

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

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_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). 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

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 probability that two tags equal when their relative data parts are identical. This probability is expressed as $\Pr[\text{Tag Collision}]$ in this paper.

Y Set Collision Under Replay Attack

1.3 The Y Set Collision in Each Case Of Input

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