Stream Ciphers and Coding Theory

Tor Helleseth
University of Bergen
Norway

Outline

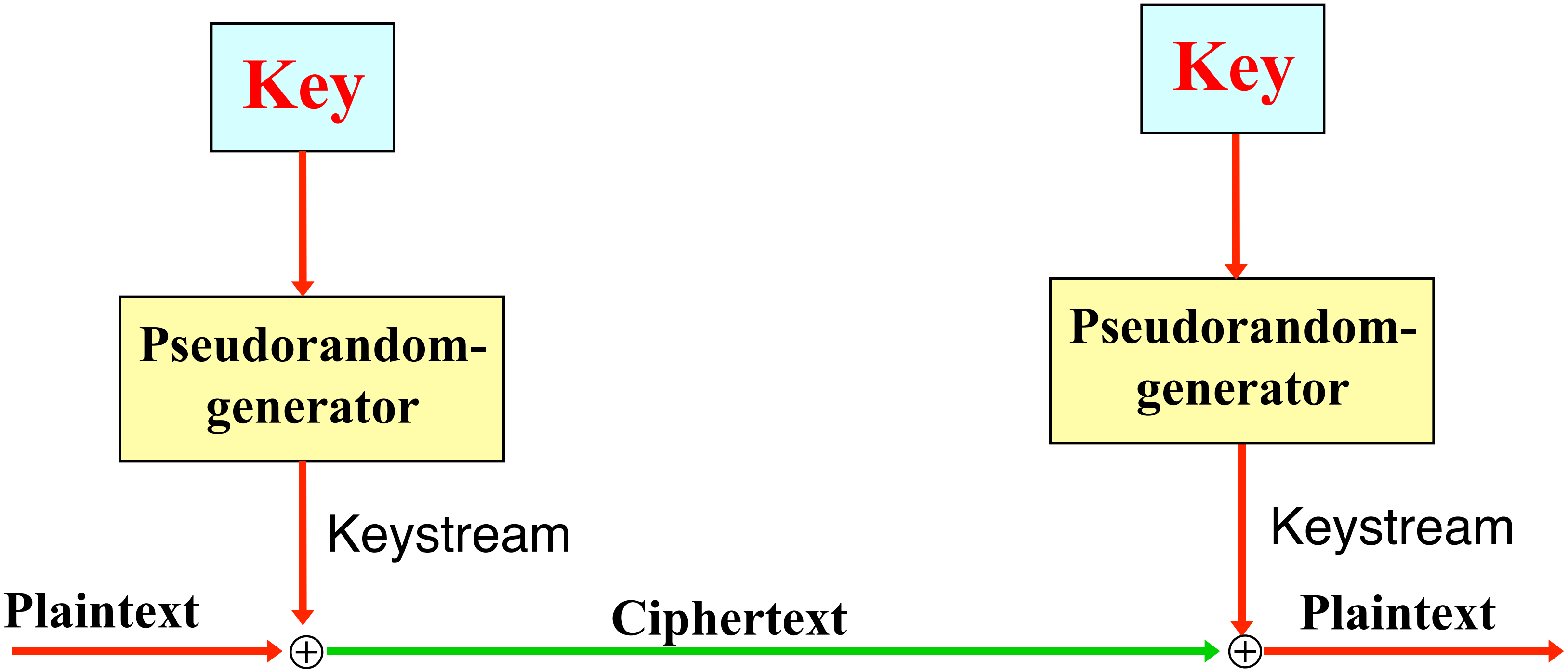
- Stream ciphers
- Building blocks in stream ciphers
  - m-sequences
  - Clock-control registers / Nonlinear combiner / Filter generator
- Correlation attacks - connections to coding theory
- Algebraic attacks
  - Linearization attack
  - Rønjom-Helleseth attack
    - Multivariate representation / Univariate representation
- Algebraic attacks - connections to coding theory
  - Algebraic immunity (AI)
  - Spectral immunity (SI)

Some known stream ciphers

- **RC4** - Secure Socket Layer (SSL) Protocol
- **A5** - Global System for Mobil Communication (GSM)
- **E0** - Bluetooth stream cipher
- **SNOW** - Word oriented stream ciphers for software implementation (European NESSIE project)
- **ZUC** - Chinese stream cipher

- **Grain, Trivium, Mickey** – Stream ciphers from eSTREAM project initiated by ECRYPT – a European Network of Excellence in Cryptography

Stream Cipher



Requirements for a good keystream

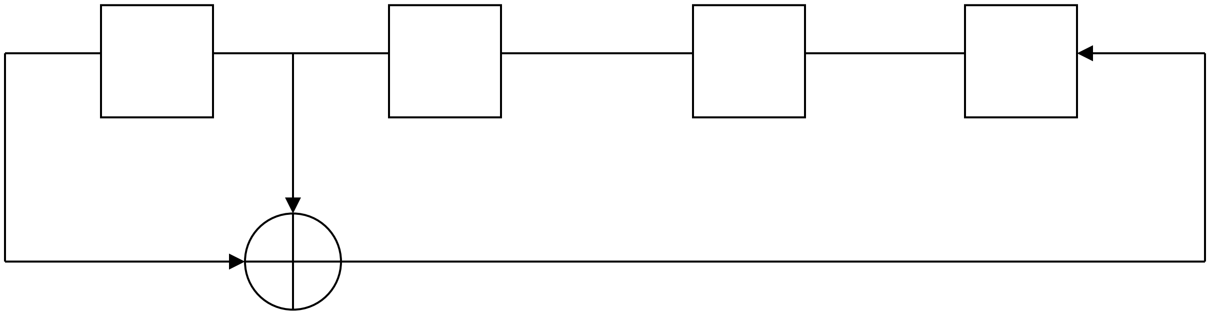
- Good randomness distribution
- Long period
- High complexity

Motivation of Stream Ciphers

- Block ciphers are frequently used in a stream cipher mode (Counter, OFB, CFB mode)
- Direct construction may improve performance
  - Higher speed in software
  - Less complexity in hardware
  - Lower power consumption etc.

- **ECRYPT** - A European Network of Excellence initiated an eSTREAM project
  - More than 30 streamciphers submitted 2005
  - 8 ciphers in hardware in the final phase 3
  - Grain, Trivium, Mickey, Pomaranch …

m-Sequence (Example)



$s_{t+4} = s_{t+1} + s_t$

$g(x) = x^4 + x + 1$

(s_t) : 000100110101111…

Properties of m-sequences

- Period $\varepsilon = 2^n - 1$
- Balanced
- Run property
- All possible nonzero n-tuples occur during a period
- $s_t + s_{t+\tau} = s_{t+\gamma}$

m-Sequences in Stream Ciphers

Positive features

+ Randomness distribution
+ Long period
+ Easy to generate (using linear shift registers)

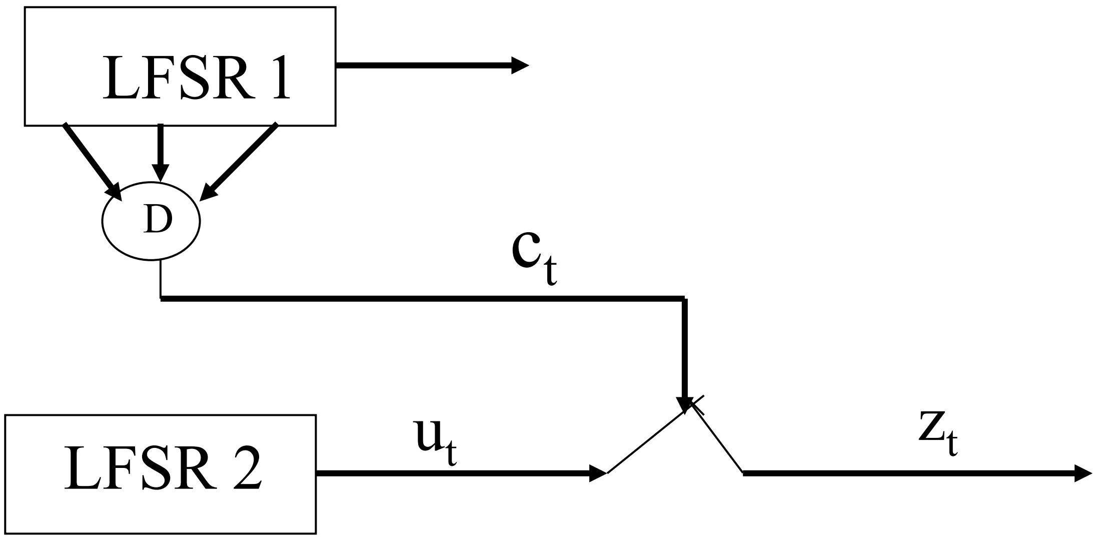
Negative features

- Too much linearity
- Easy to reconstruct g(x) from 2n consecutive bits
  (n linear equation in n unknowns, complexity $O(n^3)$)
  (Berlekamp-Massey algorithm, complexity $O(n\log_2 n)$)

Nonlinear Components in Stream Cipher

- Techniques to get higher linear complexity
  - The LFSRs are clocked irregularly
  - The LFSR bits are sent through a nonlinear function
    - Nonlinear combiner (several shift registers)
      - Attacks are using correlation attacks (based on coding theory)
    - Filter generator (one shift register)
      - Algebraic attacks (solving nonlinear equations)

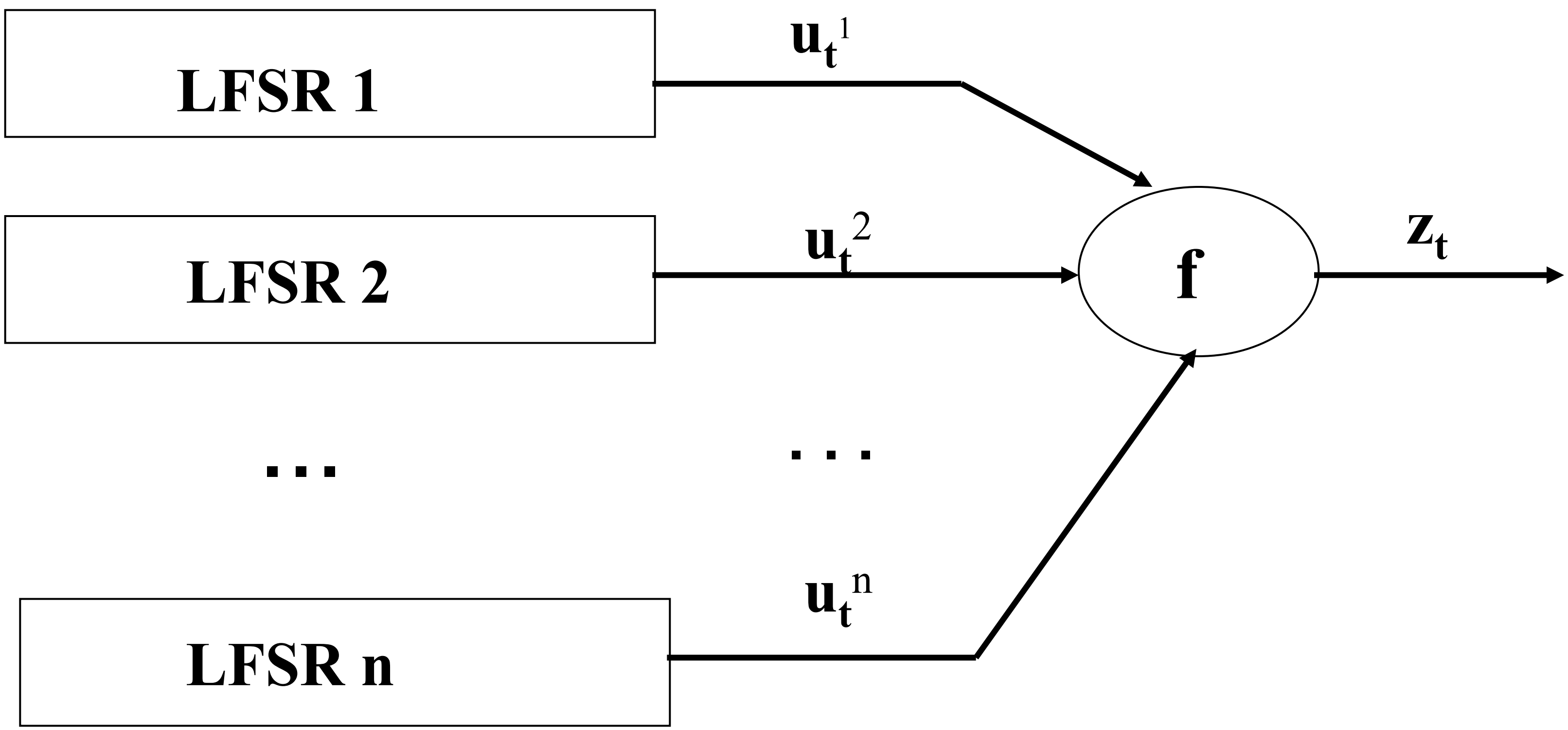
Clock Controlled LFSRs



- LFSR 1 generates an m-sequence mapped by D to an integer clock sequence c_t used to select the bits in another m-sequence u_t generated by LFSR 2 that is the output bit z_t

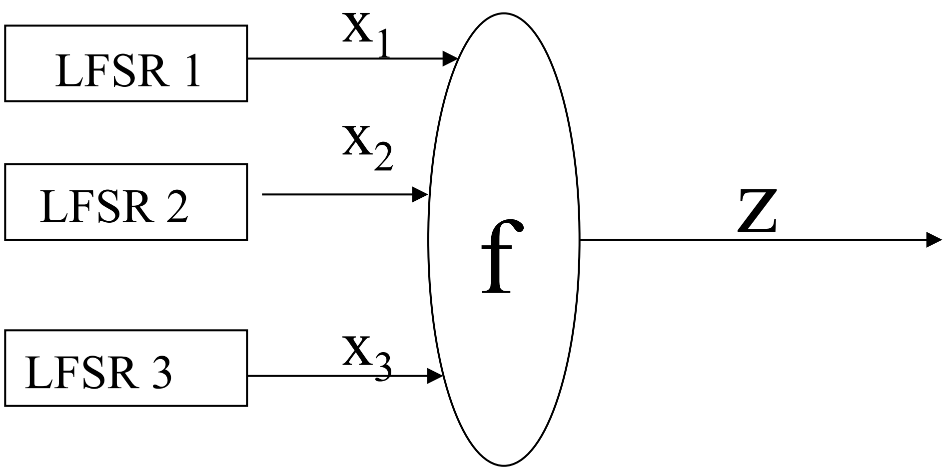
Nonlinear Combining LFSRs

- Using several LFSRs



$$f(x_1,x_2,\ldots,x_n) = \Sigma\, a_{i_1 i_2 .. i_n}\, x_{i_1} x_{i_2} \ldots x_{i_n}$$

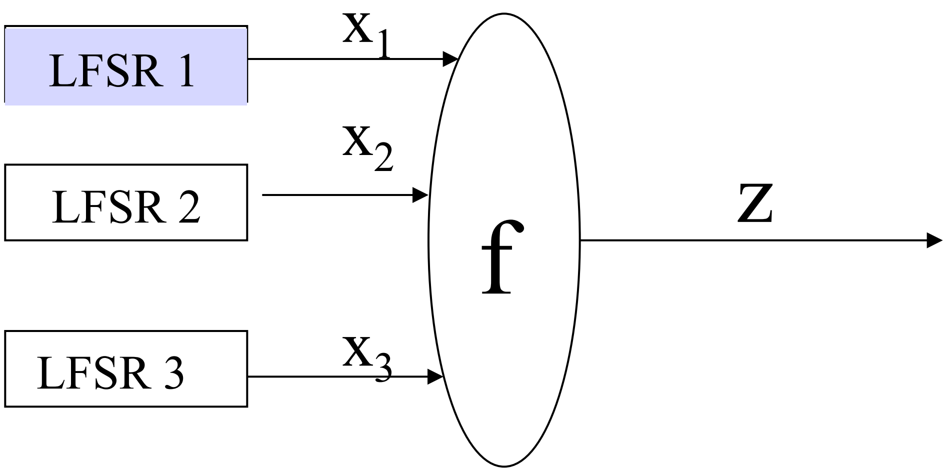
Geffe generator



The LFSRs generate m-sequence of period 2^{n_i} - 1, gcd $(n_i,n_j)=1$

- $z = f(x_1,x_2,\ldots,x_n) = x_1x_2+x_2x_3+x_3$
- $x_2=1 \rightarrow f = x_1$
- $x_2=0 \rightarrow f = x_3$
- Period = $(2^{n_1}-1)(2^{n_2}-1)(2^{n_3}-1)$
- Linear complexity = $n_1n_2+n_2n_3+n_3$

Correlation attack - Geffe generator

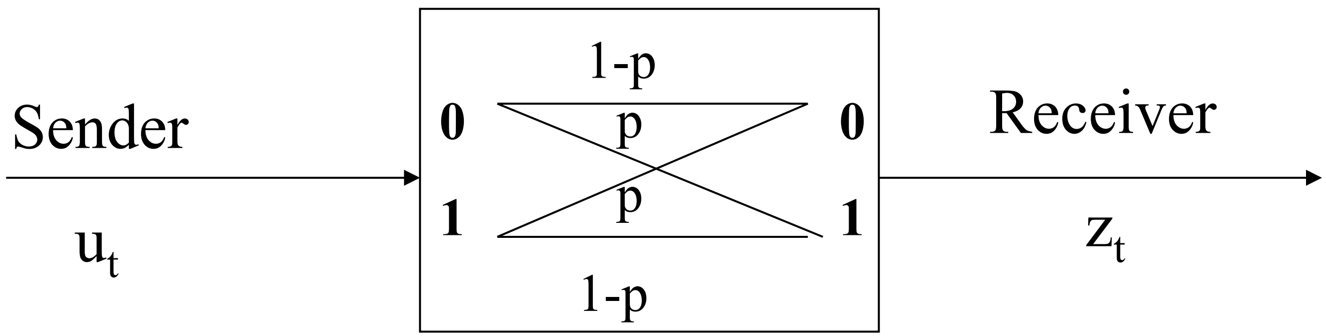


Correlation attack of Geffe generator

(NB! Prob($z = x_1$) = ¾)

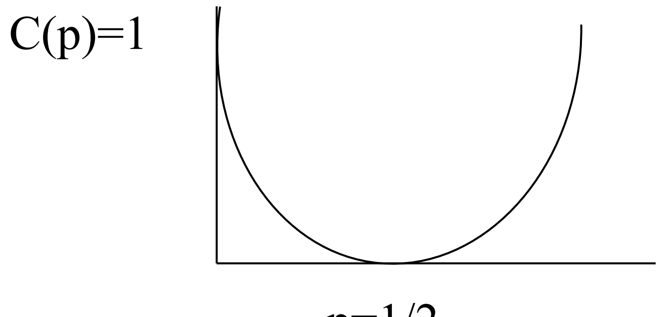
- Guess initial state of LFSR 1
- Compare x_1 and z
  - If agreement ¾ , guess is likely to be correct
  - If agreement ½ , guess is likely to be wrong

Binary Symmetric Channel-BSC_p



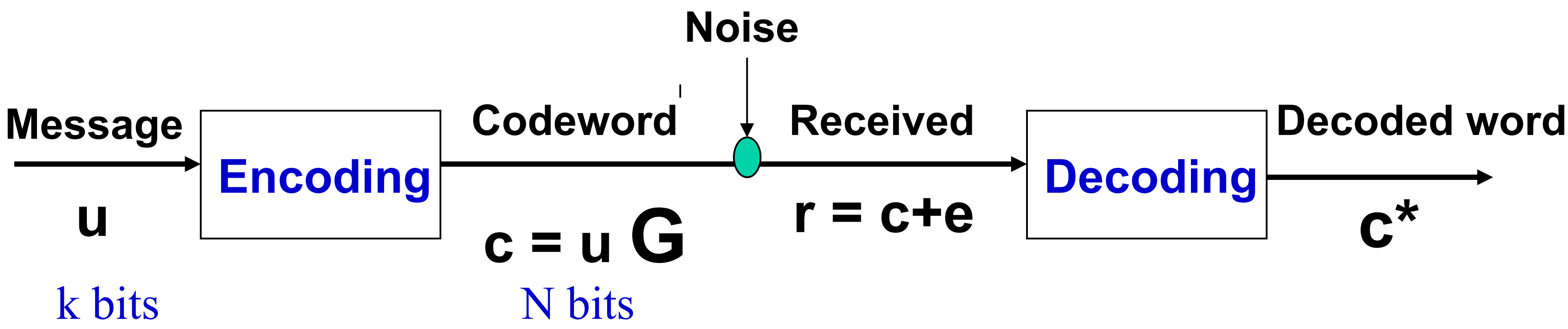
- $p = P(u_t \neq z_t)$
- Capacity of BSC_p

$$C(p) = 1 + p\log_2 p + (1-p)\log_2(1-p)$$



C(0.25) = 0.19

Coding Theory



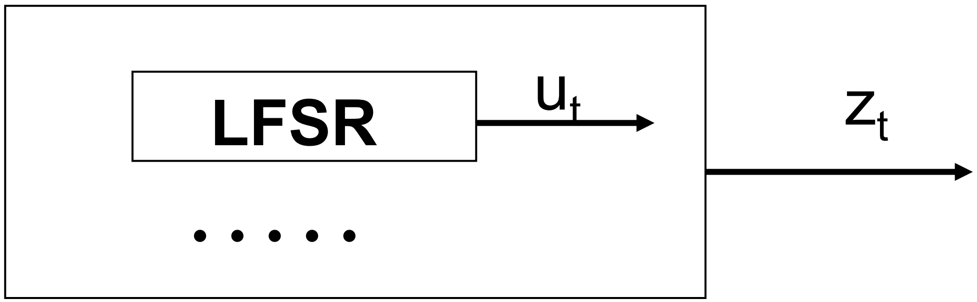
- C is an [N,k,d] linear (block) code if C is a k-dimensional subspace of $\{0,1\}^N$ of minimum Hamming distance d.

  (Rate of the code C is $R = k/N$)

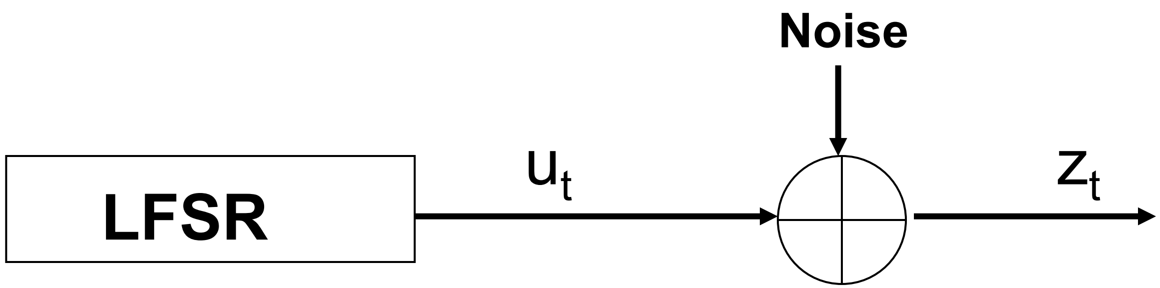
- For some codes C there are efficient methods to decode any received vector to the closest codeword

  (Viterbi decoding, Iterative decoding)

Correlation Attack



Binary Symmetric Channel (BSC)



- Correlation attacks are possible when there exists a crossover probability between the LFSR stream u_t and the key stream z_t

$$p = P(u_t \neq z_t) \neq 0.5$$

Correlation Attack

- Suppose a correlation $p_i \neq 0.5$ between i-th LFSR register and the keystream ($p_i = P(x_i = f(x_1, x_2, \ldots, x_n))$)
- Guess initial state for the i-th register and compare its output with the keystream
- Select initial state giving sequence closest to keystream

- **Complexity** is $O(\Sigma_i 2^{L_i} N_i)$
  - L_i length if i-th register
  - "Error–free decoding" decoding if $\mathbf{L_i/N_i < C(p_i)}$
  - $\mathbf{N_i \approx 2 \cdot L_i/C(p_i)}$ **-** number of bits needed
- Complexity is much less than $O(N2^{L_i + L_2 + \ldots + L_n})$

- Note that this attack needs to guess a full register

Fast correlation attacks

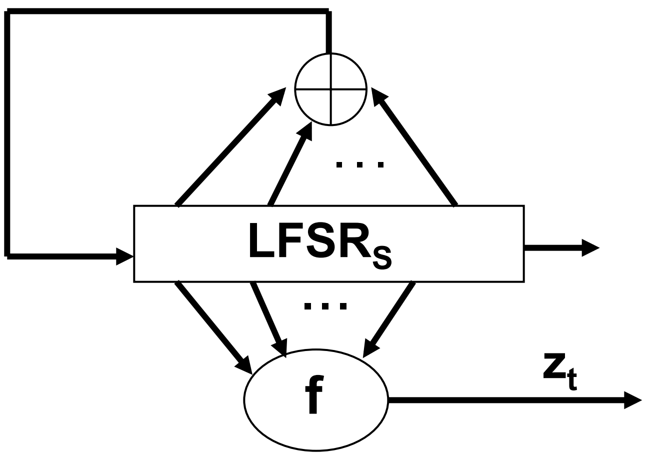
- Need a correlation $p \neq 0.5$ between keystream and register
- Do **not** need to guess a full register
- Construct a new linear code where bits are linear combinations of a subset of bits in initial state of register.
- Each code position estimated by few $w \leq 4$ keystream bits

- Ideas from coding theory are used to construct the closest codeword i.e., bits in the subset
- Efficient implementations of Viterbi decoder with rate

  $R = 10^{-10}$ and error probability $p = 0.49$

Filter Generator

- LFSR of length n generating an m-sequence (s_t) of period 2^n-1 determined by initial state $(s_0,s_1,\ldots,s_{n-1})$
- Primitive characteristic polynomial with root α
- Nonlinear Boolean function $f(x_0,x_1,\ldots,x_{n-1})$ of degree d

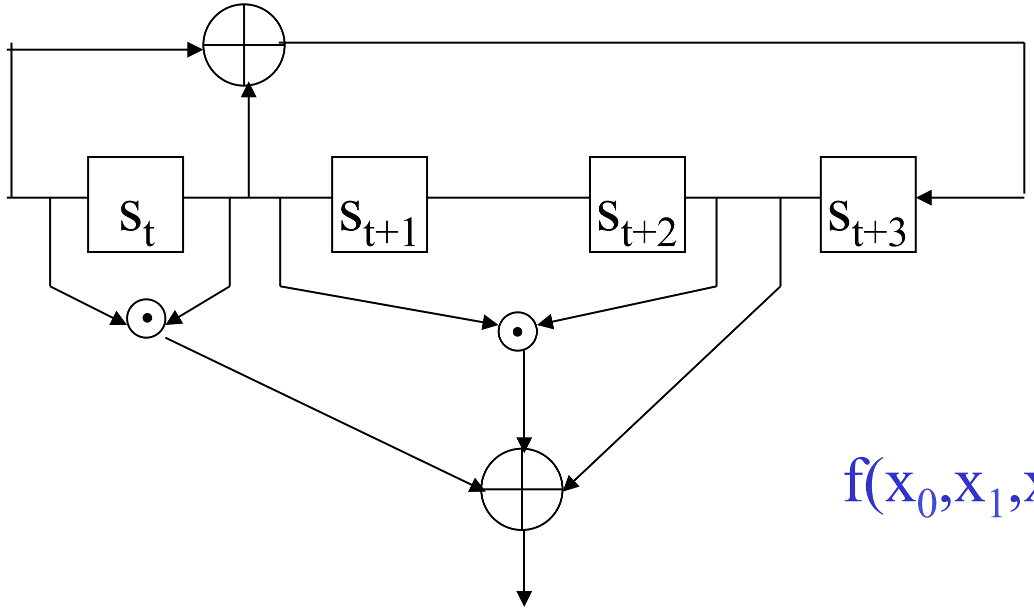


Keystream

$$z_t = f(s_t,s_{t+1},\ldots,s_{t+n-1}) = f_t(s_0,s_1,\ldots,s_{n-1})$$

$$f(x_0,x_1,\ldots,x_{n-1}) = \Sigma\, c_{a_0a_1..a_{r-1}}\, x_{a_0}x_{a_1}\ldots x_{a_{r-1}} = \Sigma_A\, c_A x_A$$

Example – Filter Generator



$g(x)=x^4+x+1$

$s_{t+4}=s_{t+1}+s_t$

$f(x_0,x_1,x_2,x_3) = x_0x_1+x_1x_3+x_3$

$$z_t = s_ts_{t+1} + s_{t+1}s_{t+3} + s_{t+3}$$

$$z_0 = f(s_0,s_1,s_2,s_3) = s_0s_1+s_1s_3+s_3 \quad (= f_0)$$

$$z_1 = f(s_1,s_2,s_3,s_4) = f(s_1,s_2,s_3,s_0+s_1) = s_0+s_1+s_0s_2 \quad (= f_1)$$

$$z_2 = f(s_2,s_3,s_4,s_5) = f(s_2,s_3,s_0+s_1,s_1+s_2) = s_1+s_2+s_1s_3 \quad (= f_2)$$

....

Multivariate Equations

$z_0 = s_0s_1+s_1s_3+s_3$
$z_1 = s_0s_2+s_0+s_1$
$z_2 = s_1s_3+s_1+s_2$
$z_3 = s_0s_2+s_1s_2+s_2+s_3$
$z_4 = s_1s_3+s_2s_3+s_0+s_1+s_3$
$z_5 = s_0s_2+s_0s_3+s_1s_2+s_1s_3+s_0+s_1+s_2 \quad \ldots$

Linearization gives a linear system with $\binom{4}{2} + \binom{4}{1} = 10$ unknowns

$z_0 = a_4 + a_8 + a_3$
$z_1 = a_5 + a_0 + a_1$
$z_2 = a_8 + a_1 + a_2$
$z_3 = a_5 + a_7 + a_2 + a_3$
$z_4 = a_8 + a_9 + a_0 + a_1 + a_3$
$z_5 = a_5 + a_6 + a_7 + a_8 + a_0 + a_1 + a_2 \quad \ldots$

Solve by using Gaussian elimination

Standard Linearization Attack

- Shift register m-sequence (s_t) of period $2^n - 1$
- Boolean function $f(x_0,x_1,\ldots,x_{n-1})$ of degree d

$$z_t = f(s_t,s_{t+1},\ldots,s_{t+n-1}) = f_t(s_0,s_1,\ldots,s_{n-1})$$

- Nonlinear equation system of degree d in n unknowns $s_0,\ldots,s_{n-1}$
- Reduce to linear system: D unknown monomials
- $D = \binom{n}{d} + \binom{n}{d-1} + \ldots + \binom{n}{1}$
- Need about D keystream bits
- Complexity D^ω , $\omega = \log_2 7 \approx 2.807$

Example - Coefficient Sequences

- Let $s_{t+4}=s_{t+1}+s_t$ i.e., $s_4=s_1+s_0$
- Boolean function

$$f(x_0,x_1,x_2,x_3) = x_2+x_0x_1+x_1x_2x_3+x_0x_1x_2x_3$$

- $z_t=f(s_t,s_{t+1},s_{t+2},s_{t+3}) = s_{t+2}+s_ts_{t+1}+s_{t+1}s_{t+2}s_{t+3}+s_ts_{t+1}s_{t+2}s_{t+3}$

- $z_0 = f_0(s_0,s_1,s_2,s_3) = s_2+s_0s_1+s_1s_2s_3+ s_0s_1s_2s_3$
- $z_1 = f_1(s_0,s_1,s_2,s_3) = s_3+s_1s_2+ s_0s_2s_3 +s_0s_1s_2s_3$
- $z_2 = f_2(s_0,s_1,s_2,s_3) = s_0+s_1+s_1s_3+s_2s_3 +s_0s_1s_3+s_1s_2s_3+ s_0s_1s_2s_3$
- $z_3 = f_3(s_0,s_1,s_2,s_3) = s_1+s_2+s_0s_2 +s_0s_3+s_1s_3+s_0s_1s_2+ s_0s_2s_3 +s_0s_1s_2s_3$
- $z_4 = f_4(s_0,s_1,s_2,s_3) = s_1+s_2+s_3+s_0s_1+s_0s_2+s_1s_2+s_0s_1s_3+ s_0s_1s_2s_3$
- $z_5 = f_5(s_0,s_1,s_2,s_3) = s_0+s_1+s_2+s_3+s_1s_3+s_2s_3+ s_0s_1s_2+ s_0s_1s_3+s_0s_1s_2s_3$

Some coefficient sequences

$I=\{0,1,2,3\}$ $K_{I,t}= 1\ 1\ 1\ 1\ 1\ 1\ldots$

$I=\{0,2,3\}$ $K_{I,t}= 0\ 1\ 0\ 1\ 0\ 0\ldots$

$I=\{1,3\}$ $K_{I,t}= 0\ 0\ 1\ 1\ 0\ 1\ldots$

Rønjom-Helleseth Algebraic Attack

- Recovering initial state of filter generator in complexity
  - Pre-computation $O(D\ (\log_2 D)^3)$
  - Attack $O(D)$
  - Need D keystream bits

- Main idea - Coefficient sequences of $I=\{i_0,i_1,\ldots,i_{r-1}\}$
  - Consider (binary) coefficient $K_{I,t}$ in $f_t(s_0,s_1,\ldots,s_{n-1})$ of the monomial $s_I=s_{i_0}s_{i_1}\ldots s_{i_{r-1}}$ at time t
  - $K_{I,t}$ obeys some nice recursions that can be computed
  - Construct a recursion generating all coefficient sequences for all $K_{I,t}$ for all I with $|I|\geq 2$

$$p(x) = \Pi_{2 \leq wt(j) \leq d} (x+\alpha^j) = \Sigma\, p_j\, x^j$$

  - Gives a simple linear equation system in n variables

Key Argument in Attack

- From the received keystream z_j for j=0,1,..,D-1 compute for t=0,1,..,n-1

$$z_t^* = \Sigma_j\, p_j z_{t+j} \qquad (= \Sigma_j\, p_j f_{t+j}(s_0,s_1,\ldots,s_{n-1}))$$
$$= \Sigma_j\, p_j\, \Sigma_I\, s_I K_{I,t+j}$$
$$= \Sigma_I\, s_I\, \Sigma_j\, p_j K_{I,t+j}$$
$$= \Sigma_{|I|\leq 1}\, s_I\, \Sigma\, p_j K_{I,t+j}$$
$$= \text{Affine in } s_0,s_1,\ldots,s_{n-1}$$

gives a linear n x n system of equations for finding the (initial state) $s_0,s_1,\ldots,s_{n-1}$

Multivariate - Univariate

- Let $x = \Sigma_i x_i \alpha_i$ where $\alpha_1,\ldots,\alpha_n$ basis $GF(2^n)$
- 1-1 correspondence $GF(2)^n \leftrightarrow GF(2^n)=GF(q)$
- $(x_1,\ldots,x_n) \leftrightarrow x$
- Then Boolean function ”becomes univariate”

$$f(x_1,\ldots,x_n) = f(x)$$

  for some polynomial $f(x)$ in $GF(2^n)[x]$ of degree at most 2^n-2 (if we do not care for the value at 0)
- The degree d of $f(x_1,\ldots,x_n)$ is the largest $wt(j)$ such that a coefficient in $f(x)$ of x^j is nonzero

Rønjom-Helleseth Attack - Univariate

- Let L be the shift operator of the LFSR
  - $L(s_t,\ldots,s_{t+n-1}) = (s_{t+1},\ldots,s_{t+n})$
- Define $f(\alpha^t) = f(L^t(s_0,\ldots,s_{n-1}))$
- Let x denote the unknown initial state, then
  - $z_t = f(x\alpha^t)$ where we want to find x
- Univariate equation system in x
  - $z_0 = f_0(x) = f(x) = c_0 + c_1 x + \ldots + c_{q-2} x^{q-2}$
  - $z_1 = f_1(x) = f(x\alpha) = c_0 + c_1 \alpha x + \ldots + c_{q-2} \alpha^{q-2} x^{q-2}$
  - $z_2 = f_2(x) = f(x\alpha^2) = c_0 + c_1 \alpha^2 x + \ldots + c_{q-2} \alpha^{2(q-2)} x^{q-2}$

  ………………

Coefficient sequences - Univariate

- The coefficient sequence for x^k for $f_t(x)$ is

$$w_t = c_k \alpha^{kt}$$

and has characteristic polynomial $m(x) = x + \alpha^k$

- Computing

$$u_t = z_{t+1} + \alpha^k z_t = \Sigma\, b_i\, x^i$$

gives $b_k=0$

- Using characteristic polynomial $m(x) = \Pi_{i\neq k}(x + \alpha^i)$ on the keystream

$$u_t = \Sigma\, m_j z_{t+j} = c_k m(\alpha^k)\, \alpha^{kt}\, x^k$$

- Hence, we find x^k and x if $\gcd(k,2^n-1)=1$

Algebraic attacks - Multivariate

Definition

The Boolean function $g(x_0,\ldots,x_{n-1})$ is an annihilator of $f(x_0,\ldots,x_{n-1})$ if

$$f(x_0,\ldots,x_{n-1})\, g(x_0,\ldots,x_{n-1}) = 0 \text{ for all } x_0,\ldots,x_{n-1}$$

Definition

The algebraic immunity of f

$$AI(f) = \min\{\deg(g) \mid fg=0 \text{ or } (1+f)g=0\}$$

Note that if $z_t=1$ then

$$f(s_t,\ldots,s_{t+n})\, g(s_t,\ldots,s_{t+n}) = z_t\, g(s_t,\ldots,s_{t+n})$$
$$= g_t(s_0,\ldots,s_{n-1}) = 0$$

Coding theory – Cyclic Codes

Definition –Linear $[N,k,d]_q$ code

C is an $[N,k,d]_q$ code iff

1) C subset of dimension k over $GF(q)^N$

2) $d = \min\{d_H(c_1, c_2) \mid c_1 \neq c_2 \in C\}$

Definition – Cyclic code

$C = (G(x)) \pmod{x^n - 1}$

(= Ideal generated by G(x))

Spectral Immunity

Definition

The spectral immunity of (z_t) is the smallest linear complexity(LC) of a sequence (u_t) over $GF(2^n)$ such that

$$z_t u_t = 0 \text{ or } (1+z_t)\, u_t = 0 \text{ for all } t$$

Let $z_t = f(x\alpha^t)$ and $u_t = g(x\alpha^t)$ where (u_t) annihilates (z_t)

Then if $z_t=1$ we obtain

$$g(x\alpha^t) = 0 \rightarrow \Sigma\, g_i\, \alpha^{ti} x^i = 0 \qquad \text{(Note: } wt(g)=LC(u_t))$$

- Linear system in the LC unknowns $x^{i_1}, x^{i_2}, \ldots, x^{i_{LC}}$
- Knowing $2 \cdot LC(u_t)$ bits finds $x^{i_1}, \ldots$ and hence x

Spectral immunity and cyclic codes(I)

Theorem

Let $z_t = f(x\alpha^t)$ and $u_t = g(x\alpha^t)$ be such that

$$f(x)\, g(x) = 0 \text{ for all } x \text{ in } GF(2^n)$$

Then $g(x)$ is a codeword in the cyclic code C_f with symbols from $GF(2^n)$ and generator polynomial

$$G_f = \gcd(f(x)+1, x^{q-1}+1)$$

Proof:

Follows since $f(x)$ is Boolean and only takes on the values 0 and 1. Therefore the elements in $GF(2^n)$ are zeros of either $f(x)$ or $f(x)+1$

Spectral immunity and cyclic codes(II)

Theorem

The spectral immunity(SI) of (z_t) is the smallest weight of a codeword in the codes over $GF(2^n)$ with generator polynomials

$$G_f = \gcd(f(x)+1, x^{q-1}+1)$$

$$G_{f+1} = \gcd(f(x), x^{q-1}+1)$$

Corollary

$$SI \leq D = \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{AI}$$

SI versus AI

Corollary

$SI \le D = \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{AI}$

- SI large $\rightarrow$ AI large
- AI Large $\not\rightarrow$ SI large

Can use codes G_f and G_{f+1} to evaluate AI

$$AI = \min\{ wt(i) \mid g_i \neq 0 \text{ for } g(x) \text{ in } C_f \text{ or } C_{f+1}\}$$

Tapping positions of Filter generator

- Let f be a Boolean function in k variables $f(x_1,\ldots,x_k)$
- $z_t = f(s_{t+i_1}, s_{t+i_2}, \ldots, s_{t+i_k})$, $0 \leq i_1 < i_2 < \ldots < i_k < n$
- In most applications $k \leq 20$

Rule-of-thumb

Select tapping positions such that all differences between $\{i_1, i_2, \ldots, i_k\}$ are different.

"Bad" tapping positions

Example

- Let $z_t=f(s_0, s_1,\ldots, s_{k-1})$, i.e., tapping positions $T=\{0,1,\ldots,k-1\}$
- Let N_0 resp. N_1 be the zeros (resp. ones) of f
- Since f is balanced $|N_0|=|N_1|=2^{k-1}$

- $z_0=f(s_0, s_1,\ldots, s_{k-1})$ implies $(s_0, s_1,\ldots, s_{k-1}) \in N_{z_0}$
- $z_1=f(s_1, s_2,\ldots, s_k)$ implies $(s_1, s_2,\ldots, s_k) \in N_{z_1}$
- There are $\approx 2^{k-1}$ possibilities for $(s_0, s_1,\ldots, s_k)$

- Next $z_2 = f(s_2, s_3,\ldots, s_{k+1})$ implies $(s_2, s_3,\ldots, s_{k+1}) \in N_{z_2}$
- Similarly there are $\approx 2^{k-1}$ possibilities for $(s_0, s_1,\ldots, s_{k+1})$
- Continuing gives finally $\approx 2^{k-1}$ possibilities for $(s_0, s_1,\ldots, s_{n-1})$
- Testing all 2^{k-1} possibilities finds initial state

"Better" tapping positions

- Subspace metric

$$d_S(U,V) = \dim(U) + \dim(V) - 2\dim(U+V)$$

- Each tapping position defines a cyclic subspace
- Let $G = [1\ \alpha\ \alpha^2\ \ldots\ \alpha^{2^n-2}] = [g_0\, g_1\ \ldots\ g_{2^n-2}]$, n x (2^n-1) matrix
- Let $S_0=(s_0,s_1,\ldots,s_{n-1})$ then $s_t=S_0\cdot g_t$

Tapping positions $\{i_1,i_2,\ldots,i_k\}$

t=0: $V = < g_{i_1},g_{i_2},\ldots,g_{i_k} >$

t=1: αV

$t=2^n-2$: $\alpha^{2^n-2}V$

Cyclic subspace codes: $C = \{ \alpha^t V \mid t=0,1,\ldots,2^n-2\}$

- Good such code exists with $d_{min}= 2k-2$ is shown by:
  - E. Ben-Sasson, T. Etzion, A. Gabizon and N. Raviv, "Subspace polyomials ad cyclic Subspace Codes"

"Bad Subspace" tapping positions

$s_{i_1} = S_0 \cdot g_{i_1}$

$\dots$

$s_{i_k} = S_0 \cdot g_{i_k}$

$V = \langle g_{i_1}, \dots, g_{i_k} \rangle$

$s_{i_1+\tau} = S_0 \cdot g_{i_1+\tau}$

$\dots$

$s_{i_k+\tau} = S_0 \cdot g_{i_k+\tau}$

$\alpha^\tau V = \langle g_{i_1+\tau}, \dots, g_{i_k+\tau} \rangle$

Suppose $d_S(V, \alpha^\tau V) = 2$ i.e., $\dim(V + \alpha^\tau V) = k+1$

$z_0 = f(s_{i_1}, \dots, s_{i_k})$ implies 2^{k-1} choices of $(s_{i_1}, \dots, s_{i_k})$

$z_\tau = f(s_{i_1+\tau}, \dots, s_{i_k+\tau})$ implies 2^{k-1} choices of $(s_{i_1+\tau}, \dots, s_{i_k+\tau})$

- This leads to 2^{k-1} possibilities of $(s_{i_1}, \dots, s_{i_k}, s_{i_1+\tau})$ since wlog $V + \alpha^\tau V$ is spanned by $(g_{i_1}, \dots, g_{i_k}, g_{i_1+\tau})$
- Continuing this argument gives many bits of initial state

Summary

- Stream ciphers
- Correlation attacks and decoding of codes
- Algebraic attacks
  - Linearization attack
  - Rønjom-Helleseth attack
- Spectral immunity(SI) over $GF(2^n)$
- Connections between SI and cyclic codes
- Connections between the spectral immunity(SI) and the algebraic immunity(AI)
- Connections between choice of tapping positions and good subspace codes

References

- S. Rønjom and T. Helleseth, A new attack on the filter generator, *IEEE Trans. Inf. Theory*, vol. 53, no. 5, pp. 1752-1758, May 2007

- T. Helleseth and S. Rønjom, Simplifying algebraic attacks with univariate analysis," in *Proceedings of the 2011 IEEE Information Theory and Applications Workshop (ITA)*, IEEE, Feb. 2011, pp. 1-7.

- S. Rønjom and T. Helleseth, Attacking the filter generator over GF(2^m), in Arithmetic of Finite Fields, ser. *Lecture Notes in Computer Science*, vol. 4547, pp. 264-275.

- S. Rønjom and T. Helleseth, The linear vector space spanned by the nonlinear filter generator, in Sequences, Subsequences, and Consequences, ser. *Lecture Notes in Computer Science*, vol. 4893, 2007, pp. 169-183.

- G. Gong, S. Rønjom, T. Helleseth, and H. Hu, Fast discrete Fourier spectra attacks on stream ciphers, *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5555-5565, Aug. 2011

- E. Ben-Sasson, T. Etzion, A. Gabizon, N. Raviv, Subspace Polynomials and Cyclic Subspace codes, unpublished manuscript