Hindawi
Security and Communication Networks
Volume 2018, Article ID 9715947, 12 pages
https://doi.org/10.1155/2018/9715947

Research Article

Close to Optimally Secure Variants of GCM

Ping Zhang,[1] **Hong-Gang Hu**,[1] **and Qian Yuan**[2]

[1]*Key Laboratory of Electromagnetic Space Information, CAS, University of Science and Technology of China, Hefei 230027, China*
[2]*School of Economics and Management, Southeast University, Nanjing 211189, China*

Correspondence should be addressed to Ping Zhang; zgp@mail.ustc.edu.cn

Received 21 August 2017; Revised 5 December 2017; Accepted 16 January 2018; Published 6 March 2018

Academic Editor: Kamal D. Singh

The Galois/Counter Mode of operation (GCM) is a widely used nonce-based authenticated encryption with associated data mode which provides the birthday-bound security in the nonce-respecting scenario; that is, it is secure up to about $2^{n/2}$ adversarial queries if all nonces used in the encryption oracle are never repeated, where n is the block size. It is an open problem to analyze whether GCM security can be improved by using some simple operations. This paper presents a positive response for this problem. Firstly, we introduce two close to optimally secure pseudorandom functions and derive their security bound by the hybrid technique. Then, we utilize these pseudorandom functions that we design and a universal hash function to construct two improved versions of GCM, called OGCM-1 and OGCM-2. OGCM-1 and OGCM-2 are, respectively, provably secure up to approximately $2^n/67(n-1)^2$ and $2^n/67$ adversarial queries in the nonce-respecting scenario if the underlying block cipher is a secure pseudorandom permutation. Finally, we discuss the properties of OGCM-1 and OGCM-2 and describe the future works.

1. Introduction

Authenticated Encryption. An authenticated encryption (AE) mode is a cryptographic scheme which guarantees privacy and authenticity of the message concurrently. So far, a large number of AE schemes have emerged. Particularly, the CAESAR competition that started in 2012 promotes enormously the development of AE schemes. AE has been widely applied to many environments. According to the application requirements classification, this includes AE with associated data (AEAD) [1, 2], parallelizable AE [3–5], online AE [6–9], tweakable AE [9–14], deterministic AE [10, 15, 16], wide block AE [17], XOR-based AE [18], and dedicated AE algorithms [19]. According to the design approaches classification, this includes generic composed AE [20], block cipher-based AE [3–6, 21], stream-cipher-based AE [18, 22], permutation-based AE [23–26], keyed-function-based AE [27, 28], tweakable block cipher-based AE [9–14], and hybrid AE [17, 19, 29].

Birthday-Bound Security and Beyond-Birthday-Bound Security. Most AE modes, such as [6, 7, 9, 20, 21, 26], just offer birthday-bound security; that is, they are secure up to roughly $2^{n/2}$ adversarial queries, where n is the block size. The currently utilized block cipher is AES (the block size $n = 128$). If AES is used in the block cipher modes of operation, 128-bit security degrades into at most about 64-bit security, which is unacceptable in some special environments. Therefore, it is vitally important to design AE modes that ensure beyond-birthday-bound (BBB) security. The so-called BBB security means that an AE mode is provably secure up to approximately $2^{rn/(r+1)}$ adversarial queries, where $r \geq 2$ is an integer. If an AE mode is provably secure up to roughly 2^n adversarial queries, we say that it provides optimal security. In order to achieve a stronger security (BBB security or optimal security), AE modes usually compromise the efficiency of the hardware and software implementation. For example, we often utilize multiple block ciphers or their sum to construct a BBB-secure pseudorandom function. The higher the number of invoking the underlying block cipher, the greater the cost. Therefore, the efficiency of BBB-secure AE modes is generally low. In recent years, AE modes that ensure BBB security appeared endless, such as [10–12, 22–24, 30–32].

Problem Statement. The Galois/Counter Mode of operation (GCM) [33] designed by McGrew and Viega is a nonce-based AEAD scheme. GCM combines the counter mode used

in the encryption part and the polynomial hash function used in the authentication part and is included in the block cipher AE modes of operation recommended by NIST. Its security depends on the nonce-respecting setting that all nonces used in the encryption queries are distinct. Iwata et al. [34] pointed out that the previous claimed security was flawed and presented a new provable security, which was later improved by Niwa et al. [35]. GCM retains birthday-bound security and has better security bounds for 96-bit nonces. For the attacks of GCM, Saarinen showed weak keys of GHASH and the cycling attacks on GCM in [36]. Other researches related to GCM include [37–44]. GCM has been widely applied in the IEEE 802.1AE Ethernet security, IEEE 802.11ad, IETF IPsec standards, SSH, TLS, and so on. GCM is proven to be secure up to roughly $2^{n/2}$ adversarial queries in the nonce-respecting scenario, assuming that the underlying block cipher is a secure pseudorandom permutation. In other words, for AES-GCM, its security guarantee is lost after at most only 2^{64} adversarial queries, which is not sufficiently secure in some special settings. Therefore, in this paper, we consider the question of whether we can design a scheme that provides better security (such as BBB security or optimal security) to improve the security guarantee of GCM.

Our Contributions. This paper gives a positive response for the above question. We first introduce a basic tool: close to optimally secure pseudorandom functions (PRFs) which are, respectively, designed by the Encrypted Davies-Meyer (EDM) [45] and EDM Dual (EDMD) [46] constructions. Then we construct two improved versions of GCM, called OGCM-1 and OGCM-2, which are parallelizable nonce-based close to optimally secure AEAD modes. OGCM-1 and OGCM-2 are, respectively, provably secure up to approximately $2^n/67(n-1)^2$ and $2^n/67$ adversarial queries in the nonce-respecting scenario if the underlying block cipher is a secure pseudorandom permutation (PRP). In fact, they are based on the "Encryption-then-MAC" approach, where the encryption part utilizes a multi-EDM or multi-EDMD function to set up a close to optimally secure key-stream generator and then the MAC part combines an EDM or EDMD construction and an almost-XOR-universal (AXU) hash function to generate an authentication tag.

OGCM-1 and OGCM-2 balance the security and the efficiency of the software and hardware implementation. Take AES-OGCM-1 or AES-OGCM-2 as an example; that is, the underlying block cipher is instantiated with AES. First, from the point of view of security, they achieve at most about 107.9565-bit or 121.9339-bit security which is better than that of AES-GCM (at most about 64-bit security). In the nonce-respecting scenario, they can encrypt at most 2^{96} plaintexts (as the nonce length is 96 bits) and the maximum block length of each plaintext is about 2^{32} blocks (64 GBytes). Second, from the point of view of efficiency, they invoke $2m+2$ block ciphers and $a+m+1$ finite-field multiplications, where m is the number of the plaintext blocks and a is the number of the associated data blocks. Compared with AES-GCM, the efficiency is about half of it. Therefore, AES-OGCM-1 and AES-OGCM-2 sacrifice the efficiency of the software and hardware implementation to achieve a strong security. The comparisons among AES-GCM, AES-OGCM-1, and AES-OGCM-2 are shown in Table 1.

Table 1: Comparisons among AES-GCM [34], AES-OGCM-1, and AES-OGCM-2. The nonce length is restricted to 96 bits. "n.r." denotes nonce-respecting. "$A \rightsquigarrow B$" means A can be reduced to B. Let m be the block length of the plaintext and a be the block length of associated data.

	AES-GCM [34]	AES-OGCM-1	AES-OGCM-2
# keys	1	$3 \rightsquigarrow 1$	$3 \rightsquigarrow 1$
CTR-like	Yes	Yes	Yes
Block size n	128	128	128
Nonce scenario	n.r.	n.r.	n.r.
Assumption	PRP	PRP	PRP
Security (bits)	64	107.9565	121.9339
# block cipher calls	$m+2$	$2m+2$	$2m+2$
# multiplications	$a+m+1$	$a+m+1$	$a+m+1$

Organizations of This Paper. Some preliminaries are presented in Section 2. A basic tool is provided in Section 3. OGCM-1 is described in Section 4. Security results of OGCM-1 are derived in Section 5. OGCM-2 and its security are shown in Section 6. Section 7 describes some discussions and future works. Finally, we end up with a conclusion in Section 8.

2. Preliminaries

Notations. Let $\{0,1\}^*$ be the set containing all finite strings (including an empty string ε). For a finite string $x \in \{0,1\}^*$, $|x|$ stands for its length in bits and $|x|_n = \lceil |x|/n \rceil$ means the length of n-bit blocks for any integer $n \geq 1$, where $\lceil \cdot \rceil$ denotes the operation that rounds up from a floating-point number to an integer. The n-bit zero string is written as $0^n \in \{0,1\}^n$. For two finite strings x and y, let $x \parallel y$ or xy be the concatenation of them. If x and y are two equal-length strings, let $x \oplus y$ denote the XOR of them. For a finite string $x \in \{0,1\}^*$ with $|x| \geq n$, let $\mathrm{msb}_n(x)$ be the most significant n-bit of x. Given two positive integers n and m such that $m \leq 2^n - 1$, let $[m]_n$ be the n-bit binary representation of m. Let $\mathrm{inc}(\cdot)$ be the function for increment which takes an n-bit input x and returns an incremented value $x+1 \bmod 2^n$. For $i \geq 1$, $\mathrm{inc}^i(x)$ denotes that x is incremented i times. For a finite set X, let $x \xleftarrow{\$} X$ denote the value x randomly drawn from X and let $|X|$ denote the number of elements in X. Let $[a,b]$ be a set of all integers from a to b; that is, $[a,b] = \{x \in \mathbb{Z} : a \leq x \leq b\}$. Let $\mathscr{A}^{\mathcal{O}} = 1$ be an event that an adversary $\mathscr{A}$ outputs 1 after interacting with the oracle $\mathcal{O}$.

Block Ciphers and Keyed Functions. A block cipher is a mapping $E : \mathscr{K}_e \times \{0,1\}^n \to \{0,1\}^n$, which takes a key $K \in \mathscr{K}_e$ and a plaintext $M \in \{0,1\}^n$ as input and returns a ciphertext $C \in \{0,1\}^n$. For any fixed $K \in \mathscr{K}_e$, $E_K : \{0,1\}^n \to \{0,1\}^n$ is

an n-bit permutation and its inverse is written as $D_K = E_K^{-1}$. Let Perm(n) be a set of all n-bit permutations. Suppose that $\mathscr{A}$ is an adversary which has access to an encryption oracle. Let $K \xleftarrow{\$} \mathscr{K}_e$ and $\pi \xleftarrow{\$} \text{Perm}(n)$; then the PRP-advantage of $\mathscr{A}$ against E is defined as

$$Adv_E^{prp}(\mathscr{A}) = \left|\Pr\left[\mathscr{A}^{E_K(\cdot)} = 1\right] - \Pr\left[\mathscr{A}^{\pi(\cdot)} = 1\right]\right|, \quad (1)$$

where the probabilities are taken over the random choices of K and π and also over internal coins of $\mathscr{A}$, if any. If $\text{Adv}_E^{\text{prp}}(\mathscr{A})$ is negligible, the underlying block cipher E_K is a secure pseudorandom permutation (PRP).

A keyed function is a mapping $F : \mathscr{K}_f \times \{0,1\}^m \to \{0,1\}^n$, which takes a key $K \in \mathscr{K}_f$ and a plaintext $M \in \{0,1\}^m$ as input and returns a ciphertext $C \in \{0,1\}^n$. For any fixed $K \in \mathscr{K}_f$, $F_K : \{0,1\}^m \to \{0,1\}^n$ is a function from $\{0,1\}^m$ to $\{0,1\}^n$. Let Func(m,n) be a set of all functions from $\{0,1\}^m$ to $\{0,1\}^n$. If $m = n$, we write Func(n). Suppose that $\mathscr{A}$ is an adversary which has access to an encryption oracle. Let $K \xleftarrow{\$} \mathscr{K}_f$ and $R \xleftarrow{\$} \text{Func}(m,n)$; then the PRF-advantage of $\mathscr{A}$ against F is defined as

$$\text{Adv}_F^{\text{prf}}(\mathscr{A}) = \left|\Pr\left[\mathscr{A}^{F_K(\cdot)} = 1\right] - \Pr\left[\mathscr{A}^{R(\cdot)} = 1\right]\right|, \quad (2)$$

where the probabilities are taken over the random choices of K and R and also over internal coins of $\mathscr{A}$, if any. If $\text{Adv}_F^{\text{prf}}(\mathscr{A})$ is negligible, the underlying keyed function F_K is a secure pseudorandom function (PRF).

If the resources owned by all adversaries are at most S, the maximum advantage is defined as $\text{Adv}(S) = \max_{\mathscr{A}}\text{Adv}(\mathscr{A})$, where S includes the running time t, the total number of oracle queries q, the maximum block length m, and the total number of blocks in all queries (query complexity) σ.

Universal Hash Functions. Let $n \geq 1$; a keyed hash function $H : \mathscr{K}_h \times \mathscr{D} \to \{0,1\}^n$ is a mapping which takes a key $K_h \in \mathscr{K}_h$ and a message $x \in \mathscr{D}$ as input and returns an output $y \in \{0,1\}^n$. We say H is an (ϵ,δ)-almost-XOR-universal ((ϵ,δ)-AXU) hash function, if, for any $x \in \mathscr{D}$ and $y \in \{0,1\}^n$, $\Pr[K_h \xleftarrow{\$} \mathscr{K}_h : H_{K_h}(x) = y] \leq \delta$ and, for any two distinct $x, x' \in \mathscr{D}$ and $y \in \{0,1\}^n$, $\Pr[K_h \xleftarrow{\$} \mathscr{K}_h : H_{K_h}(x) \oplus H_{K_h}(x') = y] \leq \epsilon$. If $\delta = 2^{-n}$, H is called an ϵ uniform AXU (ϵ-AXU for short) hash function.

Finite Field. Given a basis, the finite field GF(2^n) can be seen as the set $\{0,1\}^n$. For an n-bit string $a = a_{n-1}\cdots a_1 a_0$, we can define a polynomial $a(x) \in \mathbb{Z}[x]$ by $a(x) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where $a_i \in \{0,1\}$ for any $i \in [0, n-1]$. Hence, any integer between 0 and $2^n - 1$ can also be viewed as a polynomial with binary coefficients of degree at most $n-1$. For example, 2 corresponds to x, 3 corresponds to $x+1$, and 7 corresponds to x^2+x+1. The addition in the field GF(2^n) is the addition of polynomials over GF(2). We denote this operation by bitwise XOR, that is, $a \oplus b$, where $a, b \in \text{GF}(2^n)$. In order to define the multiplication operation over GF(2^n), we need to introduce an irreducible polynomial $f(x)$ of degree n over GF(2). For $n = 128$, $f(x) = x^{128} + x^7 + x^2 + x + 1$. The multiplication of two elements $A \in \text{GF}(2^n)$ and $B \in \text{GF}(2^n)$ is defined as the corresponding polynomial multiplication over GF(2) reduced modulo $f(x)$, that is $A(x)B(x) \bmod f(x)$.

Authenticated Encryption. A conventional nonce-based authenticated encryption with associated data (AEAD) scheme Π consists of an encryption algorithm $\mathscr{E} : \mathscr{K} \times \mathscr{N} \times \mathscr{H} \times \mathscr{M} \to \mathscr{C} \times \mathscr{T}$ and a decryption algorithm $\mathscr{D} : \mathscr{K} \times \mathscr{N} \times \mathscr{H} \times \mathscr{C} \times \mathscr{T} \to \mathscr{M} \cup \{\perp\}$; that is,

$$\begin{aligned}(C,T) &\longleftarrow \mathscr{E}_K(N,A,M) = \mathscr{E}(K,N,A,M),\\ \frac{M}{\perp} &\longleftarrow \mathscr{D}_K(N,A,C,T) = \mathscr{D}(K,N,A,C,T),\end{aligned} \quad (3)$$

where $K \in \mathscr{K}$ is a key, $N \in \mathscr{N}$ is a nonce, $A \in \mathscr{H}$ is associated data, $\mathscr{H} \subseteq \{0,1\}^*$, $M \in \mathscr{M}$ is a plaintext, $\mathscr{M} \subseteq \{0,1\}^*$, $C \in \mathscr{C}$ is a ciphertext, $\mathscr{C} \subseteq \{0,1\}^*$, $T \in \mathscr{T}$ is a tag, $\mathscr{T} \subseteq \{0,1\}^*$, and $\perp$ is an error symbol which indicates the failure of the decryption oracle. $\mathscr{E}_K(N,A,M) = (C,T)$ iff $\mathscr{D}_K(N,A,C,T) = M$. A secure AEAD scheme returns $\perp$ if it receives an error (N,A,C,T) pair. If there is no associated data, A is seen as an empty string.

3. Basic Tool: Close to Optimally Secure PRFs

3.1. Multi-Encrypted-Davies-Meyer (Multi-EDM) Function F_1. In this section, we set up a new function F_1 which is constructed from the EDM construction [45].

Assuming that P_1 and P_2 are two independent and random permutations on n-bit, we define a function $F_1 : \{0,1\}^l \to \{0,1\}^{ns}$ as $F_1(x) = (y_1, y_2, \ldots, y_s)$, where $y_i = P_2(P_1(\text{inc}^i(x \parallel [0]_{n-l})) \oplus \text{inc}^i(x \parallel [0]_{n-l})) \in \{0,1\}^n$ for $i \in [1,s]$, $l \leq n$, and $x \in \{0,1\}^l$. Note that we must ensure $s \leq 2^{n-l} - 1$.

We have the following theorem for information-theoretic security of the function F_1.

Theorem 1. *Let $\mathscr{A}$ be an adversary with access to the function F_1. Let $\xi \geq 2$ be any threshold. Assuming that $\mathscr{A}$ makes at most $q \leq 2^n/(67\xi^2)$ oracle queries, generating at most $\sigma = qs$ blocks, then the PRF-advantage of $\mathscr{A}$ against F_1 is upper-bounded by*

$$Adv_{F_1}^{prf}(\mathscr{A}) \leq \frac{\sigma}{2^n} + \frac{\binom{\sigma}{\xi+1}}{2^{n\xi}}. \quad (4)$$

The result of Theorem 1 shows that F_1 constructed by P_1 and P_2 achieves BBB security. If $\xi = 2$ and $q \leq 2^{n-8}$, then the PRF-advantage of $\mathscr{A}$ against F_1 is upper-bounded by $1.5\sigma^{3/2}/2^n$, which means that F_1 is a provably BBB-secure PRF up to approximately $2^{2n/3}$ adversarial queries. If $\xi = n-1$ and $q \leq 2^n/67(n-1)^2$, then the PRF-advantage of $\mathscr{A}$ against F_1 is upper-bounded by $\sigma/2^n$, which means that F_1 is a close to optimally secure PRF up to approximately $2^n/67(n-1)^2$ adversarial queries.

The proof of Theorem 1 utilizes the hybrid technique. The security of the function F_1 can be reduced to the security of the EDM construction [46] which utilizes Patarin's mirror theory.

Proof. Let $R \xleftarrow{\$} \mathrm{Func}(l, ns)$ and $r \xleftarrow{\$} \mathrm{Func}(l, n)$; then the PRF-advantage of $\mathscr{A}$ against the function F_1 is shown as follows:

$$\mathrm{Adv}^{\mathrm{prf}}_{F_1}(\mathscr{A}) = \left|\Pr\left[\mathscr{A}^{F_1(\cdot)} = 1\right] - \Pr\left[\mathscr{A}^{R(\cdot)} = 1\right]\right|. \quad (5)$$

Let $f : \{0,1\}^l \to \{0,1\}^n$ be a reduced EDM construction obtained by fixing $n - l$ bits. Let $\mathscr{B}$ be an adversary which has access to the reduced EDM function f or the random function r and makes q_i queries for the ith f. According to the security of the EDM construction, if $q \le 2^n/67\xi^2$ and $\xi \ge 2$, we have

$$\begin{aligned}\mathrm{Adv}^{\mathrm{prf}}_{f}(\mathscr{B}) &= \left|\Pr\left[\mathscr{B}^{f(\cdot)} = 1\right] - \Pr\left[\mathscr{B}^{r(\cdot)} = 1\right]\right| \\ &\le \frac{q_i}{2^n} + \frac{\binom{q_i}{\xi+1}}{2^{n\xi}}.\end{aligned} \quad (6)$$

We construct a hybrid function H^i_s as follows. The first i functions are f and the rest of the functions are r, that is, $H^i_s = (\underbrace{f, \ldots, f}_{i}, \underbrace{r, \ldots, r}_{s-i})$. If $i = 0$, then $H^0_s = (\underbrace{r, \ldots, r}_{s}) = R$. If $i = s$, then $H^s_s = (\underbrace{f, \ldots, f}_{s}) = F_1$. Then the PRF-advantage of $\mathscr{A}$ against F_1 is upper-bounded by

$$\begin{aligned}\mathrm{Adv}^{\mathrm{prf}}_{F_1}(\mathscr{A}) &= \left|\Pr\left[\mathscr{A}^{F_1(\cdot)} = 1\right] - \Pr\left[\mathscr{A}^{R(\cdot)} = 1\right]\right| \\ &= \left|\Pr\left[\mathscr{A}^{H^s_s} = 1\right] - \Pr\left[\mathscr{A}^{H^0_s} = 1\right]\right| \\ &= \left|\sum_i \left(\Pr\left[\mathscr{A}^{H^{i+1}_s} = 1\right] - \Pr\left[\mathscr{A}^{H^i_s} = 1\right]\right)\right| \\ &\le \sum_i \left|\Pr\left[\mathscr{B}^{f(\cdot)} = 1\right] - \Pr\left[\mathscr{B}^{r(\cdot)} = 1\right]\right| \\ &\le \sum_i \frac{q_i}{2^n} + \frac{\binom{q_i}{\xi+1}}{2^{n\xi}} \le \frac{\sigma}{2^n} + \frac{\binom{\sigma}{\xi+1}}{2^{n\xi}},\end{aligned} \quad (7)$$

where the inequality is obtained by $\sum_i q_i = \sigma$. The proof is finished. □

3.2. Multi-EDM-Dual (Multi-EDMD) Function F_2. In this section, we set up another new function F_2 which is constructed from the EDMD construction [46].

Assuming that P_1 and P_2 are two independent and random permutations on n-bit, we define a function $F_2 : \{0,1\}^l \to \{0,1\}^{ns}$ as $F_2(x) = (y_1, y_2, \ldots, y_s)$, where $y_i = P_2(P_1(\mathrm{inc}^i(x \parallel [0]_{n-l}))) \oplus P_1(\mathrm{inc}^i(x \parallel [0]_{n-l})) \in \{0,1\}^n$ for $i \in [1, s]$, $s \le 2^{n-l} - 1$, $l \le n$, and $x \in \{0,1\}^l$.

We have the following theorem for information-theoretic security of the function F_2.

Theorem 2. *Let $\mathscr{A}$ be an adversary with access to the function F_2. Assuming that $\mathscr{A}$ makes at most $q \le 2^n/67$ oracle queries, generating at most $\sigma = qs$ blocks, then the PRF-advantage of $\mathscr{A}$ against F_2 is upper-bounded by*

$$Adv^{prf}_{F_2}(\mathscr{A}) \le \frac{\sigma}{2^n}. \quad (8)$$

The proof of Theorem 2 is similar to that of Theorem 1. Therefore, here we omit it.

The result of Theorem 2 shows that F_2 constructed by P_1 and P_2 is a provably secure PRF up to approximately $2^n/67$ adversarial queries; that is, F_2 achieves close to optimal security. This is consistent with the views of Mennink and Neves [48].

4. OGCM-1: Close to Optimally Secure Variant of GCM

In this section, we utilize the close to optimally secure PRF F_1 to build an improved variant of GCM, called OGCM-1. OGCM-1 achieves close to optimal security in the nonce-respecting scenario assuming that the underlying block cipher is a secure PRP. OGCM-1 is a two-pass nonce-based AEAD scheme employing the "Encryption-then-MAC" approach, where the encryption part utilizes the close to optimally secure PRF F_1 to set up a stream-cipher encryption mode and the MAC part combines an AXU hash function and the EDM construction to generate an authentication tag.

Let $n, k, l, \tau > 0$ be integers. Fix a block cipher $E : \mathscr{K}_e \times \{0,1\}^n \to \{0,1\}^n$ and an ϵ-AXU hash function $H : \mathscr{K}_h \times \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^n$; the encryption algorithm of OGCM-1 is described as $\mathscr{E} : \mathscr{K} \times \mathscr{N} \times \mathscr{H} \times \mathscr{M} \to \mathscr{C} \times \mathscr{T}$, where $\mathscr{K} = \mathscr{K}^2_e \times \mathscr{K}_h = \{0,1\}^k$ is the key space, $\mathscr{N} = \{0,1\}^l$ is the nonce space, $\mathscr{H} \subseteq \{0,1\}^*$ is the associated data space, $\mathscr{M} \subseteq \{0,1\}^*$ is the plaintext space, $\mathscr{C} \subseteq \{0,1\}^*$ is the ciphertext space, and $\mathscr{T} = \{0,1\}^\tau$ is the tag space. It takes the key $K = (K_1, K_2, K_h) \in \mathscr{K}$, the nonce $N \in \mathscr{N}$, the associated data $A \in \mathscr{H}$, and the plaintext $M \in \mathscr{M}$ as input and returns the ciphertext $C \in \mathscr{C}$ and the tag $T \in \mathscr{T}$, where $K_1, K_2 \in \mathscr{K}_e$ and $K_h \in \mathscr{K}_h$. The decryption algorithm of OGCM-1 $\mathscr{D} : \mathscr{K} \times \mathscr{N} \times \mathscr{H} \times \mathscr{C} \times \mathscr{T} \to \mathscr{M} \cup \perp$ is the inverse of the encryption algorithm $\mathscr{E}$. It takes $K = (K_1, K_2, K_h), N, A, C$, and T as input and returns either M or a special symbol $\perp$. Here $\perp$ always returns a failure of the decryption oracle.

The overview of OGCM-1 is depicted in Figure 1. The encryption and decryption algorithms of OGCM-1 are given in Algorithms 1, 2, and 3. We recommend restricting AES-OGCM-1 to 96-bit nonces; that is, $n = 128$ and $l = 96$.

5. Security of OGCM-1

5.1. Security Models of AEAD Schemes. Privacy (confidentiality) and authenticity (integrity) are two important security metrics of AEAD modes. Let $k \ge 1$ be an integer, $K \xleftarrow{\$} \{0,1\}^k$ be the key randomly drawn from $\{0,1\}^k$, and $\Pi = (\mathscr{E}_K(\cdot,\cdot,\cdot), \mathscr{D}_K(\cdot,\cdot,\cdot,\cdot))$ be a nonce-based AEAD scheme.

Privacy. Let $\$(\cdot,\cdot,\cdot)$ be a random oracle that takes (N, A, M) as input and returns a random string of length $|C| + |T|$. Let $\mathscr{A}$ be an adversary which has access to an oracle (either the encryption oracle $\mathscr{E}_K(\cdot,\cdot,\cdot)$ or the random oracle $\$(\cdot,\cdot,\cdot)$) and returns $b \in \{0,1\}$. We say that $\mathscr{A}$ is a nonce-respecting adversary if all nonces $N^1, \ldots, N^q$ are always distinct for all

Input: three keys (K_1, K_2, K_h), a nonce N, an associated data A, and a plaintext M
Output: a ciphertext C and a tag T
Partition M into $M_1 \| \cdots \| M_m$,
$|M_i| = n$ for $1 \le i \le m-1$ and $0 < |M_m| \le n$
$Y_0 = N \| 0^{n-l-1}1$
$S_0 \leftarrow E_{K_2}(E_{K_1}(Y_0) \oplus Y_0)$
for $i = 1$ to m
    $Y_i \leftarrow \text{inc}(Y_{i-1})$
    $S_i \leftarrow E_{K_2}(E_{K_1}(Y_i) \oplus Y_i)$
for $i = 1$ to $m-1$
    $C_i \leftarrow S_i \oplus M_i$
$C_m \leftarrow \text{msb}_{|M_m|}(S_m) \oplus M_m$
$C \leftarrow C_1 \| \cdots \| C_m$
$S \leftarrow S_0 \oplus H_{K_h}(A, C)$
$T \leftarrow \text{msb}_\tau(S)$
return $C \| T$

Algorithm 1: The encryption algorithm of OGCM-1.

Input: three keys (K_1, K_2, K_h), a nonce N, an associated data A, a ciphertext C, and a tag T
Output: a plaintext M or $\perp$
$Y_0 = N \| 0^{n-l-1}1$
$S_0 \leftarrow E_{K_2}(E_{K_1}(Y_0) \oplus Y_0)$
$S \leftarrow S_0 \oplus H_{K_h}(A, C)$
$T' \leftarrow \text{msb}_\tau(S)$
If $T' = T$, then
    Partition C into $C_1 \| \cdots \| C_m$,
    $|C_i| = n$ for $1 \le i \le m-1$ and $0 < |C_m| \le n$
    for $i = 1$ to m
        $Y_i \leftarrow \text{inc}(Y_{i-1})$
        $S_i \leftarrow E_{K_2}(E_{K_1}(Y_i) \oplus Y_i)$
    for $i = 1$ to $m-1$
        $M_i \leftarrow S_i \oplus C_i$
    $M_m \leftarrow \text{msb}_{|C_m|}(S_m) \oplus C_m$
    $M \leftarrow M_1 \| \cdots \| M_m$
    return M
else return $\perp$.

Algorithm 2: The decryption algorithm of OGCM-1.

encryption queries $(N^1, A^1, M^1), \ldots, (N^q, A^q, M^q)$. Without loss of generality, we assume that $\mathscr{A}$ is a nonce-respecting adversary and never makes trivial queries for which their responses are obviously known. Then the PRIV-advantage of $\mathscr{A}$ against $\Pi = (\mathscr{E}_K(\cdot,\cdot,\cdot), \mathscr{D}_K(\cdot,\cdot,\cdot,\cdot))$ is defined as

$$\text{Adv}_\Pi^{\text{priv}}(\mathscr{A}) = \left|\Pr\left[\mathscr{A}^{\mathscr{E}_K(\cdot,\cdot,\cdot)} = 1\right] - \Pr\left[\mathscr{A}^{\$(\cdot,\cdot,\cdot)} = 1\right]\right|. \quad (9)$$

Authenticity. Let $\mathscr{A}$ be an adversary which has access to the encryption oracle $\mathscr{E}_K(\cdot,\cdot,\cdot)$ and the decryption oracle $\mathscr{D}_K(\cdot,\cdot,\cdot,\cdot)$. Firstly, the adversary $\mathscr{A}$ queries (N^i, A^i, M^i) to $\mathscr{E}_K(\cdot,\cdot,\cdot)$ and returns $(C^i, T^i) = \mathscr{E}_K(N^i, A^i, M^i)$, where $i \in [1, q]$. Then $\mathscr{A}$ forges a challenge query $(N, A, C, T) \notin \{(N^i, A^i, C^i, T^i)\}_{i=1}^q$ to $\mathscr{D}_K(\cdot,\cdot,\cdot,\cdot)$. The forgery attempt succeeds if $\mathscr{D}_K(N, A, C, T) \neq \perp$. Without loss of generality, we assume that $\mathscr{A}$ is a nonce-respecting adversary and never makes trivial queries for which their responses are obviously known. Then the AUTH-advantage of $\mathscr{A}$ against $\Pi = (\mathscr{E}_K(\cdot,\cdot,\cdot), \mathscr{D}_K(\cdot,\cdot,\cdot,\cdot))$ is defined as

$$\text{Adv}_\Pi^{\text{auth}}(\mathscr{A}) = \Pr\left[\mathscr{A}^{\mathscr{E}_K(\cdot,\cdot,\cdot),\mathscr{D}_K(\cdot,\cdot,\cdot,\cdot)} \text{ forges}\right]. \quad (10)$$

5.2. Main Results and Security Proofs. Assuming that the underlying block cipher E is a secure PRP, OGCM-1 achieves close to optimal security in the information-theoretic setting. Detailedly speaking, the privacy and authenticity of OGCM-1 are provably secure up to $q \simeq 2^n/67(n-1)^2$ adversarial queries in the nonce-respecting scenario if the underlying block cipher is a secure PRP. First, we present the privacy of OGCM-1 as follows.

Theorem 3 (privacy of OGCM-1). *Let* $E : \mathscr{K}_e \times \{0,1\}^n \to \{0,1\}^n$ *be a block cipher and* $H : \mathscr{K}_h \times \{0,1\}^* \times \{0,1\}^* \to$

Input: a hash key K_h, an associated data A, and a ciphertext C
Output: a hash value H
$X \leftarrow A \parallel 0^{|A|_n \cdot n - |A|} \parallel C \parallel 0^{|C|_n \cdot n - |C|} \parallel [|A|]_{n/2} \parallel [|C|]_{n/2}$
Partition X into $X_1 \parallel \cdots \parallel X_x$, $|X_i| = n$ for $1 \le i \le x$
$H \leftarrow 0$
for $i = 1$ to x
$H \leftarrow (H \oplus X_i) \cdot K_h$
return H

Algorithm 3: The hash algorithm $H_{K_h}(A, C)$.

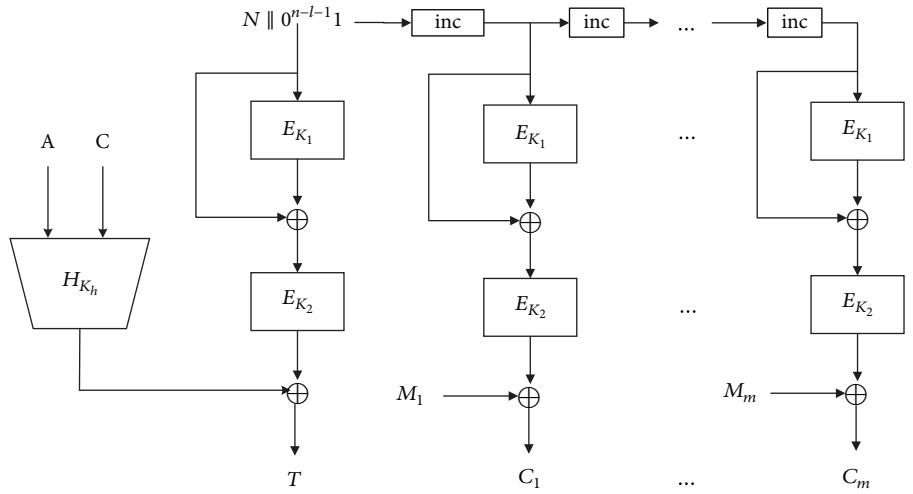

Figure 1: OGCM-1: a close to optimally secure variant of GCM.

$\{0,1\}^n$ *be an* ϵ*-AXU hash function, where* $\mathcal{K}_e$ *and* $\mathcal{K}_h$ *are two nonempty sets of keys. Let* $\mathcal{A}$ *be a nonce-respecting adversary which makes at most* $q \le 2^n/67(n-1)^2$ *queries with the maximum block length* m *and the running time* t *to OGCM-1. Then there exists another adversary* $\mathcal{A}'$ *against the PRP-security of* E*, making at most* $\sigma = q(m+1)$ *oracle queries and running in time at most* $O(t + t(\sigma))$*, such that, for any adversary* $\mathcal{A}$*,*

$$Adv^{priv}_{OGCM\text{-}1[E]}(\mathcal{A}) \le 2Adv^{prp}_{E}(\mathcal{A}') + \frac{\sigma}{2^n}. \tag{11}$$

The proof of Theorem 3 includes two steps. Firstly, we replace E_{K_1} and E_{K_2} with two random and independent permutations on n-bit P_1 and P_2, where K_1 and K_2 are randomly and independently drawn from $\mathcal{K}_e$. Let $P = (P_1, P_2)$ and let OGCM-1[P] be the new construction. By the hybrid argument, it is easy to show that there exists another adversary $\mathcal{A}'$ against the PRP-security of E, making at most $\sigma = q(m+1)$ oracle queries and running in time at most $t' = O(t + t(\sigma))$, such that

$$\begin{aligned}\mathrm{Adv}^{\mathrm{priv}}_{\mathrm{OGCM\text{-}1}[E]}(\mathcal{A}) &\le 2\mathrm{Adv}^{\mathrm{prp}}_{E}(\mathcal{A}') \\ &\quad + \mathrm{Adv}^{\mathrm{priv}}_{\mathrm{OGCM\text{-}1}[P]}(\mathcal{A}).\end{aligned} \tag{12}$$

Then, our goal is to upper-bound $\mathrm{Adv}^{\mathrm{priv}}_{\mathrm{OGCM\text{-}1}[P]}(\mathcal{A})$. Therefore, we introduce Lemma 4 as follows.

Lemma 4. *Let* $P = (P_1, P_2)$ *be two permutations randomly and independently chosen from* Perm(n)*. Let* $\mathcal{A}$ *be a nonce-respecting adversary which makes at most* $q \le 2^n/67(n-1)^2$ *queries to OGCM-1*[P]*, generating at most* σ *blocks. Then, for any adversary* $\mathcal{A}$*,*

$$Adv^{priv}_{OGCM\text{-}1[P]}(\mathcal{A}) \le \frac{\sigma}{2^n}. \tag{13}$$

Proof. Our proof utilizes a contradiction argument. The main idea is as follows. If there exists a nonce-respecting adversary $\mathcal{A}$ against OGCM-1[P] such that $\mathrm{Adv}^{\mathrm{priv}}_{\mathrm{OGCM\text{-}1}[P]}(\mathcal{A}) > \sigma/2^n$, then we can construct a nonce-respecting adversary $\mathcal{B}$ against F_1 such that $\mathrm{Adv}^{\mathrm{prf}}_{F_1}(\mathcal{B}) > \sigma/2^n$, which derives a contradiction with Theorem 1. The details of our proof are described as follows.

Let $\mathcal{E}[P]$ be the encryption algorithm of OGCM-1[P] and \$ be a random function that takes (N, A, M) as input and always returns a random string of length $|C| + |T|$. Suppose, to the contrary, that there exists a nonce-respecting adversary $\mathcal{A}$ against OGCM-1[P] such that

$$\begin{aligned}&\mathrm{Adv}^{\mathrm{priv}}_{\mathrm{OGCM\text{-}1}[P]}(\mathcal{A}) \\ &= \left|\Pr\left[\mathcal{A}^{\mathcal{E}[P](\cdot,\cdot,\cdot)} = 1\right] - \Pr\left[\mathcal{A}^{\$(\cdot,\cdot,\cdot)} = 1\right]\right| > \frac{\sigma}{2^n},\end{aligned} \tag{14}$$

/ PRF-adversary $\mathscr{B}$ against F_1 /
If $\mathscr{A}$ makes the ith query (N^i, A^i, M^i):
$m = \lceil |M^i|/n \rceil$
$X^i = N^i \| 0^{n-l}$, $K_h \xleftarrow{\$} \mathscr{K}_h$
$S_0^i \| S_1^i \| \cdots \| S_m^i = \mathscr{O}(X^i)$
for $j = 1$ to $m-1$: $C_j^i = M_j^i \oplus S_j^i$
$C_m^i = M_m^i \oplus \mathrm{msb}_{|M_m^i|}(S_m^i)$
$C^i = C_1^i \| C_2^i \| \cdots \| C_m^i$
$T^i = \mathrm{msb}_\tau(S_0^i \oplus H_{K_h}(A^i, C^i))$
return (C^i, T^i)
If $\mathscr{A}$ **returns** b:
output b

Algorithm 4: Codes of PRF-adversary $\mathscr{B}$ against F_1 using the PRIV-adversary $\mathscr{A}$.

where $\mathscr{A}$ makes q queries with the block length m to OGCM-1[P], generating $\sigma = q(m+1)$ blocks.

Let $R \in \mathrm{Func}(l, ns)$ be a random function, where $s = m+1$. Consider an adversary $\mathscr{B}$ that makes q queries to an oracle $\mathscr{O}$, either F_1 or R, generating $\sigma = qs$ blocks, where $\mathscr{B}$ uses $\mathscr{A}$ as a subroutine (see Algorithm 4).

If $\mathscr{O}$ is F_1, then $\mathscr{B}$ provides a perfect simulation of $\mathscr{E}[P]$ for $\mathscr{A}$. Therefore, $\Pr[\mathscr{B}^{F_1(\cdot)} = 1] = \Pr[\mathscr{A}^{\mathscr{E}[P](\cdot,\cdot,\cdot)} = 1]$. Similarity, if $\mathscr{O}$ is R, then $\mathscr{B}$ provides a perfect simulation of the random function \$ for $\mathscr{A}$. Therefore, $\Pr[\mathscr{B}^{R(\cdot)} = 1] = \Pr[\mathscr{A}^{\$(\cdot,\cdot,\cdot)} = 1]$. It follows that

$$\begin{aligned}\mathrm{Adv}_{F_1}^{\mathrm{prf}}(\mathscr{B}) &= \left|\Pr\left[\mathscr{B}^{F_1(\cdot)} = 1\right] - \Pr\left[\mathscr{B}^{R(\cdot)} = 1\right]\right| \\ &= \left|\Pr\left[\mathscr{A}^{\mathscr{E}[P](\cdot,\cdot,\cdot)} = 1\right] - \Pr\left[\mathscr{A}^{\$(\cdot,\cdot,\cdot)} = 1\right]\right| \\ &= \mathrm{Adv}_{\mathrm{OGCM\text{-}1}[P]}^{\mathrm{priv}}(\mathscr{A}) > \frac{\sigma}{2^n},\end{aligned} \tag{15}$$

which contradicts Theorem 1. Therefore, our (contradiction) hypothesis does not hold; that is, the original proposition holds where

$$\mathrm{Adv}_{\mathrm{OGCM\text{-}1}[P]}^{\mathrm{priv}}(\mathscr{A}) \le \frac{\sigma}{2^n}. \tag{16}$$

The proof of Lemma 4 is finished. □

Therefore, combining (12) and (13), the result of Theorem 3 is derived. The privacy of OGCM-1 is secure up to $q \simeq 2^n/67(n-1)^2$ adversarial queries in the nonce-respecting scenario assuming that the underlying block cipher is a secure PRP. Next, we provide the authenticity of OGCM-1.

Theorem 5 (authenticity of OGCM-1). *Let $E : \mathscr{K}_e \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher and $H : \mathscr{K}_h \times \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^n$ be an ϵ-AXU hash function, where $\mathscr{K}_e$ and $\mathscr{K}_h$ are two nonempty sets of keys. Let $\mathscr{A}$ be a nonce-respecting adversary which makes at most $q \le 2^n/67(n-1)^2$ encryption queries and one forgery attempt to OGCM-1. The maximum block length is m and the running time is at most t. Then there exists another adversary $\mathscr{A}'$ against the PRP-security of E, making at most $\sigma = (q+1)(m+1)$ oracle queries and running in time at most $O(t + t(\sigma))$, such that, for any adversary $\mathscr{A}$,*

$$\begin{aligned}Adv_{OGCM\text{-}1[E]}^{auth}(\mathscr{A}) \le 2Adv_E^{prp}\left(\mathscr{A}'\right) + \frac{\sigma}{2^n} + \epsilon + \frac{n}{2^n} \\ + \frac{1}{2^\tau - q}.\end{aligned} \tag{17}$$

The proof of Theorem 5 includes two steps. Firstly, we replace E_{K_1} and E_{K_2} with two random and independent permutations P_1 and P_2. Let $P = (P_1, P_2)$ and let OGCM-1[P] be the new construction. It is easy to show that there exists another adversary $\mathscr{A}'$ against the PRP-security of E, making at most $\sigma = (q+1)(m+1)$ oracle queries and running in time at most $t' = O(t + t(\sigma))$, such that

$$\begin{aligned}\mathrm{Adv}_{\mathrm{OGCM\text{-}1}[E]}^{\mathrm{auth}}(\mathscr{A}) \le 2\mathrm{Adv}_E^{\mathrm{prp}}\left(\mathscr{A}'\right) \\ + \mathrm{Adv}_{\mathrm{OGCM\text{-}1}[P]}^{\mathrm{auth}}(\mathscr{A}).\end{aligned} \tag{18}$$

Next, our goal is to upper-bound $\mathrm{Adv}_{\mathrm{OGCM\text{-}1}[P]}^{\mathrm{auth}}(\mathscr{A})$. Therefore, we introduce Lemma 6 as follows.

Lemma 6. *Let $\tau > 0$ be an integer. Let $P = (P_1, P_2)$ be two permutations randomly and independently chosen from $Perm(n)$. Let H be an ϵ-AXU hash function. Let $\mathscr{A}$ be a nonce-respecting adversary which makes at most $q \le 2^n/67(n-1)^2$ encryption queries and one forgery attempt to OGCM-1[P], generating at most σ blocks. Then, for any adversary $\mathscr{A}$,*

$$Adv_{OGCM\text{-}1[P]}^{auth}(\mathscr{A}) \le \frac{\sigma}{2^n} + \epsilon + \frac{n}{2^n} + \frac{1}{2^\tau - q}. \tag{19}$$

Proof. We assume that the nonce-respecting adversary $\mathscr{A}$ makes one forgery attempt after q encryption queries, generating at most σ blocks. Detailedly speaking, $\mathscr{A}$ firstly makes q queries $(N^1, A^1, M^1), \ldots, (N^q, A^q, M^q)$ to the encryption oracle and returns $(C^1, T^1), \ldots, (C^q, T^q)$. Then $\mathscr{A}$ makes one forgery attempt (N', A', C', T') to the decryption oracle. Note that $(N', A', C', T') \notin \{(N^i, A^i, C^i, T^i)\}_{i=1}^q$.

According to the definition of the AUTH-advantage, we have

$$\mathrm{Adv}_{\mathrm{OGCM\text{-}1}[P]}^{\mathrm{auth}}(\mathscr{A}) = \Pr\left[\mathscr{A}^{\mathscr{E}[P],\mathscr{D}[P]} \text{ forges}\right] \tag{20}$$

$$\le \left|\Pr\left[\mathscr{A}^{\mathscr{E}[P],\mathscr{D}[P]} \text{ forges}\right] - \Pr\left[\mathscr{A}^{\$_1,\$_2} \text{ forges}\right]\right| \tag{21}$$

$$+ \Pr\left[\mathscr{A}^{\$_1,\$_2} \text{ forges}\right], \tag{22}$$

where $\mathscr{E}[P]$, $\mathscr{D}[P]$ are the encryption and decryption algorithms of OGCM-1[P], $\$_1$ is a random oracle which always returns a random string $(C, T) \xleftarrow{\$} \mathscr{C} \times \mathscr{T}$, and $\$_2$ is a random oracle which always returns a random string or a reject symbol; that is, $M/\perp \xleftarrow{\$} \mathscr{M} \cup \{\perp\}$.

For (21), we have

$$(21) = \mathrm{Adv}_{\mathrm{OGCM\text{-}1}[P]}^{\mathrm{priv}}(q+1, \sigma) \le \frac{\sigma}{2^n}, \tag{23}$$

which is shown in the privacy proof and $\sigma = (q+1)(m+1)$.

For (22), we consider the forgery attempt (N', A', C', T'). As $\mathscr{A}$ is a nonce-respecting adversary, there is at most one response (N^i, A^i, C^i, T^i) of the encryption oracle such that $N' = N^i$, where $i \in [1, q]$. Assuming that there exists a dummy key K_h, we discuss the following two cases in the single forgery attempt.

Case 1. There exist one (N^i, A^i, C^i, T^i) such that $N' = N^i$ for some $i \in [1, q]$. According to the properties of the AXU hash function H, we have

$$\Pr\left[\mathrm{msb}_\tau\left(H_{K_h}\left(A', C'\right) \oplus H_{K_h}\left(A^i, C^i\right)\right) = T' \oplus T^i\right] \leq \epsilon. \tag{24}$$

Case 2. There is no (N^i, A^i, C^i, T^i) such that $N' = N^i$ for any $i \in [1, q]$; that is, N' is new. Let l be the nonce length. We consider the following subcases in this case.

Case 2-1. There exist $(A^i, C^i, T^i) = (A', C', T')$ for multiple $i \in [1, q]$. In the encryption queries, there are at most $n - 1$ collisions for $q \leq 2^n/67(n-1)^2$ queries; that is, the number of the same (A^i, C^i, T^i) pair is at most $n - 1$. Then we have

$$\Pr\left[P_2\left(P_1\left(Y_0^i\right) \oplus Y_0^i\right) = P_2\left(P_1\left(Y_0'\right) \oplus Y_0'\right)\right] \leq \frac{(n-1)}{2^n}, \tag{25}$$

where $Y_0^i = N^i \parallel 0^{n-l-1}1$ and $Y_0' = N' \parallel 0^{n-l-1}1$.

Case 2-2. There is no $(A^i, C^i, T^i) = (A', C', T')$ for any $i \in [1, q]$. In this subcase, we further discuss the following two subcases.

Case 2-2-1. There exist $(A^i, C^i) = (A', C')$ and $T^i \neq T'$ for some $i \in [1, q]$. Then $H_{K_h}(A^i, C^i) = H_{K_h}(A', C')$. Therefore, we have

$$\Pr\left[\mathrm{msb}_\tau\left(S_0^i \oplus S_0'\right) = T^i \oplus T'\right] \leq \frac{1}{\left(2^\tau - q\right)}, \tag{26}$$

where $S_0^i = P_2(P_1(Y_0^i) \oplus Y_0^i)$, $Y_0^i = N^i \parallel 0^{n-l-1}1$, $S_0' = P_2(P_1(Y_0') \oplus Y_0')$, and $Y_0' = N' \parallel 0^{n-l-1}1$.

Case 2-2-2. There is no $(A^i, C^i) = (A', C')$ for any $i \in [1, q]$. According to the properties of the AXU hash function H, we have

$$\Pr\left[\mathrm{msb}_\tau\left(S_0' \oplus H_{K_h}\left(A', C'\right)\right) = T'\right] \leq \frac{1}{2^n}, \tag{27}$$

where $S_0' = P_2(P_1(Y_0') \oplus Y_0')$ and $Y_0' = N' \parallel 0^{n-l-1}1$.

Summarizing above all mutually exclusive cases, the success probability of the single forgery attempt is upper-bounded by

$$\epsilon + \frac{n}{2^n} + \frac{1}{\left(2^\tau - q\right)}. \tag{28}$$

Combining (21), (22), (23), and (28), the AUTH-advantage of $\mathscr{A}$ against OGCM-1[P] is upper-bounded by

$$\mathrm{Adv}^{\mathrm{auth}}_{\mathrm{OGCM\text{-}1}[P]}(\mathscr{A}) \leq \frac{\sigma}{2^n} + \epsilon + \frac{n}{2^n} + \frac{1}{2^\tau - q}. \tag{29}$$

The proof of Lemma 6 is finished. □

Therefore, combining (18) and (19), the result of Theorem 5 is derived. If $\epsilon \simeq 2^{-n}$ and $\tau = n$, the authenticity of OGCM-1 is secure up to $q \simeq 2^n/67(n-1)^2$ adversarial queries in the nonce-respecting scenario assuming that the underlying block cipher is a secure PRP.

6. OGCM-2: A Dual Variant of OGCM-1

In this section, we utilize the close to optimally secure PRF F_2 to build another improved variant of GCM, called OGCM-2. OGCM-2 achieves close to optimal security in the nonce-respecting scenario assuming that the underlying block cipher is a secure PRP. OGCM-2 is a two-pass nonce-based AEAD scheme employing the "Encryption-then-MAC" approach, where the encryption part utilizes a multi-EDMD function F_2 to set up a stream-cipher encryption mode and the MAC part combines an AXU hash function and the EDMD construction to generate an authentication tag.

The overview of OGCM-2 is depicted in Figure 2. The encryption and decryption algorithms of OGCM-2 are given in Algorithms 5 and 6.

The security of OGCM-2 is derived in the following theorem.

Theorem 7 (security of OGCM-2). *Let $\tau \geq 1$. Let $\mathscr{A}$ be a nonce-respecting adversary which makes at most $q \leq 2^n/67$ encryption queries and one forgery attempt and runs in time at most t to OGCM-2. Then there exists another adversary $\mathscr{A}'$ against the PRP-security of E, making at most σ oracle queries and running in time at most $O(t + t(\sigma))$, such that, for any adversary $\mathscr{A}$,*

$$\mathrm{Adv}^{\mathrm{priv}}_{\mathrm{OGCM\text{-}2}[E]}(\mathscr{A}) \leq 2\mathrm{Adv}^{\mathrm{prp}}_E\left(\mathscr{A}'\right) + \frac{\sigma}{2^n},$$
$$\mathrm{Adv}^{\mathrm{auth}}_{\mathrm{OGCM\text{-}2}[E]}(\mathscr{A}) \leq 2\mathrm{Adv}^{\mathrm{prp}}_E\left(\mathscr{A}'\right) + \frac{\sigma}{2^n} + \epsilon + \frac{n}{2^n} + \frac{1}{2^\tau - q}. \tag{30}$$

The proof of Theorem 7 is similar to the proofs of Theorems 3 and 5. Therefore we omit it.

According to Theorem 7, assuming that the underlying block cipher E is a secure PRP and $\epsilon \simeq 2^{-n}$ and $\tau = n$, the privacy and authenticity of OGCM-2 are provably secure up to $q \simeq 2^n/67$ adversarial queries in the nonce-respecting scenario.

7. Discussions and Future Works

Compared with GCM, both OGCM-1 and OGCM-2 achieve a balance between the security and the efficiency.

Input: three keys (K_1, K_2, K_h), a nonce N, an associated data A, and a plaintext M
Output: a ciphertext C and a tag T

Partition M into $M_1 \| \cdots \| M_m$,
$|M_i| = n$ for $1 \le i \le m-1$ and $0 < |M_m| \le n$
$Y_0 = N \| 0^{n-l-1}1$
$S_0 \leftarrow E_{K_2}(E_{K_1}(Y_0)) \oplus E_{K_1}(Y_0)$
for $i = 1$ to m
    $Y_i \leftarrow \text{inc}(Y_{i-1})$
    $S_i \leftarrow E_{K_2}(E_{K_1}(Y_i)) \oplus E_{K_1}(Y_i)$
for $i = 1$ to $m-1$
    $C_i \leftarrow S_i \oplus M_i$
$C_m \leftarrow \text{msb}_{|M_m|}(S_m) \oplus M_m$
$C \leftarrow C_1 \| \cdots \| C_m$
$S \leftarrow S_0 \oplus H_{K_h}(A, C)$
$T \leftarrow \text{msb}_\tau(S)$
return $C \| T$

Algorithm 5: The encryption algorithm of OGCM-2.

Input: three keys (K_1, K_2, K_h), a nonce N, an associated data A, a ciphertext C, and a tag T
Output: a plaintext M or $\perp$

$Y_0 = N \| 0^{n-l-1}1$
$S_0 \leftarrow E_{K_2}(E_{K_1}(Y_0)) \oplus E_{K_1}(Y_0)$
$S \leftarrow S_0 \oplus H_{K_h}(A, C)$
$T' \leftarrow \text{msb}_\tau(S)$
If $T' = T$, then
    Partition C into $C_1 \| \cdots \| C_m$,
    $|C_i| = n$ for $1 \le i \le m-1$ and $0 < |C_m| \le n$
    for $i = 1$ to m
        $Y_i \leftarrow \text{inc}(Y_{i-1})$
        $S_i \leftarrow E_{K_2}(E_{K_1}(Y_i)) \oplus E_{K_1}(Y_i)$
    for $i = 1$ to $m-1$
        $M_i \leftarrow S_i \oplus C_i$
    $M_m \leftarrow \text{msb}_{|C_m|}(S_m) \oplus C_m$
    $M \leftarrow M_1 \| \cdots \| M_m$
    return M
else return $\perp$.

Algorithm 6: The decryption algorithm of OGCM-2.

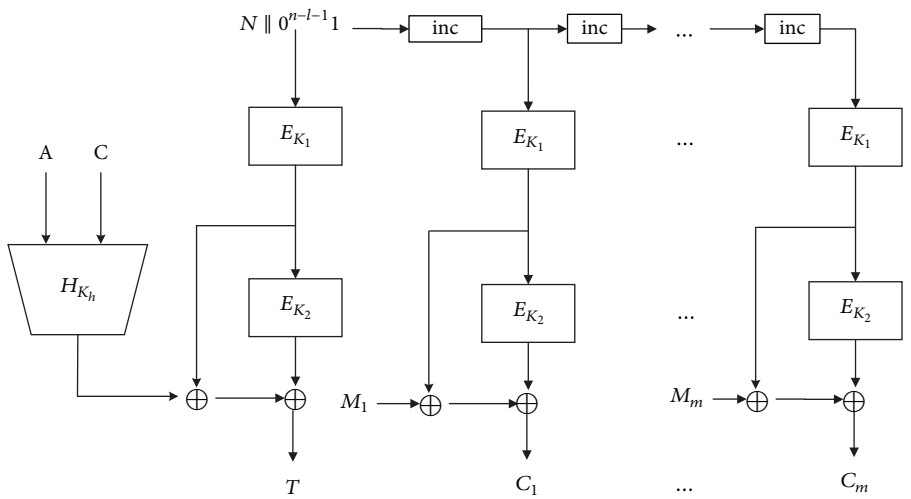

Figure 2: OGCM-2: a dual variant of OGCM-1.

Table 2: Comparison of AE schemes that provide BBB security. "$A \rightsquigarrow B$" means A can be reduced to B. "n.r." denotes nonce-respecting and "n.m." denotes nonce-misuse. "PRP" stands for pseudorandom permutation, "TPRP" stands for tweakable PRP, and "PRF" stands for pseudorandom function. Let m be the block length of the plaintext and a be the block length of associated data. Let $r, \omega \geq 2$ be two integers. Let $\simeq$ stand for approximately equal to. For example, $\simeq$128 means that it is approximately equal to 128.

	CHM	GCM-SIVr	OGCM-1	OGCM-2	SCT	SIVx	RWCTRN
# keys	1	$r^2 + 2r \rightsquigarrow 3r$	$3 \rightsquigarrow 1$	$3 \rightsquigarrow 1$	1	1	$2 \rightsquigarrow 1$
Nonce scenario	n.r.	n.m.	n.r.	n.r.	n.m.	n.m.	n.r.
Assumption	PRP	PRP	PRP	PRP	TPRP	TPRP	PRF
Block size n	128	128	128	128	128	128	256
Security (bits)	85.3333	$128r/(r+1)$	107.9565	121.9339	$\simeq$128	$\simeq$128	248
# primitive Calls	$m + \lceil m/\omega \rceil + 2$	$r(m+r)$	$2m+2$	$2m+2$	$a + 2m + 3$	$a + 2m + 2$	$m+2$
# multiplications	$a+m$	$r(a+m+1)$	$a+m+1$	$a+m+1$	0	0	$a+m+1$
Reference	[30]	[32]	This paper	This paper	[12]	[11]	[47]

From the perspective of security, they enjoy close to optimal security in the nonce-respecting scenario assuming that the underlying block cipher is a secure PRP. They can encrypt at most 2^l plaintexts in the nonce-respecting scenario and the maximum block length of the plaintext is $2^{n-l} - 1$, where l is the nonce length and n is the block size. The privacy of OGCM-1 (resp., OGCM-2) is upper-bounded by $\sigma/2^n$ and the authenticity of OGCM-1 (resp., OGCM-2) is upper-bounded by $\sigma/2^n + \epsilon + n/2^n + 2/2^\tau$, for $q \simeq 2^n/67(n-1)^2$ (resp., $q \simeq 2^n/67$) adversarial queries and one forgery attempt, where q is the number of the encryption queries, σ is the query complexity, and τ is the bit length of the authentication tag. In other words, the privacy and authenticity of OGCM-1 ensure at most about $(n - \log 67 - 2\log(n-1))$-bit security, while the privacy and authenticity of OGCM-2 ensure at most about $(n - \log 67)$-bit security, where $\log x$ denotes the log (base 2) of x. Let $n = 128$, $l = 96$, $\epsilon = 2^{-n}$, and $\tau = 128$. AES-OGCM-1 and AES-OGCM-2 can encrypt at most 2^{96} plaintexts in the nonce-respecting scenario, the maximum length of the plaintext is about 2^{32} blocks (64 GBytes), and the privacy and authenticity achieve roughly 107.9565-bit or 121.9339-bit security which is better than those of AES-GCM (about 64-bit security). Alike GCM, OGCM-1 and OGCM-2 are based on polynomial AXU hash functions which may introduce some attacks, such as [36, 37, 42, 43].

From the perspective of efficiency, they invoke two block ciphers for encrypting each plaintext block (that is to say, their rate is 1/2) and inherit most of the advantages of GCM (such as parallelizable, stream-cipher encryption, and high speed implementation). Specifically, they utilize three keys, call the underlying block cipher $2m + 2$ times, and use $a + m + 1$ finite-field multiplications, while GCM is based on one key, calls the underlying block cipher $m + 2$ times, and utilizes $a + m + 1$ finite-field multiplications, where m (resp., a) is the block length of the plaintext (resp., associated data). Compared with GCM, the efficiency is about half of it. Therefore, OGCM-1 and OGCM-2 compromise the efficiency of the software and hardware implementation to enhance the security.

Compared with some existing BBB-secure AE schemes, OGCM-1 and OGCM-2 are block cipher-based nonce-respecting AE modes that ensure close to optimal security and provide good efficiency. Details are shown in Table 2. Note that RWCTRN [47] is based on the PRF assumption. Therefore, its block size n is at least 256.

OGCM-1 and OGCM-2 utilize three keys, which increase the cost of key management. Therefore, we introduce a key deriving method which converts a key to multiple keys. Here, the hash-function key K_h and the block cipher keys (K_1, K_2) can be derived from a secret key K by encrypting three distinct constants. Thus, we can obtain reduced single-key OGCM-1 and OGCM-2 schemes.

This paper focuses on the strong security of GCM in the nonce-respecting scenario. A natural direction for future work is how we can design an improved mode that provides strong security in the nonce-misuse and even other misuse scenarios (e.g., the releasing of unverified plaintext and decryption misuse scenarios).

8. Conclusions

This paper focuses on the strong security of GCM and presents two close to optimally secure variants OGCM-1 and OGCM-2. They are based on the "Encryption-then-MAC" approach, where the encryption part utilizes multiple EDM or EDMD constructions to set up a close to optimally secure key-stream generator and then the MAC part combines an AXU hash function and one EDM or EDMD construction to generate an authentication tag. OGCM-1 and OGCM-2 achieve a balance between the security and the efficiency. In terms of security, OGCM-1 guarantees at most roughly $(n - \log 67 - 2\log(n-1))$-bit security and OGCM-2 guarantees at most roughly $(n - \log 67)$-bit security, where n is the block size. In terms of efficiency, their rate is 1/2; that is, they invoke two block ciphers for encrypting each plaintext block. Compared with GCM [33] and CHM [30], OGCM-1 and OGCM-2 guarantee stronger security but achieve lower efficiency. Compared with GCM-SIVr [32], OGCM-1 and OGCM-2 guarantee close to optimal security and achieve higher efficiency.

GCM is a NIST recommended block cipher mode of operation and has wide applications, but it only ensures the birthday-bound security. OGCM-1 and OGCM-2 that provide close to optimal security are the extensions of GCM, which is of great significance in practice.

Conflicts of Interest

There are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by National Natural Science Foundation of China (Grant nos. 61522210 and 61632013).

References

[1] P. Rogaway, "Authenticated-encryption with associated-data," in *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS '02)*, pp. 98–107, Washington, Wash, USA, November 2002.

[2] Y. Sasaki and K. Yasuda, "A new mode of operation for incremental authenticated encryption with associated data," in *Selected areas in cryptography—SAC 2015*, vol. 9566 of *Lecture Notes in Computer Science*, pp. 397–416, Springer, Heidelberg, Germany, 2016.

[3] C. S. Jutla, "Encryption modes with almost free message integrity," in *Advances in cryptology—EUROCRYPT 2001 (Innsbruck)*, vol. 2045 of *Lecture Notes in Computer Science*, pp. 529–544, Springer, Heidelberg, Germany, 2001.

[4] P. Rogaway, "Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC," in *Advances in cryptology—ASIACRYPT 2004*, vol. 3329 of *Lecture Notes in Computer Science*, pp. 16–31, Springer, Heidelberg, Germany, 2004.

[5] P. Rogaway, M. Bellare, and R. S. Ferguson, "OCB: a block-cipher mode of operation for efficient authenticated encryption," *ACM Transactions on Information and System Security*, vol. 6, no. 3, pp. 365–403, 2003.

[6] E. Andreeva, A. Bogdanov, A. Luykx, B. Mennink, E. Tischhauser, and K. Yasuda, "Parallelizable and authenticated online ciphers," in *Advances in cryptology—ASIACRYPT 2013*, vol. 8269 of *Lecture Notes in Computer Science*, pp. 424–443, Springer, Heidelberg, Germany, 2013.

[7] F. Abed, S. Fluhrer, C. Forler et al., "Pipelineable on-line encryption," in *Fast Software Encryption*, vol. 8540 of *Lecture Notes in Computer Science*, pp. 205–223, Springer, Heidelberg, Germany, 2015.

[8] L. Bossuet, N. Datta, C. Mancillas-Lopez, and M. Nandi, "ELmD: a pipelineable authenticated encryption and its hardware implementation," *IEEE Transactions on Computers*, vol. 65, no. 11, pp. 3318–3331, 2016.

[9] E. Fleischmann, C. Forler, and S. Lucks, "McOE: a family of almost foolproof on-line authenticated encryption schemes," in *Fast Software Encryption*, vol. 7549 of *Lecture Notes in Computer Science*, pp. 196–215, Springer, Heidelberg, Germany, 2012.

[10] C. Forler, E. List, S. Lucks, and J. Wenzel, "Efficient beyond-birthday-bound-secure deterministic authenticated encryption with minimal stretch," in *ACISP 2016: Information Security and Privacy*, vol. 9723 of *Lecture Notes in Computer Science*, pp. 317–332, Springer, Heidelberg, Germany, 2016.

[11] E. List and M. Nandi, "Revisiting full-PRF-secure PMAC and using it for beyond-birthday authenticated encryption," in *Topics in cryptology—CT-RSA 2017*, vol. 10159 of *Lecture Notes in Computer Science*, pp. 258–274, Springer, Heidelberg, Germany, 2017.

[12] T. Peyrin and Y. Seurin, "Counter-in-tweak: authenticated encryption modes for tweakable block ciphers," in *Advances in Cryptology–CRYPTO 2016*, vol. 9814 of *Lecture Notes in Computer Science*, pp. 33–63, Springer, Heidelberg, Germany, 2016.

[13] M. Liskov, R. L. Rivest, and D. Wagner, "Tweakable block ciphers," in *Advances in Cryptology–CRYPTO 2002*, vol. 2442 of *Lecture Notes in Computer Science*, pp. 31–46, Springer, Heidelberg, Germany, 2002.

[14] M. Liskov, R. L. Rivest, and D. Wagner, "Tweakable block ciphers," *Journal of Cryptology*, vol. 24, no. 3, pp. 588–613, 2011.

[15] T. Iwata and K. Yasuda, "HBS: a single-key mode of operation for deterministic authenticated encryption," in *Fast Software Encryption*, vol. 5665 of *Lecture Notes in Computer Science*, pp. 394–415, Springer, Heidelberg, Germany, 2009.

[16] P. Rogaway and T. Shrimpton, "A provable-security treatment of the key-wrap problem," in *Advances in cryptology—EUROCRYPT 2006*, vol. 4004 of *Lecture Notes in Computer Science*, pp. 373–390, Springer, Heidelberg, Germany, 2006.

[17] V. T. Hoang, T. Krovetz, and P. Rogaway, "Robust authenticated-encryption AEZ and the problem that it solves," in *Advances in Cryptology–EUROCRYPT 2015*, vol. 9056 of *Lecture Notes in Computer Science*, pp. 15–44, Springer, Heidelberg, Germany, 2015.

[18] N. Ferguson, D. Whiting, B. Schneier, J. Kelsey, S. Lucks, and T. Kohno, "Helix: fast encryption and authentication in a single cryptographic primitive," in *Fast Software Encryption*, vol. 2887 of *Lecture Notes in Computer Science*, pp. 330–346, Springer, Heidelberg, Germany, 2003.

[19] H. Wu and B. Preneel, "AEGIS: a fast authenticated encryption algorithm," in *Selected Areas in Cryptography—SAC 2013*, vol. 8282 of *Lecture Notes in Computer Science*, pp. 185–201, Springer, Heidelberg, Germany, 2014.

[20] M. Bellare and C. Namprempre, "Authenticated encryption: relations among notions and analysis of the generic composition paradigm," in *Advances in Cryptology–ASIACRYPT 2000*, vol. 1976 of *Lecture Notes in Computer Science*, pp. 531–545, Springer, Heidelberg, Germany, 2000.

[21] M. Bellare, P. Rogaway, and D. Wagner, "The EAX mode of operation," in *FSE 2004: Fast Software Encryption*, B. Roy and W. Meier, Eds., vol. 3017 of *Lecture Notes in Computer Science*, pp. 389–407, Springer, Heidelberg, Germany, 2004.

[22] T. Krovetz, "HS1-SIV," 2015, https://competitions.cr.yp.to/round2/hs1sivv2c.pdf.

[23] P. Jovanovic, A. Luykx, and B. Mennink, "Beyond $2^{c/2}$ security in sponge-based authenticated encryption modes," in *Advances in Cryptology–ASIACRYPT 2014*, vol. 8873 of *Lecture Notes in Computer Science*, pp. 85–104, Springer, Heidelberg, Germany, 2014.

[24] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schlaffer, "Ascon v1.2," 2016, https://competitions.cr.yp.to/round3/asconv12.pdf.

[25] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Duplexing the sponge: single-pass authenticated encryption and other applications," in *SAC 2011: Selected Areas in Cryptography*, vol. 7118 of *Lecture Notes in Computer Science*, pp. 320–337, Springer, Heidelberg, Germany, 2012.

[26] R. Granger, P. Jovanovic, B. Mennink, and S. Neves, "Improved masking for tweakable blockciphers with applications to authenticated encryption," in *Advances in Cryptology–EUROCRYPT 2016*, vol. 9665 of *Lecture Notes in Computer Science*, pp. 263–293, Springer, Heidelberg, Germany, 2016.

[27] S. Cogliani, D. S. Maimuţ, D. Naccache et al., "OMD: a compression function mode of operation for authenticated encryption," in *Selected areas in cryptography—SAC 2014*, vol. 8781 of *Lecture Notes in Computer Science*, pp. 112–128, Springer, Heidelberg, Germany, 2014.

[28] R. Reyhanitabar, S. Vaudenay, and D. Vizár, "Boosting OMD for almost free authentication of associated data," in *FSE 2015: Fast Software Encryption*, vol. 9054 of *Lecture Notes in Computer Science*, pp. 411–427, Springer, Heidelberg, Germany, 2015.

[29] K. Minematsu, "Parallelizable rate-1 authenticated encryption from pseudorandom functions," in *Advances in Cryptology–EUROCRYPT 2014*, vol. 8441 of *Lecture Notes in Computer Science*, pp. 275–292, Springer, Heidelberg, Germany, 2014.

[30] T. Iwata, "New blockcipher modes of operation with beyond the birthday bound security," in *Fast Software Encryption*, vol. 4047 of *Lecture Notes in Computer Science*, pp. 310–327, Springer, Heidelberg, Germany, 2006.

[31] T. Iwata, "Authenticated encryption mode for beyond the birthday bound security," in *Advances in Cryptology–AFRICACRYPT 2008*, vol. 5023 of *Lecture Notes in Computer Science*, pp. 125–142, Springer, Heidelberg, Germany, 2008.

[32] T. Iwata and K. Minematsu, "Stronger security variants of GCM-SIV," *IACR Transactions on Symmetric Cryptology*, vol. 2016, no. 1, pp. 134–157, 2016.

[33] D. A. McGrew and J. Viega, "The security and performance of the Galois/counter mode (GCM) of operation," in *Progress in cryptology—INDOCRYPT 2004*, vol. 3348 of *Lecture Notes in Computer Science*, pp. 343–355, Springer, Heidelberg, Germany, 2004.

[34] T. Iwata, K. Ohashi, and K. Minematsu, "Breaking and repairing GCM security proofs," in *Advances in cryptology—CRYPTO 2012*, vol. 7417 of *Lecture Notes in Computer Science*, pp. 31–49, Springer, Heidelberg, Germany, 2012.

[35] Y. Niwa, K. Ohashi, K. Minematsu, and T. Iwata, "GCM security bounds reconsidered," in *Fast Software Encryption*, vol. 9054 of *Lecture Notes in Computer Science*, pp. 385–407, Springer, Heidelberg, Germany, 2015.

[36] M. J. O. Saarinen, "Cycling attacks on GCM, GHASH and other polynomial MACs and hashes," in *Fast Software Encryption*, A. Canteaut, Ed., Lecture Notes in Computer Science, pp. 216–225, Springer, Heidelberg, Germany, 2012.

[37] M. A. Abdelraheem, P. Beelen, A. Bogdanov, and E. Tischhauser, "Twisted polynomials and forgery attacks on GCM," in *Advances in Cryptology–EUROCRYPT 2015*, vol. 9056 of *Lecture Notes in Computer Science*, pp. 762–786, Springer, Heidelberg, Germany, 2015.

[38] M. Bellare and B. Tackmann, "The multi-user security of authenticated encryption: AES-GCM in TLS 1.3," in *Advances in cryptology—CRYPTO 2016*, vol. 9814 of *Lecture Notes in Computer Science*, pp. 247–276, Springer, Heidelberg, Germany, 2016.

[39] H. Böck, A. Zauner, S. Devlin, J. Somorovsky, and P. Jovanovic, "Nonce-disrespecting adversaries: practical forgery attacks on GCM in TLS," 2016, https://eprint.iacr.org/2016/475.pdf.

[40] S. Gueron and Y. Lindell, "GCM-SIV: full nonce misuse-resistant authenticated encryption at under one cycle per byte," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, CCS 2015*, pp. 109–119, Denver, Colo, USA, October 2015.

[41] K. Aoki and K. Yasuda, "The security and performance of 'GCM' when short multiplications are used instead," in *Information Security and Cryptology*, vol. 7763 of *Lecture Notes in Computer Science*, pp. 225–245, Springer Berlin Heidelberg, Heidelberg, Germany, 2013.

[42] W.-S. Yap, S. L. Yeo, S.-H. Heng, and M. Henricksen, "Security analysis of GCM for communication," *Security and Communication Networks*, vol. 7, no. 5, pp. 854–864, 2014.

[43] B. Zhu, Y. Tan, and G. Gong, "Revisiting MAC forgeries, weak keys and provable security of Galois/counter mode of operation," in *Cryptology and network security*, vol. 8257 of *Lecture Notes in Computer Science*, pp. 20–38, Springer, Heidelberg, Germany, 2013.

[44] T. Iwata and Y. Seurin, "Reconsidering the security bound of AES-GCM-SIV," 2017, https://eprint.iacr.org/2017/708.pdf.

[45] B. t. Cogliati and Y. Seurin, "EWCDM: an efficient, beyond-birthday secure, nonce-misuse resistant MAC," in *Advances in cryptology—CRYPTO 2016*, vol. 9814 of *Lecture Notes in Computer Science*, pp. 121–149, Springer, Heidelberg, Germany, 2016.

[46] B. Mennink and S. Neves, "Encrypted davies-meyer and its dual: towards optimal security using mirror theory," in *Advances in cryptology—CRYPTO 2017*, vol. 10403 of *Lecture Notes in Computer Science*, pp. 556–583, Springer, Heidelberg, Germany, 2017.

[47] P. Zhang, H. G. Hu, and P. Wang, "Efficient beyond-birthday-bound secure authenticated encryption modes," *Science China Information Sciences*, 2017.

[48] B. Mennink and S. Neves, "Optimal PRFs from Blockcipher Designs," *IACR Transactions on Symmetric Cryptology*, vol. 2017, no. 3, pp. 228–252, 2017.