CS641A

Modern Cryptology

Indian Institute of Technology, Kanpur

Date of Submission: June 15, 2020

Assignment

7

Instructions.

- This is a written assignment.
- Your answers should be precise and clearly written in LaTeX.

WECCAK (WEAK-KECCAK)

Consider a variant of KECCAK hash function which we will be called as WECCAK (WEAK-KECCAK). The following is the description of WECCAK.

1. Input to the hash function is a message $M \in \{0,1\}^*$.
2. M is padded with minimum number of zeros such that bit-length of padded message is a multiple of 184.
3. The padded message is divided into blocks of 184 bits. Let's call them $M_1, M_2, \ldots, M_r$.
4. A state in WECCAK hash function is a $5 \times 5 \times 8$ 3-dimensional array.
5. Initial state S contains all zeros.
6. The first mesage block M_1 is appended with 16 zeros to form M_1' and is XORed with S. (This procedure is similar to KECCAK).
7. This state is given as input to a function F (which will be defined later) and let's call its output as O_1. The output of F is also a $5 \times 5 \times 8$ 3-dimensional array.
8. The second message block M_2 is appended with 16 zeros to form M_2' and is XORed with O_1 and is given as input to F.
9. This is continued for r times.
10. The output of WECCAK is the initial 80 bits of O_r. (This is similar to KECCAK).
11. For more details on KECCAK, refer https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

Let $R = \chi \circ \rho \circ \pi \circ \theta$ (θ, ρ, π, χ are the same as defined in KECCAK). Please note that now in all operations z indices are modulo 8.

1. Compute the inverse of χ and θ.
2. Claim about the security of WECCAK with $F = R \circ R$. (Give a preimage, collision and second preimage attack).