1 Approach

1.1 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.

- The attacker monitoring the data and try to interpreted the meaning. This kind of attacks, named passive attacks in some articles, threats the confidentiality of the data.
- The attacker try to modify the valid data on the transferring path and on the memory by injecting malicious data. This kind of attacks, named active attacks, threats the integrity of the data.

The objective of active attacks effecting the behaviour of the system by tampering the data used. We categorize active attacks that can be conducted on CETD-MAC to two degrees according to the resources of injected data:

- Spoofing attack: the fake data from the adversary is directly injected to the path or memory, or replaces existing valid data. Under spoofing attack, the nonce in CETD-MAC is unchanged when verifying the fake data.
- Replaying or Relocating attack: the valid data at address A in old write-read period T1 or the data from another address B in current write-read period T2 is adopted as fake data to replace the valid data at address A in period T2. Under replay and relocating attack, the nonce in CETD-MAC is changed when verifying the fake data.

1.2 Security Weakness of CETD-MAC

1.2.1 Input Bit Frequency and Tag Collision Probability

As the shuffle and cycle shift operation is relocating bits in the input data and will not introduce new bits, the frequency of 1s and 0s in Y block set is same as the frequency in the input data block set. We found that the frequency of 1s and 0s in the input data block set determine the number of possible distinct tags. This assertion is depicted in Theorem 1.1

Theorem 1.1. *Assume the length of a tag n bits and the number of input blocks is x, then the number of possible distinct tags N is determined by the number of 1s k. The correlation of N and k is depicted in the following equation:*

$$N =$$

$$\sum_{i=0}^{k/2} \binom{k-2*i}{n} \text{if } k \text{ is even and } k \leq n$$

$$=$$

$$\sum_{i=0}^{k-1/2} \binom{k-2*i}{n} \textit{if } k \textit{ is odd and } k \textit{ ¡ } n$$

$$=$$

$$\sum_{i=0}^{(x*n-k)/2} \binom{x*n-k-2*i}{n} \textit{if } k \textit{ is even and } k \geq \textit{(x-1)*}n$$

$$=$$

$$\sum_{i=0}^{x*n-k-1/2} \binom{x*n-k-2*i}{n} \textit{if } k \textit{ is odd and } k \textit{ ¿ (x-1)*}n$$

$$=$$

$$2^{n-1} \textit{if } n \textit{ ¡ } k \textit{ ¡ (x-1)*}n \tag{1}$$

1.2.2 Spoofing Attack Case

1.2.3 Replay and Relocating Attack

1.3 Security Optimization of CETD-MAC

1.3.1 Do not use additional operation or data

The Operations Adopted in Original CETD-MAC

Cost and Performance Advantage of Original CETD-MAC

Why impossible to enhance security with existing operations and nonce

1.3.2 Using New Operations

.1 Security Theorem Proof