1 The Collision Probability of Y Set

1.1 Preliminaries

The Equality of Two Sets Assume there are two sets, marked as X_A and X_B, having same NO. of elements and the number is M. Each element is given an index from 1 to M. The definition of Identical Index Equality is expressed here:

Definition 1.1. *Identical Index Equality(IIE): For any $i \in [1,M]$, $X\_A[i]=X\_B[i]$.*

The definition of Cross Index Equality is expressed here:

Definition 1.2. *Cross Index Equality(CIE): For any $i,j \in [1,M]$, $X\_A[i] = X\_B[j]$, where $i \neq j$*

Any two sets that have same number of elements can be splited into several sub-groups and each sub-groups contains several (X_A[i],X_B[i]) pairs. The number of sub-groups various from 1 to M. We give the definition of set level equality of two sets with same number of elements:

Definition 1.3. *Set Level Equality(SLE): Each sub-set have one of the two kinds of Equality.*

For two sets X_A and X_B, if there is no way of split that at least one sub-set is of CIE and there are at least one way of split that all sub-sets are of IIE, then such X_A and X_B are IIE only Sets. The definition of CIE only Sets is given in same way.

1.1.1 Replay Attack and Y Set Collision

The Message Sets in CETD Under Replay Attack The Cost-Effective Tag Design can be expressed as the following procedure:

- The data is split into blocks. The block length is tag length. The block set is marked as D
- The content of blocks are shuffled. The output set of shuffle is marked as X.
- The content of each block is rotate shifted. The output set of rotate shift is marked as Y.
- All the blocks in Y is XORed to form the tag T.
- The control parameters is retrived from the segment of nonce N. The parameter set of shuffle is marked as S. The set for rotate shift is R.

In replay attack, the adversary replaces 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 D_A and D_B and

related tags T_a and T_b are identical respectively, while the nonce N_A and N_B are randomly generated and the equality is unpredictable if their generator is of high quality. The shifting bits parameter segment on the nonce R_A and R_B, are randomly generated. We can see that if the Y set for the old time point, marked as Y_A, is SLE to the Y set for new time point, marked as Y_B, T_a=T_b.

Based on the concept of set equality, the message block sets in the generation of T_a and verification of T_b meet the following properties if the replay attack succeeds:

- D_A and D_B are IIE.
- If the shuffle stage does not work. X_A=D_A, X_B=D_B
- Y_A and Y_B are SLE

In this scenario, the probability of a successful attack can be expressed as the equation 1.1:

Definition 1.4. *Pr[Successful Replay Attack] = Pr[T_a = T_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)]*

D_A and D_B sets are of Identical Index Equality. Y_A and Y_B is of Set Level Equality.

For easy understanding, we assume the shuffle stage does not work at first, which means D_A = X_A = D_B = X_B(IIE). 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(SLE).

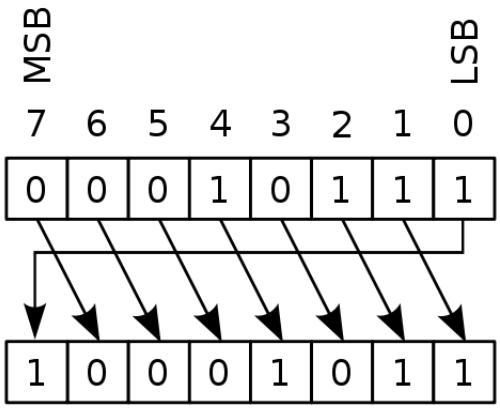
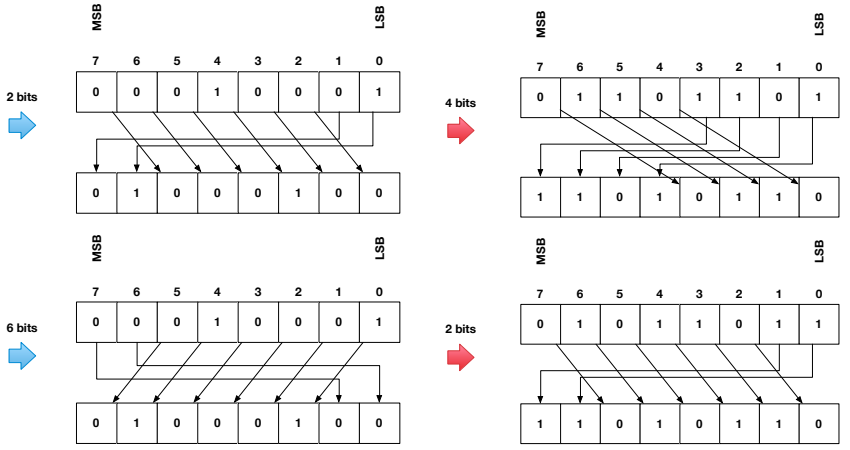


Figure 1: The Concept of Rotate Shifting(Right)



(a) Same Block Shifted Different Bits (b) Different Blocks Shifted Different Bits

Figure 2: The Examples of Y Block Collision

1.1.2 Rotate Shifting Introduction

Unlike logical shifting and arithmetic shifting, rotate shifting behaves like whirling a wheel. The empty position in a message block 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 block depends on the value of block and the bits shifted. If two message blocks whose value are identical are shifted with distinct bits, the result blocks may be identical. That means when shifting bits fixed,the mapping from X blocks to the shifted result blocks is not injection. This case is expressed in Figure 2(a).

For two distinct X blocks, however, their result blocks may be identical when their shifting bits are distinct. This case is expressed in Figure 2(b). When the shifting bits of two message blocks are identical, the equality of result blocks is same as the equality of their input blocks.

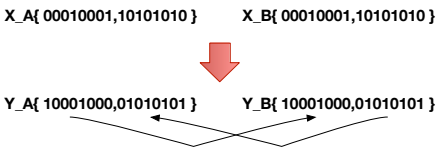
1.2 Rotate Shifting and Y Set Collision

Assume the shuffle stage does not work, then D_A= X_A=D_B=X_B, which means the following properties exist in X_A and X_B:

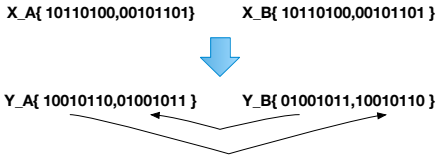
- X_A[i] = X_B[i] for all i∈[1,M], M is the number of elements
- The equality of elements in a X set is uncertain.

Then X_A and X_B are of Identical Index Equality. All the analysis in this section is based on the assumption that shuffle stage does not work.

If such X_A and X_B result two Y sets of Set Level Equality, the related tag $T_a = T_b$.

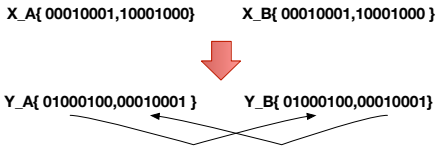


(a) Only Single Block Equality

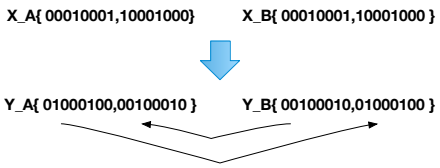


(b) Only Set Level Equality

Figure 3: X Set Pairs with Only One Type of Y Equality



(a) Single Block Equality Case



(b) Set Level Equality Case

Figure 4: A X Set Pair with Two Types of Y Equality

Figure 3 and Figure 4 express the examples of X sets that lead to SLE Y sets with distinct R sets. In this paper, we analyze the cases of the input set pair (X_A and X_B) of shifting stage in CETD under replay attack that can lead to Y set pair collision(SLE).

1.2.1 Case of X Sets Resulting Y Set Collision

If R_A and R_B are IIE, then for any two identical set X_A and X_B, Y_A and Y_B are IIE. If there is at least one pair of blocks in R_A and R_B, marked as (R_A[i], R_B[i]), is distinct, then equality of Y_A and Y_B is uncertain.

Assume the number of distinct block pairs in R_A and R_B is R_d. For these R block pairs, their related X_A and X_B blocks formed a sub-group, marked as X_A_s and X_B_s, and this sub-group is IIE. The related sub-group in Y_A is marked as Y_A_s and the one in Y_B for Y_B_s.

In this part, we discuss the equality case of Y_A_s and Y_B_s

Identical Index Equality Case If Y_A_s and Y_B_s are IIE, then for all i$\in$[1, R_d] the following two properties are met:

- $Y\_A_s[i] = Y\_B_s[i]$
- $R\_A_s[i] \neq Y\_B_s[i]$
- $X\_A_s[i] = X\_B_s[i]$

Figure 2(a) provides a instance of IIE Y sets. The identical block pairs (X_A_s[i],X_B_s[i]) that lead to IIE Y_A_s and Y_B_s have the property in Theorem 1.1:

Theorem 1.1. *Assume X_A[i] and X_B[i] are two identical block from two sub-group X_A_s and X_B_s with same index i. X_A[i] and X_B[i] have same number of bits $N=2^n$. The result of rotate shifting X_A[i] and X_B[i] with distinct shifting bit parameter R_A[i] and R_B[i] are marked as Y_A[i] and Y_B[i].*

Then Y_A[i] and Y_B[i] can be identical only when X_A[i] and X_B[i] are 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]

Cross Index Equality Case If Y_A_s and Y_B_s are CIE, then for all distinct (i,j) that i,j$\in$[1, R_d] the following two properties are met:

- $Y\_A_s[i] = Y\_B_s[j]$
- $R\_A_s[i] \neq Y\_B_s[i]$
- $X\_A_s[i] = X\_B_s[i]$

Figure 2(b) provides an instance of CIE Y sets. The blocks in X_A_s and X_B_s that lead to CIE Y_A_s and Y_B_s have the property in Theorem 1.2:

Theorem 1.2. *If Y_A_s and Y_B_s are CIE, each element in X_A_s can be formed by rotate shifting another element in X_A_s.*

If each element in X_A_s is formed by a pattern can be formed by rotate shifting another element in X_B_s then the related Y_A_s and Y_B_s can be either IIE or CIE or SLE. The proof of Theorem 1.1 and Theorem 1.2 can be refered in appendix.

1.3 The Probability of Y Set Collision

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. The following properties are met by any cases of D sets and R sets in replay attack:

- D_A[i] = D_B[i] for all i∈[1,M]
- If R_A[i]=R_B[i] and X_A[i]=X_B[i], then Y_A[i]=Y_B[i].

1.3.1 Identical Index Equality Case

From Theorem 1.1 we know that Y_A and Y_B can be IIE if each element in X_A is formed by a pattern P whose length P_L is 2^p. Assume two identical sets X_A and X_B satisfy the following properties:

- Each element is formed by a pattern with same length P_L = 2^p
- Each element cannot be formed by rotate shifting any other element.

We call this kind of X_A and X_B Identical Pattern Length(IPL) IIE X Sets, short for IPL X sets. IPL X sets can form IIE Y sets. Assume D_A set is randomly generated, then the probability of a IPL D_A is expressed as:

Definition 1.5. *Pr[IPL D(X)] =*

The probability of IIE of Y_A and Y_B is marked as Pr[IIE Y sets] and expressed as the following way:

Definition 1.6. *Pr[IIE Y sets] =*

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

M is the No. of elements in a set

As D_A[i]=X_A[i]=X_B[i]=D_B[i] for all i∈[1,M], 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[i] ≠ R_B[i]]. We use Pr[Y block collision] to express this probability.

Pr[Y block collision] is expressed in Theorem 1.3:

Theorem 1.3. *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 :*

$$Pr[Yblockcollision] = 1/2^p$$

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

1.3.2 Cross Index Equality 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.

Assume two identical sets X_A and X_B satisfy the following properties:

- Each element can be formed by rotate shifting any other element in the set
- None of the elements is formed by pattern.

As each element in the X set can be formed by rotate shifting a base block, we call such X set Same Base Block(SBB) X sets, short for SBB X sets. If none of the element is formed by a pattern ,we call such X set SBB only sets.

Assume D_A and D_B are randomly generated, the probability of generating SBB only D set is expressed:

Definition 1.7. *Pr[SBB only D]=*

Using SBB only X_A and X_B, the probability of CIE of Y_A and Y_B is marked as Pr[CIE Y Sets] and expressed as the following way:

Definition 1.8. *Pr[CIE Y Sets] =*

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

where M is the No. of elements in a set, $i,j\in[1,M]$ and $i\neq j$

For two randomly generated R_A and R_B, the probability that Y_A and Y_B are CIE when X_A and X_B are SBB only is expressed in the following theorem:

Theorem 1.4. *Assume X_A and X_B are SBB only, R_A and R_B are randomly generated,then:*
Pr[CIE Y Sets]:

$$(\sum_{K=1}^{min(N,M)} \binom{N}{K} * (M!/v1!v2!v3!\cdots vk!)^2)/(N^M)^2$$

The proof of this theorm is expressed in the appendix.

1.3.3 The Intersection Case

If the blocks in X set is formed by rotate shifting a base block and this base block is formed by a pattern, then such X set pair X_A and X_B can result either IIE or CIE Y set pairs.

Assume the R_A and R_B are randomly generated, the probability that Y_A and Y_B are SLE is expressed in the following theorem:

Theorem 1.5. *Assume X_A and X_B are both SBB and IPL, R_A and R_B are randomly generated,then:*
Pr[SLE Y Sets]:

$$(\sum_{K=1}^{min(N,M)} \binom{N}{K} * (M!/v1!v2!v3!\cdots vk!)^2)/(N^M)^2$$

The proof of this theorm is expressed in the appendix.

1.4 A General Case of Sets in CETD

The general Case of D sets During the replay attack, the D_A and D_B sets are IIE. Any D set can be splited into sub-groups of blocks in the following way:

$$D = IIEonly, CIEonly, Intersection, Noregularity \quad (1)$$

The No. of the elements in these sub-groups is marked as M_{IIE}, M_{CIE}, M_{inter}, M_{non}. The following equations are met:

M_{IIE}, M_{CIE}, M_{inter}, M_{non} $\in$[0,M]

M_{IIE}+ M_{CIE}+M_{inter}+ M_{non} = M

(2)

The General Case of X Sets In general case, the shuffle stage can change the split of blocks. For a D set that contains regularity, shuffle can reduce the No. of regularity sub-groups and the No. of elements in each group. The properties of no regularity sub-group is analyzed in the next section.

A Proof of Pattern Introduction

A.1 Proof of Theorem 1.1

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 δ=|R_A[i]-R_B[i] | has such correlation:

- If δ = 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].

A.2 Proof of Theorem 1.2

According to the proof of Theorem 1.1, the Assume Y_A[i] and Y_B[j] are identical. That means the following equations are met:

- Y_A[i][b] = X_A[i][(b+R_A[i]) mod N]
- Y_B[j][b] = X_B[j][(b+R_A[j]) mod N]
- $Y\_A[i]_b = Y\_B[j]_b$
- X_A[i][(b+R_A[i]) mod N] = X_B[j][(b+R_A[j]) mod N]

We can see that for any b$\in$[1,N], X_A[i][(b+R_A[i]) mod N] = X_B[j][(b+R_A[j]) mod N] when Y_A[i]=Y_B[j]. This means if rotate shifting X bits, X_A[i]=X_B[i]. Theorem 1.2 get proved.

Proof of Corollary 1.3 According to the definition of set level equality, Y_A[i]=Y_B[j] for i,j$\in$[1,M], i$\neq$j and X_A[i] $\neq$. As R_A $\neq$ R_B, there is at least one pair (R_A[i],R_B[i]) is distinct. As the related X_A[i] is identical to X_B[i], X_A[i] is formed by pattern based on Theorem 1.1.

B Proof of Probability Computation

B.1 Proof of Theorem 1.3

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] | X_A[i] = X_B[i] & 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

If all the X block pairs is formed by a pattern with length of P_L and none of a block in X_A can be formed by rotate shifting another block, then for two randomly generated R_A and R_B set, Pr[IIE Y Set] = $(1/P\_L)^M$.

B.2 Proof of Theorem 1.4

From Theorem 1.1 we can see that if a X block is formed by a pattern, then the No. of distinct values in the range of Y block is P_L. While the domain of a R block has N distinct values, then for a block X, there are N/P_L distinct R values that lead to a Y value.

If a X block is not formed by a pattern, then for each distinct R value, there is a distinct Y value. That means for a given X set that none of the blocks is formed by a pattern, each R set will lead to a distinct Y set. The map between R set and Y set is bijection.

When each R block is randomly generated, the possible combination of R sets is N^M. That means for a given X set, the No. of possible Y set is N^M.

Assume X_A and X_B are IIE and each block can be formed by rotate shifting another block in the set. On the other hand, none of blocks is formed by a pattern. Then the sub-group of blocks in X_A and X_B can form CIE with specific R_A and R_B set.

Assume set Y_A and Y_B are SLE, then Y_B is a permutation of Y_A. This concept can be modeled in the following way:

- Assume the M elements in Y_A contain K distinct values. The No. of the elements that have each value are marked as v1,v2...vk.
- IF the elements in Y_B are a permutation of the elements in Y_A, then Y_A and Y_B are SLE.

Based on the basic concept in Combinatorics, the No. of a permutation of Y_A that contains K distinct value can be expressed in the following equation:

Definition B.1. *No. of Permutation with K distinct Values:*

$$\binom{M}{v1} * \binom{M-v1}{v2} * \binom{M-v1-v2}{v3} \cdots * \binom{vk}{vk} = M!/v1!v2!v3! \cdots vk!$$

As any one of the elements in X set can be formed by rotate shifting another element, then the No. of distinct values of M elements, K, various from 1 to M. If Y_A has K distinct values, the No. of possible combination of these K elements in Y_A can be expressed as Com_Y_A:

Definition B.2. *Com_Y_A:*

$$M!/v1!v2!v3!\cdots vk!$$

For each case of Y_A in Com_Y_A, the No. of Y_B to form SLE is also Com_Y_A. Then if Y_A has K distinct values, Pr[CIE Y sets] can be expressed as:

Definition B.3. *Pr[CIE Y Sets]:*

$$\binom{N}{K} * (M!/v1!v2!v3!\cdots vk!)^2/(N^M)^2$$

If R_A and R_B are randomly generated, then the value of K various from 1 to M. We do th sum to get the expression in Theorem 1.4

Definition B.4. *Pr[CIE Y Sets]:*

$$(\sum_{K=1}^{min(N,M)} \binom{N}{K} * (M!/v1!v2!v3!\cdots vk!)^2)/(N^M)^2$$

B.3 Proof of Theorem 1.5

If the element contains both the properties of CIE and IIE, then the following properties:

- For two distinct sets R_A and R_B, Y_A and Y_B can be IIE
- For each value of a Y block, there are N/P_L distinct R block that can shift X to this Y. That means for a distinct Y set, the No. of R sets is not one.
- For two distinct sets R_A and R_B, Y_A and Y_B can be CIE

Base on the Theorem 1.1, if the X block is formed by pattern, then the No. of values in the range of Y is P_L, base on theorem 1.4, the Pr[SLE Y sets] can be expressed as:

Definition B.5. *Pr[SLE Y Sets:]:*

$$\binom{P\_L}{K} * (M!/v1!v2!v3!\cdots vk!)^2)/(P\_L^M)^2$$

If R_A and R_B are randomly generated, then the value of K various from 1 to M. We do th sum to get the expression in Theorem 1.5

Definition B.6. *Pr[SLE Y Sets]:*

$$(\sum_{K=1}^{min(P\_L,M)} \binom{P\_L}{K} * (M!/v1!v2!v3!\cdots vk!)^2)/(P\_L^M)^2$$