Selective DFT Attacks on Stream Ciphers and Spectral Immunity of Boolean Functions

Honggang Hu

Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1, Canada
Email: h7hu@ecemail.uwaterloo.ca

Joint work with Guang Gong, Sondre Rønjom, and Tor Helleseth.

February 25, 2010

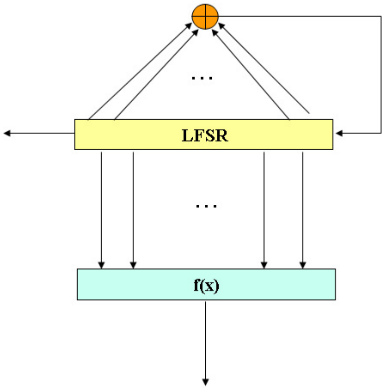
Boolean Functions

- Any boolean function f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ can be represented as a multivariate polynomial over $\mathbb{F}_2$ (**algebraic normal form**),

$$f(x_1, x_2, ..., x_n) = a_0 + \sum_{1\le i\le n} a_i x_i + \sum_{1\le i<j\le n} a_{i,j} x_i x_j + ... + a_{1,2,...,n} x_1 x_2 ... x_n,$$

  where $a_0, a_i, a_{i,j}, ..., a_{1,2,...,n} \in \mathbb{F}_2$.
- The **algebraic degree** of f is the algebraic degree of its algebraic normal form.

Filtering Generators



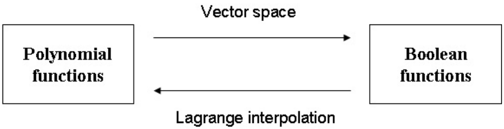
Algebraic Attacks

N. Courtois and W. Meier, 2003,

- The **algebraic immunity** $AI(f)$ of f is the minimal degree of g such that $fg = 0$ or $(f+1)g = 0$.
- $f(L^t(k_0, k_1, ..., k_{n-1})) \cdot g(L^t(k_0, k_1, ..., k_{n-1})) = 0$
- $AI(f) \leq \lceil \frac{n}{2} \rceil$

Correspondence

- Polynomial functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$
- Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$



Polynomial Form

- Let $f(x)$ be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.
- The polynomial form of $f(x)$:

$$f(x) = \sum_{k=0}^{2^n-1} F_k x^k, x \in \mathbb{F}_{2^n}$$

- $F_k \in \mathbb{F}_{2^n}$, and $F_{2^i k} = F_k^{2^i}, i = 0, 1, ..., n-1$
- The **algebraic degree** of f is given by the largest **Hamming weight** of k such that $F_k \neq 0$.
- $N(f)$: the number of nonzero coefficients, i.e., $N(f) = |\{F_k | F_k \neq 0, k = 0, 1, ..., 2^n - 1\}|$

Trace Representation

- Any nonzero function $f(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ can be represented as

$$f(x) = \sum_{k \in \Gamma(n)} Tr_1^{n_k}(F_k x^k) + F_{2^n-1} x^{2^n-1}, F_k \in \mathbb{F}_{2^{n_k}}, F_{2^n-1} \in \mathbb{F}_2$$

- $\Gamma(n)$ is the set consisting of all **coset leaders** modulo $2^n - 1$, $n_k | n$ is the size of the coset C_k, and $Tr_1^{n_k}(x)$ is the **trace function** from $\mathbb{F}_{2^{n_k}}$ to $\mathbb{F}_2$.

An Example

- $\mathbb{F}_{2^3} : x^3 + x + 1 = 0$
- Let $\alpha \in \mathbb{F}_{2^3}$ satisfy $\alpha^3 + \alpha + 1 = 0$.
- $\{1, \alpha, \alpha^2\}$
- $f(x) = Tr(x^3)$
- $x = x_0 + x_1\alpha + x_2\alpha^2$
- $g(x_0, x_1, x_2) = f(x) = x_0 + x_1 + x_2 + x_1x_2$

Selective DFT Attacks

- $f(x)$ is the key stream generating function, i.e., $\{f(\beta\alpha^i)\}$ is the key stream, and β **is the key**
- Find $g(x)$ with **small** $N(g)$ such that $fg = 0$ or $(1+f)g = 0$
- $fg = 0 \Rightarrow$ if $f(\beta\alpha^i) = 1$, then $g(\beta\alpha^i) = 0$
- Using around $N(g)$ such i, we may find β, the key
- We need to solve a system of **linear equations** with $N(g)$ variables

An Example

- The generating polynomial of $\mathbb{F}_{2^5}$ is $x^5 + x^3 + 1$.
- Let $\alpha \in \mathbb{F}_{2^5}$ satisfy $\alpha^5 + \alpha^3 + 1 = 0$.
- $f(x) = Tr(\alpha^{27}x + \alpha^9 x^3 + \alpha^{14}x^7 + \alpha^7 x^{11}), g(x) = Tr(\alpha^{29}x^5)$
- $f(x) \cdot g(x) = 0$
- The **algebraic immunity** of $f(x)$ is 2.
- Suppose that the key stream **s** we got is just the first **10 bits** of $\{f(\alpha^i)\}$: 1110000101
- Because $s_i = 1$ for $i = 0, 1, 2, 7, 9$, we know $g(\beta\alpha^i) = 0$ for $i = 0, 1, 2, 7, 9$.

An Example (Cont.)

- In order to get the key β, we need to solve the **equations**

$$\begin{cases} Tr(G_5\beta^5) = 0, \\ Tr(G_5\beta^5\alpha^5) = 0, \\ Tr(G_5\beta^5\alpha^{10}) = 0, \\ Tr(G_5\beta^5\alpha^{35}) = Tr(G_5\beta^5\alpha^4) = 0, \\ Tr(G_5\beta^5\alpha^{45}) = Tr(G_5\beta^5\alpha^{14}) = 0. \end{cases}$$

- Let $G_5\beta^5 = x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3 + x_4\alpha^4$.

An Example (Cont.)

- Then we need to solve the equation

$$\begin{pmatrix} 1 & Tr(\alpha) & Tr(\alpha^2) & Tr(\alpha^3) & Tr(\alpha^4) \\ Tr(\alpha^4) & Tr(\alpha^5) & Tr(\alpha^6) & Tr(\alpha^7) & Tr(\alpha^8) \\ Tr(\alpha^5) & Tr(\alpha^6) & Tr(\alpha^7) & Tr(\alpha^8) & Tr(\alpha^9) \\ Tr(\alpha^{10}) & Tr(\alpha^{11}) & Tr(\alpha^{12}) & Tr(\alpha^{13}) & Tr(\alpha^{14}) \\ Tr(\alpha^{14}) & Tr(\alpha^{15}) & Tr(\alpha^{16}) & Tr(\alpha^{17}) & Tr(\alpha^{18}) \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

- $$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

An Example (Cont.)

- The solutions are

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \text{ or } \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

- Hence $\beta = 0$ or 1, and $\beta = 1$ is the **right answer**.

Comparison

- Algebraic attack: $\sum_{i=0}^{2} \binom{5}{i} = 16$ key stream bits, a system of linear equations with 16 variables
- Selective DFT attack: 10 key stream bits, a system of linear equations with 5 variables

Spectral Immunity

- The **spectral immunity** $SI(f)$ of f is the minimal $N(g)$ of g such that $fg = 0$ or $(f + 1)g = 0$.
- A **new design criterion** for Boolean functions employed in cryptography.

Algebraic Immunity and Spectral Immunity

- The generating polynomial of $\mathbb{F}_{2^5}$ is $x^5 + x^3 + 1$.
- Let $\alpha \in \mathbb{F}_{2^5}$ satisfy $\alpha^5 + \alpha^3 + 1 = 0$.
- $f(x) = Tr(x + \alpha^9 x^3 + \alpha^{11} x^7 + \alpha^{29} x^{11})$
- $AI(f) = 2$
- $f(x) \cdot Tr(\alpha^4 x^{11}) = 0$
- The **best case** from the viewpoint of the selective DFT attacker.

Upper Bound

- If f is balanced, then $SI(f) \leq 2^{n-1} + 1$.

Carlet and Feng, 2008

- $\mathbb{F}_{2^n}, n \geq 2$
- $f(0) = 1, f(\alpha^i) = 1$ for $i = 0, 1, 2, ..., 2^{n-1} - 2, f(\alpha^i) = 0$ for $i = 2^{n-1} - 1, 2^{n-1}, ..., 2^n - 2$
- $SI(f) \geq 2^{n-1}$

Thank You!