

1 Approach

Notation Let $\{0,1\}^n$ be the set of all n-bit binary strings. The set of all binary string is expressed as $\{0,1\}^*$. For a string $X \in \{0,1\}^n$, $|X|$ is its length in bits, and $|X|_l = \lceil |X|/l \rceil$ is the length of X in l-bit blocks. Let 0^l and 1^l denote bit strings of all zeros and all ones. For a bit string X and an integer l that $|X| \geq l$, $\text{msb}_l(X)$ denotes the most significant l bits(left most l bits) of X and $\text{lsb}_l(X)$ for least significant l bits(right most l bits) of X . For two bit string X and Y , we denote $X\|Y$ or XY as the their concatenation. For bit string X whose length in bits is multiple of integer l , we denote X parted into l-bit sub-strings as $X = (X[1]X[2] \dots X[n])_l$, where $X[1], X[2], \dots, X[n] \in \{0,1\}^l$. The number of bits in a string of X is denoted as $\text{len}(X)$.

The block cipher encryption of a string X with a secret key K is denoted as $E_K(X)$.

1.1 The MAC Scheme in Cost-Effective Tag Design

In this article, we name the MAC scheme adopted in Cost-Effective Tag Design[] CETD-MAC.

Shuffle Rounds, Input Length and Tag Length Let $E_K(X)$ be the block cipher encryption with secret key K and accepting X as input. We denote $\pi = E_K(X)$. Then $\pi: \{0,1\}^n \rightarrow \{0,1\}^n$.