Side-channel Analysis of Six SHA-3 Candidates

http://www.firstlight.cn 2010-08-20

In this paper we study six 2nd round SHA-3 candidates from a side-channel cryptanalysis point of view. For each of them, we give the exact procedure and appropriate choice of selection functions to perform the attack. Depending on their inherent structure and the internal primitives used (Sbox, addition or XOR), some schemes are more prone to side channel analysis than others, as shown by our simulations.

存档文本