GIFT-COFB is Tightly Birthday Secure with Encryption Queries

Akiko Inoue and Kazuhiko Minematsu

NEC, Kawasaki, Japan
a_inoue@nec.com,k-minematsu@nec.com

Abstract. GIFT-COFB is a finalist of NIST Lightweight cryptography project that aims at standardizing authenticated encryption schemes for constrained devices. It is a block cipher-based scheme and comes with a provable security result. This paper studies the tightness of the provable security bounds of GIFT-COFB, which roughly tells that, if instantiated by a secure n-bit block cipher, we need $2^{n/2}$ encrypted blocks or $2^{n/2}/n$ decryption queries to break the scheme. This paper shows that the former condition is indeed tight, by presenting forgery attacks that work with $2^{n/2}$ encrypted blocks with single decryption query. This fills the missing spot of previous attacks presented by Khairallah, and confirms the tightness of the security bounds with respect to encryption. We remark that our attacks work independent of the underlying block cipher.

1 Introduction

NIST Lightweight cryptography project[1] aims at standardizing authenticated encryption (AE) schemes for constrained devices. It started in Feburary 2019. In March 2021, 10 finalists were announced. GIFT-COFB [1] is one of these finalists. It is a variant of the COFB block cipher mode of operation proposed at CHES 2017 [3]. It is designed to enable a fast operation with small footprint. The original COFB works with any block cipher, and GIFT-COFB specifies 128-bit block version of GIFT [2] as its internal block cipher.

The provable security of GIFT-COFB and COFB has been studied [1, 3], and the security bounds with respect to the combined notion of privacy (confidentiality) and authenticity (integrity) were presented. In particular, assuming the nonce-respecting adversary and that the underlying block cipher is a random permutation, GIFT-COFB's bound is roughly $\sigma^2/2^n + nq_d/2^{n/2}$ for $\sigma = \sigma_e + \sigma_d + q_e + q_d$, where σ_e (σ_d) denotes the total queried blocks in encryption (decryption) queries, and q_e (q_d) denotes the number of encryption (decryption) queries.

This bound suggests that, if

(1) σ_e reaches $2^{n/2}$, or
(2) σ_d reaches $2^{n/2}$, or

[1] https://csrc.nist.gov/projects/lightweight-cryptography

(3) q_d reaches $2^{n/2}/n$,

the bound reaches 1 hence no security guarantee is possible.

Recently Khairallah [4,5,6] studied the tightness of the bound. He showed attacks with $q_d = 2^{n/2}$ with about $\sigma_e = 2^{n/2}$ or $\sigma_e = 2^{n/4}$, called Weak Key attack and Mask collision attack [4, 5]. He finally showed one with $q_e = 1$, $\sigma_e = O(1)$ (few blocks) and $q_d = 2^{n/2}$, called Mask Presuming attack [6]. The last one implies that the tightness condition (3) has only the small gap of $\log n$ factor. For (2) it remains unsolved. Both might be an artifact in the proofs however there is no clear answer so far.

It is natural to ask the tightness of (1). In this paper, we present an attack with $\sigma_e = 2^{n/2}$ and $q_d = 1$. As in the previous attacks, this attack breaks the authenticity, and matches the aforementioned bound. Hence, our result showed that (1) is indeed tight.

Comparison of attack complexity. Table 1 shows the required complexities for the attacks against GIFT-COFB. All are forgery attacks that break authenticity. The block size is $n = 128$ and the maximum input block length of GIFT-COFB is 2^{51}, hence the Attack 1 at least needs $\sigma_e = 2^{128-51\cdot 2+51} = 2^{77}$. This attack does not achieve birthday complexity of $2^{n/2}$, but we show it as a warm-up.

Our attacks complement [6] with regard to the balance of required encryption and decryption complexity.

Table 1: Required complexities for successful forgery attacks. For Attack 1, each query is 2^ℓ blocks. GIFT-COFB specifies $n = 128$ and $\ell \leq 2^{51}$.

	Enc complexity (σ_e)	Dec complexity (q_d)
Weak Key [4]	$2^{n/2}$	$2^{n/2}$
Mask Collision [5]	$2^{n/4}$	$2^{n/2}$
Mask Presuming [6]	$O(1)$	$2^{n/2}$
Attack 1 (Ours)	$2^{n-\ell^2+\ell}$	1
Attack 2 (Ours)	$2^{n/2}$	1

2 Notation

For the specification of GIFT-COFB refer to the specification document [1]. We use the same notations as [1] to describe our attacks. See also Figure 1.

3 Attack 1

Our first attack searches over the collision of the mask value within one encryption query. A mask is written as $2^i 3^j L$ for some integer i and j and L is the first

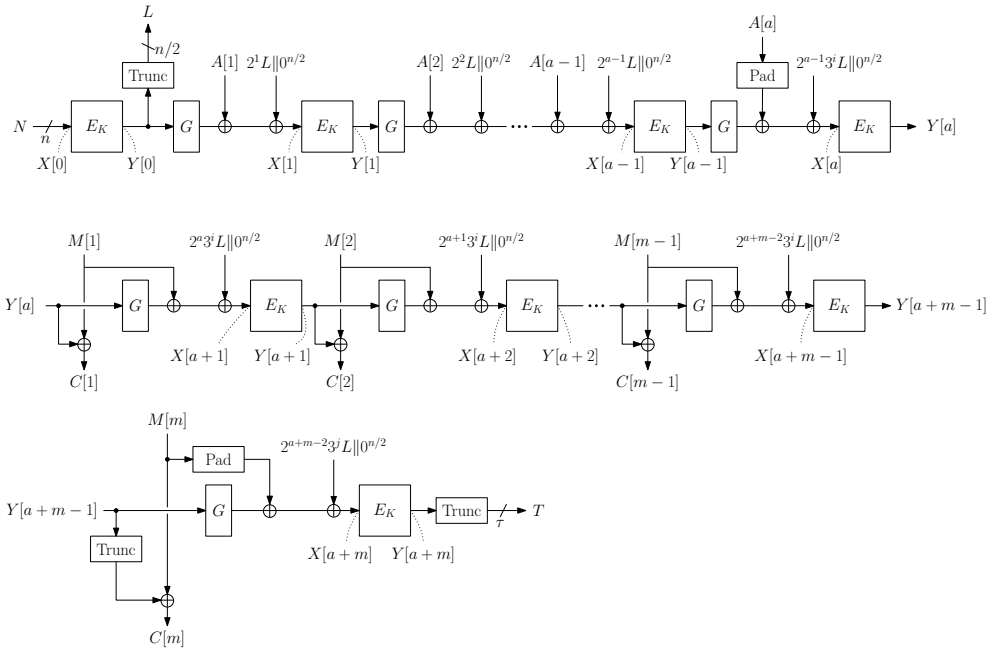

Fig. 1: GIFT-COFB.

$n/2$ bits of $E_K(N)$ for nonce N and the block cipher encryption E_K. The index i works as a block counter, and j works as a domain separator, and 2^i and 3^j denotes the elements of $\mathrm{GF}(2^{n/2})$, $\mathtt{x}^i$ and $(\mathtt{x}+\mathtt{1})^j$ [1]. In the attack 1, we derive L from one encryption query whose length is long enough to occur the collision of the inputs of block cipher. Specifically, the attack is as follows. For the ease of sake, AD is always empty, the last message block is always complete. The tag length is n bits as specified.

1. The attacker queries (N, M) to the encryption oracle and obtain its outputs. Suppose that she obtains (N, M, C, T) such that $M = M[1] \,\|\, \cdots \,\|\, M[m]$ and $C = C[1] \,\|\, \cdots \,\|\, C[m]$.
2. For $i \in \{1, \ldots, m\}$, the attacker derives $Y[i]$ by computing $M[i] \oplus C[i]$.
3. Suppose that the collision $Y[i] = Y[j]$ occurs for $i \neq j$ and $i, j \in \{2, \ldots, m\}$. Then $X[i] = X[j]$ holds, so the attacker obtains $G(Y[i-1]) \oplus M[i-1] \oplus 2^{i-1}3^2 L \,\|\, 0^{n/2} = G(Y[j-1]) \oplus M[j-1] \oplus 2^{j-1}3^2 L \,\|\, 0^{n/2}$. From this equation, she can derive L.
4. The attacker queries (N', C', T') to the verification (decryption) oracle such that $N' = N$, $T' = Y[m]$, $C' = C[1] \,\|\, \cdots \,\|\, C[m-2] \,\|\, C'[m-1]$, and

$$C'[m-1] = Y[m-1] \oplus M[m-1] \oplus 2^{m-1}3^2 L \,\|\, 0^{n/2} \oplus 2^{m-2}3^3 L \,\|\, 0^{n/2}.$$

Let T^* be the valid tag for (N', C'), and suppose $T^* = E_K(X'[m])$. Then the following equation holds.

$$\begin{aligned}
X'[m] &= G(Y'[m-1]) \oplus Y'[m-1] \oplus C'[m-1] \oplus 2^{m-2}3^3L \,\|\, 0^{n/2} \\
&= G(Y[m-1]) \oplus Y[m-1] \oplus C'[m-1] \oplus 2^{m-2}3^3L \,\|\, 0^{n/2} \\
&= G(Y[m-1]) \oplus Y[m-1] \oplus Y[m-1] \oplus M[m-1] \\
&\quad \oplus 2^{m-1}3^2L \,\|\, 0^{n/2} \oplus 2^{m-2}3^3L \,\|\, 0^{n/2} \oplus 2^{m-2}3^3L \,\|\, 0^{n/2} \\
&= G(Y[m-1]) \oplus M[m-1] \oplus 2^{m-1}3^2L \,\|\, 0^{n/2} \\
&= X[m].
\end{aligned}$$

Thus, $T^* = E_K(X'[m]) = E_K(X[m]) = Y[m]$ holds. This forgery query is not trivial (*i.e.*, not trivially obtained by the encryption query) and will be accepted with probability 1.

Complexity. To expect a collision between masks in the above procedure 3, we need $m \approx O(2^{n/2})$ since $Y[\cdot]$ is n bits. However, when $n = 128$, GIFT-COFB accepts 2^{51} input blocks at the maximum, due to the limitation of mask function [1] (also see the proposition 6 of [7]). Therefore, we need to repeat this procedure about 2^{26} times, each of 2^{51} blocks. Thus, the attacker needs roughly $\sigma_e \approx 2^{77}$ and $q_d = 1$ as described earlier.

4 Attack 2

We present a refined attack that achieves truly birthday complexity. In the Attack 2, we derive the difference of two mask values from two encryption queries taking different nonce values. While the Attack 1 crucially relies on that fact that the mask collision involves single L, it is still possible to mount a forgery attack by finding a collision involving two Ls. Specifically, the attack is as follows. Again we assume empty AD, and the last message block is always complete. The tag length is n bits as specified.

1. The attacker queries (N_1, M_1) and (N_2, M_2) to the encryption oracle and obtain their outputs. Suppose she obtains (N_1, M_1, C_1, T_1) and (N_2, M_2, C_2, T_2) such that $M_1 = M_1[1] \,\|\, \cdots \,\|\, M_1[m]$, $M_2 = M_2[1] \,\|\, \cdots \,\|\, M_2[m]$, and $m \geq 3$.
2. For $i \in \{1, \ldots, m\}$ and $j \in \{1, 2\}$, the attacker derives $Y_j[i]$ by computing $M_j[i] \oplus C_j[i]$. Let $Y_j[m+1] = T_j$.
3. Suppose that the collision $Y_1[a] = Y_2[b]$ occurs for $a, b \in \{2, \ldots, m\}$, $a \leq b$ [2], and $(a, b) \neq (2, m)$. Then $X_1[a] = X_2[b]$ holds, so the attacker obtains $G(Y_1[a-1]) \oplus M_1[a-1] \oplus 2^{a-1}3^2L_1 \,\|\, 0^{n/2} = G(Y_2[b-1]) \oplus M_2[b-1] \oplus 2^{b-1}3^2L_2 \,\|\, 0^{n/2}$, where L_1 and L_2 are the mask origin values of queries (N_1, M_1, C_1, T_1) and (N_2, M_2, C_2, T_2), respectively. From this equation, she obtains the difference of mask values, $\Delta := 2^{a-1}3^2L_1 \oplus 2^{b-1}3^2L_2$.

[2] We can assume $a \leq b$ without loss of generality.

4. Suppose $b \neq m$ [3]. The attacker queries (N', C', T') to the verification oracle such that $N' = N_1$, $T' = T_1$, $C' = C'[0] \| \cdots \| C'[m]$, where

$$
\begin{aligned}
&C'[i] = C_1[i], \quad (i \neq a,\, i \neq a+1)\\
&C'[a] = C_2[b] \oplus 2\Delta \| 0^{n/2},\\
&C'[a+1] = Y_2[b+1] \oplus M_1[a+1] \oplus G(Y_2[b+1]) \oplus G(Y_1[a+1]).
\end{aligned}
$$

The following equations hold.

$$
\begin{aligned}
X'[a+1] &= G(Y'[a]) \oplus Y'[a] \oplus C'[a] \oplus 2^a 3^2 L_1 \| 0^{n/2}\\
&= G(Y_1[a]) \oplus Y_1[a] \oplus C'[a] \oplus 2^a 3^2 L_1 \| 0^{n/2}\\
&= G(Y_2[b]) \oplus Y_2[b] \oplus C_2[b] \oplus 2\Delta \| 0^{n/2} \oplus 2^a 3^2 L_1 \| 0^{n/2}\\
&= G(Y_2[b]) \oplus Y_2[b] \oplus C_2[b] \oplus 2(2^{a-1} 3^2 L_1 \oplus 2^{b-1} 3^2 L_2) \| 0^{n/2} \oplus 2^a 3^2 L_1 \| 0^{n/2}\\
&= G(Y_2[b]) \oplus Y_2[b] \oplus C_2[b] \oplus 2^b 2^3 L_2 \| 0^{n/2}\\
&= X_2[b+1],\\
X'[a+2] &= G(Y'[a+1]) \oplus Y'[a+1] \oplus C'[a+1] \oplus 2^{a+1} 3^j L_1 \| 0^{n/2}\\
&= G(Y_2[b+1]) \oplus Y_2[b+1] \oplus C'[a+1] \oplus 2^{a+1} 3^j L_1 \| 0^{n/2}\\
&= G(Y_2[b+1]) \oplus Y_2[b+1] \oplus Y_2[b+1] \oplus M_1[a+1]\\
&\quad \oplus G(Y_2[b+1]) \oplus G(Y_1[a+1]) \oplus 2^{a+1} 3^j L_1 \| 0^{n/2}\\
&= G(Y_1[a+1]) \oplus M_1[a+1] \oplus 2^{a+1} 3^j L_1 \| 0^{n/2}\\
&= X_1[a+2],
\end{aligned}
$$

where $j = 2$ if $a \neq m-1$. Otherwise, $j = 3$. Since $C'[i] = C_1[i]$ for $i \neq a$ and $i \neq a+1$, $X'[m+1] = X_1[m+1]$ and $T^* = E_K(X'[m+1]) = E_K(X_1[m+1]) = T_1 = T'$. As the probability of $X_1[a+1] = X_2[b+1]$ is expected to be small, this forgery query is not trivial and will be accepted with probability 1.

Extensions. The above attack poses some limitations such as $b \neq m$. This can be circumvented as follows.

1. When $b = m$ *i.e.*, $Y_1[a] = Y_2[m]$, the attack can be mounted if $a \neq 2$. The attacker follows the procedures 1 – 3 in the Attack 2. Then she queries (N', C', T') to the verification oracle such that $N' = N_2$, $T' = T_2$, $C' = C'[0] \| \cdots \| C'[m]$, where

$$
\begin{aligned}
&C'[i] = C_2[i], \quad (i \neq m-2,\, i \neq m-1)\\
&C'[m-2] = Y_2[m-2] \oplus M_1[a-2] \oplus G(Y_2[m-2]) \oplus G(Y_1[a-2]) \oplus 2^{-1}\Delta,\\
&C'[m-1] = Y_1[a-1] \oplus M_2[m-1] \oplus G(Y_1[a-1]) \oplus G(Y_2[m-1]).
\end{aligned}
$$

[3] The case $b = m$ is described later.

As above, the following equations hold.

$$\begin{aligned}
X'[m-1] &= G(Y'[m-2]) \oplus Y'[m-2] \oplus C'[m-2] \oplus 2^{m-2}3^2L_2 \,\|\, 0^{n/2} \\
&= G(Y_2[m-2]) \oplus Y_2[m-2] \oplus C'[m-2] \oplus 2^{m-2}3^2L_2 \,\|\, 0^{n/2} \\
&= G(Y_2[m-2]) \oplus Y_2[m-2] \oplus Y_2[m-2] \oplus M_1[a-2] \\
&\quad \oplus G(Y_2[m-2]) \oplus G(Y_1[a-2]) \\
&\quad \oplus 2^{-1}(2^{a-1}3^2L_1 \oplus 2^{m-1}3^2L_2) \,\|\, 0^{n/2} \oplus 2^{m-2}3^2L_2 \,\|\, 0^{n/2} \\
&= M_1[a-2] \oplus G(Y_1[a-2]) \oplus 2^{a-2}3^2L_1 \,\|\, 0^{n/2} \\
&= X_1[a-1], \\
X'[m] &= G(Y'[m-1]) \oplus Y'[m-1] \oplus C'[m-1] \oplus 2^{m-1}3^2L_2 \,\|\, 0^{n/2} \\
&= G(Y_1[a-1]) \oplus Y_1[a-1] \oplus C'[m-1] \oplus 2^{m-1}3^2L_2 \,\|\, 0^{n/2} \\
&= G(Y_1[a-1]) \oplus Y_1[a-1] \oplus Y_1[a-1] \oplus M_2[m-1] \\
&\quad \oplus G(Y_1[a-1]) \oplus G(Y_2[m-1]) \oplus 2^{m-1}3^2L_2 \,\|\, 0^{n/2} \\
&= M_2[m-1] \oplus G(Y_2[m-1]) \oplus 2^{m-1}3^2L_2 \,\|\, 0^{n/2} \\
&= X_2[m] (= X_1[a]).
\end{aligned}$$

Since $C'[m] = C_2[m]$, $T^* = T_2 = T'$ holds.

2. When $a = b = m + 1$, the attacker can mount almost the same attack as the case of $b = m$.
3. When the collision of $Y[\cdot]$ occurs in one encryption query, the attacker can mount the Attack 1.

Complexities. The attacker needs roughly $\sigma_e = 2^{n/2}$ encrypted blocks and $q_d = 1$ for the attack 2. Suppose that the attacker queries plaintext of m blocks q_e times. At least, there are $\binom{(m-2)q_e}{2}$ possible pairs of $Y[\cdot]$ to induce the above attacks (including other cases). Thus, $\sigma_e = 2^{n/2}$ is necessary and sufficient.

Acknowledgments

The authors would like to thank Tetsu Iwata, Yu Sasaki and Mustafa Khairallah for useful feedback.

References

1. Banik, S., Chakraborti, A., Iwata, T., Minematsu, K., Nandi, M., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: GIFT-COFB. Submission to NIST Lightweight Cryptography (2019)
2. Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: GIFT: A Small Present - Towards Reaching the Limit of Lightweight Encryption. In: CHES. Lecture Notes in Computer Science, vol. 10529, pp. 321–345. Springer (2017)

3. Chakraborti, A., Iwata, T., Minematsu, K., Nandi, M.: Blockcipher-Based Authenticated Encryption: How Small Can We Go? In: CHES. Lecture Notes in Computer Science, vol. 10529, pp. 277–298. Springer (2017)
4. Khairallah, M.: Weak Keys in the Rekeying Paradigm: Application to COMET and mixFeed. IACR Trans. Symmetric Cryptol. **2019**(4), 272–289 (2019)
5. Khairallah, M.: Observations on the Tightness of the Security Bounds of GIFT-COFB and HyENA. Cryptology ePrint Archive, Report 2020/1463 (2020), `https://eprint.iacr.org/2020/1463`
6. Khairallah, M.: Security of COFB against Chosen Ciphertext Attacks. Cryptology ePrint Archive, Report 2021/648 (2021), `https://eprint.iacr.org/2021/648`
7. Rogaway, P.: Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 16–31. Springer, Heidelberg (Dec 2004). https://doi.org/10.1007/978-3-540-30539-2_2