Fast Linear Subspace Attacks on Stream Ciphers

Guang Gong

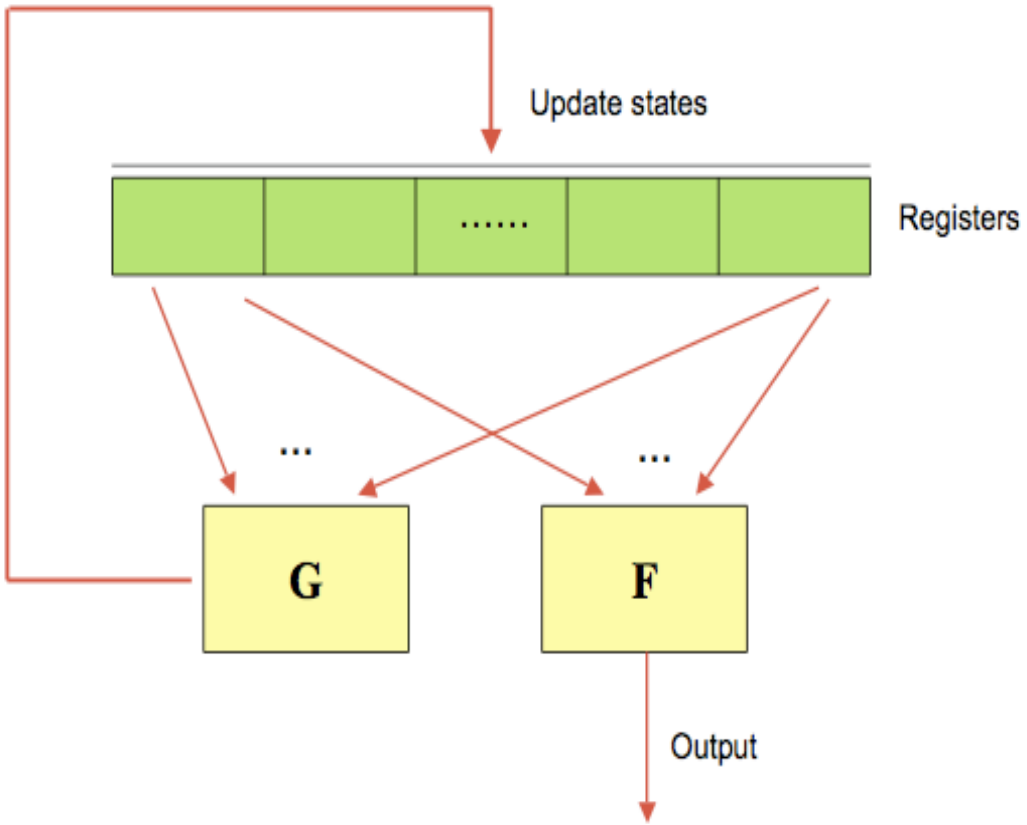
Department of Electrical and Computer Engineering
University of Waterloo
CANADA
<http://comsec.uwaterloo.ca/~ggong>

Joint work with Sondre Rønjom, Tor Helleseth, and Honggang Hu

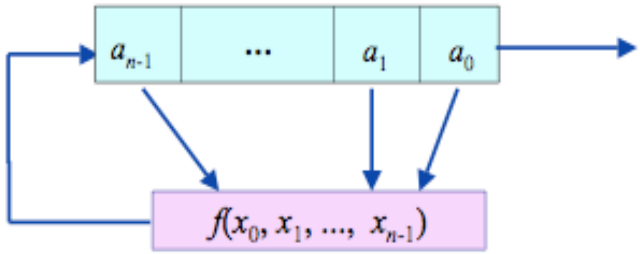
Outline

- **Basic Concepts** and Properties of Sequences
- **(Discrete) Fourier Transform (DFT)** of Shifts and Convolution of DFT
- **Fast** Selective DFT Attacks on Filtering Generators
- **Comparisons** with Fast Algebraic Attacks
- **New Security Criteria:** Spectral Immunity

A General Model of PSGs



Linear Feedback Shift Register (LFSR) Sequences



- We associate $f(x_0, \cdots, x_{n-1})$ with

  $$f(x_0, \cdots, x_{n-1} = c_0 x_0 + \cdots + c_{n-1} x_{n-1} \leftrightarrow t(x) = x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + 1$$

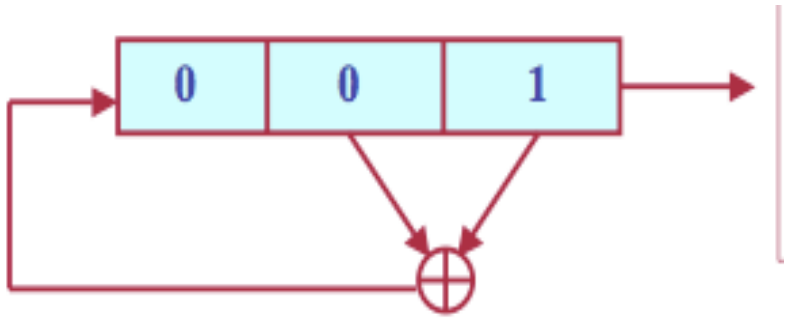
  a polynomial over $\mathbb{F}_2$.
- An output sequence of the LFSR satisfies the following recursive relation

  $$a_{n+k} = \sum_{i=0}^{n-1} c_i a_{k+i}, k = 0, 1, \cdots, \quad (1)$$

  $(a_0, \cdots, a_{n-1})$ is an **initial state** of **a**.
- $t(x)$ is called a **characteristic polynomial of a** (the **reciprocal** of $t(x)$ is referred to as a **feedback polynomial of a**, and we also say that **a** is generated by $t(x)$.
- **a is an *m*-sequences** is $t(x)$ is primitive (Golomb, 1954).

Example

The sequence $\mathbf{a} = 1001011$ is an m-sequence of period 7 generated by an LFSR with $t(x) = x^3 + x + 1$.



Minimal Polynomials and Linear Span

- A **minimal polynomial** of **a** is a polynomial with smallest degree which generates **a**. Let $m(x)$ be the minimal polynomial of a, then $m(x) \mid t(x)$.
- **Linear span** of **a** is the degree of $m(x)$, denoted as $LS(\mathbf{a})$, and $m(x)$ can be found using the Berlekamp-Massey algorithm from any $2LS(\mathbf{a})$ **consecutive bits of a**.
- **Linear span** of **a** is the degree of $m(x)$, denoted as $LS(\mathbf{a})$, and $m(x)$ can be found using the Berlekamp-Massey algorithm from any $2LS(\mathbf{a})$ **consecutive bits of a**.

The Shift Operator

- The **(Left cyclically) shift operator** L:

$$L\mathbf{a} = a_1, a_2, \cdots,$$
$$L^r\mathbf{a} = a_r, a_{r+1}, \cdots.$$

If $\mathbf{b} = L^r\mathbf{a}$, then we say that they are **shift equivalent**. Otherwise, they are **shift distinct**.

- **Example**: let

$$\mathbf{a} = 1001011$$
$$\mathbf{b} = 1011100$$
$$\mathbf{c} = 1110100$$

then **a and b are shift equivalent**, and **a and c are shift distinct**.

DFT and Inverse DFT of Binary Sequences

- **Notation:** $N|2^n - 1$, $\mathbb{F}_q = GF(q)$, $\{a_t\}$: a binary sequence with period N; α: an **element** in $\mathbb{F}_{2^n}$ with order N.
- The **(discrete) Fourier Transform (DFT)** of $\{a_t\}$ is defined by

$$A_k = \sum_{t=0}^{N-1} a_t \alpha^{-tk}, \ k = 0, 1, \ldots, N-1.$$

- The **inverse DFT (IDFT)** is given by

$$a_t = \sum_{k=0}^{N-1} A_k \alpha^{kt}, \quad t = 0, 1, \ldots, N-1.$$

- $\{A_k\}$ is called the DFT spectral sequence of **a** (with respect to α).

Trace Representation

- Let $A(x) = \sum_{k=0}^{N-1} A_k x^k$. Then $a_t = A(\alpha^t)$ and $A(x)$ can be written as

$$A(x) = \sum_k Tr_1^{m_k}(A_k x^k) \tag{2}$$

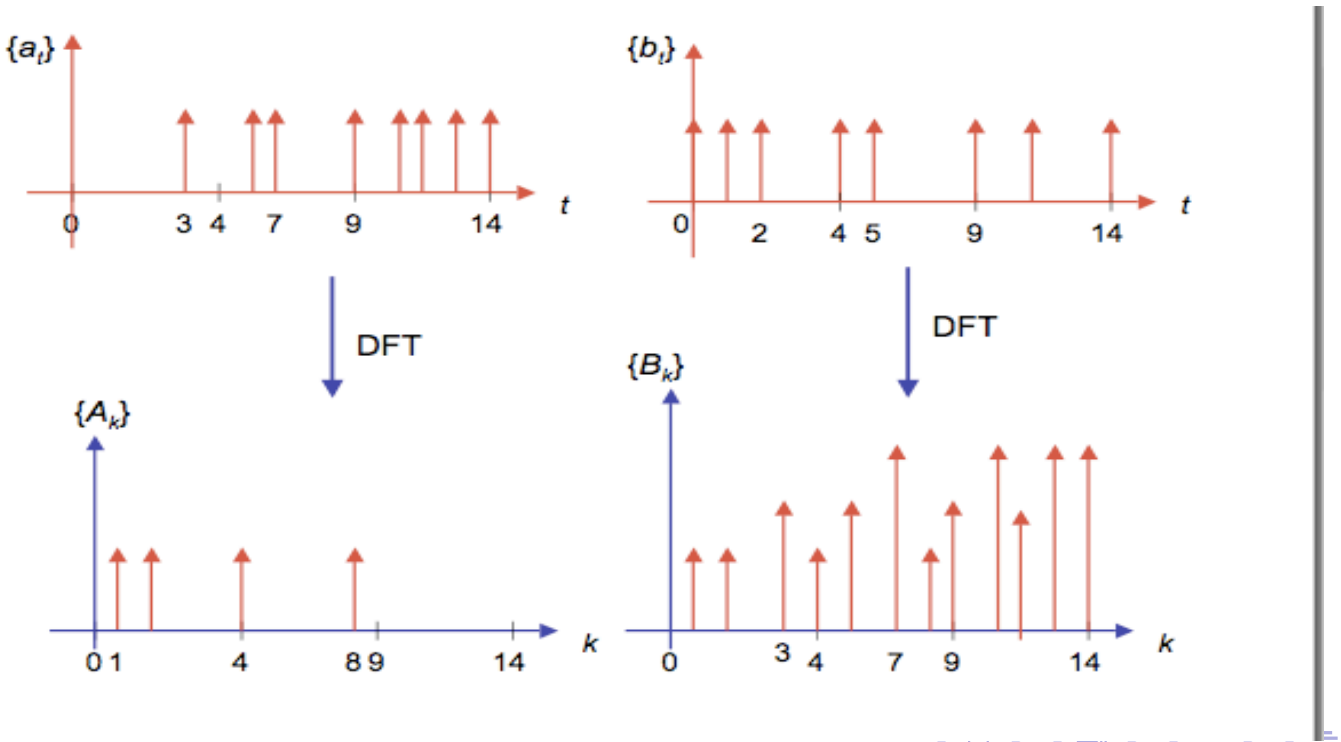
where the k's are **(cyclotomic) coset leaders** modulo N, $m_k \mid n$ is the length of the coset which contains k, and $Tr_1^{m_k}(x)$ is a trace function from $\mathbb{F}_{2^{m_k}}$ to $\mathbb{F}_2$. This is called a **trace representation** of $\{a_t\}$.

- Some times, for simplicity, we may use $Tr(x)$ for all terms in $A(x)$ where $Tr(x)$ represents from which field to $\mathbb{F}_2$ depends on the size of the coset containing k.
- The linear span of **a** is equal to the number of nonzero spectra of **a**.

Example 1

α: a primitive element in $\mathbb{F}_{2^4}$ with $\alpha^4 + \alpha + 1 = 0$:

Sequences in Time Domain	DFT Spectral Sequences in Frequency Domain
a =00010 01101 01111	A =0110100010000 0
b =1110110001010 01	B =011α 1 0 $\alpha^2\alpha^6 1 \alpha^8 0 \alpha^3\alpha^4\alpha^9\alpha^{12}$



Example 1 (cont.)

Trace Representation	Linear Span
$A(x) = Tr(x)$ $a_t = Tr(\alpha^t), 0 \leq t < 15$	4
$B(x) = Tr(x + \alpha x^3 + \alpha^6 x^7)$ $b_t = B(\alpha^t), 0 \leq t < 15$	12

DFT of Shifts

- A sequence $\mathbf{b} = \{b_t\}$ is a **shift** of **a** if and only in the DFT of **b** is given by

$$B_k = \beta^k A_k, 0 \leq k < N, \beta \in \mathbb{F}_{2^n}.$$

In this case,

$$b_t = A(\beta\alpha^t), t = 0, 1, \cdots,$$

i.e., $B(x) = A(\beta x)$.

- The shift operator **does not change** the **minimal polynomial** of **a**, nor the linear span.

Example 2

- For α, a primitive root of $x^4 + x + 1$ which defines $\mathbb{F}_{2^4}$, let

$a =$**00010 01101 01111**	$A(x) = Tr(x)$, and
$\mathbf{b} =$ **01101 01111 00010**	$B(x) = Tr(\alpha^5 x)$

In this case $\mathbf{b} = L^5\mathbf{a}$, a shift of **a**.

DFT Convolution and Product Sequences

- Let **a** and **b** be two sequences of period N with their respective DFTs $A = \{A_k\}$ and $B = \{B_k\}$.
- For the **term-by-term product $\mathbf{c} = \mathbf{a} \cdot \mathbf{b}$** where $c_t = a_t b_t$, $0 \leq t < N$, let the DFT of $\{c_t\}$ be $C = \{C_k\}$. Then C is a **convolution** of A and B, denoted as $C = A * B$ where

$$C_k = \sum_{i+j=k(\bmod N)} A_i B_j, 0 \leq k < N.$$

Example 3

- Let **b** be the sequence in Example 1, i.e.,

$$\begin{aligned}
\mathbf{b} &= 1110110001001001 \leftrightarrow B(x) = Tr(x + \alpha x^3 + \alpha^6 x^7) \\
\mathbf{a} &= 0001100011100011 \leftrightarrow A(x) = Tr(\alpha^2 x^3) \\
&\Longrightarrow \\
\mathbf{c} = \mathbf{a} \cdot \mathbf{b} &= 0000100001000001 \leftrightarrow C = B * A \\
&\Longrightarrow C(x) = B(x)A(x) = Tr(\alpha^3 x^3) + 1
\end{aligned}$$

Selective or Fast Selective DFT Attacks

Selective Filters in DFT Domain

- Let

$$\mathcal{N}_{\mathbf{a}} = \{k \mid A_k \neq 0, k \text{ **is a coset leader** } \bmod N\},$$

$p_k(x)$ be the minimal polynomial (MP) of α^k over $\mathbb{F}_2$, and let $q(x) = \sum_{i=0}^{r} c_i x^i$ be a polynomial over $\mathbb{F}_2$ of degree r.

- The MP $p(x)$ of $\mathbf{a}$ is equal to the product of p_k for all $k \in \mathcal{N}_{\mathbf{a}}$.
- **Applying $q(L)$ to a**, we have

$$v_t = \sum_{i=0}^{r} c_i a_{i+t}, t = 0, 1, \cdots,$$

which is a **linear filtered** sequence from $\mathbf{a}$.

DFT of $\{v_t\}$

Proposition 1. The DFT of $\{v_t\}$ is given by

$$V_k = A_k q(\alpha^k), 0 \leq k < N.$$

Interesting Cases of DFT of $\{v_t\}$

- **Two Extreme Cases:**
  - **Case 1.** $p(x) \mid q(x)$. Thus $q(\alpha^k) = 0, \forall k \in \mathcal{N}_{\mathbf{a}}$. Hence

$$V_k = 0, 0 \le k < N \Longrightarrow \mathbf{v} \text{ is a zero sequence.}$$

  - **Case 2.** $\gcd(p(x), q(x)) = 1$. Then $q(\alpha^k) \neq 0, \forall k \in \mathcal{N}_{\mathbf{a}}$.

$$(V_k = 0 \Longleftrightarrow A_k = 0)$$

$\{v\}$ has the **same minimal polynomial** as **s**, so does **a**, and **v** is a shift of **a** when α is a primitive element in $\mathbb{F}_{2^n}$ (in this case **a** has period $2^n - 1$).

Selective Case

- Let $c(x) = \gcd(p(x), q(x))$, $c(x) \neq 1$ **and** $c(x) \neq p(x)$**.** Then

$$c(x) = \prod_{k \in \mathcal{T}} p_k(x)$$

where $\mathcal{T} \subset \mathcal{N}_{\mathbf{a}}$, and

$$V_k = q(\alpha^k) A_k \neq 0 \Longleftrightarrow q(\alpha^k) \neq 0 \Longleftrightarrow k \in \mathcal{N}_{\mathbf{a}} \setminus \mathcal{T}.$$

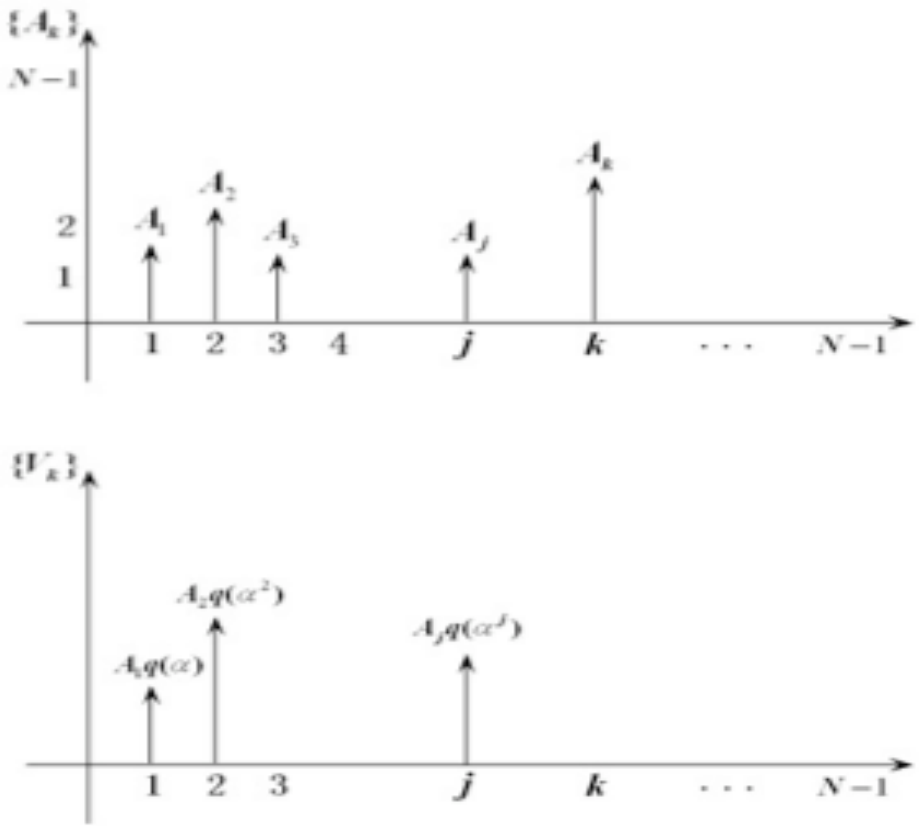


Figure: **Selective DFT Spectra**

Selective DFT (Cont.)

- For the **selective case**, when $q(x)$ is applied to **a**, the nonzero DFT spectra of the resulting sequence is equal to a **subset of the nonzero DFT spectra** of **a**. Thus the linear span of **v** is less than the linear span of **a**.
- The functionality of $q(x)$ here is **analog to filters** used in communication systems for **selecting frequency** band for increasing or reducing bandwidth of transmitted signals.
- Thus $q(x)$ is referred to as **a selective DFT filter of a**.

Computing DFT of Shifted Sequences

- **Question.** Given $\{A_k\}$ and j (consecutive) bits of $\mathbf{s}$, a shift of $\mathbf{a}$, without loss in generality, we could assume that $(s_0, s_1, \cdots, s_{j-1})$ is known, find the DFT of $\mathbf{s}$.
- Since $S_k = \beta^k A_k, \beta \in \mathbb{F}_{2^n}$, it is enough to find β.
- **A Very Old Naive Method**: Directly solving a system of the linear equations in variables $\{\beta^k\}$ where $j = LS(\mathbf{a})$.
- **Selective DFT** when $j = LS(\mathbf{a})$.
- **Fast Selective DFT** when $j < LS(\mathbf{a})$.

A Very Old Naive Method

- If a **set P is a subset** consisting of coset leaders modulo N, then we use $\overline{P}$ to represent the set $\cup_{k\in P} C_k$ where C_k is the coset modulo N containing k as the coset leader.
- We write $\overline{\mathcal{N}}_{\mathbf{a}} = \{k_0, k_1, \cdots, k_{LS(\mathbf{a})-1}\}$ (note that $LS(\mathbf{a})$ is equal to the cardinality of $\overline{\mathcal{N}}_{\mathbf{a}}$.) Then

$$b_t = \sum_{k\in\mathcal{N}_{\mathbf{a}}} Tr(A_k \beta^k \alpha^{tk}) = \sum_{i=0}^{j-1} A_{k_i} \beta^{k_i} \alpha^{tk_i}, t = 0, 1, \cdots, j-1.$$

Let $x_i = \beta^{k_i}, i = 0, 1, \cdots, LS(\mathbf{a}) - 1$. Then the above is a system of m linear equations in $LS(\mathbf{a})$ unknowns $\{x_i\}$.

Naive Method (Cont.)

- Put $m = LS(\mathbf{a})$. The matrix form is given by

$$b = Mx$$

where $s = (s_0, s_1, \cdots, s_{j-1})^T$ where v^T means the transpose of the vector v, $x = (x_0, x_1, \cdots, x_{m-1})^T$, and

$$M = \prod_{i=0}^{l-1} A_{k_i} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha^{k_0} & \alpha^{k_1} & \alpha^{k_2} & \cdots & \alpha^{k_{m-1}} \\ \alpha^{2k_0} & \alpha^{2k_1} & \alpha^{2k_2} & \cdots & \alpha^{2k_{m-1}} \\ \vdots & & & & \\ \alpha^{(j-1)k_0} & \alpha^{(j-1)k_1} & \alpha^{(j-1)k_2} & \cdots & \alpha^{(j-1)k_{m-1}} \end{bmatrix}$$

- M is a $j \times m$ **Vandermonde matrix over** $\mathbb{F}_{2^n}$.

Naive Method (Cont.)

- Thus it has the **unique** solution if and only if $m = j = LS(\mathbf{a})$.
- Hence from known m bits of $\mathbf{s}$ **(not necessarily consecutive)**, the DFT of $\mathbf{s}$ can be uniquely determined by solving a system of m linear equations over $\mathbb{F}_{2^n}$ with **computational complexity** $O(m^{2.37}\eta(n))$ where $\eta(n) = n \log n \log\log n$.

Selective DFT Attack

Input: Given $(a_0, \cdots, a_{j-1})$ and $\{A_k\}$ where $j = LS(\mathbf{a})$ with spectral sequence $\beta^k A_k, k = 0, \cdots, N-1$.
Output: β.
Procedure

- **Randomly** select $k \in \mathcal{N}_{\mathbf{a}}$ with coset size n (not necessary $\gcd(k, N) = 1$), and set $q(x) = p(x)/p_k(x)$ with $r = deg(q) = m - n$.
- **Applying $q(L)$ to $(s_0, s_1, \cdots)$**, compute

$$v_t = \sum_{i=0}^{r} c_i s_{i+t}, t = 0, 1, \cdots, n-1.$$

- From

$$v_t = Tr(\gamma \alpha^{tk}), t = 0, 1, \cdots, n-1$$

solve for γ in a system of n linear equations over $\mathbb{F}_{2^n}$ with the complexity $O(n^{2.37}\eta(n))$. (Compared with the naive method $O(m^{2.37}\eta(n))$ where $m >> n$.)

Selective DFT Attack (Cont.)

- Note that $\gamma = A_k q(\alpha^k)\beta^k$. If $\gcd(k, N) = 1$, we obtain

$$\beta = \gamma^{k'}[A_k q(\alpha^k)]^{-k'}, k' = k^{-1}.$$

- If $\gcd(k, N) \neq 1$, using the **multiplexing** method to reconstruct β (omitted there for the multiplexing method).

Fast Selective DFT Attack

Input: Given $(a_0, \cdots, a_{j-1})$ and $\{A_k\}$ where $j < LS(\mathbf{a})$ with spectral sequence $\beta^k A_k, k = 0, \cdots, N-1$.
Output: β.
Procedure

- Select $\mathbf{b} = \{b_t\}$ to compute the **term-by-term product** $\mathbf{u} = \{u_t\}$ (i.e., $u_t = s_t b_t$) where $b_t = B(\beta\alpha^t), t \geq 0$ and $u_t = U(\beta\alpha^t)$ with $|\overline{\mathcal{N}}_{\mathbf{b}} \cup \overline{\mathcal{N}}_{\mathbf{u}}| < LS(\mathbf{s})$.
- Compute $m_{\mathbf{u}}(x)$, the minimal polynomial of $\mathbf{u}$, and $q(x) = \prod_{k \in \mathcal{T}} p_k(x)$ where

$$\mathcal{T} = \begin{cases} \mathcal{N}_{\mathbf{u}} \setminus \mathcal{N}_{\mathbf{b}} & \emptyset \subseteq \mathcal{N}_{\mathbf{u}} \cap \mathcal{N}_{\mathbf{b}} \subset \mathcal{N}_{\mathbf{u}} \quad \textbf{Type 1} \\ \subset \mathcal{N}_{\mathbf{u}}^* & \mathcal{N}_{\mathbf{b}}^* = \mathcal{N}_{\mathbf{u}}^* \quad \textbf{Type 2} \end{cases}$$

where $\mathcal{T}$ contains at least one k with coset size n for the type 2 and $\mathcal{N}_{\mathbf{x}}^*$ denotes the set of nonzero coset leaders in $\mathcal{N}_{\mathbf{x}}$.

Fast Selective DFT Attack (Cont.)

- $\Longrightarrow$ degree of $q(x)$ is $r = |\overline{\mathcal{T}}|$, and $n \le r < LS(\mathbf{u})$.
- For $q(L) = \sum_{i=0}^{r} c_i L^i$, compute

$$\gamma_{k,t} = U_k q(\alpha^k)\alpha^{tk}, \quad k \in \overline{\mathcal{J}}, \begin{cases} \mathcal{J} = \mathcal{N}_{\mathbf{b}} \cap \mathcal{N}_{\mathbf{u}} & \textbf{for } q(x) \textbf{ of type 1} \\ \mathcal{J} = \mathcal{N}_{\mathbf{b}} \setminus \mathcal{T} & \textbf{for } q(x) \textbf{ of type 2} \end{cases}$$
$$t = 0, 1, \cdots, LS(\mathbf{b}) - 1.$$

  where $J \subseteq \mathcal{N}_{\mathbf{b}}$.

- Compute

$$\eta_{k,t} = B_k f_t(\alpha^k)\alpha^{tk}, t = 0, 1, \cdots, LS(\mathbf{b}) - 1, k \in \overline{\mathcal{N}}_{\mathbf{b}}$$
$$f_t(x) = \sum_{i=0}^{r} c_i s_{i+t} x^i$$

- Form a **system of $LS(\mathbf{b})$ equations:**

$$\sum_{k \in \overline{\mathcal{J}}} \gamma_{k,t}\beta^k = \sum_{k \in \overline{\mathcal{N}}_{\mathbf{b}}} \eta_{k,t}\beta^k, t = 0, 1, \cdots, LS(\mathbf{b}) - 1.$$

  which are in $LS(\mathbf{b})$ unknowns β^k ($\overline{\mathcal{N}}_{\mathbf{b}} = LS(\mathbf{b})$), and solve for $\beta^k \Longrightarrow \beta$.

Applications to Attacks on Stream Ciphers

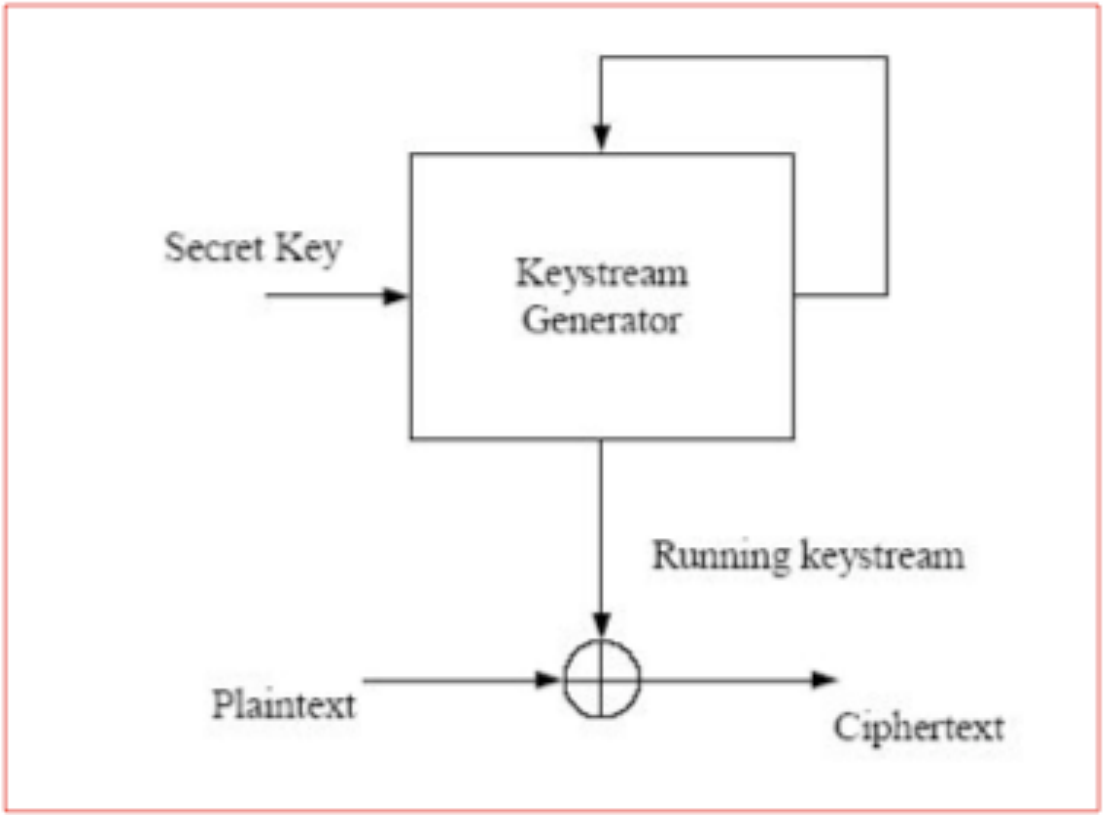


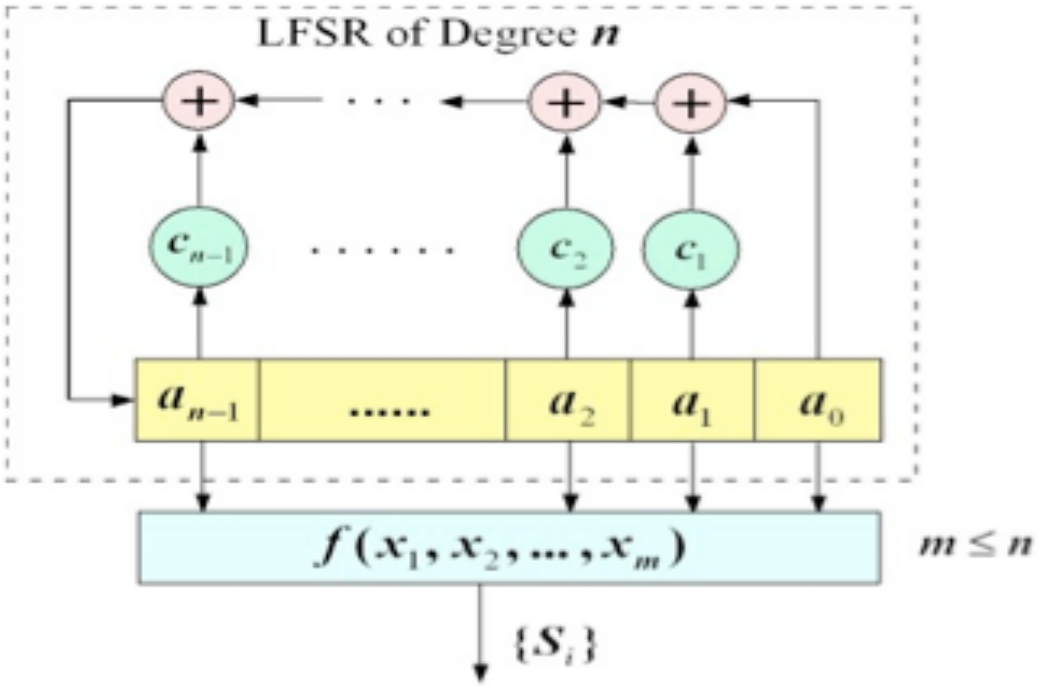
Figure: **A General Model of Stream Cipher**

Example: Filtering Sequence Generators

- Let $\mathbf{w} = \{w_t\}$ be an m-sequence of period $2^n - 1$, and $0 \le d_0 < d_1 < \cdots < d_{m-1} < n$. A sequence $\mathbf{s} = \{s_t\}$ is referred to as a **filtering sequence** if

$$s_t = f(w_{d_0+t}, w_{d_1+t}, \cdots, w_{d_{m-1}+t}) =, t = 0, 1, \cdots \tag{3}$$

where $f(x_0, x_1, \cdots, x_{m-1})$ is a boolean function in m variables. The boolean function f is referred to as a **filtering function**.



Known Plaintext Attack

- An **initial state** of the LFSR is a key when $\{s_t\}$ is served as a key stream generator, denoted by $K = (k_0, \cdots, k_{n-1}), k_i \in \mathbb{F}_2$.
- Then

$$s_t = f(L^t(k_0, k_1, \cdots, k_{n-1})) = f_t(k_0, \cdots, k_{n-1}), t = 0, 1, \cdots$$

where

$$f_t(x_0, \cdots, x_{n-1}) = f(L^t(x_0, \cdots, x_{n-1})).$$

- **Known plaintext attack**: if a certain plaintext is known, then some bits of $\{s_t\}$ can be recovered. If the key can be recovered from those known bits of $\{s_t\}$, then the rest of bits of the key stream can be reconstructed.

Properties of Filtering Sequence Generators

- We denote the degree of $f(x_0, \cdots, x_{m-1})$ by $deg(f)$. The DFT of $\{s_t\}$ has the following structure:

$$S_k = 0, \textbf{ for } H(k) \geq deg(f)$$

  where $H(k)$ is the Hamming weight of k.
- **w** has the trace representation $Tr(\beta x)$ for some $\beta \in \mathbb{F}_{2^n}$. Thus those β's and initial states of the LFSR are in **one-to-one correspondence**.
- Let $\{a_t\}$ be a filtering sequence corresponds to an initial state with $\beta = 1$. Then any filtering sequence **s is a shift of a**.

Shifts and Keys

- **Recovering a key** in the filtering sequence is to recover an **initial state** in the LFSR, which is equal to **recover** β.
- The **initial state of the LFSR** can be recovered
  - by either the **selective DFT** if the number of known consecutive bits of $\{s_t\}$ is equal to the linear span of $\{s_t\}$,
  - or by the **fast selective DFT** if it is less than its linear span, as presented before.

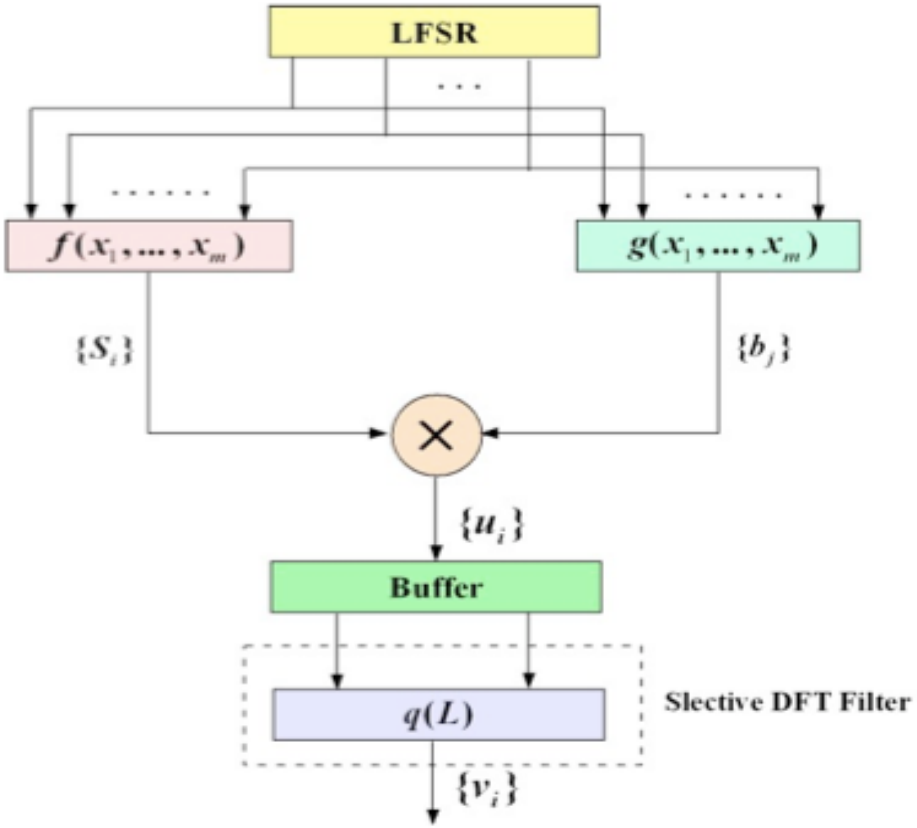


Figure: **(Fast) Select DFT Attacks on a Filtering Generator**

How Good the Selective DFT Attack?

Case 1: # required consecutive bits $= LS(\mathbf{s})$

- Rønjom-Helleseth (06): $q(x)$ is the quotient of the minimal polynomial of $\mathbf{s}$ and the minimal polynomial of α. So, $q(L)$ **removes all DFT spectra except for A_1**. It works if $A_1 \neq 0$.
- Rønjom-Gong-Helleseth (07): $q(x)$ is the quotient of the minimal polynomial of $\mathbf{s}$ and the minimal polynomial of α^k. So, $q(L)$ **removes all DFT spectra except for A_k** for some k with $A_k \neq 0$ and $\gcd(k, N) = 1$.
- **Selective DFT (new case)**: In Rønjom-Gong-Helleseth (07)'s work, k does not need to be relatively coprime with N, it is enough that the coset size of k is equal to n.

Selective DFT and Rønjom *et al.* Attacks

Rønjom-Helleseth (06)			
# required	# unknowns	$deg(q)$	solvable
consecutive bits	in equations		
$LS(\mathbf{s})$	n	$LS(\mathbf{s}) - n$ not applicable if $A_1 = 0$	solving a system of homogeneous equations over $\mathbb{F}_2$ in n unknowns solve for all n unknowns

Selective DFT and Rønjom *et al.* Attacks (Cont.)

Rønjom-Gong-Helleseth (07)			
# required consecutive bits	# unknowns in equations	$deg(q)$	solvable
$LS(\mathbf{s})$	n	$LS(\mathbf{s}) - n$ not applicable if $\gcd(k, N) \neq 1$	solving a system of homogeneous equations over $\mathbb{F}_{2^n}$ in n unknowns obtaining one unknown is enough
New Case of Selective DFT			
Replace the condition $\gcd(k, N) = 1$ by $\lvert C_k \rvert = n$			

Compared with Fast Algebraic Attack

Case 2: # required consecutive bits $< LS(\mathbf{s})$

Summary of the time complexity and required known bits of the linearization, algebraic attack, and fast algebraic attacks.

Methods and Equations	The Number of Unknowns	Minimum Required Known Bits
Linearization (folk sense): $f_t(K) = s_t$	T_μ $\mu = deg(f)$	T_μ
Algebraic Attack : (Paratin'96, Courtois *et al.*'03) Find g such that $fg = 0$ $s_t g_t(K) = 0$	T_τ $\tau = deg(g)$ The best case: τ=algebraic immunity of f<μ	T_τ
Fast Algebraic Attacks: (Courtois'03 [a], Armknecht-Ars'05 [b]): a) find g such that $fg = h \neq 0$; b) applying $q(x)$ to $s_t g_t(K) = h_t(K)$ $\sum_{i=0}^{r} c_i s_{i+t} g_{i+t}(K) = \sum_{i=0}^{r} c_i h_{i+t}(K)$	T_d $d = deg(g)$, $e = deg(h)$	$\gamma = T_d + (T_e - \delta T_d)$ $\delta = 0$ [a], $\delta = 1$ [b]; $d < e$ $r = deg(q)$ consecutive bits

Fast Algebraic Attack

- The case of Courtois'03: $q(x)$ is the product of the minimal polynomials of α^k for all k with $H(k) \leq d$ $(= deg(g))$, so $\{v_t\}$ **is a zero sequence**.
- The case of Armknecht-Ars'05: $q(x)$ **is equal to** $p_e(x)/p_d(x)$ where $p_k(x)$ is the product of the minimal polynomials of α^i for all i with $H(i) \leq k$. So nonzero spectra of the DFT of $\{v_t\}$ is a subset of that of **b**.
- In order to get T_d **equations** from applying $q(L)$ to $\{s_t g_t(k_0, k_1, \cdots, k_{n-1})\}$, it needs to know $(s_0, s_1, \cdots, s_{T_d+deg(q)-1})$ for creating a system of homogeneous equations in linearized variables of **boolean function** $g_t(k_0, k_1, \cdots, k_{n-1})$**.**

Compared with Fast Algebraic Attack

	# required consecutive bits	# unknowns in equations	$deg(q)$	solvable
Fast Algebraic Attack	$T_d + (T_e - \delta T_d)$	T_d	$T_e - \delta T_d$	solving a system of homogeneous equations over $\mathbb{F}_2$ in T_d unknowns
Fast Selective DFT Attack	$LS(\mathbf{b}) + deg(q)$	$LS(\mathbf{b}) < T_d$	$< LS(\mathbf{u}) < T_e - T_d$	solving a system of homogeneous equations over $\mathbb{F}_{2^n}$ in $LS(\mathbf{b})$ unknowns,

Difference between the Fast Algebraic Attacks and Selective DFT Attacks

- **Coefficients** of monomial terms in $b_t = g_t(x_0, x_1, \cdots, x_{n-1})$ in variables $x_0, x_1, \cdots, x_{n-1}$ are **changed for each** t, but the DFT of $\{b_t\}$ are only changed by a **scalar multiple of** β^k where β corresponds to the desired initial state.
- The number of nonzero coefficients of variables (linearized case) in $g_t(x_0, x_1, \cdots, x_{n-1})$ are **dynamically changed** which is **bounded by** T_d, but the number of nonzero DFT spectral of $\{b_t\}$ remains as a **constant which is** $LS(\mathbf{b})$, the linear span of $\mathbf{b}$.
- This phenomenon is not **astonished**, since it is an analogue to a cosine function $\cos x$ which is hard to predict the values in reals. But the Fourier transform of $\cos x$ has only **two pulses (i.e., two values)**, which is a simplest case in spectral analysis.

Spectral Immunity

Resistant to Fast Selective DFT Attack

The sequence $\mathbf{s}$ is said to be *resistant to the fast selective DFT attack* if $|\mathcal{N}_{\mathbf{s}}| = 1$ (i.e., the minimal polynomial of $\mathbf{s}$ is irreducible) or $LS(\mathbf{u}+\mathbf{b}) \geq LS(\mathbf{s})$ for any sequence $\mathbf{b} \in \mathbb{Z}_2^N$ with $LS(\mathbf{b}) < LS(\mathbf{s})$ and $\mathbf{u} \neq 0$, where $\mathbf{u}$ is the term-by-term product sequence of $\mathbf{s}$ and $\mathbf{b}$.

Spectral Immunity

Let

$$P_{\mathbf{s}} = \min_{\mathbf{b} \in \mathbb{Z}_0^N} \{LS(\mathbf{b}) \,|\, \mathbf{s} \cdot \mathbf{b} = 0 \text{ or } (\mathbf{s}+1)\mathbf{b} = 0\}.$$

Then $P_{\mathbf{s}}$ is referred to as the ***spectral immunity*** of $\mathbf{s}$.

Example: Filtering Generator

- Let **w** be a sequence generated by the primitive polynomial $x^4 + x + 1$, and **s** be a **filtering sequence** generated by $s_t = f(w_t, w_{t+1}, w_{t+2}, w_{t+3})$, where $f(x_0, x_1, x_2, x_3) = x_1 + x_0x_2 + x_0x_3 + x_0x_1x_2$.
- $LS(\mathbf{s}) = \sum_{i=1}^{3} \binom{4}{i} = 14$ which is the maximal achievable linear complexity for a filtering function of degree 3.
- The **algebraic immunity** of f, $AI(f)$, is equal to 2.
- Then $P_{\mathbf{s}}$ is not bigger than the linear complexity of a sequence $b_t = g(w_t, w_{t+1}, w_{t+2}, w_{t+3})$, where g is in a function in the set consisting of the annihilators of f, i.e., $g \in ANN(f) = \{g \mid fg = 0 \text{ or } (f+1)g = 0\}$.
- It is easily verified that $P_{\mathbf{s}} \leq \sum_{i=1}^{AI(f)} \binom{4}{i} = 10$.
- Let $b_t = w_t + w_{t+2} + w_tw_{t+1} + w_{t+1}w_{t+2} + w_tw_{t+3}$, then $LS(\mathbf{b}) = 4$ with the minimal polynomial $x^4 + x^3 + x^2 + x + 1$. Thus $P_{\mathbf{s}} = 4$.

Example: Filtering Generator (Cont.)

- This means that there exist an annihilator which yields a system containing linear equations in **at most 4 unknowns**, while applying a fast algebraic attack one ends up with a **quadratic equation system** with 10 unknowns.

Open Questions

- How to construction functions which are **resistant** to the fast selective DFT attack ?(Note that stop-and-go generated sequences resist this attack, why?)
- **What** is the bounds of spectral immunity?
- The method introduced here is of **only theoretical** interests, if the **DFT spectra** is unknown. In general, the degree of the filtering function or combiner functions are relatively easier to obtain than the DFT of the key stream sequences, which leads to the following problem.
- How to estimate the DFT spectrum of the **product** sequence?

Reference

- Guang Gong, Sondre Rønjom, Tor Helleseth, and Honggang Hu, Fast Linear Subspace Attacks on Stream Ciphers, Technical Report, CACR 2009-04, 2009, University of Waterloo, Canada. Submitted to *IEEE Transactions on Information Theory*.