GIFT-COFB

Subhadeep Banik\textsuperscript{1}, Avik Chakraborti\textsuperscript{2}, Tetsu Iwata\textsuperscript{3}, Kazuhiko Minematsu\textsuperscript{4}, Mridul Nandi\textsuperscript{5}, Thomas Peyrin\textsuperscript{6,7}, Yu Sasaki\textsuperscript{2}, Siang Meng Sim\textsuperscript{6} and Yosuke Todo\textsuperscript{2}

\textsuperscript{1} LASEC, Ecole Polytechnique Fédérale de Lausanne, Switzerland
\textsuperscript{2} NTT Secure Platform Laboratories, Japan
\textsuperscript{3} Nagoya University, Japan
\textsuperscript{4} NEC Corporation, Japan
\textsuperscript{5} Indian Statistical Institute, Kolkata, India
\textsuperscript{6} Nanyang Technological University, Singapore
\textsuperscript{7} Temasek Laboratories@NTU, Singapore

\texttt{giftcofb@googlegroups.com}
\url{https://www.isical.ac.in/~lightweight/COFB/}

\section*{Abstract}
In this article, we propose GIFT-COFB, an Authenticated Encryption with Associated Data (AEAD) scheme, based on the GIFT lightweight block cipher and the COFB lightweight AEAD operating mode. We explain how these two primitives can fit together and the various design adjustments possible for performance and security improvements. We show that our design provides excellent performances in all constrained scenarios, hardware or software, while being based on a provably-secure mode and a well analysed block cipher.

\textbf{Keywords:} GIFT · COFB · authenticated encryption · lightweight · lower bound

\section{Introduction}

Confidentiality and authentication are two critical security properties, historically offered with separated cryptographic components. However, due to the possible security issues that might arise when combining these two components and in a hope for performance gains, so-called authenticated encryption (AE) is now becoming more prominent. AE is a symmetric-key cryptographic scheme providing both confidentiality and authenticity in a single primitive. In 2002, Rogaway \cite{Rogaway2002} proposed the concept of Authenticated Encryption with Associated Data (AEAD), well adopted nowadays, which allows in addition a user to authenticate some associated data, without encrypting it (typically some Internet packet header).

Due to the recent rise in communication networks operated on small devices, the era of the so-called Internet of Things, AE is expected to play a key role in securing these networks. After a decade of many advances in the field of lightweight symmetric-key cryptography, an extremely lightweight block cipher – \textsc{GIFT} \cite{GIFT} and a very low state size AEAD scheme – \textsc{COFB} \cite{COFB} were concurrently proposed at CHES 2017 conference. The former is an ad-hoc primitive while the latter is an operating mode, but both primarily focus on obtaining very good hardware implementation results. \textsc{GIFT} reduces the footprint of its algorithmic operations to the bare minimum without compromising its security (actually improving it when compared to \textsc{PRESENT} cipher \cite{PRESENT}, probably the most famous lightweight block cipher). On the other hand, \textsc{COFB} minimises the additional state required for a rate-1 block cipher based AEAD scheme. It was then very natural to match these
two primitives to build a very efficient candidate for the NIST lightweight cryptography competition. Yet, several details need to be handled when matching, in order to maintain the full performance and ensure compliance with NIST requirements.

In this work, we describe the GIFT-COFB authenticated encryption, which instantiates the COFB (COmbined FeedBack) block cipher based AEAD mode with the GIFT block cipher, but with several small tweaks on both COFB and GIFT to further improve their efficiency. Here, we consider the overhead in size, thus the state memory size beyond the underlying block cipher itself (including the key schedule) as one of the main criteria we want to minimize, which is particularly relevant for hardware implementations.

This version supports all the desirable properties mentioned in the NIST lightweight cryptography portfolio [14], and it is efficient for lightweight implementations as well.

There are many approaches for designing a secure and lightweight block cipher based AEAD. We focus on using the lightweight, very efficient and well analyzed block cipher GIFT-128 [3] and minimizing the total encryption/decryption state size by using combined feedback over the block cipher output and the data blocks along with a tweak dependent secret masking (as used in XEX [21]). This combination helps us to minimize the amount of masking by a factor of 2 from [21].

The COFB mode achieves several interesting features. It provides a high rate of 1 (i.e., it needs only one block cipher call per input block). The mode is inverse-free, as it does not need a block cipher inverse during decryption or decryption. In addition to these features, this mode has a very small state size, namely $1.5n + k$ bits, where $n$ and $k$ denote the underlying block cipher block size and key size respectively.

Our Contributions. In this article, we describe GIFT-COFB, an Authenticated Encryption with Associated Data (AEAD) scheme, based on the GIFT-128 lightweight block cipher and the COFB lightweight AEAD operating mode. We analyse how these two primitives can be adapted to fit together and how various design adjustments that we made to improve performance and security. We recall that COFB is a provably secure operating mode and that GIFT block cipher has been thoroughly analysed by its designers and retains a very comfortable security margin even after a lot of third party analysis. We show that our design provides excellent performances in all constrained scenarios, both hardware and software.

Organisation of the paper. We first introduce some notations in Section 2 and describe our proposal GIFT-COFB in Section 3. Then, we explain the design rationale in Section 4 and recall security analysis conducted on the mode COFB and on the internal primitive GIFT in Section 5. Finally, we report latest hardware and software implementation results in Sections 6 and 7.

2 Preliminaries

2.1 Notation

For any $X \in \{0, 1\}^*$, where $\{0, 1\}^*$ is the set of all finite bit strings (including the empty string $\epsilon$), we denote the number of bits of $X$ by $|X|$. Note that $|\epsilon| = 0$. For a string $X$ and an integer $t \leq |X|$, $\text{Trunc}_t(X)$ is the first $t$ bits of $X$. Throughout this document, $n$ represents the block size in bits of the underlying block cipher $E_K$. Typically, we consider $n = 128$ and GIFT-128 is the underlying block cipher, where $K$ is the 128-bit GIFT-128 key. For two bit strings $X$ and $Y$, $X \| Y$ denotes the concatenation of $X$ and $Y$. A bit string $X$ is called a complete (or incomplete) block if $|X| = n$ (or $|X| < n$, respectively). We write the set of all complete (or incomplete) blocks as $B$ (or $B^<$, respectively). Note that $\epsilon$ is considered as an incomplete block and $\epsilon \in B^<$. Let $B^{\geq} = B^< \cup B$ denote the set
of all blocks. For $B \in \mathcal{B}^{-}$, we define $\overline{B}$ as follows:

$$
\overline{B} = \begin{cases} 
10^{n-1} & \text{if } B = \epsilon \\
B \parallel 10^{n-1-|B|} & \text{if } B \neq \epsilon \text{ and } |B| < n \\
B & \text{if } |B| = n
\end{cases}
$$

Given non-empty $Z \in \{0, 1\}^*$, we define the parsing of $Z$ into $n$-bit blocks as

$$(Z[1], Z[2], \ldots, Z[z]) \parallel \cdots \parallel Z,$$

where $z = \lceil |Z|/n \rceil$, $|Z[i]| = n$ for all $i < z$ and $1 \leq |Z[z]| \leq n$ such that $Z = (Z[1] \parallel Z[2] \parallel \cdots \parallel Z[z])$. If $Z = \epsilon$, we let $z = 1$ and $Z[1] = \epsilon$. We write $||Z|| = z$ (number of blocks present in $Z$). Given any sequence $Z = (Z[1], \ldots, Z[s])$ and $1 \leq a \leq b \leq s$, we represent the sub sequence $(Z[a], \ldots, Z[b])$ by $Z[a..b]$. For integers $a \leq b$, we write $[a..b]$ for the set $\{a, a+1, \ldots, b\}$. For two bit strings $X$ and $Y$ with $|X| \geq |Y|$, we define the extended xor-operation as

$$X \overline{\oplus} Y = X[1..|Y|] \parallel Y \text{ and }$$

$$X \overline{\oplus} Y = X \parallel (Y[0^{|X|}-|Y|]),$$

where $(X[1], X[2], \ldots, X[x]) \parallel \cdots \parallel X$ and thus $X[1..|Y|]$ denotes the first $|Y|$ bits of $X$. When $|X| = |Y|$, both operations reduce to the standard $X \oplus Y$.

Let $\gamma = (\gamma[1], \ldots, \gamma[s])$ be a tuple of equal-length strings. We define $\text{mcoll}(\gamma) = r$ if there exist distinct $i_1, \ldots, i_r \in [1..s]$ such that $\gamma[i_1] = \cdots = \gamma[i_r]$ and $r$ is the maximum of such integer. We say that $(i_1, \ldots, i_r)$ is an $r$-multi-collision set for $\gamma$.

### 2.2 Underlying Finite Field $\mathbb{F}_{2^n}$

Let $\mathbb{F}_{2^n}$ denote the binary Galois field of size $2^s$, for a positive integer $s$. Field addition and multiplication between $a, b \in \mathbb{F}_{2^n}$ are represented by $a \oplus b$ (or $a + b$ whenever understood) and $a \cdot b$ respectively. Any field element $a \in \mathbb{F}_{2^n}$ can be represented by any of the following equivalent ways for $a_{0}, a_{1}, \ldots, a_{s-1} \in \{0, 1\}$:

- An $s$-bit string $a_{s-1} \cdots a_{0} \in \{0, 1\}^s$.
- A polynomial $a(x) = a_{0} + a_{1}x + \cdots + a_{s-1}x^{s-1}$ of degree at most $(s - 1)$.

### 2.3 Choice of Primitive Polynomials

In our construction, the primitive polynomial $[1]$ used to represent the field $\mathbb{F}_{2^{64}}$ is

$$p_{64}(x) = x^{64} + x^{4} + x^{3} + x + 1.$$  

We denote the primitive element $0^{s-2}10 \in \mathbb{F}_{2^n}$ by $\alpha_s$ (here $s = 64$). We use $\alpha$ to mean $\alpha_4$ for notational simplicity. The field multiplication $a(x) \cdot b(x)$ is the polynomial $r(x)$ of degree at most $(s - 1)$ such that $a(x)b(x) \equiv r(x) \mod p_s(x)$.

**Multiplication by Primitive Element $\alpha$.** We first see an example how we can multiply by $\alpha = \alpha_s$. Multiplying an element $b := b_{63}b_{62} \cdots b_{0} \in \mathbb{F}_{2^{64}}$ by the primitive element $\alpha$ of $\mathbb{F}_{2^{64}}$ can be done very efficiently as follows:

$$b \cdot \alpha = \begin{cases} 
b \ll 1, & \text{if } b_{63} = 0, \\
b \ll 1 \parallel 0^{59}11011, & \text{else},
\end{cases}$$

where $(b \ll r)$ denotes left shift of $b$ by $r$ bits. For $b \in \mathbb{F}_{2^{64}}$, we use $2 \cdot b$ (or $2^m \cdot b$) and $3 \cdot b$ (or $3^m \cdot b$) to denote $\alpha \cdot b$ (or $\alpha^m \cdot b$) and $(1 + \alpha) \cdot b$ (or $(1 + \alpha)^m \cdot b$), respectively.
2.4Authenticated Encryption and Security Definitions

An authenticated encryption or AE algorithm takes a nonce $N$ (which is a value never repeats at encryption) together with associated data $A$ and plaintext $M$, the encryption function of AE, $\mathcal{E}_K$, produces a tagged-ciphertext $(C,T)$ where $|C| = |M|$ and $|T| = t$. It provides both privacy of a plaintext $M \in \{0,1\}^*$ and authenticity or integrity of $M$ as well as associate data $A \in \{0,1\}^*$. The corresponding decryption function, $\mathcal{D}_K$, takes $(N,A,C,T)$ and returns a decrypted plaintext $M$ when the verification on $(N,A,C,T)$ is successful, otherwise returns the atomic error symbol denoted by $\perp$.

Privacy. Given an adversary $A$, we define the PRF-advantage of $A$ against $\mathcal{E}$ as

$$\text{Adv}_{\mathcal{E}}^{\text{prf}}(A) = \max_A \text{Adv}_{\mathcal{E}}^{\text{prf}}(A),$$

where the maximum is taken over all adversaries running in time $t$ and making $q$ queries with the total number of blocks in all the queries being at most $\sigma$. If $\mathcal{E}_K$ is an encryption function of AE, we call it the privacy advantage and write as $\text{Adv}_{\mathcal{E}}^{\text{prv}}(q,\sigma,t)$, as the maximum of all nonce-respecting adversaries (that is, the adversary can arbitrarily choose nonces provided all nonce values in the encryption queries are distinct).

Authenticity. We say that an adversary $A$ forges an AE scheme $(\mathcal{E},\mathcal{D})$ if $A$ is able to compute a tuple $(N,A,C,T)$ satisfying $\mathcal{D}_K(N,A,C,T) \neq \perp$, without querying $(N,A,M)$ for some $M$ to $\mathcal{E}_K$ and receiving $(C,T)$, i.e. $(N,A,C,T)$ is a non-trivial forgery.

In general, a forger can make $q_f$ forging attempts without restriction on $N$ in the decryption queries, that is, $N$ can be repeated in the decryption queries and an encryption and a decryption query can use the same $N$. The forging advantage for an adversary $A$ is written as $\text{Adv}_{\mathcal{E}}^{\text{auth}}(A) = \Pr[A^{\mathcal{E}} \text{ forges}]$, and we write

$$\text{Adv}_{\mathcal{E}}^{\text{auth}}((q,q_f),(\sigma,\sigma_f),t) = \max_A \text{Adv}_{\mathcal{E}}^{\text{auth}}(A)$$

to denote the maximum forging advantage for all adversaries running in time $t$, making $q$ encryption and $q_f$ decryption queries with total number of queried blocks being at most $\sigma$ and $\sigma_f$, respectively.

Unified Security Notion for AE. The privacy and authenticity advantages can be unified into a single security notion as introduced in [10, 22]. Let $A$ be an adversary that only makes non-repeating queries to $\mathcal{D}_K$. Then, we define the AE-advantage of $A$ against $\mathcal{E}$ as

$$\text{Adv}_{\mathcal{E}}^{\text{AE}}(A) = |\Pr[A^{\mathcal{E}K:D_K} = 1] - \Pr[A^{\mathcal{E}K} = 1]|,$$

where $\perp$-oracle always returns $\perp$ and $\$-oracle is as the privacy advantage. We similarly define $\text{Adv}_{\mathcal{E}}^{\text{AE}}((q,q_f),(\sigma,\sigma_f),t) = \max_A \text{Adv}_{\mathcal{E}}^{\text{AE}}(A)$, where the maximum is taken over all adversaries running in time $t$, making $q$ encryption and $q_f$ decryption queries with the total number of blocks being at most $\sigma$ and $\sigma_f$, respectively.

Block Cipher Security. We use a block cipher $E$ as the underlying primitive, and we assume the security of $E$ as a PRP (pseudorandom permutation). The PRP-advantage of a block cipher $E$ is defined as $\text{Adv}_E^{\text{PRP}}(A) = |\Pr[A^{\mathcal{E}K} = 1] - \Pr[A^{\mathcal{P}} = 1]|$, where $\mathcal{P}$ is a random permutation uniformly distributed over all permutations over $\{0,1\}^n$. We write

$$\text{Adv}_E^{\text{PRP}}(q,t) = \max_A \text{Adv}_E^{\text{PRP}}(A),$$

where the maximum is taken over all adversaries running in time $t$ and making $q$ queries. Here, $\sigma$ does not appear as each query has a fixed length.
Coefficients-H Technique. Coefficients-H technique was developed by Patarin, that is a convenient tool for bounding the advantage (see [15, 9]). We will use this technique (without giving a proof) to prove our security claims. Consider two oracles $O_0 = (\emptyset, \bot)$ (the ideal oracle) and $O_1$ (the real oracle, i.e., our construction). Let $\mathcal{V}$ denotes the set of all possible views an adversary can obtain. For any view $\tau \in \mathcal{V}$, we will denote the probability to realize the view as $ip_{\text{real}}(\tau)$ (or $ip_{\text{ideal}}(\tau)$) when it is interacting with the real oracle (or ideal oracle, respectively). We call these interpolation probabilities. Without loss of generality, we assume that the adversary is deterministic and fixed. Then, the probability space for the interpolation probabilities is uniquely determined by the underlying oracle. As we deal with stateless oracles, these probabilities are independent of the order of queries and responses in the view. Suppose we have a set of views, $\mathcal{V}_{\text{good}} \subseteq \mathcal{V}$, which we call good views, and the following conditions hold:

1. In the game involving the ideal oracle $O_0$ (and the fixed adversary), the probability of getting a view in $\mathcal{V}_{\text{good}}$ is at least $1 - \epsilon_1$.

2. For any view $\tau \in \mathcal{V}_{\text{good}}$, we have $ip_{\text{real}}(\tau) \geq (1 - \epsilon_2) \cdot ip_{\text{ideal}}(\tau)$.

Then we have $|\Pr[A^{O_0} = 1] - \Pr[A^{O_1} = 1]| \leq \epsilon_1 + \epsilon_2$. The proof can be found, e.g., in [9]. We will later use this result to prove the security of our construction in Theorem 1 by defining certain $\mathcal{V}_{\text{good}}$ for our games, and evaluating the bounds, $\epsilon_1$ and $\epsilon_2$.

3 Specification

3.1 Syntax

The encryption algorithm (with authentication), denoted as $\text{GIFT-COFB}(K, N, A, M) \mapsto (C, T)$, takes as input an encryption key $K \in \{0, 1\}^{128}$, a nonce $N \in \{0, 1\}^{128}$, associated data $A \in \{0, 1\}^*$, and a message $M \in \{0, 1\}^*$. The nonce $N$ can include a counter to make the nonce non-repeating. It generates a ciphertext $C \in \{0, 1\}^{|M|}$ and a tag $T \in \{0, 1\}^{128}$.

The decryption algorithm (with verification), denoted as $\text{GIFT-COFB}^{-1}(K, N, A, C, T) \mapsto M$, takes $(K, N, A, C, T)$ as input. It generates a message $M \in \{0, 1\}^{|C|}$ or a special symbol $\bot$ denoting rejection.

3.2 Building Blocks of GIFT-COFB

3.2.1 Building Blocks of COFB

Block Cipher. The underlying encryption cipher, $E_K$, is an 128-bit block cipher with 128-bit key equivalent to GIFT-128 but with a small tweak in the input and output data format. See Section 3.2.2 for the specification and Section 4.2 for the rationale.

Padding Function. For $x \in \{0, 1\}^*$, we define padding function $\text{Pad}$ as

$$\text{Pad}(x) = \begin{cases} x & \text{if } x \neq \epsilon \text{ and } |x| \mod n = 0 \\ x || 10^{n - (|x| \mod n) - 1} & \text{otherwise.} \end{cases}$$

Note that $\text{Pad}(\epsilon) = 10^{n - 1}$.
Feedback Function. Let $Y \in \{0,1\}^{128}$ and $(Y[1], Y[2]) \leftarrow Y$, where $Y[i] \in \{0,1\}^{64}$. We define $G : \{0,1\}^{128} \rightarrow \{0,1\}^{128}$ as

$$G(Y) = (Y[2], Y[1] \ll 1),$$

where for a string $X$, $X \ll r$ is the left rotation of $X$ by $r$ bits. We also view $G$ as the $128 \times 128$ non-singular binary matrix, so we write $G(Y)$ and $G \cdot Y$ interchangeably. For $M \in \{0,1\}^{128}$ and $Y \in \{0,1\}^{128}$, we define $\rho(Y, M) = G \cdot Y \oplus M$. The feedback function $\rho$ and its corresponding $\rho'$ are defined as

$$\rho(Y, M) = (\rho_1(Y, M), Y \oplus M),$$

$$\rho'(Y, C) = (\rho_1(Y, Y \oplus C), Y \oplus C).$$

Note that when $(X, M) = \rho'(Y, C)$ then $X = (G \oplus I) \cdot Y \oplus C$, where $I$ is the $128 \times 128$ identity matrix. Our choice of $G$ ensures that $G \oplus I$ has rank $n-1$ (precisely, 127, in our construction with $n = 128$). When $Y$ is chosen randomly, both $\rho_1(Y, M)$ (during encryption) and $\rho_1(Y, Y \oplus C)$ (during decryption) also has almost full entropy. We need this property when we bound probability of bad events later.

Tweak Value for The Last Block. Given the last block of associated data, $A \in \{0,1\}^*$, we define $\delta_A \in \{1,2\}$ as follows:

$$\delta_A = \begin{cases} 1 & \text{if } A \neq \epsilon \text{ and } n \text{ divides } |A| \\ 2 & \text{otherwise.} \end{cases}$$

Given the last block of either a message or a ciphertext, $Z \in \{0,1\}^*$, we define $\delta_Z \in \{1,2\}$ as follows:

$$\delta_Z = \begin{cases} 1 & \text{if } n \text{ divides } |Z| \\ 2 & \text{otherwise.} \end{cases}$$

This will be used to differentiate the cases that the last block of $A$ or $Z$ is $n$ bits or shorter, for $Z$ being a message or a ciphertext. We also define a formatting function $\text{Fmt}$ for a pair of bit strings $(A, Z)$. Let $(A[1], \ldots, A[a]) \leftarrow A$ and $(Z[1], \ldots, Z[z]) \leftarrow Z$. We define $t[i]$ as follows:

$$t[i] = \begin{cases} (i, 0) & \text{if } i < a \\ (a-1, \delta_A) & \text{if } i = a \\ (i-1, \delta_A) & \text{if } a < i < a+z \\ (a+z-2, \delta_A + \delta_Z) & \text{if } i = a+z \end{cases}$$

Now, the formatting function $\text{Fmt}(A, Z)$ returns the following sequence

$$\left\{ (A[1], t[1]), \ldots, (A[a], t[a]) \right\} \cup \left\{ (Z[1], t[a+1]), \ldots, (Z[z], t[a+z]) \right\}$$

where the first coordinate of each pair specifies the input block to be processed, and the second coordinate specifies the exponents of $\alpha$ and $1+\alpha$ to determine the constant over $\text{GF}(2^{n/2})$. Let $\mathbb{Z}_{\geq 0}$ be the set of non-negative integers and $X$ be some non-empty set. We say that a function $f : X \rightarrow (B \times \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0})^+$ is prefix-free if for all $X \neq X'$, $f(X) = (Y[1], \ldots, Y[\ell])$ is not a prefix of $f(X') = (Y'[1], \ldots, Y'[\ell'])$ (in other words, $(Y[1], \ldots, Y[\ell]) \neq (Y'[1], \ldots, Y'[\ell'])$). Here, for a set $S$, $S^+$ means $S \cup S^2 \cup \cdots$, and we have the following lemma.

Lemma 1. The function $\text{Fmt}(\cdot)$ is prefix-free.

The proof is more or less straightforward and hence we skip it.
### 3.2.2 GIFT building blocks

**Initialization and Finalization.** The 128-bit plaintext $P$ is loaded into the cipher state $S$ which will be expressed as 4 32-bit segments, $S = \{S_0, S_1, S_2, S_3\}$, where $S_i \in \{0,1\}^{32}$. On the other hand, the 128-bit secret key $K$ is loaded into the key state $KS$ which will be expressed as 8 16-bit words, $KS = \{W_0, W_1, \ldots, W_7\}$, where $W_i \in \{0,1\}^{16}$.

\[
\text{Initialize}(P) = \begin{bmatrix}
S_0 \\
S_1 \\
S_2 \\
S_3
\end{bmatrix} \leftarrow \begin{bmatrix}
B_0 & B_1 & B_2 & B_3 \\
B_4 & B_5 & B_6 & B_7 \\
B_8 & B_9 & B_{10} & B_{11} \\
B_{12} & B_{13} & B_{14} & B_{15}
\end{bmatrix},
\]

\[
\text{Initialize}(K) = \begin{bmatrix}
W_0 & W_1 \\
W_2 & W_3 \\
W_4 & W_5 \\
W_6 & W_7
\end{bmatrix} \leftarrow \begin{bmatrix}
B_0||B_1 & B_2||B_3 \\
B_4||B_5 & B_6||B_7 \\
B_8||B_9 & B_{10}||B_{11} \\
B_{12}||B_{13} & B_{14}||B_{15}
\end{bmatrix},
\]

where $B_i$ are the arriving bytes.

The function Finalize will be the reverse process, outputting the state byte by byte.

**SubCells Function.** We denote the SubCells function $S \leftarrow \text{SubCells}(S)$ as the following set of instructions:

\[
S_1 \leftarrow S_1 \oplus (S_0 \& S_2)
\]

\[
S_0 \leftarrow S_0 \oplus (S_1 \& S_3)
\]

\[
S_2 \leftarrow S_2 \oplus (S_0 \mid S_1)
\]

\[
S_3 \leftarrow S_3 \oplus S_2
\]

\[
S_1 \leftarrow S_1 \oplus S_3
\]

\[
S_3 \leftarrow \sim S_3
\]

\[
S_2 \leftarrow S_2 \oplus (S_0 \& S_1)
\]

where $\&$, $\mid$ and $\sim$ are AND, OR and NOT operation respectively.

**PermBits Function.** We define the parsing of $S_i$ into 32 individual bits as

\[
(S_i[31], S_i[30], \ldots, S_i[0]) \leftarrow S_i
\]

We denote

\[
\text{PermBits}(S) = \{Pb_0(S_0), Pb_1(S_1), Pb_2(S_2), Pb_3(S_3)\},
\]

where $Pb_i$ is described in Table 1, the row “Index” shows the indexing of the 32 bits in all $S_i$'s and the row “$S_i$” shows the ending position of the bits. For example, $S_1[1]$ (the 2nd rightmost bit) is shifted 1 position to the right, to the initial position of $S_1[0]$, while $S_1[0]$ is shifted 8 positions to the left where $S_1[8]$ was.

**AddRoundKey Function.** We define the AddRoundKey function $\text{AddRoundKey}$ as

\[
\text{AddRoundKey}(S, KS, i) = \{S_0, S_1 \oplus (W_6 \mid W_7), S_2 \oplus (W_2 \mid W_3), S_3 \oplus \text{Const}_i\},
\]

where $\text{Const}_i = 0x8000000XY$ is the $i$-th round constant and the byte $XY = 00c_5c_4c_3c_2c_1c_0$ is the round constant generated using the a 6-bit affine LFSR, whose state is updated as follows:

\[c_5\|c_4\|c_3\|c_2\|c_1\|c_0 \leftarrow c_4\|c_3\|c_2\|c_1\|c_0\|c_5 \oplus c_4 \oplus 1.\]
Table 1: Specifications of bit permutation $Pb_i$.

<table>
<thead>
<tr>
<th>Index</th>
<th>31</th>
<th>30</th>
<th>29</th>
<th>28</th>
<th>27</th>
<th>26</th>
<th>25</th>
<th>24</th>
<th>23</th>
<th>22</th>
<th>21</th>
<th>20</th>
<th>19</th>
<th>18</th>
<th>17</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Pb_0$</td>
<td>29</td>
<td>25</td>
<td>21</td>
<td>17</td>
<td>13</td>
<td>9</td>
<td>5</td>
<td>1</td>
<td>30</td>
<td>26</td>
<td>22</td>
<td>18</td>
<td>14</td>
<td>10</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>$Pb_1$</td>
<td>30</td>
<td>26</td>
<td>22</td>
<td>18</td>
<td>14</td>
<td>10</td>
<td>6</td>
<td>2</td>
<td>31</td>
<td>27</td>
<td>23</td>
<td>19</td>
<td>15</td>
<td>11</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>$Pb_2$</td>
<td>31</td>
<td>27</td>
<td>23</td>
<td>19</td>
<td>15</td>
<td>11</td>
<td>7</td>
<td>3</td>
<td>28</td>
<td>24</td>
<td>20</td>
<td>16</td>
<td>12</td>
<td>8</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>$Pb_3$</td>
<td>28</td>
<td>24</td>
<td>20</td>
<td>16</td>
<td>12</td>
<td>8</td>
<td>4</td>
<td>0</td>
<td>29</td>
<td>25</td>
<td>21</td>
<td>17</td>
<td>13</td>
<td>9</td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>

The six bits, $c_i$, are initialized to zero, and updated before being used in a given round. The values of the constants for each round are given in the table below, encoded to byte values for each round, with $c_0$ being the least significant bit.

<table>
<thead>
<tr>
<th>Rounds</th>
<th>Constants</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 16</td>
<td>01,03,07,0F,1F,3E,3D,3B,37,2F,1E,3C,39,33,27,0E</td>
</tr>
<tr>
<td>17 - 32</td>
<td>1D,3A,35,2B,16,2C,18,30,21,02,05,0B,17,2E,1C,38</td>
</tr>
<tr>
<td>33 - 48</td>
<td>31,23,06,0D,18,36,2D,1A,34,29,12,24,08,11,22,04</td>
</tr>
</tbody>
</table>

Key State Update Function. The key state update function KeyUpdate is defined as follows:

$$\text{KeyUpdate}(KS) = \{W_6 \gg 2, W_7 \gg 12, W_0, W_1, W_2, W_3, W_4, W_5\}$$

3.3 GIFT-COFB Pseudocode

We present the specifications of GIFT-COFB in Fig. 1, where $\alpha$ and $(1 + \alpha)$ are written as 2 and 3. See also Fig. 2. The encryption and decryption algorithms are denoted by COFB-$E_K$ and COFB-$D_K$. We remark that the nonce length is 128 bits, which is enough for the security up to the birthday bound. The nonce is processed as $E_K(N)$ to yield the first internal chaining value. The encryption algorithm takes $A$ and $M$, and outputs $C$ and $T$ such that $|C| = |M|$ and $|T| = 128$. The decryption algorithm takes $(N, A, C, T)$ and outputs $M$ or ⊥. Both encryption and decryption algorithms use block cipher $E_K$ and the key $K$ is implicitly given to them.

4 Design Rationale

As both GIFT and COFB are already well-established primitives, in this section we explain the rationale for this combination, followed by the tweaks we made to these original publications to enhance the performance and security.

4.1 AEAD Scheme: GIFT-COFB

COFB is a block cipher based authenticated encryption mode that uses GIFT-128 as the underlying block cipher and GIFT-COFB can be viewed as an efficient integration of the
Algorithm COFB-\(E_K(N, A, M)\)
1. \(Y[0] \leftarrow E_K(N), \ L \leftarrow \text{Trunc}_{n/2}(Y[0])\)
2. \((A[1], \ldots, A[a]) \leftarrow \text{Pad}(A)\)
3. if \(M \neq \epsilon\) then
   4. \((M[1], \ldots, M[m]) \leftarrow \text{Pad}(M)\)
5. for \(i = 1\) to \(a - 1\)
6. \(L \leftarrow 2 \cdot L\)
7. \(X[i] \leftarrow A[i] \oplus G \cdot Y[i - 1] \oplus L[0]^n/2\)
8. \(Y[i] \leftarrow E_K(X[i])\)
9. if \(|A| \mod n = 0\) and \(A \neq \epsilon\) then \(L \leftarrow 3 \cdot L\)
else \(L \leftarrow 3^2 \cdot L\)
11. if \(M = \epsilon\) then \(L \leftarrow 3^2 \cdot L\)
12. \(X[a] \leftarrow A[a] \oplus G \cdot Y[a - 1] \oplus L[0]^n/2\)
13. \(Y[a] \leftarrow E_K(X[a])\)
14. for \(i = 1\) to \(m - 1\)
15. \(L \leftarrow 2 \cdot L\)
16. \(C[i] \leftarrow M[i] \oplus Y[i + a - 1]\)
17. \(X[i + a] \leftarrow M[i] \oplus G \cdot Y[i + a - 1] \oplus L[0]^n/2\)
18. \(Y[i + a] \leftarrow E_K(X[i + a])\)
19. if \(M \neq \epsilon\) then
20. if \(|M| \mod n = 0\) then \(L \leftarrow 3 \cdot L\)
else \(L \leftarrow 3^2 \cdot L\)
22. \(C[m] \leftarrow M[m] \oplus Y[a + m - 1]\)
23. \(X[a + m] \leftarrow M[m] \oplus G \cdot Y[a + m - 1] \oplus L[0]^n/2\)
24. \(Y[a + m] \leftarrow E_K(X[a + m])\)
25. \(C \leftarrow \text{Trunc}_{\lfloor n/2 \rfloor}([C[1]] \ldots [C[m]])\)
26. \(T \leftarrow \text{Trunc}_{\lfloor n/2 \rfloor}(Y[a + m])\)
27. else \(C \leftarrow \epsilon, T \leftarrow \text{Trunc}_{\lfloor n/2 \rfloor}(Y[a])\)
28. return \((C, T)\)

Algorithm \(E_K(X)\)
1. \(S \leftarrow \text{Initialize}(X)\)
2. \(KS \leftarrow \text{Initialize}(K)\)
3. for \(i = 1\) to 40
4. \(S \leftarrow \text{SubCells}(S)\)
5. \(S \leftarrow \text{PermBits}(S)\)
6. \(S \leftarrow \text{AddRoundKey}(S, KS, i)\)
7. \(KS \leftarrow \text{KeyUpdate}(KS)\)
8. \(Y \leftarrow \text{Finalize}(S)\)
9. return \(Y\)

Algorithm COFB-\(D_K(N, A, C, T)\)
1. \(Y[0] \leftarrow E_K(N), \ L \leftarrow \text{Trunc}_{n/2}(Y[0])\)
2. \((A[1], \ldots, A[a]) \leftarrow \text{Pad}(A)\)
3. if \(C \neq \epsilon\) then
   4. \((C[1], \ldots, C[c]) \leftarrow \text{Pad}(C)\)
5. for \(i = 1\) to \(a - 1\)
6. \(L \leftarrow 2 \cdot L\)
7. \(X[i] \leftarrow A[i] \oplus G \cdot Y[i - 1] \oplus L[0]^n/2\)
8. \(Y[i] \leftarrow E_K(X[i])\)
9. if \(|A| \mod n = 0\) and \(A \neq \epsilon\) then \(L \leftarrow 3 \cdot L\)
else \(L \leftarrow 3^2 \cdot L\)
11. if \(C = \epsilon\) then \(L \leftarrow 3^2 \cdot L\)
12. \(X[a] \leftarrow A[a] \oplus G \cdot Y[a - 1] \oplus L[0]^n/2\)
13. \(Y[a] \leftarrow E_K(X[a])\)
14. for \(i = 1\) to \(c - 1\)
15. \(L \leftarrow 2 \cdot L\)
16. \(M[i] \leftarrow Y[i + a - 1] \oplus C[a]\)
17. \(X[i + a] \leftarrow M[i] \oplus G \cdot Y[i + a - 1] \oplus L[0]^n/2\)
18. \(Y[i + a] \leftarrow E_K(X[i + a])\)
19. if \(C \neq \epsilon\) then
20. if \(|C| \mod n = 0\) then
   21. \(L \leftarrow 3 \cdot L\)
   22. \(M[c] \leftarrow Y[a + c - 1] \oplus C[c]\)
   23. else
   24. \(L \leftarrow 3^2 \cdot L, \ c' \leftarrow |C| \mod n\)
   25. \(M[c] \leftarrow \text{Trunc}_{\lfloor n/2 \rfloor}(Y[a + c - 1] \oplus C[c])\)
   26. \(X[a + c] \leftarrow M[c] \oplus G \cdot Y[a + c - 1] \oplus L[0]^n/2\)
   27. \(Y[a + c] \leftarrow E_K(X[a + c])\)
   28. \(M \leftarrow \text{Trunc}_{\lfloor n/2 \rfloor}(M[1]) \ldots M[c]\)
   29. \(T' \leftarrow \text{Trunc}_{\lfloor n/2 \rfloor}(Y[a + c])\)
   30. else \(M \leftarrow \epsilon, T' \leftarrow \text{Trunc}_{\lfloor n/2 \rfloor}(Y[a])\)
31. if \(T' = T\) then return \(M, \) else return \(\bot\)

Figure 1: The encryption and decryption algorithms of GIFT-COFB.
Figure 2: Encryption of COFB. In the rightmost figure, the case of encryption for empty $M$ (hence a MAC for $(N,A)$) can be highlighted as $T = \text{Trunc}_\tau(Y[a])$
Figure 3: 2 rounds of GIFT-128.

4.2 Underlying Block Cipher: GIFT

GIFT-128 is an 128-bit Substitution-Permutation network (SPN) based block cipher with a key length of 128-bit. It is a 40-round iterative block cipher with identical round function. For brevity, we simply call it GIFT.

There are different ways to perceive GIFT-128, the more pictorial description is detailed in Section 2 of [4], which looks like a larger version of PRESENT cipher with 32 4-bit S-boxes and an 128-bit bit permutation (see Figure 3). In our work, we use an alternative description of GIFT, using bitslice description which is similar to Appendix A of [4]. Note that the security properties are equivalent up to bit arrangement of the plaintext and ciphertext.

GIFT is considered to be one of the lightest design existing in the literature. It is denoted as “Small PRESENT” as the design rationale of GIFT follows that of PRESENT [7]. However, GIFT has got rid of several well known weaknesses existing in PRESENT with regards to linear cryptanalysis. Overall GIFT promises much increased efficiency (both lighter and faster) over PRESENT. GIFT is a very simple design that outperforms even SIMON and SKINNY for round based implementations. It consists of very simple operations such that the total hardware footprint is almost consumed by the underlying and the cipher storage. The design is somewhat “optimal” as a weaker S-box (than GIFT S-box) would lead to a weaker design. The linear layer is completely free for a round-based implementation in hardware (consisting of simply bit-wiring) and the constants are generated thanks to a very lightweight LFSR. The key schedule is also very light, simply consisting of shifts. The presented security analysis details and hardware implementation results also support the claims made by the designers.

Although there is almost no impact on hardware implementation, there are several motivations for using bitslice implementation (non-LUT based) instead of LUT based implementation of GIFT when we consider software implementation. Here, we will state the 3 most obvious benefits relating to its 3 steps in a round function.

Constant time non-linear layer. For LUT based implementation, we can consider updating 2 GIFT S-boxes (1 byte) in a single memory call with a reasonable 256 entries LUT. This would require 16 lookups and it takes approximately 16 to 64 cycles to do all S-boxes in a round, assuming a few cycles to access the RAM. Using bitslice implementation, it requires just 11 basic operations (or 10 with XNOR operation) to compute all the S-boxes.
in parallel. And more importantly, using bitslice implementation has the nice feature that
it doesn’t need any RAM and that it is constant time, mitigating potential timing attacks.

**Efficient linear layer.** While it is basically free on hardware, for software implementation
it is extremely slow and complex to implement. This effect can be reduced by doing several
blocks in parallel using none other than bitslice implementation. Even for a single block
encryption, bitslice implementation is still more efficient that LUT based implementation
because of the way the bits are packed.

**Simpler key addition.** For LUT based implementation, the subkeys need to be XORed
to bit positions that are 3 bits apart, making the key addition tedious and non-trivial. An
option is to precompute the subkeys, but even so the key addition would require several
XOR operations to update the 128-bit state. Using bitslice, the bits that were once 3 bits
apart are now packed together in 32-bit words, making the key addition as simple as just
2 XOR operations.

### 4.3 Authenticated Encryption Mode: COFB

COFB is a lightweight AEAD mode. The mode presented in this write up differs slightly
with the original proposal. They are as follows.

- We change the nonce to be 128 bits.
- We change the feedback (more precisely the $G$ matrix) to make it more hardware
efficient.
- We now deal with empty data. We change the mask update function for the purpose.
- We change the padding for the associated data. To be precise, if the associated data
is empty, then padding the associated data will yield the constant block $10^{n-1}$ ($n$:
block cipher state size).

We observed that, the updates make the design more lightweight and more efficient to
deal with short data inputs. However, these updates do not have impact on the security of
the mode (only a nominal 1-bit security degradation).

### 5 Security

#### 5.1 Security proof of COFB

We present the security analysis of COFB in Theorem 1.

**Theorem 1** (Main Theorem).

\[
\text{Adv}^{\text{AE}}_{\text{COFB}}((q, q_f), (\sigma, \sigma_f), t) \leq \text{Adv}^{\text{PRP}}_{\text{GIFT}}(q', t') + \frac{q'}{2^n} + \frac{1}{2^{n/2}} + \frac{q_f(n + 4)}{2^{n/2+1}} + \frac{3\sigma^2 + q_f + (q + \sigma + \sigma_f) \cdot \sigma_f}{2^n}
\]

where $q' = q + q_f + \sigma + \sigma_f$, which corresponds to the total number of block cipher calls
through the game, and $t' = t + O(q')$.

**Proof.** We assume $q' \leq 2^{2^n-1}$. We make a transition by using an $n$-bit (uniform) random
permutation $P$ instead of $E_K$, which is GIFT, and next an $n$-bit (uniform) random function
$R$ instead of $P$. The first two terms in our bounds comes from these two transitions using
the standard PRP-PRF switching lemma and the computation to the information security reduction (e.g., see [5]).

Thus we only need a bound for COFB with R, denoted by COFB-R. Here, we prove

\[ \text{Adv}^{\text{AE}}_{\text{COFB-R}}((q_f, q_f), (\sigma, \sigma_f), \infty) \leq \frac{1}{2^{n/2}} + \frac{q_f(n + 4)}{2^{n/2} + 1} + \frac{2\sigma^2 + q_f + (q + \sigma + \sigma_f) \cdot \sigma_f}{2^{2n}}. \]  

(1)

Let \((N_i, A_i, M_i)\) and \((C_i, T_i)\) denote the i-th encryption query and response for \(1 \leq i \leq q\). We use the notation \((A_i[1], \ldots, A_i[a_i]) \longleftarrow \text{Pad}(A_i), (M_i[1], \ldots, M_i[m_i]) \longleftarrow \text{Pad}(M_i)\) and \((C_i[1], \ldots, C_i[m_i]) \longleftarrow \text{Pad}(C_i)\). Let \(\ell_i = a_i + m_i + 1\), which denotes the total input block length (including nonce) for the i-th encryption query. The i-th decryption query is \((N_i^*, A_i^*, C_i^*, T_i^*)\) with a response \(Z_i^*\) (either \(\perp\) for an invalid decryption attempt or a message). We similarly define \(c_i^*\) and \(a_i^*\), and write \(\ell_i^* = a_i^* + c_i^* + 1\). We have \(\sigma = \sum_i \ell_i\) and \(\sigma_f = \sum_i \ell_i^*\). We also use the notation \((L_i[j], R_i[j]) \sim \text{Fmt}(X_i[j])\) for all \(i \in [1..q]\) and \(j \in [1..\ell_i]\).

**Real Oracle.** Real oracle follows COFB-R (where \(E_K\) is replaced by \(R\)). We use \(X_i[j]\) (resp. \(Y_i[j]\)) for \(i = 1, \ldots, q\) and \(j = 0, \ldots, \ell_i\) for the j-th input (resp. output) of the internal R invoked during the i-th encryption query, with the order of invocation shown in Fig. 1. We set \(X_i[0] = N_i\) and \(Y_i[\ell_i] = T_i\). We write \(L_i = \text{Trunc}_{n/2}(Y_i[0])\).

The following relaxations are introduced that only gain the advantage. After making all the encryption queries and forging attempts, release all the Y-values for the encryption queries only. The transcript due to encryption queries consists of \((N_i, A_i, M_i, Y_i)\), where \(Y_i\) denotes \((Y_i[0], \ldots, Y_i[\ell_i]) = Y_i[0..\ell_i]\).

**Ideal Oracle.** In case of the ideal oracle, all these variables corresponding to \(Y\) will be chosen uniformly and independently, where at the plaintext encryption phase \(Y_i[j]\) is randomly chosen and used to determine \(C_i[j]\) as \(C_i[j] = Y_i[j - 1] \oplus M_i[j]\), and at AD processing phase it is a dummy and has no influence to the response \((C_i, T_i)\). For decryption queries, the ideal oracle always returns \(Z_i^* = \perp\) (here we assume that the adversary makes only fresh queries).

**Views.** In our case, a view \(\tau\) is defined by the following tuple:

\[ \tau = ((N_i, A_i, M_i, Y_i)_{i \in \{1, \ldots, q\}}, (N_i^*, A_i^*, C_i^*, T_i^*, Z_i^*)_{i' \in \{1, \ldots, q'\}}). \]

Note that, \(X_i\)-values of encryption queries are also uniquely determined following construction based on \(N_i, A_i, M_i\) and \(Y_i\).

**Definition of \(p_i\) and \(i'\).** For the i-th decryption query, we define \(p_i = -1\) if there is no \(j\) with \(N_j = N_i^*\). In this case \(i'\) is not defined. Otherwise, there is a unique index \(i'\) with \(N_{i'} = N_i^*\). We define \(p_i\) as the length of the longest common prefix of \(\text{Fmt}(A_i^*, C_i^*)\) and \(\text{Fmt}(A_{i'}, C_{i'})\). Since \(\text{Fmt}\) is prefix-free, it holds that \(p_i < \min\{\ell_i^*, \ell_{i'}\}\).

**Bad Views.** The complement of the set of bad views is defined to be the set of good views. A view is called bad if one of the following events occurs:

\(B_1:\) \(X_i[j_1] = X_i[j_2]\) for some \((i_1, j_1) \neq (i_2, j_2)\) where \(j_1, j_2 > 0\).

\(B_2:\) \(Y_i[j_1] = Y_i[j_2]\) for some \((i_1, j_1) \neq (i_2, j_2)\) where \(j_1, j_2 > 0\).

\(B_3:\) \(\text{mcoll}(R) > n/2\) where \(R\) is the tuple of all \(R_i[j]\) values.

\(B_4:\) \(X_i^*[p_i + 1] = X_i[j_1]\) for some \((i, i_1, j_1)\) with \(j_1 \neq 0\).

\(B_5:\) \(p_i = \ell_i^* - 1\) and \(X_i^*[p_i + 1] = X_i[j_1]\) for some \((i, i_1, j_1)\) with \(Y_i[j_1] = T_i^*\).
\[ B6: \] \( p_i \neq -1 \) and \( X_i^* [p_i + 1] = X_i^* [0] \) for some \((i, i')\).

\[ B7: \] \( p_i \neq -1, \ell_i - 1 \) and \( X_i^* [p_i + 1] = X_i^* [0] \) and \( X_i^* [p_i + 2] = X_i^* [j_2] \) for some \( i_1 \neq i' \) and \((i_2, j_2)\).

\[ B8: \] For some \( i, Z_i^* \neq i \). This clearly cannot happen for the ideal oracle case.

We add some intuitions on these events. When \( B1 \) does not hold, then all the inputs for the random function are distinct for encryption queries, which makes the responses from encryption oracle completely random in the “real” game.

\[ B2 \] event is an auxiliary event which is required to bound \( B5 \).

Similarly, \( B3 \) would be required to bound the probability of the other bad events. When \( B3 \) does not hold, then at the right half of \( X_i[j] \) we see at most \( n/2 \) multi-collisions.

A successful forgery is to choose one of the \( n/2 \) multi-collision blocks and forge the left part so that the entire block collides. Forging the left part has \( 2^{-n/2} \) probability due to randomness of masking. So, when \( B3 \) does not hold, then the \((p_i + 1)\)-st input for the \( i \)-th forging attempt will be fresh with a high probability and so all the subsequent inputs will remain fresh with a high probability. The event \( B4 \) to \( B7 \) are different cases for which \((p_i + 1)\)-st input for the \( i \)-th forging attempt are not fresh.

A view is called good if none of the above events hold. Let \( V_{\text{good}} \) be the set of all such good views. The following lemma bounds the probability of not realizing a good view while interacting with the ideal oracle (this will complete the first condition of the Coefficients-H technique).

**Lemma 2.**

\[
\Pr_{\text{ideal}} [\tau \notin V_{\text{good}}] \leq \frac{1}{2^{n/2}} + \frac{q_f(n + 4)}{2^{n/2 + 1}} + \frac{2\sigma^2}{2^n}
\]

**Proof of Lemma 2.** Throughout the proof, we assume all probability notations are defined over the ideal game. We bound all the bad events individually and then by using the union bound, we will obtain the final bound.

1. \( \Pr[B1] \leq \sigma^2/2^n + 1: \) For any \((i_1, j_1) \neq (i_2, j_2) \) with \( j_1, j_2 \geq 1 \), the equality event \( X_{i_1}[j_1] = X_{i_2}[j_2] \) has a probability at most \( 2^{-n} \) since this event is a non-trivial linear equation on \( Y_{i_1}[j_1 - 1] \) and \( Y_{i_2}[j_2 - 1] \) and they are independent to each other.

2. \( \Pr[B2] \leq \sigma^2/2^n + 1: \) This case is similar to the previous case.

3. \( \Pr[B3] \leq 1/2^{n/2}: \) The event \( B3 \) is a multi-collision event for randomly chosen \( \sigma \) many \( n/2 \)-bit strings as \( Y \) values are mapped in a regular manner (see the feedback function) to \( R \) values. From the union bound, we have

\[
\Pr[B3] \leq \left( \frac{\sigma}{2} \right) \frac{1}{2^{n/2}} < \sigma \frac{2^{n/2} + 1}{2^n} \leq \left( \frac{2^{n/2} - 1}{2^{n/2}} \right)^{n/2} \leq \frac{1}{2^n},
\]

where the last inequality follows from the assumption \( \sigma \leq 2^{(n/2) - 2} \) since otherwise the theorem is trivially true.

4. \( \Pr[B4 \land B3^c] \leq nq_f/2^{n/2 + 1}: \) We can assume that \( B3 \) does not hold so the maximum number of multi-collision on \( R \)-values is at most \( n \). Now fix \((i_1, j_1) \) with \( i_1 \neq i' \) and hence due to randomness of \( L_i \), the probability of this case is at most \( 1/2^{n/2} \).

Let us assume that \( i_1 = i' \) and so \( j_1 \neq p_i + 1 \). Once again it is easy to see that \( X_i^* [p_i + 1] = X_i^* [j_1] \) reduces to a non-trivial equation in \( L_{i'} \). Thus, the probability of this case is also at most \( 1/2^{n/2} \). By union bound the probability of this event is at most \( 0.5n/2^{n/2} \) for all \( i \). Summing over all decryption queries, we get \( \Pr[B4 \land B3^c] \leq nq_f/2^{n/2 + 1} \).
(5) $\text{Pr}[B5 \land B2^c] \leq q_f/2^{n/2}$: As $B2$ does not hold, there can be at most one $(i_1, j_1)$ for which $Y_{i_1|j_1} = T_{i_1}^r$ (for a given $i$). If there is any such $(i_1, j_1)$, $X_{i_1|j_1}^r = 1 = X_{i_1|j_1}^i$ can hold with probability at most $1/2^{n/2}$. Summing over all decryption queries, we get $\text{Pr}[B5 \land B2^c] \leq q_f/2^{n/2}$.

(6) $\text{Pr}[B6] \leq q_f/2^{n/2}$: This is a non-trivial equation in $L_0$ and hence it holds with probability at most $1/2^{n/2}$ for every $i$. Thus, $\text{Pr}[B6] \leq q_f/2^{n/2}$.

(7) $\text{Pr}[B7 \land B3^c] \leq \frac{2\sigma q_f}{2^{n/2}}$:

For a fixed $i$, we have

$$\text{Pr}[X_i^r[p_i + 1] = X_i^i[0]] = \text{Pr}[(G + I) \cdot Y_i^r[p_i] \oplus L_i^{p_i} \oplus C_i^r[p_i + 1] = N_i^i],$$

where $L_i^{p_i}$ is the $p_i$-th value of the $p_i$-th encryption query. This is bounded by $1/2^{n/2}$. Now given $L_i^{p_i}$, (the randomness of the first collision), $X_i^r[p_i + 2] = (G + I) \cdot Y_i^r[0] \oplus L_i^{p_i + 1} \oplus C_i^r[p_i + 2]$ has $(n - 1)$-bit entropy of $(G + I) \cdot Y_i^r[0]$ (since $G + I$ has rank $n - 1$). So,

$$\text{Pr}[B7 \land B3^c] \leq q_f \cdot \frac{q}{2^{n/2}} \cdot \frac{2\sigma}{2^{n/2}} = \frac{2\sigma q_f}{2^{3n/2}}.$$

Summarizing, we have

$$\text{Pr}_{\text{ideal}}[\tau \not\in V_{\text{good}}] \leq \text{Pr}[B1] + \text{Pr}[B2] + \text{Pr}[B3] + \text{Pr}[B4 \land B3^c] + \text{Pr}[B5 \land B2^c]$$

$$+ \text{Pr}[B6] + \text{Pr}[B7 \land B3^c] + \text{Pr}[B8]$$

$$\leq 1 + \frac{\sigma q_f}{2^{n/2}} + \frac{2\sigma^2}{2^n} + \frac{2\sigma q_f}{2^{3n/2}}$$

$$\leq \frac{1}{2^{n/2}} + \frac{q_f(n + 1)}{2^{n/2 + 1}} + \frac{3\sigma^2}{2n}.$$  

For the last inequality we assume $q_f \leq 2^n/2$ and $q \leq \sigma$ since otherwise the bound is trivially true. This concludes the proof.

\[\square\]

**Lower Bound of $i_p_{\text{ideal}}(\tau)$.** We consider the ratio of $i_p_{\text{real}}(\tau)$ and $i_p_{\text{ideal}}(\tau)$. In this paragraph we assume that all the probability space, except for $i_p_{\text{ideal}}(\ast)$, is defined over the real game. We fix a good view

$$\tau = ((N_i^i, A_i^i, M_i, Y_i)_{i \in \{1, \ldots, q\}}, (N_i^{r}, A_i^{r}, C_i^{r}, T_i^{r}, Z_i^{r})_{i \in \{1, \ldots, q_r\}}),$$

where $Z_i^r = \bot$. We separate $\tau$ into

$$\tau_c = (N_i^i, A_i^i, M_i, Y_i)_{i \in \{1, \ldots, q\}}$$

and $\tau_d = (N_i^r, A_i^r, C_i^r, T_i^r, Z_i^r)_{i \in \{1, \ldots, q_r\}}$,  

and we first see that for a good view $\tau$, $i_p_{\text{ideal}}(\tau)$ equals to $1/2^{n(q + \sigma)}$.

Now we consider the real case. Since $B1$ and $B2$ do not hold with $\tau$, all inputs of the random function inside $\tau_c$ are distinct, which implies that the released $Y$-values are independent and uniformly random. The variables in $\tau_c$ are uniquely determined given these $Y$-values, and there are exactly $q + \sigma$ distinct input-output of $R$. Therefore, $\text{Pr}[\tau_c]$ is exactly $2^{-n(q + \sigma)}$.

We next evaluate

$$i_p_{\text{real}}(\tau) = \text{Pr}[\tau_c, \tau_d] = \text{Pr}[\tau_c] \cdot \text{Pr}[\tau_d|\tau_c] = \frac{1}{2^{n(q + \sigma)}} \cdot \text{Pr}[\tau_d|\tau_c].$$  

(2)
We observe that $\Pr[\tau_d|\tau_e]$ equals $\Pr[\perp_{\text{all}}|\tau_e]$, where $\perp_{\text{all}}$ denotes the event that $Z^*_i = \perp$
for all $i = 1, \ldots, q_f$, as other variables in $\tau_d$ are determined by $\tau_e$.

Let $\eta$ denote the event that, for all $i = 1, \ldots, q_f$, $X^*_i[j]$ for $p_i < j \leq \ell^*_i$ is not colliding to $X$-values (represented by $X^*_i[j_i]$) in $\tau_e$ and $X^*_i[j]$ for all $j \neq j_i$. For $j = p_i + 1$, the above condition is fulfilled by $B4$ except the case when $X^*_i[p + 1]$ collides with some nonce in $\tau_e$ and it is not the last block. This case, fulfilled by $B5, B6$ and $B7$ holds for $j = p_i + 2$. Thus, depending on the cases, $X^*_i[p_i + 1]$ or $X^*_i[p_i + 2]$ are fresh and almost uniformly random (almost due to 1-bit entropy degradation, since the rank of $G + I$ is $n − 1$). Hence, all the subsequent $X^*$ values are also fresh and almost uniform random due to the property of feedback function (here, observe that the mask addition between the chain of $Y^*_i[j]$ to $X^*_i[j + 1]$ does not reduce the randomness).

Now we have $\Pr[\perp_{\text{all}}|\tau_e] = 1 - \Pr[(\perp_{\text{all}})^c|\tau_e]$, and we also have $\Pr[(\perp_{\text{all}})^c|\tau_e] = \Pr[(\perp_{\text{all}})^c, \eta|\tau_e] + \Pr[(\perp_{\text{all}})^c, \eta'|\tau_e]$. Here, $\Pr[(\perp_{\text{all}})^c, \eta|\tau_e]$ is the probability that at least one $T^*_i$ for some $i = 1, \ldots, q_f$ is correct as a guess of $Y^*_i[\ell^*_i]$. Here $Y^*_i[\ell^*_i]$ is completely random from $\eta$, hence using the union bound we have

$$\Pr[(\perp_{\text{all}})^c, \eta|\tau_e] \leq \frac{q_f}{2^n}.$$ 

For $\Pr[(\perp_{\text{all}})^c, \eta'|\tau_e]$, which is at most $\Pr[\eta'|\tau_e]$, the above observation suggests that this can be evaluated by counting the number of possible bad pairs (i.e., a pair that a collision inside the pair violates $\eta$) among the all $X$-values in $\tau_e$ and all $X^*$-values in $\tau_d$, as in the same manner to the collision analysis of e.g., CBC-MAC using $R$. For each $i$-th decryption query, the number of bad pairs is at most $(q + \sigma + \ell^*_i) \cdot \ell^*_i \leq (q + \sigma + \sigma_f) \cdot \ell^*_i$. Therefore, the total number of bad pairs is $\sum_{1 \leq i \leq q_f} (q + \sigma + \sigma_f) \cdot \ell^*_i \leq (q + \sigma + \sigma_f) \cdot \sigma_f$, and we have

$$\Pr[(\perp_{\text{all}})^c, \eta'|\tau_e] \leq \frac{(q + \sigma + \sigma_f) \cdot \sigma_f}{2^n}.$$ 

Combining all, we have

$$i_{\text{real}}(\tau) = \frac{1}{2^n (q + \sigma_f)} \cdot \Pr[\tau_d|\tau_e] = i_{\text{ideal}}(\tau) \cdot \Pr[\perp_{\text{all}}|\tau_e]$$

$$\geq i_{\text{ideal}}(\tau) \cdot (1 - \Pr[(\perp_{\text{all}})^c, \eta|\tau_e] + \Pr[(\perp_{\text{all}})^c, \eta'|\tau_e])$$

$$\geq i_{\text{ideal}}(\tau) \cdot \left(1 - \frac{q_f + (q + \sigma + \sigma_f) \cdot \sigma_f}{2^n}\right).$$

5.2 Brief summary of security analysis of GIFT

The thorough security analysis of GIFT-128 is provided in Section 4 of [4] and by third party cryptanalysis. Here we highlight several important features.

**Differential cryptanalysis.** Zhu et al. applied the mixed-integer-linear-programming based differential characteristic search method for GIFT-128 and found an 18-round differential characteristic with probability $2^{-109}$ [25], which was further extended to a 23-round key recovery attack with complexity $(Data, Time, Memory) = (2^{120}, 2^{120}, 2^{80})$. We expect that full (40) rounds are secure against differential cryptanalysis.

**Linear cryptanalysis.** GIFT-128 has a 9-round linear hull effect of $2^{-45.99}$, which means that we would need around 27 rounds to achieve correlation potentially lower than $2^{-128}$. Therefore, we expect that 40-round GIFT-128 is enough to resist against linear cryptanalysis.
**Integral attacks.** The lightweight 4-bit S-box in GIFT may allow efficient integral attacks. The bit-based division property is evaluated against GIFT-128 by the designers, which detected a 11-round integral distinguisher.

**Meet-in-the-middle attacks.** Meet-in-the-middle attack exploits the property that a part of key does not appear during a certain number of rounds. The designers and the follow-up work by Sasaki [23] showed the attack against 15-rounds of GIFT-64 and mentioned the difficulty of applying it to GIFT-128 because of the larger ratio of the number of subkey bits to the entire key bits per round; each round uses 32 bits and 64 bits of keys per round in GIFT-64 and GIFT-128, respectively, while the entire key size is 128 bits for both.

## 6 Hardware Implementation Details

The COFB mode was designed with rate 1, that is every message block is processed only once. Such designs are not only beneficial for throughput, but also energy consumption. However the design does need to maintain an additional 64 bit state, which requires a 64-bit register to additionally included in any hardware circuit that implements it. Although this might not be energy efficient for short messages, in the long run COFB performs excellently with respect to energy consumption. The GIFT block cipher was designed with a motivation for good performance on lightweight platforms. The roundkey addition for the cipher is over only half the state and the key schedule being only a bit permutation does not require logic gates. These characteristics make the GIFT family of block ciphers well suited for lightweight applications. In fact as reported in [3], among the block ciphers defined for 128-bit block size GIFT-128 has the lowest hardware footprint and very low energy consumption. Thus GIFT-COFB combines the best of both the advantages of the design ideologies.

### 6.1 Hardware API

NIST has yet to publish a hardware API for the evaluation of the lightweight candidates, and the discussion about the best way forward is still ongoing. Hence we use a minimal API, designed to be simple enough such that it can easily be plugged into existing systems and ensures that any AEAD scheme can be used in all possible configuration such as no associated data or plaintexts blocks and partially filled blocks. Our reasoning for favoring this simpler API is to ensure that no significant energy is consumed to handle the API itself, e.g. the CAESAR HW API [12] requires padding to be done by the circuit, which brings a large array of multiplexers and amplifies the energy consumption for each loaded authenticated data and message block. Nonetheless, a preprocessor circuit could be placed before our AE schemes to ensure CAESAR HW API compatibility. The individual signals are defined in the following way:

**CLK, RST:** System clock and active-low reset signal. We distinguish two different clock rates; 10 MHz for the partially unrolled versions and 20 MHz for the fully unrolled implementations. Inverse gating technique uses only the first phase of the clock cycle to compute the full block cipher call, therefore the clock period is doubled to ensure all glitches are stabilized during this clock phase.

**KEY, NONCE:** Key and nonce vectors. These signals are stable once the circuit is reset and are kept active during the entire computation.

**DATA:** Single data vector that comprises both associated data and regular plaintext material. This choice saves an additional large multiplexer, since all the schemes process associated data and plaintext blocks separately and not in parallel.
EAD, EPT: Single bit signals that indicate whether there are no associated data blocks (EAD) or no plaintext blocks (EPT). Both signals are supplied with the reset pulse and remain stable throughout the computation.

LBLK, LPRT: Single bit signals that indicate whether currently processed block is the last associated data block or the last plaintext block (LBLK), and also whether it is partially filled (LPRT). Both signals are supplied alongside each data block and remain stable during its computation.

BRDY, ARDY: Single bit output indicators whether the circuit has finished processing a data block and a new one can be supplied on the following rising clock edge (BRDY) or the entire AEAD computation has been completed (ARDY).

CT, TAG: Separate ciphertext and tag vectors. This again saves an additional multiplexer in schemes where the ciphertext and tag are not ready at the same time, or they appear at different wires.

Figure 4 details the hardware circuit for round based GIFT-COFB. The mode is designed to require one additional 64-bit state apart from the ones used in the block cipher circuit. Thus the design requires an additional 64-bit register. The initial nonce (denoted by $Nonce$ in the above figure) to the encryption routine, and other control signals are generated.
centrally depending on the length of the plaintext and associated data. Depending on
the phase of operation the state register may need to feed either the nonce, the output
of the GIFT-128 round function, which is the sum of the encryption output, associated
data/plain text and the additional state Delta.

The state Delta is updated by multiplying with suitable filed elements of the form
\( \gamma = \alpha^x (1 + \alpha)^y \) with \( x + y \leq 4 \). Thus we allocate 4 clock cycles to compute the potential
Delta update signal. Depending on the value of \( \gamma \), we update the Delta register by either
doubling, tripling or the identity operation. For example if \( \gamma = \alpha^2 \), we execute doubling for
2 cycles and the identity operation for 2 more cycles. Thus in addition to the field operation,
the circuit requires a 3:1 multiplexer controlled by a Sel signal generated centrally.

### 6.2 Timing

The GIFT-128 block cipher takes \( T_E = 40 \) cycles to complete one encryption function. This is the number of clock cycles required in the encryption of the nonce. Each block
of associated data would take \( T_E \) cycles to process. Before each block of associated data
or plaintext is processed we spend \( D_u = 4 \) cycles to update the Delta. Thus if \( n_n, n_m \)
are the total number of associated data/ message blocks an encryption pass requires
\( T = T_E + (n_n + n_m)(T_E + D_u) \) cycles to compute.

### 6.3 Clock Gating

The state register in Figure 4, requires an additional Enable signal to prevent overwrite
when the Delta register is being computed. A flip-flop with such an additional functionality
usually requires more hardware area. One could circumvent this requirement by gating
the clock signal input to the flip-flop bank, so as to prevent unwanted overwrites. This not
only brings down the area of the circuit but also power and energy consumptions.

### 6.4 Performance

We present the synthesis results for the design. The following design flow was used: first
the design was implemented in VHDL. Then, a functional verification was first done using
Mentor Graphics Modelsim software. The designs were synthesized using the standard cell
library of the 90nm logic process of STM (CORE90GPHVT v2.1.a) with the Synopsys
Design Compiler, with the compiler being specifically instructed to optimize the circuit for
area. A timing simulation was done on the synthesized netlist. The switching activity of
each gate of the circuit was collected while running post-synthesis simulation. The average
power was obtained using Synopsys Power Compiler, using the back annotated switching
activity.

Our smallest implementation of GIFT-COFB (with clock gating) occupied 3271 GE.
The power consumed at an operating frequency of 10 MHz is 118.8 \( \mu \)W. The energy
consumption figures for various lengths of data inputs are given in the first two rows of
Table 2.

### 6.5 Threshold Implementation

The algebraic degree of the GIFT S-box is 3 (same as PRESENT) and as such constructing
threshold circuits is slightly more difficult than for quadratic S-boxes, since it is known
that a threshold construction of any function with algebraic degree \( d \) requires at least \( d + 1 \)
shares [6]. However threshold implementations of the round-based GIFT-128 circuit has
been extensively studied in [11]. Since the S-box is cubic, the number of direct shares it
must be decomposed to needs to be at least 4. However, the authors in [11] report three
philosophies.
Table 2: Implementation results for GIFT-COFB. (Power reported at 10 MHz). Circuits with clock gating are suffixed by "-CG". The notations (xSK), (xS) denote circuits with x shares with/without keypath shared.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Clock</th>
<th>Area</th>
<th>Power</th>
<th>Energy(nJ)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Gated</td>
<td>(GE)</td>
<td>(µW)</td>
<td>AD PT</td>
</tr>
<tr>
<td>Unshared</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COFB</td>
<td>NO</td>
<td>3446</td>
<td>122.0</td>
<td>2.098</td>
</tr>
<tr>
<td>COFB-CG</td>
<td>YES</td>
<td>3271</td>
<td>118.8</td>
<td>2.043</td>
</tr>
<tr>
<td>4 Shares</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COFB(4S)</td>
<td>NO</td>
<td>20292</td>
<td>794.0</td>
<td>13.657</td>
</tr>
<tr>
<td>COFB(4S)-CG</td>
<td>YES</td>
<td>19506</td>
<td>789.6</td>
<td>13.581</td>
</tr>
<tr>
<td>COFB(4S)</td>
<td>NO</td>
<td>22510</td>
<td>896.7</td>
<td>15.423</td>
</tr>
<tr>
<td>COFB(4S)-CG</td>
<td>YES</td>
<td>21697</td>
<td>902.0</td>
<td>15.514</td>
</tr>
<tr>
<td>3 Shares</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COFB(3S)</td>
<td>NO</td>
<td>11186</td>
<td>423.7</td>
<td>14.067</td>
</tr>
<tr>
<td>COFB(3S)-CG</td>
<td>YES</td>
<td>10555</td>
<td>400.6</td>
<td>13.300</td>
</tr>
<tr>
<td>COFB(3S)</td>
<td>NO</td>
<td>13131</td>
<td>504.8</td>
<td>16.759</td>
</tr>
<tr>
<td>COFB(3S)-CG</td>
<td>YES</td>
<td>12179</td>
<td>444.9</td>
<td>14.771</td>
</tr>
</tbody>
</table>

The first decomposes the S-box as the composition $F \circ G$ of two quadratic S-boxes $F, G$, and implements each decomposed S-box using 3 shares with a register separating the two shared implementations, as in [16]. As such complete evaluation of the substitution layer requires 2 clock cycles instead of one. A second optimization uses the fact that the shares of both $G, F$ are algebraically similar to each other, and differs only in the order of input bits. Hence the authors can further apply an optimization due to [13], that reduces the area of the circuit by implementing the shares over 3 cycles, using a multiplexer to permute the order of bits each time. The third is a direct sharing approach using 4 shares.

For this work, since we focus on energy minimization as an additional optimizable metric, we focus on only the constructions that evaluate the Substitution layer in at most two cycles. Thus we adopted two approaches:

1. **Direct Sharing using 4 shares**: A direct implementation using 4 shares is a straightforward one as the GIFT s-box has an algebraic degree of 3. This circuit requires 4 registers to implement each state share as well as 4 registers to store the shared values of $\Delta$. One may choose or not to share the key path which would require one or 4 registers to implement the keyschedule.

Since the s-box computation can be done in one cycle, the number of cycles that this circuit takes to compute the ciphertext/tag pair is the same as the unshared version. Figure 5, gives a block level representation of the circuit (the key path is omitted for simplicity). As can be seen in the figure, depending on whether the key path is shared or not we need 3/6 random 128 bit masks to do all computations.

2. **Decomposing as $F \circ G$ using 3 shares**: Since the GIFT s-box is quadratic, it can be decomposed as $F \circ G^1$, where $F$ and $G$ are quadratic s-boxes. Each of these functions can be constructed using 3 shares. To prevent propagation of glitches from the $G$ to the $F$ layer, we need to put register banks in between them. Hence one substitution layer evaluation is carried out over 2 clock cycles, computation of an

\[\text{for the exact description of the algebraic expressions for the shared } F, G, S \text{ boxes please refer to [11]}\]
Figure 5: GIFT-COFB using 4 shares (key path is omitted for simplicity)

encryption operation requires \(2 \cdot T_E = 80\) cycles. Hence an encryption pass requires
\[T = 2 \cdot T_E + (n_a + n_m)(2 \cdot T_E + D_u)\] cycles to compute. So this type of construction is considerably slower. On the other hand, from Figure 6, it is clear that depending on whether the key path is shared, the construction requires 2/4 random 128 bit masks.

Table 2 tabulates detailed experimental results of all threshold circuits constructed with 3 as well as 4 shares. The smallest threshold circuit, is the one with 3 shares after applying clock gating and occupies 10555 GE.

7 Software Implementation Details

In this section, we discuss software implementation of GIFT-128. Due to its inherent bitslice structure, it seems natural to consider that the most efficient software implementations of GIFT-128 will be a bitslice strategy, which also offers a constant-time guarantee. This is also the reason why we have used bitslice loading of plaintext/key when using GIFT-128 in the operating mode. The COFB mode being rate-1 and quite simple, as long as a non-parallel implementation is used the entire GIFT-COFB primitive will have similar throughput to GIFT-128 as the input to be handled becomes longer.

Indeed, since COFB is not a parallel operating mode, one can’t use several consecutive encryption blocks, which might prevent us to fully use the power of bitslice implementations. More precisely, as the GIFT-128 Sbox size is 4 bits, one will need \(x\) parallel blocks on a 32x-bit architecture. This fits perfectly architecture of 32-bit or less. For bigger registers, one can simply use dummy extra blocks (blocks with random or zero data) to simulate a real bitslice implementation (1 dummy block for 64-bit registers, 3 dummy blocks for 128-bit registers, etc.), which will of course lead to an efficiency penalty. We note however that on a server communicating with several clients, one could consider avoiding the dummy blocks penalty by ciphering all these communications in parallel.

Assume then an architecture with 32-bit registers. The 128-bit plaintext, already in bitslice form, is directly loaded in four registers (similarly for the key). The implementation of the Sbox is straightforward and is provided below. It requires only 6 XORs, 3 ANDs, 1...
OR and 1 NOT instruction.

Applying the subkeys and constants is also straightforward with XOR instructions (one could even consider that subkeys/constants are precomputed and stored in memory). A much more difficult task if to apply the bit permutation, as it is quite costly the move individual bits around in software. A crucial property of the GIFT bit permutations is that a bit in slice $i$ is always sent to the same slice $i$ during this permutation. Thus, applying the bit permutation layer means simply permuting the ordering of the bits inside the registers independently. Fortunately, we have found a new representation of the GIFT-64 and GIFT-128 bit permutations that makes it efficient and simple to implement in software. This strategy, named fix-slicing [2], indeed leads to very efficient one-block constant-time GIFT-128 implementations on 32-bit architectures such as ARM Cortex-M family of processors (79 cycles/byte on ARM Cortex-M3), making GIFT-COFB one of the most efficient candidate according to microcontroller benchmarks [17, 24]. Using smaller architecture will not be an issue as we will actually save more operations comparatively, since part of the bit permutation can be done by proper unrolling and register scheduling. This is confirmed with 8-bit AVR benchmarks [17, 24] where GIFT-COFB is again ranked among the top candidates. Note that using exactly this implementation will also provide decent performance on recent high-end processors (and excellent performances if parallel computations of GIFT-COFB instances are considered and vector instructions are used).
8 Other Implementation/Benchmarking Results on GIFT-COFB

8.1 Software Benchmarking by Renner et. al. [17]

This benchmark results are mainly obtained on five different microcontroller unit platforms. The results are based on the custom made performance evaluation framework, introduced at the NIST LWC Workshop in November 2019. Precisely, the result contains speed, ROM and RAM and benchmarks for software implementations of the 2nd round candidates. We would like to point that, though GIFT-COFB is not designed for microcontrollers, it still stands among the top five designs. The detailed table can be found in [17].

8.2 Software Implementations and Benchmarking by Weatherley [24]

Rhys Weatherley provides efficient 8-bit AVR and 32-bit ARM Cortex-M3 implementations of GIFT-COFB using the fix-slicing strategy. All these implementations are available on the corresponding GitHub repository and benchmarks on these two platforms are provided. Again, we point that, though GIFT-COFB is not designed for microcontrollers, it still ranks at 3rd place among all NIST competition candidates.

8.3 Hardware Benchmarking by Rezvani et. al. [18]

This work implements 6 NIST LWC Round 2 candidates SpoC, GIFT-COFB, COMET-AES, COMET-CHAM, ASCON, and Schwaemm and Esch, on Artix-7, Spartan-6, and Cyclone-V. The results show that SpoC, GIFT-COFB and COMET-CHAM achieves the lowest increase in dynamic power with increasing frequency.

8.4 Hardware Benchmarking by Rezvani et. al. [19]

This work implements three NIST LWC Round 2 candidates GIFT-COFB, SpoC and Spook and few other CAESAR candidates on Artix7. All the implementations are validated on the CAESAR API. The results depict that GIFT-COFB has the highest throughput-to-area (TPA) ratio at 0.154 Mbps/LUT which is a 4.4 factor margin over Spook.

9 Conclusion

In this work, we presented a lightweight and efficient AEAD scheme GIFT-COFB that instantiate AEAD operating mode COFB with block cipher GIFT. In comparison with the previous publications [3, 8], small but significant tweaks are introduced to both COFB and GIFT to further improve the efficiency and performance. With provable security bounds for the operating mode and thorough security analysis, including third party cryptanalysis, on the underlying block cipher primitive, GIFT-COFB is one of the more well-established and competitive candidates in the NIST lightweight cryptography competition.

References


