1 The Collision Probability ofY Set

Glossary The symbol, abbreviation and marks needed in expressing the shift stage and probability computation.

1.1 Preliminaries

Rotate Shifting This paragraph introduce the mechanism of block rotate shifting stage in CETD.

- rotate shifting is like whirling a wheel.
- the output blk of rotate shifting is determined by the input blk and the shift control parameter(No. of bits shifted)
- The value of input and output blks may not be 1-1 map.

Unlike logical shifting and arithmetic shifting, rotate shifting behaves like whirling a wheel. The empty position in a message blk shifted is filled by the bits shifted out. Figure 1 express the concept of rotate shift.

We can refer that the result of rotate shifting a message blk depends on the value of blk and the bits shifted. If two message blocks whose value are identical are shifted with distinct R_is, the result blocks may be identical.That means when R_i fixed,the mapping from message blocks to the shifted result blocks is not injection. This case is expressed in Figure 2(a). For two distinct message blocks, however, their result blocks may be identical when their R_is are distinct. This case is expressed in Figure 2(b). When the R_is of two message blocks are identical, the equality of result blocks is same as the equality of their input blocks.

1.2 Rotate Shifting and Y Set Collision

Y Set Collision This paragraph should introduce some simple examples of Y Set Collision, explain in detail that what kind of input pair can cause Y set collision.

- The blk-pair equality is maintained:(pattern and single block collision)
- Two distinctive blks produce an identical blk pair(shifting base and the effect on Y set)
- A special case, blks containing internal pattern and derived from same base.

Replay Attack In the context of this paper, replay attack refers to the circumstances that the adversary copy the data-tag message block pair from memory at an old time point and try to pass the verification with this old copy at a new time point. In the scenario of replay attack , the data part and tag

part of two message block pairs are identical respectively. The security of a tag generation design is evaluated by the probabilty that two tags equal when their relative data parts are identical. This probability is expressed as Pr[Tag Collision] in this paper. Figure x shows the status of each stage in CETD under replay attack. In this section , we analyze the behaviour of old and new Y set. (figure show two CETD scheme, representing old and new data)

1.2.1 Y Set Collision Under Replay Attack

Single Block Collision As shown in Figure 2(a), two identical X blocks can result two identical Y blocks while their relative Ri are distinct. We found that the identical X block pair X_a=X_b resulting identical Y blocks with distinct Ris have a common property, this property is expressed in Theorem 1.

Theorem 1.1. *Assume the two identical X blocks have same number of bits $N=2^n$. The result blocks Y_a and Y_b from rotate shifting two identical X blocks X_a=X_b with distinct R_a and R_b, can be identical only when X_a is formed by repeating a binary pattern P, which is a binary segment. The length of this pattern P can be expressed as:*

$P\_L = 2^p$, $p\in[0,n-1]$

The Collision of Block Set From Figure 2(b) we can see that two distinct X block X_a and X_b can result two identical Y blocks Y_a=Y_b when the relative $R_a \neq R_b$. Assume there are two identical X block sets X_A and X_B and the number of elements in each set is M. X_A[i] = X_B[i] for all i$\in$ [1,m] and none of the element is formed with pattern. We found that the result Y sets Y_A and Y_B can be identical in set level. These two X sets resulting two set level identical Y sets have a common property. This property is expressed in Theorem 2.

Theorem 1.2. *Assume the two X block set X_A and X_B have same number of element and this number is M. X_A[i]=X_B[i] for all i$\in$[1,m] and none of the element has pattern discussed in Theorem 1.1. Given two set level distinct shifting parameter sets R_A and R_B, the result sets Y_A and Y_B can be identical in set level if and only if:*

All the elements in X_A are formed by shifting a base block X_{base}.

Corollary 1.3. *If each element in the X sets discussed in Theorem 1.2 is formed by binary pattern discussed in Theorem 1.1, the result set Y_A and Y_B can be identical in both set level and block level.*

The proof of Theorem 1 and Theorem can be refered in appendix.

1.3 The Y Set Collision in Each Case Of Input

As discussed in Section x,

Probability of Y Set Collision This section should compute the Y set collision probability under replay attack for each input case.

- The condition of X set pair under replay attack: Xa[i] = Xb[i]
- The Probability of Y set pair collision for each case of X set pair.
- A general case of X set pair and the related Y set collision probability

A Proof of Theorem 1.1 and Theorem 1.2

A.1 Proof of Theorem 1

A.2 Proof of Theorem 2

B