1 Related Work Analysis

1.1 Tag Designs

A Cost-Effective Tag Design Tag Design Base: Original Base

Motivation: Create a tag design with minimum on-chip storage cost and use minimum No. of block encryption.

Approach: The operations used in CETD is bit segment swap and rotate shift. Bit segment swap is operated among all blocks; each round two blocks are picked and do the swap. The parameter of each round decides the indexes of blocks to swap, the index of start bit in each block and the segment length. Rotate shifting is operated in each block. The parameter of each block decide the shift bits. The parameters are segments on a nonce. The input of nonce generation is (addr, crt, rnd) tuple. For each tag, the tuple is distinct, then the nonce is random.

The Tag Size Selection: What is the purpose in real world application? Cost Effective?

The security: The design paper did not provide the systematically security evaluation. In this paper, our main motivation is analyzing the security of CETD under some specific attacks.

Improving Cost, Performance, and Security of Memory Encryption and Authentication Tag Design Base: GCM

Motivation:

Approach:

Performance:

Security: