Forgery attack on the authentication encryption GIFT-COFB*

Zhe CEN[1], Xiutao FENG[2]**, Zhangyi Wang[3] and Chunping CAO[1]

[1] Department of Computer Science and Technology, University of Shanghai for Science and Technology, Shanghai 200093, China
[2] Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Sciences, CAS, Beijing 100089, China
[3] School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China

Abstract. GIFT-COFB is one of the round 2 candidate algorithms of NIST lightweight cryptography. In this paper we present a forgery attack on GIFT-COFB. In our attack, the block cipher GIFT is viewed as a block box, and for an arbitrary ciphertext (C, T) with at least twice the block length of GIFT-COFB, if an attacker knows arbitrary two successive blocks of message M corresponding to C, he/she can forge infinite new valid ciphertexts (C', T') such that for each (C', T'), there exists a plaintext M' satisfying (C', T')=GIFT-COFB(M'). The above result shows that GIFT-COFB can not resist against the forgery attack.

Keywords: Lightweight cryptography, GIFT-COFB, forgery attack

1 Introduction

In recent years, there are increasing areas in which small computing devices were used to finish some simple work, such as Radio-Frequency Identification (FRID) tags, sensor node, smart card and so on. However, due to the effectiveness and implementation cost, the traditional cryptographic algorithms might not be able to fit well into the limited recourses of constrained environment. Thus National Institute of Standards and Technology (NIST) started a lightweight cryptography standardization project [1] that aimed to develop a strategy for the standardization of lightweight cryptography algorithms. Total 56 cipher algorithms were selected as the round 1 candidate algorithms in the lightweight cryptography standardization project, both of which are authenticated ciphers. At present, 32 of them were left and selected the round 2 candidate algorithms.

Forgery attack is a common attack on authenticated ciphers. Its main goal is to forge a new legal pair of ciphertext and authentication tag from one or some known 2-tuples (C, T) or 3-tuples (M, C, T), where M denotes a plaintext, C and

* This work was supported by National Natural Science Foundation (Grant 61572491, 61972297) and National Key Research and Development Project(Grant 2018YFA0704705).

** Corresponding author: fengxt@amss.ac.cn

T denote its corresponding ciphertext and authentication tag respectively. In [2], Yuan et. al proposed a general distinguishing attack which leads to a forgery attack directly on Alred construction[3]. In [4], Feng et al. presented a state recovery attack against PANDA-s and further deduced a forgery attack against PANDA-s. In [5], Meltem et al. listed some forgery attacks of the round 1 candidate algorithms which NIST announced, including Bleep64 [6] [7], CLAE [8], FlexAEAD [9] [10], GAGE and InGAGE [11], HERN and HERON [12], Liliput-AE [13] [14], Limdolen [15] [16], Qameleon [17], Quartet [18], Remus [19], and so on.

GIFT-COFB [20] is one of the round 2 candidate algorithms in the ongoing NIST lightweight cryptography standardization project. It is an authenticated cipher designed by S. Ba et al. by means of instantiating the block cipher COFB (Combined FeedBack)[21] based on AEAD (Authenticated Encryption with Associated Data) mode with the block cipher GIFT-128[22]. GIFT-COFB takes a 128-bit encryption key, a 128-bit nonce, an arbitrary length associated data and an arbitrary length plaintext as input and outputs a ciphertext with the same length as plaintext and a 128-bit authentication tag. In this work we regard GIFT-128 as a black box and present a forgery attack on GIFT-COFB. For a given pair of ciphertext and authentication tag (C, T), if two successive blocks of message M corresponding to C are known, our attack will work and infinite new legal ciphertext C' and authentication tag T' can be forged, that is, for each (C', T'), there exists a message M' such that $(C', T') = \text{GIFT-COFB}(M')$. Our result shows that GIFT-COFB can not resist to the forgery attack.

The rest of the paper is organized as follows: in section 2, we recall GIFT-COFB briefly, and in section 3, we propose a forgery attack of GIFT-COFB. Finally we conclude this paper in section 4.

2 GIFT-COFB

In this section we recall GIFT-COFB briefly. GIFT-COFB is an authentication encryption algorithm with the COFB mode structure based on the block cipher GIFT-128. Since our attack is irrelevant to the initialization and associated data process of GIFT-COFB, we omit them and only introduce the process of plaintext encryption of GIFT-COFB. At the same time, we regard GIFT-128 as a black box which is denoted by E_k since our attack also does not involve internal details in GIFT-128. More details about GIFT-COFB can be found in [20] .

GIFT-COFB is a combination of two algorithms: an authenticated encryption algorithm COFB-ε_K and a verified decryption algorithm COFB-D_K. The former takes as input an encryption key K of length $k = 128$ bits, a nonce N of length $n = 128$ bits, an associated data A and a message M, both of which have an arbitrary length. Its output is an authenticated ciphertext C with the same length as M and an authentication tag T of size $t = 128$ bits. The latter takes as input an encryption key K, a nonce N, an associated data A, a ciphertext C and an authenticated tag T, and outputs a plaintext M with the same length as C only if the verification of tag is correct, and $\perp$ (error symbol) if the tag verification fails.

In COFB-ε_K, we get a 128-bit $Y[0]$ after the initialization and associated data process and take it as the input of the process of plaintext encryption, which is shown in Fig. 1.

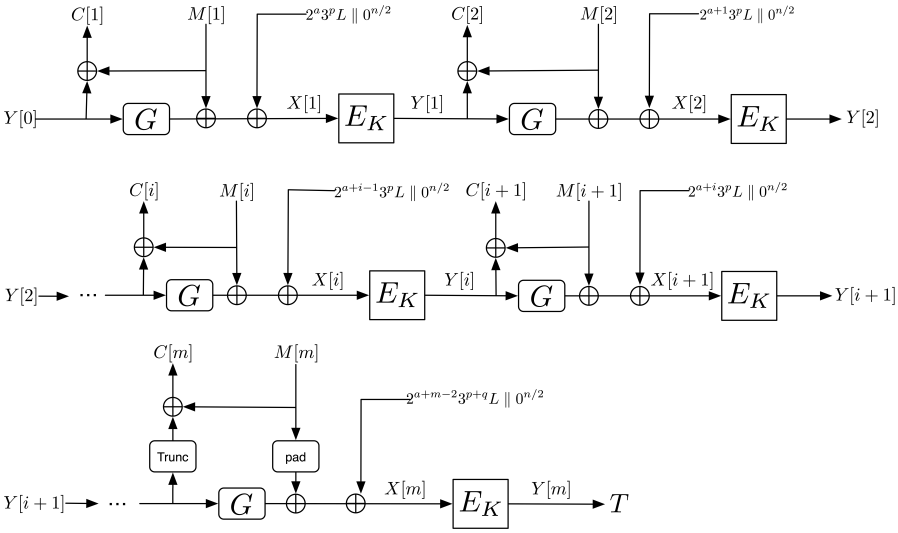

Fig. 1. The process of plaintext encryption in COFB-ε_K

Let $M = M[1] \parallel M[2] \parallel \cdots \parallel M[m]$ be the plaintext, $\mathrm{Trunt}_t(X)$ be the first t bits of X, $a = |A|/n$, $F_{2^{64}}$ be the finite field defined by the primitive polynomial $p_{64}(X) = X^{64} + X^4 + X^3 + X + 1$ and α be a root of $p_{64}(X) = 0$. Denote by ε an incomplete block. For any $b \in F_{2^{64}}$, $2^i b$ and $3^i b$ denote $\alpha^i b$ and$(1+\alpha)^i b$ respectively. The encryption is described in Algorithm 1:

Feedback Function G. Let $Y = Y[1] \parallel Y[2] \in (0,1)^n$, where $Y[1], Y[2] \in (0,1)^{n/2}$. The feedback function G is defined as

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

where $X \lll r$ means the left rotation of a string X by r bits.

3 Forgery attack on GIFT-COFB

Let (C, T) be a pair of ciphertext and authentication tag transported in some communication session, where $C = C[1] \parallel C[2] \parallel \cdots \parallel C[m]$ and m is an integer such that $m \geq 2$. Denote by $M = M[1] \parallel M[2] \parallel \cdots \parallel M[m]$ the plaintext corresponding to C in GIFT-COFB. In our attack, we assume at least

Algorithm 1 The encryption of COFB-ε_K

```
$L \leftarrow Trunc_{n/2}(Y[0])$
$(M[1], ..., M[m]) \xleftarrow{n} Pad(M)$
**if** $|A| \mod n = 0$ *and* $A \neq \epsilon$ **then**
    $p = 1$
**else**
    $p = 2$
**end if**
**for** $i = 1$ to $m - 1$ **do**
    $C[i] \leftarrow M[i] \oplus Y[i-1]$
    $X[i] \leftarrow M[i] \oplus G(Y[i-1]) \oplus 2^{a+i-1}3^{p}L \parallel 0^{n/2}$
    $Y[i] \leftarrow E_K(X[i])$
**end for**
**if** $|M[m]| \mod n = 0$ **then**
    $q = 1$
**else**
    $q = 2$
**end if**
$C[m] \leftarrow M[m] \oplus Y[m-1]$
$X[m] \leftarrow M[m] \oplus G(Y[m-1]) \oplus 2^{a+m-2}3^{p+q}L \parallel 0^{n/2}$
$Y[m] \leftarrow E_K(X[m])$
$T = Y[m]$
```

2 successive blocks in M are known. According to Algorithm 1 and Fig. 1, it is known that the input $X[i]$ and output $Y[i]$ of E_K are computed by the following equations:

$$Y[i] = M[i+1] \oplus C[i+1],$$
$$X[i] = G(Y[i-1]) \oplus M[i] \oplus D(i),$$

where $D(i)$ is defined as:

$$D(i) = \begin{cases} 2^{(a+i-1)}3L \parallel 0^{n/2} & i \in \{1, 2, ..., m-1\} \\ 2^{(a+i-2)}3^2L \parallel 0^{n/2} & i = m \end{cases}.$$

3.1 A basic forgery attack with two blocks

In this section, we only consider a simple situation that $m = 2$. The process of plaintext encryption is shown in Fig. 2. We have the following equations:

$$X[1] = G(Y[0]) \oplus M[1] \oplus D(1),$$
$$Y[1] = M[2] \oplus C[2],$$
$$Y[0] = M[1] \oplus C[1].$$

Below we construct a pair of ciphertext and authenticated tag (C', T'), where $C' = C'[1] \parallel C'[2]$. Let $M' = M'[1] \parallel M'[2]$ be the plaintext corresponding to C'.

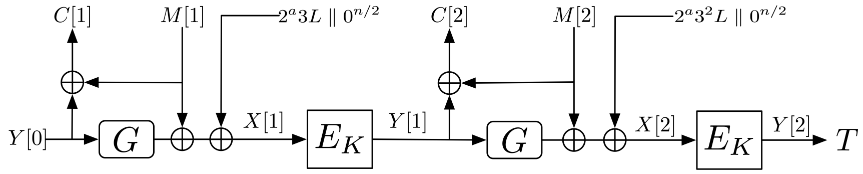

Fig. 2. The encryption of plaintext with two blocks

In order to distinguish all variables deduced by M and C, we assume all variables with prime are derived from M' and C' in Fig. 2. Here we take $C'[1] = C[1]$ and $X'[2] = X[1]$. It follows that $Y'[1] = Y[1]$ and $M'[1] = M[1]$. From Fig. 2, we have

$$\begin{aligned} M'[2] &= X'[2] \oplus G(Y'[1]) \oplus D(2), \\ C'[2] &= M'[2] \oplus Y'[1], \\ T' &= Y'[2] = E_K(X'[2]) = E_K(X[1]) = Y[1]. \end{aligned}$$

Therefore,

$$\begin{aligned} M'[2] &= X[1] \oplus G(M[2] \oplus C[2]) \oplus D(2) \\ &= G(Y[0]) \oplus M[1] \oplus D(1) \oplus G(M[2] \oplus C[2]) \oplus D(2) \\ &= G(M[1] \oplus C[1]) \oplus M[1] \oplus D(1) \oplus G(M[2] \oplus C[2]) \oplus D(2), \\ C'[2] &= G(M[1] \oplus C[1]) \oplus M[1] \oplus D(1) \oplus G(M[2] \oplus C[2]) \oplus D(2) \oplus M[2] \oplus C[2], \\ T' &= M[2] \oplus C[2]. \end{aligned}$$

It is easy to verify that $(C', T') = \text{GIFT-COFB}(M')$ with the same key, nonce and associated data. If $X[1] \neq X[2]$, then $C' \neq C$ and (C', T') is a new valid pair of ciphertext and authentication tag of COFB-ε_K.

3.2 A forgery attack with repeated blocks

In this section we will construct a pair of ciphertext and authenticated tag (C', T') from $M = M[1] \parallel M[2]$ and $C = C[1] \parallel C[2]$ by means of block-repeating technique, where $C' = C'[1] \parallel C'[2] \parallel \cdots \parallel C'[\tau]$ and τ is an arbitrary integer such that $\tau \geq 2$. Let $M' = M'[1] \parallel M'[2] \parallel \cdots \parallel M'[\tau]$ be the plaintext corresponding to C'. Keep all notations in Section 3.1. Take $C'[1] = C[1]$ and $X'[i] = X[1]$ for all $i \in \{2, 3, \cdots, \tau\}$. It follows that $M'[1] = M[1]$ and $Y'[i] = Y[1]$ for all $1 \leq i \leq \tau$. Similarly to the above section, we have

$$\begin{aligned} M'[i] &= X'[i] \oplus G(Y'[i-1]) \oplus D(i), \\ C'[i] &= M'[i] \oplus Y'[i-1], \\ T' &= Y'[\tau] = E_K(X'[\tau]) = E_K(X[1]) = Y[1]. \end{aligned}$$

Therefore,

$$\begin{aligned}
M'[i] &= X[1] \oplus G(Y[1]) \oplus D(i)\\
&= G(Y[0]) \oplus M[1] \oplus D(1) \oplus G(M[2] \oplus C[2]) \oplus D(i)\\
&= G(M[1] \oplus C[1]) \oplus M[1] \oplus D(1) \oplus G(M[2] \oplus C[2]) \oplus D(i),\\
C'[i] &= G(M[1] \oplus C[1]) \oplus M[1] \oplus D(1) \oplus G(M[2] \oplus C[2]) \oplus D(i) \oplus M[2] \oplus C[2],\\
T' &= M[2] \oplus C[2].
\end{aligned}$$

where $i \in \{2, 3, \cdots, m\}$. It is known that $(C', T') =$ GIFT-COFB(M') with the same key, nonce and associated data. Thus (C', T') is a new valid pair of ciphertext and authentication tag of COFB-ε_K.

3.3 A general forgery attack with many blocks

In this section we consider a general situation that $m \geq 2$ as shown in Fig. 1. Without loss of generality, we denote by $M[i]$ and $M[i+1]$ two successive known blocks of M, where $1 \leq i \leq m-1$. Combining two methods mentioned in Sections 3.1 and 3.2, we construct a pair of ciphertext and authenticated tag (C', T'), where

$$C = C'[1] \parallel C'[2] \parallel \cdots \parallel C'[i] \parallel C'[i+1] \parallel \cdots \parallel C'[\tau],$$

and τ is an arbitrary given integer such that $\tau \geq i+1$. Let $M = M'[1] \parallel M'[2] \parallel \cdots \parallel M'[i] \parallel M'[i+1] \parallel \cdots \parallel M'[\tau]$ be the plaintext corresponding to C'. Here we take $C'[j] = C[j]$ for all $j \in \{1, 2, ..., i\}$ and $X'[j] = X[i]$ for all $j \in \{i+1, i+2, \cdots, \tau\}$. It follows that $M'[j] = M[j]$ for all $j \in \{1, 2, ..., i\}$ and $Y'[j] = Y[i]$ for all $j \in \{i, i+1, \cdots, \tau\}$. From Fig. 1, we have

$$\begin{aligned}
M'[j] &= X'[j] \oplus G(Y'[j-1]) \oplus D(j),\\
C'[j] &= M'[j] \oplus Y'[j-1],\\
T' &= Y'[\tau] = E_K(X'[\tau]) = E_K(X[i]) = Y[i].
\end{aligned}$$

Therefore,

$$\begin{aligned}
M'[j] =& X[i] \oplus G(Y[i]) \oplus D(j)\\
=& G(Y[i-1]) \oplus M[i] \oplus D(i) \oplus G(Y[i]) \oplus D(j)\\
=& G(M[i] \oplus C[i]) \oplus M[i] \oplus D(i) \oplus G(M[i+1] \oplus C[i+1]) \oplus D(j),\\
C'[j] =& G(M[i] \oplus C[i]) \oplus M[i] \oplus D(i) \oplus G(M[i+1] \oplus C[i+1]) \oplus D(j) \oplus Y[i]\\
=& G(M[i] \oplus C[i]) \oplus M[i] \oplus D(i) \oplus G(M[i+1] \oplus C[i+1]) \oplus D(j)\\
& \oplus M[i+1] \oplus C[i+1],\\
T' =& M[i+1] \oplus C[i+1],
\end{aligned}$$

where $j \in \{i+1, i+2, \cdots, \tau\}$.

It is easy to check that $(C', T') =$ GIFT-COFB(M') with the same key, nonce and associated data. Note that τ is an arbitrary integer such that $\tau \geq i+1$, thus we can forge infinite new valid pairs (C', T'). What is more, we can choose the different i to forge different valid pairs (C', T') when more successive blocks of M are known.

4 Conclusion

In this paper we propose a forgery attack against GIFT-COFB. Our attack will work if at least two successive complete blocks of the message M corresponding to C are known, and infinite new valid pairs (C', T') are forged from (C, T). Our result shows that GIFT-COFB can not resist against the forgery attack.

References

1. National Institute of Standards and Technology (NIST): Lightweight cryptography standardization process (2019), https://csrc.nist.gov/projects/ lightweight-cryptography.
2. Z. Yuan, K. T. Jia, W. Wang and X. Y. Wang, "Distinguishing and forgery attacks on alred and its AES-based instance Alpha-MAC", Cryptology ePrint Archive, https://eprint.iacr.org/2008/516. 2008.
3. J. Daemen, V. Rijmen, "A new MAC construction Alred and a specific Instance Alpha-MAC", FSE 2005, LNCS 3557, pp.1-17, 2005.
4. X.T. Feng, F. Zhang and H. Wang, "A practical forgery and state recovery attack on the authenticated cipher PANDA-s". Cryptology ePrint Archive, http://eprint.iacr.org/2014/325. 2014.
5. T. S. Meltem, M. Kerry, . ada, C. Donghoon and B. Lawrence, "Status report on the first round of the NIST lightweight cryptography standardization process", https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8268.pdf. 2019.
6. H. Bartlett, OFFICIAL COMMENT: Bleep64. Official comments received on Bleep64. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/Bleep64-official-comment.pdf. 2019.
7. R. Yann, OFFICIAL COMMENT: Bleep64. Official comments received on Bleep64. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/Bleep64-official-comment.pdf. 2019.
8. A. Schrottenloher, OFFICIAL COMMENT: CLAE. Official comments received on CLAE. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/CLAE-official-comment.pdf. 2019.
9. M. Eichlseder, OFFICIAL COMMENT: FlexAEAD. Official comments received on FlexAEAD. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/FlexAEAD-official-comment.pdf. 2019.
10. M. Eichlseder, D. Kales and M. Schofnegger, "Forgery attacks on FlexAE and FlexAEAD", Cryptology ePrint Archive, https://eprint.iacr.org/2019/679. 2019.

11. N. Bagheri, OFFICIAL COMMENT: GAGE AEAD. Official comments received on GAGE and InGAGE. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/GAGE-and-InGAGE-official-comment.pdf. 2019.
12. A. Mege, OFFICIAL COMMENT: HERN & HERON. Official comments received on HERN & HERON. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/HERN-and-HERON-official-comment.pdf. 2019.
13. O. Dunkelman OFFICIAL COMMENT: Lilliput-AE. Official comments received on Lilliput-AE. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/Lilliput-AE-official-comment.pdf. 2019.
14. O. Dunkelman, N. Keller, E. Lambooij and Y. Sasaki, ”A Practical Forgery Attack on Lilliput-AE”, Cryptology ePrint Archive, https://eprint.iacr.org/2019/867. 2019.
15. R. Rohit R, OFFICIAL COMMENT: Limdolen. Official comments received on Limdolen. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/Limdolen-official-comment.pdf. 2019.
16. R. Rohit and G. Gong, ”Practical forgery attacks on Limdolen and HERN”, Cryptology ePrint Archive, https://eprint.iacr.org/2019/907. 2019.
17. A. Jha, OFFICIAL COMMENT: Qameleon. Official comments received on Qameleon. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/Qameleon-official-comment.pdf. 2019.
18. L. Perrin, OFFICIAL COMMENT: Quartet. Official comments received on Quartet. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/Quartet-official-comment.pdf. 2019.
19. A. Jha, OFFICIAL COMMENT: REMUS [AD-INT]. Official comments received on REMUS. Available at https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/REMUS-official-comment.pdf. 2019.
20. B. Subhadeep, C. Avik, I. Tetsu, M. Kazuhiko, N. Mridul, P. Thomas, S. Yu, S. M. Siang and T. Yosuke, GIFT-COFB. Submission to Round 1 of the NIST Lightweight Cryptography Standardization process, https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/gift-cofb-spec-round2.pdf. 2019.
21. C. Avik, I. Tetsu, M. Kazuhiko and N. Mridul, ”Blockcipher-based authenticated encryption: how small can we go?”, CHES 2017, pp.277298, 2017.
22. B. Subhadeep, P. K. Sumit, P. Thomas, S. Yu, S. M. Siang and T. Yosuke, ”GIFT: A small present towards reaching the limit of lightweight encryption”, CHES 2017, pp.321-345, 2017.