


Article

# A Single-Key Variant of LightMAC\_Plus

Haitao Song 

Department of Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China; allen5@sjtu.edu.cn

**Abstract:** LightMAC\_Plus proposed by Naito (ASIACRYPT 2017) is a blockcipher-based MAC that has beyond the birthday bound security without message length in the sense of PRF (Pseudo-Random Function) security. In this paper, we present a single-key variant of LightMAC\_Plus that has beyond the birthday bound security in terms of PRF security. Compared with the previous construction LightMAC\_Plus1k of Naito (CT-RSA 2018), our construction is simpler and of higher efficiency.

**Keywords:** symmetric cryptography; LightMAC\_plus; single key; provable security; MAC; message authentication code

## 1. Introduction

A MAC (Message Authentication Code) is a fundamental symmetric-key primitive that produces a tag to authenticate a message. MACs are often based on a blockcipher (e.g., CBC-MAC [1], PMAC [2], OMAC [3], LightMAC [4]) so that these become secure PRFs (Pseudo-Random Functions) under the standard assumption that the underlying keyed blockciphers are pseudo-random permutations because of the well known observation that PRFs are secure MACs [1]. Most blockcipher-based MACs have a security bound that is called birthday security, i.e., against up to  $O(2^{n/2})$  adversarial queries (here  $n$  is the block length of the underlying blockcipher).

However the birthday bound security may not be enough for blockciphers with short block sizes such as TripleDES and lightweight blockciphers such as PRESENT [5], LED [6], GIFT [7]. Therefore, designing a MAC with beyond birthday-bound security is an important research of MAC design. This kind of MACs contribute not only to the longevity of 128-bit blockciphers but also to blockciphers with short block sizes. To go beyond birthday-bound security, a series of blockcipher-based MACs have been proposed, including SUM-ECBC [8], PMAC\_Plus [9] and 3kf9 [10].

LightMAC [4] is a variant of PMAC [2] and the first blockcipher-based MAC with birthday security without message length. In LightMAC, for each  $n$ -bit blockcipher call, an  $m$ -bit counter and an  $(n - m)$ -bit message block are input. By the presence of counters, LightMAC becomes a secure PRF up to  $O(2^{n/2})$  tagging queries. LightMAC, adopts the counter-based construction used in the protected counter sum [11] and XOR MAC [12] to avoid the input collision. So the input for the  $i$ -th blockcipher call is  $\langle i \rangle_m \| M_i$ , where  $\langle i \rangle_m$  represents the corresponding  $m$ -bit binary number of  $i$  and  $M_i$  represents the  $i$ -th message block of  $n - m$  bits. For LightMAC, the xor value of the blockcipher outputs becomes a hash value, and then a tag is defined by encrypting the hash value. LightMAC\_Plus proposed by Naito [13] is a blockcipher-based MAC which is beyond birthday secure up to roughly  $2^{2n/3}$  (tagging or verification) queries. LightMAC\_Plus follows the Double-Block Hash-then-Sum (DbHtS), where a message is first mapped into a  $2n$ -bit string by a double-block hash function and then the two encrypted values of each  $n$ -bit half is xor-summed to generate the tag. Datta et al. [14] have proved that both three-key and two-key DbHtS constructions can achieve beyond-birthday-bound security with a bound  $q^3/2^{2n}$  where  $q$  is the number of MAC queries. Leurent et al. [15] show attacks on all three-key DbHtS constructions with query complexity  $2^{3n/4}$ . Very recently, Kim et al. [16] give a tight provable bound  $q^{4/3}/2^n$  for three-key DbHtS constructions. Compared with LightMAC,



**Citation:** Song, H. A Single-Key Variant of LightMAC\_Plus. *Symmetry* **2021**, *13*, 1818. <https://doi.org/10.3390/sym13101818>

Academic Editors: Jose M. Rodriguez and José M. Sigarreta

Received: 3 August 2021

Accepted: 23 September 2021

Published: 29 September 2021

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2021 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

LightMAC\_Plus has a better security bound but the key size is increased and the efficiency is degraded.

Naito also proposed LightMAC\_Plus1k [17] which is a single key variant of LightMAC\_Plus. LightMAC\_Plus1k has been proved the same level of security as LightMAC\_Plus. To reduce the number of the keys from three to one, Naito use the first two bits for the domain separation: in the hash part, the most significant bit of an input to the blockcipher is set to zero; in the finalization function, the most significant two bits are 10 and 11. Moreover, by using of the domain separation, a 4-bit security degradation is compromised from LightMAC\_Plus to LightMAC\_Plus1k.

### Our Contributions

Our main contribution in this paper is to design a simpler and more efficient single key variant of LightMAC\_Plus, but with the same secure level as LightMAC\_Plus1k. The new construction is called 1k-LightMAC\_Plus. In order to reduce the key size, we also use the domain separation technique. Different from LightMAC\_Plus1k, the hash function for 1k-LightMAC\_Plus remains the same with LightMAC\_Plus. In the finalization function, the least significant bit of an input to one of two keyed blockciphers is fixed to zero and the other is fixed to one. Due to the domain separation, the two blockciphers calling with the same key in the finalization function have completely distinct input sets. What is more, we proved that 1k-LightMAC\_Plus has the same security level as LightMAC\_Plus1k in the sense of PRF security.

## 2. Preliminaries

### 2.1. Notations

$\{0, 1\}^n$  represents the set of all strings of length  $n$ . For any two strings  $X, Y \in \{0, 1\}^*$ , denote their concatenation as  $X||Y$ , and denote their bitwise exclusive or as  $X \oplus Y$ .  $|X|$  denotes the bit length of string  $X$ . We use  $N = 2^n$ . We use  $\mathbf{1}$  and  $\mathbf{0}$  to denote the  $n$ -bit binary string  $0^{n-1}||1$  and  $0^n$ , respectively. Moreover we denote  $a \in \{b, b \oplus 1\}$  as  $a =_1 b$  for  $a, b \in \{0, 1\}^n$ . That is,  $a =_1 b$  implies either  $a = b$  or  $a = b \oplus 1$  but not both. The natural index set  $\{1, 2, \dots, q\}$  is denoted as  $[q] := [1 \dots q]$  for a positive integer  $q$ . For a given ordered set  $\mathcal{S}$  we use  $\min \mathcal{S}$  to denote the minimum element of  $\mathcal{S}$ .  $\mathcal{X} \cap \mathcal{Y}$  denotes the intersection of set  $\mathcal{X}$  and  $\mathcal{Y}$ . If  $\mathcal{X} \cap \mathcal{Y} = \emptyset$  then we write  $\mathcal{X} \sqcup \mathcal{Y}$  to denote the disjoint union. The set of all functions from  $\mathcal{X}$  to  $\mathcal{Y}$  is denoted as  $\text{Func}(\mathcal{X}, \mathcal{Y})$  and the set of all permutations over  $\mathcal{X}$  is denoted as  $\text{Perm}(\mathcal{X})$ . The notation  $X \stackrel{\$}{\leftarrow} \mathcal{S}$  means that  $X$  is chosen uniformly at random from a finite set  $\mathcal{S}$  and independently of all other random variables defined so far. We also denote  $\mathbf{P}(a, b)$  as the number of permutations of taking  $b$  objects from  $a$  distinct objects at a time, which means that  $\mathbf{P}(a, b) = \prod_{i=1}^b (a - (i - 1))$ . For a list  $\mathcal{L} = \{(a_1, b_1), \dots, (a_\ell, b_\ell)\}$ ,  $\text{Dom}(\mathcal{L}) := \{a_1, \dots, a_\ell\}$ ,  $\overline{\text{Dom}}(\mathcal{L}) := \{0, 1\}^n \setminus \{a_1, \dots, a_\ell\}$  and  $\text{Rng}(\mathcal{L}) := \{b_1, \dots, b_\ell\}$ ,  $\overline{\text{Rng}}(\mathcal{L}) := \{0, 1\}^n \setminus \{b_1, \dots, b_\ell\}$ .

### 2.2. Security Definitions

$F : \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{Y}$  is a keyed function with domain  $\mathcal{X} \subseteq \{0, 1\}^*$ , range  $\mathcal{Y}$  and key space  $\mathcal{K}$ . We also write  $F_K(X)$  for  $F(K, X)$ . A  $(q, t, \sigma)$ -distinguisher in the presence of  $F$  is an algorithm  $\mathcal{A}$  that has oracle access to a function with domain  $\mathcal{X}$  and range  $\mathcal{Y}$ . Assume that  $\mathcal{A}$  makes at most  $q$  queries and totally  $\sigma$  blocks one whose running time is at most  $t$ , and finally outputs a single bit. The PRF-security of  $F$ , i.e., distinguishing  $F$  from  $R$  that is randomly uniformly chosen from  $\text{Func}(\mathcal{X}, \mathcal{Y})$ , is defined as

$$\text{Adv}_F^{\text{prf}}(\mathcal{A}) \stackrel{\text{def}}{=} \left| \Pr \left[ K \stackrel{\$}{\leftarrow} \mathcal{K} : \mathcal{A}^{F_K} = 1 \right] - \Pr \left[ R \stackrel{\$}{\leftarrow} \text{Func}(\mathcal{X}, \mathcal{Y}) : \mathcal{A}^R = 1 \right] \right|.$$

$F_K(X)$  becomes a permutation When  $\mathcal{X} = \mathcal{Y}$ . Then the PRP-security of  $F$  can be defined as follows.

$$\text{Adv}_F^{\text{prp}}(\mathcal{A}) \stackrel{\text{def}}{=} \left| \Pr \left[ K \stackrel{\$}{\leftarrow} \mathcal{K} : \mathcal{A}^{F_K} = 1 \right] - \Pr \left[ R \stackrel{\$}{\leftarrow} \text{Perm}(\mathcal{X}) : \mathcal{A}^R = 1 \right] \right|.$$

When  $atk \in \{prf, prp\}$ , we define

$$\text{Adv}_F^{\text{atk}}(q, t, \sigma) \stackrel{\text{def}}{=} \max_{\mathcal{A}} \text{Adv}_F^{\text{atk}}(\mathcal{A})$$

### 2.3. H-Coefficient Technique

Now we introduce a proof technique named the H-Coefficient technique [18,19]. Here just a brief description is provided, and interested readers can refer to [18,19] for a complete explanation. We assume that the distinguisher  $\mathcal{A}$  is information-theoretic, which is computationally not bounded. Therefore, without loss of generality we assume  $\mathcal{A}$  is deterministic. Suppose  $\mathcal{A}$  interacts with one of two oracles, the “real world” oracle  $\mathcal{O}$  or the “ideal world” oracle  $\mathcal{Q}$ . The query-response tuples that  $\mathcal{A}$  receives is called a view. Let  $X$  (resp.  $Y$ ) be the probability distribution of the view when  $\mathcal{A}$  interacts with  $\mathcal{O}$  (resp.  $\mathcal{Q}$ ). Let  $\mathcal{T}$  be the set of all *attainable* views  $\tau$  when interacting with  $\mathcal{Q}$ , that is  $\mathcal{T} = \{\tau \mid \Pr[Y = \tau] > 0\}$ .

The H-Coefficient technique partitions  $\mathcal{T}$  into two subsets  $\mathcal{T}_{\text{good}}$  and  $\mathcal{T}_{\text{bad}}$  which are disjoint such that  $\mathcal{T} = \mathcal{T}_{\text{good}} \cup \mathcal{T}_{\text{bad}}$ . If there exist  $0 \leq \epsilon_1, \epsilon_2 \leq 1$  so that

- For  $\forall \tau \in \mathcal{T}_{\text{good}}$ , it holds that

$$\frac{\Pr[X = \tau]}{\Pr[Y = \tau]} \geq 1 - \epsilon_1.$$

- For a view  $\tau \stackrel{\$}{\leftarrow} \mathcal{T}$ , it holds that

$$\Pr[\tau \in \mathcal{T}_{\text{bad}}] \leq \epsilon_2.$$

Then the advantage of  $\mathcal{A}$  can be bounded as

$$\text{Adv}(\mathcal{A}) \leq \epsilon_1 + \epsilon_2.$$

## 3. 1k-LightMAC\_Plus

### 3.1. Specification

In this section, we introduce our single-key variant of LightMAC\_Plus, which is called 1k-LightMAC\_Plus. The XOR of two independent permutations is a “natural” PRP-to-PRF method. If only a single permutation is to be used, one can simulate this independence through domain separation. Therefore, domain separation can be used to reduce the number of keys. We process the finalization function of LightMAC\_Plus with a same key but the least significant bit of an input to one of two keyed blockciphers is fixed to 0 and the other is fixed to 1.

The details for 1k-LightMAC\_Plus is presented in Algorithm 1 (the subfunction used in Algorithm 1 is defined as Algorithm 2) and depicted in Figure 1.

---

#### Algorithm 1 1k-LightMAC\_Plus $[E_K](M)$ .

---

- 1:  $(v, w) \leftarrow \text{InternalHash}[E_K](M)$
  - 2:  $T_1 \leftarrow E_K(v)$
  - 3:  $T_2 \leftarrow E_K(w)$
  - 4:  $T \leftarrow T_1 \oplus T_2$
  - 5: **Return**  $T$
-

**Algorithm 2** InternalHash $[E_K](M)$ .

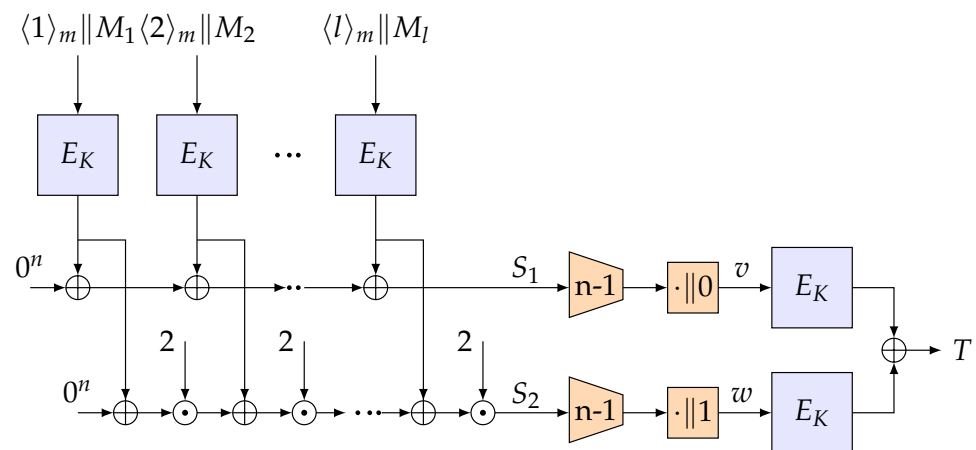
---

```

1:  $M \leftarrow M \| 10^*$ 
2:  $M_1 M_2 \dots M_L \leftarrow \text{Partition}(M), S_1 = 0^{n-1}, S_2 = 0^{n-1}$ 
3: for  $i = 1, 2, \dots, l$  do
4:    $B_i \leftarrow \langle i \rangle_m \| M_i; C_i \leftarrow E_K(B_i)$ 
5:    $S_1 \leftarrow S_1 \oplus C_i; S_2 \leftarrow S_2 \oplus 2^{l-i+1} \cdot C_i$ 
6: end for
7:  $v_0 \leftarrow \text{lsb}_{n-1}(S_1); w_0 \leftarrow \text{lsb}_{n-1}(S_2)$ 
8:  $v \leftarrow v_0 \| 0; w \leftarrow w_0 \| 1$ 
9: Return  $(v, w)$ 

```

---

**Figure 1.** Illustration of 1k-LightMAC\_Plus.

### 3.2. Security Bound

**Theorem 1.** Any distinguisher with running time  $t$ , making  $q$ -tuple of distinct messages with an aggregate of total  $\sigma$ -many blocks, can distinguish 1k-LightMAC\_Plus $[E]$  from a uniform random function by

$$\text{Adv}_{1\text{k-LightMAC\_Plus}[E]}^{\text{prf}}(q, t, \sigma) \leq \text{Adv}_E^{\text{prp}}(2q + \sigma + 2, t') + \frac{147q^2\sigma^2}{N^3} + \frac{114q\sigma^2}{N^2} + \frac{16\sigma}{N} + \frac{q}{N}$$

where  $t' = t + O(2q + \sigma + 2)$ .

The proof is provided in next section.

## 4. Proof of Theorem 1

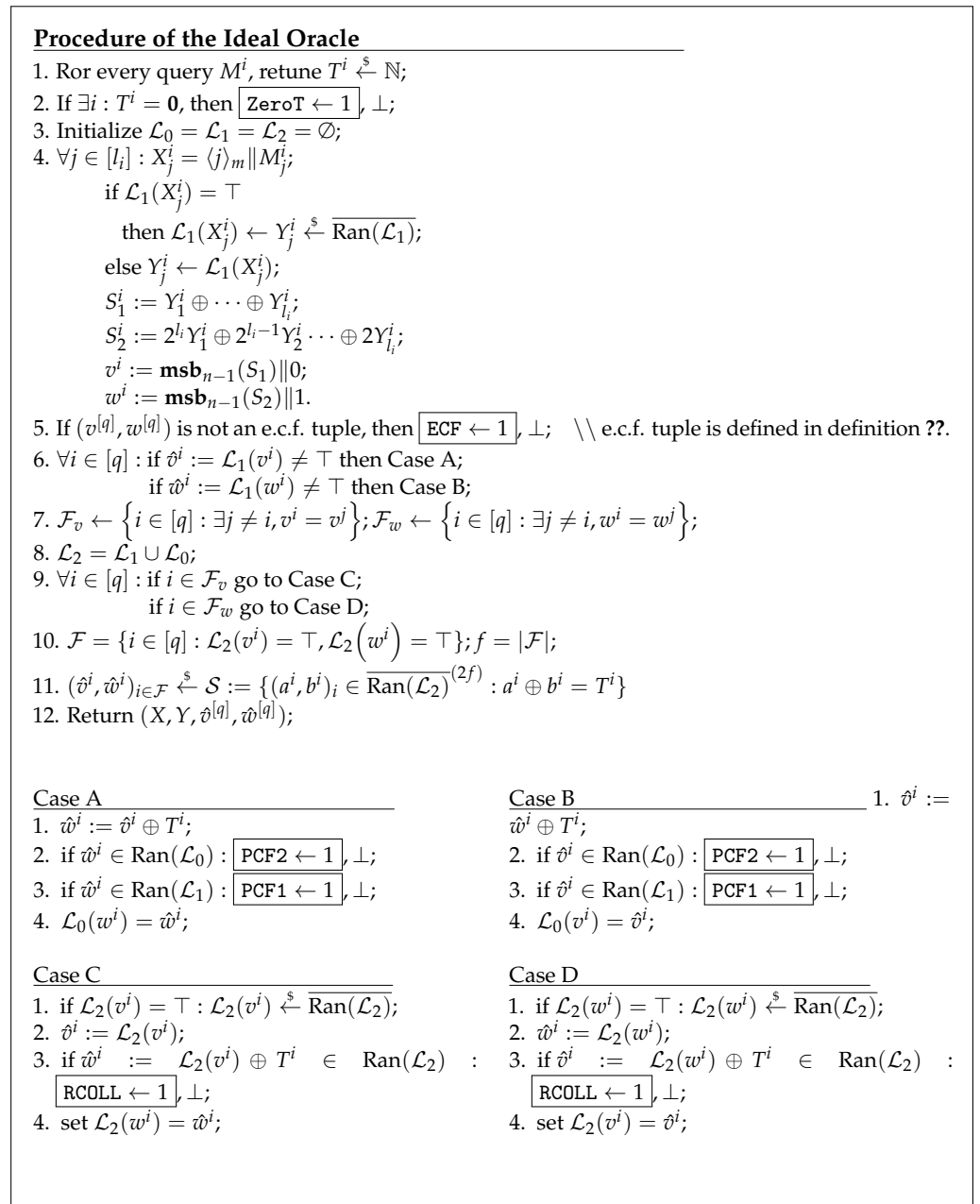
In this section, we prove Theorem 1 with the H-coefficient technique.

### 4.1. Initialization

We assume that the distinguisher  $\mathcal{A}$  interacts with either the ideal oracle or the real oracle 1k-LightMAC\_Plus with a random permutation  $\Pi$  and that the distinguisher  $\mathcal{A}$  always makes deterministic and non-repeating queries.

#### 4.1.1. Ideal Oracle

The ideal oracle defined here is comprised of two phases: (a) One is called online phase. For each query  $M^i$  made by  $\mathcal{A}$ , the oracle samples the response  $T^i \xleftarrow{\$} \{0, 1\}^n$  and then returns it to the distinguisher  $\mathcal{A}$ . (b) The other is called offline phase. In this phase, the oracle samples the internal hash value for each query in a without-replacement manner from  $\{0, 1\}^n$ . During the sampling, if some specific event happens, then the oracle aborts the process. The ideal oracle is formally shown in Figure 2.



**Figure 2.** Ideal Oracle: boxed items denote bad events.  $\perp$  and  $\top$  denote the abort symbol and an undefined variable, respectively.

#### 4.1.2. Views

At the end of  $\mathcal{A}$  interacting with the oracle and before  $\mathcal{A}$  outputting the bit, we reveal the values of internal computations  $(X, Y, \hat{v}^{[q]}, \hat{w}^{[q]})$  to  $\mathcal{A}$ . Thus, the view of  $\mathcal{A}$  is in the form

$$\tau = (M^{[q]}, T^{[q]}, X, Y, \hat{v}^{[q]}, \hat{w}^{[q]}).$$

For two block tuples  $X, Y$ , if there exist permutations  $\pi \in \text{Perm}$  such that  $\pi(x^i) = y^i$ , we call  $X$  and  $Y$  permutation compatible, denoted as  $X \xrightarrow{\pi} Y$ . It is straightforward that in the real world an attainable transcript must satisfy the following two conditions at the same time.

$$\begin{aligned} \hat{v}^i \oplus \hat{w}^i &= T^i, \forall i \in [q] \text{ and} \\ (X, v^{[q]}, w^{[q]}) &\xrightarrow{\pi} (Y, \hat{v}^{[q]}, \hat{w}^{[q]}). \end{aligned}$$

The notation  $X_{id}$  represents the probability distribution of transcript  $\tau$  induced by the ideal world, while  $X_{re}$  represents that induced by the real world. We call a transcript  $\tau$  attainable if  $\Pr[X_{id} = \tau] > 0$ . All such attainable views contribute to a set  $\mathcal{T}$ . Besides, we partition  $\mathcal{T}$  into two disjoint subsets  $\mathcal{T}_{\text{good}}$  and  $\mathcal{T}_{\text{bad}}$  such that  $\mathcal{T} = \mathcal{T}_{\text{good}} \cup \mathcal{T}_{\text{bad}}$ .

#### 4.2. Analysis of Bad Events

We define bad events in the ideal world according to the freshness of  $v^i$  and  $w^i$ , which consists of four different cases. Here we first introduce a definition.

**Definition 1.** Let  $X$  be the set of all the inputs  $X_j^i$  of internal hash part for  $\forall i \in [q]$  and  $\forall j \in [l_i]$ . If there exists an  $i \in [q]$  s.t.  $v^i$  is non-fresh in the union set  $v^{[q]} \cup X$  and simultaneously  $w^i$  is non-fresh in the union set  $w^{[q]} \cup X$ , then the tuple  $(v^{[q]}, w^{[q]})$  is called “an extended covered tuple”. Otherwise, the tuple is said to be “an e.c.f tuple” (short for “an extended cover free tuple”).

Both  $v^i$  and  $w^i$  are non-fresh

In this case, a bad event ECF occurs (defined in Figure 2). For 1k-lightMAC\_Plus, “Non-fresh”  $v^i$  can collide with some previous  $v$  or some input blocks and so is  $w^i$ .

$v^i$  is fresh and  $w^i$  is non-fresh

In this case, bad events PCF1 PCF2 and RCOLL happen.

$v^i$  is non-fresh and  $w^i$  is fresh

This is similar to the “ $v^i$  is fresh and  $w^i$  is non-fresh” case.

Both  $v^i$  and  $w^i$  are fresh.

Owing to the computation of the internal hash part there may exist some inputs–output couples of the random permutation  $\Pi$  that have been defined previously. In this case, the final part is the sum of two identical random permutations under conditional distribution. Here we introduce an observation on the conditional distribution of the sum of two identical random permutations by Datta et al. [20].

**Lemma 1** ([20], Section 3). For any set  $Y$  with size  $d$  and a  $k$  tuple  $t^{[k]} := (t^1, \dots, t^k)$  of non zero  $n$  bit strings, let

$$\mathcal{H} = (h_0^i, h_1^i)_i : h_0^i \oplus h_1^i = t^i, \forall i \in [k], (h_0^i, h_1^i)_i \in (\mathbb{N} \setminus Y)^{(2k)}.$$

Then,  $|\mathcal{H}| \geq \frac{\mathbf{P}(N-d, 2k)}{N^k} (1 - \mu_2)$  where  $\mu_2 = \frac{kd^2 + 2dk^2 + 4k^3}{(N-d-2k)^2} / 3$ . Moreover, if  $d + 2k \leq \frac{N}{2}$ , then  $\mu_2 \leq \frac{4kd^2 + 8dk^2 + 6k^3}{N^2}$ .

Interested readers can refer to Section 3 of paper [20] for full proof. We define the event

$$\text{Bad} := \text{ZeroT} \vee \text{ECF} \vee \text{PCF1} \vee \text{PCF2} \vee \text{RCOLL},$$

then it follows that

$$\begin{aligned} \Pr[X_{id} \in \mathcal{T}_{\text{bad}}] &\leq \Pr[\text{ZeroT}] + \Pr[\text{ECF} | \overline{\text{ZeroT}}] + \Pr[\text{PCF1} | \overline{\text{ZeroT}}] \\ &\quad + \Pr[\text{PCF2} | \overline{\text{ZeroT}}] + \Pr[\text{RCOLL} | \overline{\text{ZeroT}}] \end{aligned} \quad (1)$$

At first we bound  $\Pr[\text{ZeroT}]$ . If  $\exists i \in [q]$  s.t.  $T^i = 0$ , then the bad flag ZeroT is set to 1. For a fixed  $i \in [q]$  it is obvious that  $\Pr[T^i = 0] = \frac{1}{N}$  because each  $T^i$  is chosen uniformly and independently in the ideal oracle. Therefore, we get

$$\Pr[\text{ZeroT}] = \Pr\left[\bigvee_{i=1}^q T^i = \mathbf{0}\right] \leq \sum_{i=1}^q \Pr[T^i = \mathbf{0}] = \frac{q}{N}. \quad (2)$$

Then we focus on  $\Pr[\text{ECF}|\overline{\text{ZeroT}}]$ . If the bad tag ECF is set to 1, at least one of the following cases happens: (1)  $v^i =_1 X_\alpha^j, w^i =_1 X_\beta^k$ ; (2)  $v^i =_1 X_\alpha^j, w^i = w^k$ ; (3)  $v^i = v^j, w^i =_1 X_\beta^k$ ; and (4)  $v^i = v^j, w^i = w^k$ . We denote these four cases as  $\text{ECF}_1, \text{ECF}_2, \text{ECF}_3$  and  $\text{ECF}_4$  in order. Note that  $v^i = v^j$  is equivalent to  $S_1^i =_1 S_1^j$  and  $w^i = w^j$  is equivalent to  $S_2^i =_1 S_2^j$  (line 4 in Figure 2 for the definition of  $S_1$  and  $S_2$ ).

Now we concentrate on the upper bound of  $\Pr[\text{ECF}_1|\overline{\text{ZeroT}}]$ . For different indices  $i, j \in [q]$  we define the set  $\text{NEQ}_{i,j} := \{\alpha \in [\min l_i, l_j] : M_\alpha^i \neq M_\alpha^j\} \cup \{\alpha : \min\{l_i, l_j\} + 1 \leq \alpha \leq \max\{l_i, l_j\}\}$ . It means that the set  $\text{NEQ}_{i,j}$  consists of all the index couples for which the two corresponding message blocks are not equal. Assume that  $\gamma = \min \text{NEQ}_{i,j}$  and  $l_i \leq l_j$  and it is straightforward that  $\gamma \leq l_j$ . The equations  $v^i =_1 X_\alpha^j$  and  $w^i =_1 X_\beta^k$  can be rewritten in matrix form with respect to variable  $Y$  as follows:

$$\begin{pmatrix} \mathbf{1} & b & \cdots \\ 2^{l_i-\gamma+1} & X_\beta^k \oplus b' & \cdots \end{pmatrix} \cdot \begin{pmatrix} Y_\gamma^i \\ \mathbf{1} \\ \vdots \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \mathbf{0} \end{pmatrix}$$

where  $b, b' \in \{0, 1\}$ . If  $b = 1$  and  $2^{l_i-\gamma+1} = X_\beta^k \oplus b'$  hold, then  $\text{rank} \geq 1$ , otherwise  $\text{rank} = 2$ . To analyze the solution of the matrix, another lemma [20] is introduced here.

**Lemma 2** ([20], Section 2.4). Assume that  $S \subseteq \mathbb{N}$  and the size of  $S$  is  $N'$ .  $Y_i$  is sampled from  $S$  in a without-replacement manner for  $1 \leq i \leq s$  and Let  $Y := (Y_1, \dots, Y_s)$ .  $A$  is a fixed  $b \times s$  matrix with rank  $n$ . For any  $b \times 1$  vector  $v$ , the following inequality holds.

$$\Pr\left[(A)_{b \times s} \cdot Y^T = v\right] \leq \frac{1}{\mathbf{P}(N' - s + n, n)}.$$

Interested readers can refer to Section 2 of paper [20] for full proof.

$$\begin{aligned} \Pr[\text{ECF}_1|\overline{\text{ZeroT}}] &\leq \sum_{i,j,k} \sum_{\alpha,\beta} \Pr[v^i =_1 X_\alpha^j \wedge w^i =_1 X_\beta^k|\overline{\text{ZeroT}}] \\ &\leq \sum_{i,j,k} \sum_{\alpha,\beta} \Pr[w^i =_1 X_\beta^k|\overline{\text{ZeroT}}] \cdot \Pr[v^i =_1 X_\alpha^j|\overline{\text{ZeroT}}] \\ &\leq \sum_{i,j,k} \sum_{\alpha,\beta} \frac{4}{N} \cdot \frac{4}{N} \\ &\leq \frac{16q\sigma^2}{N^2} \end{aligned}$$

$\Pr[\text{ECF}_2], \Pr[\text{ECF}_3]$  and  $\Pr[\text{ECF}_4]$  can be proven in a similar analysis:

$$\begin{aligned} \Pr[\text{ECF}_2|\overline{\text{ZeroT}}] &\leq \frac{16q\sigma^2}{N^2} \\ \Pr[\text{ECF}_3|\overline{\text{ZeroT}}] &\leq \frac{16q\sigma^2}{N^2} \\ \Pr[\text{ECF}_4|\overline{\text{ZeroT}}] &\leq \frac{16q\sigma^2}{N^2} \end{aligned}$$

In total, we have

$$\Pr[\text{ECF}|\overline{\text{ZeroT}}] \leq \frac{64q\sigma^2}{N^2} \quad (3)$$

Next, we bound  $\Pr[\text{PCF1}|\overline{\text{ZeroT}}]$ . The bad flag PCF1 occurs in Case A or Case B (refer to Figure 2). We separate event PCF1 into two disjointed events in terms of Case A or Case B. We define  $\text{PCF1}_1 := (v^i =_1 X_\alpha^j) \wedge (Y_\alpha^j \oplus Y_\beta^k = T^i)$  and  $\text{PCF1}_2 := (w^i =_1 X_\alpha^j) \wedge (Y_\alpha^j \oplus Y_\beta^k = T^i)$ .

Now we bound the probability of PCF1<sub>1</sub>. The equations  $v^i =_1 X_\alpha^j$  and  $Y_\alpha^j \oplus Y_\beta^k = T^i$  can be rewritten as:

$$\begin{pmatrix} \mathbf{1} & X_\alpha^j \oplus b & \cdots \\ \mathbf{0}/\mathbf{1} & T^i & \cdots \end{pmatrix} \cdot \begin{pmatrix} Y_\gamma^{l_i} \\ \mathbf{1} \\ \vdots \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \mathbf{0} \end{pmatrix}$$

where  $b \in \{0, 1\}$ . If  $X_\alpha^j \oplus b$  and  $Y_\gamma^{l_i} = Y_\alpha^j$  holds or  $X_\alpha^j \oplus b$  and  $Y_\gamma^{l_i} = Y_\beta^k$  holds, then  $\text{rank} \geq 1$ , otherwise  $\text{rank} = 2$ . Then we bound the probability in the following.

$$\begin{aligned} \Pr[\text{PCF1}_1|\overline{\text{ZeroT}}] &\leq \sum_{i,j,k} \sum_{\alpha,\beta} \Pr[v^i =_1 X_\alpha^j \wedge Y_\alpha^j \oplus Y_\beta^k = T^i|\overline{\text{ZeroT}}] \\ &= \sum_{i,j,k} \sum_{\alpha,\beta} \Pr[v^i =_1 X_\alpha^j|\overline{\text{ZeroT}}] \cdot \Pr[Y_\alpha^j \oplus Y_\beta^k = T^i|v^i =_1 X_\alpha^j \wedge \overline{\text{ZeroT}}] \\ &\leq \sum_{i,j,k} \sum_{\alpha,\beta} \frac{4}{N} \cdot \frac{2}{N} \\ &\leq \frac{8q\sigma^2}{N^2} \end{aligned}$$

$\Pr[\text{PCF1}_2]$  can be proven in a similar analysis:

$$\Pr[\text{PCF1}_2|\overline{\text{ZeroT}}] \leq \frac{16q\sigma^2}{N^2}$$

To sum up, we can obtain the following result

$$\Pr[\text{PCF1}|\overline{\text{ZeroT}}] \leq \frac{32q\sigma^2}{N^2} \quad (4)$$

Next we concentrate on  $\Pr[\text{PCF2}|\overline{\text{ZeroT}}]$ . The bad flag PCF2 occurs in Case A or Case B (refer to Figure 2). We separate event PCF2 into three disjointed events. We define  $\text{PCF2}_1 := (v^i =_1 X_\alpha^j) \wedge (v^k =_1 X_\beta^l) \wedge (Y_\alpha^j \oplus Y_\beta^l = T^i \oplus T^k)$ ,  $\text{PCF2}_2 := (v^i =_1 X_\alpha^j) \wedge (w^k =_1 X_\beta^l) \wedge (Y_\alpha^j \oplus Y_\beta^l = T^i \oplus T^k)$  and  $\text{PCF2}_3 := (w^i =_1 X_\alpha^j) \wedge (w^k =_1 X_\beta^l) \wedge (Y_\alpha^j \oplus Y_\beta^l = T^i \oplus T^k)$ .

To obtain a good bound, we introduce a property [20].

**Property 1** ([20], Appendix B).  $M^i$  and  $M^j$  are two different messages. On condition that  $\sigma \leq \frac{N}{2}$  the following inequalities hold.

$$(a) \Pr[v^i =_1 v^j \wedge \overline{\text{ZeroT}}] \leq \frac{4(\max\{l_i, l_j\} + 1)}{N}, (b) \Pr[w^i =_1 w^j \wedge \overline{\text{ZeroT}}] \leq \frac{4}{N}.$$

Interested readers can refer to Appendix B of paper [20] for full proof.



Firstly, we bound the probability of  $\Pr[\text{PCF2}_1|\overline{\text{ZeroT}}]$ . We analyze it by whether the condition  $T_i$  equals  $T^k$  or not. If  $T_i = T^k$ , then  $Y_\alpha^j = Y_\beta^l$ . Because  $Y$ 's are the outputs of a permutation, we obtain that  $X_\alpha^j = X_\beta^l$ . Furthermore,  $v^i = v^k$ . Therefore,

$$\begin{aligned} \Pr[\text{PCF2}_1|\overline{\text{ZeroT}} \wedge (T^i = T^k)] &= \Pr[v^i = v^k|\overline{\text{ZeroT}}] \\ &\leq \frac{4(\max\{l_i, l_j\} + 1)}{N} \\ &\leq \frac{4\sigma}{N} \end{aligned}$$

The first inequality is deduced from the property.

Furthermore, when  $T^i \neq T^k$ , the three included events  $(v^i =_1 X_\alpha^j) \wedge (v^k =_1 X_\beta^l) \wedge (Y_\alpha^j \oplus Y_\beta^l = T^i \oplus T^k)$  of  $\text{PCF2}_1$  can be written as the following matrix equality with respect to variable  $Y$ :

$$\underbrace{\begin{pmatrix} \mathbf{1} & \mathbf{0}/\mathbf{1} & X_\alpha^j \oplus b & \dots \\ \mathbf{0} & \mathbf{1} & X_\beta^l \oplus b' & \dots \\ \mathbf{0}/\mathbf{1} & \mathbf{1} & T^i \oplus T^j & \dots \end{pmatrix}}_A \cdot \begin{pmatrix} Y_\alpha^j \\ Y_\beta^l \\ \mathbf{1} \\ \vdots \end{pmatrix} = \begin{pmatrix} \mathbf{0} \\ \mathbf{0} \\ \mathbf{0} \end{pmatrix}$$

where  $b \in \{0, 1\}$ . Define event  $E := (X_\alpha^j \oplus b \oplus T^i \oplus T^k = 0)$ . If  $E$  holds and  $(A[1][2], A[3][1])$  equals to  $(1, 1)$  simultaneously, then  $\text{rank}(A) \geq 2$ , otherwise  $\text{rank}(A) = 3$ . Therefore,

$$\begin{aligned} \Pr[\text{PCF2}_1|\overline{\text{ZeroT}} \wedge (T^i \neq T^k)] &\leq \Pr[\text{PCF2}_1|\overline{B} \wedge \overline{\text{ZeroT}} \wedge (T^i \neq T^k)] + \\ &\Pr[\text{PCF2}_1|B \wedge \overline{\text{ZeroT}} \wedge (T^i \neq T^k)] \cdot \Pr[B|(T^i \neq T^k)] \\ &\leq \sum_{i,j,k,l} \sum_{\alpha,\beta} \frac{49}{N^3} \leq \frac{49q^2\sigma^2}{N^3} \end{aligned}$$

Therefore, we can obtain

$$\Pr[\text{PCF2}_1|\overline{\text{ZeroT}}] \leq \frac{49q^2\sigma^2}{N^3} + \frac{4\sigma}{N}.$$

$\Pr[\text{PCF2}_2]$  and  $\Pr[\text{PCF3}]$  can be proven in a similar analysis:

$$\begin{aligned} \Pr[\text{PCF2}_2|\overline{\text{ZeroT}}] &\leq \frac{49q^2\sigma^2}{N^3} + \frac{\sigma}{N} \\ \Pr[\text{PCF2}_3|\overline{\text{ZeroT}}] &\leq \frac{49q^2\sigma^2}{N^3} + \frac{2\sigma}{N} \end{aligned}$$

In total, we have

$$\Pr[\text{PCF2}|\overline{\text{ZeroT}}] \leq \frac{147q^2\sigma^2}{N^3} + \frac{7\sigma}{N}. \tag{5}$$

Finally we analyze the bounding of  $\Pr[\text{RCOLL}|\overline{\text{ZeroT}}]$ . The bad flag  $\text{RCOLL}$  occurs in Case C or Case D (refer to Figure 2). We separate  $\text{RCOLL}$  into  $\text{RCOLL}_1$  and  $\text{RCOLL}_2$  and define  $\text{RCOLL}_1 := (v^i =_1 v^j) \wedge (\hat{w}^i \in \text{Ran}(\mathcal{L}_2))$  and  $\text{RCOLL}_2 := (w^i =_1 w^j) \wedge (\hat{v}^i \in \text{Ran}(\mathcal{L}_2))$ .

$$\begin{aligned}
\Pr[\text{RCOLL}_1|\overline{\text{ZeroT}}] &= \sum_{i,j} \Pr[v^i =_1 v^j \wedge \hat{w}^i \in \text{Ran}(\mathcal{L}_2)|\overline{\text{ZeroT}}] \\
&= \sum_{i,j} \Pr[v^i =_1 v^j|\overline{\text{ZeroT}}] \cdot \Pr[\hat{w}^i \in \text{Ran}(\mathcal{L}_2)] \\
&\stackrel{*}{\leq} \sum_{i,j} \frac{2(\max\{l_i, l_j\} + 1)}{N} \cdot \frac{2q + \eta}{N} \\
&\leq \frac{6\sigma}{N}
\end{aligned}$$

Because the number of elements in  $\text{Ran}(\mathcal{L}_2)$  is at most  $2q + \eta$ , the inequality (\*) holds from the property. The last inequality holds owing to  $q \leq \sigma \leq N^2$ . Similarly one can show

$$\Pr[\text{RCOLL}_2|\overline{\text{ZeroT}}] \leq \frac{3\sigma}{N}$$

So we can obtain

$$\Pr[\text{RCOLL}|\overline{\text{ZeroT}}] \leq \frac{9\sigma}{N} \quad (6)$$

From inequalities (1)–(6), we can obtain

$$\Pr[X_{id} \in \mathcal{T}_{bad}] \leq \frac{147q^2\sigma^2}{N^3} + \frac{96q\sigma^2}{N^2} + \frac{16\sigma}{N} + \frac{q}{N} \quad (7)$$

#### 4.3. Analysis of Good Transcripts

Having defined bad events and computed the upper bound of the probability of each bad transcript in the ideal world, it remains to lower bound  $\Pr[X_{re} = \tau] / \Pr[X_{id} = \tau]$  for a good transcript  $\tau$ .

Firstly, we discuss in an ideal oracle what properties a good transcript have. For each  $i \in \mathcal{F}$  (line 10 of Figure 2), both  $v^i$  and  $w^i$  are fresh; therefore, it is the same case with the corresponding  $\hat{v}^i$  and  $\hat{w}^i$ . As ECF is not set to one, for each  $i \notin \mathcal{F}$  either  $\hat{v}^i$  or  $\hat{w}^i$  is fresh (but not both). Assume the size of  $\mathcal{F}$  is  $f$ , then there are  $q - f$  non-fresh message blocks and  $q + f$  fresh message blocks.

Denote  $\mathcal{F}'_v$  as the set of all the indices  $i$  s.t.  $v^i$  is in collision with some input of the hash computation and  $\mathcal{F}'_w$  is defined in a similar way. Then we define an equivalence relation  $\sim_v$  on  $\mathcal{F}_v := [q] \setminus (\mathcal{F}'_v \cup \mathcal{F})$  (line 6 of Figure 2) as  $i \sim_v j$  if  $v_i = v_j$ . Also the equivalence relation  $i \sim_w j$  on  $\mathcal{F}_w := [q] \setminus (\mathcal{F}'_w \cup \mathcal{F})$  is defined similarly. Here, we would like to point out that we cannot have  $v_j = w_j$  because we have applied domain-separation technique by setting the most significant bit as 0 and 1, respectively.  $\sim_v$  and  $\sim_w$  are equivalence relations on  $\mathcal{F}_v$  and  $\mathcal{F}_w$ , respectively. We partition the set  $\mathcal{F}_v$  as  $C_1 \sqcup \dots \sqcup C_t$  where each  $C_j$  is a subset of  $\mathcal{F}_v$  and the set  $\mathcal{F}_w$  as  $C'_1 \sqcup \dots \sqcup C'_t$  where  $C'_j$  is a subset of  $\mathcal{F}_w$ . The equivalence class  $C_j$  is called “the  $v$ -class” and  $C'_j$  “the  $w$ -class”. We point that each part contains at least two elements. Let  $c_j = \min C_j$  be the minimum value of partition  $C_j$  and so is  $c'_j = \min C'_j$ . So, when  $i = c_j$  or  $i = c'_j$  for some  $j \in [t]$  or  $j' \in [t']$ , we sample the output  $\mathcal{L}_2(\cdot)$  (Case C or Case D, respectively in Figure 2), which dominates the outputs for each element with respect to the corresponding equivalent class  $C_j$  or  $C'_{j'}$ , respectively.

Upon the above analysis, we can obtain that different elements in tuple  $(v^{[q]}, w^{[q]})$  have different corresponding elements in  $(\hat{v}^{[q]}, \hat{w}^{[q]})$  for a good transcript. Hence there exists a permutation  $\Pi$  such that the two tuples  $(v^{[q]}, w^{[q]})$  and  $(\hat{v}^{[q]}, \hat{w}^{[q]})$  are part of its inputs and outputs, respectively.

**Lemma 3.** Assuming that  $\tau = (M^{[q]}, T^{[q]}, X, Y, \hat{v}^{[q]}, \hat{w}^{[q]})$  is a good transcript, we can obtain

$$\frac{\Pr[X_{re} = \tau]}{\Pr[X_{id} = \tau]} \geq 1 - \frac{18q\sigma^2}{N^2} \quad (8)$$

**Proof.** Define a set  $\mathcal{I} = \mathcal{F} \cup \mathcal{F}_v \cup \mathcal{F}_w$ . In addition, assume that the size of  $\mathcal{L}_1$  is  $\eta$ .

$$\begin{aligned}
 \Pr[X_{id} = \tau] &= \Pr[T^{[q]} \wedge \mathcal{L}_1(X_j^i) = Y_j^i \wedge \mathcal{L}_2(v^{i'}) = \hat{v}^{i'} \wedge \mathcal{L}_2(w^{i'}) = \hat{w}^{i'}, \forall i' \in \mathcal{I}] \\
 &= \frac{1}{N^q} \times \Pr[\underbrace{\mathcal{L}_1(X_j^i) = Y_j^i}_{B1} \wedge \underbrace{\mathcal{L}_2(v^{i'}) = \hat{v}^{i'}}_{B2} \wedge \underbrace{\mathcal{L}_2(w^{i'}) = \hat{w}^{i'}}_{B3}, \forall i' \in \mathcal{I}] \\
 &= \frac{1}{N^q} \times \Pr[B1] \times \Pr[B2 \wedge B3|B1] \\
 &= \frac{1}{N^q} \times \frac{1}{\mathbf{P}(N, \eta)} \times \Pr[B2 \wedge B3|B1] \tag{9}
 \end{aligned}$$

Now we focus on the item  $\Pr[B2 \wedge B3|B1]$ .

$$\begin{aligned}
 \Pr[B2 \wedge B3|B1] &= \Pr[\underbrace{B2 \wedge B3, \forall i' \in \mathcal{I} \setminus \mathcal{F}}_{B4} | B1] \times \Pr[B2 \wedge B3, \forall i' \in \mathcal{F} | B1 \wedge B4]. \\
 &= \frac{1}{\mathbf{P}(N - (2f + \eta), t + t')} \times \Pr[B2 \wedge B3, \forall i' \in \mathcal{F} | B1 \wedge B4] \tag{10}
 \end{aligned}$$

Assuming that  $\eta + 2f \leq \frac{N}{2}$ ,  $\eta \leq \sigma$  and  $f \leq q \leq \sigma$ , with Lemma 1 we have

$$\begin{aligned}
 \Pr[B2 \wedge B3, \forall i' \in \mathcal{F} | B1 \wedge B4] &\leq \frac{N^f}{\mathbf{P}(N - \eta, 2f) \times \left(1 - \frac{4f\eta^2 + 8f^2\eta + 6f^3}{N^2}\right)} \\
 &\leq \frac{N^f}{\mathbf{P}(N - \eta, 2f) \times \left(1 - \frac{18q\sigma^2}{N^2}\right)}. \tag{11}
 \end{aligned}$$

Following (9)–(11), we can obtain

$$\Pr[X_{id} = \tau] \leq \frac{1}{N^q} \times \frac{1}{\mathbf{P}(N, \eta)} \times \frac{1}{\mathbf{P}(N - (2f + \eta), t + t')} \times \frac{N^f}{\mathbf{P}(N - \eta, 2f) \times \left(1 - \frac{18q\sigma^2}{N^2}\right)} \tag{12}$$

Next, for a good transcript  $\tau$  the interpolation probability in the real world is computed.

$$\Pr[X_{re} = \tau] = \frac{1}{P(N, \eta)} \times \frac{1}{P(N - \eta, t + t' + q + f)} \tag{13}$$

Following the Equations (12) and (13), we have that

$$\begin{aligned}
 \frac{\Pr[X_{re} = \tau]}{\Pr[X_{id} = \tau]} &\geq \frac{N^q \times P(N - (2f + \eta), t + t') \times P(N - \eta, 2f) \times \left(1 - \frac{18q\sigma^2}{N^2}\right)}{P(N - \eta, t + t' + q + f) \times N^f} \\
 &= \frac{N^{q-f}}{P(N - (t + t' + q + 2f), q - f)} \times \left(1 - \frac{18q\sigma^2}{N^2}\right) \\
 &\geq 1 - \frac{18q\sigma^2}{N^2} \tag{14}
 \end{aligned}$$

Finally, by applying the H-coefficient technique in Section 2.3 with the Equations (7) and (14), we conclude the proof for Theorem 1.  $\square$

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Conflicts of Interest:** The author declares no conflict of interest.

## References

1. Bellare, M.; Kilian, J.; Rogaway, P. The Security of the Cipher Block Chaining Message Authentication Code. *J. Comput. Syst. Sci.* **2000**, *61*, 362–399. [[CrossRef](#)]
2. Black, J.; Rogaway, P. A Block-Cipher Mode of Operation for Parallelizable Message Authentication. In *Advances in Cryptology—EUROCRYPT 2002, Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, 28 April–2 May 2002, Proceedings*; Knudsen, L.R., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2002; Volume 2332, pp. 384–397. [[CrossRef](#)]
3. Iwata, T.; Kurosawa, K. OMAC: One-Key CBC MAC. In *Fast Software Encryption, 10th International Workshop, FSE 2003, Lund, Sweden, 24–26 February 2003, Revised Papers*; Johansson, T., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2887, pp. 129–153. [[CrossRef](#)]
4. Luykx, A.; Preneel, B.; Tischhauser, E.; Yasuda, K. A MAC Mode for Lightweight Block Ciphers. In *Fast Software Encryption—23rd International Conference, FSE 2016, Bochum, Germany, 20–23 March 2016, Revised Selected Papers*; Peyrin, T., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9783, pp. 43–59. [[CrossRef](#)]
5. Bogdanov, A.; Knudsen, L.R.; Leander, G.; Paar, C.; Poschmann, A.; Robshaw, M.J.B.; Seurin, Y.; Vikkelsoe, C. PRESENT: An Ultra-Lightweight Block Cipher. In *Cryptographic Hardware and Embedded Systems—CHES 2007, 9th International Workshop, Vienna, Austria, 10–13 September 2007, Proceedings*; Paillier, P., Verbauwhede, I., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4727, pp. 450–466. [[CrossRef](#)]
6. Guo, J.; Peyrin, T.; Poschmann, A.; Robshaw, M.J.B. The LED Block Cipher. In *Cryptographic Hardware and Embedded Systems—CHES 2011—13th International Workshop, Nara, Japan, 28 September–1 October 2011, Proceedings*; Preneel, B., Takagi, T., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6917, pp. 326–341. [[CrossRef](#)]
7. 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 *Cryptographic Hardware and Embedded Systems—CHES 2017—19th International Conference, Taipei, Taiwan, 25–28 September 2017, Proceedings*; Fischer, W., Homma, N., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2017; Volume 10529, pp. 321–345. [[CrossRef](#)]
8. Yasuda, K. The Sum of CBC MACs Is a Secure PRF. In *Topics in Cryptology—CT-RSA 2010, The Cryptographers’ Track at the RSA Conference 2010, San Francisco, CA, USA, 1–5 March 2010, Proceedings*; Pieprzyk, J., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2010; Volume 5985, pp. 366–381. [[CrossRef](#)]
9. Yasuda, K. A New Variant of PMAC: Beyond the Birthday Bound. In *Advances in Cryptology—CRYPTO 2011—31st Annual Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2011, Proceedings*; Rogaway, P., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6841, pp. 596–609. [[CrossRef](#)]
10. Zhang, L.; Wu, W.; Sui, H.; Wang, P. 3kf9: Enhancing 3GPP-MAC beyond the Birthday Bound. In *Advances in Cryptology—ASIACRYPT 2012—18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, 2–6 December 2012, Proceedings*; Wang, X., Sako, K., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7658, pp. 296–312. [[CrossRef](#)]
11. Bernstein, D.J. How to Stretch Random Functions: The Security of Protected Counter Sums. *J. Cryptol.* **1999**, *12*, 185–192. [[CrossRef](#)]
12. Bellare, M.; Guérin, R.; Rogaway, P. XOR MACs: New Methods for Message Authentication Using Finite Pseudorandom Functions. In *Advances in Cryptology—CRYPTO ’95, 15th Annual International Cryptology Conference, Santa Barbara, CA, USA, 27–31 August 1995, Proceedings*; Coppersmith, D., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1995; Volume 963, pp. 15–28. [[CrossRef](#)]
13. Naito, Y. Blockcipher-Based MACs: Beyond the Birthday Bound Without Message Length. In *Advances in Cryptology—ASIACRYPT 2017—23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, 3–7 December 2017, Proceedings, Part III*; Takagi, T., Peyrin, T., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2017; Volume 10626, pp. 446–470. [[CrossRef](#)]
14. Datta, N.; Dutta, A.; Nandi, M.; Paul, G. Double-block Hash-then-Sum: A Paradigm for Constructing BBB Secure PRF. *IACR Trans. Symmetric Cryptol.* **2018**, *2018*, 36–92. [[CrossRef](#)]
15. Leurent, G.; Nandi, M.; Sibleyras, F. Generic Attacks Against Beyond-Birthday-Bound MACs. In *Advances in Cryptology—CRYPTO 2018—38th Annual International Cryptology Conference, Santa Barbara, CA, USA, 19–23 August 2018, Proceedings, Part I*; Shacham, H., Boldyreva, A., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2018; Volume 10991, pp. 306–336. [[CrossRef](#)]
16. Kim, S.; Lee, B.; Lee, J. Tight Security Bounds for Double-Block Hash-then-Sum MACs. In *Advances in Cryptology—EUROCRYPT 2020—39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, 10–14 May 2020, Proceedings, Part I*; Canteaut, A., Ishai, Y., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2020; Volume 12105, pp. 435–465. [[CrossRef](#)]
17. Naito, Y. Improved Security Bound of LightMAC\_Plus and Its Single-Key Variant. In *Topics in Cryptology—CT-RSA 2018—The Cryptographers’ Track at the RSA Conference 2018, San Francisco, CA, USA, 16–20 April 2018, Proceedings*; Smart, N.P., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2018; Volume 10808, pp. 300–318. [[CrossRef](#)]

18. Patarin, J. The “Coefficients H” Technique. In *Selected Areas in Cryptography, 15th International Workshop, SAC 2008, Sackville, NB, Canada, 14–15 August Revised Selected Papers*; Avanzi, R.M., Keliher, L., Sica, F., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5381, pp. 328–345. [[CrossRef](#)]
19. Chen, S.; Steinberger, J.P. Tight Security Bounds for Key-Alternating Ciphers. In *Advances in Cryptology—EUROCRYPT 2014—33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, 11–15 May 2014. Proceedings*; Nguyen, P.Q., Oswald, E., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8441, pp. 327–350. [[CrossRef](#)]
20. Datta, N.; Dutta, A.; Nandi, M.; Paul, G.; Zhang, L. Single Key Variant of PMAC\_Plus. *IACR Trans. Symmetric Cryptol.* **2017**, *2017*, 268–305. [[CrossRef](#)]