Implementation of SPECK 2n/mn

Project of

Security of Computer and Embedded systems

Lecturer: Prof. Dr. Elif Bilge Kavun

Exchange student: Farzaneh Arzaghi

Winter sem 20/21

Implementation of SPECK 128/128

According to the table below we can determine the cipher block's parameters.

block size $2n$	key size mn	word size n	key words m	rot α	rot β	rounds T
32	**64**	16	4	7	2	22
48	**72**	24	3	8	3	22
	96		4			23
64	**96**	32	3	8	3	26
	128		4			27
96	**96**	48	2	8	3	28
	144		3			29
128	**128**	64	2	8	3	32
	192		3			33
	256		4			34

Table 4.1: SPECK parameters.

Specify parameters:

block size $(2n) = 128$

key size $(mn) = 128$

word size $(n) = 64$

key words $(m) = 2$

rot $(\alpha) = 8$

rot $(\beta) = 3$

Rounds $(T) = 32$

Key Schedules:

The SPECK key schedules generate round keys k_i.

K is a key for SPECK 2n block cipher. we can write $K = (L_{m-2}, \ldots, L_0, k_0)$

m can be $\{2, 3, 4\}$.

If we have
$$\begin{cases} m = 2 \longrightarrow K = (L_0, k_0) \\ m = 3 \longrightarrow K = (L_1, L_0, k_0) \\ m = 4 \longrightarrow K = (L_2, L_1, L_0, k_0) \end{cases} \Longrightarrow$$

we use k_0 for the first round key then use $k_0, L_0, \ldots L_{m-2}$ and the formula below to generate $k_1, k_2, \ldots$ for the rest of the rounds

In this question we have $m=2$ and $K=(L_0,k_0) \longrightarrow K$ is an input

sequaces k_i and L_i are defined by:

$$\begin{cases} L_{i+m-1} = (k_i + S^{-\alpha} L_i) \oplus i \\ k_{i+1} = S^{\beta} k_i \oplus L_{i+m-1} \end{cases}$$

- The value k_i is the ith round key, for $0 \leqslant i < \underline{T-1}$

  always we have k_0 in all versions so we need to generate just $T-1$ keys

- $+$ is addition modulo 2^n
- left circular shift, S^j, by j bits
- right circular shift, S^{-j}, by j bits

In this question: $0 \leqslant i < \underbrace{32-1}_{=31}$

$m=2$

$K=(L_0,k_0)$

$\alpha=8$

$\beta=3$

$\xrightarrow[i=0]{\text{For Example}}$ $L_1 = (k_0 + S^{-8} L_0) \oplus 0$

$k_1 = S^3 k_0 \oplus L_1$

$\xrightarrow[i=1]{\text{another Example}}$ $L_2 = (k_1 + S^{-8} L_1) \oplus 1$

$k_2 = S^3 k_1 \oplus L_2$

$\vdots$

$\xrightarrow{i=30}$ $L_{31} = (k_{30} + S^{-8} L_{30}) \oplus (30)_2$

$k_{31} = S^3 k_{30} \oplus L_{31}$

all the keys generate $\{k_{31}, k_{31}, \dots k_2, k_1, k_0\}$

For computing L_1: L_0 is circular shifted right by eight (S^{-8}) then the result is added with k_0 (OR XORed with k_0 because we have addition modulo 2^n) finally the result XORed with i.

For computing k_1: k_0 is circular shifted left by three (S^3) then the result XORed with L_1 that we computed in the previous step.

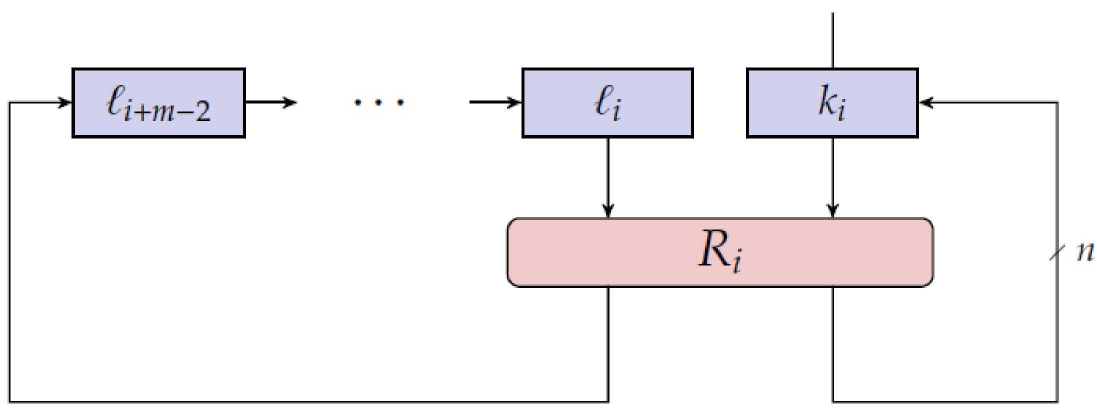


Figure 4.3: SPECK key expansion, where R_i is the SPECK round function with i acting as round key.

Round Function:

The SPECK 2n encryption maps make use of the following operations on n-bit words:

- bitwise XOR ($\oplus$)
- addition modulo 2^n ($+$)
- left and right circular shifts, S^j and S^{-j}, respectively, by j bits.

Key-dependent SPECK 2n round function defined by:

$$R_k(x,y) = ((S^{-\alpha}x + y) \oplus k,\ S^{\beta}y \oplus (S^{-\alpha}x + y) \oplus k)$$

for this question: $m = 2$, $\alpha = 8$, $\beta = 3$ $\longrightarrow R_k(x,y) = ((S^{-8}x + y) \oplus k,\ S^{3}y \oplus (S^{-8}x + y) \oplus k)$

- k is a round key
- x is the leftmost word of the cipher block
- y is the right most word

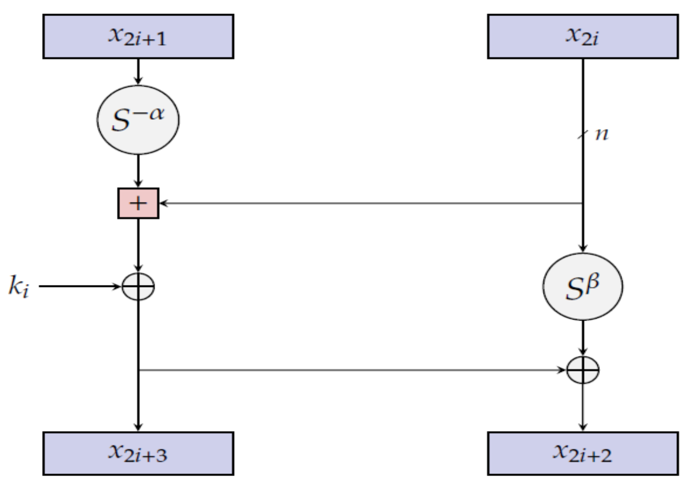
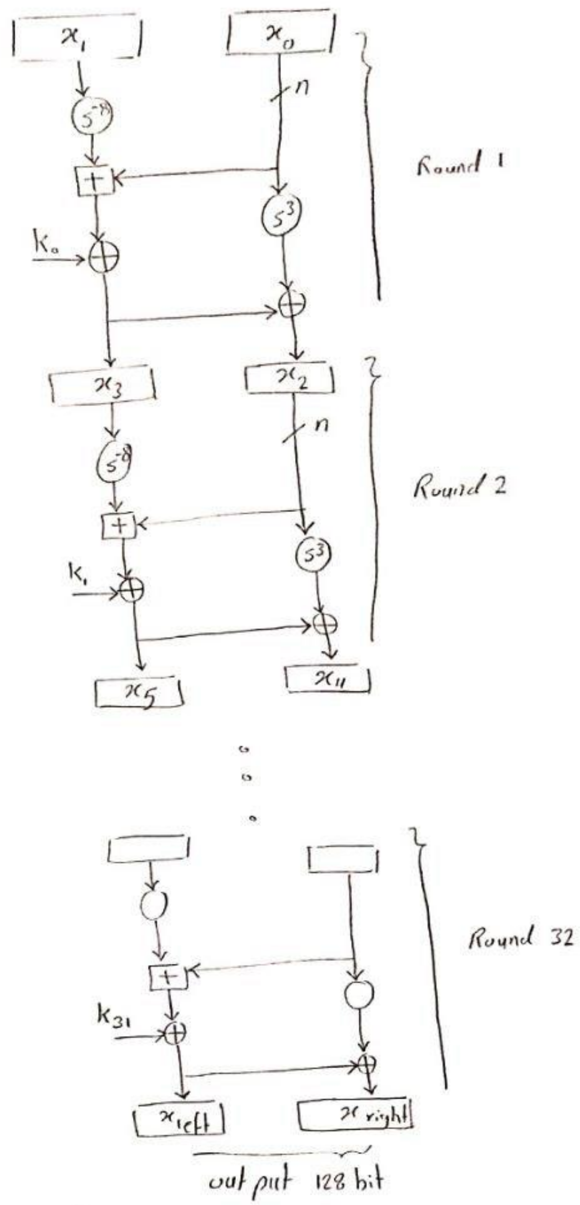


Figure 4.1: SPECK round function; (x_{2i+1}, x_{2i}) denotes the subcipher after i steps of encryption.

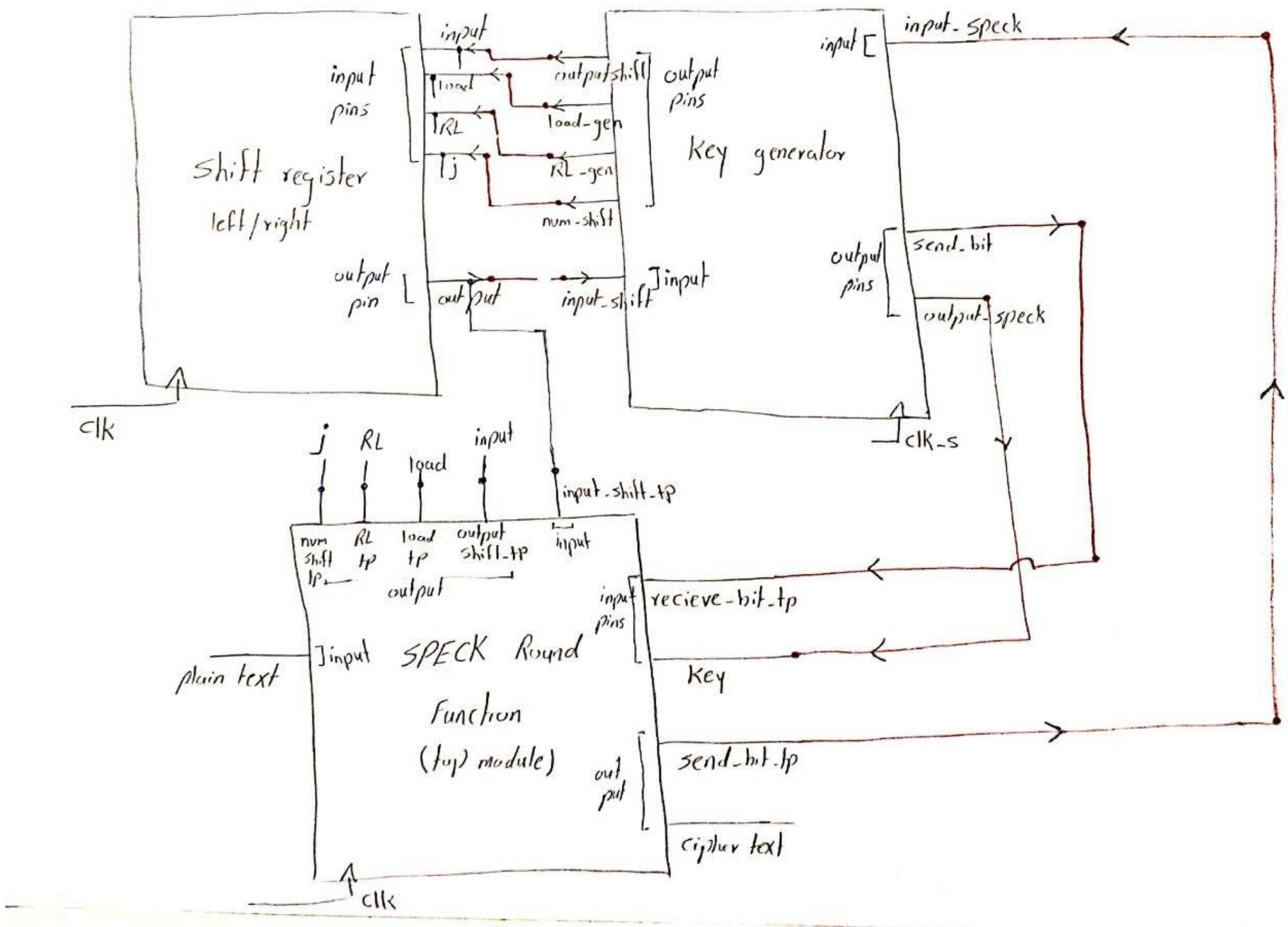


Note that SPECK can be realized as the composition of two Feistel-like maps with respect to two different types of addition, namely,

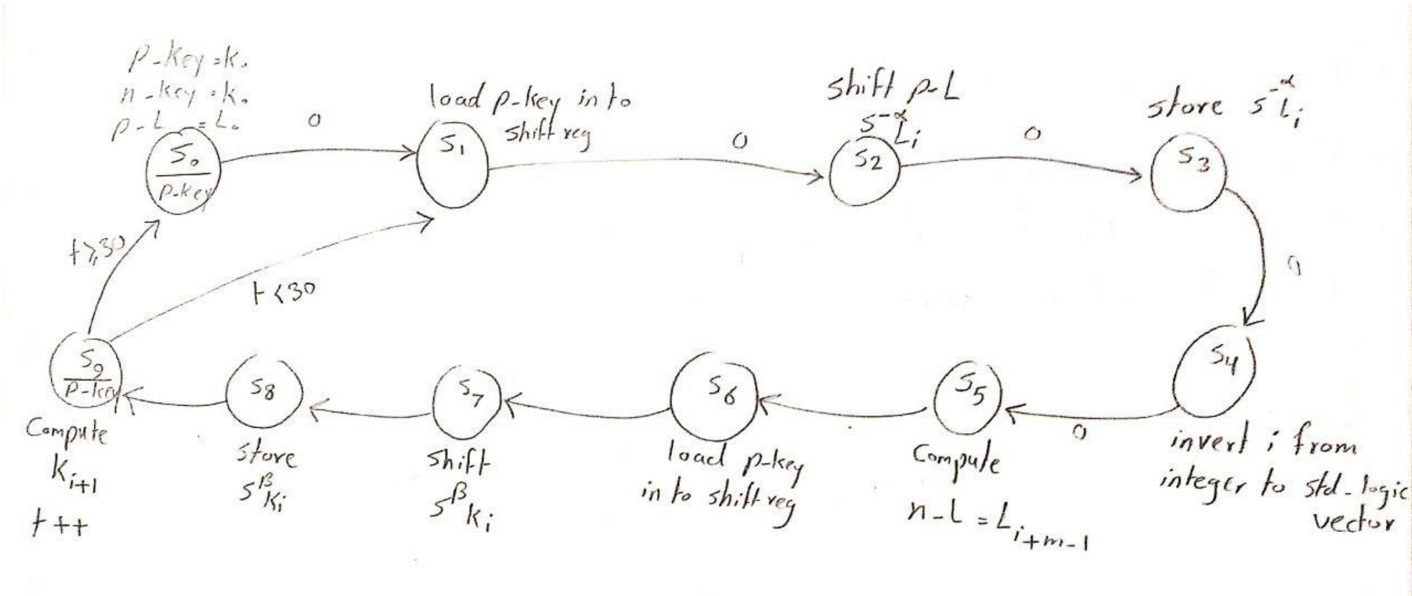
$$(x,y) \to (y, (S^{-\alpha}x + y) \oplus k) \quad \text{and} \quad (x,y) \to (y, S^{\beta}x \oplus y)$$

Code

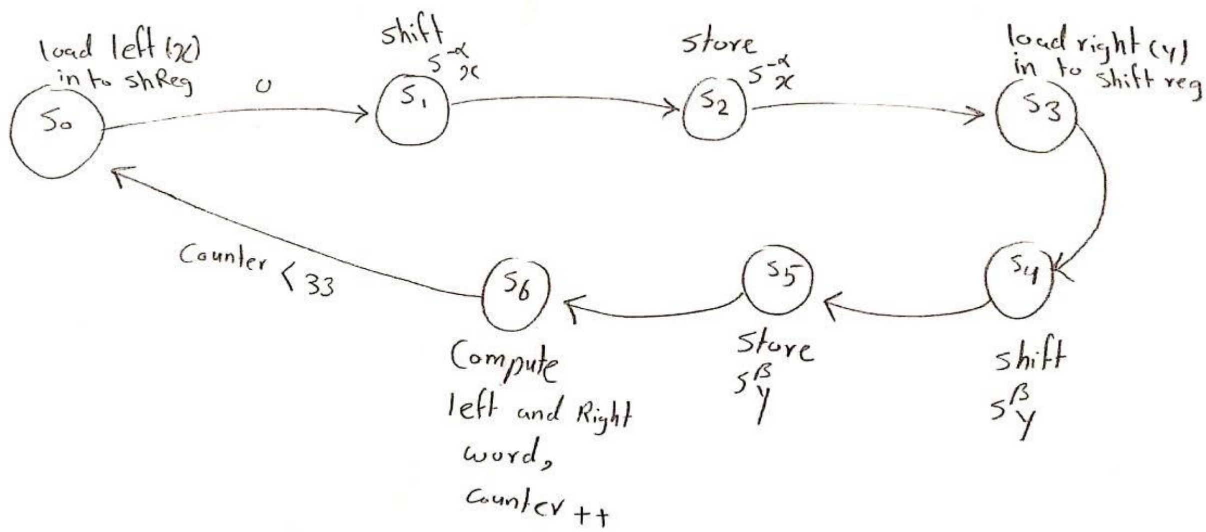
Block diagram



Key generator state machine:



SPECK function state machine:



References

Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., and Wingers, L. (2013). The SIMON and SPECK families of lightweight block ciphers. *cryptology eprint archive*.

Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., and Wingers, L. (2015). SIMON and SPECK: Block Ciphers for the Internet of Things. *Cryptology ePrint Archive*.