1 The Collision Probability of Y Set

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.

The Concept of Rotate Shifting 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.

The Behaviour of Rotate Shifting We can refer that the result of rotate shifting a message blk depends on the value of blk and the bits shifted.

1.2 Rotate Shifting and Y Set Collision

Y Set Collision This paragraph should introduce some simple examples of 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.

1.3 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