

1 The Collision Probability of Y Set

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

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-sets and each sub-sets contains several $(X_A[i], X_B[i])$ pairs. The number of sub-sets 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

- D_A and D_B are definitely IIE.
- $X_A = D_A$, $X_B = D_B$
- Y_A and Y_B are just SLE
- when Y_A and Y_B are SLE, tag 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 respectively, while the nonce N_A and N_B are randomly generated and the equality is unpredictable if their generator is of high quality. That means the shifting bits parameter segment on the nonce R_A and R_B , are randomly generated.

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

Definition 1.4. $Pr[Successful\ Replay\ Attack] = Pr[Tag_a = Tag_b \mid (D_A = D_B) \ \& \ (R_A \text{ and } R_B \text{ are random})] = Pr[Y_A = Y_B \mid (D_A = D_B) \ \& \ (R_A \text{ and } R_B \text{ are random})]$

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

We can see that the set level equality of Y_A and Y_B will directly leads to the collision of tag and cause the succeed of replay attack. 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).

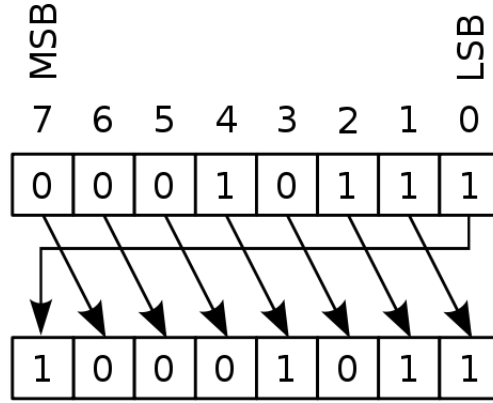


Figure 1: The Concept of Rotate Shifting(Right)

1.1.2 Rotate Shifting Introduction

- the concept of rotate shift
- The examples of X,R,Y

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 R_i s, 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).

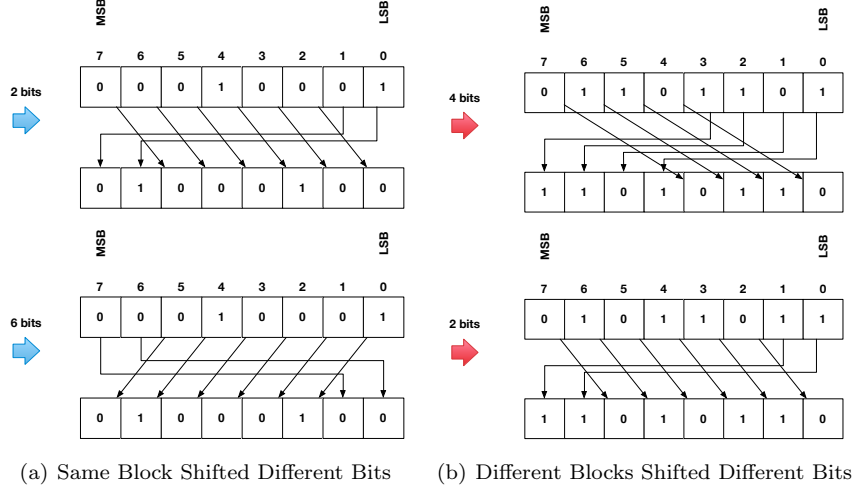


Figure 2: The Examples of Y Block Collision

For two distinct message blocks, however, their result blocks may be identical when their R_i s are distinct. This case is expressed in Figure 2(b). When the R_i s 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

- distinct pairs in R sets: IIE pairs and CIE pairs
- X block pairs causing IIE Y block pairs
- X block pairs causing CIE Y block pairs

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.

That means 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 using two identical shifting bits parameter sets R_A and R_B , the related tag $T_a = T_b$.

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).

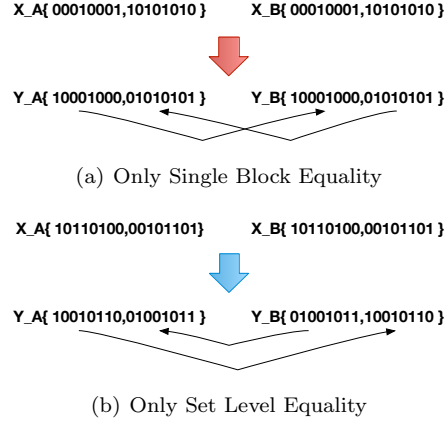


Figure 3: X Set Pairs with Only One Type of Y Equality

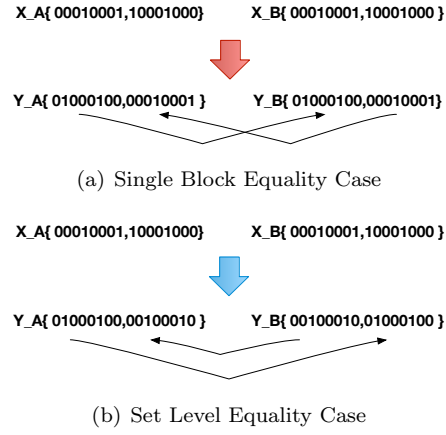


Figure 4: A X Set Pair with Two Types of Y Equality

1.2.1 Case of X Sets Resulting Y Set Collision

- If $R_A \neq R_B$, there is at least one pair distinct
- the related x blocks pairs should generate a SLE y pairs.
- if the Y pairs are iie, then each X block pair has pattern
- if the Y pairs are cie, then each X block in a sub-set is from a same base

Identical Index Equality Case As shown in Figure 2(a), two identical X blocks can result two identical Y blocks while their relative shifting bit parameter $R[i]$ and $R[j]$ are distinct. We found that the identical X block pair $X_A[i]=X_B[i]$ resulting identical Y blocks with distinct $R_A[i]$ and $R_B[i]$ have a common property, this property is expressed in Theorem 1.

Theorem 1.1. *Assume $X_A[i]$ and $X_B[i]$ are two identical block from two set X_A and X_B 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:*

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

Assume the two X sets X_A and X_B are identical and can form single block equality. Base on Theorem 1.1, we can conclude the corollary of the relationship between X set pair and Y set pair for single block case.

Corollary 1.2. *Assume there is M elements in X_A and X_B . If there is at least one $i \in [1, M]$, $X_A[i] = X_B[i]$ is formed by repeating a pattern P_i whose length is $P \cdot L_i = 2^p i$, then Y_A and Y_B can be single block identical with some two distinct shifting bits parameter sets R_A and R_B .*

Cross Index Equality Case From Figure 2(b) we can see that two distinct X block $X_A[i]$ and $X_B[j]$ can result two identical Y blocks $Y_A[i]=Y_B[j]$ when the relative $R_A[i] \neq R_B[j]$.

Assume the element in a set with distinct indexes are distinct. We found that two distinct blocks $X_A[i]$ and $X_B[j]$ resulting identical Y blocks with distinct $R_A[i]$ and $R_B[j]$ have a common property. This property is expressed in Theorem 2.

Theorem 1.3. *Assume $X_A[i]$ and $X_B[j]$ are two distinct blocks from two set X_A and X_B and $i \neq j$. $X_A[i]$ and $X_B[j]$ have same number of bits $N=2^n$. The result of rotate shifting $X_A[i]$ and $X_B[j]$ with distinct shifting bit parameter $R_A[i]$ and $R_B[j]$ are marked as $Y_A[i]$ and $Y_B[j]$.*

Then $Y_A[i]$ and $Y_B[j]$ can be identical when $X_A[i]$ can be rotate shifted to $X_B[j]$

Assume the two X sets X_A and X_B are identical and can form set level equality. Base on Theorem 1.2, we can conclude the corollary of the relationship between X set pair and Y set pair for set level equality.

Corollary 1.4. *Assume there are M elements in X_A and X_B . If there is at least two pairs of data, marked as $(X_A[i], X_B[j])$ and $(X_A[j], X_B[i])$ where $i, j \in [1, M]$ and $i \neq j$, that $X_A[i]$ can be formed by shifting $X_A[j]$, then Y_A and Y_B can be set level identical with some two distinct shifting bits parameter sets R_A and R_B .*

An Intersection Case Base on Corollary 1.3 and Corollary 1.4, we can draw the following corollary for the X set pairs that can form both set level and single block equality:

Corollary 1.5. *Assume there is M elements in X_A and X_B . If there are at least two pairs of data, marked as $(X_A[i], X_B[j])$ and $(X_A[j], X_B[i])$ where $i, j \in [1, M]$ and $i \neq j$, that $X_A[i]$ can be formed by shifting $X_A[j]$ and $X_A[i] = X_B[i]$ or $X_A[j] = X_B[j]$ is formed by repeating a pattern P_i whose length is $P_L = 2^p$, then Y_A and Y_B can be either set level or single block identical with some two distinct shifting bits parameter sets R_A and R_B .*

The proof of Theorem 1.1 and Theorem 1.2 and Corollary 1.2 to 1.5 can be refered in appendix.

1.3 The Probability of Y Set Collision

- Assume the sub-set contains M blocks, the probability that they are both pattern
- if they are both pattern, the probability that Y set are iie
- the probability that they are from same base
- if they are same base, the pro that Y set is cie
- the probability that bothe pattern and same base
- if both, the pro of Y SLE

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 Equality Case

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.

Such two sets X_A and X_B can only result single block identical Y_A and Y_B . The probability of single block equality of Y_A and Y_B is marked as $\Pr[SBE]$ and expressed as the following way:

Definition 1.5. $\Pr[SBE] =$

$$\prod_{i=1}^M \Pr[Y_A[i] = Y_B[i]]$$

M is the No. of elements in a set

As $D_A[i]=X_A[i]=X_B[i]=D_B[i]$ for all $i \in [1, M]$, $\Pr[Y_A[i] = Y_B[i]]$ can be expressed as $\Pr[Y_A[i] = Y_B[i] \mid X_A[i] = X_B[i] \ \& \ R_A \text{ and } R_B \text{ are randomly generated}]$. We use $\Pr[Y \text{ block collision}]$ to express this probability.

If $R_A[i] = R_B[i]$ for all $i \in [1, M]$, then $\Pr[Y_A[i] = Y_B[i]] = 1$. When R_A and R_B is distinct, then at least one $(R_A[i], R_B[i])$ pair in two R sets is distinct. $\Pr[Y \text{ block collision}]$ is expressed in Theorem 1.3:

Theorem 1.6. *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 $\Pr[Y \text{ block collision}] = 1/2^p$*

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

1.3.2 Set Level 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 $\Pr[\text{set level collision} \mid X \text{ collision} \ \& \ R \text{ distinct}]$
- 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.

Such two sets X_A and X_B can only result set level identical Y_A and Y_B . The probability of set level equality of Y_A and Y_B is marked as $\Pr[SLE]$ and expressed as the following way:

Definition 1.6. $\Pr[SLE] =$

$$\prod_{i=1, j=1}^M \Pr[Y_A[i] = Y_B[j]]$$

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

what to say next

- for any Y_A , the set level identical Y_B is a permutation of Y_A
- The No. of Y_B is effected by the value distribution of elements in Y_A

1.3.3 The Intersection Case

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 several to 1 Y problem
- express the Probability with combinatorics

1.4 A General Condition of X Set and Related Y Set Collision

what to say in this section

- If shuffle stage works, the properties in some block pairs in D_A and D_B can be eliminated, while the remaining blocks maintain the pattern
- the no-pattern block pairs follow the analysis in Main Case 3.
- these patterned block pairs can be splited into several, each group is a kind of pattern.
- the pattern in any two group is distinct
- assume the No. of element in each group is expressed as M_i , then the theorem of each case of X sets can be applied in each group

A Proof of Pattern Introduction

A.1 Proof of Theorem 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 $\delta = P_L$ then $Y_A[i] = Y_B[i]$ where P_L the length of pattern

Proof of Corollary 1.2 According to the definition of set block equality, $Y_A[i] = Y_B[i]$ for all $i \in [1, M]$. 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.

A.2 Proof of Theorem 2

Assume $Y_A[i]$ and $Y_B[j]$ are identical. That means the following equations are met:

- $Y_A[i][b] = X_A[i][(b + R_A[i]) \bmod N]$
- $Y_B[j][b] = X_B[j][(b + R_A[j]) \bmod N]$
- $Y_A[i]_b = Y_B[j]_b$
- $X_A[i][(b + R_A[i]) \bmod N] = X_B[j][(b + R_A[j]) \bmod N]$

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 $X_A[i] \neq X_B[j]$. As $R_A \neq R_B$, there is at least one pair $(R_A[i], R_B[j])$ is distinct. As the related $X_A[i]$ is identical to $X_B[j]$, $X_A[i]$ is formed by pattern based on Theorem 1.1.

B Proof of Probability Computation

B.1 Proof of Theorem 1.4

B.2 Proof of Theorem 1.5