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
We associate $f(x_0, \cdots, x_{n-1})$ with
\[ f(x_0, \cdots, x_{n-1} = c_0x_0 + \cdots + c_{n-1}x_{n-1} \leftrightarrow t(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + 1 \]
a polynomial over $\mathbb{F}_2$.

An output sequence of the LFSR satisfies the following recursive relation
\[ a_{n+k} = \sum_{i=0}^{n-1} c_ia_{k+i}, \quad k = 0, 1, \cdots, \quad (1) \]

$(a_0, \cdots, a_{n-1})$ 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).
The sequence $a = 1001011$ is an $m$-sequence of period 7 generated by an LFSR with $t(x) = x^3 + x + 1$. 
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 \( LS(a) \), and \( m(x) \) can be found using the Berlekamp-Massey algorithm from any \( 2LS(a) \) consecutive bits of \( a \).
The Shift Operator

- The \textbf{(Left cyclically) shift operator} $L$:

\[
L \mathbf{a} = a_1, a_2, \ldots,
\]
\[
L' \mathbf{a} = a_r, a_{r+1}, \ldots.
\]

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

\begin{itemize}
  \item \textbf{Example}: let
  \[
  \mathbf{a} = 1001011
  \]
  \[
  \mathbf{b} = 1011100
  \]
  \[
  \mathbf{c} = 1110100
  \]
  \end{itemize}

then \textbf{a and b are shift equivalent}, and \textbf{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 $N$; $\alpha$: 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

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

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

\[
A(x) = \sum_k Tr_{m_k}^{m_k}(A_k x^k)
\]  \( (2) \)

where the \( k \)'s are (cyclotomic) coset leaders modulo \( N \), \( m_k | n \) is the length of the coset which contains \( k \), and \( Tr_{m_k}^{m_k}(x) \) 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

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

<table>
<thead>
<tr>
<th>Sequences in Time Domain</th>
<th>DFT Spectral Sequences in Frequency Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a = 00010 \ 01101 \ 01111$</td>
<td>$A = 011010001000000$</td>
</tr>
<tr>
<td>$b = 111011000101001$</td>
<td>$B = 011 \alpha \ 1 \ 0 \ \alpha^2 \alpha^6 \ 1 \alpha^8 \ 0 \ \alpha^3 \ \alpha^4 \ \alpha^9 \ \alpha^{12}$</td>
</tr>
</tbody>
</table>
### Example 1 (cont.)

<table>
<thead>
<tr>
<th>Trace Representation</th>
<th>Linear Span</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A(x) = Tr(x)$</td>
<td>4</td>
</tr>
<tr>
<td>$a_t = Tr(\alpha^t), 0 \leq t &lt; 15$</td>
<td></td>
</tr>
<tr>
<td>$B(x) = Tr(x + \alpha x^3 + \alpha^6 x^7)$</td>
<td>12</td>
</tr>
<tr>
<td>$b_t = B(\alpha^t), 0 \leq t &lt; 15$</td>
<td></td>
</tr>
</tbody>
</table>
A sequence $b = \{b_t\}$ is a **shift** of $a$ if and only if in the DFT of $b$ is given by

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

In this case,

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

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

The shift operator **does not change** the minimal polynomial of $a$, nor the linear span.
For $\alpha$, a primitive root of $x^4 + x + 1$ which defines $\mathbb{F}_{2^4}$, let

$$a = 00010\ 01101\ 01111$$
$$b = 01101\ 01111\ 00010$$

$A(x) = Tr(x)$, and
$B(x) = Tr(\alpha^5 x)$

In this case $b = L^5 a$, a shift of $a$. 
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 \( c = a \cdot b \) 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 \( C = A \ast B \) where

\[
C_k = \sum_{i+j=k \pmod{N}} A_i B_j, \quad 0 \leq k < N.
\]
Example 3

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

\[
\begin{align*}
\textbf{b} &= 111011000101001 \leftrightarrow B(x) = Tr(x + \alpha x^3 + \alpha^6 x^7) \\
\textbf{a} &= 000110001100011 \leftrightarrow A(x) = Tr(\alpha^2 x^3) \\
\end{align*}
\]

\[\text{⇒} \quad \textbf{c} = \textbf{a} \cdot \textbf{b} = 000010000100001 \leftrightarrow C = B \ast A\]

\[\text{⇒} \quad C(x) = B(x)A(x) = Tr(\alpha^3 x^3) + 1\]
Selective or Fast Selective DFT Attacks

Selective Filters in DFT Domain

Let

$$\mathcal{N}_a = \{ k \mid A_k \neq 0, k \text{ is a coset leader } \mod N \}$$,

$$p_k(x)$$ be the minimal polynomial (MP) of $$\alpha^k$$ 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 $$a$$ is equal to the product of $$p_k$$ for all $$k \in \mathcal{N}_a$$.

Applying $$q(L)$$ to $$a$$, we have

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

which is a linear filtered sequence from $$a$$. 
Proposition 1. The DFT of \( \{ v_t \} \) is given by

\[ V_k = A_k q(\alpha^k), \quad 0 \leq k < N. \]
Interesting Cases of DFT of \( \{v_t\} \)

Two Extreme Cases:

- **Case 1.** \( p(x) \mid q(x) \). Thus \( q(\alpha^k) = 0, \forall k \in \mathcal{N}_a \). Hence

  \[
  V_k = 0, 0 \leq k < N \implies v \text{ is a zero sequence.}
  \]

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

  \[
  (V_k = 0 \iff A_k = 0)
  \]

\( \{v\} \) has the **same minimal polynomial** as \( s \), so does \( a \), and \( v \) is a shift of \( a \) when \( \alpha \) is a primitive element in \( \mathbb{F}_{2^n} \) (in this case \( a \) has period \( 2^n - 1 \)).
Let \( c(x) = \gcd(p(x), q(x)), c(x) \neq 1 \text{ and } c(x) \neq p(x) \). Then

\[
c(x) = \prod_{k \in T} p_k(x)
\]

where \( T \subset N_a \), and

\[
V_k = q(\alpha^k)A_k \neq 0 \iff q(\alpha^k) \neq 0 \iff k \in N_a \setminus T.
\]
Figure: Selective DFT Spectra
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 \( s \), a shift of \( a \), without loss in generality, we could assume that \((s_0, s_1, \cdots, s_{j-1})\) is known, find the DFT of \( s \).

- Since \( S_k = \beta^k A_k, \beta \in \mathbb{F}_{2^n} \), it is enough to find \( \beta \).

- **A Very Old Naive Method:** Directly solving a system of the linear equations in variables \( \{\beta^k\} \) where \( j = LS(a) \).

- **Selective DFT** when \( j = LS(a) \).

- **Fast Selective DFT** when \( j < LS(a) \).
If a **set** \( P \) **is a subset** consisting of coset leaders modulo \( N \), then we use \( \overline{P} \) to represent the set \( \bigcup_{k \in P} C_k \) where \( C_k \) is the coset modulo \( N \) containing \( k \) as the coset leader.

We write \( \overline{N}_a = \{ k_0, k_1, \cdots, k_{LS(a) - 1} \} \) (note that \( LS(a) \) is equal to the cardinality of \( \overline{N}_a \)). Then

\[
 b_t = \sum_{k \in \overline{N}_a} \text{Tr}(A_k \beta^k \alpha^{tk}) = \sum_{i=0}^{j-1} A_{ki} \beta^{ki} \alpha^{tk_i}, \quad t = 0, 1, \cdots, j - 1.
\]

Let \( x_i = \beta^{ki}, \quad i = 0, 1, \cdots, LS(a) - 1 \). Then the above is a system of \( m \) linear equations in \( LS(a) \) unknowns \( \{x_i\} \).
Naive Method (Cont.)

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

\[
b = Mx
\]

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

\[
M = \prod_{i=0}^{l-1} A_{k_i}
\]

\[
\begin{bmatrix}
1 & 1 & 1 & \cdots & 1 \\
\alpha^{k_0} & \alpha^{k_1} & \alpha^{k_2} & \cdots & \alpha^{k_{m-1}} \\
\alpha^{2k_0} & \alpha^{2k_1} & \alpha^{2k_2} & \cdots & \alpha^{2k_{m-1}} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\alpha^{(j-1)k_0} & \alpha^{(j-1)k_1} & \alpha^{(j-1)k_2} & \cdots & \alpha^{(j-1)k_{m-1}}
\end{bmatrix}
\]

- \( M \) is a \( j \times m \) Vandermonde matrix over \( \mathbb{F}_{2^n} \).
Thus it has the **unique** solution if and only if \( m = j = LS(a) \).

Hence from known \( m \) bits of \( s \) (not necessarily consecutive), the DFT of \( s \) 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 \(j = LS(a)\) with spectral sequence \(\beta^k A_k, k = 0, \cdots, N - 1\).

Output: \(\beta\).

Procedure

- Randomly select \(k \in \mathbb{N}_a\) with coset size \(n\) (not necessary \(gcd(k, N) = 1\)), and set \(q(x) = p(x)/p_k(x)\) with \(r = \text{deg}(q) = m - n\).

- 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 \(\gamma\) in a system of \(n\) linear equations over \(\mathbb{F}_{2^n}\) with the complexity \(O(n^{2.377} \eta(n))\). (Compared with the naive method \(O(m^{2.377} \eta(n))\) where \(m >> n\).)
Note that $\gamma = A_k q(\alpha^k)\beta^k$. If $\gcd(k, N) = 1$, we obtain

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

If $\gcd(k, N) \neq 1$, using the **multiplexing** method to reconstruct $\beta$ (omitted there for the multiplexing method).
Fast Selective DFT Attack

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

Output: \(\beta\).

Procedure

1. Select \(b = \{b_t\}\) to compute the term-by-term product \(u = \{u_t\}\) (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 \(|N_b \cup N_u| < LS(s)|\).
2. Compute \(m_u(x)\), the minimal polynomial of \(u\), and \(q(x) = \prod_{k \in \mathcal{T}} p_k(x)\) where

\[
\mathcal{T} = \begin{cases} 
N_u \setminus N_b & \emptyset \subset N_u \cap N_b \subset N_u & \text{Type 1} \\
\subset N_u^* & N_b^* = N_u^* & \text{Type 2}
\end{cases}
\]

where \(\mathcal{T}\) contains at least one \(k\) with coset size \(n\) for the type 2 and \(N_x^*\) denotes the set of nonzero coset leaders in \(N_x\).
→ degree of \( q(x) \) is \( r = |\overline{\mathcal{I}}| \), and \( n \leq r < LS(u) \).

For \( q(L) = \sum_{i=0}^{r} c_i L^i \), compute

\[
\gamma_{k,t} = U_k q(\alpha^k) \alpha^{tk}, \quad k \in \overline{\mathcal{J}}, \quad \begin{cases} 
\mathcal{J} = \mathcal{N}_b \cap \mathcal{N}_u & \text{for } q(x) \text{ of type 1} \\
\mathcal{J} = \mathcal{N}_b \setminus \mathcal{T} & \text{for } q(x) \text{ of type 2}
\end{cases}
\]

\( t = 0, 1, \cdots, \text{LS}(b) - 1 \).

where \( J \subseteq \mathcal{N}_b \).

Compute

\[
\eta_{k,t} = B_k f_t(\alpha^k) \alpha^{tk}, \quad t = 0, 1, \cdots, \text{LS}(b) - 1, \quad k \in \overline{\mathcal{N}}_b
\]

\[
f_t(x) = \sum_{i=0}^{r} c_i S_{i+t} x^i
\]

Form a system of \( LS(b) \) equations:

\[
\sum_{k \in \overline{\mathcal{J}}} \gamma_{k,t} \beta^k = \sum_{k \in \overline{\mathcal{N}}_b} \eta_{k,t} \beta^k, \quad t = 0, 1, \cdots, \text{LS}(b) - 1.
\]

which are in \( LS(b) \) unknowns \( \beta^k \) (\( \overline{\mathcal{N}}_b = LS(b) \)), and solve for \( \beta^k \Rightarrow \beta \).
Applications to Attacks on Stream Ciphers

Figure: A General Model of Stream Cipher
Example: Filtering Sequence Generators

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

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

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

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

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

\[
S_k = 0, \quad \text{for } H(k) \geq \text{deg}(f)
\]

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 \( \beta \)'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 \( a \).
Recovering a key in the filtering sequence is to recover an initial state in the LFSR, which is equal to recover $\beta$.

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
Case 1: # required consecutive bits = $LS(s)$

- Rønjom-Helleseth (06): $q(x)$ is the quotient of the minimal polynomial of $s$ and the minimal polynomial of $\alpha$. 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 $s$ and the minimal polynomial of $\alpha^k$. 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

<table>
<thead>
<tr>
<th>Rønjom-Helleseth (06)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong># required</strong></td>
</tr>
<tr>
<td>consecutive bits</td>
</tr>
<tr>
<td>$LS(s) - n$</td>
</tr>
</tbody>
</table>

- **G. Gong (University of Waterloo)**
- **Fast DFT Attacks**
- **2009 37 / 47**
**Selective DFT and Rønjom *et al.* Attacks (Cont.)**

<table>
<thead>
<tr>
<th>Rønjom-Gong-Helleseth (07)</th>
</tr>
</thead>
<tbody>
<tr>
<td># required consecutive bits</td>
</tr>
<tr>
<td>$LS(s)$</td>
</tr>
</tbody>
</table>

New Case of Selective DFT

Replace the condition $\gcd(k, N) = 1$ by $|C_k| = n$
## Compared with Fast Algebraic Attack

### Case 2: # required consecutive bits $< LS(s)$

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

<table>
<thead>
<tr>
<th>Methods and Equations</th>
<th>The Number of Unknowns</th>
<th>Minimum Required Known Bits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Linearization</strong> (folk sense): $f_t(K) = s_t$</td>
<td>$T_\mu$</td>
<td>$T_\mu$</td>
</tr>
<tr>
<td>$\mu = \deg(f)$</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Algebraic Attack</strong> :</td>
<td>$T_\tau$</td>
<td>$T_\tau$</td>
</tr>
<tr>
<td>(Paratin'96, Courtois et al.'03)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Find $g$ such that $fg = 0$</td>
<td>$\tau = \deg(g)$</td>
<td></td>
</tr>
<tr>
<td>$s_t g_t(K) = 0$</td>
<td>The best case:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$\tau =$ algebraic immunity of $f_{&lt;\mu}$</td>
<td></td>
</tr>
<tr>
<td><strong>Fast Algebraic Attacks</strong>:</td>
<td>$T_d$</td>
<td>$\gamma = T_d + (T_e - \delta T_d)$</td>
</tr>
<tr>
<td>(Courtois'03 [a], Armknecht-Ars'05 [b]):</td>
<td></td>
<td>$\delta = 0$ [a], $\delta = 1$ [b]; $d &lt; e$</td>
</tr>
<tr>
<td>a) find $g$ such that $fg = h \neq 0$;</td>
<td>$d = \deg(g)$, $e = \deg(h)$</td>
<td></td>
</tr>
<tr>
<td>b) applying $q(x)$ to $s_t g_t(K) = h_t(K)$</td>
<td></td>
<td>$r = \deg(q)$</td>
</tr>
<tr>
<td>$\sum_{i=0}^{r} c_i s_{i+t} g_{i+t}(K) = \sum_{i=0}^{r} c_i h_{i+t}(K)$</td>
<td></td>
<td>Consecutive bits</td>
</tr>
</tbody>
</table>
The case of Courtois’03: $q(x)$ is the product of the minimal polynomials of $\alpha^k$ 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 $\alpha^i$ 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 $\{s_tg_t(k_0, k_1, \cdots, k_{n-1})\}$, 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

<table>
<thead>
<tr>
<th></th>
<th># required consecutive bits</th>
<th># unknowns in equations</th>
<th>$\text{deg}(q)$</th>
<th>solvable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast Algebraic Attack</td>
<td>$T_d + (T_e - \delta T_d)$</td>
<td>$T_d$</td>
<td>$T_e - \delta T_d$</td>
<td>solving a system of homogeneous equations over $\mathbb{F}_2$ in $T_d$ unknowns</td>
</tr>
<tr>
<td>Fast Selective DFT Attack</td>
<td>$\text{LS}(\mathbf{b}) + \text{deg}(q)$</td>
<td>$\text{LS}(\mathbf{b}) &lt; T_d$</td>
<td>$\text{LS}(\mathbf{u}) &lt; T_e - T_d$</td>
<td>solving a system of homogeneous equations over $\mathbb{F}_{2^n}$ in $\text{LS}(\mathbf{b})$ unknowns,</td>
</tr>
</tbody>
</table>
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** \( \beta^k \) where \( \beta \) 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** \( LS(b) \), the linear span of \( b \).

- 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.
Resistant to Fast Selective DFT Attack

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

Spectral Immunity

Let

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

Then $P_s$ is referred to as the spectral immunity of $s$. 
Example: Filtering Generator

Let \( \mathbf{w} \) be a sequence generated by the primitive polynomial \( x^4 + x + 1 \), and \( \mathbf{s} \) be a \textbf{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 \textbf{algebraic immunity} of \( f \), \( AI(f) \), is equal to 2.

Then \( P_s \) 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 \( P_s \leq \sum_{i=1}^{4} \binom{4}{i} = 10. \)

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 \( P_s = 4 \).
This means that there exist an annihilator which yields a system containing linear equations in \textit{at most 4 unknowns}, while applying a fast algebraic attack one ends up with a \textit{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?