1 The Collision Probability of Y Set

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

Replay Attack and Y Set Collision In replay attack, the adversary replace a data-tag pair on the memory with a pair copied from the same address at an old time point. That means for the two pairs at different time point, the two message block sets and related tags are identical respectly, while the shift bit parameter set R_A and R_B are randomly generated and the equality is unpredictable if their generator is of high quality. In this senario, the probability of a successful attack can be expressed as the equation 1.1:

Definition 1.1. *Pr[Successful Replay Attack] = Pr[Tag_a = Tag_b | (D_A = D_B) & (R_A and R_B are random)] = Pr[Y_A = Y_B | (D_A = D_B) & (R_A and R_B are random)]*

We can see that the collision of Y set will directly leads to the collision of tag and cause the succeed of replay attack. Hence the Y set is the output of rotate shifting stage in CETD, we will analyze the properties of block rotate shifting and the cases of input sets that can result Y set collision.

1.1 Preliminaries

What to say in this section

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

What to say in this section

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.

1.2.1 Y Set Collision Under Replay Attack

Single Block Collision Case 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∈[0,n-1]

The single block equality of two Y sets is defined in Defination 1.2:

Definition 1.2. *Assume there are M elements in each Y set, single block equality means Y_A[i] = Y_B[i] for all i∈[1,m]*

Block Set Collision Case 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 ≠ 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∈ [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∈[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 none of any two elements in X set are shifted from a same base block, the Y set collision is single block equality.*

Corollary 1.4. *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 1.1 and Theorem 1.2 can be refered in appendix. At the end of this section, add a group of figures of three cases.

1.3 The Y Set Collision in Each Case Of Input

what to say in this section

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

Hence the shift bit parameter set R_A and R_B are randomly generated, the probability of Y set collision for each input case is determined by the number of specific combinations of R_A and R_B. The computation of Pr[Y_A = Y_B] is based on this idea.

1.3.1 Single Block Collision only Case

what to say in this section

The Probability of Two Identical Y Block As discussed in above section, if each element in the X set is formed by a pattern P with pattern lentgh $P_l = 2^p$ and none of the element can be formed by rotate shifting the left elements, the result Y sets Y_A and Y_B have probability of Single Block Equality(SBE). This probability can be expressed as the following way:

Definition 1.3. *Pr[SBE] =*

$$\prod_{i=1}^{M} Pr[Y\_A[i] = Y\_B[i]]$$

M is the No. of elements in a set

Assume the shuffle stage of CETD does not work. That means D_A[i]=X_A[i]=X_B[i]=D_B[i] for all i∈[1,M]. Then Pr[Y_A[i] = Y_B[i]] can be expressed as Pr[Y_A[i] = Y_B[i] — X_A[i] = X_B[i] & R_A and R_B are randomly generated]. We use Pr[Y block collision] to express this probability.

If R_A[i] = R_B[i] for all i∈[1,M], then Pr[Y_A[i] = Y_B[i]] = 1. When R_A and R_B is distinct, then at least one R_A[i]-R_A[i] pair int two R sets is distinct. For a distinct R block pair, their related Y block pair can be identical when the related X pair is formed by pattern. The probability is expressed in Theorem 1.3:

Theorem 1.5. *If the No. of bits of each block in X_A[i]-X_B[i] pair is $N=2^n$, the pattern length $P_l=2^p$ where $p\in[0,n-1]$. The pattern contains no internal sub-pattern, then Pr[Y block collision] = $1/2^p$*

If each X set contains M elements, Pr[SBE] = $(1/2^p)^M$. The proof of theorem can be refered in appendix.

1.3.2 Block Set Collision only Case

What to say in this section

- In general condition, Y_A and Y_B are multisets. If Y_A and Y_B are identical in set level, then Y_B is a permutation of Y_A.
- how to make two identical Y block with two distinct X block and R block: if there is no pattern, for each value of block, the responding Y block is definite. 1 r map to 1 Y value
- How to represent the expression of Pr[set level collision | X collision & R distinct]
- If Y_A is identical to Y_B in set level, element in Y_B can be regarded as a multiset permutation of set Y_A.

If an element in an X set, marked as X[i], can be formed by rotate shifting another element in X, marked as X[i] where i≠j, then we call these two block "same base element". Two same base elements can result two identical Y blocks with distinct shifting bit R[i]≠R[j].

When none of an element in a X set contains a pattern, we call this X set a no-pattern set. Assume X_A and X_B are two identical no-pattern sets. It is impossible to two distinct R sets on X_A and X_B to form two single-block-equality Y sets . However, if there is some elements in X_A set are same base elemnts, Y_A and Y_B can have Set Level Equality(SLE).

Assume all elements in X_A set are same base elments.

1.3.3 Intersection of the Two Cases

What to say in this section

- If there is pattern in the block, for each element, the mapping between r and Y is not 1-to-1.
- Compute set level equality first, then solve the severl r to 1 Y problem
- express the Probability with combinatorics

1.3.4 A General Condition of X Set

what to say in this section

A Proof of Theorem 1.1 and Theorem 1.2

A.1 Proof of Theorem 1

A.2 Proof of Theorem 2

B Proof of Theorem 1.3

C Proof of Theorem 1.4 and 1.5

C.1 Proof of Theorem 1.4

C.2 Proof of Theorem 1.5