KU LEUVEN

Imec-COSIC, ESAT

On the SNOW Stream Ciphers

Liliya Kraleva and Chaoyun Li
liliya.kraleva@esat.kuleuven.be

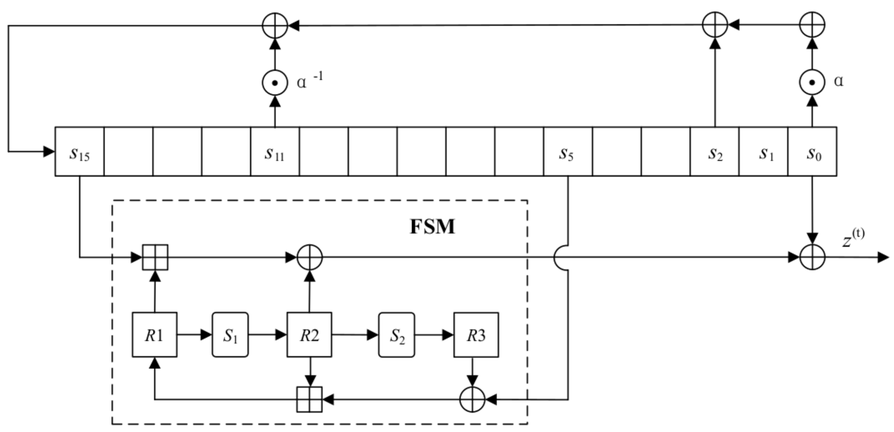

Figure 1: Diagram of the keystream mode of SNOW 3G

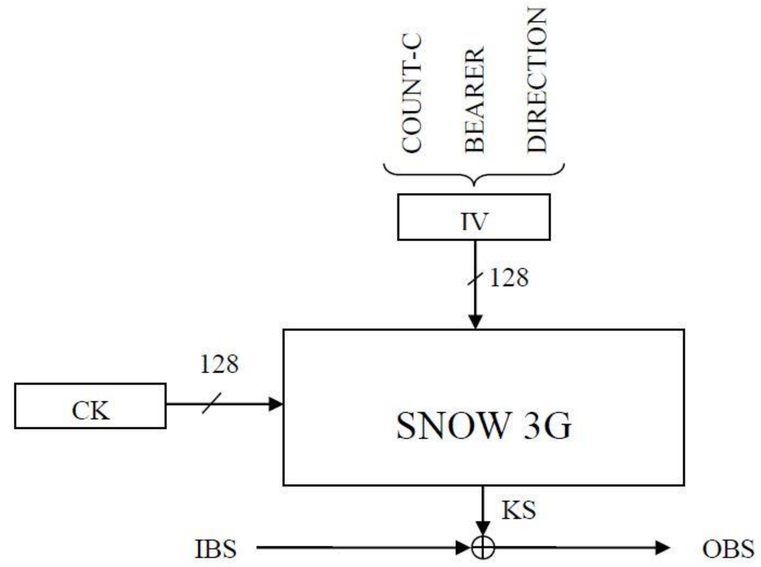

Figure 2: Diagram of UAE2:

SNOW 3G is the core of the UEA2 & UIA2 algorithms of the 3GGP.

1. Differential attacks revisited

Table 1: The propagation of the difference a for SNOW 3G/2.0, where (s_{15}, z) and $(s_{15}*, z^*)$ are based on Algorithms 1 and 2 respectively, and $a = 0x80000000; b = 80800000; c = ??000000; d = ??800000; e = ??000000; f = ??800000; g = ??008000; h = ????8000; i = ????0000; j = ????AA; k, l =$ unknown.

r	s0	s1	s2	s3	s4	s5	s6	s7	s8	s9	s10	s11	s12	s13	s14	s15	s15*	R1	R2	R3	z	z^*
SNOW 3G																						
11	0	0	0	0	a	a	a	a	a	b	c	d	e	f	g	h	00??8000	a	0	0	????8000	$????(A \oplus 0x80)A$
12	0	0	0	a	a	a	a	a	b	c	d	e	f	g	h	i	00??0000	a	$\Delta S_1(a)$	0	????AA	?
13	0	0	a	a	a	a	a	b	c	d	e	f	g	h	i	j	8???8000	$\Delta(a+\Delta S_1(a))$	$\Delta S_1'(a)$	$\Delta S_2 S_1(a)$	?	?
14	0	a	a	a	a	a	b	c	d	e	f	g	h	i	j	k	80????80	$\Delta((a \oplus S_2 S_1(a)) + R_2^{13})$	$\Delta S_1(a+S_1(a))$	$\Delta S_2 S_1'(a)$	?	?
15	a	a	a	a	a	b	c	d	e	f	g	h	i	j	k	l	d0????17	$\Delta((a \oplus S_2 S_1'(a)) + R_2^{14})$	$\Delta S_1(R_1^{14})$	$\Delta S_2(R_2^{14})$	?	?
SNOW 2.0																						
11	0	0	0	0	a	a	a	a	a	b	c	d	e	f	g	h	00??8000	a	0	-	????8000	$????(A \oplus 0x80)A$
12	0	0	0	a	a	a	a	a	b	c	d	e	f	g	h	i	00??0000	a	$\Delta S_1(a)$	-	????AA	?
13	0	0	a	a	a	a	a	b	c	d	e	f	g	h	i	j	8???8000	$\Delta(a+\Delta S_1(a))$	$\Delta S_1'(a)$	-	?	?
14	0	a	a	a	a	a	b	c	d	e	f	g	h	i	j	k	80????80	$\Delta(a+\Delta S_1'(a))$	$\Delta S_1(\Delta(a+\Delta S_1(a))$	-	?	?
15	a	a	a	a	a	b	c	d	e	f	g	h	i	j	k	l	d0????17	$\Delta(b+\Delta S_1(a+S_1(a)))$	$\Delta S_1(\Delta(a+\Delta S_1'(a))$	-	?	?

2. Analyze the DDTs of some compositions of Sboxes

$$DDT[X', Y'] = \#\{X \mid S(X + X') - S(X) = Y'\}$$

Table 2: Shows the possible number of output values for the last byte of some Sbox combinations, a=0x800000.

Sbox	Possible values
$\Delta S_1(a)$	127
$\Delta S_1(a) \oplus \Delta S_1'(a)$	~31
$\Delta S_2 S_1(a)$	126
$\Delta S_1(a) \oplus \Delta S_2 S_1(a)$	~24

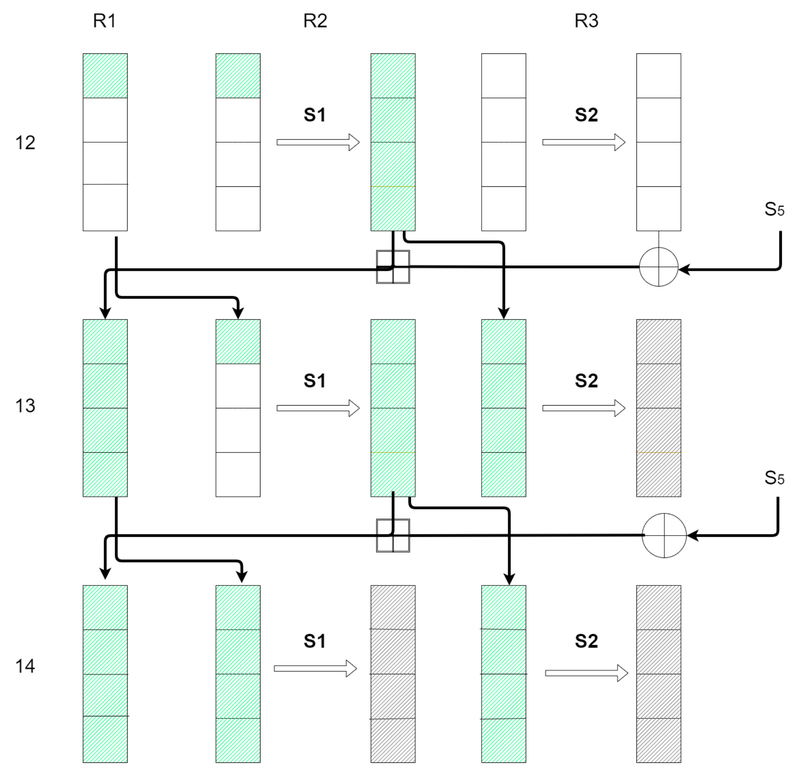

Figure 3:How the Sboxes are activated for 3 consecutive rounds, when $IV' = IV \oplus 0x800000$

3. Count the number of active Sboxes

Over two rounds of SNOW 2.0 we have at least 5 active Sboxes starting from 2 rounds after the difference enters the FSM, unless the difference is canceled locally. For SNOW 3G we have at least 10 active Sboxes.

Future work

- Extend the analysis of Sbox compositions
- Attack UAE2 by using the SNOW keystream differences

References:
[1]Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2.Document 2:SNOW3G Specification, 2006. https://www.gsma.com/aboutus/wp-content/uploads/2014/12/snow3gspec.pdf
[2] S. Ma, J. Guan: "Differential attacks on reduced-round SNOW 3G and SNOW 3G(+)",IET Inf. Secur., 14(5):587–594, 2020
[3] J. Daemen, V. Rijmen: "The Design of Rijndael: AES - The Advanced EncryptionStandard", Information Security and Cryptography, Springer 2002