

Nomenclature

\oplus	Bitwise exclusive-xor operation(XOR)
(M,T)	Message M and its tag T
$\{0,1\}^n$	Set of all n-bit binary strings
Adv_{F1}^{F0}	The probability for an adversary to distinguish between two functions F0 and F1
Block Length	The number of bits of a block
$E_k(M)$	Encrypt input M with secret key k
$F_k(M)$	Function F processing input M with secret information k
Forgery_{MAC}	The probability that $\text{Forgery}(MAC, A)=1$ for an adversary A and a MAC scheme
$\text{Forgery}(MAC, A)$	Forgery experiment on a MAC scheme with the adversary A. Return 1 if A succeed a forgery attack otherwise 0
$\text{GF-mult}(A,B)$	Galois Field multiplication with A and B
$\text{Len}(M)$	The block length of block M
MAC	Message Authentication Code: A short message block generated with message protected. MAC is concatenated to the rightmost of the message in transmission
$\text{Pr}[A]$	The probability that event A happens
PRF	Pseudo-random Function
PRP	Pseudo-random Permutation
Tag	The output short block of a MAC generation scheme
$\text{TG}(M, \dots)$	A MAC Scheme processing the message M with secret information in the arguments list
Tom	A concatenated to the leftmost of B
UF-CMA	Unforgeability under adaptive Chosen Message Attack
$\text{VF}(M,T, \dots)$	Verify the message M and tag T with the secret information in the arguments list. Return 1 if $\text{TG}(M, \dots) = T$ and 0 if not.

1 Notations and Definitions

In this part we firstly depict the notations of symbols used to describe Cost-Effective Tag Design(CETD) and the MAC scheme adopted, CETD-MAC. Then we present the security definition of MAC schemes in computational scenario.

1.1 Notations of Symbols

Let $\{0,1\}^n$ be the set of all n-bit binary strings. The set of all binary string is expressed as $\{0,1\}^*$. For a string $X \in \{0,1\}^n$, $|X|$ is its length in bits, and $|X|_l = \lceil |X|/l \rceil$ is the length of X in l-bit blocks. Let 0^l and 1^l denote bit strings of all zeros and all ones. For a bit string X and an integer l that $|X| \geq l$, $\text{msb}_l(X)$ denotes the most significant l bits(left most l bits) of X and $\text{lsb}_l(X)$ for least significant l bits(right most l bits) of X. For two bit string X and Y, we denote $X\|Y$ or XY as the their concatenation. For bit string X whose length in bits is multiple of integer l, we denote X parted into l-bit sub-strings as $X = (X[1]X[2] \dots X[n])_l$, where $X[1], X[2], \dots, X[n] \in \{0,1\}^l$. The number of bits in a string of X is denoted as $\text{len}(X)$.

The block cipher encryption of a string X with a secret key K is denoted as $E_K(X)$. $E_K(X)$ expresses the String mapping of $\{0,1\}^n \rightarrow \{0,1\}^n$ where n is the $\text{len}(X)$ and $\text{len}(\text{output})$.

1.2 Security Definition in Computational Scenario

Threat Model of Tag Designs The attacks discussed in this article mainly situated on the probing and tampering the data transferred between chip and external memory. In this scenario, the adversary can conduct types of attacks on the (ciphertext, tag) pair stored on the external memory or in the transformation between chip and memory. We call these two types of integrity attack content modification attack and copy-then-replay attack.

When conducting a content modification attack, then adversary modifies the content of a (ciphertext, tag) pair. At least one of ciphertext and tag are distinct to the original one sent from the chip. When the chip reads the modified pair (C1, T1), this pair is verified by $\text{VF}(C1, T1, \dots)$. If $\text{VF}(C1, T1, \dots)=1$, then the modified pair passes and the content modifying attack succeeds.

For a copy-then-replay attack, we make the following denotion first:

- A_{origin} : The address of the external memory frame M attacked
- A_{copy} : The address of the external memory frame M1 which is copied by the adversary as the fake frame
- TS_{origin} : The generation time stamp of the external memory frame M attacked
- TS_{copy} : The generation time stamp of the external memory frame M2. M2 and M has same address while TS_{M2} is previous of TS_M

During a copy-then-replay attack on a memory frame M whoes address is A_{origin} and time stamp is TS_{origin} , the adversary A replace M with a copy. This copy can be a frame from other address A_{copy} or one at same address but copied at an old time stamp TS_{copy} . The copy is a valid pair from the chip. When the chip reads the modified frame, the fake pair(C2, T2) is verified by $\text{VF}(C2, T2, \dots)$ and the copying-then-replying attack succeeds if $\text{VF}(C2, T2, \dots)=1$.

If the fake pair from the adversary passes the verification, the integrity of the data is broken. To defend content modification attack, the MAC scheme should ensure that when the secret information used in tag generation collides for two distinct input data, the related two tags should have low probability to be identical. For copying-then-replaying attack, identical input data should have low probability to lead to tag collision if the secret information used in tag generation are distinct.

Implementation Security of Cost-Effective Tag Design As the MAC scheme adopted in cost-effective tag design(CETD) is a stateful scheme, the input of nonce generation should be distinct for any two write-read period. This is the security requirement in implementation level.

In CETD tag design, a input of nonce generation is a tuple(addr,ctr, rnd). The meaning of each element in the tuple is listed below:

- Addr: The address of ciphertext
- Ctr: A incrementing counter
- Rnd: A random number

Security Analysis Model In our security analysis of CETD-MAC scheme, the adversary A has access to the tag generation scheme and verification scheme. A can input chosen ciphertexts to the tag generation scheme and determine whether the nonce for his chosen ciphertexts are fixed or not. He can acquire the value of the tag for each his chosen ciphertext while cannot access the value of the related nonce. After analyzing several valid ciphertext-tag pairs, A sends his fake pair (C_{fake}, T_{fake}) to the verification scheme. The verification scheme generates the tag T of C_{fake} and the fake pair passes the verification if T is identical to T_{fake} . Our security analysis on CETD-MAC is modeled like this:

- For content-modification attack, the adversary A fixes the nonce and inputs distinct ciphertexts to the tag generation scheme.
- For copying-then-replaying attack, the value of ciphertexts are fixed to a value C chosen by A. A inputs C continually and as the tag generation scheme to maintain the nonce distinct for each input.

After several rounds of inputting, the adversary analyses the value of tags for his chosen inputs then sends his fake pair (C_{fake}, T_{fake}) to the verification scheme.

Chosen Message Attack In [], the authors provided a security analysis of CETD-MAC scheme. The adversary is assumed to conduct brute force attack in which he randomly chooses a ciphertext C and a nonce N. Then he keeps C and N fixed and tries different tags until a tag T can pass the verification with C and N. All the tags tried until passing the verification form a set named tag exploration space. The author assumed a MAC to be secure if the following conditions are met:

- The size of tag exploration space is large
- If the ciphertext and nonce is randomly generated and unaccessible to the adversary, the probability to pass the verification for each tag in the tag exploration space is identical

Based the above two conditions, the author assume CETD-MAC is secure.

Goldwasser et al. introduced the concept of unforgeability of chosen message attack in [1]. The adversary can select numbers of valid ciphertext-tag pairs, observe the relationship between each ciphertext and its tag, then send a fake ciphertext-tag pair to the verification stage based on the observation. The adversary A1 conducting chosen-message attack is more strategical compare with the one A2 for brute-force attack in content modification scenario, which means A1 can try less number of ciphertext-tag pairs to pass the verification. For instance, if there is a type of relationship between ciphertext and tag for a MAC scheme, A1 will realise this relationship and conduct two types of attack with high probability of passing: just modifying ciphertext from C1 to C2 and C2 has high probability to generate same tag T1; or send new pair (C2,T2) to the verification where C2 and T2 meet the relationship. In A1's eyes, for given ciphertext C and a unknown nonce N, the tags in the tag domain has different probability to pass the verification while the probability is identical to A2.

In this article, we assume the adversary can choose the ciphertext in both content modification and copy-then-replay attack. The adversary aims to find groups of inputs that the two inputs from same group has probability of tag collision that is much larger than $1/2^n$, where n is $\text{Len}(\text{tag})$.

Content Modification Scenario

Copy-then-Replay Scenario Our security definition of MAC schemes under replay attack follows the definition chosen-message attack. An adversary is given access to a tag generation black-box(named oracle) and a message-tag pair verification oracle. The encryption key is maintained unchanged while the nonce value is updated for each calling of tag generation oracle no matter whether the value of input message collide with a value in old timestamp. Secret key and nonces are kept in trusted area and cannot be acquired by the adversary. The adversary can copy the message-tag pairs in old time stamp. When conducting the replay attack, the adversary replaces a memory frame containing a data-tag pair in new timestamp with a copy from his storage. The forgery advantage $F_{CETD-MAC}$ under replay attack is the probability that the adversary can get the verification oracle to accept the replace data-tag pair.

Assume the copy with old timestamp from the adversary is expressed as (M,T1) where M is the message and T1 is the corresponding tag, and the nonce of (M,T1) is denoted as N1. When applying M to the tag generation at a new time point, we mark the corresponding tag T2 and the nonce N2. If the adversary can succeed a replay attack, then T1 is identical to T2 regardless of the equality of N1 and N2. Then $F_{CETD-MAC}$ under replay attack can

be denoted as the probability $\Pr[T1 = T2 \mid \text{Message value is } M \ \& \ N1, N2 \text{ are randomly generated}]$.

According to the design of CETD-MAC, the tag can be expressed as $Y[1] \oplus Y[2] \oplus \dots \oplus Y[x]$, x is the number of input sub-blocks to CETD-MAC. If the following equation is met: $Y_1[1] \oplus Y_1[2] \dots \oplus Y_1[x] \oplus Y_2[1] \oplus Y_2[2] \dots \oplus Y_2[x] = 0$, where Y_1 blocks produce $T1$ and Y_2 blocks generate $T2$, then $T1$ is identical to $T2$. This equation indicates that the behaviour of block-level rotate shifting stage effect the probability of tag collision directly. For easy understanding, we firstly analyze the case that shuffle stage does not work under replay attack, which means $X_1[i]$ is identical to $X_2[i]$ for any $i \in [1, x]$. The analysis of effect from shuffle stage on X blocks follows then.

In replay attack, the adversary replace the memory frame written in new time point Time_2 with a copy from old time stamp Time_1 . The content in memory frame is a data-tag pair. To defend the replay attack, a tuple(address, counter, random number) is adopted as input to block cipher encryption to generate the nonce, which serves the control parameter for each stage in tag generation. The tuple is distinct for each data message. Assume the block cipher adopted behaves like PRF, the nonce under replay attack is random and distributed uniformly for each data message. To Cost-Effective Tag design, the security of integrity of data message replays on the security of CETD-MAC scheme.

2 CETD-MAC Definition

In this article, we name the MAC scheme adopted in Cost-Effective Tag Design[] CETD-MAC. We briefly depict the design of CETD-MAC scheme and related notations.

Definition of CETD-MAC Scheme CETD-MAC scheme can be expressed as $\text{tag} = \text{CETD-MAC}(M, \text{nonce-input})$. The input arguments of CETD-MAC are message M and a tuple named nonce-input. The tuple nonce-input is the concatenation of the memory address of M , a counter and a random number, denoted as $\text{nonce-input} = (\text{address} \parallel \text{counter} \parallel \text{random})$. The length of nonce-input, $\text{len}(\text{nonce-input})$, is identical to the length of input to block cipher $E_K(X)$. The output of CETD-MAC is named tag, whose length is optional. We use Sub-BLK-No to express the value of $\text{len}(M)/\text{len}(\text{tag})$. One preliminary of CETD-MAC is that Sub-BLK-No should be no less than 2 to assure that swapping stage can work and 0s will be concatenated to the leftmost of input message when Sub-BLK-No is not integer. The concept of CETD-MAC is expressed in Figure ??.

We follow the definition of CETD-MAC in [?].

- Message is splitted to sub-blocks each of whose length is tag length
- The first stage is several rounds of bit-segment swapping. For each round , two sub-blocks are randomly chosen. Introduce shuffle parameter $V[i]$

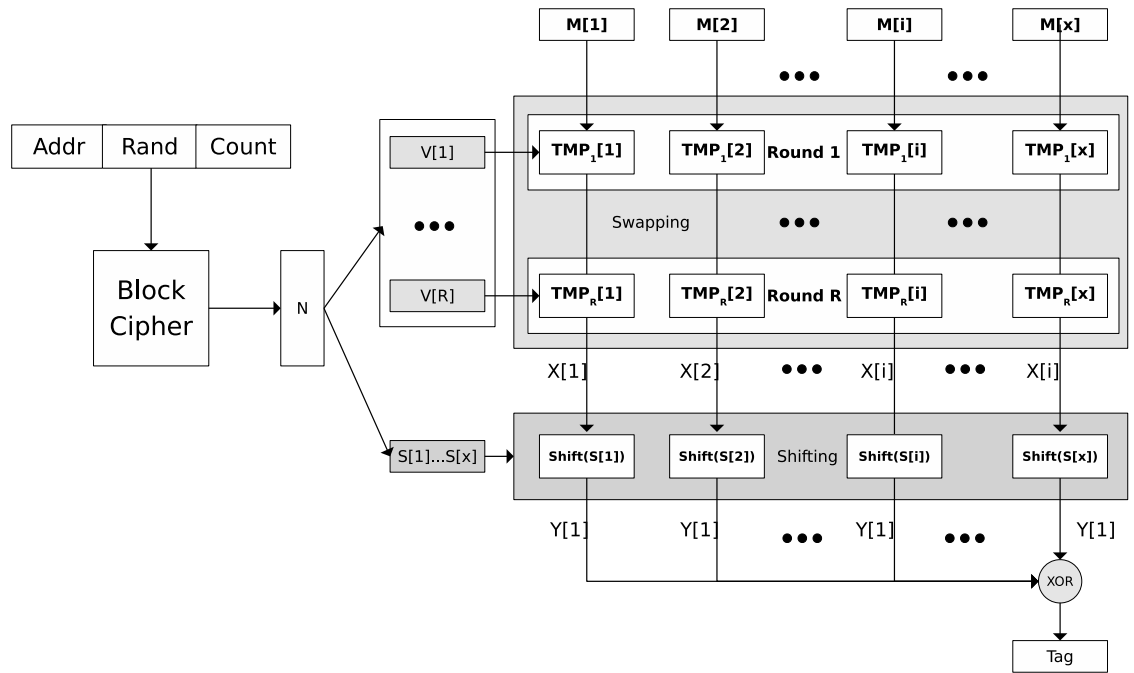


Figure 1: The CETD-MAC Scheme

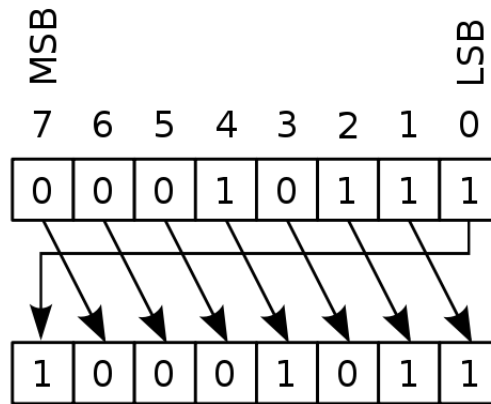


Figure 2: The Concept of Rotate Shifting(Right)

- The output sub-blocks from swapping stage, named X blocks, are sent to block-level rotate shifting stage. Each X block is rotate shifted for several bits. The concept of rotate shifting is expressed in Fig 2 Introduce shift parameter $S[i]$
- The output sub-blocks from shifting stage, named Y blocks, are XORed to form the final tag

As the nonce is generated by block cipher encryption E_K . Assume E_K performance like a ideal random value generator, for two distinct input nonce-input1 and nonce-input2, the corresponding nonce values N1 and N2 should be random and the probability that N1 is identical to N2 should be $1/2^n$, where n is $\text{len}(N1)$.

3 Security Analysis of CETD-MAC

In this section we analysis the security of cost-effective tag design. We firstly introduce our security evaluation model of tag design. This model splits the security analysis into two steps: scheme security and implementation security. We analysis

3.1 Computational Based Security Analysis of CETD-MAC

In this section we discuss the security of CETD-MAC under two tpyes of integrity attack. The adversary is assumed to know the length of ciphertext and tag on the memory frame he acquired. We prove that the probability that the fake pair passes the verification scheme under both two attacks is determined by the proportion of the 1s and 0s in the input ciphertexts and provide the equations quantifying this relationship. This fact indicates that the adversary can choose special ciphertext-tag pairs which have higher probability to pass the verification compared with other pairs.

3.1.1 Content Modification Attack Scenario

In the computational model based security analysis on MAC schemes, a secure MAC scheme should ensure that for any two input messages in the domain, the probability that their tags collide should be no more than an upper bound. This definition of secure MAC scheme is widely accepted and has been adopted in the security analysis of iterated MAC schemes such as CBC-MAC [1] and its variants [2], and parallel MAC schemes such as PMAC [3] and its variants[4]. This definition emphasizes that when the key used in the MAC scheme is unaccessible to the adversary, the adversary cannot find any relationship between a given tag and a given input message. In the eyes of the adversary, a given tag can be generated by any message in the input domain and for a given input message, its tag can be any one value in the tag range.

In this part we prove that for CETD-MAC, the input ciphertexts have relationship between their tags. For a given tag, the number of possible inputs is limited and can be computed based on the tag value. On the other hand, for a give input ciphertext, the number of possible tag value is also limited and can be computed based on the ciphertext value. This fact indicates that when modifying the ciphertext part C1 of a memory frame, the number of possible ciphertexts C2 to replace C1 is limited. On the other hand, the adversary can manifest the fake ciphertext-tag pair $C_{fake}-T_{fake}$ based on the relanship between a ciphertext and its tag quantified in thei part and win a much high probability to pass the verification stage compared with randomly choosing a ciphertext and a tag.

When conducting content modification attack, the adversary modifies the content of a memory frame from (C, T) to (C1, T1). When the verification stage VF read the modified (C1, T1) pair, VF computes C1's tag, marked as

T_{tmp} , using the nonce N which is also used in computing T . If T_{tmp} is identical to $T1$, then the content modification attack succeed. We can see that in content modification attack, for two pairs (C_{origin}, T_{origin}) and $(C2, T1)$, their nonce N and $N1$ are identical. To succeed the content modification attack, the adversary will choose the $C1$ that has high probability to get tag value T

Diffusion Operations Do Not Introduce New Bits In CETD-MAC scheme, the shuffle and shift stage relocate bits in the ciphertext to new index. Even though the new index of each bit in the ciphertext is unpredictable as the nonce is the output of a PRF and unaccessible to the adversary, it is certain the output of shift shuffle and shift stage contain same bits as the ciphertext. Assume ciphertext is consist of m blocks each of whose length is n bits, and there are totally k 1s in the $m*n$ bits in the ciphertext. The the output of shuffle and shift stage also have k 1s and $m*n - k$ 0s.

As mentioned before, the 0-1 proportion is maintained during the shuffle and shift operation. That means if two distinct ciphertext $C1$ and $C2$ have same proportion, marked as $k/m*n-k$, the 0-1 proportion in their corresponding shift outputs $Y1$ and $Y2$ is also $k/m*n-k$. If we fix a nonce and keep querying ciphertext with same 0-1 proportion, the outputs of shift stage can be regarded as a seg of $m*n$ bits messages with same 0-1 proportion but uncertain bit distribution. If a ciphertext has k 1s, then the distinct ciphertexts have k 1s form a set S_n^k and the set size is $\binom{n}{k}$, marked as C_n^k . The i th element in set S_n^k is marked as $C[i]$ and the tag of $C[i]$ is $T[i]$. We fix a nonce N for the set S_n^k and compute $T[1]$. We discuss possible distribution of k 1s in m Y blocks according to the value of k compared with $m*n$ to see the number of possible distinct values of $T1$.

Firstly, we assume k is no larger than n . When xoring Y blocks to generate $T[1]$, the j th bit of $T[1]$, marked as $T[1][j]$, is computed as $T[1][j] = Y1[1][j] \oplus Y1[2][j] \oplus Y1[m][j]$, where $Y1[i][j]$ is the j th bit in the i th Y block. We call the j th bit in all Y blocks a j th column. The j th bit of $T1$ is formed by xoring all the bits in the j th column of Y block. It is obvious that $T1$ can have at most k 1s and the number of distinct $T1$ with k 1s is $\binom{n}{k}$. In this case all the k 1s distribute in distinct k column. If we want new value of $T1$, we need to move one of 1 to another column. This relocation reduce the number of 1s in $T1$ from k to $k-2$, leading to $\binom{n}{k-2}$ new distinct values of $T1$. If we want more new values, we need to keep move 1s to another column like this way and each time of relocation reduce 2 1s in $T1$, which means the possible number of 1s in $T1$ can be $k, k-2, k-4, \dots, 0$ (if k is even) or 1 (if k is odd). Then we draw the following Theorem:

Theorem 3.1. *Assume a ciphertext consist of m n -bits blocks has k 1s and k is no larger than n , then the the number of possible distinct value of its tag when the nonce is unaccessible is compute with the equation: No of distinct tags is $\sum_{i=0}^{k/2} \binom{n}{k-2*i}$ if k is even or $\sum_{i=0}^{(k-1)/2} \binom{n}{k-2*i}$ if k is odd*

When k is identical to n or $n-1$, the number of distinct tags is 2^{n-1} .

If k is larger than n and no larger than $m^*(n-1)$, for any k in this domain, it is possible to generate a tag containing 0 to n 1s. That means for any $k \in [n, m^*(n-1)]$, the number of possible distinct tags for a ciphertext is 2^{n-1} .

When k is larger than $m^*(n-1)$, the way to compute number of possible distinct tags is similar to the case that k is no larger than n . In this case, the tag can have at most $n - (k \bmod n)$ 0s the value with less number of 0s can be acquired by overlapping 0s in one column. The number of possible distinct tag values can be computed with the following equation: No of distinct tags is $\sum_{i=0}^{(m*n-k)/2} \binom{n}{k-2*i}$ if k is even or $\sum_{i=0}^{(m*n-k+1)/2} \binom{n}{k-2*i}$ if k is odd

Forgery Attack on CETD-MAC in Content Modification Scenario In content modification attack, the adversary acquires a valid memory frame and try to modify the content. If the adversary knows the length of ciphertext and the tag, he will know the value of the ciphertext and the tag. According to the previous analysis on the relationship between bit proportion and possible tag values, the adversary can conduct the following two types of modification on the frame:

1. Select a new ciphertext that has T_{origin} in its possible tag domain. A better choice is to select a ciphertext with same number of 1s as the tag T_{origin}
2. Replace the frame with a new pair (C2, T2) that T2 is in the possible tag domain of C2

From Theorem ?? we know that if the number of 1s in $m*n$ bits is too large (more than $m^*(n-1)$) or too small (less than n), the possible tag domain size is small. This fact

3.1.2 Copy-then-Replay Attack Scenario

When conducting copy-then-replay, the adversary replace a valid memory frame with his stored copy of a frame from other address or same address but older time point. The probability that the adversary succeed the copy-then-replay attack is determined by the probability that for a fixed input C , the two tags $T1$ and $T2$ are identical when their nonce $N1$ and $N2$ are randomly generated.

As depicted in Section ??, the 0-1 proportion of a ciphertext is maintained to the output blocks (Y blocks) of shift stage. This fact means for a fixed input, the Y block set $Y1$ and $Y2$ for two randomly generated nonce $N1$ and $N2$ have same 0-1 proportion.

Forgery Attack on CETD-MAC in Copy-then-Replay Scenario As the probability that two tags collide when their inputs are identical and their nonce are randomly generated is determined by the 0-1 proportion of their inputs, the adversary can just attack the frame with the copy whose ciphertext has many 1s (more than $m^*(n-1)$) or few 1s (fewer than n). Two extreme case is all 0 and all 1 ciphertexts, no matter what nonce is adopted, their tags will always be 0.

3.2 Security Enhancement of CETD-MAC with Its Operations

In this part we try to enhance the security of CETD-MAC without introducing new operations or data. We analyze the functionality of each operation first and discuss whether it is necessary to maintain each operation in the new design.

3.2.1 Design Rationale of Original CETD-MAC Scheme

CETD-MAC scheme is consist of three stages: bit-segment shuffle with user chosen shuffle round, then cycle shift for each output block of shuffle stage with randomly chosen shift length and finally xor all output block of shift stage to the tag. It is insecure to construct with only one of the three stages.

XOR stage The xor operation is a common choice for parallel MAC schemes to convert an n-bits block to a n-bits tag. It has been analyzed by Bellare in [1] that it is insecure to construct a MAC scheme with xor operation only as simply swapping the order of two blocks in the input can lead to tag collision. The input blocks must be processed before sent to xor stage to ensure that simply changing the order of two input blocks in the input will change the input set of xor stage.

Cycle Shift Stage In original CETD-MAC scheme, cycle shift stage, short for shift stage, locates before the xor stage. For each input block of shift stage, the number of bits shifted is determined by the value of a nonce segment. Shift stage can defend the attacks such as changing the order of two input blocks as the adversary has no access to the nonce value and then can not predict the number of bits shifted of each block, then has no idea that changing the order of which two blocks lead to tag collision with high probability. However, it is still insecure to construct a MAC scheme by adopting shift stage then xor stage, as for some input blocks which are consist of one kind of patterns, shifting different number of bits can still lead to same output block. This fact means that reordering the blocks formed by a pattern have higher probability to lead to tag collision than other blocks. This fact is depicted in detail in Appendix ??.

Bit-Segment Shuffle Stage Shuffle stage swaps two bit-segments in each round. As the index and offset of swapping in each round is determined by the nonce, the adversary cannot predict which blocks participate the shuffle. One problem to use shuffle without shift is that if the number of blocks are large while the number of shuffle round is small, the number of blocks participating the shuffle is small. This fact is serious in copy-then-replay attack as majority of blocks may not participate shuffle and the content of these unshuffled blocks will be maintained until the next stage. If the operation linked to shuffle is the xor stage directly without shift stage, according to Equation ?? we can see that the probability of tag collision is determined by th

and the adversary can repeat some blocks in the input as he wish to enhance the collision probability of the output from shuffle. In the original CETD-MAC, the shift stage will help re-ordering the bits in the output blocks from shuffle stage to ensure that the input blocks of xor stage is hard for the adversary to predict.

Diffusion is insufficient to construct a secure MAC scheme We can see what shuffle and shift do is reordering the bits in the input message blocks. We give each input bit a index from 1 to $m \cdot n$. When the nonce is fixed and unknown, we are certain for two inputs M1 and M2 the bits with same index will be relocated to same new index. The adversary does not know the exact bit distribution of the input blocks to xor stage but he knows that the 0-1 proportion is same as the input of CETD-MAC. As depicted in Section ??, the odd-even property of the tag is identical to its input, and the number of possible distinct tag values can be predict based on the number of 1s in the input. When realized this fact, the adversary just needs to choose a tag value that has same odd-even property and the number of 1s is no more than $\min(n, k)$, there k is the number of 1s in the input.

Content Modification Scenario In content modification scenario, the adversary keeps modifying a memory frame in an address until the frame passes verification. The modification will be previous to the next write operation from the chip the same address.

Copy-then-Replay Scenario To eliminate this weakness, we need to add a operation to make sure that if the adversary does not know the value of the fixed nonce, he cannot predict the 0-1 proportion and bit distribution of the input blocks of xor stage.

No-linearity and Random Bit Injection In cite, R and J depicted the design rationale of each operation in Rij AES. Their should be three types of operations in a block cipher design serving as no-linearity, random-bit injection and diffusion. In original CETD-MAC scheme, both shuffle and shift operation achieve the diffusion, while no operation can inject random bits for each input and all the operation in the CETD-MAC is linear.

4 Security Improved CETD-MAC

We have shown that the original CETD-MAC cannot effectively defend two types of integrity attacks as the number of distinct tags is determined by the proportion of 1s and 0s. In this section, we propose several approaches to improve the security of CETD-MAC. Firstly we tried to utilize the nonce and the operation existing in the original CETD-MAC design and then prove the reason that this attempt cannot succeed. Then we proposed our rationale on improvement based on the instruction from [].

No-linearity and Random Bits Injection: Approaches in other schemes

Galois Field Multiplication As mentioned in Section ??, it is insufficient to use linear operation only to construct a secure MAC scheme. The reason is that linear operations can diffuse the bit distribution of the input while can not introduce new bits. On the other hand, the input and the output of linear operation has linear relationship and the adversary can find the relationship and conduct successful forgery attack since then without acquiring the nonce or the key.

We need to add non-linearity random bit injection operation. For the MAC schemes constructed with block cipher, such as CBC-MAC (and its variants) and PMAC (and its variants), the block cipher usually contains these two operations. R and J mentioned in [] the galois field multiplication and its inverse operation can serve as non-linearity operation. For example in Rij AES, the ByteSub provide non-linearity to the input by adopting the galois multiplication inverse to each input byte then affine transformation with a constant matrix to the input. Random bits that stored in a roundkey, which is acquired by expanding the encryption key, is injected to the input by xoring the roundkey with processed input.

In GMAC, the author utilized the galois field multiplication other than block cipher to process each input block serially. Each input block does galois field multiplication with H, which is acquired by encrypting constant 0 with a secret key. The output of multiplication is xored with the next input block to serve as the multiplicand for H. The advantage of multiplying each xored input block with H compared with calling the encryption function to the input block directly is that the non-linearity and random bit injection is combined to one round operation, which reduces the space cost and enhances the processing speed.

The application of GF multiplication in GMAC inspired us on the security optimization of original CETD-MAC scheme as for each ciphertext to be processed, a nonce is generated with block cipher. The nonce or its segment can serve as the H in the GF multiplication in GMAC.

4.1 Improved CETD-MAC with higher security level

In this part we introduce our improved version of CETD-MAC. In our first attempt of improvement, we do galois field multiplication, short for gf-mult, to each input block with a segment extracted from nonce. We call this first attempt Fully-GFM CETD-MAC as each input block will participate the galois multiplication. We also introduce its variant named Selected-GFM CETD-MAC in which the number of input blocks doing gf-mult is determined by user choice, just as what shuffle stage does.

Adding gf-mult before shuffle can inject random bits to the inputs and the adversary cannot predict the tag based on the input value according to the attack strategy depicted in Section ?. This improvement works for all the input value except for all 0 input as the output of 0 gf-mult with any value will be 0. To address this problem, we introduce our second version of improved CETD-MAC scheme named Flip-then-GFM CETD-MAC scheme. We randomly flip each input block and then do selected gf-mult as we did in the variant of first

version. We will show that our second version of improved CETD-MAC is secure under two types of integrity attacks in this part.

4.1.1 Fully-GFM CETD-MAC

Our first design draft based on the original CETD-MAC are described in Algorithm ???. We name this design Fully GF-Mult CETD-MAC, which means each input will do Galois field multiplication with a nonce segment.

Selected-GFM CETD-MAC

4.1.2 Flip-then-GFM CETD-MAC

Block Flipping

4.2 Our Optimization of Original CETD-MAC

Defending Content Modification Attack Hence the adversary can know the possible input set for a given tag, he can modify the content of ciphertext on the frame to a fake one that has the same number of 1s as the tag and this way of modification has the highest passing probability. On the other hand, as he knows the possible tag set for a given ciphertext, he can choose the tag for his fake ciphertext's set to evade the tag values that can not be generated with C_{fake} with any nonce.

To eliminate these advantages that left to the adversary by the original CETD-MAC, one idea is to make the relationship of 0-1 proportion between ciphertext and its tag unpredictable if the nonce is unknown.

As the 0-1 proportion of the tag is determined by its input ciphertext, we need to ensure that no matter how we modify the input, the value of the tag for the modified input is unpredictable. Th

Algorithm 1 Fully Galois Field Multiplication

Input:

The set of positive samples for current batch, P_n ;
The set of unlabelled samples for current batch, U_n ;
Ensemble of classifiers on former batches, E_{n-1} ;

Output:

Ensemble of classifiers on the current batch, E_n ;
1: Extracting the set of reliable negative and/or positive samples T_n from U_n with help of P_n ;
2: Training ensemble of classifiers E on $T_n \cup P_n$, with help of data in former batches;
3: $E_n = E_{n-1} \cup E$;
4: Classifying samples in $U_n - T_n$ by E_n ;
5: Deleting some weak classifiers in E_n so as to keep the capacity of E_n ;
6: **return** E_n ;
7: **for** each $i \in [1, 9]$ **do**
8: initialize a tree T_i with only a leaf (the root);
9: $T = T \cup T_i$;
10: **end for**
11: **for all** c such that $c \in \text{RecentMBatch}(E_{n-1})$ **do**
12: $T = T \cup \text{PosSample}(c)$;
13: **end for**
14: **for** $i = 1; i < n; i++$ **do**
15: // Your source here;
16: **end for**
17: **for** $i = 1$ to n **do**
18: // Your source here;
19: **end for**
20: // Reusing recent base classifiers.
21: **while** $(|E_n| \leq L_1) \text{ and } (D \neq \phi)$ **do**
22: Selecting the most recent classifier c_i from D ;
23: $D = D - c_i$;
24: $E_n = E_n + c_i$;
25: **end while**

A The Security Weakness of CETD-MAC Scheme

B Proof of Assertions in Section ??

As depicted in above section, if the MAC scheme is secure under replay attack, the tags should be random and distributed uniformly with repeated inputs. This property ensure the probability of the replayed data-tag pair passing verification is low. If the tags from a MAC scheme have high probability to be identical for repeated inputs, the MAC scheme is vulnerable to replay attack.

We denote the data M and the tag in the forgery frame $T1$. The output blocks from shuffle stage in generating $T1$ is denoted as $X1$ blocks and the output from shifting stage are $Y1$ blocks. When the forgery frame is read to be verified, the output or shuffle stage is $X2$ blocks and $Y2$ blocks for the output from shifting stage. The tag generated by verification is $T2$.

In this section, we depict the weaknesses we found in CETD-MAC under replay attack. These weaknesses let the CETD-MAC to produce tags with high collision probability with when replaying some chosen inputs. The tags with highly collision probability ease the adversary's attack.

Exposing the Weakness of CETD-MAC As the security of CETD-MAC is not provided in [], we do not know the randomness of tags under replay attack. To begin with, we conduct a simulation of replay attack on inputs formed by two 8-bit blocks concatenated. The hexadecimal value of the input various from 0x0000 to 0xFFFF. For each input, we static the tag distinction rate(TDR) under 1000 times replay attack. TDR is acquired by dividing the number of distinct values of 1000 tags with 2^8 . If TDR is low, the tag collision probability is high. Figure ?? expresses the TDR of all inputs. We can see that for some specific inputs the TDR is extremely low which means the collision probability is high. The experiment results expressed in Figure ?? introduce the motivation of systematically analyzing the security of CETD-MAC under replay attack. We examined the behaviour of each stage in CETD-MAC scheme and found that each stage have a set of inputs with high probability leading output collision.

Weakness of Shuffle Stage Under replay attack, the input data M is identical for the verifaciton and the replayed data-tag pair from the adversary. The basic requirement of shuffle stage is diordering the bits in M and ensure the distinction of the outputs, X blocks. If for some specific M , the X block set $X1$ for the verifaciton is identical to the set $X2$ for the adversary's data, shuffle stage is assumed lose the effect.

According to the original design of CETD-MAC, a segment of nonce is extracted as the control parameter to a round of shuffle. As nonce is the output of block cipher encryption, we assume the control parameter random. We denote this segment $R[i]$ where is expressed the i th round of shuffle. $R[i]$ is splitted to five bit segment components as $R[i] = (\text{index1}||\text{offset1}||\text{index2}||\text{offset2}||\text{segment length})$. Index determine which two blocks are selected for shuffle and offset de-

terminates the beginning bit of bit segment. The length of bit segment in block1 and block2 is determined by segment length.

We initialize the analysis of shuffle stage at 1 round shuffle. During the replay attack, when the shuffle parameters $R_1[1]$ and $R_2[1]$ is identical, the outputs of shuffle stage X1 and X2 are identical. If $R_1[1]$ and $R_2[1]$ are distinct, the equality of X1 and X2 are determined by the input M, and the two R parameters.

Assume the number of blocks in input M is x and the shuffle parameters $R_1[1]$ and $R_2[1]$ are distinct. Due to the randomness of block cipher encryption, the bit segment from nonce is assumed to be random and the value distributed uniformly. This property lead to the fact that when $R_1[1]$ and $R_2[1]$ are distinct there is at least one component pair is distinct. The analysis of the behaviour of one round shuffle is classified with each component pair. The following paragraphs in shuffle analysis is not finished, needs further discussion.

When Index Are Distinct Assume the $R_1[1]$ and $R_2[1]$ are distinct in the index components. If one pair of index is identical and the other is distinct, there are three pairs of M blocks involved in the one round shuffle, marked as $(M_1[i], M_2[i])$, $(M_1[j], M_2[j])$ and $(M_1[k], M_2[k])$.

If both two pairs of index are distinct, there are four pairs involved in the one round shuffle, marked as $(M_1[i], M_2[i])$, $(M_1[j], M_2[j])$, $(M_1[k], M_2[k])$ and $(M_1[h], M_2[h])$.

We can see that if the blocks in a input data M involved in the shuffle has common bit segment, there is possibility to form identical X blocks. The longer the big segment is, the higher the probability that X collision occurs.

When Offset Are Distinct If the $R_1[1]$ and $R_2[1]$ are distinct in the offset components, there are two M block pairs involved, marked as $(M_1[i], M_2[i])$, $(M_1[j], M_2[j])$.

When Segment Length Are Distinct If the $R_1[1]$ and $R_2[1]$ are distinct in the offset components, there are two M block pairs involved, marked as $(M_1[i], M_2[i])$, $(M_1[j], M_2[j])$.

We can see that when the segment-length components is distinct, the X collision can be triggered with M blocks with comon bit segment.

Combination of Cases

B.1 Shift Stage Weaknesses and Assertions Proof

Weakness of Shifting Stage

XOR Operation and Tag Collision The tag T from CETD-MAC can be expressed as the following Equation 2:

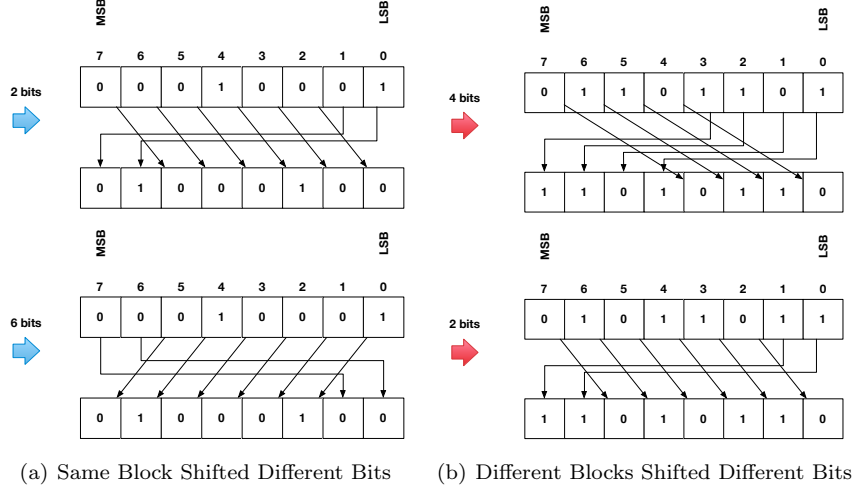


Figure 3: The Examples of Y Block Collision

$$T = Y[1] \oplus Y[2] \oplus \dots \oplus Y[x] \quad (1)$$

Then $\Pr[T1 = T2]$ can be expressed as the Equation ??:

$$\Pr[T1 = T2] = Y_1[1] \oplus Y_1[2] \oplus \dots \oplus Y_1[x] \oplus Y_2[1] \oplus Y_2[2] \oplus \dots \oplus Y_2[x] \quad (2)$$

We define the concept "equivalent set" as the set whose elements are identical. We denote Y_{all} as $Y1 \cup Y2$, and Y_{sub} as a sub-set of Y_{all} . $\sum_{i=1}^x Y_{sub}[i]$ is denoted as $Y_{sub}[1] \oplus \dots \oplus Y_{sub}[x]$. Assume Y_{sub} is an equivalent set, then $\sum_{i=1}^x Y_{sub}[i]$ is identical to 0 if x is an even number and to $Y_{sub}[1]$ if x is an odd number.

Assume Y_{all} can be splitted to several distinct equivalent Y_{sub} sets and the number of distinct Y_{sub} sets each of whom contains odd number of elements is k , then the result of $\sum_{i=1}^2 x \oplus Y_{all}[i]$ can be expressed as $\sum_{i=1}^k Y_{dist}[i]$, where Y_{dist} is denoted as the set of k distinct values. The $\Pr[T1 = T2]$ is identical to $\sum_{i=1}^k Y_{dist}[i]$.

We can see that the probability of tag collision is determined by the number of distinct values in the union of $Y1$ and $Y2$, which are the output sets from rotate shifting stage. If the shifting stage can not ensure the randomness of Y sets if X set collision occurs, the related tags have high probability to collide. Figure ?? gives the examples of the outputs from shifting stage that lead tag collision. There are two types of repeated X sets leading to high probability of tag collision, denoted as sequence-level pattern and set-level pattern.

The Sequence-level Pattern Collision Firstly, we treat blocks as a block sequences, which means in a block sequence, each block has a unique index. The definition of block sequence equality is expressed below:

Definition B.1. *Sequence Equality: Two block sequences $X1$ and $X2$ are equal in sequence-level if $X_1[i]$ is identical to $X_2[i]$ for any $i \in [1, x]$.*

Assume the shuffle stage does not work, then the following fact exist:

- $X1$ and $X2$ are two identical block sequences in sequence-level

In block-level rotate shifting stage, a segment from nonce, marked as S , is adopted as the parameter of shifting bits. S is a concatenation of sub-blocks and is denoted as $S = (S[1] || S[2] \dots S[x])$, where x is the number of blocks in X sequence. The value of $S[i]$ the bits shifted for $X[i]$ block. For two identical blocks $X_1[i]$ and $X_2[i]$, the output blocks $Y_1[i]$ and $Y_2[i]$ are identical if $S_1[i]$ is identical to $S_2[i]$. We found that $Y_1[i]$ and $Y_2[i]$ still have probability to be identical if $X_1[i]$ is formed by a repeated short bit segment named pattern. This property is depicted in Proposition 1.1:

Theorem B.1. *Let $X_1[i]$ and $X_2[i]$ be two identical block and $\text{len}(X_1[i]) = N$, $N = 2^n$. Let $S_1[i]$ and $S_2[i]$ be two distinct shifting bit parameters for $X_1[i]$ and $X_2[i]$. Then $Y_1[i]$ and $Y_2[i]$ can be identical only when $X_1[i]$ is formed by repeating a binary bit segment named pattern and marked as P . The length of P $\text{len}(P)$ has the following format: $P \cdot L = 2^p$, $p \in [0, n-1]$*

Base on Theorem B.1, we got the following corollaries:

Corollary B.2. *If a pattern P is not formed by a sub-pattern with shorter length, we call P a distinct pattern with length $P \cdot L$. The No. of distinct patterns with length $P \cdot L = 2^p$ is $2^{2^p} - 2^{2^{p-1}}$*

Corollary B.3. *Assume the length of a pattern-forming X block is $N = 2^n$, then the No. of all possible distinct patterns is $2^{N/2}$*

When the adversary conducts the replay attack on the data concatenated by pattern-formed blocks, the probability that Y block collision is high when shuffle stage does not work. The proof of Theorem B.1, Corollary B.2 and B.3 is expressed in the appendix.

The Probability of Tag Collision Under Sequence Pattern Attack For two identical X blocks $X_A[i]$ and $X_B[i]$, the probability that $Y_A[i] = Y_B[i]$ when $R_A[i]$ and $R_B[i]$ are randomly generated is marked as $\text{Pr}[Y \text{ block collision}]$. $\text{Pr}[Y \text{ block collision}]$ is expressed in Theorem B.4:

Theorem B.4. *Assume for two identical blocks $X_1[i]$ and $X_2[i]$ the length is $N = 2^n$, and the pattern length $P_l = 2^p$ where $p \in [0, n-1]$. If the pattern contains no internal sub-pattern, then :*

$$\text{Pr}[Y_1[i] = Y_2[i]] = 1/2^p \quad (3)$$

The Set-level Pattern Collision Secondly we treat blocks as a set allowing the existence of identical elements. We give the definition of block set equality below:

Definition B.2. *Set Equality: Two block sets $X1$ and $X2$ are identical in set-level if the following properties are met:*

- $X1$ and $X2$ have same number of elements
- The number of elements for each distinct value in $X1$ is identical to the number in $X2$

When none of block in a X block sequence is formed by repeated pattern, it is impossible to make two Y sequences with block sequence equality by using two distinct s sequences. This assertion can be proved based on the proof of Proposition 1.1. However, we found that it is possible to form two Y sets with block set equality by using two distinct s sequences. The set-level identical Y sets can lead to tag collision directly. This attack is expressed in Theorem B.5:

Theorem B.5. *Let $X_1[i]$ and $X_2[j]$ be two distinct block and $\text{len}(X_1[i])=\text{len}(X_2[j])=N$, $N=2^n$. Let $S_1[i]$ and $S_2[j]$ be two distinct blocks of shifting bit parameters for $X_1[i]$ and $X_2[j]$. Then $Y_1[i]$ and $Y_2[j]$ can be identical if and only if $X_1[i]$ can be formed by rotate shifting $X_2[j]$.*

Based on Theorem B.5, we got the following corollary:

Corollary B.6. *For the rotate shifting stage, when the distinct input blocks $X_1[i]$ and $X_2[j]$ have the property that $X_1[i]$ can be formed by rotate shifting $X_2[j]$, and the shifting bits parameter $S_1[i]$ and $S_2[j]$ are distinct, the probability that the output blocks $Y_1[i]$ and $Y_2[j]$ are identical is:*

$$\Pr[Y_1[i]=Y_2[j]] = 1/n \tag{4}$$

When the adversary conducts replay attack on the memory frame whose data part is concatenated by blocks that are formed by shifting a common base block, each element in $X1$ sequence can be formed by rotate shifting another element and the probability of forming identical Y sets is high, which will lead to tag collision. This fact is obvious if the shuffle stage cannot change the content of input data M .

The Probability of Tag Collision Under Set Pattern Attack Assume $X1$ and $X2$ are identical in sequence level and each block in $X1$ can be formed by rotate shifting another block in $X1$. From Corollary B.6 we know that for a N -bit block, the size of domain is 2^N and half of the domain is formed by

repeated pattern. This fact also indicates that half of the domain of a block is not formed with a pattern, totally $2^{N/2}$ distinct values.

Assume the X sets under replay attack, marked as X1 and X2, are identical in sequence level and none of the blocks is formed by a repeated pattern. If all the X blocks are formed by rotate shifting a base block which is not consist of a pattern, we denoted such X1 and X2 sets same base sets, short for SBS sets.

When X1 and X2 are SBS sets, the probability that Y1 and Y2 are identical in set level if shifting control paramter sets S1 and S2 are randomly generated is denoted as $\Pr[Y1 \text{ and } Y2 \text{ are set-level equal} \mid X1 \text{ and } X2 \text{ are SBS sets}]$ i, short for $\Pr[Y \text{ Sets Collision}]$

The lower bound of $\Pr[Y1 \text{ and } Y2 \text{ are set-level equal} \mid X1 \text{ and } X2 \text{ are SBS sets}]$ is expressed in Theorem B.7.

Theorem B.7.

$$\Pr[Y \text{ Sets Collision}] \geq (\sum_{k=1}^{\min(N,x)} (P_n^k * 1/2 * S(x,k)^2)) / (N^{2x}) \quad (5)$$

$S(x,k)$ is the Stirling Number with x and k as inputs.

The Vulnerable Inputs Set of CETD-MAC Under Replay Attack As summarized before, the shuffle stage is vulnerable to inputs that contains long all-0 or all-1 bit segments. After splitting a input to blocks, shuffle stage cannot effectively change the bit distribution of input blocks and the output of shuffle stage, X blocks, have big probability to be identical to the input. On the other hand, shifting stage is vulnerable to the input formed with a type of patterns. The patterns can exist in sequence level or set level. The pattern in the input of shifting stage have good chance to induce identical Y sets and directly produce tag collisions. We can see that if the input chosen by the adversary for replay attacks is the in the intersection of vulnurable inputs of shuffle and shifting stage, none of the stages can effectively randomize the input data M under replay attack, then there is good chance to form identical Y sets even if the nonce is generated from secure block cipher encryption.

The proof of theorems is expressed in the appendix.

B.2 Proof of Theorem B.1

This part proves that if two identical block $X_A[i]$ and $X_B[i]$ are shifted different bits and the result blocks remain identical, $X_A[i]$ is formed by pattern. The pattern length and $\delta = |R_A[i] - R_B[i]|$ has such correlation:

- If $\Delta = P_L$ then $Y_A[i] = Y_B[i]$ where P_L the length of pattern

Assume the length of $X_A[i]$ is N bits, where $N = 2^n$. When $X_A[i]$ is formed by a pattern whose length is $P_L = 2^p$ bits, then the domain of $Y_A[i]$ has P_L distinct values. There are N/P_L distinct $R_A[i]$ values that shift $X_A[i]$ to a $Y_A[i]$.

B.3 Proof of Theorem B.4

For identical each block pair $X_A[i]$ and $X_B[i]$, the No. of combination of $R_A[i]$ and $R_B[i] = N*N$, where N is the length a X block. If $X_A[i]$ is formed by pattern, then $Y_A[i]=Y_B[i]$ if $|R_A[i]-R_B[i]| = P_L * K$, where P_L is the pattern length and K is a positive integer. Then for two random $R_A[i]$ and $R_B[i]$, $\Pr[Y_A[i]=Y_B[i] \mid X_A[i] = X_B[i] \ \& \ \text{pattern} = P_L]$ (shoft for $\Pr[Y_A[i] = Y_B[i]]$) can be expressed in the following way:

- $\Pr[Y_A[i]=Y_B[i]] = N * (N/P_L)/(N*N) = 1/P_L$

B.4 Proof of Theorem B.5

If two distinct X blocks result two identical Y block. Assume the shift bits parameter blocks are $R_A[i]$ and $R_B[i]$. Then $X_A[i]$ can be formed by rotate shifting $Y_A[i]$ for $(N-R_A[i]) \bmod N$ bits. $X_B[i]$ can be formed for $(N-R_B[i]) \bmod N$ bits. $X_B[i]$ can be formed by rotate shifting $X_A[i]$ for $(R_A[i] + N - R_B[i]) \bmod N$ bits. Theorem 1.2 proved.

B.5 Proof of Theorem B.7

As the input sets of rotate shifting stage, $X1$ and $X2$, contain the following properties:

- $X1$ and $X2$ are identical in sequence level
- Each block in $X1$ can be formed by rotate shifint another block in $X1$ for several bits

After the shifting stage, the number of distinct block value in $Y1$ set, denoted as k , fall in the domain $[1, \min[N, x]]$. For each k , $Y1$ and $Y2$ set are identical in set level if the following properties are met:

- $Y2$ blocks have k distinct values
- Assume the k distinct values in $Y1$ is formed as: value1 has $v1$ blocks, value2 has $v2$ blocks, ..., valuek has vk block and $\sum_{i=1}^k v_i = x$. Then the distribution of k values amount x blocks in $Y2$ set is same as the distribution in $Y1$ sets.

For example, assume there is 2 distinct values among 4 blocks in $Y1$ set, then there are two types of distribution of blocks can be (1,3) or (2,2). For type (1,3) there is four different ways to distribute 4 blocks and for type (2,2) there is three ways. The number of ways to distribute 2 values to 4 blocks is $4+3=7$. If the distribution in $Y1$ is (1,3), then $Y2$ set is identical to $Y1$ set if the distribution of blocks in $Y2$ is (1,3). When there are k distinct values among x blocks, the number of ways to distribute k values to x blocks is know as Stirling Number of Second Type, marked as $S(x,k)$. Assume there are k_x types of distribution and

the number of ways to distribute k values for each distribution type is denoted as V_1, V_2, \dots, V_{k-x} . Then $\sum_{i=1}^{k-x} V_i = S(x, k)$

For each type of Y1 blocks distribution whose distribution ways number is V_i , the number of Y2 sets that are identical to Y1 is V_i . Then for each type of distribution, the probability that Y1 and Y2 set are identical in set level can be expressed as:

$$V_i^2 / (N^x)^2 \quad (6)$$

Then the probability that if there are k distinct values in Y1 set Y1 and Y2 are identical in set level can be expressed as:

$$P_N^k * \sum_{i=1}^{k-x} V_i^2 / (N^x)^2 \quad (7)$$

As $S(x, k) = \sum_{i=1}^{k-x} V_i$, $\sum_{i=1}^{k-x} V_i^2$ is no less than $1/2 * S(x, k)^2$. Then the following inequation stands:

$$P_N^k * \sum_{i=1}^{k-x} V_i^2 / (N^x)^2 \geq P_N^k * 1/2 * S(x, k)^2 / (N^x)^2 \quad (8)$$

As the domain of k is $[1, \min(x, N)]$, then:

$$\Pr[Y1 = Y2 \mid S1 \text{ and } S2 \text{ are random}] = (\sum_{k=1}^{\min(x, N)} (P_N^k * 1/2 * S(x, k)^2)) / (N^x)^2 \quad (9)$$

Theorem B.7 is proved.

B.6 Security Enhanced CETD-MAC

In this section we provide an modification of original CETD-MAC. Our approach does not require additional component or information to the original CETD-MAC. We then prove that the optimized CETD-MAC can fix the weakness and protect input message from replay attack.

Inspiration As depicted above, if a input message is consisted of blocks formed with a type of pattern and the proportion of 0s and 1s in the message is extremely unbalanced, the message cannot be effectively randomized by neither the shuffle stage nor the shifting stage. That means the message has high probability to induce identical Y sets or Y sequences under replay attack. The identical Y sets or Y sequences will directly induce tag collision then succeed the replay attack.

Solution As discussed above, the reason of high probability of tag collision for some specific inputs under replay attack is that neither the shuffle or the shift stage can randomize the input then the Y sets collide easily. The solution should be randomize the outputs from shuffle, shift or the xor stage.

As the the outputs from shuffle and shift stage is consist of multiple blocks, all the blocks should be randomnized, otherwise the patterns existing in the input data M remains in some blocks. The cost and lattency of such a optimization of CETD-MAC is dependent on the length of input data M, which is not efficient if the input is long.

Our solution is expressed as below:

- Xor a random block to the output of XOR operation
- Assume the MSB bits of nonce are adopted as control paramters for shuffle and shifting stage, we choose LSB bits on the nonce as the random block
- The random block is denoted as Mask_Tag, and $\text{len}(\text{Mask_Tag}) = \text{len}(\text{Tag})$.

We denote the output of original CETD-MAC scheme in our optimized scheme T_xor and tag of optimized scheme for T, the probability of tag collision of optimized scheme is expressed as $\text{Pr}[\text{tag collision}]$.

The computation of $\text{Pr}[\text{tag collision}]$ is expressed below:

$$\begin{aligned} \text{Pr}[\text{tag collision}] &= \text{Pr}[\text{Mask_Tag1} \oplus \text{T_xor1} \oplus \text{Mask_Tag2} \oplus \text{T_xor2} = 0] \\ &= \text{Pr}[\text{Mask_Tag1} \oplus \text{Mask_Tag2} = k \mid k = \text{T_xor1} \oplus \text{T_xor2}] \end{aligned} \tag{10}$$

As nonce is the output of block cipher encryption, the big segment of nonce is assumed as a output from PRF. Then $\text{Pr}[\text{tag collision}] = 1/2^{\text{len}(T)}$. This result means our optimized scheme can assure the randomness of tags under replay attack and is secure.

C Experiments and Results

D Proof of Assertions