivial input or output collision of the permutation π_1 .

401 **Definition 2 (Bad Transcript for ppTES*).** *An attainable transcript $\tau' = (\tau, \tau_p, \tau'_p, K_h)$*
 402 *is called bad for ppTES* if any of the following conditions hold:*

- 403 - B.1 : $\exists i \neq j \in [q]$ such that, $U^i = U^j$.
 404 - B.2 : $\exists i \neq j \in [q]$ such that $V^i = V^j$.
 405 - B.3 : $\exists i \in [q]$ and $j \in [q_p]$ such that $U^i = x_j$.
 406 - B.4 : $\exists i \in [q]$ and $j \in [q_p]$ such that $V^i = y_j$.
 407 - B.5 : $\exists i, j \in [q]$ such that $Z^i = Z^j$.

Lemma 2. Let T_{id} be the random variable that takes the transcript resulting from the interaction between the distinguisher and the ideal world and \mathcal{V}_b be the set of all attainable bad transcripts for ppTES*. Then we have,

$$\Pr[T_{\text{id}} \in \mathcal{V}_b] \leq \epsilon_{\text{bad}} = q^2 \epsilon_{\text{axu}} + 2qq_p \epsilon_{\text{reg}} + \frac{q^2}{2^{n+1}}.$$

408 **Proof.** By the union bound,

$$\Pr[T_{\text{id}} \in \mathcal{V}_b] \leq \sum_{i=1}^4 \Pr[\text{B.}i] + \Pr[\text{B.5} \mid \overline{\text{B.1}} \wedge \overline{\text{B.2}} \wedge \overline{\text{B.3}} \wedge \overline{\text{B.4}}]. \quad (8)$$

409 In the following, we bound the probability of all the bad events individually. The lemma
 410 will follow by adding the individual bounds.

411 **Bounding B.1.** For two fixed values of i and j , we compute the probability of the event
 412 $U^i = U^j$. Note that $U^i = U^j$ implies the hash equation: $H_{K_h}(\mathbf{M}_{\mathbf{R}}^i \| T^i) \oplus H_{K_h}(\mathbf{M}_{\mathbf{R}}^j \| T^j) =$
 413 $M_1^i \oplus M_1^j$. By fixing the value of all other random variables in the hash equation, the prob-
 414 ability of this event is bounded by the AXU advantage of the hash function. Therefore,
 415 by summing over all possible choices of i and j , we have

$$\Pr[\text{B.1}] \leq \binom{q}{2} \epsilon_{\text{axu}}. \quad (9)$$

416 **Bounding B.2.** This event is similar to that of B.1 where we consider the output collision
 417 of π . Note that, $V^i = V^j$ implies the hash equation: $H_{K_h}(\mathbf{C}_{\mathbf{R}}^i \| T^i) \oplus H_{K_h}(\mathbf{C}_{\mathbf{R}}^j \| T^j) =$
 418 $C_1^i \oplus C_1^j$. Similar to B.1, we bound the event using the AXU advantage of the the hash
 419 function and thus we have

$$\Pr[\text{B.2}] \leq \binom{q}{2} \epsilon_{\text{axu}}. \quad (10)$$

420 **Bounding B.3.** For two fixed values of i and j , we compute the probability of the event
 421 $U^i = x_j$. Note that $U^i = x_j$ implies the hash equation: $H_{K_h}(\mathbf{M}_{\mathbf{R}}^i \| T^i) = M_1^i \oplus x_j$. By
 422 fixing the value of all other random variables in the hash equation, the probability of this
 423 event is bounded by the AR advantage of the hash function. Therefore, by summing over
 424 all possible choices of i and j , we have

$$\Pr[\text{B.3}] \leq qq_{p_1} \epsilon_{\text{reg}}. \quad (11)$$

425 **Bounding B.4.** For two fixed values of i and j , we compute the probability of the event
 426 $V^i = y_j$. Note that $V^i = y_j$ implies the hash equation: $H_{K_h}(\mathbf{C}_R^i \| T^i) = C_1^i \oplus y_j$. Similar
 427 to B.3, we bound the event using the AR advantage of the hash function and thus we
 428 have

$$\Pr[\text{B.4}] \leq qq_{p_1} \epsilon_{\text{reg}}. \quad (12)$$

429 **Bounding B.5 | $\overline{\text{B.1}} \wedge \overline{\text{B.2}} \wedge \overline{\text{B.3}} \wedge \overline{\text{B.4}}$.** To bound this event, we first fix the value of
 430 i and j . Note that $Z^i = Z^j$ implies $U^i \oplus V^i = U^j \oplus V^j$. Now, due to the condition, we
 431 have $U^i \neq U^j$ and $V^i \neq V^j$. Therefore, we obtain the following hash equation:

$$H_{K_h}(\mathbf{M}_R^i \| T^i) \oplus H_{K_h}(\mathbf{C}_R^i \| T^i) \oplus H_{K_h}(\mathbf{M}_R^j \| T^j) \oplus H_{K_h}(\mathbf{C}_R^j \| T^j) = W, \quad (13)$$

432 where $W = M_1^i \oplus M_1^j \oplus C_1^i \oplus C_1^j$. W.l.o.g we assume that $i < j$. If the j -th query is an
 433 encryption query, then C_1^j is uniformly distributed in the ideal world and if the j -th query
 434 is a decryption query, then M_1^j is uniformly distributed in the ideal world. Combining
 435 the above two arguments and by varying over all possible choices of indices, we have

$$\Pr[\text{B.5}] \leq \frac{\binom{q}{2}}{2^n}. \quad (14)$$

The proof follows from Eqn. (8)-Eqn. (12) and Eqn. (14). \square

436 5.4 Analysis of Good Transcript

437 In this section, we show that for a good transcript $\tau' = (\tau, \tau_{p_1}, \tau_{p_2}, k_h)$, realizing τ' is
 438 almost as likely in the real world as in the ideal world.

Lemma 3. *Let $\tau' = (\tau, \tau_{p_1}, \tau_{p_2}, k_h)$ be a good transcript. Then*

$$\frac{\Pr[\text{T}_{\text{re}} = \tau']}{\Pr[\text{T}_{\text{id}} = \tau']} \geq 1.$$

439 **Proof.** Since, in the ideal world, the encryption and the decryption oracle behaves per-
 440 fectly random, we have

$$\Pr[\text{T}_{\text{id}} = \tau'] = \frac{1}{|\mathcal{K}_h|} \frac{1}{\mathbf{P}(2^n, q_{p_1})} \cdot \frac{1}{\mathbf{P}(2^n, q_{p_2})} \cdot \frac{1}{2^{n\sigma}}, \quad (15)$$

441 where σ is the total number of blocks queried among all q construction queries that
 442 includes encryption and decryption queries.

443 **REAL INTERPOLATION PROBABILITY.** Since, τ' is a good transcript, all the inputs and
 444 outputs of π_1 are fresh. Moreover, all Z_i values are distinct. Therefore, the outputs of ρ
 445 are all uniformly random. Since, there are total $q_{p_1} + q$ many invocations of π_1 , we have

$$\Pr[\text{T}_{\text{re}} = \tau'] = \frac{1}{|\mathcal{K}_h|} \frac{1}{\mathbf{P}(2^n, q_{p_1} + q)} \cdot \frac{1}{\mathbf{P}(2^n, q_{p_2})} \cdot \frac{1}{(2^n)^{\sigma-q}}. \quad (16)$$

By doing a simple algebraic calculation, it is easy to see that the ratio of Eqn. (16) to Eqn. (15) is at least 1 and hence proves the result. \square

By combining Lemma 2, Lemma 3, Theorem 2, Eqn. (6) and Eqn. (7), the result follows. \square

446 6 ppCTR: Public Permutation Based Length Expanding PRF

In this section, we propose ppCTR, a public permutation based length expanding PRF. Our proposed construction is a public permutation variant of the block cipher based standard counter mode encryption where the block cipher is replaced by a single round EM [36] cipher. The working principle of ppCTR is as follows: it takes an n -bit public random permutation π and an n -bit random key k . Then for any n -bit input value z and an integer b , it outputs b many blocks where the j -th block S_j is defined as follows:

$$S_j \triangleq \pi(z \oplus \gamma^j k) \oplus \gamma^j k, \quad j \in [b],$$

where γ is the root of a primitive polynomial of $\text{GF}(2^n)$. In the following section, we

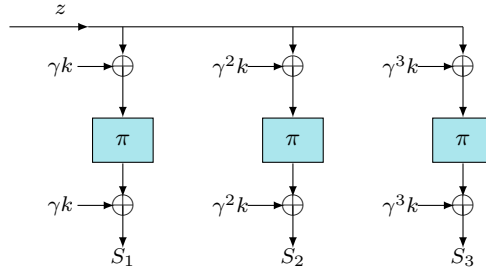


Fig. 6.1. ppCTR construction with an n -bit input z and an integer $b = 3$ and corresponding output $S_1 \| S_2 \| S_3$. π is the public random permutation, k is the key and γ is the root of a primitive polynomial of $\text{GF}(2^n)$.

447

448 state and prove that ppCTR is a public permutation based secure LENPRF against all
 449 adversaries that makes roughly $2^{n/2}$ construction and primitive queries. It is needless to
 450 say that the above bound is tight as EM cipher is known to have a tight birthday bound
 451 security [36].

452 6.1 Security Analysis of ppCTR

453 In this section, we show that ppCTR is a public permutation based length expanding
 454 PRF.

455 **Theorem 4.** Let $\pi \leftarrow_{\$} \text{Perm}(n)$ be an n -bit public random permutation and let $K \leftarrow_{\$} \{0, 1\}^n$
 456 be an n -bit random key. Then, for any (q, q_p, σ) adversary D against the LENPRF security
 457 of $\text{ppCTR}[\pi, K]$, we have

$$\text{Adv}_{\text{ppCTR}}^{\text{LENPRF}}(D) \leq \frac{\sigma^2}{2^n} + \frac{2\sigma q_p}{2^n},$$

458 where σ is the total number of blocks queried across all q queries.

Proof. Let D_{\max} be the distinguisher with maximum distinguishing advantage in distinguishing the following two worlds: (a) in the real world it interacts with $\mathcal{O}_{\text{re}} = (\text{ppCTR}[\pi, K], \pi^{\pm})$ for a random n -bit key K and a random n -bit permutation π and (b) in the ideal world it has access to $\mathcal{O}_{\text{id}} = (\rho, \pi^{\pm})$, where ρ works in the similar way as shown in Fig. 4.2. It makes q construction queries and q_p primitive queries. After the interaction is over, the real world returns K to D_{\max} and the ideal world randomly samples a dummy key $K \leftarrow_{\$} \{0, 1\}^n$ and returns to D_{\max} . Finally, D_{\max} outputs a bit. Let $\tau \triangleq \{(z_1, b_1, \mathbf{S}^1), (z_2, b_2, \mathbf{S}^2), \dots, (z_q, b_q, \mathbf{S}^q)\}$ be the list of construction queries and responses, where $\mathbf{S}^i = (S_1^i, \dots, S_{b_i}^i)$ and $\tau_p \triangleq \{(x_1, y_1), (x_2, y_2), \dots, (x_{q_p}, y_{q_p})\}$ be the list of primitive queries and responses to π made by D_{\max} . Let $\sigma = (b_1 + \dots + b_q)$ denotes the total number of blocks queried across all q queries. The triplet $\tau' = (\tau, \tau_p, K)$ constitutes the query transcript of the attack. We define a relation \sim over τ such that $(z_i, b_i, \mathbf{S}_i) \sim (z_j, b_j, \mathbf{S}_j)$ if and only if $z_i = z_j$. Thus, \sim induces a partition on τ and let us assume we have r many such partitions. Each partition contains c_i many elements and therefore, $c_1 + \dots + c_r = q$. Note that, there exists a total ordering among b_i values in each component. This allows us to sort the elements of each component in the ascending order of their b values. After rearrangement, we have the following:

$$\left\{ \begin{array}{l} \{(z_1, b_1^1, \mathbf{S}_1^1), \dots, (z_1, b_{c_1}^1, \mathbf{S}_{c_1}^1)\} \\ \{(z_2, b_1^2, \mathbf{S}_1^2), \dots, (z_2, b_{c_2}^2, \mathbf{S}_{c_2}^2)\} \\ \vdots \quad \quad \quad \vdots \quad \quad \quad \vdots \quad \quad \quad \vdots \\ \{(z_r, b_1^r, \mathbf{S}_1^r), \dots, (z_r, b_{c_r}^r, \mathbf{S}_{c_r}^r)\} \end{array} \right.$$

459 Note that, for each $i \in [r]$, $b_{c_i}^i \geq b_{c_i-1}^i \geq \dots \geq b_1^i$ and \mathbf{S}_j^i is a prefix of \mathbf{S}_{j+1}^i for all $j \in [c_i]$.

460 6.2 Definition and Probability of Bad Transcripts

461 In this section, we define bad transcripts and bound their probability in the ideal world.
 462 Informally, we define an event to be bad if it introduces any non-trivial input or output
 463 collision of the permutation π .

464 **Definition 3. (Bad Transcript for ppCTR)** : An attainable transcript $\tau' = (\tau, \tau_p, K)$
 465 is called a **bad transcript** for ppCTR if any of the following conditions hold:

- 466 - **B.1** : $\exists i \neq j \in [r], \alpha \in [\ell_{c_i}]$ and $\beta \in [\ell_{c_j}]$ such that $z_i \oplus \gamma^\alpha K = z_j \oplus \gamma^\beta K$.
 467 - **B.2** : $\exists i \in [r], j \in [q_p]$ and $\alpha \in [\ell_{c_i}]$ such that $z_i \oplus \gamma^\alpha K = x_j$.
 468 - **B.3** : $\exists i \neq j \in [r], \alpha \in [\ell_{c_i}]$ and $\beta \in [\ell_{c_j}]$ such that $S_\alpha^i \oplus \gamma^\alpha K = S_\beta^j \oplus \gamma^\beta K$.
 469 - **B.4** : $\exists i \in [r], j \in [q_p]$ and $\alpha \in [\ell_{c_i}]$ such that $S_\alpha^i \oplus \gamma^\alpha K = y_j$.

Lemma 4. Let T_{id} be the random variable that takes the transcript resulting from the interaction between the distinguisher and the ideal world and \mathcal{V}_b be the set of all attainable bad transcripts for ppCTR. Then we have,

$$\Pr[T_{\text{id}} \in \mathcal{V}_b] \leq \epsilon_{\text{bad}} = \frac{\sigma^2}{2^n} + \frac{2\sigma q_p}{2^n}.$$

470 **Proof.** By the union bound,

$$\Pr[T_{\text{id}} \in \mathcal{V}_b] \leq \sum_{i=1}^4 \Pr[\text{B.i}]. \quad (17)$$

471 In the following, we bound the probability of all the bad events individually. The lemma
 472 will follow by adding the individual bounds.

473 **Bounding B.1.** To bound this event, we first fix a value of the indices $i \neq j \in [r]$ and
 474 $\alpha \in [\ell_{c_i}], \beta \in [\ell_{c_j}]$. For such a fixed choice of indices, we bound the probability of the
 475 event $z_i \oplus \gamma^\alpha K = z_j \oplus \gamma^\beta K$. Now, if $\alpha = \beta$, then the probability of the event is zero as
 476 $z_i \neq z_j$. Therefore, we assume that $\alpha \neq \beta$. For this choice of indices, we write the event
 477 as

$$K = (\gamma^\alpha \oplus \gamma^\beta)^{-1}(z^i \oplus z^j). \quad (18)$$

478 The probability of Eqn. (18) is 2^{-n} , due to the randomness of the key K . Therefore, by
 479 varying over all possible choices of i, j, α and β , we have

$$\Pr[\text{B.1}] \leq \frac{\sigma^2}{2^{n+1}}. \quad (19)$$

480 **Bounding B.2.** For a fixed choice of $i \in [r], j \in [q_p]$ and $\alpha \in [\ell_{c_i}]$, the probability of the
 481 event $K = \gamma^{-\alpha}(z^i \oplus x_j)$ is bounded by 2^{-n} due to the randomness of K . Therefore, by
 482 varying over all possible choices of i, j and α , we have

$$\Pr[\text{B.2}] \leq \frac{q_p}{2^n}(b_{c_1} + \dots + b_{c_r}) \leq \frac{\sigma q_p}{2^n}. \quad (20)$$

483 **Bounding B.3.** Bounding this event is similar to that of B.1. To bound this event, we
 484 first fix the value of the indices $i \neq j \in [r]$ and $\alpha \in [\ell_{c_i}], \beta \in [\ell_{c_j}]$. For such a fixed choice
 485 of indices, we bound the probability of the event $S_\alpha^i \oplus \gamma^\alpha K = S_\beta^j \oplus \gamma^\beta K$. Now we have
 486 the following two cases:

- **Case A.** Let us consider that $\alpha = \beta$. As $i \neq j$, without loss of generality, we assume that $i < j$. Therefore, the event boils down to $S_\alpha^i = S_\alpha^j$, which is bounded by 2^{-n} due to the randomness of S_α^j . Therefore, by varying over all possible choices of i, j and α , we have

$$\Pr[\text{B.3}] \leq \frac{\sigma^2}{2^{n+1}}$$

- 487 - **Case B.** if $\alpha \neq \beta$, then the event can be equivalently written as

$$K = (\gamma^\alpha \oplus \gamma^\beta)^{-1}(S_\alpha^i \oplus S_\beta^i). \quad (21)$$

Since, $\alpha \neq \beta$, we have $\gamma^\alpha \oplus \gamma^\beta \neq 0$ and therefore, the probability of Eqn. (21) is 2^{-n} due to the randomness of the key K . Therefore, by varying over all possible choices of i, j, α and β , we have

$$\Pr[\text{B.3}] \leq \frac{\sigma^2}{2^{n+1}}.$$

- 488 By taking the maximum of the above two, we have

$$\Pr[\text{B.3}] \leq \frac{\sigma^2}{2^{n+1}}. \quad (22)$$

- 489 **Bounding B.4.** Bounding this event is exactly identical to that of B.2, where we use the
490 randomness of K to bound the event. Therefore, we have

$$\Pr[\text{B.4}] \leq \frac{q_p}{2^n}(b_{c_1} + \dots + b_{c_r}) \leq \frac{\sigma q_p}{2^n}. \quad (23)$$

The proof follows from Eqn. (17) and Eqn. (19)-Eqn. (23). \square

491 6.3 Analysis of Good Transcript

- 492 In this section, we show that for a good transcript $\tau' = (\tau, \tau_p, k)$, realizing τ' is almost as
493 likely in the real world as in the ideal world.

Lemma 5. *Let $\tau' = (\tau, \tau_p, k)$ be a good transcript. Then*

$$\frac{\Pr[\text{T}_{\text{re}} = \tau']}{\Pr[\text{T}_{\text{id}} = \tau']} \geq 1.$$

- 494 **Proof.** Consider a good transcript $\tau' = (\tau, \tau_p, k)$. In the ideal world, ρ randomly sam-
495 ples nb_{c_i} bit output for i -th class and the key k is sampled uniformly from $\{0, 1\}^n$ and
496 independent to all other sampled random variables. Thus, we have

$$\Pr[\text{T}_{\text{id}} = \tau'] = \frac{1}{2^n} \cdot \frac{1}{\mathbf{P}(2^n, q_p)} \cdot \prod_{i=1}^r \frac{1}{2^{nqb_{c_i}}}. \quad (24)$$

497 For computing the real interpolation probability, as τ' is good, all the inputs and outputs
 498 of π are distinct. The total number of π invocations including the primitive queries is
 499 $(b_{c_1} + \dots + b_{c_r} + q_p)$. Therefore,

$$\Pr[\mathsf{T}_{\text{re}} = \tau'] = \frac{1}{2^n} \cdot \frac{1}{\mathbf{P}(2^n, b_{c_1} + \dots + b_{c_r} + q_p)}. \quad (25)$$

It is trivial to see that the ratio of Eqn. (25) to Eqn. (24) is at least 1. Hence the result of Lemma 5 follows. Finally, by combining Lemma 4, Lemma 5 and Theorem 2, the result of Theorem 4 follows. \square

500 6.4 ppHCTR : An Instantiation of ppTES with ppCTR and PolyHash

501 We instantiate the public permutation based length expanding PRF $F_k^{\pi_2}$ of ppTES[$\pi_1, \pi_2, k,$
 502 H] with ppCTR[π_2, k] and its underlying AXUAR hash function H_{k_h} with the PolyHash
 503 function Poly_{k_h} , as described in Eqn. (3), to realize a practical candidate of a public
 504 permutation based TES, referred to as ppHCTR[$\pi_1, \pi_2, k, \text{Poly}_{k_h}$]. We assume that the
 505 tweak is μ blocks long, i.e., $\text{tw} = n\mu$ and thus, for any $i \in [q]$, the maximum degree of
 506 $\text{Poly}_{k_h}(M_2^i \parallel \dots \parallel M_{l_i}^i \parallel T^i)$ is $\hat{l}_i + \mu$, where $\hat{l}_i = \lceil \frac{|M_{\mathbf{R}}^i|}{n} \rceil$. Since, $\hat{l}_i \leq \ell$ for all $i \in [q]$, where
 507 ℓ denotes the maximum number of message blocks among all q queries, therefore the
 508 AXU and the AR advantage of the PolyHash function is $(\ell + \mu)/2^n$. Note that, ppHCTR
 509 requires two independent n -bit random permutations π_1 and π_2 , an n -bit random key K
 510 and an independent n -bit random hash key K_h for the PolyHash function. Security result
 511 of ppHCTR follows trivially from Theorem 3 and Theorem 4 which can be summarized
 512 as follows:

513 **Theorem 5.** *Let $\pi_1, \pi_2 \leftarrow_{\$} \text{Perm}(n)$ be two independent n -bit public random permutations
 514 and let $K \leftarrow_{\$} \{0, 1\}^n$ be an n -bit random key. Let $K_h \leftarrow_{\$} \{0, 1\}^n$ be an n -bit random hash
 515 key of PolyHash function as described in Eqn. (3). Then, for any $(q_e, q_d, q_{p_1} + q_{p_2}, \ell, \sigma)$ in-
 516 formation theoretic non-trivial adaptive CCA distinguisher D against the tSPRP security
 517 of ppHCTR[$\pi_1, \pi_2, K, \text{Poly}_{K_h}$], we have*

$$\text{Adv}_{\text{ppHCTR}}^{\text{tSPRP}}(D) \leq \frac{\sigma^2}{2^n} + \frac{2\sigma q_{p_2}}{2^n} + \frac{q^2 \ell}{2^n} + \frac{2q q_{p_1} \ell}{2^n} + \frac{\mu q^2}{2^n} + \frac{2\mu q q_p}{2^n} + \frac{q^2}{2^{n+1}} + \frac{q(q-1)}{2^{n+1}},$$

518 where $q = q_e + q_d$, ℓ is the maximum number of message blocks and μ is the number of
 519 tweak blocks.

520 7 ppHCTR+ : A Single-Keyed Variant of ppHCTR

521 In the last section, we have seen that ppHCTR, a public permutation based TES, requires
 522 two independent n -bit public random permutations and two independent n -bit keys. In

523 this section, we propose a single permutation and single keyed variant of ppHCTR, referred
 524 to as ppHCTR+. The construction is based on an n -bit public random permutation π
 525 and an n -bit random hash key of the PolyHash function as described in Eqn. (3). We
 526 consider that the tweak size is μ blocks long. The encryption and decryption algorithm
 of ppHCTR+ is shown in Fig. 7.1.

ppHCTR+.Enc $_{k_h}^\pi(T, M)$	ppHCTR+.Dec $_{k_h}^\pi(T, C)$
1. $(M_1 \ \dots \ M_l) \leftarrow \text{parse}_n(M)$;	1. $(C_1 \ \dots \ C_l) \leftarrow \text{parse}_n(C)$;
2. $\mathbf{M}_L \leftarrow M_1; \mathbf{M}_R \leftarrow (M_2 \ \dots \ M_l)$;	2. $\mathbf{C}_L \leftarrow C_1; \mathbf{C}_R \leftarrow (C_2 \ \dots \ C_l)$;
3. $U \leftarrow M_L \oplus \text{Poly}_{k_h}(\mathbf{M}_R \ T)$;	3. $V \leftarrow C_1 \oplus \text{Poly}_{k_h}(\mathbf{C}_R \ T)$;
4. $V \leftarrow \pi(U); Z \leftarrow U \oplus V$;	4. $U \leftarrow \pi^{-1}(V); Z \leftarrow U \oplus V$;
5. for $j = 1$ to $l - 1$	5. for $j = 1$ to $l - 1$
6. $Z_j \leftarrow Z \oplus j$;	6. $Z_j \leftarrow Z \oplus j$;
7. $S_j \leftarrow \pi(Z_j) \oplus Z_j$;	7. $S_j \leftarrow \pi(Z_j) \oplus Z_j$;
8. $\mathbf{S} \triangleq (S_1 \ \dots \ S_{l-1})$;	8. $\mathbf{S} \triangleq (S_1 \ \dots \ S_{l-1})$;
9. $\mathbf{C}_R \leftarrow \mathbf{M}_R \oplus \text{first}(\mathbf{M}_R , \mathbf{S})$;	9. $\mathbf{M}_R \leftarrow \mathbf{C}_R \oplus \text{first}(\mathbf{C}_R , \mathbf{S})$;
10. $C_L \leftarrow V \oplus \text{Poly}_{k_h}(\mathbf{C}_R \ T)$;	10. $M_L \leftarrow V \oplus \text{Poly}_{k_h}(\mathbf{M}_R \ T)$;
11. return $(C_L \ \mathbf{C}_R)$;	11. return $(M_L \ \mathbf{M}_R)$;

Fig. 7.1. ppHCTR+ based on an n -bit public random permutation π and an n -bit random hash key k_h . Left part is the encryption algorithm and right part is its decryption algorithm.

527 To see the dataflow of the encryption algorithm we consider an input message $M =$
 528 $(M_1 \| M_2)$, where $|M_1| = |M_2| = n$, i.e., M consists of two full blocks. Therefore, in step
 529 (2) of the algorithm, the variable \mathbf{M}_L is assigned to M_1 and \mathbf{M}_R is assigned to M_2 . In
 530 step (3) of the algorithm, we evaluate the poly hash Poly_{k_h} on $(M_2 \| T)$ which results to
 531 $M_2 \cdot k_h^3 \oplus T \cdot k_h^2 \oplus (|M_2| + |T|) \cdot k_h$ which is xored with the n -bit value M_1 to produce
 532 U . In step (4), we take the xor of U and $V = \pi(U)$ to produce Z . In step (6) and (7),
 533 we compute the key stream $\mathbf{S} = S_1$ where each $|S_1| = n$ by $S_1 = \pi(Z \oplus 1) \oplus (Z \oplus 1)$.
 534 Since, $|\mathbf{M}_R| = n$, \mathbf{C}_R will be $M_2 \oplus S_1$, which becomes the input along with tweak T
 535 to the poly hash function Poly_{k_h} . Evaluation of the poly hash on input $\mathbf{C}_R \| T$ results to
 536 $\mathbf{C}_R \cdot k_h^3 \oplus T \cdot k_h^2 \oplus (|\mathbf{C}_R| + |T|) \cdot k_h$. Then the result is xored with V to produce C_L , which
 537 is returned along with \mathbf{C}_R as the encryption of $M = M_1 \| M_2$. The decryption works in a
 538 similar way.
 539

540 7.1 Security Result of ppHCTR+

541 The security result of ppHCTR+ is as follows:

542 **Theorem 6.** Let $\pi \leftarrow_s \text{Perm}(n)$ be an n -bit public random permutation and let $K_h \leftarrow_s \{0, 1\}^n$
 543 be an n -bit random hash key of PolyHash function as described in Eqn. (3). Then, for any
 544 $(q_e, q_d, q_p, \ell, \sigma)$ information theoretic non-trivial adaptive CCA distinguisher D against the
 545 tSPRP security of $\text{ppHCTR}+[\pi, \text{Poly}_{K_h}]$, we have

$$\text{Adv}_{\text{ppHCTR}+}^{\text{tSPRP}}(D) \leq \frac{9\sigma^2}{2^n} + \frac{6\mu\sigma^2}{2^n} + \frac{4q_p\sigma(\mu+1)}{2^n} + \frac{q(q-1)}{2^{n+1}},$$

546 where σ is the total number of message blocks for all $q \triangleq q_e + q_d$ queries and μ is the
 547 number of tweak blocks.

548 8 Proof of Theorem 6

549 In section 6.4, we propose ppHCTR , which uses two independent random permutations
 550 and two independent random keys, which allowed us to use the generic security result of
 551 ppTES in order to derive the security result of ppHCTR . However, for the single keyed
 552 variant of it, we cannot use the generic result of ppTES due to the input / output
 553 dependency and that demands an independent security proof for $\text{ppHCTR}+$.

554 For the sake of simplicity, we refer $\text{ppHCTR}+[\pi, \text{Poly}_{K_h}]$ as $\text{ppHCTR}+$ when the underlying
 555 primitives are assumed to be understood. By Theorem 1, we have

$$\text{Adv}_{\text{ppHCTR}+}^{\text{tSPRP}}(D) \leq \text{Adv}_{\text{ppHCTR}+}^{\pm\text{rnd}}(D) + \frac{q(q-1)}{2^{n+1}}, \quad (26)$$

556 where recall that n is the minimum message length allowed for $\text{ppHCTR}+$. Therefore, we
 557 bound the $\pm\text{rnd}$ advantage of $\text{ppHCTR}+$. Let D be any information theoretic non-trivial
 558 adaptive deterministic CCA distinguisher with access to the oracles in either of the follow-
 559 ing two worlds: in the real world it interacts with $\mathcal{O}_{\text{re}} = (\text{ppHCTR}+. \text{Enc}_{K_h}^\pi, \text{ppHCTR}+. \text{Dec}_{K_h}^\pi,$
 560 $\pi^\pm)$ for an n -bit random hash key K_h and a random n -bit permutation π or in the ideal
 561 world it interacts with $\mathcal{O}_{\text{id}} = (\$, \$_1, \pi^\pm)$, where $\$$ and $\$_1$ are two independent random
 562 functions such that for any input, it responds with uniform values. Now, our goal is to
 563 upper bound the maximum advantage in distinguishing the real world from the ideal one.

564
 565 Let D be the maximum distinguishing advantage achieving distinguisher that makes q_e
 566 (resp. q_d) encryption (resp. decryption) queries and q_p primitive queries. After the in-
 567 teraction is over, the underlying hash key is revealed to D and finally, D outputs a bit.
 568 Let $\tau \triangleq \{(T^1, M^1, C^1), (T^2, M^2, C^2), \dots, (T^q, M^q, C^q)\}$ be the list of construction queries
 569 and responses and $\tau_p \triangleq \{(x_1, y_1), (x_2, y_2), \dots, (x_{q_p}, y_{q_p})\}$ be the list of primitive queries
 570 and responses where each T^i is exactly μ blocks long. The triplet $\tau' = (\tau, \tau_p, K_h)$ consti-
 571 tutes the query transcript of the attack. Now, we characterize the set of bad transcripts
 572 and good transcripts.

573 **8.1 Definition and Probability of Bad Transcripts**

574 In this section, we define bad transcripts and bound their probabilities in the ideal world.
 575 The defining criterion of the bad event is any non-trivial collision in the input or output
 576 of the permutation. As defined in Fig. 7.1, $\mathbf{M}_{\mathbf{R}}^i$ denotes $M_2^i \parallel \dots \parallel M_{l_i}^i$ and $\mathbf{C}_{\mathbf{R}}^i$ denotes
 577 $C_2^i \parallel \dots \parallel C_{l_i}^i$. Moreover, for a transcript τ' , we denote $U^i = \text{Poly}_{K_h}(\mathbf{M}_{\mathbf{R}}^i \parallel T^i) \oplus M_1^i$, $V^i =$
 578 $\text{Poly}_{K_h}(\mathbf{C}_{\mathbf{R}}^i \parallel T^i) \oplus C_1^i$ and $Z_{\alpha}^i = U^i \oplus V^i \oplus \langle \alpha \rangle$.

579 **Definition 4. (Bad Transcript for ppHCTR+)** : An attainable transcript $\tau' = (\tau, \tau_p, K_h)$
 580 is called a bad transcript for ppHCTR+ if any of the following conditions hold:

- 581 - B.1 : $\exists i \neq j \in [q]$ such that, $U^i = U^j$.
- 582 - B.2 : $\exists i, j \in [q]$ and $\alpha \in [l_j - 1]$ such that, $U^i = Z_{\alpha}^j$.
- 583 - B.3 : $\exists i, j \in [q]$, $\alpha \in [l_i - 1]$ and $\beta \in [l_j - 1]$ with $(i, \alpha) \neq (j, \beta)$ such that $Z_{\alpha}^i = Z_{\beta}^j$,
 584 where $(i, \alpha) \neq (j, \beta)$.
- 585 - B.4 : $\exists i \neq j \in [q]$ such that $V^i = V^j$.
- 586 - B.5 : $\exists i, j \in [q]$ and $\alpha \in [l_j - 1]$ such that $V^i = Z_{\alpha}^j \oplus M_{\alpha+1}^j \oplus C_{\alpha+1}^j$.
- 587 - B.6 : $\exists i, j \in [q]$, $\alpha \in [l_i - 1]$ and $\beta \in [l_j - 1]$ with $(i, \alpha) \neq (j, \beta)$ such that $Z_{\alpha}^i \oplus$
 588 $M_{\alpha+1}^i \oplus C_{\alpha+1}^i = Z_{\beta}^j \oplus M_{\beta+1}^j \oplus C_{\beta+1}^j$.
- 589 - B.7 : $\exists i \in [q]$ and $j \in [q_p]$ such that $U^i = x_j$.
- 590 - B.8 : $\exists i \in [q]$, $j \in [q_p]$ and $\alpha \in [l_i - 1]$ such that $Z_{\alpha}^i = x_j$.
- 591 - B.9 : $\exists i \in [q]$ and $j \in [q_p]$ such that $V^i = y_j$.
- 592 - B.10 : $\exists i \in [q]$, $j \in [q_p]$ and $\alpha \in [l_i - 1]$ such that $Z_{\alpha}^i \oplus M_{\alpha+1}^i \oplus C_{\alpha+1}^i = y_j$.

Lemma 6. Let \mathbf{T}_{id} be the random variable that takes the transcript resulting from the interaction between the distinguisher and the ideal world and \mathcal{V}_{b} be the set of all attainable bad transcripts for ppHCTR+. Then, by assuming $q \leq \sigma$, we have

$$\Pr[\mathbf{T}_{\text{id}} \in \mathcal{V}_{\text{b}}] \leq \epsilon_{\text{bad}} = \frac{9\sigma^2}{2^n} + \frac{6\mu\sigma^2}{2^n} + \frac{4q_p\sigma(\mu+1)}{2^n}.$$

593 **Proof.** By the union bound,

$$\Pr[\mathbf{T}_{\text{id}} \in \mathcal{V}_{\text{b}}] \leq \sum_{i=1}^{10} \Pr[\text{B.i}]. \quad (27)$$

594 In the following, we bound the probability of all the bad events individually. The lemma
 595 will follow by adding the individual bounds.

596 NOTATION. We consider that the tweak is μ blocks long, i.e., $\text{tw} = n\mu$. Therefore, for
 597 any $i \in [q]$, the maximum degree of $\text{Poly}_{k_h}(\mathbf{M}_{\mathbf{R}}^i \parallel T^i)$ is $\hat{l}_i + \mu$, where $\hat{l}_i \triangleq \lceil \frac{|\mathbf{M}_{\mathbf{R}}^i|}{n} \rceil$. Let $\hat{l}_{i,j}$
 598 denotes $\max\{\hat{l}_i, \hat{l}_j\} + \mu$ and $\hat{\sigma} = q\mu + (\hat{l}_1 + \dots + \hat{l}_q)$ denotes the total number of message

599 blocks of $\mathbf{M}_{\mathbf{R}}^i$ (including the tweak blocks) across all q queries. Therefore, $\sigma = (\hat{\sigma} - q\mu + q)$
 600 which implies that $\sigma - q = \hat{l}_1 + \dots + \hat{l}_q$. Since, $\hat{\ell}_{i,j} \leq \hat{l}_i + \hat{l}_j + \mu$, we have

$$\sum_{1 \leq i < j \leq q} \hat{\ell}_{i,j} \leq \binom{q}{2} \mu + \sum_{1 \leq i < j \leq q} (\hat{l}_i + \hat{l}_j) \leq (q-1)\hat{\sigma} \leq q\sigma + \mu q^2. \quad (28)$$

Bounding B.1. Bounding this event is equivalent to bounding

$$\text{Poly}_{K_h}(\mathbf{M}_{\mathbf{R}}^i \| T^i) \oplus \text{Poly}_{K_h}(\mathbf{M}_{\mathbf{R}}^j \| T^j) = M_1^i \oplus M_1^j.$$

601 If $\mathbf{M}_{\mathbf{R}}^i \| T^i = \mathbf{M}_{\mathbf{R}}^j \| T^j$ then the probability of this event is zero, otherwise it is bounded by
 602 the AXU advantage of the PolyHash and hence from Eqn. (28) and by assuming $q \leq \sigma$,
 603 we have

$$\Pr[\text{B.1}] \leq \sum_{1 \leq i < j \leq q} \frac{\hat{\ell}_{i,j}}{2^n} \leq \frac{q\sigma + \mu q^2}{2^n} \leq \frac{\sigma^2(\mu + 1)}{2^n}. \quad (29)$$

604 **Bounding B.2.** To bound the probability of B.2, we first fix the value of i, j and α .
 605 Note that $Z_\alpha^j = Z^j \oplus \langle \alpha \rangle$. Therefore, $U^i = Z_\alpha^j$ implies $U^i \oplus U^j \oplus V^j = \langle \alpha \rangle$. Now, this
 606 essentially implies the following hash equation:

$$\text{Poly}_{K_h}(\mathbf{M}_{\mathbf{R}}^i \| T^i) \oplus \text{Poly}_{K_h}(\mathbf{M}_{\mathbf{R}}^j \| T^j) \oplus \text{Poly}_{K_h}(\mathbf{C}_{\mathbf{R}}^j \| T^j) = M_1^i \oplus M_1^j \oplus C_1^j \oplus \langle \alpha \rangle. \quad (30)$$

607 Based on the values of i and j , we have the following two subcases:

- **Case A:** If $i \neq j$, then we first assume that $i < j$. Then, if the j -th query is an encryption query, then C_1^j is random and therefore by conditioning on the hash key and using the randomness of C_1^j , probability of Eqn. (30) can be bounded by 2^{-n} as C_1^j is uniformly distributed in the ideal world. Similarly, if the j -th query is a decryption query, then M_1^j is random and therefore by conditioning on the hash key and using the randomness of M_1^j , probability of Eqn. (30) can be bounded by 2^{-n} as M_1^j is uniformly distributed in the ideal world. Therefore, by varying over possible choices of i and (j, α) , we have

$$\Pr[\text{B.2}] \leq \frac{q\sigma}{2^n}.$$

On the other hand if $i > j$, then by conditioning all other random variables, we bound the probability of the event using the AXU advantage of the PolyHash function. Therefore, we have

$$\Pr[\text{B.2}] \leq \sum_{1 \leq i < j \leq q} \frac{\hat{\ell}_{i,j}}{2^n} \leq \frac{q\sigma + \mu q^2}{2^n}.$$

608 By considering the maximum of the above two, we have

$$\Pr[\text{B.2}] \leq \frac{q\sigma + \mu q^2}{2^n}. \quad (31)$$

609 - **Case B:** If $i = j$, then, Eqn. (30) boils down to the following hash equation:

$$\text{Poly}_{K_h}(\mathbf{C}_R^i \| T^i) = C_1^i \oplus \langle \alpha \rangle. \quad (32)$$

610 Note that for a fixed choice of i and α , Eqn. (32) can be bounded by the AR advantage
611 of the PolyHash function. Therefore,

$$\Pr[\text{B.2}] = \sum_{i=1}^q \sum_{\alpha=1}^{\hat{l}_i} \frac{\hat{l}_i + \mu}{2^n} = \frac{1}{2^n} \sum_{i=1}^q \hat{l}_i^2 + \frac{1}{2^n} \sum_{i=1}^q \hat{l}_i \mu \leq \frac{\sigma^2 + q^2}{2^n} + \frac{\mu\sigma}{2^n}. \quad (33)$$

612 By considering both the cases and by assuming $q \leq \sigma$, we have

$$\Pr[\text{B.2}] \leq \frac{\sigma^2 + q^2 + \mu\sigma}{2^n} + \frac{q\sigma + \mu q^2}{2^n} \leq \frac{3\sigma^2(\mu + 1)}{2^n}. \quad (34)$$

Bounding B.3. To bound the probability of B.3, we first fix the value of i, j, α and β such that $(i, \alpha) \neq (j, \beta)$. Note that $Z_\alpha^i = Z_\beta^j$ implies the following hash equation:

$$\text{Poly}_{K_h}(\mathbf{M}_R^i \| T^i) \oplus \text{Poly}_{K_h}(\mathbf{M}_R^j \| T^j) \oplus \text{Poly}_{K_h}(\mathbf{C}_R^i \| T^i) \oplus \text{Poly}_{K_h}(\mathbf{C}_R^j \| T^j) = W,$$

613 where $W = M_1^i \oplus M_1^j \oplus C_1^i \oplus C_1^j \oplus \langle \alpha \rangle \oplus \langle \beta \rangle$. Note that for $i = j$, the probability of
614 this event is zero. For $i \neq j$, without loss of generality we assume that $i < j$, if the
615 j -th query is an encryption query, then C_1^j is uniformly distributed in the ideal world
616 which is used to bound the probability of the event by conditioning the hash key and
617 all other random variables. Similarly, if the j -th query is a decryption query, then M_1^j
618 is uniformly distributed in the ideal world which is used to bound the probability of the
619 event by conditioning the hash key and all other random variables. Combining the above
620 two arguments with the assumption $q \leq \sigma$ and by varying over all possible choices of
621 indices, we have

$$\Pr[\text{B.3}] = \frac{\binom{\sigma-q}{2}}{2^n} \leq \frac{\sigma^2 + q^2}{2^{n+1}} \leq \frac{\sigma^2}{2^n}. \quad (35)$$

Bounding B.4. Bounding this event is equivalent to bounding

$$\text{Poly}_{K_h}(\mathbf{C}_R^i \| T^i) \oplus \text{Poly}_{K_h}(\mathbf{C}_R^j \| T^j) = C_1^i \oplus C_1^j.$$

622 If $\mathbf{C}_R^i \| T^i = \mathbf{C}_R^j \| T^j$ then the probability of this event is zero, otherwise it is bounded
623 by the AXU advantage of the PolyHash and hence from Eqn. (28) and by the assumption
624 $q \leq \sigma$, we have

$$\Pr[\text{B.4}] \leq \sum_{1 \leq i < j \leq q} \frac{\hat{\ell}_{i,j}}{2^n} \leq \frac{q\sigma + \mu q^2}{2^n} \leq \frac{\sigma^2(\mu + 1)}{2^n}. \quad (36)$$

625 **Bounding B.5.** We first fix the values of i, j and α and compute the probability of
626 $V^i = M_{\alpha+1}^j \oplus C_{\alpha+1}^j \oplus Z_\alpha^j$. This event boils down to computing the probability of the
627 following event: $\text{Poly}_{K_h}(\mathbf{C}_R^i \| T^i) \oplus \text{Poly}_{K_h}(\mathbf{M}_R^j \| T^j) \oplus \text{Poly}_{K_h}(\mathbf{C}_R^j \| T^j) = W$,
628 where $W = C_1^i \oplus M_{\alpha+1}^j \oplus C_{\alpha+1}^j \oplus M_1^j \oplus C_1^j \oplus \langle \alpha \rangle$. Now, we have two subcases as follows:

629 - **Case A:** if $i = j$, then we have $\text{Poly}_{K_h}(\mathbf{M}_{\mathbf{R}}^i \| T^i) = C_1^i \oplus M_{\alpha+1}^i \oplus C_{\alpha+1}^i \oplus M_1^i \oplus C_1^i \oplus$
 630 $\langle \alpha \rangle$, which can be bounded using the AR advantage of the PolyHash function after
 631 conditioning all other random variables. Therefore, by assuming $q \leq \sigma$, we have

$$\Pr[\text{B.5}] = \sum_{i=1}^q \sum_{\alpha=1}^{\hat{l}_i} \frac{\hat{l}_i + \mu}{2^n} = \frac{1}{2^n} \sum_{i=1}^q \hat{l}_i^2 + \frac{1}{2^n} \sum_{i=1}^q \hat{l}_i \mu \leq \frac{2\sigma^2}{2^n} + \frac{\mu\sigma}{2^n}. \quad (37)$$

632 - **Case B:** Now we consider the case when $i \neq j$ and without loss of generality we
 633 assume that $i < j$. Then by fixing the hash key K_h , the probability of the above
 634 event is the probability over the random draw of C_1^j (if j -th query is an encryption
 635 query) or M_1^j (if j -th query is a decryption query), which is at most 2^{-n} . Therefore,
 636 varying over all the possible choice of i, j and α and $q \leq \sigma$, we have

$$\Pr[\text{B.5}] \leq \frac{q\sigma}{2^n} \leq \frac{\sigma^2}{2^n}. \quad (38)$$

637 Taking the maximum of Eqn. (37) and (38), we have

$$\Pr[\text{B.5}] \leq \frac{2\sigma^2}{2^n} + \frac{\mu\sigma}{2^n}. \quad (39)$$

638 **Bounding B.6.** To bound this event we first fix i, j and α, β and then we compute the
 639 probability of $M_{\alpha+1}^i \oplus C_{\alpha+1}^i \oplus Z_{\alpha}^i = M_{\beta+1}^j \oplus C_{\beta+1}^j \oplus Z_{\beta}^j$. Now, we have the following
 640 subcases based on the values of i and j .

641 - **Case A:** If $i = j$, then the above event boils down to the following event $M_{\alpha+1}^i \oplus$
 642 $C_{\alpha+1}^i \oplus M_{\beta+1}^i \oplus C_{\beta+1}^i = \langle \alpha \rangle \oplus \langle \beta \rangle$. Since $\alpha \neq \beta$, without loss of generality we assume
 643 that $\alpha < \beta$. Therefore, using the randomness of C_{β}^i (if i -th query is encryption) or
 644 using the randomness of M_{β}^i (if i -th query is decryption), the probability of the event
 645 is bounded by 2^{-n} . By summing over all possible values of i, α and β , we have

$$\Pr[\text{B.6}] \leq \sum_{i=1}^q \frac{\binom{\hat{l}_i}{2}}{2^n} \leq \frac{1}{2^{n+1}} \left(\sum_{i=1}^q \hat{l}_i \right)^2 = \frac{(\sigma - q)^2}{2^{n+1}} \leq \frac{\sigma^2 + q^2}{2^{n+1}}. \quad (40)$$

646 - **Case B:** If $i \neq j$, then we bound the probability of the event similar to that of B.3,
 647 that is $1/2^n$ and therefore, by summing over all possible values of i, j, α and β , we
 648 have

$$\Pr[\text{B.6}] \leq \frac{\sigma^2 + q^2}{2^{n+1}}. \quad (41)$$

649 By taking the maximum of Eqn. (40) and (41) and by assuming $q \leq \sigma$, we have

$$\Pr[\text{B.6}] \leq \frac{\sigma^2 + q^2}{2^{n+1}} \leq \frac{\sigma^2}{2^n}. \quad (42)$$

650 **Bounding B.7.** Bounding this event is equivalent to bounding $\text{Poly}_{K_h}(\mathbf{M}_{\mathbf{R}}^i \| T^i) = M_1^i \oplus$
 651 x_j . This event is bounded by the AR advantage of the PolyHash and hence from Eqn. (28)
 652 and by assuming $q \leq \sigma$, we have

$$\Pr[\text{B.7}] \leq \sum_{i=1}^q \sum_{j=1}^{q_p} \frac{\hat{l}_i + \mu}{2^n} \leq \frac{(\sigma - q)q_p}{2^n} + \frac{\mu q q_p}{2^n} \leq \frac{q_p \sigma (\mu + 1)}{2^n}. \quad (43)$$

Bounding B.8. To bound the probability of B.8, we first fix the value of i, j and α . Note that $Z_\alpha^i = x_j$ implies the following hash equation: $\text{Poly}_{K_h}(\mathbf{M}_{\mathbf{R}}^i \| T^i) \oplus \text{Poly}_{K_h}(\mathbf{C}_{\mathbf{R}}^i \| T^i) = M_1^i \oplus C_1^i \oplus \langle \alpha \rangle \oplus x_j$. If the construction query comes after the primitive query then we can bound the probability of the event using the randomness of C_1^i (if the construction query is an encryption query) or using the randomness of M_1^i (if the construction query is a decryption query). Therefore, by conditioning the hash key and all other random variables, the bound will be 2^{-n} . Therefore, we have

$$\Pr[\text{B.8}] = \frac{(\sigma - q)q_p}{2^n} \leq \frac{\sigma q_p}{2^n}.$$

On the other hand, if the primitive query comes after the construction query, then we condition every other random variables and bound the probability of this event by using the AR advantage of the PolyHash function. Therefore, we have

$$\Pr[\text{B.8}] \leq \sum_{i=1}^q \sum_{j=1}^{q_p} \frac{\hat{l}_i + \mu}{2^n} \leq \frac{(\sigma - q)q_p}{2^n} + \frac{\mu q q_p}{2^n} \leq \frac{q_p (\sigma + q \mu)}{2^n}.$$

653 Therefore, by taking the maximum of the above two and by assuming $q \leq \sigma$, we have

$$\Pr[\text{B.8}] \leq \frac{q_p \sigma (\mu + 1)}{2^n}. \quad (44)$$

654 **Bounding B.9.** Bounding this event is equivalent to bounding $\text{Poly}_{K_h}(\mathbf{C}_{\mathbf{R}}^i \| T^i) = C_1^i \oplus y_j$.
 655 This event is bounded by the AR advantage of the PolyHash and hence from Eqn. (28)
 656 and by assuming $q \leq \sigma$, we have

$$\Pr[\text{B.9}] \leq \sum_{i=1}^q \sum_{j=1}^{q_p} \frac{\hat{l}_i + \mu}{2^n} \leq \frac{(\sigma - q)q_p}{2^n} + \frac{\mu q q_p}{2^n} \leq \frac{q_p \sigma (\mu + 1)}{2^n}. \quad (45)$$

657 **Bounding B.10.** To bound the probability of B.10, we first fix the value of i, j and
 658 α . Note that $M_{\alpha+1}^i \oplus C_{\alpha+1}^i \oplus Z_\alpha^i = y_j$ implies the hash equation: $\text{Poly}_{K_h}(\mathbf{M}_{\mathbf{R}}^i \| T^i) \oplus$
 659 $\text{Poly}_{K_h}(\mathbf{C}_{\mathbf{R}}^i \| T^i) = W$, where $W = M_{\alpha+1}^i \oplus C_{\alpha+1}^i \oplus M_1^i \oplus C_1^i \oplus \langle \alpha \rangle \oplus y_j$. Similar to B.8,
 660 we bound the event as

$$\Pr[\text{B.10}] \leq \frac{q_p \sigma (\mu + 1)}{2^n}. \quad (46)$$

The proof follows from Eqn. (27), Eqn. (29)-Eqn. (46) and $q \leq \sigma$. \square

661 **8.2 Analysis of Good Transcript**

662 In this section, we show that for a good transcript $\tau' = (\tau, \tau_p, k_h)$, realizing τ' is almost
 663 as likely in the real world as in the ideal world.

Lemma 7. *Let $\tau' = (\tau, \tau_p, k_h)$ be a good transcript. Then*

$$\frac{\Pr[\mathbf{T}_{\text{re}} = \tau']}{\Pr[\mathbf{T}_{\text{id}} = \tau']} \geq 1.$$

664 **Proof.** Since, in the ideal world, the encryption and the decryption oracle behaves per-
 665 fectly random, we have

$$\Pr[\mathbf{T}_{\text{id}} = \tau'] = \frac{1}{|\mathcal{K}_h|} \frac{1}{\mathbf{P}(2^n, q_p)} \frac{1}{2^{n\sigma}}, \quad (47)$$

666 where σ is the total number of message blocks queried among all q queries.

667 REAL INTERPOLATION PROBABILITY. Since τ' is a good transcript, all the inputs and
 668 outputs of π are fresh as we have eliminated all the internal input and output collisions
 669 of π , including the primitive queries while defining the bad events. Since there are total
 670 $\sigma + q_p$ invocation of π , including the primitive queries, therefore, the required probability
 671 is,

$$\Pr[\mathbf{T}_{\text{re}} = \tau'] = \frac{1}{|\mathcal{K}_h|} \frac{1}{\mathbf{P}(2^n, q_p)} \frac{1}{\mathbf{P}(2^n - q_p, \sigma)}. \quad (48)$$

By doing a simple algebraic calculation, it is easy to show that the ratio of Eqn. (48) to
 Eqn. (47) is at least 1. This proves Lemma 7. \square

By combining Lemma 6, Lemma 7, Theorem 2 and Eqn. (26), the result of Theorem 6
 follows. \square

672 DISCUSSION. We would like to note here that a simple birthday bound attack reveals
 673 the hash key of the Polyhash function for ppHCTR and ppHCTR+. This would allow an
 674 adversary to generate the ciphertext for any plaintext. The same attack also works for
 675 HCTR construction. A simple remedy of this problem is to introduce additional permu-
 676 tation calls after the hash evaluation in upper and bottom layers. This would resolve
 677 the problem of revealing the hash difference to any adversary, which in turn makes the
 678 recovery of the hash key difficult. A formal security analysis of this modified construction
 679 is beyond the scope of this paper.

680 **9 Conclusion**

681 **Permutation based cryptography is a promising new addition in the cryptographic liter-**
 682 **ature. There has been a continued effort in building cryptographic schemes using public**

683 permutations as the base primitive. Permutation based designs are generally lightweight.
 684 The overwhelming number of candidates using permutation based designs in the ongoing
 685 NIST competition of lightweight ciphers bears a proof of the fact that permutation based
 686 designs are preferred for computationally constrained scenarios.

687 There are permutation based designs available for various cryptographic schemes like
 688 authenticated encryption, authenticated encryption with associated data, message au-
 689 thentication codes, collision resistant hash etc., but to our knowledge there are no existing
 690 permutation based construction of tweakable enciphering schemes. Tweakable encipher-
 691 ing schemes are a class of encryption schemes which are length preserving and have thus
 692 found its use in low level disk encryption or encryption of any storage media which is
 693 organized as sectors. All the existing tweakable enciphering schemes are either build on
 694 top of block-ciphers, pseudorandom functions, or tweakable block ciphers [20, 38, 39, 51,
 695 11, 34, 16]. In this paper, we study the security of tweakable enciphering schemes built
 696 on a low level primitive like public random permutation. We initiate the study with a
 697 generic construction of a public permutation based TES, called ppTES. Then we con-
 698 struct ppCTR, a public permutation based length expanding PRF and finally, we propose
 699 a single keyed and single permutation based TES which we call ppHCTR+. To the best
 700 of our knowledge, this is the first provably secure public permutation based TES.

701 Our constructions, both ppTES and ppHCTR+ requires both the forward and inverse
 702 calls of the permutation. Most existing public random permutations are more efficient
 703 in their forward calls compared to the inverse calls, thus a inverse free construction
 704 like [16, 11] is worth studying. Another direction of future research would be to construct
 705 a permutation based TES which is beyond birthday bound secure.

706 References

- 707 1. <https://csrc.nist.gov/projects/hash-functions/sha-3-project>.
- 708 2. Mohammad Abbadi, M Bellare, R Canetti, H Krawczyk, M Bellare, P Rogaway, D Wagner, J Black,
 709 P Rogaway, D Boneh, et al. Deterministic authenticated-encryption: A provable-security treatment
 710 of the keywrap problem. *Journal of Applied Sciences*, 8(21):pp–1, 1996.
- 711 3. Zhenzhen Bao, Avik Chakraborti, Nilanjan Datta, Jian Guo, Mridul Nandi, Thomas Peyrin, and
 712 Kan Yasuda. Photon-beetle authenticated encryption and hash family. *NIST LWC*, 2019.
- 713 4. Daniel J. Bernstein, Stefan Kölbl, Stefan Lucks, Pedro Maat Costa Massolino, Florian Mendel, Kashif
 714 Nawaz, Tobias Schneider, Peter Schwabe, François-Xavier Standaert, Yosuke Todo, and Benoît Vigu-
 715 ier. Gimli : A cross-platform permutation. In Wieland Fischer and Naofumi Homma, editors, *Cryp-
 716 tographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei,
 717 Taiwan, September 25-28, 2017, Proceedings*, volume 10529 of *Lecture Notes in Computer Science*,
 718 pages 299–320. Springer, 2017.
- 719 5. Guido Bertoni, Joan Daemen, Seth Hoffert, Michaël Peeters, Gilles Van Assche, and Ronny Van Keer.
 720 Farfalle: parallel permutation-based cryptography. *IACR Trans. Symmetric Cryptol.*, 2017(4):1–38,
 721 2017.
- 722 6. Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Sponge-based pseudo-random
 723 number generators. In Stefan Mangard and François-Xavier Standaert, editors, *Cryptographic Hard-
 724 ware and Embedded Systems, CHES 2010, 12th International Workshop, Santa Barbara, CA, USA*,

- 725 *August 17-20, 2010. Proceedings*, volume 6225 of *Lecture Notes in Computer Science*, pages 33–47.
726 Springer, 2010.
- 727 7. Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Sponge functions. In *ECRYPT*
728 *hash workshop*, volume 2007. Citeseer, 2007.
- 729 8. Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Keccak. In *Annual interna-*
730 *tional conference on the theory and applications of cryptographic techniques*, pages 313–314. Springer,
731 2013.
- 732 9. Tim Beyne, Yu Long Chen, Christoph Dobraunig, and Bart Mennink. Elephant. *NIST LWC*, 2019.
- 733 10. Srimanta Bhattacharya and Mridul Nandi. Revisiting variable output length XOR pseudorandom
734 function. *IACR Cryptol. ePrint Arch.*, 2019:249, 2019.
- 735 11. Ritam Bhaumik and Mridul Nandi. An inverse-free single-keyed tweakable enciphering scheme.
736 In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st*
737 *International Conference on the Theory and Application of Cryptology and Information Security,*
738 *Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, volume 9453 of
739 *Lecture Notes in Computer Science*, pages 159–180. Springer, 2015.
- 740 12. Ritam Bhaumik and Mridul Nandi. An inverse-free single-keyed tweakable enciphering scheme. In
741 *International Conference on the Theory and Application of Cryptology and Information Security,*
742 pages 159–180. Springer, 2015.
- 743 13. Andrey Bogdanov, Miroslav Knezevic, Gregor Leander, Deniz Toz, Kerem Varici, and Ingrid Ver-
744 bauwhede. spongent: A lightweight hash function. In Bart Preneel and Tsuyoshi Takagi, editors,
745 *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara,*
746 *Japan, September 28 - October 1, 2011. Proceedings*, volume 6917 of *Lecture Notes in Computer*
747 *Science*, pages 312–325. Springer, 2011.
- 748 14. Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Francois-Xavier Standaert, John Steinberger,
749 and Elmar Tischhauser. Key-alternating ciphers in a provable setting: Encryption using a small
750 number of public permutations. In *Advances in Cryptology - EUROCRYPT 2012*, pages 45–62.
751 Springer, 2012.
- 752 15. Bishwajit Chakraborty and Mridul Nandi. Orange. *NIST LWC*, 2019.
- 753 16. Debrup Chakraborty, Sebati Ghosh, Cuauhtemoc Mancillas-López, and Palash Sarkar. FAST: disk
754 encryption and beyond. *IACR Cryptology ePrint Archive*, 2017:849, 2017.
- 755 17. Debrup Chakraborty, Vicente Hernandez-Jimenez, and Palash Sarkar. Another look at XCB. *Cryp-*
756 *tography and Communications*, 7(4):439–468, 2015.
- 757 18. Debrup Chakraborty, Cuauhtemoc Mancillas-López, and Palash Sarkar. STES: A stream cipher
758 based low cost scheme for securing stored data. *IACR Cryptology ePrint Archive*, 2013:347, 2013.
- 759 19. Debrup Chakraborty and Mridul Nandi. An improved security bound for HCTR. In *Fast Software*
760 *Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008,*
761 *Revised Selected Papers*, pages 289–302, 2008.
- 762 20. Debrup Chakraborty and Palash Sarkar. HCH: A New Tweakable Enciphering Scheme Using the
763 Hash-Counter-Hash Approach. *IEEE Transactions on Information Theory*, 54(4):1683–1699, 2008.
- 764 21. Donghoon Chang, Nilanjan Datta, Avijit Dutta, Bart Mennink, Mridul Nandi, Somitra Sanadhya,
765 and Ferdinand Sibleyras. Release of unverified plaintext: Tight unified model and application to
766 ANYDAE. *IACR Trans. Symmetric Cryptol.*, 2019(4):119–146, 2019.
- 767 22. Donghoon Chang and Mridul Nandi. A short proof of the PRP/PRF switching lemma. *IACR*
768 *Cryptol. ePrint Arch.*, 2008:78, 2008.
- 769 23. Shan Chen and John P. Steinberger. Tight security bounds for key-alternating ciphers. In *EURO-*
770 *CRYPT 2014. Proceedings*, pages 327–350, 2014.
- 771 24. Yu Long Chen, Eran Lambooj, and Bart Mennink. How to build pseudorandom functions from
772 public random permutations. In *Advances in Cryptology - CRYPTO 2019 - 39th Annual International*
773 *Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part I*, pages
774 266–293, 2019.

- 775 25. Benoit Cogliati and Yannick Seurin. On the provable security of the iterated even-mansour cipher
776 against related-key and chosen-key attacks. In *Annual International Conference on the Theory and*
777 *Applications of Cryptographic Techniques*, pages 584–613. Springer, 2015.
- 778 26. Joan Daemen, Seth Hoffert, Michaël Peeters, Gilles Van Assche, and Ronny Van Keer. Xoodyak, a
779 lightweight cryptographic scheme. *NIST LWC*, 2019.
- 780 27. Yuanxi Dai, Yannick Seurin, John Steinberger, and Aishwarya Thiruvengadam. Indifferentiability
781 of iterated even-mansour ciphers with non-idealized key-schedules: Five rounds are necessary and
782 sufficient. In *Annual International Cryptology Conference*, pages 524–555. Springer, 2017.
- 783 28. Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Goutam Paul. Double-block hash-then-sum: a
784 paradigm for constructing bbb secure prf. *IACR Transactions on Symmetric Cryptology*, pages
785 36–92, 2018.
- 786 29. Nilanjan Datta, Avijit Dutta, Mridul Nandi, Goutam Paul, and Liting Zhang. Single key variant of
787 pmac_plus. *IACR Transactions on Symmetric Cryptology*, pages 268–305, 2017.
- 788 30. Nilanjan Datta, Avijit Dutta, Mridul Nandi, and Kan Yasuda. Encrypt or decrypt? to make a single-
789 key beyond birthday secure nonce-based mac. In *Annual International Cryptology Conference*, pages
790 631–661. Springer, 2018.
- 791 31. Itai Dinur, Orr Dunkelman, Nathan Keller, and Adi Shamir. Key recovery attacks on iterated
792 even-mansour encryption schemes. *Journal of Cryptology*, 29(4):697–728, 2016.
- 793 32. Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schl affer. Ascon v1.2. *NIST*
794 *LWC*, 2019.
- 795 33. Avijit Dutta. Minimizing the two-round tweakable even-mansour cipher. In Shiho Moriai and Huax-
796 iong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference*
797 *on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, De-*
798 *cember 7-11, 2020, Proceedings, Part I*, volume 12491 of *Lecture Notes in Computer Science*, pages
799 601–629. Springer, 2020.
- 800 34. Avijit Dutta and Mridul Nandi. Tweakable HCTR: A BBB secure tweakable enciphering scheme.
801 In *Progress in Cryptology - INDOCRYPT 2018 - 19th International Conference on Cryptology in*
802 *India, New Delhi, India, December 9-12, 2018, Proceedings*, pages 47–69, 2018.
- 803 35. Avijit Dutta, Mridul Nandi, and Suprita Talnikar. Beyond birthday bound secure mac in faulty
804 nonce model. In *Annual International Conference on the Theory and Applications of Cryptographic*
805 *Techniques*, pages 437–466. Springer, 2019.
- 806 36. Shimon Even and Yishay Mansour. A construction of a cipher from a single pseudorandom permu-
807 tation. *J. Cryptology*, 10(3):151–162, 1997.
- 808 37. Shai Halevi. EME*: Extending EME to handle arbitrary-length messages with associated data.
- 809 38. Shai Halevi and Phillip Rogaway. A Tweakable Enciphering Mode. In Dan Boneh, editor, *CRYPTO*,
810 volume 2729 of *Lecture Notes in Computer Science*, pages 482–499. Springer, 2003.
- 811 39. Shai Halevi and Phillip Rogaway. A Parallelizable Enciphering Mode. In Tatsuaki Okamoto, editor,
812 *CT-RSA*, volume 2964 of *Lecture Notes in Computer Science*, pages 292–304. Springer, 2004.
- 813 40. Viet Tung Hoang, Ted Krovetz, and Phillip Rogaway. Robust authenticated-encryption AEZ and
814 the problem that it solves. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology*
815 *- EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of*
816 *Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, volume 9056 of
817 *Lecture Notes in Computer Science*, pages 15–44. Springer, 2015.
- 818 41. Manish Kumar. Security of XCB and HCTR. In *M.Tech.(Computer Science) Thesis*. Indian Statis-
819 tical Institute, Kolkata, 2018.
- 820 42. Moses Liskov, Ronald L Rivest, and David Wagner. Tweakable block ciphers. In *Annual International*
821 *Cryptology Conference*, pages 31–46. Springer, 2002.
- 822 43. Moses Liskov, Ronald L. Rivest, and David A. Wagner. Tweakable block ciphers. *J. Cryptology*,
823 24(3):588–613, 2011.

- 824 44. David A. McGrew and Scott R. Fluhrer. The Security of the Extended Codebook (XCB) Mode
825 of Operation. In Carlisle M. Adams, Ali Miri, and Michael J. Wiener, editors, *Selected Areas in*
826 *Cryptography*, volume 4876 of *Lecture Notes in Computer Science*, pages 311–327. Springer, 2007.
- 827 45. Bart Mennink, Reza Reyhanitabar, and Damian Vizár. Security of full-state keyed sponge and
828 duplex: Applications to authenticated encryption. In *International Conference on the Theory and*
829 *Application of Cryptology and Information Security*, pages 465–489. Springer, 2015.
- 830 46. Kazuhiko Minematsu. Beyond-birthday-bound security based on tweakable block cipher. In *Inter-*
831 *national Workshop on Fast Software Encryption*, pages 308–326. Springer, 2009.
- 832 47. NIST. Online: <https://csrc.nist.gov/projects/lightweight-cryptography>.
- 833 48. Jacques Patarin. The “Coefficients H” Technique. In *Selected Areas in Cryptography, SAC*, pages
834 328–345, 2008.
- 835 49. Phillip Rogaway, Mihir Bellare, and John Black. Sha-3 standard. *ACM Transactions on Information*
836 *and System Security (TISSEC)*, 6(3):365–403, 2003.
- 837 50. Palash Sarkar. Tweakable enciphering schemes from stream ciphers with IV. *IACR Cryptol. ePrint*
838 *Arch.*, 2009:321, 2009.
- 839 51. Peng Wang, Dengguo Feng, and Wenling Wu. HCTR: A variable-input-length enciphering mode.
840 In *Information Security and Cryptology, First SKLOIS Conference, CISC 2005, Beijing, China,*
841 *December 15-17, 2005, Proceedings*, pages 175–188, 2005.
- 842 52. Mark N Wegman and J Lawrence Carter. New classes and applications of hash functions. In *20th*
843 *Annual Symposium on Foundations of Computer Science (sfcs 1979)*, pages 175–182. IEEE, 1979.