CS381 Exercise 5

Name: Zhang Yupeng

Student ID: 5130309468

1. Prove the low-high algorithm for computing $\odot$

Proof:

We define that $a\%b$ is equal to a mod b.

The low-high algorithm for computing $\odot$ is:

$$ab\%(2^n+1) = \begin{cases} ab\%2^n - ab/2^n & ,ab\%2^n \geq ab/2^n \\ ab\%2^n - ab/2^n + 2^n + 1 & ,ab\%2^n < ab/2^n \end{cases}$$

The $ab\%2^n$ corresponds the lower n bits of ab.

The $ab/2^n$ corresponds the higher n bits of ab.

Let $ab = q(2^n+1) + r = \begin{cases} q2^n + (q+r) & ,q+r < 2^n \\ (q+1)2^n + (q+r-2^n) & ,q+r \geq 2^n \end{cases}$

First, when $q+r < 2^n$, $ab/2^n = q$, $r+q = ab - q2^n$, $r = ab - q2^n - q$

That is, $r = ab\%2^n - ab/2^n$

Next, when
$q+r \geq 2^n, ab/2^n = q+1, q+r-2^n = ab-(q+1)2^n, r = ab-(q+1)2^n-(q+1)+2^n+1$

That is, $r = ab\%2^n - ab/2^n + 2^n + 1$

So, we prove the low-high algorithm for computing $\odot$

2. Prove that the In-structure in IDEA is an involution.

Proof:

From the figure following we can see that the input of In-structure is $K_1, \ldots K_4$, and the input of MA-structure is $a = K_1 \oplus K_3$ and $b = K_2 \oplus K_4$, and the output of MA-structure is c and d.

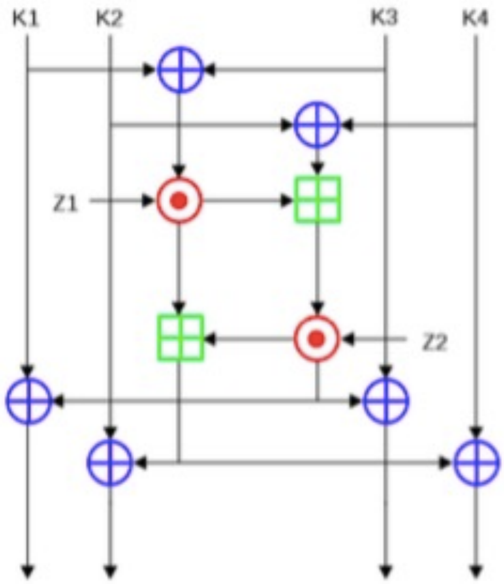

Figure 1: In-structure

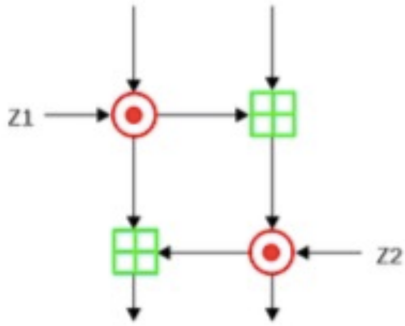

Figure 2: MA-structure

Then, we can see that after one In-structure operation, the output is:

$$K_1' = K_1 \oplus d$$

$$K_2' = K_2 \oplus c$$

$$K_3' = K_3 \oplus d$$

$$K_4' = K_4 \oplus c$$

In the second round of In-structure operation, the input of the second MA-structure will be:

$$a' = K_1' \oplus K_3' = K_1 \oplus d \oplus K_3 \oplus d = K_1 \oplus K_3$$

$$b' = K_2 \oplus K_4$$

So, the output of the second MA-structure is still c and d.

Therefore, the output of the second In-structure will be:

$$K_1'' = K_1' \oplus d = K_1 \oplus d \oplus d = K_1$$

$$K_2'' = K_2$$

$$K_3'' = K_3$$

$$K_4'' = K_4$$

So, we've proved that the In-structure is involution.