Encryption Schemes based on a Single Permutation: PCBC, POFB, PCFB and PCTR

Kaiyan Zheng[1,2,3] and Peng Wang[1,2,3]
[1]*Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*
[2]*Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing 100093, China*
[3]*School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China*

Keywords: Encryption Scheme, Blockwise Adaptive Attack, Related-key Attack, Even-Mansour.

Abstract: In this paper we discuss how to construct encryption schemes from permutations. Firstly we discuss an intuitive way to design permutation-based encryption schemes, that is by combining mainstream blockcipher-based encryption modes (such as CBC, OFB, CFB, CTR) with the Even-Mansour cipher, which is an elegant permutation-based blockcipher. Unfortunately, most of encryption schemes produced by the combination strategy are not secure enough. Then we propose 4 permutation-based encryption schemes - PCBC, POFB, PCFB and PCTR, which can resist both the blockwise adaptive attack and the $\Phi^{\oplus}$-related-key attack when using a non-repeated nonce. To illustrate it, we give a definition of the indistinguishability from random bits against blockwise adaptive chosen plaintext attack in the $\Phi^{\oplus}$-related-key setting, and then prove the security of PCBC in such definition. The other 3 schemes have similar results. Constructing from a single permutation, these 4 encryption schemes are practical, in the sense that they are less prone to misuse, bring less pressure on the key-management in real world, and apply to blockwise adaptive scenarios including real-time applications, on-line settings, memory-restricted devices, etc. Moreover they are more efficient than the Sponge construction.

1 INTRODUCTION

The winner of SHA-3 competition, a permutation-based hash function, inspires a great many studies on cryptographic permutations and permutation-based cryptographic schemes. Lots of cryptographic permutations were designed, including KECCAK (Dworkin, 2015), Prϕst (Kavun et al., 2014), PRIMATEs (Andreeva et al., 2014), Minalpher-P (Sasaki et al., 2014) - just to name a few. Numerous cryptographic schemes are designed to be based on cryptographic permutations, especially a large number of *authenticated encryption* schemes submitted to the CAESAR competition, including Ascon (Dobraunig et al., 2014), PAEQ (Biryukov and Khovratovich, 2014), KETJE (Bertoni et al., 2014), APE (Sasaki et al., 2014), OTR (Kavun et al., 2014), and so on. More other permutation-based cryptographic schemes are studied, including lightweight hash functions like SPONGENT (Bogdanov et al., 2011) and Quark (Aumasson et al., 2013), streamciphers like Salsa (Bernstein, 2008), tweakable blockciphers like XPX (Mennink, 2016) and TEM (Cogliati and Seurin, 2015), blockciphers like Even-Mansour (Even and Mansour, 1997), etc. However there are little solo studies on permutation-based encryption schemes, which motivates us to discuss how to construct encryption schemes from a single cryptographic permutation.

1.1 Background

Encryption scheme. Encryption schemes are designed to provide data confidentiality, and common encryption modes of operation are based on blockcipher, including CBC (Cipher Block Chaining), OFB (Output Feedback), CFB (Cipher Feedback) and CTR (Counter), etc. When using a random IV (Initialization Vector), these 4 modes are proved to be secure in the single-key chosen plaintext attack (CPA for short) setting (Bellare et al., 1997; Alkassar et al., 2001; Sung et al., 2001).

Unfortunately, it is a great challenge to implement random IVs in real world, and once the IV is predictable, these encryption modes, excluding CTR, are no longer secure (Duong and Rizzo, 2011; Bard, 2004; Dai, 2002; Moeller et al., 2004; Rogaway, 1996). In (Rogaway, 2004), Rogaway discussed the case when the IV is guaranteed to be a *nonce* which

Zheng, K. and Wang, P.
Encryption Schemes based on a Single Permutation: PCBC, POFB, PCFB and PCTR.
DOI: 10.5220/0006713804520460
In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, pages 452-460
ISBN: 978-989-758-282-0

takes fresh values in each encryption and even can be chosen by the adversary. Rogaway believed that nonce-based symmetric encryptions are less prone to misuse.

Blockwise adaptive attack. In some practical application environments like real-time applications, online settings, memory-restricted devices, etc., the data is processed and outputted block by block, rather than as an atomic object, arising the *blockwise adaptive attack* (Bellare et al., 2002; Fouque et al., 2003; Fouque et al., 2004; Joux et al., 2002; Bard, 2006; Bard, 2007), which assumes that the adversary can adaptively choose subsequent input blocks based on the preceding output blocks. The blockwise adaptive attack is not only of theoretical interest, owing to its operational feasibility in the Secure Shell (SSH) (Bellare et al., 2002) and the Secure Sockets Layer (SSL) (Bard, 2006).

Some encryption schemes that are secure against the traditional chosen plaintext attack turn out to suffer the blockwise adaptive attack, like CBC, while some still maintain the confidentiality against such stronger attack, like OFB, CFB and CTR using a random IV (Fouque et al., 2003; Fouque et al., 2004).

Related-key attack. The related-key attack has studied extensively for various cryptographic applications (Biham, 1993; Biryukov et al., 2009; Karpman, 2015; Bellare and Kohno, 2003; Biryukov and Khovratovich, 2009; Albrecht et al., 2011), which assumes that the adversary has the capability to query not only the scheme with the secret key K but also $\varphi(K)$ where φ is a *key-deriving-function* that can be chosen. Though this stronger attack is not far-fetched in practical scenarios, it is not covered by the classic security notions, and we have to take it into consideration when analyzing encryption schemes (no matter already designed or new).

Even-Mansour cipher. The Even-Mansour cipher (Even and Mansour, 1997), designed from a single permutation by eXclusive-ORing(XOR) two independent keys into its input and output respectively, attracts a great interest due to its elegant structure, and lots of related studies were published (Daemen, 1991; Chen and Steinberger, 2014; Dunkelman et al., 2012; Dobraunig et al., 2015). It can be simplified to the single-key version by using the same key in both the input and output (Dunkelman et al., 2012; Chen and Steinberger, 2014).

Assuming the underlying permutation be a random one that the adversary can query, both versions, though are proven to be PRP-CPA in the single-key model (Dunkelman et al., 2012; Even and Mansour, 1997; Chen and Steinberger, 2014), suffer the *related-key attack* (Dobraunig et al., 2015), which makes the Even-Mansour construction fail to be a well-suited blockcipher for many modes of operation, such as OTR (Dobraunig et al., 2015).

1.2 Motivation

How can we provide confidential protection when there is only a cryptographic permutation in hand? The notable Sponge construction designed in SHA-3 (Dworkin, 2015) is a convenient approach. However in contrast to mainstream encryption schemes designed from blockcipher, which in every call, process the message that is as large as the blocksize of the underlying blockcipher, the Sponge construction can't achieve the optimal efficiency, as the message it processes during each call of the underlying primitive is far less than the bandwidth (part of which interacts with the outer while the remaining is reserved to guarantee secure).

Another direct way to get permutation-based encryption schemes that achieve the optimal efficiency is to combine mainstream confidential modes (like CBC, OFB, CFB, CTR, etc) with the Even-Mansour construction. Nevertheless these specific schemes are *not* secure enough. When using a non-repeated nonce, most of these schemes suffer the blockwise adaptive attack, and then fail to provide confidentiality in lots of practical scenarios like real-time application, online settings, memory-restricted devices, etc. Due to the inability in the Even-Mansour construction to resist related-key attacks, these schemes are prone to suffer related-key attacks (Dobraunig et al., 2015; Karpman, 2015). In addition, once large permutations are used, the keys used in these schemes are also large (no smaller than the bandwidth of the permutations), which brings a great pressure on the key-management in real world.

Based on the above observations, we study how to design practical encryption schemes from a single cryptographic permutation. We aim at proposing nonce-respected efficient encryption schemes that, when using a key with an appropriate length, can resist both the blockwise adaptive attack and the related-key attack.

By the way, though (online) authenticated encryption schemes can meet these requirements easily, there are lots of applications where unauthenticated encryption is needed. For example, a certain proportion of errors in the recovered plaintext may be acceptable in the digitised voice or video service. Without regard to the integrity, encryption schemes are

capable to run sufficiently fast to reduce latency time, which are vital in real-time applications and on-line settings.

1.3 Our Contribution

Firstly in Section 3, we analyze 4 specific permutation-based encryption schemes, i.e. SEM-CBC, SEM-OFB, SEM-CFB and SEM-CTR, produced by combining 4 commonly-used encryption modes, i.e. CBC, OFB, CFB and CTR, with the single-key Even-Mansour cipher (SEM for short). With a random IV, these 4 schemes can provide some confidential protection, but most fail when using a non-repeated nonce, not to mention the inability to resist the blockwise adaptive attack, which restricts their usage in practical on-line/real-time scenarios. The results are concluded in Table 1. It's obvious that the direct combination strategy may fail to construct practical permutation-based encryption schemes.

In Section 4 we propose 4 permutation-based encryption schemes - PCBC, POFB, PCFB and PCTR, improved from SEM-CBC, SEM-OFB, SEM-CFB and SEM-CTR respectively. Based on a single ideal permutation, all these 4 schemes can provide confidential protection against the blockwise adaptive chosen plaintext attack in the $\Phi^{\oplus}$-related-key setting, even when using a non-repeated nonce. We give a detail proof of PCBC, and the other 3 schemes can be proved similarly. We claim that these 4 encryption schemes are very practical, because they are less prone to misuse, apply to practical blockwise adaptive scenarios, and bring less pressure on the key-management in real world. Besides, they are more efficient than the Sponge construction since the plaintext block they process during each call of the underlying permutation is as large as the bandwidth.

2 PRELIMINARIES AND SECURITY MODELS

Notations. By $\{0,1\}^n$ we denote the set of n binary bits for any $n > 0$, and $\{0,1\}^{n+} = \bigcup_{l=1}^{\infty}\{0,1\}^{nl}$. Let S be some finite set, $s \xleftarrow{\mathbb{R}} S$ denotes selecting an element at uniformly random from S and assign it to s. $|S|$ is the cardinality of S while $|s|$ is the length of s. $\|$ denotes the string concatenation operation. $Perm(n)$ denotes the set of all permutations on $\{0,1\}^n$, and $Func(n_1,n_2)$ denotes the set of all functions mapping $\{0,1\}^{n_1}$ to $\{0,1\}^{n_2}$.

Encryption Scheme. Let $\mathcal{SE} : \{0,1\}^k \times \{0,1\}^n \times \{0,1\}^{n+} \to \{0,1\}^{n+}$ be any encryption scheme, where $\{0,1\}^k, \{0,1\}^n, \{0,1\}^{n+}$ denote the space of keys, IVs and plaintexts/ciphertexts, respectively. For any $K \in \{0,1\}^k$, $\mathcal{SE}_K$ denotes the encryption function and $\mathcal{SE}_K^{-1}$ denotes its inverse, which satisfies that for any $IV \in \{0,1\}^n, M \in \{0,1\}^{n+}$, $M = \mathcal{SE}_K^{-1}(IV, \mathcal{SE}_K(IV,M))$.

Here IV denotes either a random one or a non-repeated nonce. In the former case, i.e. $IV \xleftarrow{\mathbb{R}} \{0,1\}^n$, IV acts as part of the ciphertext, while in the latter IV is assumed to be controlled by the adversary. In the remaining, we misuse the notation $\mathcal{SE}_K$ to denote the encryption oracle of $\mathcal{SE}$, which takes in a single input M when using a random IV, but a pair input (N,M) when using a non-repeated nonce. We won't emphasize it unless it causes any confusion.

Besides, we assume that the message which $\mathcal{SE}$ processes is already padded as need, i.e. a non-zero multiple of n, since the discussion of padding rules is out of the scope of our paper. Most of encryption schemes provide the CPA confidentiality only, and thus we focus on the CPA setting in this paper.

To define the confidentiality of $\mathcal{SE}$, we use *the indistinguishability from random bits* in the remaining. Denote $\$$ the function which can produce sufficient random bits on demand. Since $\mathcal{SE}$ discussed in our paper is based on permutations, we assume that the underlying ideal permutation is $\mathcal{P} \xleftarrow{\mathbb{R}} Perm(n)$ and the adversary has access to $\mathcal{P}^{\pm}$.

The CPA setting. In the single-key model, we assume that $K \xleftarrow{\mathbb{R}} \{0,1\}^k$, and the CPA oracle is either $\mathcal{SE}_K$ or $\$$. Let $\mathcal{D}$ be any CPA adversary that makes at most q non-duplicate encryption queries and at most r non-duplicate bi-directional queries to $\mathcal{P}^{\pm}$.

Thus the CPA indistinguishability (*IND-CPA* for short) of $\mathcal{SE}$ is defined by the maximum advantage at distinguishing $\{\mathcal{SE}_K, \mathcal{P}^{\pm}\}$ with $\{\$, \mathcal{P}^{\pm}\}$, that is, for $q,r \geq 0$,

$$\mathbf{Adv}_{\mathcal{SE}}^{ind-cpa}(q,r) = \max_{\mathcal{D}} \left\{ \begin{array}{r} \Pr\left[K \xleftarrow{\mathbb{R}} \{0,1\}^k : \mathcal{D}^{\mathcal{SE}_K, \mathcal{P}^{\pm}} = 1\right] \\ -\Pr\left[\mathcal{D}^{\$, \mathcal{P}^{\pm}} = 1\right] \end{array} \right\}. \quad (1)$$

Related-key setting. The indistinguishability definition in *the related-key model* used in our paper follows the theoretical framework of Bellare and Kohno (Bellare and Kohno, 2003) and Albrecht et al. (Albrecht et al., 2011). In the related-key setting, the CPA adversary has access to not only the encryption oracle $\mathcal{SE}_K$ but also $\mathcal{SE}_{\varphi(K)}$ where φ is a *key-deriving-function* chosen from a pre-described set Φ where $\Phi \subseteq Func(k,k)$.

Table 1: The security conclusion of encryption schemes appeared in this paper.

Encryption Schemes	IV Assumption	Security Definitions			
		IND-CPA	IND-BW-CPA	$\Phi^{\oplus}$-IND-CPA	$\Phi^{\oplus}$-IND-BW-CPA
SEM-CBC	random	√	×	√	×
	nonce	×	×	×	×
SEM-OFB	random	√	√	√	√
	nonce	×	×	×	×
SEM-CFB	random	√	√	√	√
	nonce	×	×	×	×
SEM-CTR	random	√	√	√	√
	nonce	√	√	×	×
PCBC	random or nonce	√	√	√	√
POFB		√	√	√	√
PCFB		√	√	√	√
PCTR		√	√	√	√

In this paper, we target the $\Phi^{\oplus}$-related-key security only, where $\Phi^{\oplus} = \{\varphi_\Delta \mid \Delta \in \{0,1\}^k\}$ and φ_Δ denotes the canonical function $K \mapsto K \oplus \Delta$. We will misuse Δ, φ_Δ in the remaining unless it is confused.

For any $\mathcal{SE}$, we define a *$\Phi^{\oplus}$-related-key oracle* $\mathrm{RK}[\mathcal{SE}] : \{0,1\}^k \times \Phi^{\oplus} \times \{0,1\}^n \times \{0,1\}^{n+} \to \{0,1\}^{n+}$. For any $\Delta \in \Phi^{\oplus}$, $\mathrm{RK}[\mathcal{SE}]_K$ computes as $\mathcal{SE}_{K\oplus\Delta}$. Similarly, we define a $\Phi^{\oplus}$-related-key oracle of $\$$ as $\mathrm{RK}[\$]$, which denotes the set of $|\Phi^{\oplus}|$ independent functions that produce random bits.

Let $\mathcal{D}$ be any $\Phi^{\oplus}$-related-key CPA adversary that makes at most q non-duplicate queries to the $\Phi^{\oplus}$-related-key oracle and at most r bi-directional non-duplicate queries to $\mathcal{P}^{\pm}$. Thus the $\Phi^{\oplus}$-related-key CPA indistinguishability ($\Phi^{\oplus}$-*IND-CPA* for short) of $\mathcal{SE}$ is defined by the maximum advantage at distinguishing $\{\mathrm{RK}[\mathcal{SE}]_K, \mathcal{P}^{\pm}\}$ with $\{\mathrm{RK}[\$], \mathcal{P}^{\pm}\}$, that is, for $q, r > 0$,

$$\mathbf{Adv}^{\Phi^{\oplus}-ind-cpa}_{\mathcal{SE}}(q,r) = \max_{\mathcal{D}} \left\{ \begin{array}{r} \Pr\left[K \xleftarrow{\mathbb{R}} \{0,1\}^k : \mathcal{D}^{\mathrm{RK}[\mathcal{SE}]_K, \mathcal{P}^{\pm}} = 1\right] \\ -\Pr\left[\mathcal{D}^{\mathrm{RK}[\$], \mathcal{P}^{\pm}} = 1\right] \end{array} \right\}. \quad (2)$$

Blockwise adaptive setting. The adversary in the blockwise adaptive setting has the capability to observe the output blocks that are already computed, before deciding subsequent input blocks, and insert any blocks as it likes based on those observations, during a single query.

Without loss of generality, let the adversary in the blockwise adaptive chosen plaintext attack (*BW-CPA* for short) query block-by-block. Take the CPA encryption oracle $\mathcal{SE}_K$ as an example, we describe briefly how the CPA adversary interacts with its oracle in the blockwise adaptive setting, and other oracles perform similarly.

Let $\overline{\mathcal{SE}}$ be the blockwise adaptive oracle of $\mathcal{SE}$, and during any i^{th} encryption query, after knowing the corresponding ciphertext blocks by querying $\overline{\mathcal{SE}}_K(M_0^i), \overline{\mathcal{SE}}_K(M_1^i), \cdots, \overline{\mathcal{SE}}_K(M_{j-1}^i)$, the BW-CPA adversary chooses the j^{th} block M_j^i and queries $\overline{\mathcal{SE}}_K(M_j^i)$, where M_0^i denotes the IV, i.e. $M_0^i = IV^i$, and M^i is the i^{th} queried plaintext that $M^i = M_1^i \cdots M_{l_i}^i$ and $j = 1, \cdots, l_i$. Note that the computation of $\overline{\mathcal{SE}}_K(M_0^i)$ may be different from that of $\overline{\mathcal{SE}}_K(M_j^i)$, according to the specific $\mathcal{SE}$ scheme.

Moreover, denote the blockwise adaptive oracle of $\$$ as $\overline{\$}$, and $\overline{\$}(M_j^i)$ will return a random bit string that has the same length of $\overline{\mathcal{SE}}_K(M_j^i)$. Similarly, define $\mathrm{RK}[\overline{\mathcal{SE}}]_K$, $\mathrm{RK}[\overline{\$}]$ as the blockwise adaptive oracle of $\mathrm{RK}[\mathcal{SE}]_K$, $\mathrm{RK}[\$]$, respectively. Let $\mathcal{D}$ be some BW-CPA adversary who makes at most q encryption queries to the blockwise adaptive oracle, and at most r bi-directional queries to the public oracle $\mathcal{P}^{\pm}$.

IND-BW-CPA. The BW-CPA indistinguishability (*IND-BW-CPA* for short) of $\mathcal{SE}$ is defined by the maximum advantage at distinguishing $\left\{\overline{\mathcal{SE}}_K, \mathcal{P}^{\pm}\right\}$ from $\left\{\overline{\$}, \mathcal{P}^{\pm}\right\}$, that is, for $q, r > 0$,

$$\mathbf{Adv}^{ind-bw-cpa}_{\mathcal{SE}}(q,r) = \max_{\mathcal{D}} \left\{ \begin{array}{r} \Pr\left[K \xleftarrow{\mathbb{R}} \{0,1\}^k : \mathcal{D}^{\overline{\mathcal{SE}}_K, \mathcal{P}^{\pm}} = 1\right] \\ -\Pr\left[\mathcal{D}^{\overline{\$}, \mathcal{P}^{\pm}} = 1\right] \end{array} \right\}. \quad (3)$$

$\Phi^{\oplus}$-IND-BW-CPA. The $\Phi^{\oplus}$-related-key BW-CPA indistinguishability ($\Phi^{\oplus}$-*IND-BW-CPA* for short) of $\mathcal{SE}$ is defined by the maximum advantage at distinguishing $\left\{\mathrm{RK}[\overline{\mathcal{SE}}]_K, \mathcal{P}^{\pm}\right\}$ from $\left\{\mathrm{RK}[\overline{\$}], \mathcal{P}^{\pm}\right\}$, that is, for $q, r > 0$,

$$\mathbf{Adv}^{\Phi^{\oplus}-ind-bw-cpa}_{\mathcal{SE}}(q,r) = \max_{\mathcal{D}} \left\{ \begin{array}{r} \Pr\left[K \xleftarrow{\mathbb{R}} \{0,1\}^k : \mathcal{D}^{\mathrm{RK}[\overline{\mathcal{SE}}]_K, \mathcal{P}^{\pm}} = 1\right] \\ -\Pr\left[\mathcal{D}^{\mathrm{RK}[\overline{\$}], \mathcal{P}^{\pm}} = 1\right] \end{array} \right\}. \quad (4)$$

3 THE COMBINATION STRATEGY

In this section, we discuss 4 specific permutation-based encryption schemes - SEM-CBC, SEM-OFB, SEM-CFB and SEM-CTR - produced by combining 4 commonly-used encryption modes, i.e. CBC, OFB, CFB and CTR, with SEM. Due to the chain structure of the modes (except CTR), nearly half of the key-$\oplus$-operations are cancelled and these schemes turn out to be very compact, showed in Fig.1 - Fig.4.

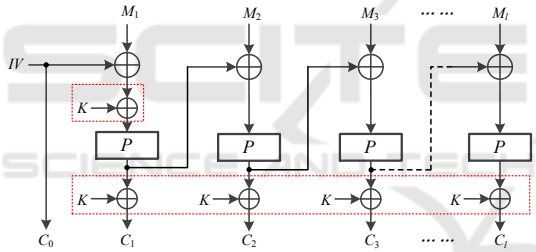

Figure 1: SEM-CBC.

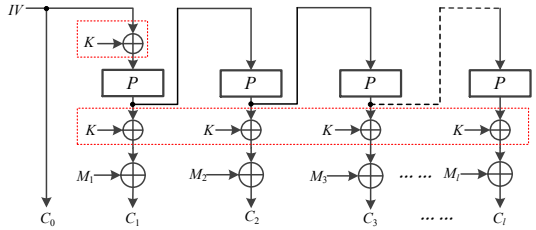

Figure 2: SEM-OFB.

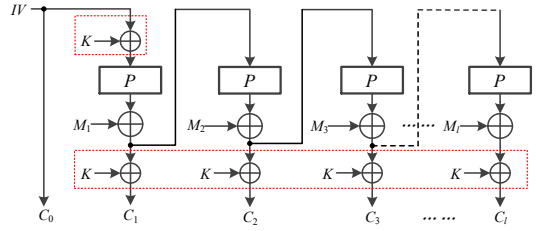

Figure 3: SEM-CFB.

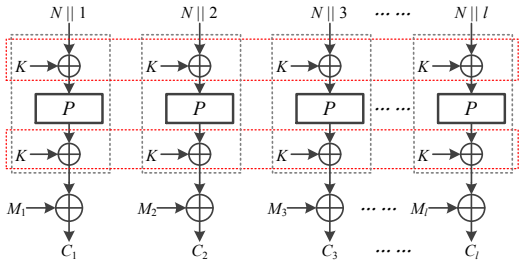

Figure 4: SEM-CTR.

The analyses of these 4 schemes are deduced from CBC, OFB, CFB and CTR directly (Bellare et al., 1997; Sung et al., 2001; Alkassar et al., 2001; Joux et al., 2002; Moeller et al., 2004; Bard, 2006; Bard, 2007), as all these 4 schemes are actually the specific cases when the underlying blockcipher is exactly the SEM blockcipher. We omit the details since the analyses are quite trivial, and the results are concluded in Table 1.

4 PERMUTATION-BASED ENCRYPTION SCHEMES: PCBC, POFB, PCFB AND PCTR

With a single cryptographic permutation in hand, how can we provide confidential protection? From above, we know that both direct ways -the Sponge construction and the combination strategy- have some deficiencies.

In this section we, inspired by the common blockcipher-based modes of operation i.e. CBC, OFB, CFB and CTR, propose 4 permutation-based encryption schemes -PCBC, POFB, PCFB and PCTR, showed in Fig.5-Fig.8. Note that in PCBC, the finite multiplication by 2 (see the red dashed in Fig. 5) in each block process is essential to resist the blockwise adaptive attack, which is unnecessary in the other 3 schemes (see the red dashed in Fig. 6-8) since the original OFB, CFB, and CTR can resist the blockwise adaptive attack, when using a random IV.

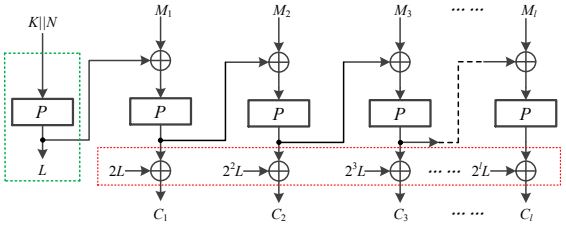

Figure 5: PCBC.

Based on a single cryptographic permutation and two simple kinds of operations - XOR and the finite

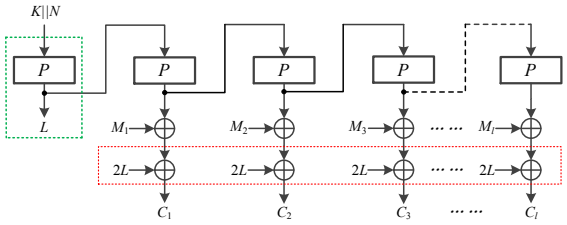

Figure 6: POFB.

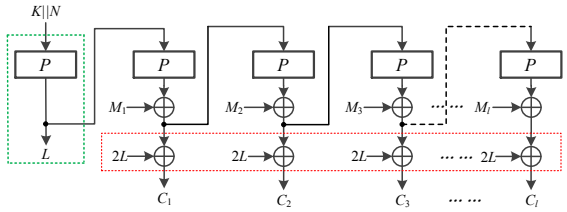

Figure 7: PCFB.

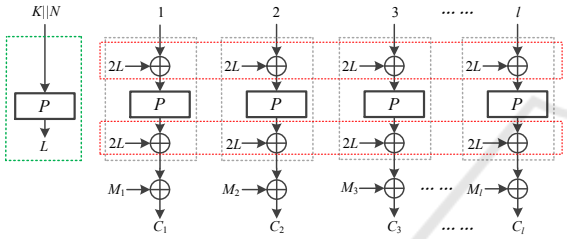

Figure 8: PCTR.

multiplication, these 4 encryption schemes are practical. Since these 4 schemes, no matter using a random IV no a non-repeated nonce, achieve $\Phi^{\oplus}$-IND-BW-CPA, which is concluded in Table 1, they are less prone to misuse, and apply to lots of practical blockwise adaptive scenarios including real-time applications, on-line settings, memory-restricted devices, etc. These schemes bring less pressure on the key-management in real world, and the key length can be chosen as need even though large permutations are used. Moreover they are more efficient than the Sponge construction, since the plaintext block processed by one call of the permutation equals exactly the bandwidth of the permutation.

In the remaining, we take PCBC as an example to prove that using a non-repeated nonce, PCBC can resist the blockwise adaptive attack in $\Phi^{\oplus}$-related-key setting, which is described formally in Theorem 1. Similar results can be deduced in POFB, PCFB and PCTR.

4.1 $\Phi^{\oplus}$-IND-BW-CPA of PCBC

Specification of PCBC. Let $\mathcal{P} \xleftarrow{\mathbb{R}} Perm(n)$ be a n-bit ideal cryptographic permutation, and k is the wanted key length, and $PCBC : \{0,1\}^k \times \{0,1\}^{n-k} \times \{0,1\}^{n+} \to \{0,1\}^{n+}$ represents the PCBC scheme. For $K \in \{0,1\}^k, N \in \{0,1\}^{n-k}, M \in \{0,1\}^{n+}$ and $C \in \{0,1\}^{n+}$ where $M = M_1 \cdots M_l$, $C = C_1 \cdots C_l$ and $|M_j| = |C_j| = n$ for $j = 1, \cdots, l$, the encryption function $C = PCBC_K(N,M)$ is defined as following:

$$
\begin{aligned}
&\textit{Encryption: } C = PCBC_K(N,M)\\
&\quad L = \mathcal{P}(K\|N); T = 2L; S = T;\\
&\quad \textit{for } j = 1 \textit{ to } l \textit{ do}\\
&\qquad T = 2T;\\
&\qquad S = \mathcal{P}(M_j \oplus S);\\
&\qquad C_j = S \oplus T;
\end{aligned}
$$

Theorem 1. *To PCBC, assuming that $\mathcal{P} \xleftarrow{\mathbb{R}} Perm(n)$ and that the $\Phi^{\oplus}$-related-key BW-CPA adversary makes q $\Phi^{\oplus}$-related-key queries including at most total σ blocks and at most r queries to $\mathcal{P}^{\pm}$,*

$$
\begin{aligned}
&\mathbf{Adv}_{PCBC}^{\Phi^{\oplus}-ind-bw-cpa}(q,r)\\
&\leq \frac{qr}{2^k} + \frac{\sigma(\sigma-1)+qr+2\sigma(q+r)}{2^n}. \qquad (5)
\end{aligned}
$$

Proof. Define the $\Phi^{\oplus}$-related-key oracle of PCBC as $\mathrm{RK}[PCBC] : \{0,1\}^k \times \Phi^{\oplus} \times \{0,1\}^{n-k} \times \{0,1\}^{n+} \to \{0,1\}^{n+}$. Without loss of generality, let $\mathcal{D}$ be any $\Phi^{\oplus}$-related-key BW-CPA adversary that makes exactly q non-duplicated related-key queries, denoted as $(\Delta^i, N^i, M^i, C^i)$, where $M^i = M^i_1 \cdots M^i_{l_i}$, $C^i = C^i_1 \cdots C^i_{l_i}$ and l_i is the total blocks of M^i, for $i = 1, \cdots, q$. Let $\sum_{i=1}^{q} l_i = \sigma$.

In the blockwise adaptive setting, during any i^{th} related-key query, $\mathcal{D}$ can delay choosing M^i_j until it knows $C^i_1, \cdots, C^i_{j-1}$ for $j = 1, \cdots, l_i$, $i = 1, \cdots, q$. Denote the $\Phi^{\oplus}$-related-key oracles in the blockwise adaptive setting as $\mathrm{RK}[\overline{PCBC}]$ and $\mathrm{RK}[\overline{\$}]$. Thus for any (Δ^i, N^i, M^i_j) queried, $\mathrm{RK}[\overline{PCBC}]_K(\Delta^i, N^i, M^i_j)$ computes: (1) if $j = 1$ the initialization is processed firstly as $L^i = \mathcal{P}((K \oplus \Delta^i)\|N^i); T^i = 2L^i; S^i = T^i$; (2) for any j, the computation is processed as $T^i = 2T^i; S^i = \mathcal{P}(M^i_j \oplus S^i); C^i_j = S^i \oplus T^i$, and C^i_j is returned.

Let $\$$ be the random function defined as before, and $\mathrm{RK}[\overline{\$}](\Delta^i, N^i, M^i_j)$ always returns a n-bit random string. Besides $\mathcal{D}$ also has access to the public permutation $\mathcal{P}^{\pm}$. Let $\mathcal{D}$ makes exactly r bi-directional queries to $\mathcal{P}^{\pm}$, denoted as (X_u, Y_u) for $u = 1, \cdots, r$.

Refer to (Chen and Steinberger, 2014), let $\mathcal{D}$ paly the "enhanced" game here, that is $\mathcal{D}$ is revealed the key after it has made all its queries but before making its final decision. Moreover in this specific case $\mathcal{D}$ is revealed more q values. More specifically, in $\mathrm{RK}[\overline{PCBC}]$ the secret key K as well as all truly L^is are revealed, while in $\mathrm{RK}[\overline{\$}]$ a dummy key $K' \xleftarrow{\mathbb{R}} \{0,1\}^k$ and q distinct dummy values L'^is randomly chosen from $\{0,1\}^n$ are given instead. Note that this game gives no disadvantage to the adversary since it can neglect the revealed information anyway.

Denote τ the transcript that $\mathcal{D}$ creates to record the queries it made and the answers it received. In more detail, let $\tau = (\tau_0, \tau_1, \tau_2)$, and τ_0, τ_1, τ_2 are defined as following:

- $\tau_0 = \{((K \oplus \Delta^i) \| N^i, L^i) \mid i = 1, \cdots, q\}$;
- $\tau_1 = \left\{(I_j^i, O_j^i) \mid j = 1, \cdots, l_i; i = 1, \cdots, q\right\}$, where $O_0^i = L^i$, $I_j^i = M_j^i \oplus O_{j-1}^i$ and $O_j^i = C_j^i \oplus (2^j L^i)$ for $j = 1, \cdots, l_i; i = 1, \cdots, q$;
- $\tau_2 = \{(X_u, Y_u) \mid Y_u = \mathcal{P}(X_u), u = 1, \cdots, r\}$.

Obviously, τ_0 mainly denotes the revealed information which in PCBC satisfies that $L^i = \mathcal{P}((K \oplus \Delta^i) \| N^i)$ for $i = 1, \cdots, q$, τ_1 denotes the rewritten form of all (M_j^i, C_j^i) pairs, which -in PCBC- are actually the input-output pairs of $\mathcal{P}$ called by $\mathrm{RK}[\overline{PCBC}]$, and τ_2 denotes the r public bi-directional queries to $\mathcal{P}^{\pm}$.

According to τ, $\mathcal{D}$ will make its final decision, which can be regarded as a (deterministic) function of the transcript τ. Let $\mathcal{T}$ denote all possible transcripts, and X denotes the transcript variable when $\mathcal{D}$ interacts with $\mathrm{RK}[\overline{PCBC}]$ while Y denotes the transcript variable when $\mathcal{D}$ interacts with $\mathrm{RK}[\bar{\$}]$. And then

$$\mathbf{Adv}_{PCBC}^{\Phi^{\oplus}-ind-bw-cpa}(q,r) \leq \Delta(X,Y), \tag{6}$$

where $\Delta(X,Y)$ denotes the statistic distance between X and Y.

Next we play the H-Coefficient technique, which is of greatly useful in proving various results on ideal cryptographic primitives such as PRP/PRF (Mennink, 2016; Hoang and Tessaro, 2016; Mouha and Luykx, 2015), to upper bound $\Delta(X,Y)$. The central idea of the H-Coefficient technique is described as following:

Lemma 1. *Let $\mathcal{T}$ participate into two disjoint subsets $\mathcal{T}_{\text{good}}$ and $\mathcal{T}_{\text{bad}}$, and $\exists \varepsilon \geq 0$ such that $\forall \tau \in \mathcal{T}_{\text{good}}$, $\Pr[X = \tau] / \Pr[Y = \tau] \geq 1 - \varepsilon$. When $\mathcal{T}_{\text{good}}$ with a small ε is large and $\mathcal{T}_{\text{bad}}$ is small,*

$$\Delta(X,Y) \leq \Pr[Y \in \mathcal{T}_{\text{bad}}] + \varepsilon. \tag{7}$$

According to Lemma 1, to upper bound $\Delta(X,Y)$ is to upper bound $\Pr[Y \in \mathcal{T}_{\text{bad}}]$ and to low bound the ratio of $\Pr[X = \tau] / \Pr[Y = \tau]$ when $\tau \in \mathcal{T}_{\text{good}}$.

UPPER BOUND $\Pr[Y \in \mathcal{T}_{\text{bad}}]$. Denote the collision happened between two sets S, S' as $\mathbf{Col}[S, S'] = \{\exists (e_1, e_2) \in S, \exists (e_1', e_2') \in S', e_1 = e_1' \vee e_2 = e_2'\}$, and $\mathbf{Col}[S] = \mathbf{Col}[S, S]$. Thus τ is defined as "bad" if any collision event, $\mathbf{Col}[\tau_0, \tau_2]$, $\mathbf{Col}[\tau_1]$ or $\mathbf{Col}[\tau_1, \tau_0 \cup \tau_2]$, happens. That is $\mathcal{T}_{\text{bad}} = \{\tau \in \mathcal{T} \mid \mathbf{Col}[\tau_0, \tau_2] \vee \mathbf{Col}[\tau_1] \vee \mathbf{Col}[\tau_1, \tau_0 \cup \tau_2]\}$ and $\mathcal{T}_{\text{good}} = \mathcal{T} \setminus \mathcal{T}_{\text{bad}}$.

In the following, we classify the collisions of $\mathcal{T}_{\text{bad}}$ that happens in Y into 4 types: (let $u = 1, \cdots, r; j = 1, \cdots, l_i, j' = 1, \cdots, l_{i'}; i, i' = 1, \cdots, q$)

- $\mathbf{Col}[\tau_0, \tau_2]$: for any i, u, since both K and L^i are randomly chosen,

$$\begin{aligned}\Pr\left[\mathbf{Col}[\tau_0, \tau_2]\right] &\leq \sum_{i=1}^{q} \sum_{u=1}^{r} \begin{pmatrix} \Pr\left[(K \oplus \Delta^i) \| N^i = X_u\right] \\ + \Pr\left[L^i = Y_u\right] \end{pmatrix} \\ &\leq \frac{qr}{2^k} + \frac{qr}{2^n}.\end{aligned}$$

- $\mathbf{Col}[\tau_1]$: for any $(i, j) \neq (i', j')$, since $L^i, L^{i'}, C_j^i$ and $C_{j'}^{i'}$ are randomly chosen,

$$\begin{aligned}\Pr\left[\mathbf{Col}[\tau_1]\right] &\leq \sum_{\substack{i,i'=1,\cdots,q; \\ j=1,\cdots,l_i, \\ j'=1,\cdots,l_{i'}; \\ (i,j)\neq(i',j')}} \begin{pmatrix} \Pr[I_j^i = I_{j'}^{i'}] \\ + \Pr[O_j^i = O_{j'}^{i'}] \end{pmatrix} \\ &\leq \frac{\binom{\sigma}{2}}{2^{n-1}} = \frac{\sigma(\sigma-1)}{2^n},\end{aligned}$$

where

$$\Pr\left[I_j^i = I_{j'}^{i'}\right] = \Pr\left[\begin{array}{c} M_j^i \oplus C_{j-1}^i \oplus 2^{j-1} L^i \\ = M_{j'}^{i'} \oplus C_{j'-1}^{i'} \oplus 2^{j'-1} L^{i'} \end{array}\right] = \frac{1}{2^n},$$

$$\Pr\left[O_j^i = O_{j'}^{i'}\right] = \Pr\left[\begin{array}{c} C_j^i \oplus 2^j L^i \\ = C_{j'}^{i'} \oplus 2^{j'} L^{i'} \end{array}\right] = \frac{1}{2^n}.$$

(Actually when $i = i'$ the collision probability here in the BW-CPA case is totally different from that in the CPA case. Let $j < j'$, the BW-CPA adversary is capable to choose $M_{j'}^{i'}$ to maximize $\Pr[M_j^i \oplus C_{j-1}^i \oplus 2^{j-1} L^i = M_{j'}^{i'} \oplus C_{j'-1}^{i'} \oplus 2^{j'-1} L^{i'}]$ since it knows $M_j^i, C_{j-1}^i, C_{j'-1}^{i'}$, while the CPA adversary isn't capable to. Thus without the finite multiplication by 2 in each block process, the BW-CPA adversary can choose $M_{j'}^{i'} = M_j^i \oplus C_{j-1}^i \oplus C_{j'-1}^{i'}$ which allows $I_j^i = I_{j'}^{i'}$.)

- $\mathbf{Col}[\tau_1, \tau_0]$: for any i, j, i', since $L^i, L^{i'}$ and C_j^i are randomly chosen,

$$\begin{aligned}&\Pr\left[\mathbf{Col}[\tau_1, \tau_0] \mid \neg\left(\mathbf{Col}[\tau_1]\right)\right] \\ &\leq \sum_{\substack{i=1,\cdots,q; \\ j=1,\cdots,l_i}} \left(\sum_{i'=1}^{q} \begin{pmatrix} \Pr\left[I_j^i = (K \oplus \Delta^{i'}) \| N^{i'}\right] \\ + \Pr\left[O_j^i = L^{i'}\right] \end{pmatrix} \right) \leq \frac{\sigma q}{2^{n-1}}.\end{aligned}$$

- $\mathbf{Col}[\tau_1, \tau_2]$: for any i, j, u, since both L^i and C_j^i are randomly chosen,

$$\begin{aligned}&\Pr\left[\mathbf{Col}[\tau_1, \tau_2] \mid \neg\left(\mathbf{Col}[\tau_1]\right)\right] \\ &\leq \sum_{\substack{i=1,\cdots,q; \\ j=1,\cdots,l_i}} \left(\sum_{u=1}^{r} \begin{pmatrix} \Pr[I_j^i = X_u] \\ + \Pr[O_j^i = Y_u] \end{pmatrix} \right) \leq \frac{\sigma r}{2^{n-1}}.\end{aligned}$$

Therefore,

$$\begin{aligned}&\Pr[\tau \in \mathcal{T}_{\text{bad}}] \\ &= \Pr\left[\mathbf{Col}[\tau_0, \tau_2] \vee \mathbf{Col}[\tau_1] \vee \mathbf{Col}[\tau_1, \tau_0 \cup \tau_2]\right] \\ &\leq \frac{qr}{2^k} + \frac{\sigma(\sigma-1) + qr + 2\sigma(q+r)}{2^n}.\end{aligned} \tag{8}$$

LOW BOUND $\Pr[X=\tau]/\Pr[Y=\tau]$ WHEN $\tau \in \mathcal{T}_{\text{good}}$. When $\tau \in \mathcal{T}_{\text{good}}$, all pairs in τ are distinct. In X, τ mainly records the randomly chosen secret key as well as the total $(q+\sigma+r)$ fresh calls to $\mathcal{P}$ (or $\mathcal{P}^{\pm}$) , that is

$$\Pr[X=\tau] = \frac{1}{2^k} \cdot \frac{1}{\binom{2^n}{q+\sigma+r}(2^n-q-\sigma-r)!}, \quad (9)$$

while in Y, τ records the dummy key, q distinct randomly-chosen L^is, σ blocks of random bits and r calls to $\mathcal{P}^{\pm}$, that is

$$\Pr[Y=\tau] = \frac{1}{2^k} \cdot \frac{1}{\binom{2^n}{q}} \cdot \frac{1}{2^{n\sigma}} \cdot \frac{1}{\binom{2^n}{r}(2^n-r)!}. \quad (10)$$

Obviously, according to (9) (10), when $\tau \in \mathcal{T}_{\text{good}}$, $\Pr[X=\tau] > \Pr[Y=\tau]$.

According to Lemma 1, (6), (8),

$$\begin{aligned} &\mathbf{Adv}^{\Phi^{\oplus}-ind-bw-cpa}_{PCBC}(q,r) \quad (11)\\ \leq &\frac{qr}{2^k} + \frac{\sigma(\sigma-1)+qr+2\sigma(q+r)}{2^n}. \end{aligned}$$

By so far, Theorem 1 is proved. □

5 CONCLUSION

In this paper, we study how to provide confidential protection with a single cryptographic permutation, and propose 4 *practical* encryption schemes - PCBC, POFB, PCFB and PCTR, by adding two simple kinds of operations - XOR and the finite multiplication. And we prove that, when using a non-repeated nonce, these 4 permutation-based encryption schemes are indistinguishable from the random function against the blockwise adaptive chosen plaintext attack in the $\Phi^{\oplus}$-related-key setting. Meanwhile they are more efficient than the Sponge construction.

ACKNOWLEDGEMENTS

The work of this paper is supported by the Fundamental Theory and Cutting Edge Technology Research Program of Institute of Information Engineering, CAS (Grant No. Y7Z0251103), and the National Natural Science Foundation of China (Grants 61472415, 61732021, 61772519).

REFERENCES

Albrecht, M. R., Farshim, P., Paterson, K. G., and Watson, G. J. (2011). On cipher-dependent related-key attacks in the ideal-cipher model. In *FSE'11, Fast Software Encryption - 18th International Workshop*. Springer.

Alkassar, A., Geraldy, A., Pfitzmann, B., and Sadeghi, A. (2001). Optimized self-synchronizing mode of operation. In *FSE'01, Fast Software Encryption - 8th International Workshop*. Springer.

Andreeva, E., Bilgin, B., Bogdanov, A., Luykx, A., Mendel, F., Mennink, B., Mouha, N., Wang, Q., and Yasuda, K. (2014). PRIMATEs v1. Submission to the CAESAR competition.

Aumasson, J., Henzen, L., Meier, W., and Naya-Plasencia, M. (2013). Quark: A lightweight hash. J. Cryptology.

Bard, G. V. (2004). The vulnerability of SSL to chosen plaintext attack. IACR Cryptology ePrint Archive.

Bard, G. V. (2006). A challenging but feasible blockwise-adaptive chosen-plaintext attack on SSL. In *SECRYPT'06, Proceedings of the International Conference on Security and Cryptography*. INSTICC Press.

Bard, G. V. (2007). Blockwise-adaptive chosen-plaintext attack and online modes of encryption. In *IMACC'07, Cryptography and Coding - 11th IMA International Conference*. Springer.

Bellare, M., Desai, A., Jokipii, E., and Rogaway, P. (1997). A concrete security treatment of symmetric encryption. In *FOCS'97, 38th Annual Symposium on Foundations of Computer Science*. IEEE Computer Society.

Bellare, M. and Kohno, T. (2003). A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. In *EUROCRYPT'03, International Conference on the Theory and Applications of Cryptographic Techniques*. Springer.

Bellare, M., Kohno, T., and Namprempre, C. (2002). Authenticated encryption in SSH: provably fixing the SSH binary packet protocol. In *CCS'02, Proceedings of the 9th ACM Conference on Computer and Communications Security*. ACM.

Bernstein, D. J. (2008). The Salsa20 family of stream ciphers. In *New Stream Cipher Designs - The eSTREAM Finalists*. Springer.

Bertoni, G., Daemen, J., Peeters, M., Van Assche, G., and Van Keer, R. (2014). CAESAR submission: Ketje v1. CAESAR First Round Submission, March.

Biham, E. (1993). New types of cryptanalytic attacks using related keys (extended abstract). In *EUROCRYPT'93, Workshop on the Theory and Application of of Cryptographic Techniques*.

Biryukov, A. and Khovratovich, D. (2009). Related-key cryptanalysis of the full AES-192 and AES-256. In *ASIACRYPT'09, 15th International Conference on the Theory and Application of Cryptology and Information Security*. Springer.

Biryukov, A. and Khovratovich, D. (2014). PAEQ: parallelizable permutation-based authenticated encryption. In *ISC'14, Information Security - 17th International Conference*. Springer.

Biryukov, A., Khovratovich, D., and Nikolic, I. (2009). Distinguisher and related-key attack on the full AES-256. In *CRYPTO'09, 29th Annual International Cryptology Conference*. Springer.

Bogdanov, A., Knezevic, M., Leander, G., Toz, D., Varici, K., and Verbauwhede, I. (2011). SPONGENT:

A lightweight hash function. In *CHES 2011, Cryptographic Hardware and Embedded Systems - 13th International Workshop*. Springer.

Chen, S. and Steinberger, J. P. (2014). Tight security bounds for key-alternating ciphers. In *EUROCRYPT'14, 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer.

Cogliati, B. and Seurin, Y. (2015). Beyond-birthday-bound security for tweakable Even-Mansour ciphers with linear tweak and key mixing. In *ASIACRYPT'15, 21st International Conference on the Theory and Application of Cryptology and Information Security*. Springer.

Daemen, J. (1991). Limitations of the Even-Mansour construction. In *ASIACRYPT'91, International Conference on the Theory and Applications of Cryptology*. Springer.

Dai, W. (2002). An attack against SSH2 protocol. Email to the SECSH Working Group ietf-ssh@ netbsd. org ftp://ftp. ietf. org/ietf-mail-archive/secsh/2002-02. mail.

Dobraunig, C., Eichlseder, M., and Mendel, F. (2015). Related-key forgeries for Prøst-OTR. In *FSE'15, Fast Software Encryption - 22nd International Workshop*. Springer.

Dobraunig, C., Eichlseder, M., Mendel, F., and Schläffer, M. (2014). Ascon v1–submission to the CAESAR competition. CAESAR First Round Submission, March.

Dunkelman, O., Keller, N., and Shamir, A. (2012). Minimalism in cryptography: The Even-Mansour scheme revisited. In *EUROCRYPT'12, 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer.

Duong, T. and Rizzo, J. (2011). Here come the xor ninjas. White paper, Netifera.

Dworkin, M. J. (2015). Sha-3 standard: Permutation-based hash and extendable-output functions.

Even, S. and Mansour, Y. (1997). A construction of a cipher from a single pseudorandom permutation. J. Cryptology.

Fouque, P., Joux, A., and Poupard, G. (2004). Blockwise adversarial model for on-line ciphers and symmetric encryption schemes. In *SAC'04, Selected Areas in Cryptography - 11th International Workshop*. Springer.

Fouque, P., Martinet, G., and Poupard, G. (2003). Practical symmetric on-line encryption. In *FSE'03, Fast Software Encryption - 10th International Workshop*. Springer.

Hoang, V. T. and Tessaro, S. (2016). Key-alternating ciphers and key-length extension: Exact bounds and multi-user security. In *CRYPTO'16, 36th Annual International Cryptology Conference*. Springer.

Joux, A., Martinet, G., and Valette, F. (2002). Blockwise-adaptive attackers: Revisiting the (in)security of some provably secure encryption models: CBC, GEM, IA-CBC. In *CRYPTO'02, 22nd Annual International Cryptology Conference*. Springer.

Karpman, P. (2015). From distinguishers to key recovery: Improved related-key attacks on even-mansour. In *ISC'15, Information Security - 18th International Conference*. Springer.

Kavun, E. B., Lauridsen, M. M., Leander, G., Rechberger, C., Schwabe, P., and Yalçın, T. (2014). Prøst. CAESAR Proposal.

Mennink, B. (2016). XPX: generalized tweakable Even-Mansour with improved security guarantees. In *CRYPTO'16, 36th Annual International Cryptology Conference*. Springer.

Moeller, B. et al. (2004). Security of CBC ciphersuites in SSL/TLS: Problems and countermeasures. Unpublished manuscript, May.

Mouha, N. and Luykx, A. (2015). Multi-key security: The Even-Mansour construction revisited. In *CRYPTO'15, 35th Annual International Cryptology Conference*. Springer.

Rogaway, P. (1996). Problems with proposed IP cryptography. Unpublished paper http://www. cs. ucdavis. edu/rogaway/papers/draftrogaway-ipsec-comments-00. txt.

Rogaway, P. (2004). Nonce-based symmetric encryption. In *FSE'04, Fast Software Encryption - 11th International Workshop*. Springer.

Sasaki, Y., Todo, Y., Aoki, K., Naito, Y., Sugawara, T., Murakami, Y., Matsui, M., and Hirose, S. (2014). Minalpher v1. Submission to the CAESAR competition.

Sung, J., Lee, S., Lim, J. I., Lee, W., and Yi, O. (2001). Concrete security analysis of CTR-OFB and CTR-CFB modes of operation. In *ICISC 2001, Information Security and Cryptology - 4th International Conference*. Springer.