



Grain

A Stream Cipher For Constrained Environments

Martin Hell, Thomas Johansson

Lund University, Sweden

{martin,thomas}@it.lth.se

Willi Meier

FH Aargau, Switzerland

meierw@aargau.ch



Motivation

- There is a need for a **secure** stream cipher that is small in hardware
- RFID tags
- A5/1 and E0 have been broken
- ECRYPT stream cipher project – profile 2 hardware



Design idea

- Bit oriented
- LFSR based
- 80 bit key, 160 bit memory
- Small additional functions
- Possibility to increase speed at expense of extra hardware

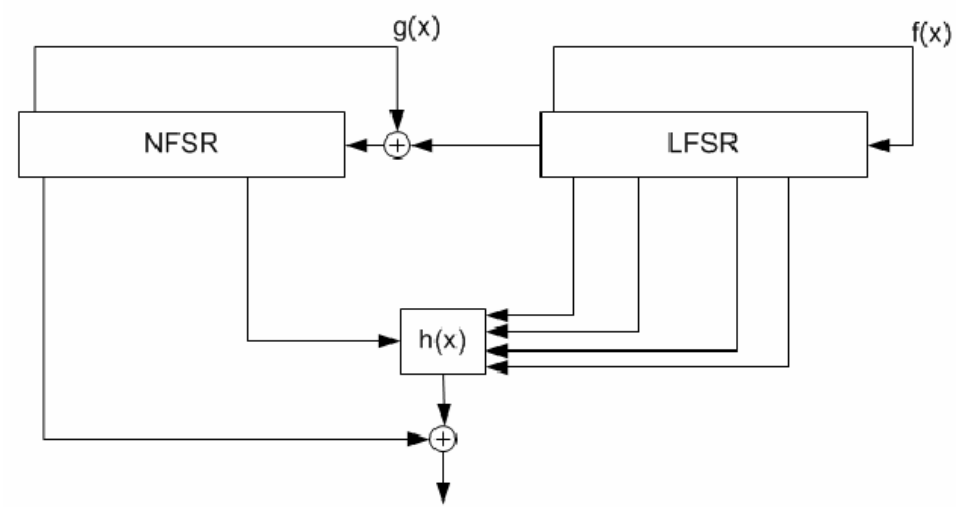
Design details

3 main parts

- 80 bit LFSR
- 80 bit NFSR
- Nonlinear filter

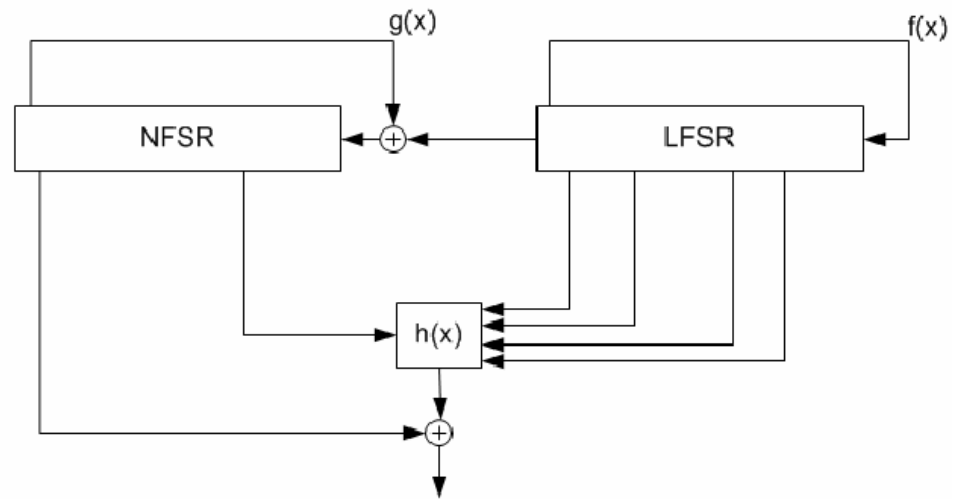
Input to NFSR xored with a LFSR bit.

Output xored with a NFSR bit.



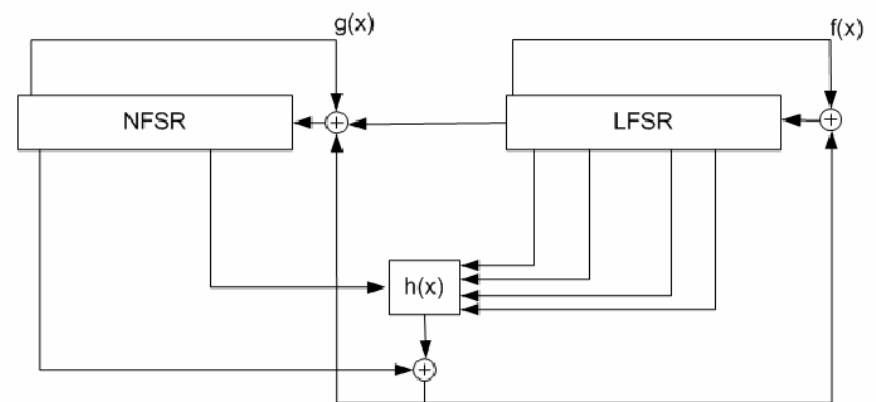
Design details

- LFSR feedback, $f(x)$
 - Primitive, weight 7
 - Guarantees minimum period of 2^{80}
- NFSR feedback, $g(x)$
 - 11 variables, max degree 6
 - One term occurs linearly
- Filter function, $h(x)$
 - 5 variables
 - Balanced
 - 1-CI (1-resilient)
 - Nonlinearity 12



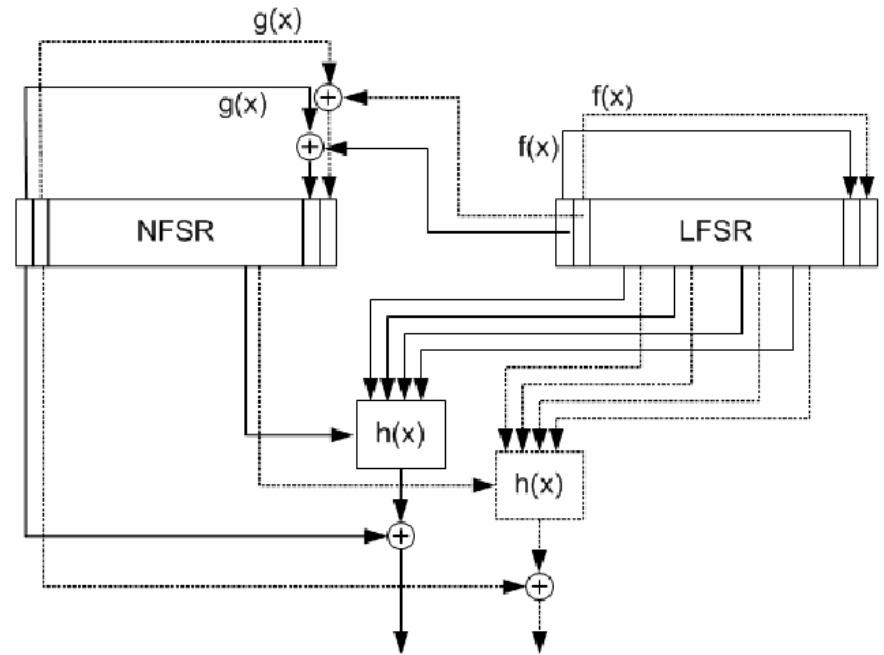
Key initialization

1. Put 80 bit key in NFSR
2. Put 64 bit IV in LFSR
3. Add ones to end of LFSR
4. Feed output of generator to the input of LFSR and NFSR
5. Clock 160 times



Increase speed

- Repeat filter and feedback functions
- Functions relatively small in hardware
- Memory is the main cost in hardware, but does not have to be repeated
- 15 rightmost cells not used in filter or feedback
- Easy to increase the speed up to 16 times original speed

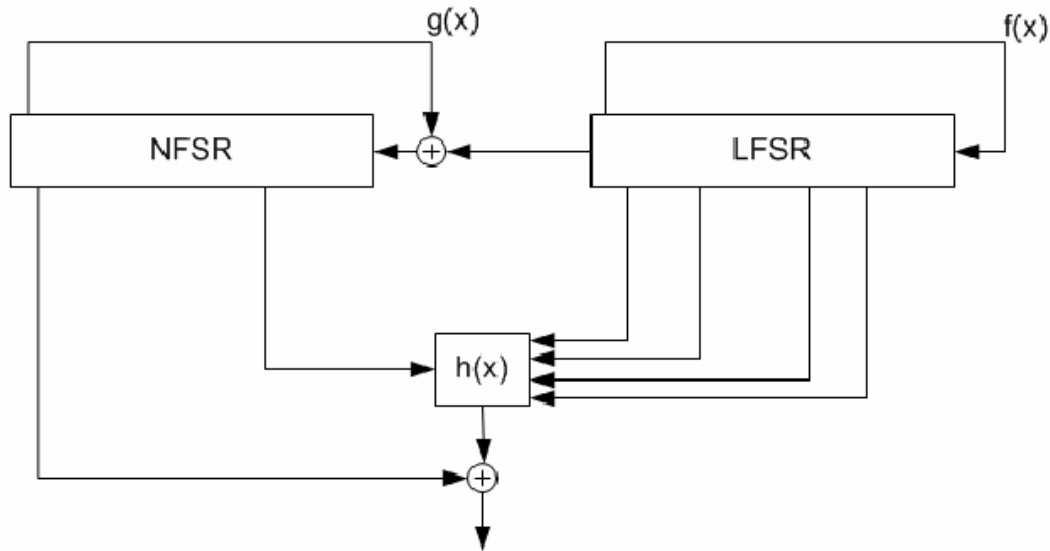


Hardware complexity

- Memory responsible for most gate count.
- Gate count for a function is not a natural constant, we chose 8 for D-flip flop.
- Gate count and throughput for Grain: (speed increased t times)

t	Gate Count	Throughput		
		MAX 3000A	MAX II	Cyclone
1	1435	49 Mbit/s	200 Mbit/s	282 Mbit/s
2	1607	98.4 Mbit/s	422 Mbit/s	576 Mbit/s
4	1950	196 Mbit/s	632 Mbit/s	872 Mbit/s
8	2636	240 Mbit/s	1184 Mbit/s	1736 Mbit/s
16	4008	-	2128 Mbit/s	3136 Mbit/s

Cryptanalysis



- Correlation attack
- Algebraic attack
- Time/Memory/Data tradeoff

- Chosen-IV attack
- Fault attack



Conclusion

- Bit oriented stream cipher targeting a small hardware implementation
- Keysize 80 bits
- Gate count is 1435 in its simplest implementation
- Possibility to increase speed at cost of extra hardware