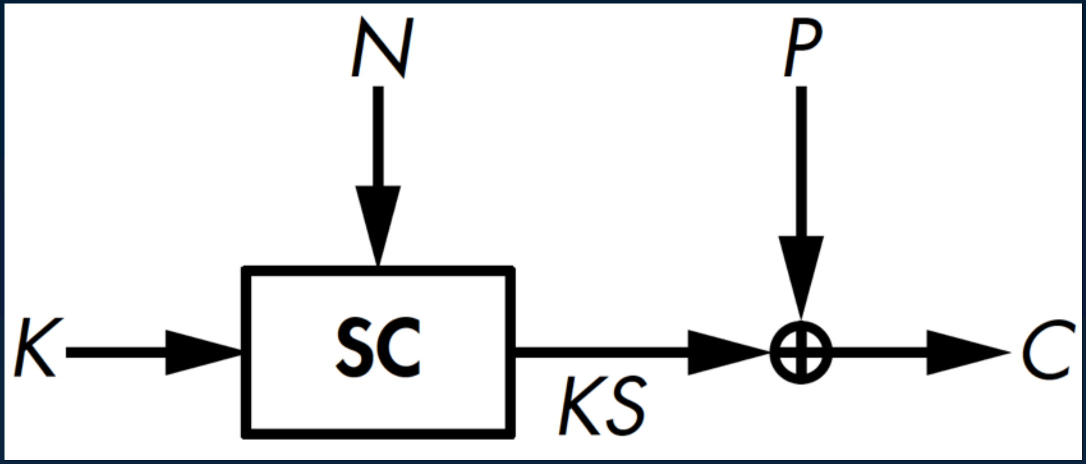
Applied Cryptography
CPEG 472/672
Lecture 4B

Instructor: Nektarios Tsoutsos

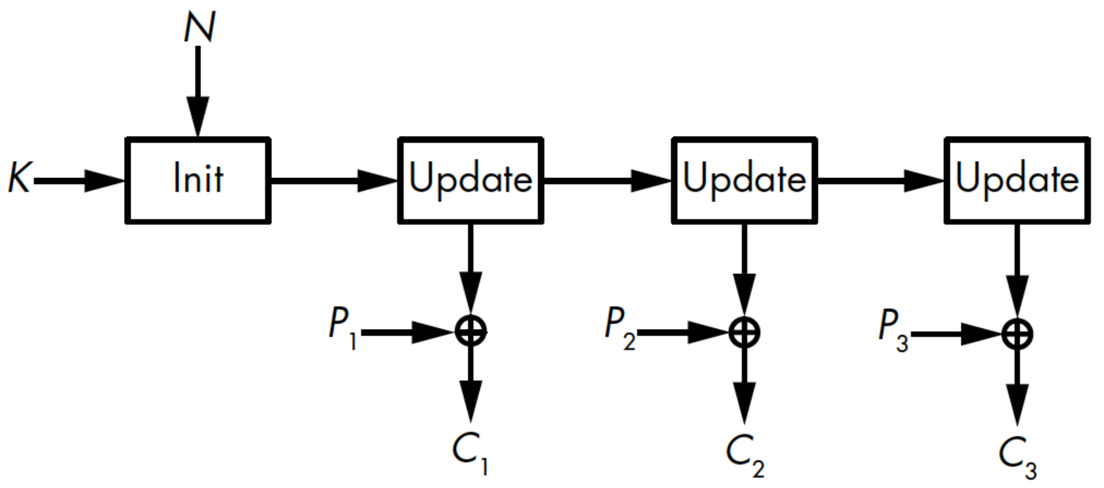
Stream Ciphers (SC)

- Similar to DRNGs
- Generate pseudorandom bits (keystream) and XOR it with plaintext
  - Uses a key K and a nonce N
  - C = P XOR KS   P=C XOR KS
  - New nonce per message when K is the same

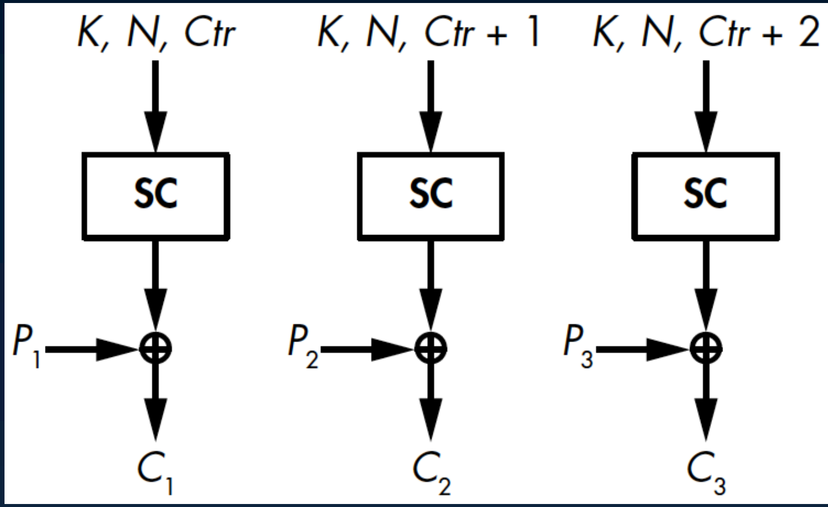


SC Types

- Stateful



- Counter-based

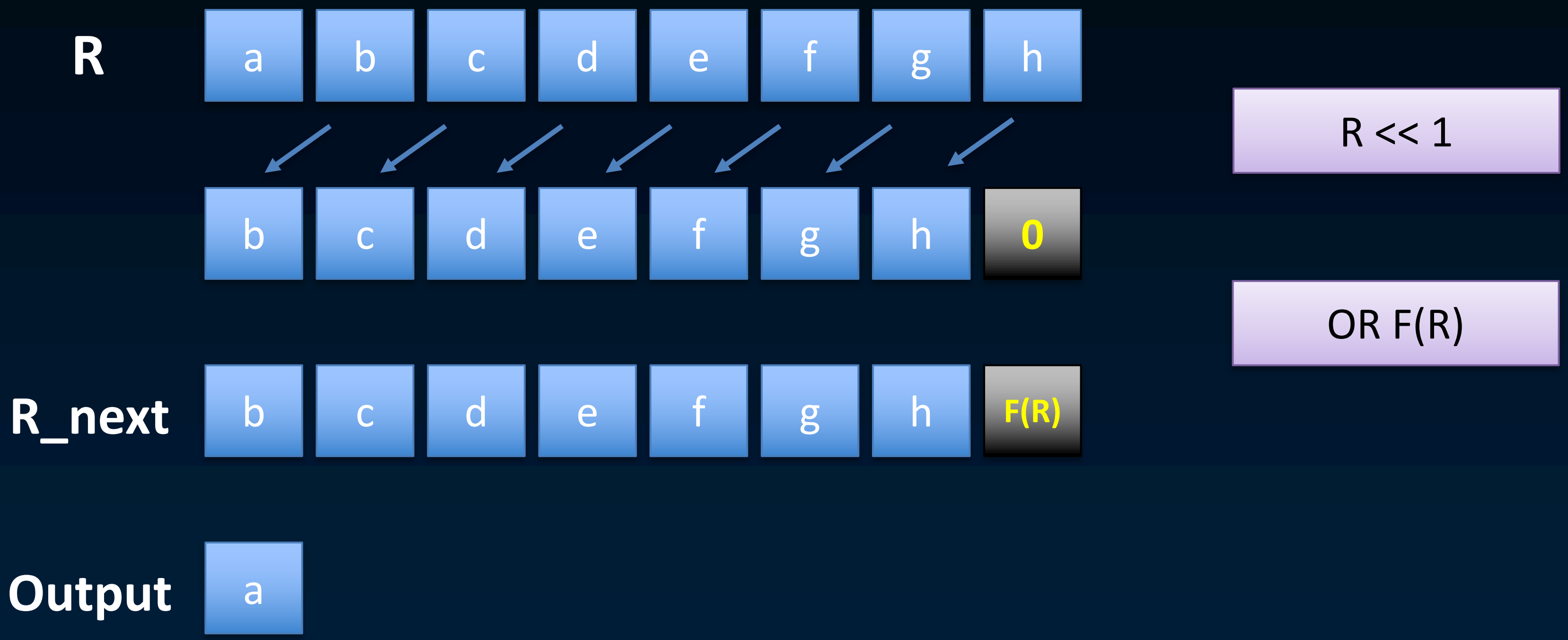


Hardware Oriented SCs

- Lower cost in HW vs. block ciphers
  - Less memory, smaller area on chip
  - Cheap fabrication costs
- Basic mechanism: FSRs
  - Feedback Shift Register
- FSR components
  - State **R** (i.e., an array of bits, a register)
  - Feedback function **f**
  - Update: change the state, return 1 bit

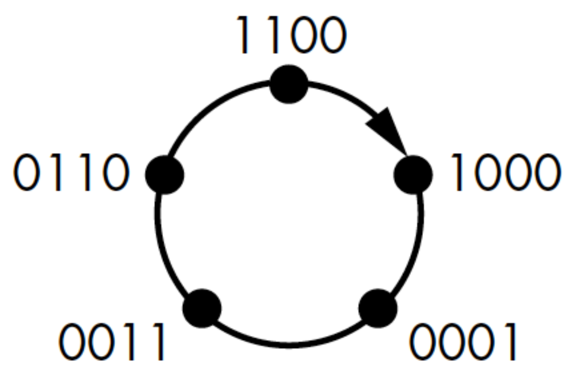
Basic FSR operation

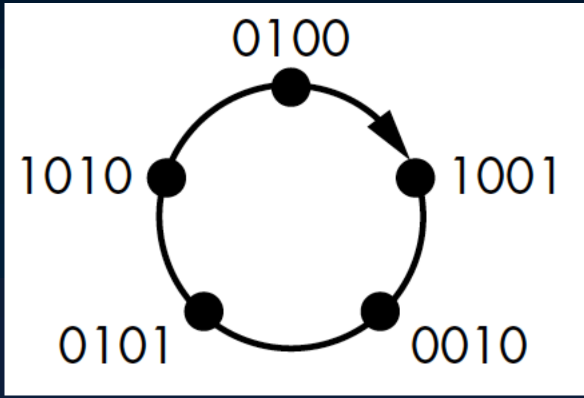
- R_next = (R << 1) OR F(R)

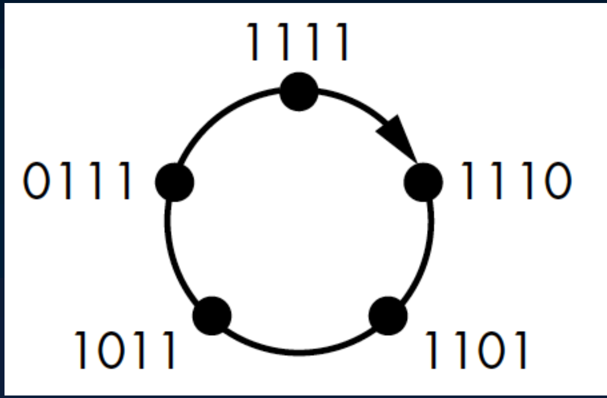


FSR period

- After P updates, we get the initial state
  - The period depends on the initial state and the feedback function
  - The output bits are repeated
- E.g., 4-bit FSR with F(R)=XOR all bits







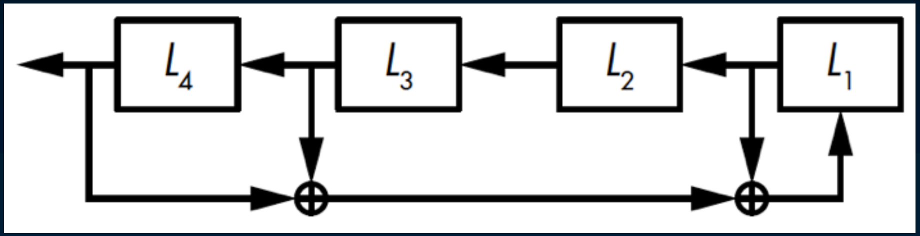
- What is the period for R=0000?

Linear FSRs

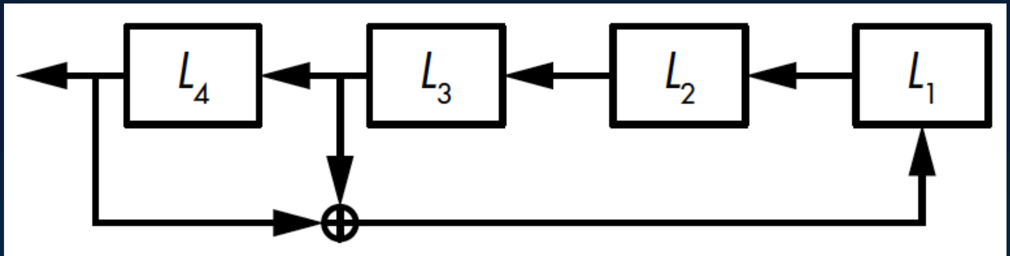
- Feedback function XORs some state bits
  - Linear operation
  - Period can be up to 2^N-1
  - Why the period is not 2^N?

Is this secure?

- Example 1

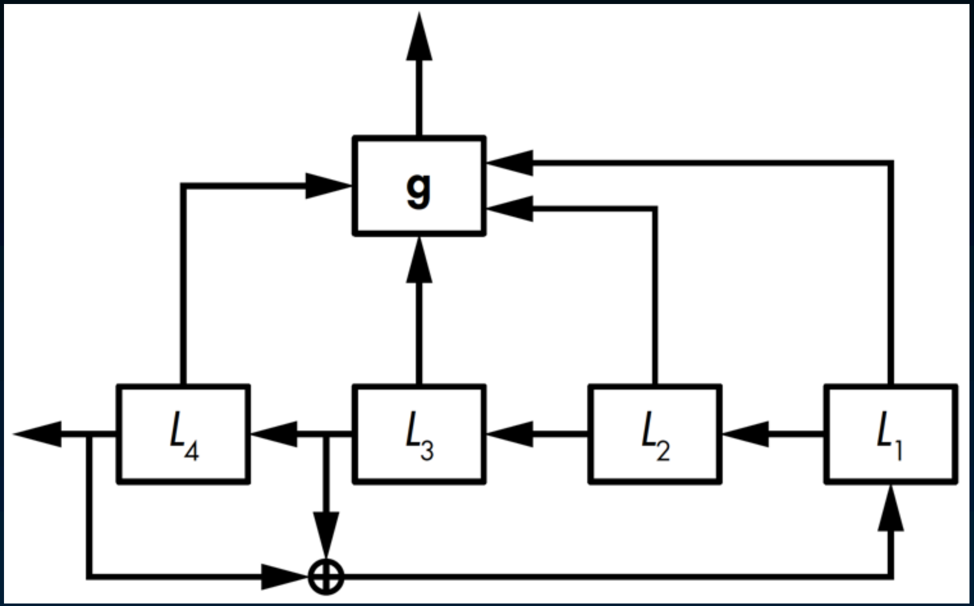


  - 0001, 0011, 0111, 1110, 1100, 0001
- Example 2



Filtered LFSRs

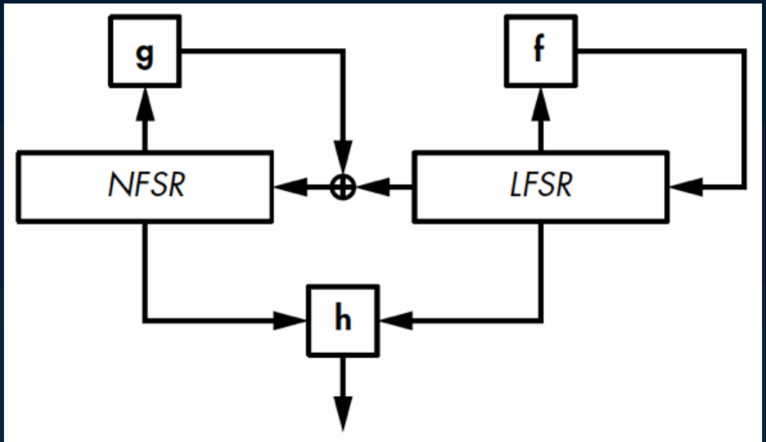
- Use a non-linear function **G**



- Attacks
  - Solve non-linear equations, compute derivatives, approximate G linearly

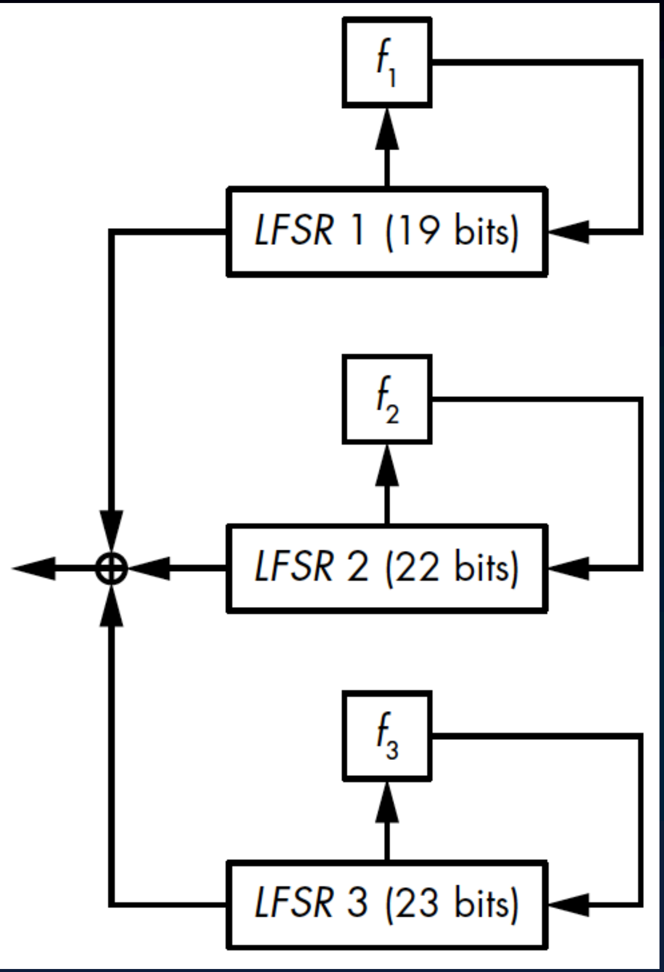
Nonlinear FSRs (NFSRs)

- Use AND and OR along with XORs
- Example
  - State=R1, R2, R3, R4
  - Output=R1+R2+R1*R2+R3*R4
  - Feedback=replace R1 with output bit above
- Example (Grain-128a)
  - Filter h
  - Nonlinear g
  - Linear f
  - Max period



Broken SCs

- A5/1
  - Three LFSRs
  - Update LFSR state based on clocking conditions
- Attacks
  - Subtle attacks
    - Guess state
  - Brutal attacks
    - Time/memory trade-off
    - Codebook attack



Reading for next lecture

- Aumasson: Chapter 5

Hands-on exercises

- Implement left shift register
- Implement a 4-bit LFSR
- Implement a 4-bit NFSR