Crypto Engineering TP — Generic second preimage attacks on long messages for narrow-pipe Merkle-Damgard hash functions

Barrois. F, Duverney. T

[2018-11-13 mar.]

1 Part one: Preparatory work

1.1 Question 1

For this function, we based our implementation on the following representation:

As the function takes as input a 48-bit message and a key of 96 bits, the values α and β are respectively set to 8 and 3. So $S^{-\alpha}$ performs a circular shift of 8 bits to the right, thus it can be done using $\text{ROTL24}_{16}()$ since this function shifts a value of 16 bits to the left, which is the same as shifting it of 8 bits to the right over 24bits. Similarly, S^{β} proceeds to a circular shift of 3 bits to the left and is implemented via a call to $\text{ROTL24}_{3}()$.

Besides, the only difficulty here lies in the order of the operations. According to the picture above, we firstly do the shift on p[1], then we perform the modular addition with p[0]. Afterwards, we xor p[1] to the key value associated to the current iteration, and finally p[0] is updated by the circular shift and the obtained value is xored to p[1].

1.2 Question 2

The $\text{speck48}_{96\text{inv}}$ process only consists in performing almost the same operations in the reverse order. There exists a few differences though:

- Because we want to invert the ciphering process, we need to apply $S^{-\beta}$ on c[0] so we call $\text{ROTL24}_{21}()$ (21 being the complement of 3 to 24), and symmetrically, we use $\text{ROTL24}_{8}()$ for S^{α} on c[1].

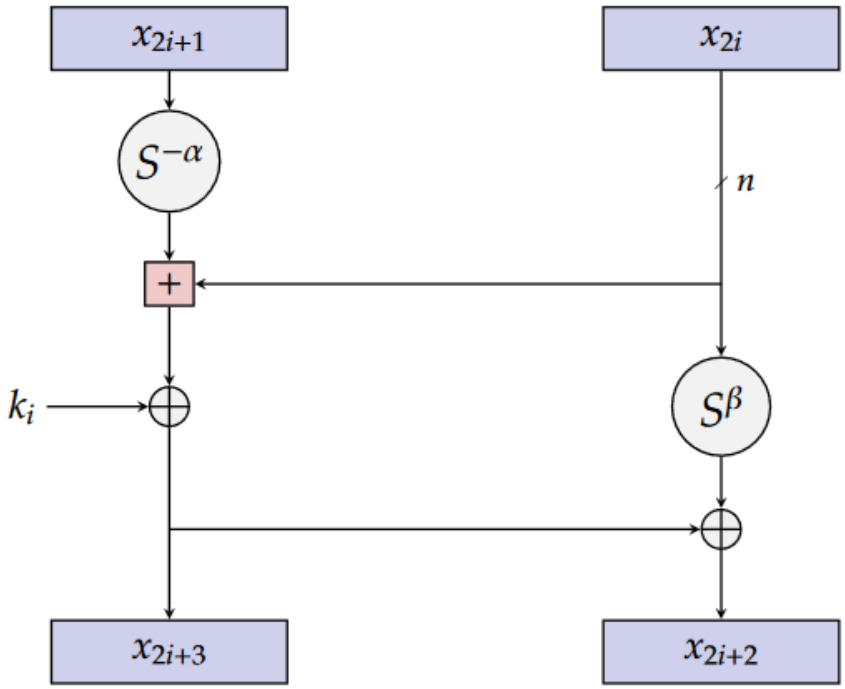

Figure 1: SPECK round function

- As a modular addition is done during the ciphering, in the case where the value of the modulo was reached, computing the substraction from the cipher will not give back then original value. In order to bypass this case, we add the value of the modulo before computing the substraction so that in any case the obtained value for c[1] will be such that 0 <= c[1] < modulo.

Remark: Actually, the value is stored in an unsigned integer so the potential negative values due to the modular operation would be arranged to the right range of values, but we left the addition with the modulo value as it would be useful in a general case with a different implementation.

2 Part two: The attack

If $a^2 = b$ and $b = 2$, then the solution must be either

$$a = +\sqrt{2}$$

or

$$a = -\sqrt{2}$$

.