Lightweight Authenticated Encryption Mode of Operation for Tweakable Block Ciphers

Yusuke Naito and Takeshi Sugawara

Mitsubishi Electric Corporation, Japan
The University of Electro-Communications, Japan

Abstract. Using a small block length is a common strategy in designing lightweight block cipher. So far, many 64-bit primitives have been proposed. However, if we use such a 64-bit primitive for an authenticated encryption with birthday-bound security, it has only 32-bit data complexity which is subject to a practical attack. To take advantage of a short block length without losing security, we propose a lightweight AEAD mode FBAE that achieves beyond-birthday-bound security. For the purpose, we extend the idea of iCOFB, originally defined with a tweakable random function, with tweakable block cipher. More specifically, we fix the tweak length which was variable in iCOFB, and further generalize the feedback function. Moreover, we improve its security bound. We evaluate the concrete hardware performances of FBAE. FBAE benefits from the small block length and shows the particularly good performances in threshold implementation.

Keywords: Authenticated encryption · beyond-birthday-bound security · tweakable blockcipher · lightweight · threshold implementation

1 Introduction

Driven by a demand for secure connectivity in resource-constrained embedded devices, lightweight cryptography has been actively studied in the last decade. Consequently, a number of lightweight block ciphers have been proposed [BBI+15, BSS+13, BJK+16, BCG+12, GPPR11, SIH+11] including PRESENT [BKL+07, SMMK13] and CLEFIA [SSA+07] standardized in ISO/IEC 29192-2.

A common strategy for designing a lightweight block cipher is to use a small block length. For example, PRESENT [BKL+07] and PRINCE [BCG+12] support 64-bit block length only. Many more algorithms such as GIFT [BPP+17] and SKINNY [BJK+16] provide 64-bit options. The small block length contributes to a smaller memory footprint and a shorter round number that is crucial for a lightweight implementation.

Resource-constrained devices are frequently used in a hostile environment in which side-channel attack (SCA) [KJJ99] should be considered. Designers face an even more challenging task of realizing an SCA-resistant implementation with a limited resource. Researchers have tackled this problem and proposed many lightweight and SCA resistant implementations [NRR06, PMK+11, MPL+11, BJK+16, GJC+17] including the ones protected by threshold implementation (TI) [NRS11]. The advantage of a block cipher with a small block length (i.e., a small state size) becomes even larger with TI in which a shared representation of the state multiplies the memory requirement.

In order to leverage the benefit of lightweight block cipher for realizing both confidentiality and integrity, lightweight modes of operation for authenticated encryption with associated data (AEAD) have been actively studied in the last few years promoted by the CAESAR competition and the NIST's move toward standardizing lightweight

Table 1: The lightweight criteria [NMSS18] and AEAD modes. The "No extra state" column shows the number of extra bits if the criterion is not satisfied.

AEAD	Primitive	Security	Lightweight criteria				Ref.
			No extra state	Inv. free	XOR only	Online	
COFB	Block cipher	$O(2^{b/2})$	$b/2$	✓	—	✓	[CIMN17]
SAEB	Block cipher	$O(2^{b/2})$	✓	✓	✓	✓	[NMSS18]
ΘCB3	TBC	$O(2^b)$	$2b$	—	—	✓	[KR11]
FBAE	TBC	$O(2^b)$	✓	✓	✓	✓	**Ours**

cryptography [NIS]. So far, lightweight and block-cipher-based AEAD modes such as COFB [CIMN17] and SAEB [NMSS18] have been proposed. However, the short block length of lightweight cryptography can be a problem for security. The lightweight AEAD modes have security up to the so-called birthday bound. More specifically, the security is ensured up to $O(2^{b/2})$ block-cipher calls when instantiated with a b-bit block cipher. With a 64-bit block cipher, the security is ensured up to 2^{32} block-cipher calls only. It is subject to a practical attack as demonstrated by the Sweet32 attack [BL16].

The use of an AEAD mode with beyond-birthday-bound (BBB) security is a solution for avoiding the birthday problem. There are block-cipher-based AEAD modes with BBB security including CHM [Iwa06], CIP [Iwa08], and AEAD modes with CLRW2 [LST12] or r-CLRW [LS13]. However, they are costly compared with the lightweight AEAD modes, since two or more independent universal hash functions are required. Another solution is to construct a (dedicated) TBC-based AEAD mode. The TBC-based AEAD modes, including ΘCB3 [KR11], $\mathbb{OTR}$ [Min14], SCT [PS16] and ZAE [IMPS17], realize better efficiency and security. Especially, ΘCB3 has the smallest state in the category of the BBB-secure AEAD modes.

1.1 Motivation, Approach, and Problems

Our motivation is to design a lightweight BBB-secure AEAD mode thereby taking advantage of a short block length without losing security. For being lightweight, we use the four criteria for lightweight AEAD [NMSS18] which is used in designing the block-cipher-based lightweight AEAD mode SAEB as shown in Table 1:

- **No extra state**: The AEAD mode uses no additional memory in addition to the ones used within the (tweakable) block cipher.
- **Inverse free**: The AEAD mode uses no decryption call of the (tweakable) block cipher.
- **XOR only**: The AEAD mode needs XOR only in addition to the (tweakable) block cipher.
- **Online**: The AEAD mode scans the incoming message only once.

Using a (dedicated) TBC is a promising approach for designing a lightweight and BBB-secure AEAD mode; however, none of the previous TBC-based AEAD modes, including ΘCB3, satisfy all the lightweight criteria (see Table 1).

Our approach is to design a (dedicated) TBC-based AEAD mode by extending the idea of iCOFB [CIMN17]. iCOFB shown in Figure 1 is a generalization of COFB by tweakable random function (TRF) having b-bit outputs, denoted by R. In iCOFB, a TRF is called for each message/ciphertext block. Feedback functions ρ/ρ' are used to map a pair of a

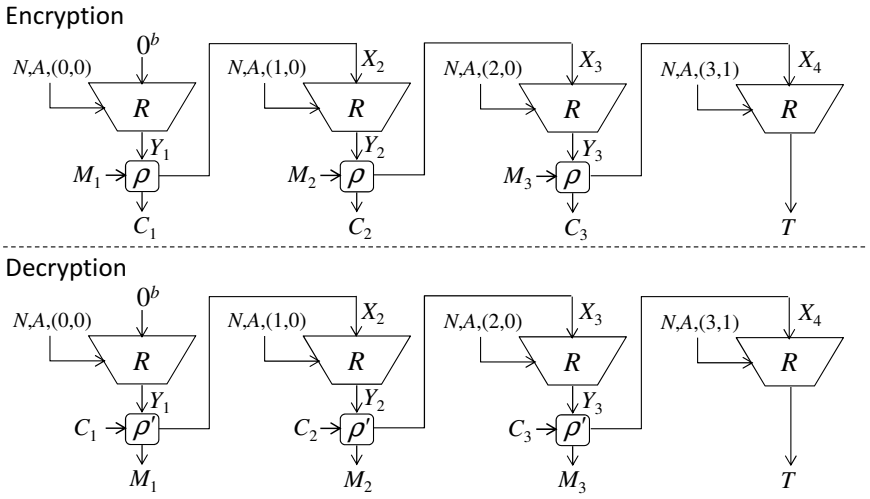

Figure 1: iCOFB. M_1, M_2, M_3 are b-bit plaintext blocks, C_1, C_2, C_3 are b-bit ciphertext blocks, and T is a b-bit tag.

TRF output Y_i and a plaintext/ciphertext block M_i/C_i to the next TRF input X_{i+1} and a ciphertext/plaintext block C_i/M_i. More specifically, the following linear functions are considered, which is expressed by a $2b \times 2b$ binary matrix.

$$\rho(Y_i, M_i) = \begin{pmatrix} X_{i+1} \\ C_i \end{pmatrix} = \begin{pmatrix} E_{1,1} & E_{1,2} \\ E_{2,1} & E_{2,2} \end{pmatrix} \begin{pmatrix} Y_i \\ M_i \end{pmatrix} \ ,$$
$$\rho'(Y_i, C_i) = \begin{pmatrix} X_{i+1} \\ M_i \end{pmatrix} = \begin{pmatrix} D_{1,1} & D_{1,2} \\ D_{2,1} & D_{2,2} \end{pmatrix} \begin{pmatrix} Y_i \\ C_i \end{pmatrix} \ .$$

After consuming all the message blocks, a TRF is called once again to generate a tag T. It was proven that iCOFB has $O(2^b)$ security with (ρ, ρ') satisfying a certain criterion (see Section 3.1).

As shown in Figure 1, iCOFB needs no extra state in addition to the ones within the underlying TRF. Besides, iCOFB takes message/ciphertext blocks online and does not need an inverse of TRF. Moreover, the linear functions ρ and ρ' can be realized with XOR only. Therefore, iCOFB satisfies all the requirements regarding TRF-based AEAD.

There are two problems in designing a TBC-based AEAD mode from the iCOFB's idea. First, since associated data (AD) is a part of a tweak, the underlying TRF should accept an arbitrary-length tweak. On the contrary, lightweight TBCs such as SKINNY accepts a fixed-length tweak only. Using the XT tweak extension [MI15] is a possible solution, but it requires a universal hash function accepting an arbitrary-length input that can be costly in implementation. Second, the security bound of iCOFB is $O(\ell_{\max} q/2^b)$ which depends on the maximum message block length $\ell_{\max}$ and the number of queries q (the sum of the numbers of encryption queries and forgery attempts). It is degraded compared with that of ΘCB3, $O(q_{\mathcal{D}}/2^b)$, wherein $q_{\mathcal{D}}$ is the number of forgery attempts. Large $\ell_{\max}$ and/or q cause a short key life: an additional cost for rekeying or a shorter product lifetime.

1.2 Contribution

We design a (fixed tweak-length) TBC-based AEAD mode called FBAE that solves the above two problems and satisfies all the lightweight criteria as shown in Table 1. Moreover, we generalize the feedback functions that cover a broader class of feedback functions including non-linear ones. Note that FBAE satisfies the criteria when the functions are

instantiated with only the XOR operations. The concrete instantiation is given later, which is called PFB.

We address the first problem by designing a new AD processing part. We introduce a (possibly non-linear) feedback function $\delta^{(a)}$ that maps an AD block A_i and an TBC output block W_i to the next TBC input V_{i+1}. A given AD is processed block by block by using a fixed-tweak TBC and the feedback function $\delta^{(a)}$.

To address the second problem, we generalize the linear feedback functions ρ and ρ' to the pairs of functions $(\gamma^{(e)}, \delta^{(e)})$ and $(\gamma^{(d)}, \delta^{(d)})$ given by

$$\delta^{(e)} : (Y_i, M_i) \mapsto X_{i+1}, \qquad \gamma^{(e)} : (Y_i, M_i) \mapsto C_i,$$
$$\delta^{(d)} : (Y_i, C_i) \mapsto X_{i+1}, \qquad \gamma^{(d)} : (Y_i, C_i) \mapsto M_i.$$

We show conditions on the generalized feedback functions (given in Sections 3.2 and 3.3) under which FBAE satisfy the security bound of $O(q_{\mathcal{D}}/2^b)$ — the same level of security as ΘCB3. The set of generalized feedback function satisfying the condition is a superset of (ρ, ρ') in iCOFB, and thus involves a broader class of functions.

The benefit of the proposed TBC-based AEAD mode is evaluated through concrete hardware implementations. In the implementations, we use a particularly efficient set of functions:

$$\delta^{(a)}(W_i, A_i) = W_i \oplus A_i,$$
$$\delta^{(e)}(Y_i, M_i) = M_i, \qquad \gamma^{(e)}(Y_i, M_i) = Y_i \oplus M_i,$$
$$\delta^{(d)}(Y_i, C_i) = Y_i \oplus C_i = M_i, \qquad \gamma^{(d)}(Y_i, C_i) = Y_i \oplus C_i.$$

We refer the specialization as the plaintext feedback mode (PFB) because the TBC input is always M_i. We remark that the encryption of PFB is parallelizable, unlike the existing lightweight AEAD modes COFB and SAEB[1]. The feature is desirable for communication between entities with asymmetric resources, e.g., a central server sends encrypted commands to many resource-constrained nodes.

In the implementations, PFB is instantiated with the lightweight TBC SKINNY-64-192. Its performance is compared with the state-of-the-art block-cipher-based alternative with the same level of security: SAEB instantiated with GIFT-128-128. For each of the AEADs, we evaluate the performances with and without TI. We show that PFB benefit from the small block length and shows the particularly good performance in implementations with the SCA countermeasure: it has the smallest circuit area compared with the SAEB implementation and the conventional implementations of Ascon [GWDE15]) and Ketje [ANR18].

1.3 Organization

This paper is organized as follows. In Section 2, we briefly review TBC and AEAD. Then, we describe the design principle and definition of FBAE in Section 3, followed by its security result is Section 4. We show hardware implementations and their performance comparison in Section 5.

1.4 Other Related Work

Regarding an independent concurrent work, Iwata, Khairallah, Minematsu and Peyrin proposed Romulus [IKMP19b] as a round 1 candidate of the lightweight crypto standard-

[1]The decryption of PFB is not parallelizable, whereas both the encryption and decryption of ΘCB3 is parallelizable. However, as shown in Table 1, ΘCB3 does not satisfy three out of the four conditions. Regarding ρ and ρ', COFB uses the other feedback functions called combined feedback, which does not offer the parallelizability. SAEB has the iterated structure of a block cipher, thus does not has the parallelizability.

ization process [NIS]. The mode of operation of Romulus-N was designed to become lightweight, using a TBC, and has many similarities to FBAE. The mode has the same level of security as FBAE [IKMP19a], where the security bound is $O(q_{\mathcal{D}}/2^b)$. The differences between FBAE and the Romulus-N mode are summarized as follows.

1. Romulus-N processes AD blocks using both tweak and input-block spaces of the underlying TBC, while FBAE does not use tweak spaces.

2. The feedback function of FBAE is more general than that of Romulus-N. Moreover, one instantiation of the feedback function PFB ensures that the encryption is parallelizable, while Romulus-N is not.

Note that Romulus-M is not online, although it is secure even in the nonce-misuse setting (FBAE and Romulus-N are not).

2 Preliminaries

2.1 Notation

Let λ be an empty string and $\{0,1\}^*$ the set of all bit strings. For an integer $i \geq 0$, let $\{0,1\}^i$ be the set of all i-bit strings, $\{0,1\}^0 := \{\lambda\}$, and $\{0,1\}^{\leq i} := \{0,1\}^1 \cup \{0,1\}^2 \cup \cdots \cup \{0,1\}^i$ the set of all bit strings of length at most i, except for λ. Let 0^i resp. 1^i be the bit string of i-bit zeros resp. ones. For an integer $i \geq 1$, let $[i] := \{1, 2, \ldots, i\}$ be the set of positive integers equal to or less than i, and $(i) := \{0\} \cup [i]$. For a non-empty set $\mathcal{T}$, $T \xleftarrow{\$} \mathcal{T}$ means that an element is chosen uniformly at random from $\mathcal{T}$ and is assigned to T. The concatenation of two bit strings X and Y is written as $X\|Y$ or XY when no confusion is possible. For integers $0 \leq i \leq j$ and $X \in \{0,1\}^j$, let $\mathsf{msb}_i(X)$ resp. $\mathsf{lsb}_i(X)$ be the most resp. least significant i bits of X, and $|X|$ the number of bits of X, i.e., $|X| = j$. For integers i and j with $0 \leq i < 2^j$, let $\mathsf{str}_j(i)$ be the j-bit binary representation of i. For an integer $b \geq 0$ and a bit string X, we denote the parsing into fixed-length b-bit strings as $(X_1, X_2, \ldots, X_\ell) \xleftarrow{b} X$, where $X = X_1\|X_2\|\cdots\|X_\ell$, $|X_i| = b$ for $i \in [\ell - 1]$, and $0 < |X_\ell| \leq b$. For an integer $b > 0$, let $\mathsf{ozp}_b : \left(\{\lambda\} \cup \{0,1\}^{\leq b}\right) \to \{0,1\}^b$ be a one-zero padding function: for a bit string $X \in \{0,1\}^{\leq b}$, $\mathsf{ozp}_b(X) = X$ if $|X| = b$; $\mathsf{ozp}_b(X) = X\|10^{b-1-|X|}$ if $|X| < b$.

2.2 Tweakable Block Cipher

A tweakable block cipher (TBC) is a set of permutations indexed by a key and a public input called tweak. Let $\mathcal{K}$ be the key spece, $\mathcal{TW}$ the tweak space, and b the input/output-block size. A TBC (encryption) is denoted by $\widetilde{E} : \mathcal{K} \times \mathcal{TW} \times \{0,1\}^b \to \{0,1\}^b$. A TBC having a key $K \in \mathcal{K}$ is denoted by $\widetilde{E}_K$, and $\widetilde{E}_K$ having a tweak $TW \in \mathcal{TW}$ is denoted by $\widetilde{E}_K^{TW}$.

In this paper, a keyed TBC is assumed to be a secure tweakable-pseudo-random permutation, or TPRP for short, which is indistinguishable from a tweakable random permutation (TRP). A tweakable permutation (TP) $\widetilde{P} : \mathcal{TW} \times \{0,1\}^b \to \{0,1\}^b$ is a set of b-bit permutations indexed by a tweak in $\mathcal{TW}$. A TP having a tweak $TW \in \mathcal{TW}$ is denoted by $\widetilde{P}^{TW}$. Let $\widetilde{\mathsf{Perm}}(\mathcal{TW}, \{0,1\}^b)$ be the set of all TPs with b-bit blocks and tweak space $\mathcal{TW}$. A TRP is defined as $\widetilde{P} \xleftarrow{\$} \widetilde{\mathsf{Perm}}(\mathcal{TW}, \{0,1\}^b)$. In the TPRP-security game, an adversary $\mathbf{A}$ has access to either the target keyed TBC $\widetilde{E}_K$ for $K \xleftarrow{\$} \mathcal{K}$ or a TRP $\widetilde{P} \xleftarrow{\$} \widetilde{\mathsf{Perm}}(\mathcal{TW}, \{0,1\}^b)$. After the interaction, $\mathbf{A}$ returns a decision bit $y \in \{0,1\}$. The output of $\mathbf{A}$ with access to an oracle $\mathcal{O}$ is denoted by $\mathbf{A}^{\mathcal{O}}$. For a TBC $\widetilde{E}$, the

TPRP-security advantage function of an adversary $\mathbf{A}$ is defined as

$$\mathbf{Adv}^{\mathsf{tprp}}_{\widetilde{E}_K}(\mathbf{A}) := \Pr\left[K \xleftarrow{\$} \mathcal{K}; \mathbf{A}^{\widetilde{E}_K} = 1\right] - \Pr\left[\widetilde{P} \xleftarrow{\$} \widetilde{\mathsf{Perm}}(\mathcal{TW}, \{0,1\}^b); \mathbf{A}^{\widetilde{P}} = 1\right],$$

where the probabilities are taken over $K, \widetilde{P}$ and $\mathbf{A}$.

The maximum over all adversaries, running in time at most t and making at most σ queries, is denoted by

$$\mathbf{Adv}^{\mathsf{tprp}}_{\widetilde{E}_K}(\sigma, t) := \max_{\mathbf{A}} \mathbf{Adv}^{\mathsf{tprp}}_{\widetilde{E}_K}(\mathbf{A}) \ .$$

2.3 Nonce-Based Authenticated Encryption with Associated Data

A nonce-based authenticated encryption with associated data (nAEAD) scheme based on a keyed TBC $\widetilde{E}_K$, denoted by $\Pi[\widetilde{E}_K]$, is a pair of encryption and decryption algorithms $(\Pi.\mathsf{Enc}[\widetilde{E}_K], \Pi.\mathsf{Dec}[\widetilde{E}_K])$. $\mathcal{K}, \mathcal{N}, \mathcal{M}, \mathcal{C}, \mathcal{A}$ and $\mathcal{T}$ are the sets of keys, nonces, plaintexts, ciphertexts, associated data (AD) and tags of $\Pi[\widetilde{E}_K]$, respectively. In this paper, the key space of $\Pi[\widetilde{E}_K]$ is equal to that of the underlying TBC. The encryption algorithm takes a nonce $N \in \mathcal{N}$, AD $A \in \mathcal{A}$, and a plaintext $M \in \mathcal{M}$, and returns, deterministically, a pair of a ciphertext $C \in \mathcal{C}$ and a tag $T \in \mathcal{T}$. The decryption algorithm takes a tuple $(N, A, C, T) \in \mathcal{N} \times \mathcal{A} \times \mathcal{C} \times \mathcal{T}$, and returns, deterministically, either the distinguished invalid (reject) symbol $\perp \notin \mathcal{M}$ or a plaintext $M \in \mathcal{M}$. We require $|\Pi.\mathsf{Enc}[\widetilde{E}_K](N, A, M)| = |\Pi.\mathsf{Enc}[\widetilde{E}_K](N, A, M')|$ when these outputs are strings and $|M| = |M'|$. We consider two security notions of nAEAD, privacy and authenticity. Here, we call queries to the encryption resp. decryption oracle "encryption queries" resp. "decryption queries."

Privacy

The privacy notion considers the indistinguishability between the encryption $\Pi.\mathsf{Enc}[\widetilde{E}_K]$ and a random-bits oracle \$, in the nonce-respecting setting. \$ has the same interface as $\Pi.\mathsf{Enc}[\widetilde{E}_K]$ and for a query (N, A, M) returns a random bit string of length $|\Pi.\mathsf{Enc}[\widetilde{E}_K](N, A, M)|$. In the privacy game, an adversary $\mathbf{A}$ interacts with either $\Pi.\mathsf{Enc}[\widetilde{E}_K]$ or \$, and then returns a decision bit $y \in \{0, 1\}$. The privacy advantage function of an adversary $\mathbf{A}$ is defined as

$$\mathbf{Adv}^{\mathsf{priv}}_{\Pi[\widetilde{E}_K]}(\mathbf{A}) := \Pr[K \xleftarrow{\$} \mathcal{K}; \mathbf{A}^{\Pi.\mathsf{Enc}[\widetilde{E}_K]} = 1] - \Pr[\mathbf{A}^{\$} = 1] \ ,$$

where the probabilities are taken over K, \$ and $\mathbf{A}$. We demand that $\mathbf{A}$ is nonce-respecting (all nonces in encryption queries are distinct).

The maximum over all adversaries, running in time at most t and making encryption queries of $\sigma_{\mathcal{E}}$ the total number of TBC calls invoked by all encryption queries, is denoted by

$$\mathbf{Adv}^{\mathsf{priv}}_{\Pi[\widetilde{E}_K]}(\sigma_{\mathcal{E}}, t) := \max_{\mathbf{A}} \mathbf{Adv}^{\mathsf{priv}}_{\Pi[\widetilde{E}_K]}(\mathbf{A}) \ .$$

When an adversary is a computationally unbounded algorithm, the time t is disregarded.

Authenticity

The authenticity notion considers the unforgeability in the nonce-respecting setting. In the authenticity game, an adversary $\mathbf{A}$ interacts with $\Pi[\widetilde{E}_K] = (\Pi.\mathsf{Enc}[\widetilde{E}_K], \Pi.\mathsf{Dec}[\widetilde{E}_K])$, and the goal of the adversary is to make a non-trivial decryption query whose response is not $\perp$. The authenticity advantage of an adversary $\mathbf{A}$ is defined as

$$\mathbf{Adv}^{\mathsf{auth}}_{\Pi[\widetilde{E}_K]}(\mathbf{A}) := \Pr[K \xleftarrow{\$} \mathcal{K}; \mathbf{A}^{\Pi.\mathsf{Enc}[\widetilde{E}_K], \Pi.\mathsf{Dec}[\widetilde{E}_K]} \text{ forges}] \ ,$$

where the probabilities are taken over K and $\mathbf{A}$. We demand that $\mathbf{A}$ is nonce-respecting (all nonces in encryption queries are distinct), that $\mathbf{A}$ never asks a trivial decryption query (N, A, C, T), i.e., there is a prior encryption query (N, A, M) with $(C, T) = \Pi.\mathsf{Enc}[\widetilde{E}_K](N, A, M)$, and that $\mathbf{A}$ never repeats a query. $\mathbf{A}^{\Pi.\mathsf{Enc}[\widetilde{E}_K],\Pi.\mathsf{Dec}[\widetilde{E}_K]}$ forges means that $\mathbf{A}$ makes a decryption query whose response is not $\perp$.

The maximum over all adversaries, running in time at most t and making at most $q_{\mathcal{E}}$ encryption queries and $q_{\mathcal{D}}$ decryption queries of σ the total number of TBC calls invoked by all queries, is denoted by

$$\mathbf{Adv}^{\mathsf{auth}}_{\Pi[\widetilde{E}_K]}((q_{\mathcal{E}}, q_{\mathcal{D}}, \sigma), t) := \max_{\mathbf{A}} \mathbf{Adv}^{\mathsf{auth}}_{\Pi[\widetilde{E}_K]}(\mathbf{A}) \ .$$

When an adversary is a computationally unbounded algorithm, the time t is disregarded.

3 FBAE: TBC-based Feedback Mode

We design a TBC-based nAEAD scheme, basing on the iCOFB design approach.

3.1 Brief Overview of iCOFB Design and Security

iCOFB given in [CIMN17] is a tweakable random-function (TRF)-based nAEAD scheme and is designed so that an extra state beyond the TRF size is not required. Let ℓ_{max} be the maximum length of ciphertext blocks, and $R : (\mathcal{N} \times \mathcal{A} \times [\ell_{\mathsf{max}}+1] \times (1)) \times \{0,1\}^b \to \{0,1\}^b$ be a TRF, where tweak elements are a nonce, AD, a counter and a domain separation. Let $\rho : \{0,1\}^b \times \{0,1\}^b \to \{0,1\}^b \times \{0,1\}^b$ be a feedback function that takes a b-bit TRF output and a b-bit plaintext block, and outputs a b-bit TRF input and a b-bit ciphertext block. Figure 1 shows the encryption and decryption procedures of iCOFB with three plaintext/ciphertext blocks.

In order for iCOFB to become lightweight, the feedback function ρ should be lightweight. [CIMN17] considers a linear function, thus ρ is expressed by a $2b \times 2b$ binary matrix:

$$\rho(Y_i, M_i) = \begin{pmatrix} X_{i+1} \\ C_i \end{pmatrix} = \begin{pmatrix} E_{1,1} & E_{1,2} \\ E_{2,1} & E_{2,2} \end{pmatrix} \begin{pmatrix} Y_i \\ M_i \end{pmatrix}$$

where $E_{i,j}$'s are $b \times b$ binary matrices. For the decryption of iCOFB, the feedback function ρ' is also expressed by a $2b \times 2b$ binary matrix:

$$\rho'(Y_i, C_i) = \begin{pmatrix} X_{i+1} \\ M_i \end{pmatrix} = \begin{pmatrix} D_{1,1} & D_{1,2} \\ D_{2,1} & D_{2,2} \end{pmatrix} \begin{pmatrix} Y_i \\ C_i \end{pmatrix}$$

where $D_{i,j}$'s are $b \times b$ binary matrices. For the correctness of iCOFB, [CIMN17] chooses the feedback function ρ' with the following conditions: $E_{2,2}$ is invertible; $D_{1,1} = E_{1,1} + E_{1,2}E_{2,2}^{-1}E_{2,1}$; $D_{1,2} = E_{1,2}E_{2,2}^{-1}$; $D_{2,1} = E_{2,2}^{-1}E_{2,1}$; $D_{2,2} = E_{2,2}^{-1}$.

Regarding the security of iCOFB, they show the following theorem.

Theorem 1 *[]If the feedback function ρ satisfies the conditions: **(A1)** $E_{2,1}$ is invertible; **(A2)** $D_{1,2}$ is invertible; **(A3)** $D_{1,1}$ is invertible, then we have for any adversary $\mathbf{A}$ making at most $q_{\mathcal{D}}$ decryption queries of*

$$\mathbf{Adv}^{\mathsf{priv}}_{\mathsf{iCOFB}[R]}(\sigma_{\mathcal{E}}) = 0 \ , \quad \mathbf{Adv}^{\mathsf{auth}}_{\mathsf{iCOFB}[R]}((q_{\mathcal{E}}, q_{\mathcal{D}}, q_{\mathcal{D}}\ell_{\mathsf{max}})) \leq \frac{q_{\mathcal{D}}(\ell_{\mathsf{max}}+1)}{2^b} \ .$$

where ℓ_{max} is the maximum query length in blocks.

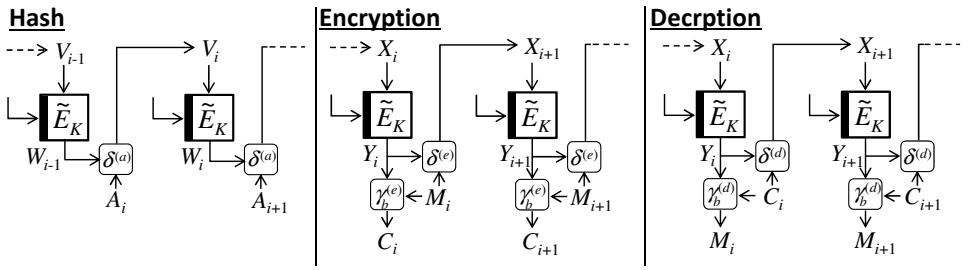

Figure 2: Core Procedures of FBAE. A_i is an i-th AD block. M_i is an i-th plaintext block. C_i is an i-th ciphertext block. Tweaks are omitted.

3.2 FBAE: Design Principle and Specification

We design FBAE (stands for FeedBack Authenticated Encryption mode), a TBC-based lightweight AEAD mode, by extending the idea of iCOFB with TBC.

Encryption/Decryption Procedures

In FBAE, a plaintext/ciphertext is partitioned into b-bit blocks, and as iCOFB, each block is processed by a TBC and a feedback function. But more general functions than the linear feedback functions ρ, ρ' are considered.

- The feedback function in the encryption is composed of the following two functions: for an integer $0 < l \leq b$,
  - $\gamma_l^{(e)} : \{0,1\}^l \times \{0,1\}^l \to \{0,1\}^l$ defines a ciphertext block $C_i \in \{0,1\}^l$ from a TBC output $Y_i \in \{0,1\}^l$ and a plaintext block $M_i \in \{0,1\}^l$ (thus $C_i = \gamma_l^{(e)}(Y_i, M_i)$), and
  - $\delta^{(e)} : \{0,1\}^b \times \{0,1\}^{\leq b} \to \{0,1\}^b$ defines a TBC input $X_{i+1} \in \{0,1\}^b$ from a TBC output $Y_i \in \{0,1\}^b$ and a plaintext block $M_i \in \{0,1\}^{\leq b}$ (thus $X_{i+1} = \delta^{(e)}(Y_i, M_i)$).

  The core procedure of the encryption of FBAE that uses these functions is given in the center of Figure 2. Note that plaintext blocks except for the last block are of $l = b$, and the last block is of $l \leq b$.

- The feedback function in the decryption is composed of the following two functions: for an integer $0 < l \leq b$,
  - $\gamma_l^{(d)} : \{0,1\}^l \times \{0,1\}^l \to \{0,1\}^l$ defines a plaintext block $M_i \in \{0,1\}^l$ from a TBC output $Y_i \in \{0,1\}^l$ and a ciphertext block $C_i \in \{0,1\}^l$ (thus $M_i = \gamma_l^{(d)}(Y_i, C_i)$), and
  - $\delta^{(d)} : \{0,1\}^b \times \{0,1\}^{\leq b} \to \{0,1\}^b$ defines a TBC input $X_{i+1} \in \{0,1\}^b$ from a TBC output $Y_i \in \{0,1\}^b$ and a ciphertext block $C_i \in \{0,1\}^{\leq b}$ (thus $X_{i+1} = \delta^{(d)}(Y_i, M_i)$).

  The core procedure of the decryption of FBAE that uses these functions is given in the right of Figure 2. Note that ciphertext blocks except for the last block are of $l = b$, and the last block is of $l \leq b$.

Hash Procedure (AD Processing)

In order to design a lightweight AEAD scheme, FBAE uses a fixed-tweak-length TBC, whereas iCOFB uses a variable-tweak-length TRF to take variable-length AD. Hence, we define additional procedure of processing variable-length AD. Similar to the encryption/decryption procedures, AD is partitioned into b-bit blocks and then the AD blocks are processed by iterating a combination of a TBC and the following feedback function.

- $\delta^{(a)} : \{0,1\}^b \times \left(\{\lambda\} \cup \{0,1\}^{\leq b}\right) \to \{0,1\}^b$ defines a TBC input $V_i \in \{0,1\}^b$ from a TBC output $W_{i-1} \in \{0,1\}^b$ and an AD block $A_i \in \{\lambda\} \cup \{0,1\}^{\leq b}$ (thus $V_i = \delta^{(a)}(W_{i-1}, A_i)$).

Note that an empty AD block is appeared when AD is an empty string, and thus the feedback function accepts an empty string. The core procedure of processing an AD block is given in the left of Figure 2.

Tweak Function

Let ℓ_{max} be the maximum block size of AD, plaintext and ciphertext. Regarding a tweak of the underlying TBC, we use the following tweak function:

- $f : [7] \times \mathcal{N} \times (\ell_{\mathsf{max}}) \to \mathcal{TW}$,

with the following condition:

- **B1**: for any $(i, N, j), (i', N', j') \in [7] \times \mathcal{N} \times (\ell_{\mathsf{max}})$ such that $(i, N, j) \neq (i', N', j')$,

$$f(i, N, j) \neq f(i', N', j').$$

The first element is used for distinguishing AD and plaintext/ciphertext, and whether the last block is a full-bit one or not, which offers a distinct permutation between the hash procedure and the encryption/decryption, and which avoids a redundant TBC call when the last block is a full-bit one. The second element is a nonce, which offers a distinct permutation for each encryption (under the nonce-respecting setting), thereby removing the birthday term regarding the number of queries. The third element is the current block number, which offers a distinct permutation for each block, thereby removing the query length from the security bound.

Specification of FBAE

The specification of FBAE is given in Algorithm 1 and is shown in Figure 3. FBAE.Hash is the hash procedure, FBAE.Enc is the encryption, and FBAE.Dec is the decryption.

For the correctness of FBAE, the following conditions are required. Let l be an integer such that $0 < l \leq b$.

- **B2**: for any $Y \in \{0,1\}^l$, $\gamma_l^{(e)}(Y, \cdot)$ is bijective and $\gamma_l^{(d)}(Y, \cdot)$ is the inverse of $\gamma_l^{(e)}(Y, \cdot)$, i.e., $M = \gamma_l^{(d)}(Y, \gamma_l^{(e)}(Y, M))$ for any $M \in \{0,1\}^l$.
- **B3**: for any $M \in \{0,1\}^l, Y \in \{0,1\}^b$, $\delta^{(e)}(Y, M) = \delta^{(d)}(Y, \gamma_l^{(e)}(\mathsf{msb}_l(Y), M))$.

3.3 Conditions on $\gamma_l^{(e)}, \gamma_l^{(d)}, \delta^{(a)}, \delta^{(e)}, \delta^{(d)}$

In order for FBAE to be secure, we require the following five conditions on $\gamma_l^{(e)}, \gamma_l^{(d)}, \delta^{(a)}, \delta^{(e)}, \delta^{(d)}$.

- **B4**: for any $M \in \{0,1\}^l$, $\gamma_l^{(e)}(\cdot, M)$ is bijective.
- **B5**: for any $C \in \{0,1\}^{\leq b}$, $\delta^{(d)}(\cdot, C)$ is bijective.

Algorithm 1 FBAE

Encryption $\mathsf{FBAE.Enc}[\widetilde{E}_K](N, A, M)$

1: $X_1 \leftarrow \mathsf{FBAE.Hash}[\widetilde{E}_K](A)$
2: **if** $A \neq \lambda \wedge |A| \mod b = 0$ **then** $x \leftarrow 2$; **else** $x \leftarrow 3$
3: **if** $M = \lambda$ **then** $\ell \leftarrow 0$; goto step 8
4: $M_1, \ldots, M_\ell \xleftarrow{b} M$
5: **for** $i = 1, \ldots, \ell$ **do**
6: $\quad Y_i \leftarrow \widetilde{E}_K^{f(x,N,i)}(X_i)$; $C_i \leftarrow \gamma_{|M_i|}^{(e)}(\mathsf{msb}_{|M_i|}(Y_i), M_i)$; $X_{i+1} \leftarrow \delta^{(e)}(Y_i, M_i)$
7: **end for**
8: **if** $M \neq \lambda \wedge |M| \mod b = 0$ **then** $y \leftarrow x + 2$; **else** $y \leftarrow x + 4$
9: $S \leftarrow X_{\ell+1}$; $T \leftarrow \mathsf{msb}_\tau\left(\widetilde{E}_K^{f(y,N,\ell)}(S)\right)$; $C \leftarrow C_1 \| \cdots \| C_\ell$
10: **return** (C, T)

Decryption $\mathsf{FBAE.Dec}[\widetilde{E}_K](N, A, C, T)$

1: $X_1 \leftarrow \mathsf{FBAE.Hash}[\widetilde{E}_K](A)$
2: **if** $A \neq \lambda \wedge |A| \mod b = 0$ **then** $x \leftarrow 2$; **else** $x \leftarrow 3$
3: **if** $C = \lambda$ **then** $\ell \leftarrow 0$; goto step 8
4: $C_1, \ldots, C_\ell \xleftarrow{b} C$
5: **for** $i = 1, \ldots, \ell$ **do**
6: $\quad Y_i \leftarrow \widetilde{E}_K^{f(x,N,i)}(X_i)$; $M_i \leftarrow \gamma_{|C_i|}^{(d)}(\mathsf{msb}_{|C_i|}(Y_i), C_i)$; $X_{i+1} \leftarrow \delta^{(d)}(Y_i, C_i)$
7: **end for**
8: **if** $C \neq \lambda \wedge |C| \mod b = 0$ **then** $y \leftarrow x + 2$; **else** $y \leftarrow x + 4$
9: $S \leftarrow X_{\ell+1}$; $\hat{T} \leftarrow \mathsf{msb}_\tau\left(\widetilde{E}_K^{f(y,N,\ell)}(S)\right)$; $M \leftarrow M_1 \| \cdots \| M_\ell$
10: **if** $T = \hat{T}$ **then return** M; **else return** $\perp$

Hash $\mathsf{FBAE.Hash}[\widetilde{E}_K](A)$

1: $A_1, \ldots, A_a \xleftarrow{b} A$; $W_0 \leftarrow 0^b$
2: **for** $i = 1, \ldots, a-1$ **do** $V_i \leftarrow \delta^{(d)}(W_{i-1}, A_i)$; $W_i \leftarrow \widetilde{E}_K^{f(1,R,i)}(V_i)$
3: $V_a \leftarrow \delta^{(d)}(W_{a-1}, A_a)$; $H \leftarrow V_a$
4: **return** H

- **B6**: for any $C, C' \in \{0,1\}^{\leq b}$ and $Y, Y' \in \{0,1\}^b$,

$$\begin{aligned}\delta^{(e)}(Y, \gamma_{|C|}^{(d)}(\mathsf{msb}_{|C|}(Y), C)) = \delta^{(d)}(Y', C') \Rightarrow &(C = C' \wedge Y = Y') \vee (C \neq C' \wedge Y \neq Y') \vee \\ &(C \neq C' \wedge Y = Y' \wedge |C| = b \wedge |C'| < b) \vee \\ &(C \neq C' \wedge Y = Y' \wedge |C| < b \wedge |C'| = b).\end{aligned}$$

- **B7**: for any $A \in \{0,1\}^{\leq b}$, $\delta^{(a)}(\cdot, A)$ is bijective.
- **B8**: for any $A, A' \in \{\lambda\} \cup \{0,1\}^{\leq b}, W, W' \in \{0,1\}^b$,

$$\begin{aligned}\delta^{(a)}(W, A) = \delta^{(a)}(W, A') \Rightarrow &(A = A' \wedge W = W') \vee (A \neq A' \wedge W \neq W') \vee \\ &(A \neq A' \wedge W = W' \wedge |A| = b \wedge |A'| < b).\end{aligned}$$

The condition **B4** ensures that for a plaintext block M_i and a TBC output Y_i, if Y_i is uniformly distributed over $\{0,1\}^b$, then so is the ciphertext block $C_i = \gamma_l^{(e)}(Y_i, M_i)$. The condition **B5** ensures that the internal state collision $\delta^{(e)}(Y_i, M_i) = \delta^{(d)}(Y_i', C_i')$ (between the encryption and decryption) depends on the randomness of the TBC output Y_i'. Thus,

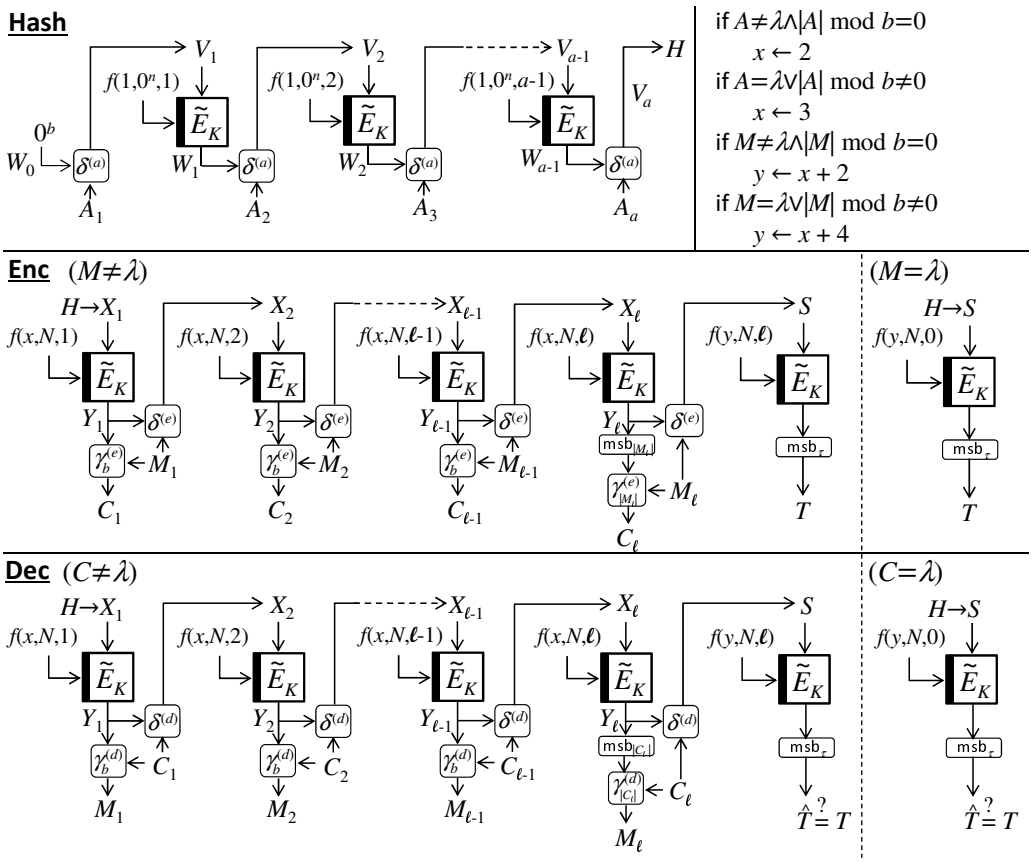

Figure 3: FBAE. $A_1, \ldots, A_a \xleftarrow{b} A$. $M_1, \ldots, M_\ell \xleftarrow{b} M$ (in the encryption algorithm) and $C_1, \ldots, C_\ell \xleftarrow{b} C$ (in the decryption algorithm).

if the output is distributed over a set $\mathcal{X}$, then the collision probability can be at most $1/|\mathcal{X}|$. Similar to the condition **B5**, the condition **B7** ensures that in the procedure of processing AD blocks, the internal state collision $\delta^{(a)}(W_i, A_i) = \delta^{(a)}(W'_i, A'_i)$ depends on the randomness of the TBC output W'_i. The conditions **B5**, **B7** are used to upper bound the authenticity advantage. The condition **B6** ensures that in the encryption and decryption procedures, no trivial collision occurs on the internal state values. Note that the conditions $(C \neq C' \wedge |C| = b \wedge |C'| < b \wedge Y = Y')$ and $(C \neq C' \wedge |C| < b \wedge |C'| = b \wedge Y = Y')$ in **B6** tolerate (possibly trivial) internal state collisions but the first element of f gets rid of the influence of the collisions. The condition **B8** is defined similarly.

It is easy to see that the classes of the functions $\gamma_l^{(e)}$, $\gamma_l^{(d)}$, $\delta^{(e)}$, $\delta^{(d)}$ with the conditions **B2**-**B6** cover the linear feedback functions ρ, ρ' with the conditions **A1**, **A2**, **A3**. The detail is given in the supplementary material A.

3.4 Lightweight Instantiations of $\gamma_l^{(e)}, \gamma_l^{(d)}, \delta^{(a)}, \delta^{(e)}, \delta^{(d)}, f$

In the section 5, we show that by hardware implementation, FBAE offers a lightweight AEAD scheme, combining with a lightweight TBC. In the implementation, the following

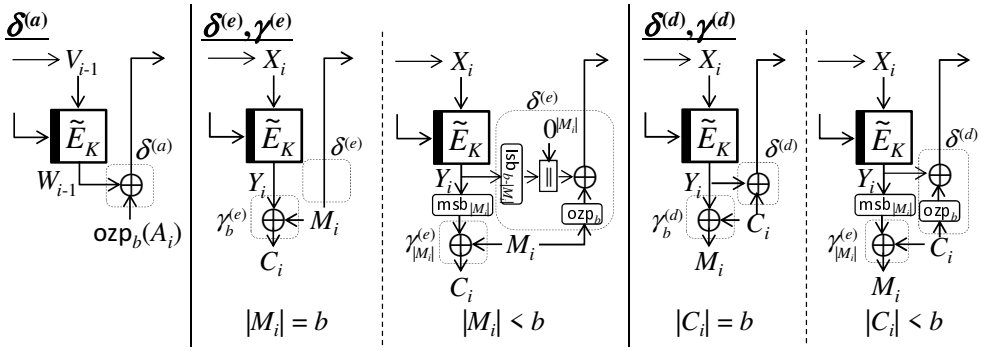

Figure 4: Lightweight Instantiations of $\delta^{(a)}, \delta^{(e)}, \delta^{(d)}, \gamma^{(e)}, \gamma^{(d)}$.

lightweight functions are used.

$$\gamma_l^{(e)}(Y_i, M_i) = Y_i \oplus M_i, \text{ where } 0 < l \leq b, \text{ and } Y_i, M_i \in \{0,1\}^l$$
$$\gamma_l^{(d)}(Y_i, C_i) = Y_i \oplus C_i, \text{ where } 0 < l \leq b, \text{ and } Y_i, C_i \in \{0,1\}^l$$
$$\delta^{(e)}(Y_i, M_i) = \mathsf{ozp}_b(M_i) \oplus \left(0^{|M_i|} \| \mathsf{lsb}_{b-|M_i|}(Y_i)\right), \text{ where } Y_i \in \{0,1\}^b, M_i \in \{0,1\}^{\leq b}.$$
$$\delta^{(d)}(Y_i, C_i) = Y_i \oplus \mathsf{ozp}_b(C_i), \text{ where } Y_i \in \{0,1\}^b, C_i \in \{0,1\}^{\leq b}.$$
$$\delta^{(a)}(W_i, A_i) = W_i \oplus \mathsf{ozp}_b(A_i), \text{ where } Y_i \in \{0,1\}^b, A_i \in \{\lambda\} \cup \{0,1\}^{\leq b}.$$

These functions are shown in Figure 4. FBAE with the above functions is called PFB (Plaintext FeedBack mode). PFB is shown in Figure 7 in the supplementary material C. It is easy to see that the above functions satisfy the conditions **B2**-**B8**. The detail is given in the supplementary material B.

The tweak function f, when $\mathcal{TW} := \{0,1\}^t$ and $\mathcal{N} := \{0,1\}^n$ such that $n + 3 + 1 \leq t$, is defined as

$$f(i, N, j) = (\mathsf{str}_3(i) \| N \| \mathsf{str}_{t-3-n}(j)),$$

which satisfies the condition **B1**.

4 Security of FBAE

The privacy and authenticity bounds of FBAE are given in the following theorem.

Theorem 2 *[] For* FBAE *with the conditions **B1**-**B8**, we have*

$$\mathbf{Adv}^{\mathsf{priv}}_{\mathsf{FBAE}[\widetilde{E}_K]}(\sigma_{\mathcal{E}}, t) \leq \mathbf{Adv}^{\mathsf{tprp}}_{\widetilde{E}_K}(\sigma_{\mathcal{E}}, t + O(\sigma_{\mathcal{E}})) \ ,$$
$$\mathbf{Adv}^{\mathsf{auth}}_{\mathsf{FBAE}[\widetilde{E}_K]}((q_{\mathcal{E}}, q_{\mathcal{D}}, \sigma), t) \leq \frac{q_{\mathcal{D}}}{2^\tau - 1/2^{b-\tau}} + \frac{q_{\mathcal{D}}}{2^b - 1} + \mathbf{Adv}^{\mathsf{tprp}}_{\widetilde{E}_K}(\sigma, t + O(\sigma)) \ .$$

The proof is given below.

4.1 Replacing the Keyed TBC E_K with a TRP $\widetilde{P}$

The keyed TBC $\widetilde{E}_K$ for $K \xleftarrow{\$} \mathcal{K}$ is replaced with a TRP $\widetilde{P} \xleftarrow{\$} \widetilde{\mathsf{Perm}}(\mathcal{TW}, \{0,1\}^b)$. By the replacement, we have

$$\mathbf{Adv}^{\mathsf{priv}}_{\mathsf{FBAE}[\widetilde{E}_K]}(\sigma_{\mathcal{E}}, t) \leq \mathbf{Adv}^{\mathsf{priv}}_{\mathsf{FBAE}[\widetilde{P}]}(\sigma_{\mathcal{E}}) + \mathbf{Adv}^{\mathsf{tprp}}_{\widetilde{E}_K}(\sigma_{\mathcal{E}}, t + O(\sigma_{\mathcal{E}})) \ , \quad (1)$$
$$\mathbf{Adv}^{\mathsf{naead}}_{\mathsf{FBAE}[\widetilde{E}_K]}((q_{\mathcal{E}}, q_{\mathcal{D}}, \sigma), t) \leq \mathbf{Adv}^{\mathsf{naead}}_{\mathsf{FBAE}[\widetilde{P}]}(q_{\mathcal{E}}, q_{\mathcal{D}}, \sigma) + \mathbf{Adv}^{\mathsf{tprp}}_{\widetilde{E}_K}(\sigma, t + O(\sigma)) \ . \quad (2)$$

Hereafter, the privacy and authenticity advantages of $\mathsf{FBAE}[\widetilde{P}]$ are upper bounded in Sections 4.2 and 4.3, respectively, where an adversary is a computationally unbounded algorithm and the complexity is solely measured by the numbers of queries. Without loss of generality, an adversary is deterministic.

4.2 Upper Bounding $\mathbf{Adv}^{\mathsf{priv}}_{\mathsf{FBAE}[\widetilde{P}]}(\sigma_{\mathcal{E}})$

The condition **B1** of the tweak function f ensures that all tweaks of $\widetilde{P}$ defined by encryption queries are distinct. Hence, the output blocks of $\widetilde{P}$ are chosen independently and uniformly at random from $\{0,1\}^b$. By the condition **B4**, all ciphertext blocks C_i defined by encryption queries are independently and uniformly distributed over $\{0,1\}^{|C_i|}$, and thus are indistinguishable from those defined by \$. Hence, we have

$$\mathbf{Adv}^{\mathsf{priv}}_{\mathsf{FBAE}[\widetilde{P}]}(\sigma_{\mathcal{E}}) = 0 \ . \tag{3}$$

4.3 Upper Bounding $\mathbf{Adv}^{\mathsf{auth}}_{\mathsf{FBAE}[\widetilde{P}]}(q_{\mathcal{E}}, q_{\mathcal{D}}, \sigma)$

Without loss of generality, assume that an adversary $\mathbf{A}$ aborts after $\mathbf{A}$ forges. Let forge_i be an event that at the i-th decryption query $\mathbf{A}$ forges (thus forge_i occurs as long as $\mathsf{forge}_1 \vee \mathsf{forge}_2 \vee \cdots \vee \mathsf{forge}_{i-1}$ does not occur). We then have

$$\mathbf{Adv}^{\mathsf{auth}}_{\mathsf{FBAE}[\widetilde{P}]}(q_{\mathcal{E}}, q_{\mathcal{D}}, \sigma) \le \sum_{i=1}^{q_{\mathcal{D}}} \Pr[\mathsf{forge}_i] \ .$$

Next, $\Pr[\mathsf{forge}_i]$ is upper bounded, where $i \in [q_{\mathcal{D}}]$. Values/variables defined at the i-th decryption query, except for the lengths a and ℓ, are denoted by using the superscript of (d). The lengths a and ℓ are denoted by a_d and ℓ_d, respectively. Similarly, for an encryption query $(N^{(e)}, A^{(e)}, M^{(e)})$, values/variables corresponding with the encryption query, except for the lengths a and ℓ, are denoted by using the superscript of (e). The lengths a and ℓ are denoted by a_e and ℓ_e, respectively. In this analysis, we consider the following types of decryption query.

- Type-1: For any previous encryption query $(N^{(e)}, A^{(e)}, M^{(e)})$,
$$N^{(e)} \neq N^{(d)} \vee y^{(e)} \neq y^{(d)} \vee \ell_e \neq \ell_d.$$
- Type-2: For some previous encryption query $(N^{(e)}, A^{(e)}, M^{(e)})$,
$$N^{(e)} = N^{(d)} \wedge y^{(e)} = y^{(d)} \wedge \ell_e = \ell_d.$$

Then,

$$\begin{aligned}\Pr[\mathsf{forge}_i] &= \Pr[\mathsf{forge}_i \wedge \mathsf{Type\text{-}1}] + \Pr[\mathsf{forge}_i \wedge \mathsf{Type\text{-}2}] \\ &= \Pr\left[\mathsf{forge}_i|\mathsf{Type\text{-}1}\right] \cdot \Pr\left[\mathsf{Type\text{-}1}\right] + \Pr\left[\mathsf{forge}_i|\mathsf{Type\text{-}2}\right] \cdot \Pr\left[\mathsf{Type\text{-}2}\right] \\ &\le \max\left\{\Pr\left[\mathsf{forge}_i|\mathsf{Type\text{-}1}\right], \Pr\left[\mathsf{forge}_i|\mathsf{Type\text{-}2}\right]\right\} \ .\end{aligned}$$

In Section 4.4, $\Pr\left[\mathsf{forge}_i|\mathsf{Type\text{-}1}\right]$ is analyzed, and in Section 4.5, $\Pr\left[\mathsf{forge}_i|\mathsf{Type\text{-}2}\right]$ is analyzed. The upper bounds (5), (6) give

$$\Pr[\mathsf{forge}_i] \le \frac{1}{2^\tau - 1/2^{b-\tau}} + \frac{1}{2^b - 1} \ .$$

Thus we have

$$\mathbf{Adv}^{\mathsf{auth}}_{\mathsf{FBAE}[\widetilde{P}]}(q_{\mathcal{E}}, q_{\mathcal{D}}, \sigma) \le q_{\mathcal{D}} \cdot \left(\frac{1}{2^\tau - 1/2^{b-\tau}} + \frac{1}{2^b - 1}\right) = \frac{q_{\mathcal{D}}}{2^\tau - 1/2^{b-\tau}} + \frac{q_{\mathcal{D}}}{2^b - 1} \ . \tag{4}$$

4.4 Analysis of $\Pr[\mathsf{forge}_i|\mathsf{Type\text{-}1}]$

Under the Type-1 decryption query and by the condition **B1**, the tweak $f(y^{(d)}, N^{(d)}, \ell_d)$, with which the TRP defines the tag $\hat{T}^{(d)}$, is distinct from all tweaks defined by the previous encryption queries, and is distinct from other tweaks defined by the i-th decryption query. Hence, $\hat{T}^{(d)}$ is uniformly distributed over $\{0,1\}^\tau$ and independent of the TRP outputs defined by the previous encryption queries and of other TRP outputs defied by the decryption query. Thus, we have

$$\Pr[\mathsf{forge}_i|\mathsf{Type\text{-}1}] \leq \frac{1}{2^\tau} \ . \tag{5}$$

4.5 Analysis of $\Pr[\mathsf{forge}_i|\mathsf{Type\text{-}2}]$

$\Pr\left[\hat{T}^{(d)} = T^{(d)} \middle| S^{(d)} \neq S^{(e)} \wedge \mathsf{Type\text{-}2}\right]$ and $\Pr\left[S^{(d)} = S^{(e)} \middle| \mathsf{Type\text{-}2}\right]$ are upper bounded, since

$$\begin{aligned}
\Pr[\mathsf{forge}_i|\mathsf{Type\text{-}2}] &= \Pr\left[\hat{T}^{(d)} = T^{(d)} \wedge S^{(d)} \neq S^{(e)} \middle| \mathsf{Type\text{-}2}\right] \\
&\quad + \Pr\left[\hat{T}^{(d)} = T^{(d)} \wedge S^{(d)} = S^{(e)} \middle| \mathsf{Type\text{-}2}\right] \\
&= \Pr\left[\hat{T}^{(d)} = T^{(d)} \middle| \mathsf{Type\text{-}2} \wedge S^{(d)} \neq S^{(e)}\right] \cdot \Pr\left[S^{(d)} \neq S^{(e)} \middle| \mathsf{Type\text{-}2}\right] \\
&\quad + \Pr\left[\hat{T}^{(d)} = T^{(d)} \middle| \mathsf{Type\text{-}2} \wedge S^{(d)} = S^{(e)}\right] \cdot \Pr\left[S^{(d)} = S^{(e)} \middle| \mathsf{Type\text{-}2}\right] \\
&\leq \Pr\left[\hat{T}^{(d)} = T^{(d)} \middle| \mathsf{Type\text{-}2} \wedge S^{(d)} \neq S^{(e)}\right] + \Pr\left[S^{(d)} = S^{(e)} \middle| \mathsf{Type\text{-}2}\right] \ .
\end{aligned}$$

The upper bounds (7), (10) give

$$\Pr[\mathsf{forge}_i|\mathsf{Type\text{-}2}] \leq \frac{1}{2^\tau - 1/2^{b-\tau}} + \frac{1}{2^b - 1} \ . \tag{6}$$

Upper Bounding $\Pr\left[\hat{T}^{(d)} = T^{(d)} \middle| \mathsf{Type\text{-}2} \wedge S^{(d)} \neq S^{(e)}\right]$

For the Type-2 decryption query, by $S^{(d)} \neq S^{(e)}$ and $f(y^{(e)}, N^{(e)}, \ell_e) = f(y^{(d)}, N^{(d)}, \ell_d)$ (the tweaks are the same), the output of the last TRP call by the decryption query is chosen uniformly at random from $\{0,1\}^b \backslash \{\widetilde{P}^{f(y^{(e)}, N^{(e)}, \ell_e)}(S^{(e)})\}$. We thus have

$$\Pr\left[\hat{T}^{(d)} = T^{(d)} \middle| \mathsf{Type\text{-}2} \wedge S^{(d)} \neq S^{(e)}\right] \leq \frac{2^{b-\tau}}{2^b - 1} = \frac{1}{2^\tau - 1/2^{b-\tau}} \ . \tag{7}$$

Upper Bounding $\Pr\left[S^{(d)} = S^{(e)} \middle| \mathsf{Type\text{-}2}\right]$

The condition of the Type-2 decryption query, $y^{(e)} = y^{(d)}$, is satisfied if and only if

$$\left(\left|A^{(d)}_{a_d}\right| = \left|A^{(e)}_{a_e}\right| = b\right) \vee \left(\left|A^{(d)}_{a_d}\right| < b \wedge \left|A^{(e)}_{a_e}\right| < b\right) \text{ and} \tag{8}$$

$$\left(\left|M^{(d)}_{\ell_d}\right| = \left|M^{(e)}_{\ell_e}\right| = b\right) \vee \left(\left|M^{(e)}_{\ell_e}\right| < b \wedge \left|M^{(d)}_{\ell_d}\right| < b\right). \tag{9}$$

Note that for the Type-2 decryption query, $\ell_e = \ell_d$ is satisfied. Let

$$I(A^{(d)}, A^{(e)}) = \left\{i \in [a_d] \middle| A^{(d)}_i \neq A^{(e)}_i\right\} \text{ and } I(C^{(d)}, C^{(e)}) = \left\{i \in [\ell_d] \middle| C^{(d)}_i \neq C^{(e)}_i\right\}$$

be sets of distinct blocks obtained from $(A^{(d)}, A^{(e)})$ and $(C^{(d)}, C^{(e)})$, respectively, where for $a_d < i$, $A^{(e)}_i := \lambda$.

Then,

$$\begin{aligned}
&\Pr\left[S^{(d)} = S^{(e)} \middle| \mathsf{Type\text{-}2}\right] \\
&= \underbrace{\Pr\left[S^{(d)} = S^{(e)} \wedge |I(C^{(d)}, C^{(e)})| = 0 \middle| \mathsf{Type\text{-}2}\right]}_{=:p_1} + \Pr\left[S^{(d)} = S^{(e)} \wedge |I(C^{(d)}, C^{(e)})| \geq 1 \middle| \mathsf{Type\text{-}2}\right] \\
&= p_1 + \underbrace{\Pr\left[S^{(d)} = S^{(e)} \middle| \mathsf{Type\text{-}2} \wedge |I(C^{(d)}, C^{(e)})| \geq 1\right]}_{=:p_2} \cdot \Pr\left[|I(C^{(d)}, C^{(e)})| \geq 1 \middle| \mathsf{Type\text{-}2}\right] \quad .
\end{aligned}$$

Regarding p_1, by the condition **B6**, for $Y, Y' \in \{0,1\}^b$ and $C \in \{0,1\}^l$, $\delta^{(e)}(Y, \gamma^{(d)}(Y, C)) = \delta^{(d)}(Y', C) \Rightarrow Y = Y'$. Hence, by $|I(C^{(d)}, C^{(e)})| = 0$, $S^{(d)} = S^{(e)} \Rightarrow H^{(d)} = H^{(e)}$ is satisfied, and we thus have

$$\begin{aligned}
p_1 &= \Pr\left[H^{(d)} = H^{(e)} \wedge |I(C^{(d)}, C^{(e)})| = 0 \middle| \mathsf{Type\text{-}2}\right] \\
&= \Pr\left[H^{(d)} = H^{(e)} \wedge a_e = a_d \wedge |I(C^{(d)}, C^{(e)})| = 0 \middle| \mathsf{Type\text{-}2}\right] \\
&\quad + \Pr\left[H^{(d)} = H^{(e)} \wedge a_e \neq a_d \wedge |I(C^{(d)}, C^{(e)})| = 0 \middle| \mathsf{Type\text{-}2}\right] \\
&= \underbrace{\Pr\left[H^{(d)} = H^{(e)} \middle| \mathsf{Type\text{-}2} \wedge a_e = a_d \wedge |I(C^{(d)}, C^{(e)})| = 0\right]}_{=:p_{1,1}} \\
&\quad \cdot \Pr\left[a_e = a_d \middle| \mathsf{Type\text{-}2} \wedge |I(C^{(d)}, C^{(e)})| = 0\right] \cdot \Pr\left[|I(C^{(d)}, C^{(e)})| = 0 \middle| \mathsf{Type\text{-}2}\right] \\
&\quad + \underbrace{\Pr\left[H^{(d)} = H^{(e)} \middle| \mathsf{Type\text{-}2} \wedge a_e \neq a_d \wedge |I(C^{(d)}, C^{(e)})| = 0\right]}_{=:p_{1,2}} \\
&\quad \cdot \Pr\left[a_e \neq a_d \middle| \mathsf{Type\text{-}2} \wedge |I(C^{(d)}, C^{(e)})| = 0\right] \cdot \Pr\left[|I(C^{(d)}, C^{(e)})| = 0 \middle| \mathsf{Type\text{-}2}\right] \\
&\leq \max\left\{p_{1,1}, p_{1,2}\right\} \cdot \Pr\left[|I(C^{(d)}, C^{(e)})| = 0 \middle| \mathsf{Type\text{-}2}\right] \quad .
\end{aligned}$$

Using these upper bounds, we have

$$\begin{aligned}
\Pr\left[S^{(d)} = S^{(e)} \middle| \mathsf{Type\text{-}2}\right] &\leq \max\left\{p_{1,1}, p_{1,2}\right\} \cdot \Pr\left[|I(C^{(d)}, C^{(e)})| = 0 \middle| \mathsf{Type\text{-}2}\right] \\
&\quad + p_2 \cdot \Pr\left[|I(C^{(d)}, C^{(e)})| \geq 1 \middle| \mathsf{Type\text{-}2}\right] \\
&\leq \max\left\{p_{1,1}, p_{1,2}, p_2\right\} \quad .
\end{aligned}$$

$p_{1,1}, p_{1,2}, p_2$ are upper bounded below.

- $p_{1,1} = \Pr\left[H^{(d)} = H^{(e)} \middle| \mathsf{Type\text{-}2} \wedge a_e = a_d \wedge |I(C^{(d)}, C^{(e)})| = 0\right]$ is upper bounded. Let $i = \max I(A^{(d)}, A^{(e)})$. Then, by the condition **B8**,

  $$H^{(e)} = H^{(d)} \Rightarrow V_i^{(e)} = V_i^{(d)}.$$

  If $i = 1$, then

  $$H^{(e)} = \delta^{(a)}(0^b, A_1^{(e)}) \text{ and } H^{(d)} = \delta^{(a)}(0^b, A_1^{(d)}).$$

  On the other hand, $A_1^{(e)} \neq A_1^{(d)}$ and the condition **B8** with the conditions in (8) (thus the last condition in **B8**, $A \neq A' \wedge |A| = b \wedge |A'| < b \wedge W = W'$, is ignored) imply

  $$H^{(e)} = \delta^{(a)}(0^b, A_1^{(e)}) \neq \delta^{(a)}(0^b, A_1^{(d)}) = H^{(d)}.$$

If $i \geq 2$, then

$$V_i^{(e)} = V_i^{(d)} \Leftrightarrow \delta^{(a)}\left(W_{i-1}^{(e)}, A_i^{(e)}\right) = \delta^{(a)}\left(W_{i-1}^{(d)}, A_i^{(d)}\right).$$

By $A_i^{(d)} \neq A_i^{(e)}$ and the condition **B8** with the conditions in (8), in order to satisfy the above equation, $W_{i-1}^{(d)} \neq W_{i-1}^{(e)}$ should be satisfied. As $W_{i-1}^{(d)}$ is chosen uniformly at random from $\{0,1\}^b \setminus \left\{W_{i-1}^{(e)}\right\}$ and $\delta^{(d)}\left(\cdot, A_i^{(d)}\right)$ is bijective from the condition **B7**, we have $p_{1,1} \leq 1/(2^b - 1)$.

- $p_{1,2} = \Pr\left[H^{(d)} = H^{(e)} \middle| \mathsf{Type\text{-}2} \wedge a_e \neq a_d \wedge |I(C^{(d)}, C^{(e)})| = 0\right]$ is upper bounded. Thus, the following equation is considered.

$$\delta^{(a)}\left(W_{a_d-1}^{(d)}, A_{a_d}^{(d)}\right) = H^{(d)} = H^{(e)} = \delta^{(a)}\left(W_{a_e-1}^{(e)}, A_{a_e}^{(e)}\right).$$

By $a_e \neq a_d$, the tweaks corresponding with the TRP outputs $W_{a_d-1}^{(d)}$ and $W_{a_e-1}^{(e)}$ are distinct. Thus, $W_{a_d-1}^{(d)}$ and $W_{a_e-1}^{(e)}$ are independently chosen, and at least one of them is chosen uniformly at random from $\{0,1\}^b$. (Note that for $x \in \{a, e\}$ if $a_x = 1$ then $H^{(x)} = \delta^{(a)}\left(0^b, A_1^{(x)}\right)$ which is a constant.) By the condition **B7**, at least one of $\delta^{(a)}\left(W_{a_d-1}^{(d)}, A_{a_d}^{(d)}\right)$ and $\delta^{(a)}\left(W_{a_e-1}^{(e)}, A_{a_e}^{(e)}\right)$ are uniformly distributed over $\{0,1\}^b$. Hence, we have $p_{1,2} \leq 1/2^b$.

- $p_2 = \Pr\left[S^{(d)} = S^{(e)} \middle| \mathsf{Type\text{-}2} \wedge |I(C^{(d)}, C^{(e)})| \geq 1\right]$ is upper bounded. Let $i = \max I(C^{(d)}, C^{(e)})$. Note that under the Type-2 decryption query, $\ell_e = \ell_d$ is satisfied. Then by the condition **B6**,

$$S_1^{(d)} = S_1^{(e)} \Leftrightarrow X_{i+1}^{(d)} = X_{i+1}^{(e)} \Leftrightarrow \delta^{(d)}\left(Y_i^{(d)}, C_i^{(d)}\right) = \delta^{(e)}\left(Y_i^{(e)}, M_i^{(e)}\right),$$

where $M_i^{(e)} = \gamma^{(d)}(\mathsf{msb}_{|C_i^{(e)}|}(Y_i^{(e)}), C_i^{(e)})$. $C_i^{(d)} \neq C_i^{(e)}$ and the condition **B6** with (9) imply $Y_i^{(d)} \neq Y_i^{(e)}$, and thus we have $X_i^{(d)} \neq X_i^{(e)}$. Hence,

$$p_2 \leq \Pr\left[\delta^{(e)}\left(Y_i^{(e)}, M_i^{(e)}\right) = \delta^{(d)}\left(Y_i^{(d)}, C_i^{(d)}\right) \middle| \mathsf{Type\text{-}2} \wedge X_i^{(d)} \neq X_i^{(e)} \wedge |I(C^{(d)}, C^{(e)})| \geq 1\right].$$

By $X_i^{(d)} \neq X_i^{(e)}$, $Y_i^{(d)}$ is chosen uniformly at random from $\{0,1\}^b \setminus \{Y_i^{(e)}\}$. As $\delta^{(d)}\left(\cdot, C_i^{(d)}\right)$ is bijective from the condition **B5**, we have $p_2 \leq 1/(2^b - 1)$.

The above upper bounds give

$$\Pr\left[S^{(d)} = S^{(e)} \middle| \mathsf{Type\text{-}2}\right] \leq \frac{1}{2^b - 1}. \tag{10}$$

4.6 Conclusion of the Proof

Putting the upper bound (3) into (1), and the upper bound (4) into (2) give those in Theorem 2.

5 Implementation

The performance of PFB is evaluated through concrete hardware implementations. For the lightweight TBC, we use a variant of SKINNY having the 64-bit block length and 192-bit

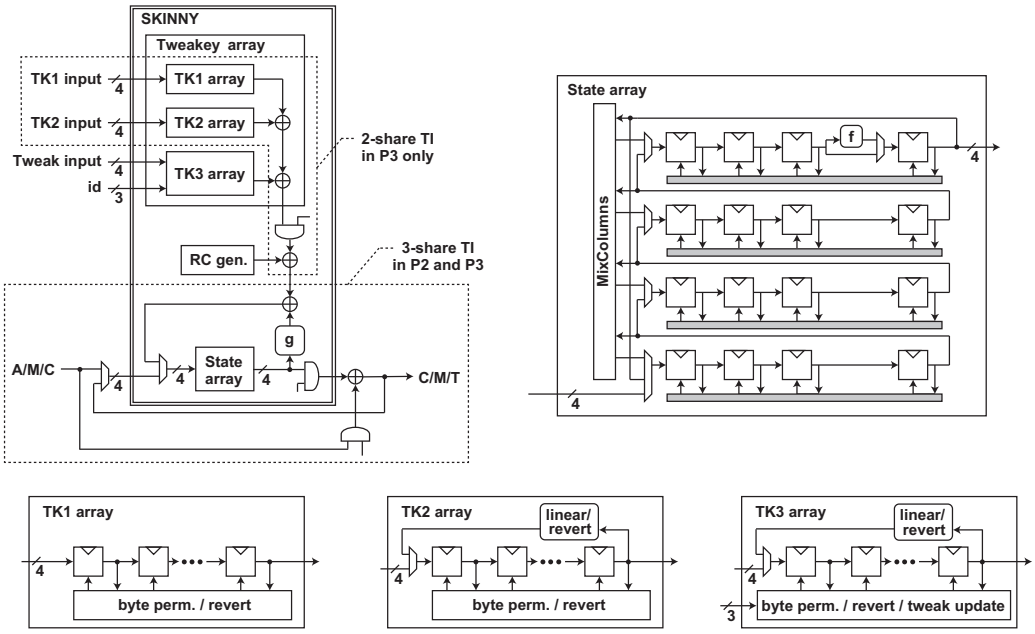

Figure 5: PFB[SKINNY] hardware architecture.

tweakey, i.e., SKINNY-64-192 [BJK+16]. Its performance is compared with the state-of-the-art alternative having the same level of security: SAEB [NMSS18] instantiated with the lightweight block cipher GIFT-128-128 [BPP+17]. In the following, SKINNY-64-192 and GIFT-128-128 are simply referred to as SKINNY and GIFT. In addition, a mode of operation M instantiated with a primitive P is described as M[P].

Design Policy For a fair comparison, PFB[SKINNY] and SAEB[GIFT] are implemented under the same design policy. They are designed as co-processors aiming at accelerating the main time-consuming part of AD processing, encryption, and decryption. Meanwhile, the co-processors expect an external controller for handling special cases such as padding and the final-block processing. In order to avoid a hidden cost, the designs hold a key, nonce, and tweak during their lifetimes. In other words, there is no need for storing them in external registers and feeding them multiple times. This policy affect the implementation of on-the-fly key scheduling as we will see in the next section. The circuit area has the highest priority in optimization. The designs are described by a hardware description language (HDL) in register-transfer level (RTL). We do not make netlist-level optimization except scan flip-flops commonly used for compact implementations [MPL+11]; the standard cells for scan flip-flops are explicitly instantiated in HDL. For SCA-protected implementations, we consider TI secure up to the first-order attacks.

5.1 PFB[SKINNY]

SKINNY uses three distinct 64-bit states namely **TK1**, **TK2**, and **TK3** for tweakey schedule. In this particular design, **TK3** stores a 64-bit tweak. The remaining **TK1** and **TK2** store a 128-bit secret key.

Fig. 5 shows the hardware architecture of PFB[SKINNY]. As shown in Fig. 5, PFB[SKINNY] is realized as a thin wrapper of the SKINNY implementation; the additional components are 4-bit XOR, selector, and AND gate only.

The SKINNY implementation follows the conventional nibble-serial architecture [BJK+16], but the tweakey-schedule implementation is designed from scratch. The implementations called the **TK1**, **TK2**, and **TK3** arrays are based on a common architecture comprising an array of scan flip-flops and integrated on-the-fly key scheduling [MPL+11] as shown in Fig. 5. However, the changes made by the on-the-fly key scheduling should be reverted to begin the next TBC call without feeding the same key again. Since SKINNY schedules **TK1**, **TK2**, and **TK3** by a nibble permutation and a nibble-wise linear transformation for each round, we can obtain efficient inverse maps that revert the final tweakey state to the initial one. Such inverse maps are integrated to the **TK1**, **TK2**, and **TK3** arrays along with the forward on-the-fly scheduling.

Based on (3.4), the 64-bit tweak is given by $\mathsf{id}\|N\|\mathsf{ctr}$: a 3-bit number distinguishing the operations $\mathsf{id} = \mathsf{str}_3(i)$, 45-bit nonce N, and a current block number realized by a 16-bit counter $\mathsf{ctr} = \mathsf{str}_{16}(j)$. id and ctr are updated for each TBC call. For an efficient computation, the **TK3** array integrates the circuit for (i) changing id and (ii) incrementing and clearing the counter ctr. Using the above functionality, a user needs to feed $\mathsf{id}\|N\|\mathsf{ctr}$ only once for a given nonce N.

Single SKINNY round uses 16 cycles, and thus SKINNY comprising 40 rounds finishes in $16 \times 40 = 640$ cycles. We need an additional 1 cycle for updating a tweak stored in the **TK3** array for the next TBC call. As a result, a 64-bit message or ciphertext block is consumed in 641 cycles.

5.2 SAEB[GIFT]

Fig. 6 shows the hardware architecture of SAEB[GIFT]. The overall architecture is based on the conventional design [NMSS18], but the shift registers for synchronization are removed considering the design policy. It is also realized as a thin wrapper of the underlying GIFT implementation.

The GIFT implementation is based on the nibble-serial architecture [BPP+17], but the key array is redesigned to efficiently reverting the changes made by on-the-fly key scheduling. Similar to SKINNY, GIFT has a linear key scheduling algorithm, and thus we can obtain an efficient inverse map that revert the final key state to the initial one. The key array is designed with a 32-bit datapath to efficiently integrate the inverse key-schedule map (the function block labeled with "revert") as shown in Fig. 6.

The S-box is split into two stages namely g and f for TI following the conventional work [GJC+17]. Consequently, a single GIFT round uses 33 cycles for 32 S-box look-ups and one pipeline latency. As a result, The 40-round operation of GIFT requires $33 \times 40 = 1,320$ cycles.

5.3 Threshold Implementation

There is an option between protected and unprotected key/tweakey schedule. Conventional attacks such as differential power analysis (DPA) [KJJ99] cannot be used to attack key schedule that is independent of an attacker-controllable input e.g., plaintext or ciphertext. That is not generally true for TBCs, but SKINNY has the same property as far as the attacker-controllable tweak is placed in **TK3**, which is scheduled independently of **TK1** and **TK2**. Consequently, some previous works prioritize circuit area and use unprotected key-schedule implementations [BJK+16, PMK+11, UHA17]. Meanwhile, if we consider a profiling attack on key/tweakey schedule, it is also reasonable to choose a protected key-schedule implementation. Considering the cost-security trade-off, we implement PFB[SKINNY] and SAEB[GIFT] with three different profiles: (**P1**) the unprotected implementation, (**P2**) TI with the unprotected key schedule and (**P3**) TI with the protected key schedule.

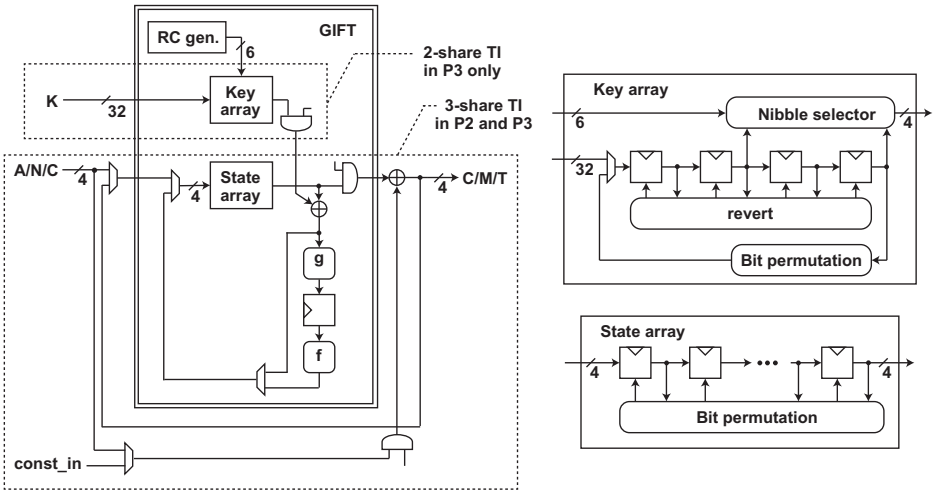

Figure 6: SAEB[GIFT] hardware architecture.

Table 2: The number of registers for implementing SKINNY and GIFT in different profiles.

Target	Profile	TI/State	TI/Key	State	Tweak/key	Total
SKINNY	(**P1**)	—	—	64	192	256
GIFT	(**P1**)	—	—	128	128	256
SKINNY	(**P2**)	✓	—	192	192	384
GIFT	(**P2**)	✓	—	384	128	512
SKINNY	(**P3**)	✓	✓	192	320	512
GIFT	(**P3**)	✓	✓	384	256	640

Table 2 summarizes the number of registers needed for the SKINNY and GIFT implementations for the different profiles. In (**P1**), both SKINNY and GIFT use 256 bits in total. In (**P2**), on the other hand, SKINNY use the smaller number of registers, 384 bits compared with 512 bits, because of the smaller block length. SKINNY still has a better performance in (**P3**) because key/tweakey schedule can be shared more efficiently. Since both GIFT and SKINNY have linear key/tweakey schedules, they can be realized with only two shares. Moreover, there is no need for protecting **TK3** of SKINNY that stores a public tweak. As a result, SKINNY and GIFT use 512 and 684 bits in (**P3**), respectively.

We use the formulae for the 3-share uniform S-boxes for SKINNY and GIFT from the conventional works [BJK+16] and [GJC+17], respectively. TI is implemented by duplicating the state/key/tweakey arrays and replacing the decomposed S-boxes (f and g) with their shared maps. Fig. 5 and 6 show the boundaries of sharing for each profile.

5.4 Performance Evaluation and Comparison

The designs are synthesized with the NanGate 45-nm standard cell library [Nan] using Synopsys Design Compiler while preserving the module hierarchy. Table 3 shows the breakdown of the post-synthesis performances.

We first discuss the unprotected implementations (**P1**). The circuit area of PFB[SKINNY] and SAEB[GIFT] are 3,111 and 2,761 [GE], respectively. SKINNY and GIFT dominate the circuit area of PFB[SKINNY] and SAEB[GIFT], The additional costs for the mode of operations are limited. The sizes of the state and key arrays are almost proportional to their register sizes, e.g., the 64-bit SKINNY state array (532 [GE]) is almost a half the size of

Table 3: Breakdown of the post-synthesis circuit area of PFB[SKINNY] and SAEB[GIFT].

Target	Component	Circuit area [GE]		
		(**P1**)	(**P2**)	(**P3**)
PFB[SKINNY]	Total	3,111	4,492	5,858
	Total/SKINNY	2,956	4,284	5,649
	Total/SKINNY/State array	532	1,757	1,757
	Total/SKINNY/Tweakey array	2,062	2,062	3,419
SAEB[GIFT]	Total	2,761	5,037	6,229
	Total/GIFT	2,541	4,756	5,947
	Total/GIFT/State array	975	2,925	2,925
	Total/GIFT/Key array	1201	1,226	2,410

the 128-bit GIFT state array (975 [GE]).

Although the PFB[SKINNY] implementation is larger than that of SAEB[GIFT] by 350 [GE], this is a positive result because (i) GIFT is known to have a better performance compared with SKINNY [BJK+16] and (ii) lightweight TBC is an emerging technology compared with lightweight block cipher. It is also note that PFB[SKINNY] is twice as fast as that of SAEB[GIFT]: PFB[SKINNY] and SAEB[GIFT] consume a 64-bit message/ciphertext block using 640 and $1,320$ cycles, respectively. Moreover, PFB has parallelizable encryption as discussed in Sect. 3.

Table 4 shows performance comparison with previous implementations. The unprotected implementations of SAEB[GIFT] and PFB[SKINNY] are smaller than previous implementations of AES-based AEs (SAEB[AES128] [NMSS18], CLOC[AES128], SILC[AES128], OTR[AES128] [BBM16]). The bit-serial Ascon implementation without an interface has a smaller circuit area of $2,570$ [GE] [GWDE15]; however, the implementation needs an additional 128-bit key register to run another encryption/decryption with the same key. If we add the size of the key register (640 [GE] for 5 [GE/bit]) to $2,570$ [GE], the Ascon implementation has the similar circuit size compared with that of PFB[SKINNY]. We also note that the Ascon implementation with an interface including a 128-bit key register has $3,750$ [GE].

We then discuss the protected implementations. With (**P2**), the PFB[SKINNY] implementation uses $4,492$ [GE] which is smaller than that of SAEB[GIFT] ($5,037$ [GE]). That is explained by the smaller number of registers summarized in Table 2. PFB[SKINNY] is still advantageous with (**P3**): the circuit areas of PFB[SKINNY] and SAEB[GIFT] are $5,858$ and $6,229$ [GE], respectively. The protected PFB implementations are smaller than that of Ascon [GWDE15]) and Ketje [ANR18] in conventional works as shown in Table 4. That is also explained by the number of registers. The sponge-based AEs have a relatively large state (384 bits for Ascon and 200 bits for Ketje-JR) that should be protected with three shares.

In summary, the unprotected PFB[SKINNY] implementation is competitive against the unprotected SAEB[GIFT] implementations and other conventional implementations. The benefit of a small block length, enable by PFB, becomes even larger with TI in which the number of registers are multiplied as shown in Table 2. As a result, the protected PFB[SKINNY] implementation outperforms that of SAEB[GIFT], Ascon [GWDE15], and Ketje [ANR18].

Table 4: Performance comparison; latency is that of a single call of a primitive (block cipher, tweakable block cipher, or permutation).

Target	TI	Area [GE]	Latency [cycles]	Standard-cell library	Ref.
PFB[SKINNY] (**P1**)	—	3,111	641	NanGate 45-nm	**Ours**
SAEB[GIFT] (**P1**)	—	2,761	1,320	NanGate 45-nm	**Ours**
SAEB[AES128]	—	3,502	231	NanGate 45-nm	[NMSS18]
CLOC[AES128]	—	4,310	210	STMicro. 90-nm	[BBM16]
SILC[AES128]	—	4,220	210	STMicro. 90-nm	[BBM16]
OTR[AES128]	—	6,770	210	STMicro. 90-nm	[BBM16]
Ascon w/o IF	—	2,570	3,072	UMC 90-nm	[GWDE15]
Ascon w/ IF	—	3,750	3,072	UMC 90-nm	[GWDE15]
Deoxys (Round*)	—	11,936	14	UMC 180-nm	[JNPS16]
Ketje-JR	—	5,447	16	NanGate 45-nm	[ANR18]
PFB[SKINNY] (**P2**)	✓	4,492	641	NanGate 45-nm	**Ours**
PFB[SKINNY] (**P3**)	✓	5,858	641	NanGate 45-nm	**Ours**
SAEB[GIFT] (**P2**)	✓	5,037	1,320	NanGate 45-nm	**Ours**
SAEB[GIFT] (**P3**)	✓	6,229	1,320	NanGate 45-nm	**Ours**
Ascon w/o IF	✓	7,970	3,072	UMC 90-nm	[GWDE15]
Ascon w/ IF	✓	9,190	3,072	UMC 90-nm	[GWDE15]
Ketje-JR	✓	18,335	16	NanGate 45-nm	[ANR18]

References

[ANR18] Victor Arribas, Svetla Nikova, and Vincent Rijmen. Guards in Action: First-Order SCA Secure Implementations of Ketje Without Additional Randomness. In *DSD 2018*, pages 492–499. IEEE Computer Society, 2018.

[BBI+15] Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: A Block Cipher for Low Energy. In *ASIACRYPT 2015*, volume 9453 of *LNCS*, pages 411–436. Springer, 2015.

[BBM16] Subhadeep Banik, Andrey Bogdanov, and Kazuhiko Minematsu. Low-area hardware implementations of CLOC, SILC and AES-OTR. In *HOST 2016*, pages 71–74. IEEE Computer Society, 2016.

[BCG+12] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications - Extended Abstract. In *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 208–225. Springer, 2012.

[BJK+16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS. In *CRYPTO 2016*, volume 9815 of *LNCS*, pages 123–153. Springer, 2016.

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In *CHES 2007*, volume 4727 of *LNCS*, pages 450–466. Springer, 2007.

[BL16] Karthikeyan Bhargavan and Gaëtan Leurent. On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 456–467. ACM, 2016.

[BPP+17] Subhadeep Banik, Sumit Kumar Pandey, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, and Yosuke Todo. GIFT: A Small Present - Towards Reaching the Limit of Lightweight Encryption. In *CHES 2017*, volume 10529 of *LNCS*, pages 321–345. Springer, 2017.

[BSS+13] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK Families of Lightweight Block Ciphers. *IACR Cryptology ePrint Archive*, 2013:404, 2013.

[CIMN17] Avik Chakraborti, Tetsu Iwata, Kazuhiko Minematsu, and Mridul Nandi. Blockcipher-Based Authenticated Encryption: How Small Can We Go? In *CHES 2017*, volume 10529 of *LNCS*, pages 277–298. Springer, 2017.

[GJC+17] Naina Gupta, Arpan Jati, Anupam Chattopadhyay, Somitra Kumar Sanadhya, and Donghoon Chang. Threshold Implementations of GIFT: A Trade-off Analysis. *IACR Cryptology ePrint Archive*, 2017:1040, 2017.

[GPPR11] Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw. The LED Block Cipher. In *CHES 2011*, volume 6917 of *LNCS*, pages 326–341. Springer, 2011.

[GWDE15] Hannes Groß, Erich Wenger, Christoph Dobraunig, and Christoph Ehrenhöfer. Suit up! - Made-to-Measure Hardware Implementations of ASCON. In *DSD 2015*, pages 645–652. IEEE Computer Society, 2015.

[IKMP19a] Tetsu Iwata, Mustafa Khairallah, Kazuhiko Minematsu, and Thomas Peyrin. Personal communication, 2019.

[IKMP19b] Tetsu Iwata, Mustafa Khairallah, Kazuhiko Minematsu, and Thomas Peyrin. Romulus v1.0, round 1 candidate of the lightweight crypto standardization process, 2019.

[IMPS17] Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, and Yannick Seurin. ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication. In *CRYPTO 2017*, volume 10403 of *LNCS*, pages 34–65. Springer, 2017.

[Iwa06] Tetsu Iwata. New Blockcipher Modes of Operation with Beyond the Birthday Bound Security. In *FSE 2006*, volume 4047 of *LNCS*, pages 310–327. Springer, 2006.

[Iwa08] Tetsu Iwata. Authenticated Encryption Mode for Beyond the Birthday Bound Security. In *AFRICACRYPT 2008*, volume 5023 of *LNCS*, pages 125–142. Springer, 2008.

[JNPS16] Jérémy Jean, Ivica Nikolic, Thomas Peyrin, and Yannick Seurin. Deoxys v1.41. Submitted to the CAESAR competition. 2016.

[KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In *CRYPTO '99*, volume 1666 of *LNCS*, pages 388–397. Springer, 1999.

[KR11] Ted Krovetz and Phillip Rogaway. The Software Performance of Authenticated-Encryption Modes. In *FSE 2011*, volume 6733 of *LNCS*, pages 306–327. Springer, 2011.

[LS13] Rodolphe Lampe and Yannick Seurin. Tweakable Blockciphers with Asymptotically Optimal Security. In *FSE 2013*, volume 8424 of *LNCS*, pages 133–151. Springer, 2013.

[LST12] Will Landecker, Thomas Shrimpton, and R. Seth Terashima. Tweakable Blockciphers with Beyond Birthday-Bound Security. In *CRYPTO 2012*, volume 7417 of *LNCS*, pages 14–30. Springer, 2012.

[MI15] Kazuhiko Minematsu and Tetsu Iwata. Tweak-Length Extension for Tweakable Blockciphers. In *IMACC 2015*, volume 9496 of *LNCS*, pages 77–93. Springer, 2015.

[Min14] Kazuhiko Minematsu. Parallelizable Rate-1 Authenticated Encryption from Pseudorandom Functions. In *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 275–292. Springer, 2014.

[MPL+11] Amir Moradi, Axel Poschmann, San Ling, Christof Paar, and Huaxiong Wang. Pushing the limits: A very compact and a threshold implementation of AES. In *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, pages 69–88, 2011.

[Nan] NanGate. NanGate FreePDK45 open cell library. http://www.nangate.com.

[NIS] NIST. Submission requirements and evaluation criteria for the lightweight cryptography standardization process.

[NMSS18] Yusuke Naito, Mitsuru Matsui, Takeshi Sugawara, and Daisuke Suzuki. SAEB: A Lightweight Blockcipher-Based AEAD Mode of Operation. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2018(2):192–217, 2018.

[NRR06] Svetla Nikova, Christian Rechberger, and Vincent Rijmen. Threshold Implementations Against Side-Channel Attacks and Glitches. In *ICICS 2006*, volume 4307 of *LNCS*, pages 529–545. Springer, 2006.

[NRS11] Svetla Nikova, Vincent Rijmen, and Martin Schläffer. Secure Hardware Implementation of Nonlinear Functions in the Presence of Glitches. *J. Cryptology*, 24(2):292–321, 2011.

[PMK+11] Axel Poschmann, Amir Moradi, Khoongming Khoo, Chu-Wee Lim, Huaxiong Wang, and San Ling. Side-Channel Resistant Crypto for Less than 2, 300 GE. *J. Cryptology*, 24(2):322–345, 2011.

[PS16] Thomas Peyrin and Yannick Seurin. Counter-in-Tweak: Authenticated Encryption Modes for Tweakable Block Ciphers. In *CRYPTO 2016*, volume 9814 of *LNCS*, pages 33–63. Springer, 2016.

[SIH+11] Kyoji Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo Shirai. Piccolo: An Ultra-Lightweight Blockcipher. In *CHES 2011*, volume 6917 of *LNCS*, pages 342–357. Springer, 2011.

[SMMK13] Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, and Eita Kobayashi. TWINE: A Lightweight Block Cipher for Multiple Platforms. In *SAC 2012*, volume 7707 of *LNCS*, pages 339–354. Springer, 2013.

[SSA+07] Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. The 128-Bit Blockcipher CLEFIA (Extended Abstract). In *FSE 2007*, volume 4593 of *LNCS*, pages 181–195. Springer, 2007.

[UHA17] Rei Ueno, Naofumi Homma, and Takafumi Aoki. Toward More Efficient DPA-Resistant AES Hardware Architecture Based on Threshold Implementation. In *COSADE 2017*, volume 10348 of *LNCS*, pages 50–64. Springer, 2017.

Supplementary Material

A The Linear Functions ρ, ρ' with A1, A2, A3 Satisfy B2-B6

We show that the linear feedback functions ρ, ρ' with the conditions **A1**, **A2**, **A3** satisfy the conditions **B2**-**B6**. As iCOFB deals with b-bit blocks, we assume that the input/output sizes of the functions $(\gamma_b^{(e)}, \gamma_b^{(d)}, \delta^{(e)}, \delta^{(d)})$ are all b bits. Note that for the linear feedback functions (ρ, ρ'), the functions $(\gamma_b^{(e)}, \gamma_b^{(d)}, \delta^{(e)}, \delta^{(d)})$ are expressed as

$$\gamma_b^{(e)}(Y, M) = E_{2,1} \cdot Y + E_{2,2} \cdot M, \qquad \delta^{(e)}(Y, M) = E_{1,1} \cdot Y + E_{1,2} \cdot M,$$
$$\gamma_b^{(d)}(Y, C) = D_{2,1} \cdot Y + D_{2,2} \cdot C, \qquad \delta^{(d)}(Y, C) = D_{1,1} \cdot Y + D_{1,2} \cdot C.$$

The Condition B2

For any $Y \in \{0,1\}^b$, as $E_{2,2}$ is invertible, $\gamma_b^{(e)}(Y, \cdot)$ is bijective. For any $Y \in \{0,1\}^b, M \in \{0,1\}^b$,

$$\begin{aligned}\gamma_b^{(d)}(Y, \gamma_b^{(e)}(Y, M)) &= D_{2,1} \cdot Y + D_{2,2} \cdot \gamma_b^{(e)}(Y, M) \\ &= D_{2,1} \cdot Y + D_{2,2} \cdot (E_{2,1} \cdot Y + E_{2,2} \cdot M) \\ &= E_{2,2}^{-1} E_{2,1} \cdot Y + E_{2,2}^{-1} \cdot (E_{2,1} \cdot Y + E_{2,2} \cdot M) \\ &= M.\end{aligned}$$

The Condition B3

For any $M, Y \in \{0,1\}^b$,

$$\begin{aligned}\delta^{(d)}(Y, \gamma_b^{(e)}(Y, M)) &= D_{1,1} \cdot Y + D_{1,2} \cdot \gamma_b^{(e)}(Y, M) \\ &= D_{1,1} \cdot Y + D_{1,2} \cdot (E_{2,1} \cdot Y + E_{2,2} \cdot M) \\ &= (E_{1,1} + E_{1,2} E_{2,2}^{-1} E_{2,1}) \cdot Y + (E_{1,2} E_{2,2}^{-1}) \cdot (E_{2,1} \cdot Y + E_{2,2} \cdot M) \\ &= E_{1,1} \cdot Y + E_{1,2} \cdot M = \delta^{(e)}(Y, M).\end{aligned}$$

The Condition B4

For any plaintext block M, as $E_{2,1}$ is invertible (from the condition **A1**), the linear function $\gamma_b^{(e)}(\cdot, M)$ is bijective.

The Condition B5

The analysis is the same as the above analysis. For any ciphertext block C, as $D_{1,1}$ is invertible (from the condition **A3**), the linear function $\delta^{(d)}(\cdot, C)$ is bijective.

The Condition B6

Since ρ, ρ' are defined only for b-bit blocks, we can ignore the conditions $(C \neq C' \wedge Y = Y' \wedge |C| = b \wedge |C'| < b)$ and $(C \neq C' \wedge Y = Y' \wedge |C| < b \wedge |C'| = b)$ in **B6**. We consider the contraposition of the condition **B6** is considered, and thus consider two cases regarding ciphertext blocks C, C' and output block Y, Y'.

1. $C \neq C'$ and $Y = Y'$.

2. $C = C'$ and $Y \neq Y'$.

For each case, we show that

$$\delta^{(e)}(Y, \gamma_b^{(d)}(Y, C)) \neq \delta^{(d)}(Y', C').$$

These functions are of the forms:

$$\begin{aligned}
\delta^{(e)}(Y, \gamma_b^{(d)}(Y, C)) &= E_{1,1} \cdot Y + E_{1,2} \cdot \gamma_b^{(d)}(Y, C) \\
&= E_{1,1} \cdot Y + E_{1,2} \cdot (D_{2,1} \cdot Y + D_{2,2} \cdot C) \\
&= (E_{1,1} + E_{1,2} \cdot D_{2,1}) \cdot Y + E_{1,2} \cdot D_{2,2} \cdot C \\
&= (E_{1,1} + E_{1,2} \cdot E_{2,2}^{-1} \cdot E_{2,1}) \cdot Y + E_{1,2} \cdot E_{2,2}^{-1} \cdot C \\
&= D_{1,1} \cdot Y + D_{1,2} \cdot C, \\
\delta^{(d)}(Y', C') &= D_{1,1} \cdot Y' + D_{1,2} \cdot C'.
\end{aligned}$$

As $D_{1,1}$ and $D_{1,2}$ are invertible from the conditions **A2** and **A3**, for each of the above cases, we have

$$\delta^{(e)}(Y, \gamma_b^{(d)}(Y, C)) \neq \delta^{(d)}(Y', C').$$

B The PFB Functions $\gamma_l^{(e)}, \gamma_l^{(d)}, \delta^{(e)}, \delta^{(d)}, \delta^{(a)}$ Satisfy B2-B8

We show that the functions of PFB given in Section 3.4 satisfy the conditions **B2**-**B8**. The functions $\gamma_l^{(e)}, \gamma_l^{(d)}, \delta^{(e)}, \delta^{(d)}$ are of the forms:

$$\begin{aligned}
&\gamma_l^{(e)}(Y, M) = Y \oplus M, \text{ where } 0 < l \leq b, \text{ and } Y, M \in \{0,1\}^l \\
&\gamma_l^{(d)}(Y, C) = Y \oplus C, \text{ where } 0 < l \leq b, \text{ and } Y, C \in \{0,1\}^l \\
&\delta^{(e)}(Y, M) = \mathsf{ozp}_b(M) \oplus \left(0^{|M|} \| \mathsf{lsb}_{b-|M|}(Y)\right), \text{ where } Y \in \{0,1\}^b, M \in \{0,1\}^{\leq b}. \\
&\delta^{(d)}(Y, C) = Y \oplus \mathsf{ozp}_b(C), \text{ where } Y \in \{0,1\}^b, C \in \{0,1\}^{\leq b}. \\
&\delta^{(a)}(W, A) = W \oplus \mathsf{ozp}_b(A), \text{ where } Y \in \{0,1\}^b, A \in \{\lambda\} \cup \{0,1\}^{\leq b}.
\end{aligned}$$

The Condition B2

It is easy to see that for any $Y \in \{0,1\}^l$, $\gamma_l^{(e)}(Y, \cdot)$ is bijective and $\gamma_l^{(d)}(Y, \cdot)$ is the inverse of $\gamma_l^{(e)}(Y, \cdot)$.

The Condition B3

Let $M \in \{0,1\}^l$, and $Y \in \{0,1\}^b$. Then

$$\begin{aligned}
\delta^{(d)}(Y, \gamma_l^{(e)}(\mathsf{msb}_l(Y), M)) &= Y \oplus \mathsf{ozp}_b\left(\gamma_l^{(e)}(\mathsf{msb}_l(Y), M)\right) \\
&= Y \oplus \mathsf{ozp}_b\left(\mathsf{msb}_l(Y) \oplus M\right) \\
&= \mathsf{ozp}_b(M) \oplus \left(0^l \| \mathsf{lsb}_{b-l}(Y)\right).
\end{aligned}$$

Hence, we have $\delta^{(e)}(Y, M) = \delta^{(d)}(Y, \gamma_l^{(e)}(\mathsf{msb}_l(Y), M))$.

The Condition B4

It is easy to see that for any $M \in \{0,1\}^l$, $\gamma_l^{(e)}(\cdot, M)$ is bijective.

The Condition B5

It is easy to see that for any $C \in \{0,1\}^{\leq b}$, $\delta^{(d)}(\cdot, C)$ is bijective.

The Condition B6

The contraposition of the condition **B6** is considered, i.e.,

$$\begin{aligned}&(C = C' \wedge Y \neq Y')\\ \vee&(C \neq C' \wedge Y = Y' \wedge |C| < b \wedge |C'| < b)\\ \vee&(C \neq C' \wedge Y = Y' \wedge |C| = b \wedge |C'| = b) \Rightarrow \delta^{(e)}(Y, \gamma^{(d)}_{|C|}(\mathsf{msb}_{|C|}(Y), C)) \neq \delta^{(d)}(Y', C').\end{aligned}$$

For $Y \in \{0,1\}^b, C \in \{0,1\}^{\leq b}$, the functions are of the forms:

$$\begin{aligned}\delta^{(e)}(Y, \gamma^{(d)}_{|C|}(\mathsf{msb}_{|C|}(Y), C)) &= \mathsf{ozp}_b(\gamma^{(d)}_{|C|}(\mathsf{msb}_{|C|}(Y), C)) \oplus \left(0^{|C|} \| \mathsf{lsb}_{b-|C|}(Y)\right)\\ &= \mathsf{ozp}_b(\mathsf{msb}_{|C|}(Y) \oplus C)) \oplus \left(0^{|C|} \| \mathsf{lsb}_{b-|C|}(Y)\right)\\ &= Y \oplus \mathsf{ozp}_b(C),\\ \delta^{(d)}(Y', C') &= Y' \oplus \mathsf{ozp}_b(C').\end{aligned}$$

Hence, the condition **B6** is satisfied.

The Condition B7

It is easy to see that for any $A \in \{0,1\}^{\leq b}$, $\delta^{(a)}(\cdot, A)$ is bijective.

The Condition B8

The contraposition of the condition **B8** is considered, i.e.,

$$\begin{aligned}&(A = A' \wedge W \neq W')\\ \vee&(A \neq A' \wedge W = W' \wedge |A| < b \wedge |A'| < b)\\ \vee&(A \neq A' \wedge W = W' \wedge |A| = b \wedge |A'| = b) \Rightarrow \delta^{(a)}(W, A) \neq \delta^{(a)}(W, A').\end{aligned}$$

Clearly, the function $\delta^{(a)}(W, A)$ satisfies the condition **B8**.

C PFB

PFB is shown in Figure 7.

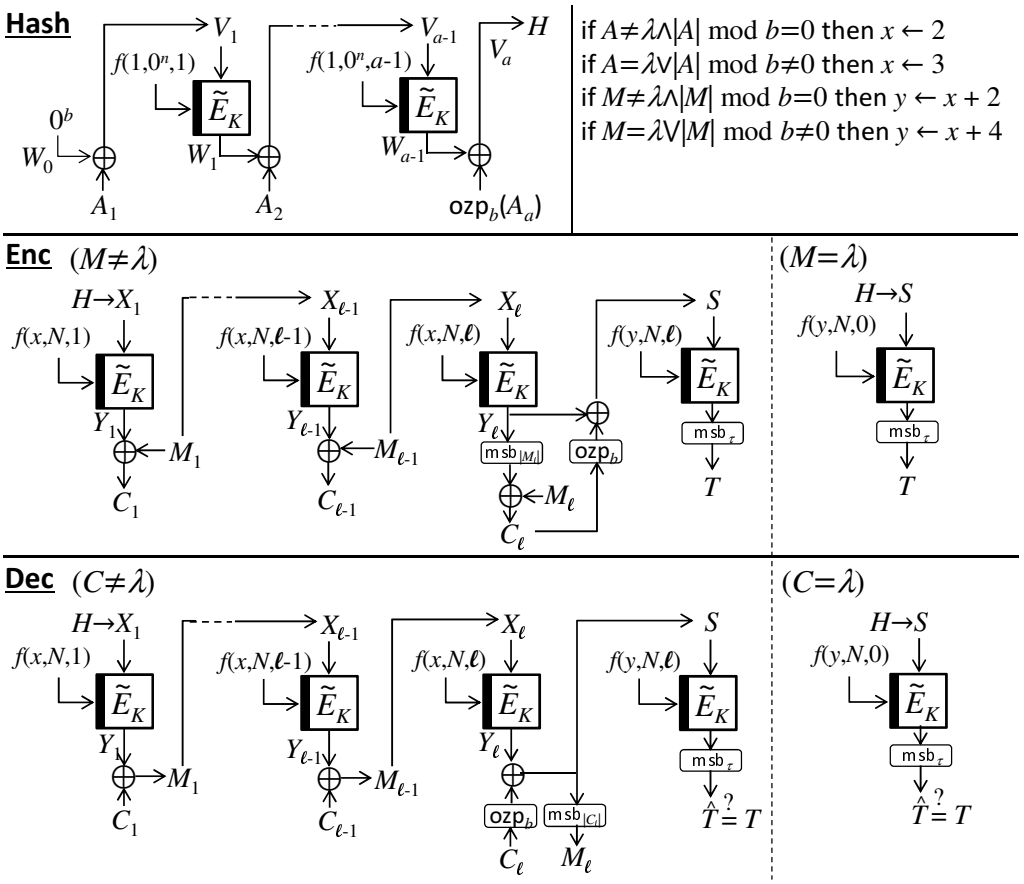
Hash
if $A \neq \lambda \wedge |A| \bmod b = 0$ then $x \leftarrow 2$
if $A = \lambda \vee |A| \bmod b \neq 0$ then $x \leftarrow 3$
if $M \neq \lambda \wedge |M| \bmod b = 0$ then $y \leftarrow x + 2$
if $M = \lambda \vee |M| \bmod b \neq 0$ then $y \leftarrow x + 4$
Enc $(M \neq \lambda)$
$(M = \lambda)$
Dec $(C \neq \lambda)$
$(C = \lambda)$

Figure 7: PFB.