Lecture 12: Stream ciphers in practice

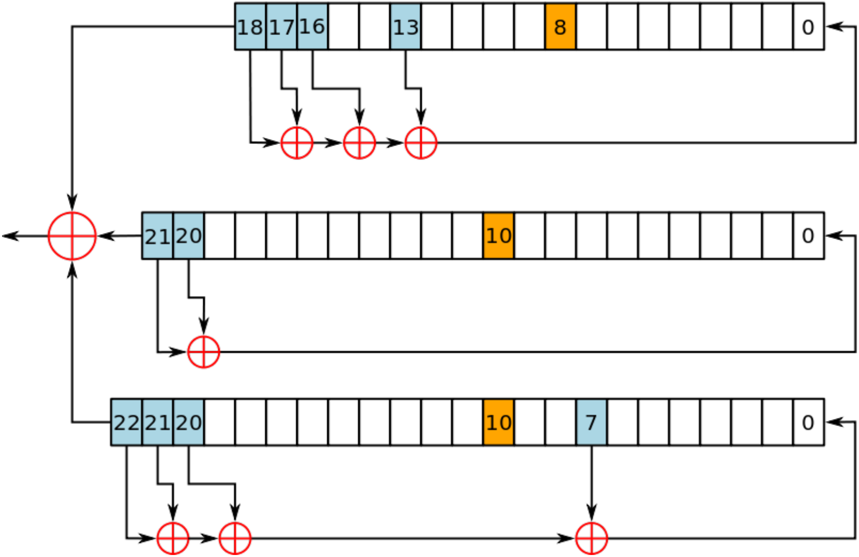
Thomas Johansson

The stream cipher A5/1

- A5/1 is a stream cipher used to provide over-the-air communication privacy in the GSM cellular telephone standard.
- It was initially kept secret, but became public knowledge through leaks and reverse engineering.
- A5/1 is used in Europe and the United States. A5/2 was a deliberate weakening of the algorithm for certain export regions
- developed in 1987

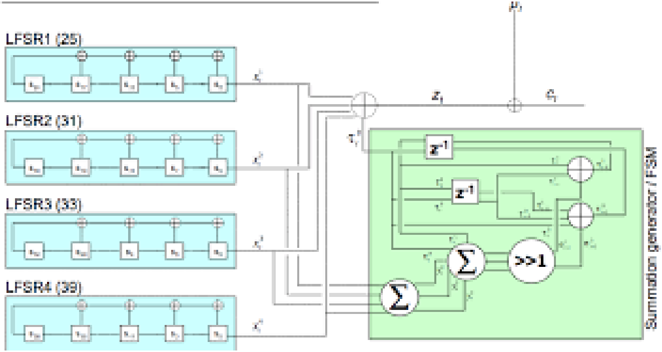
A GSM transmission and A5

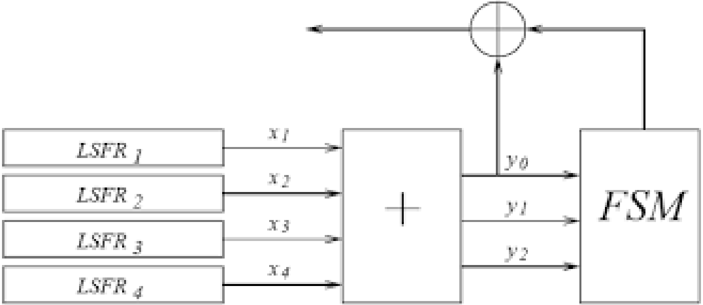
- One burst contains 114 bits available for information.
- A5/1 is used to produce for each burst a 114 bit sequence of keystream which is XORed with the 114 bits prior to modulation.
- A5/1 is initialised using a 64-bit key together with a publicly known 22-bit frame number.


18
17
16
13
8
0
21
20
10
0
22
21
20
10
7
0

The stream cipher E0 used in Bluetooth

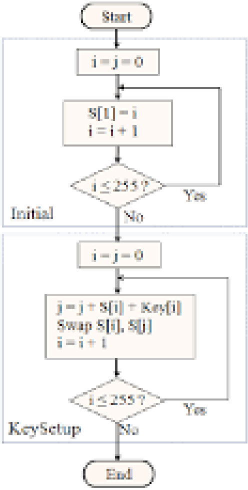
- E0 is a stream cipher used in the Bluetooth protocol.
- The key length may vary, but is generally 128 bits.
- uses four shift registers of differing lengths (25, 31, 33, 39 bits) and two internal states, each 2 bits long.
- The setup: An initial 132-bit state is produced at the first stage using four inputs (the 128-bit key, the Bluetooth address on 48 bits and the 26-bit master counter). The output is then processed by a polynomial operation and the resulting key goes through the second stage, which generates the stream used for encoding.


LFSR1 (25)
LFSR2 (31)
LFSR3 (33)
LFSR4 (39)
z_t
μ_t
c_t
z^{-1}
z^{-1}
Σ
Σ
>>1
Summation generator / FSM

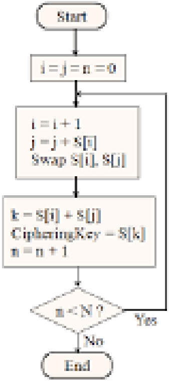

x_1
x_2
x_3
x_4
LSFR 1
LSFR 2
LSFR 3
LSFR 4
+
y_0
y_1
y_2
FSM

The stream cipher RC4

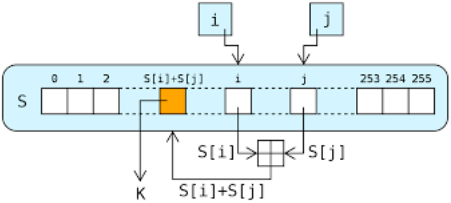
- RC4 is the most widely used software stream cipher and is used in popular protocols such as SSL, WEP, WPA.
- RC4 was designed by Ron Rivest of RSA Security in 1987.
- RC4 was initially a trade secret, but in September 1994 a description of it was leaked.


Start
i = j = 0
S[i] = i
i = i + 1
i ≤ 255 ?
Yes
No
Initial
i = j = 0
j = j + S[i] + Key[i]
Swap S[i], S[j]
i = i + 1
i ≤ 255 ?
Yes
No
KeySetup
End

KSA

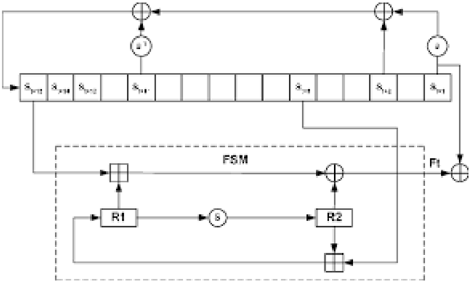

Start
i = j = n = 0
i = i + 1
j = j + S[i]
Swap S[i], S[j]
k = S[i] + S[j]
CipheringKey = S[k]
n = n + 1
n < N ?
Yes
No
End

PRGA

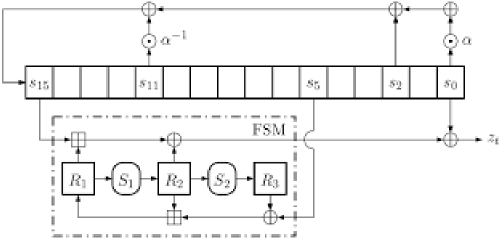

i
j
S
0
1
2
S[i]+S[j]
i
j
253
254
255
S[i]
S[j]
K
S[i]+S[j]

The SNOW stream ciphers

- Design from Lund University.
- SNOW 2.0 is an ISO standard.
- SNOW 3G is used in UMTS and LTE standards.



α^{-1}
α
s_{t+15}
s_{t+14}
s_{t+13}
s_{t+11}
s_{t+5}
s_{t+2}
s_t
FSM
Ft
R1
S
R2



α^{-1}
α
s_{15}
s_{11}
s_5
s_2
s_0
FSM
z_t
R_1
S_1
R_2
S_2
R_3