

# 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 split into several sub-groups and each sub-groups contains several  $(X\_A[i], X\_B[i])$  pairs. For two specific sets, 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-group have one of the two kinds of Equality.*

For two sets  $X\_A$  and  $X\_B$ , if there is no way of splitting that at least one sub-group 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  $D$ , and the No. of blocks is  $M$ .
- 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.**  $Pr[Successful\ Replay\ Attack] = Pr[T_a = T_b \mid (D_A = D_B) \ \& \ (R_A \text{ and } R_B \text{ are random})] = Pr[Y_A = Y_B \mid (D_A = D_B) \ \& \ (R_A \text{ and } R_B \text{ are random})]$

$D_A$  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).

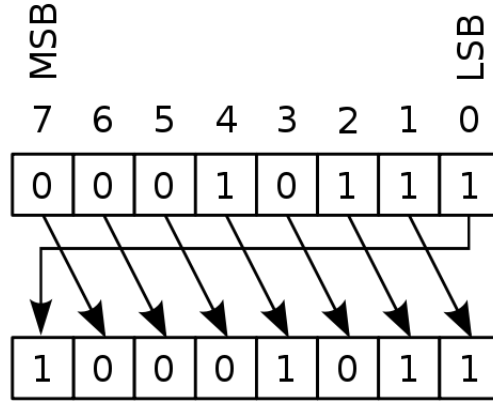


Figure 1: The Concept of Rotate Shifting(Right)

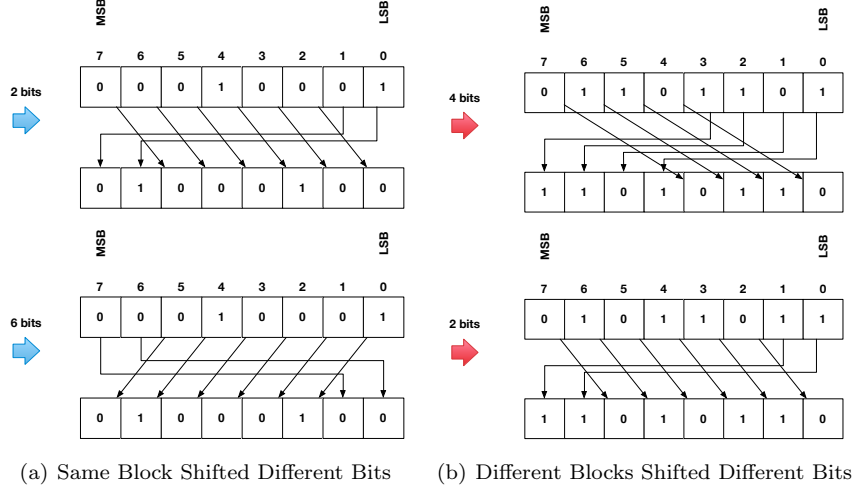


Figure 2: The Examples of Y Block Collision

### 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  $i \in [1, M]$ ,  $M$  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  $T_a = T_b$ .

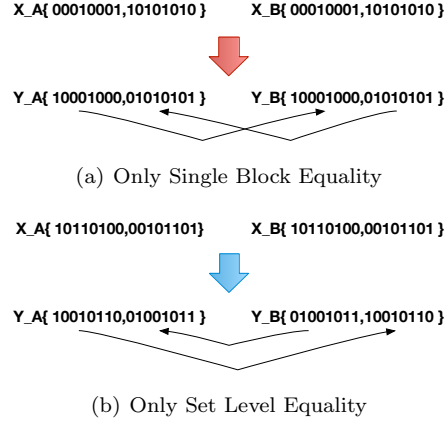


Figure 3: X Set Pairs with Only One Type of Y Equality

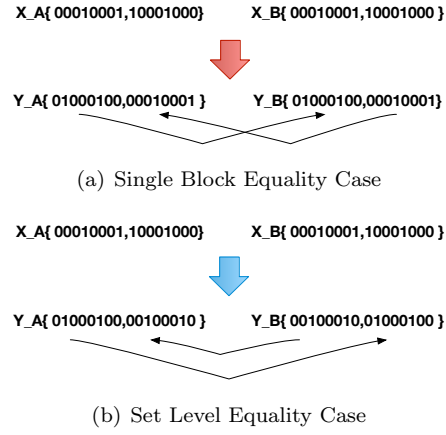


Figure 4: A X Set Pair with Two Types of Y Equality

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:*

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

Base on Theorem 1.1, we got the following corollaries:

**Corollary 1.2.** *If a pattern is not formed by a pattern with short length, we call it a distinct pattern of length  $P.L$ . The No. of distinct patterns with length  $P.L = 2^p$  is  $2^{2^p} - 2^{2^{p-1}}$*

**Corollary 1.3.** *Assume the length of a block is  $N=2^n$ , then the No. of all distinct patterns with all possible length is  $2^{N/2}$*

**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 1.4.** *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  $i \in [1, M]$
- 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

When  $R_A[i]$  and  $R_B[i]$  are distinct for some  $i \in [1, M]$ , the  $Y_A[i]$  and  $Y_B[i]$  blocks can form an IIE sub-group if each  $X_A[i]$  and  $X_B[i]$  block is formed by a pattern.

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  $\Pr[Y \text{ block collision}]$ .

$\Pr[Y \text{ block collision}]$  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 :*

$$\Pr[Y \text{ block collision}] = 1/2^p$$

### 1.3.2 Cross Index Equality Case

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.

From Corollary 1.3 we know that for a block that is N bits long, the No. of possible values that is formed by a pattern is  $2^{N/2}$ , which also means the No. of distinct values that is not formed by a pattern is  $2^{N/2}$ . Assume D\_A and D\_B are randomly generated, the probability of generating SBB only D set is expressed:

**Definition 1.5.**  $Pr[SBB \text{ only } D(X)] =$

$$2^{n/2} * N^{M-1} / (2^N)^M$$

Using SBB only X\_A and X\_B, the probability of CIE of Y\_A and Y\_B is marked as  $Pr[CIE \text{ Y Sets}]$  and expressed as the following way:

**Definition 1.6.**  $Pr[CIE \text{ Y Sets}] =$

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

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 1.6.** Assume X\_A and X\_B are SBB only, R\_A and R\_B are randomly generated, then:

$Pr[CIE \text{ Y Sets}]$ :

$$\left( \sum_{K=1}^{\min(N, M)} \binom{N}{K} * (M! / v_1! v_2! v_3! \dots v_k!)^2 \right) / (N^M)^2$$

### 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 1.7.** Assume  $X_A$  and  $X_B$  are both SBB and IPL,  $R_A$  and  $R_B$  are randomly generated, then:

$Pr[SLE \ Y \ Sets] =$

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

The proof of theorems 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 split 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:

$$M_{IIE}, M_{CIE}, M_{inter}, M_{non} \in [0, M] \quad (2)$$

$$M_{IIE} + M_{CIE} + M_{inter} + M_{non} = M \quad (3)$$

**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  $\delta = |R_A[i] - R_B[i]|$  has such correlation:

- If  $\Delta = P \cdot L$  then  $Y_A[i] = Y_B[i]$  where  $P \cdot L$  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  $P \cdot L = 2^p$  bits, then the domain of  $Y_A[i]$  has  $P \cdot L$  distinct values. There are  $N / P \cdot L$  distinct  $R_A[i]$  values that shift  $X_A[i]$  to a  $Y_A[i]$ .



## A.2 Proof of Theorem 1.2

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 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  $R\_B[i]$ ,  $\Pr[Y\_A[i]=Y\_B[i] \mid X\_A[i] = X\_B[i] \ \& \ \text{pattern} = P\_L]$  (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.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  $v_1, v_2 \dots v_k$ .
- 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]:*

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

### 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  $K$  varies from 1 to  $M$ . We do the sum to get the expression in Theorem 1.5

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

$$\left( \sum_{K=1}^{\min(P, L, M)} \binom{P-L}{K} * (M! / v_1! v_2! v_3! \dots v_k!)^2 \right) / (P-L)^M)^2$$