

1 Tag Frequency Diagrams

1.1 Experiment Setup

The Input Blocks of Tags In this experiment, the length of a input block, D , to CETD is 16 bits. The hexadecimal domain of D block is $[0x0000, 0xFFFF]$. The tag length is set to 8 bits, so the input block D is split into two sub-blocks D_a and D_b . Each sub-block has a length of 8 bits.

Our experiment simulate the replay attack. Using each distinct value in the domain of D as input to CETD, we generated 1000 tags. For the input of nonce for each tag, the following two principles is met:

- The counter is distinct
- The random number is randomly generated by PRF

Hence the block cipher we use in nonce generation is AES, each nonce in the 1000 times tag generation is randomly generated. We want to examine the distribution of distinct tag values for each distinct D block.

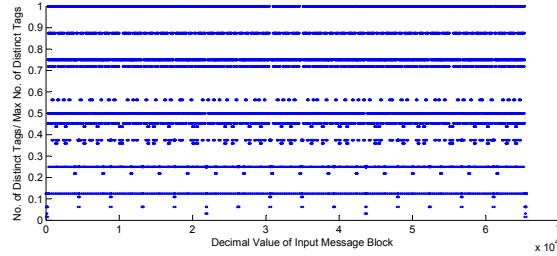


Figure 1: The tag value frequency diagram for all D blocks. Y axis expresses the frequency of tag values of a D value divided by the maximum frequency

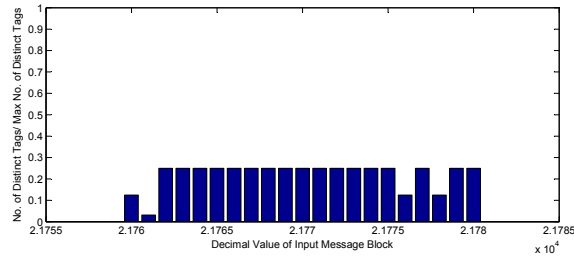


Figure 2: The tag value frequency diagram for a part of D blocks

1.2 The Results

The Frequency Diagram of All D Values The tag frequency diagram of all D values is expressed in Figure 1. From the figure we can see that the frequency of tag varies to different levels. Figure enlarge a part of Figure 1 to help clarify the tag frequency of each D block.

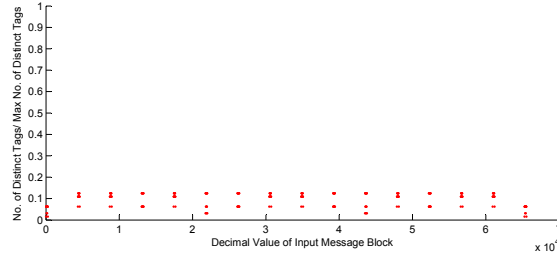


Figure 3: The tag value frequency diagram for D blocks formed by pattern sub-blocks.

The Frequency Diagram of D Values formed by Pattern Sub-blocks

As analyzed before, the tag has more probability to collide under replay attack if each sub-block of D is formed by a pattern. We found all the D values formed by two pattern sub-blocks. Figure 2 expresses the tag frequency values of these D blocks.

We can see that the tag frequency of all D blocks formed by pattern sub-blocks is small. These points on the Fig 3 exactly match the lowest points in Fig 1.