State of the art

- eSTREAM Project
  - ECRYPT Network of Excellence
    - Call for stream ciphers; 34 candidates
  - Profile 1. Stream ciphers for software applications with high throughput requirements
    - HC-128, Rabbit, Salsa20/12, SOSEMANUK
  - Profile 2. Stream ciphers for hardware applications with restricted resources
    - Grain v1, MICKEY v2, Trivium

Feb-24 Stream Ciphers 28

28

eSTREAM performance

- RC4 126 Mb/s (*)
- Salsa 20/12 643 Mb/s
- Sosemanuk 727 Mb/s
- (*) AMD Opteron 2.2. GHz (Linux)

Feb-24 Stream Ciphers 29

29

Stream Ciphers

CONTENT SCRAMBLING SYSTEM (CSS) (DVD)

Feb-24 Stream Ciphers 30

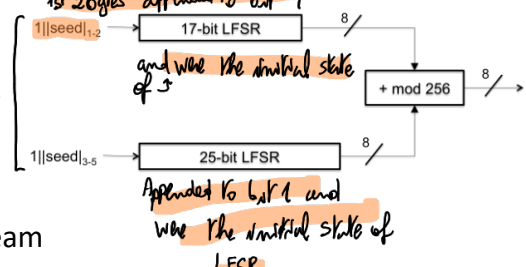
30

Content Scrambling System: stream cypher

UNIVERSITÀ DI PISA

- Seed (key)
  - initial states of the LFSRs 5 bytes (80 bit) 40
- Each round
  - 8 CLK cycles
  - Each LFSR produces 8 bits
  - LFSR's outputs are added mod 256(*) so producing the key stream
    - (*) neglect carry bit for simplicity

1st 2 bytes appended to bit 1 and were the initial state of 5



Appended to bit 1 and were the initial state of LFSR

For each clock cycle you generate a bit. When you have 8 bits you sum in mod 256 and those are 8 bits of the key stream

Feb-24 Stream Ciphers 31

31

So for brute force you need 2^{40} trials for the key. But you can do it in less.

- Suppose you have a prefix of 20 bytes of the DVD. You can compute a prefix of the stream.

Content Scrambling System

- Easy to break in 2^{17} steps (<< 2^{40})
- Known-plaintext attack
  - A prefix$|_{1\text{-}20}$ of the (cleartext) movie is known => a prefix of the keystream$|_{1\text{-}20}$ can be computed
    - E.g., 20 initial bytes in mpeg
- For details
    - https://www.cs.cmu.edu/~dst/DeCSS/Kesden/

Feb-24 Stream Ciphers 32

32

Content Scrambling System

- Attack algorithm
  - For all possible initial setting of LFSR-17 (2^{17})
    1. Run LFSR-17 to get 20 bytes of output
    2. Subtract LFSR-17$|_{1\text{-}20}$ from keystream$|_{1\text{-}20}$ and obtain a candidate output of LFSR-25$|_{1\text{-}20}$
    3. Check whether LFSR-25$|_{1\text{-}20}$ is consistent with LSFR-25
       a. If it is consistent then we have found correct initial setting of both and the algorithm is finished!
       b. Otherwise, go to 1 and test the next LFSR-17 initial setting
  - Using key, generate entire CSS output
  - Complexity
    - At most, the attack need to try all the possible initial setting of LFSR-17 (2^{17})

Feb-24 Stream Ciphers 33

33