CS641A Assignment-7

Sherlocked

Bholeshwar Khurana (170214) **Yaghyesh Chouhan (170813)** **Sarthak Dubey (180674)**

WECCAK (WEAK-KECCAK)

Let $R = \chi \circ \rho \circ \pi \circ \theta$ (same as defined in KECCAK).

1. Compute the inverse of χ and θ.
Computing the inverse of χ: [1]
If all output bits b_0, b_1, b_2, b_3, b_4 are known, then we can exactly determine the input bits a_0, a_1, a_2, a_3, a_4 using (χ^{-1}):

$$a_i = b_i \oplus (b_{i+1} \oplus 1).(b_{i+2} \oplus (b_{i+3} \oplus 1).b_{i+4})$$

Computing the inverse of θ: [2]
Computing the inverse of θ can be done by adopting a polynomial notation. The state can be respresented by a polynomial in the three variables x, y, z with binary coefficients. Here the coefficient of the monomial $x^i y^j z^k$ denotes the value of bit $a[i][j][k]$. The exponents i and j range from 0 to 4 and the exponent k ranges from 0 to $w-1$ (In our case $w = 8$). In this representation a translation $\tau[t_x][t_y][t_z]$ corresponds with the multiplication by the monomial $x^{t_x} y^{t_y} z^{t_z}$ modulo the three polynomials $1 + x^5$, $1 + y^5$ and $1 + z^w$. More exactly, the polynomial representing the state is an element of a polynomial quotient ring defined by the polynomial ring over GF(2)$[x, y, z]$ modulo the ideal generated by $\langle 1 + x^5, 1 + y^5, 1 + z^w \rangle$. A translation corresponds with multiplication by $x^{t_x} y^{t_y} z^{t_z}$ in this quotient ring. The z-period of a state a is d if d is the smallest nonzero integer such that $1 + z^d$ divides a. Let a' be the polynomial corresponding to the z-reduced state of a, then a can be written as

$$a = (1 + z^d + z^{2d} + ... + z^{w-d}) \times a' = \frac{1 + z^w}{1 + z^d} \times a'$$

When the state is represented by a polynomial, the mapping θ can be expressed as the multiplication (in the quotient ring defined above) by the following polynomial:

$$1 + \bar{y}(x + x^4 z) \text{ with } \bar{y} = \sum_{i=0}^{4} y^i = \frac{1 + y^5}{1 + y} \tag{1}$$

The inverse of θ corresponds with the multiplication by the polynomial that is the inverse of polynomial (1). For our case $w = 8$. We assume the inverse is of the form $1 + \bar{y}Q$ with Q a polynomial in x and z only:

$$(1 + \bar{y}(x + x^4 z)) \times (1 + \bar{y}Q) = 1 \mod \langle 1 + x^5, 1 + y^5, 1 + z^8 \rangle$$

We can solve the equation using SAGE.
The Hamming weight of the polynomial of θ^{-1} is of the order $b/2$.

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

Preimage attack:
We have found the inverse of χ and θ, the other two operations ρ and π are linear and hence invertible. This implies that F is invertible, as a result R is invertible. For preimage attack, we know the the first

80 bits of the output. We can vary the remaining 120 bits till we get an x such that the last 16 bits of $F^{-1}(x)$ are 0. Now the first 184 bits of $F^{-1}(x)$ are the preimage of the initial 80 bits given. This way we can do the preimage attack.

Second-preimage attack:
We can deduce second preimage attack on similar grounds as the first preimage attack.

Collision attack:
We can do collision attack on WECCAK by choosing two inputs which will provide the same first 80 bits on applying F. We can choose 2^{40} plain texts from birthday problem and can do the collision attack.

REFERENCES:

[1] Kumar R., Rajasree M.S., AlKhzaimi H. (2018) Cryptanalysis of 1-Round KECCAK. In: Joux A., Nitaj A., Rachidi T. (eds) Progress in Cryptology – AFRICACRYPT 2018. AFRICACRYPT 2018. Lecture Notes in Computer Science, vol 10831. Springer, Cham

[2] The KECCAK-reference: https://keccak.team/files/Keccak-reference-3.0.pdf

[3] Wikipedia