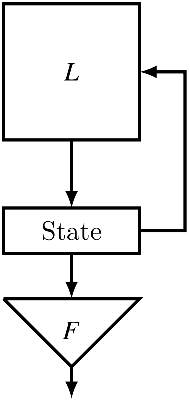
Algebraic Attacks Revisited

Yann Rotella

June 15, 2018
CCA 2018

Context



Classical criteria

Boolean functions:

Algebraic immunity: $\mathsf{AI}(F) = \min\{\deg(g); gf = 0 \text{ or } g(f+1) = 0\}$.

Non-linearity: minimal distance to all affine functions.

d-Resiliency: $f + g$ balanced for all g of $d < n$ variables.

Sequences:

Linear complexity: size of smallest recurring relation.

Table of contents

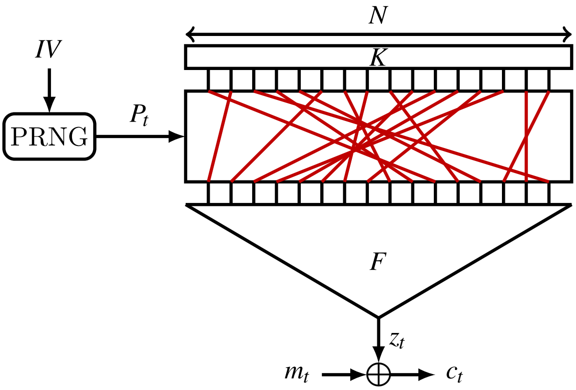
Outline

1. FLIP (Multivariate)
2. Goldreich's PRG (Multivariate)
3. Filtered LFSR (Univariate)
4. New criteria

FLIP

- Pierrick Méaux, Anthony Journault, François-Xavier Standaert and Claude Carlet,
  Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts,
  EUROCRYPT 2016.
- Sébastien Duval, Virginie Lallemand, Yann Rotella,
  Cryptanalysis of the FLIP family of stream ciphers,
  CRYPTO 2016

Specifications of FLIP



Very sparse equations

$$F(x) = x_1 + x_2 + x_3 + \cdots$$
$$+ x_i x_{i+1} + x_{i+2} x_{i+3} + \cdots$$
$$+ x_j + x_{j+1} x_{j+2} + x_{j+3} x_{j+4} x_{j+5} + x_{j+6} x_{j+7} x_{j+8} x_{j+9} + \cdots$$

- The constant key register
- The low number of monomials of degree ≥ 3 in F: $k-2$

Preliminary version of FLIP

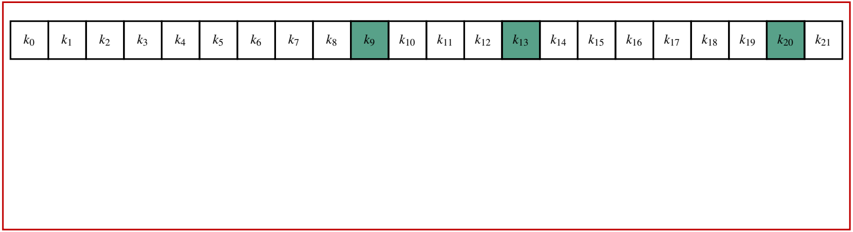
FLIP(n_1,n_2,n_3)	n_1	n_2	n_3	degree	**N**	Security
FLIP(47,40,105)	47	40	105	14	192	80
FLIP(87,82,231)	87	82	231	21	400	128

$$\begin{aligned} F(x_0,\cdots,x_{191}) = & x_0 + \ldots + x_{46} \\ & + x_{47}x_{48} + \ldots + x_{85}x_{86} \\ & + x_{87} + x_{88}x_{89} + \ldots + x_{178}x_{179}\cdots x_{191} \end{aligned}$$

Our attack: Guess and Determine

1. Guess ℓ random positions of zero bits
2. Keep an equation when there is at least one null bit in each monomial of degree at least 3
3. Solve the system of degree 2

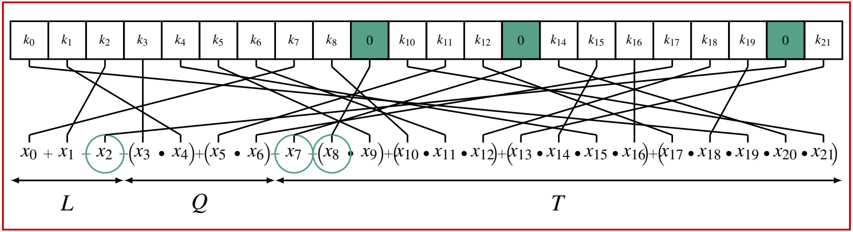
Our attack: Guess and Determine



Our attack: Guess and Determine

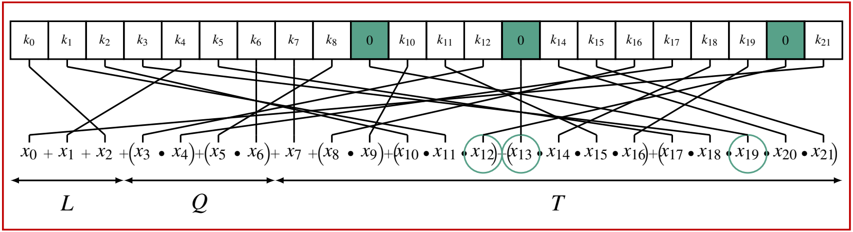
k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	0	k_{10}	k_{11}	k_{12}	0	k_{14}	k_{15}	k_{16}	k_{17}	k_{18}	k_{19}	0	k_{21}

Our attack: Guess and Determine



$$z_i = k_7 + k_2 + k_3 k_1 + k_{11} k_{17} + 0 + 0 + k_8 k_6 k_{18} + k_{21} k_{15} + k_{21} k_{15} k_4 k_{16} + k_{12} k_{19} k_0 k_{14} k_{10}$$

Our attack: Guess and Determine



$$z_{i+1} = k_{21} + k_4 + k_0 + k_{12}k_{17} + k_8k_6 + k_7 + k_{16}k_{10}$$

First step: guess

Key: N-bit vector of Hamming weight $\frac{N}{2}$.

Probability of having a right guess:

$$\mathbb{P}_{rg} = \frac{\binom{\frac{N}{2}}{\ell}}{\binom{N}{\ell}} \simeq 2^{-12.5}$$

Second step: get equations of degree ≤ 2

If $\ell = k - 2$

$$\mathbb{P}_{\ell=k-2} = \frac{k!/2}{\binom{N}{\ell}} \simeq 2^{-26}$$

General case :

$$\mathbb{P}_{\ell} = \frac{\sum_{i_1+i_2+\cdots+i_{k-2}\leq \ell} \binom{3}{i_1}\binom{4}{i_2}\cdots\binom{k}{i_{k-2}}\binom{N-m}{\ell-I}}{\binom{N}{\ell}}$$

$\rightarrow$ In average, we need $\mathbb{P}_{\ell}^{-1}$ bits of keystream to obtain 1 equation of degree 2

Last step: solving the system

$$v_\ell = N - \ell + \binom{N-\ell}{2}$$

1. Reach v_ℓ independent equations
2. Linearization
3. Gauss elimination

Complexity

Time:

$$C_T = \frac{1}{\mathbb{P}_{rg}} \times v_\ell^3$$

Data:

$$C_D = v_\ell \times \frac{1}{\mathbb{P}_\ell}$$

Memory:

$$C_M = v_\ell^2$$

Complexity

Time:

$$C_T = \frac{1}{\mathbb{P}_{rg}} \times v_\ell^3$$

Data:

$$C_D = v_\ell \times \frac{1}{\mathbb{P}_\ell}$$

Memory:

$$C_M = v_\ell^2$$

80-bit security claim:

$$C_T = 2^{54.5}, C_D = 2^{40.3}, C_M = 2^{28.0}$$

128-bit security claim:

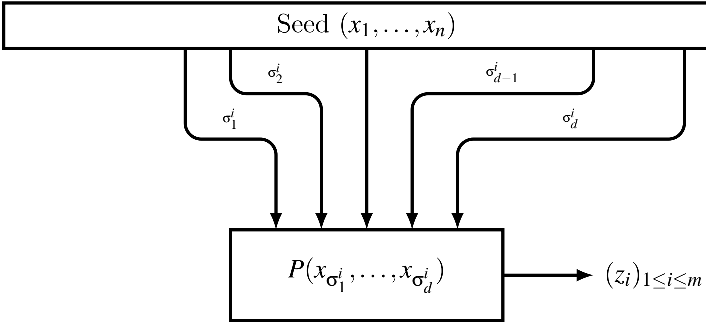
$$C_T = 2^{68.1}, C_D = 2^{58.5}, C_M = 2^{32.3}$$

Full version of FLIP

	N	λ
$\text{FLIP}(42, 128, \Delta_{8,9})$	530	80
$\text{FLIP}(82, 224, \Delta_{8,16})$	1394	128

Outline

Description



$m = n^s$, s is the stretch.

Bibliography

- Oded Goldreich,
  Candidate One-Way Functions Base on Expander Graphs,
  Cryptology ePrint Archive, Report 2000/063.
- Ryan O'Donnell et David Witmer,
  Goldreich's PRG: Evidence for Near-Optimal Polynomial Stretch,
  IEEE 29th Conference on Computational Complexity, CCC 2014, Vancouver, BC, Canada, June 11-13, 2014,
- Benny Applebaum et Shachar Lovett,
  Algebraic attacks against random local functions and their countermeasures,
  STOC 2016

- Our attack: joint work with Geoffroy Couteau, Aurélien Dupin, Pierrick Méaux et Mélissa Rossi

First technique: Guess and Determine

- FLIP: overdetermined
- Goldreich's PRG: underdetermined

$$P_5(x_1, x_2, x_3, x_4, x_5) = x_1 + x_2 + x_3 + x_4 x_5$$

For all possible values of the ℓ bits:

- Solve the correponding linear system of n linear equations.

Complexity: $\ell < n^{2-s} \rightarrow O\left(n^3 2^{n-s}\right)$
Conjectured secure up to $s < 1.5$

Second technique: derive new equations

$$x_{i_1} + x_{i_2} + x_{i_3} + x_{i_4}x_{i_5} = y_i \quad (1)$$

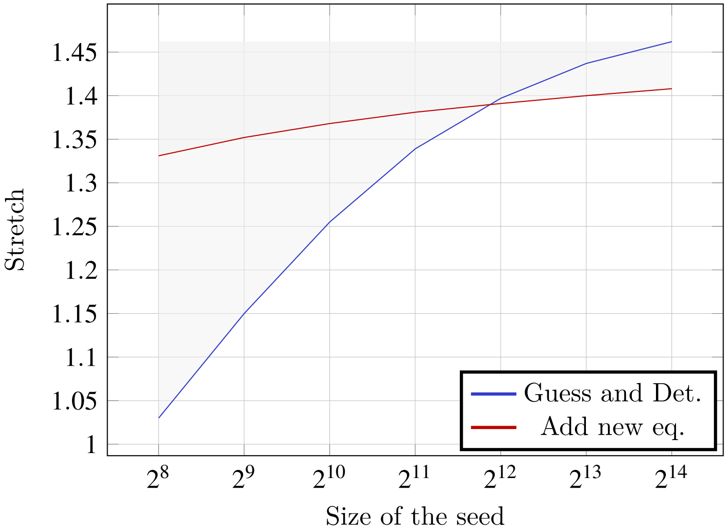
$$x_{j_1} + x_{j_2} + x_{j_3} + x_{j_4}x_{j_5} = y_j \quad (2)$$

using (1): $x_{i_4}x_{i_1} + x_{i_4}x_{i_2} + x_{i_4}x_{i_3} + x_{i_4}x_{i_5} = x_{i_4}y_i$

if $x_{i_4}x_{i_5} = x_{j_4}x_{j_5}$: $x_k y_i + x_k y_j = x_k x_{i_1} + x_k x_{i_2} + x_k x_{i_3} + x_k x_{j_1} + x_k x_{j_2} + x_k x_{j_3}$

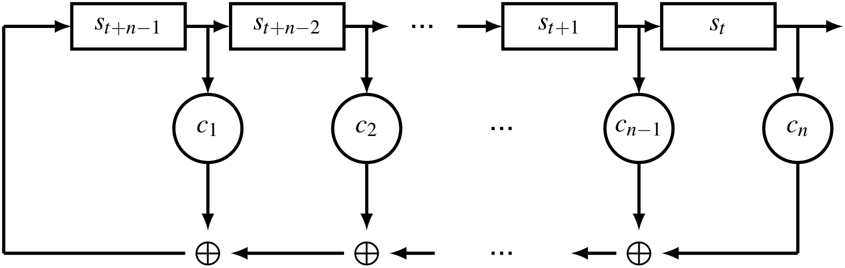
if $x_{i_4} = x_{j_4}$: $x_{j_5} \times (1) + x_{i_5} \times (2)$

Experimental results



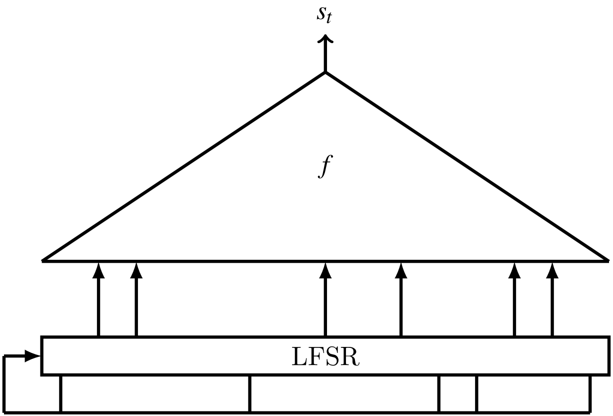
Outline

Linear Feedback Shift Register



$$P_R(X) = 1 + \sum_{i=1}^{n} c_i X^i$$

Filtered LFSR



Example on $\mathbb{F}_2^8$

$$
\begin{aligned}
&F(x_0,x_1,x_2,x_3,x_4,x_5,x_6,x_7) = \\
&x_0x_1x_2x_3x_4 + x_0x_1x_2x_3x_7 + x_0x_1x_2x_4x_6 + x_0x_1x_2x_4x_7 + x_0x_1x_2x_5x_7 + x_0x_1x_2x_6x_7 + x_0x_1x_2x_6 + \\
&x_0x_1x_2 + x_0x_1x_3x_4x_6 + x_0x_1x_3x_5x_7 + x_0x_1x_3x_5 + x_0x_1x_3x_6x_7 + x_0x_1x_4x_5x_6 + x_0x_1x_4x_6x_7 + \\
&x_0x_1x_4x_6 + x_0x_1x_5x_6x_7 + x_0x_1x_5x_6 + x_0x_1x_5x_7 + x_0x_1x_6x_7 + x_0x_1 + x_0x_2x_3x_4x_5 + x_0x_2x_3x_4x_6 + \\
&x_0x_2x_3x_5x_6 + x_0x_2x_3x_6x_7 + x_0x_2x_3x_6 + x_0x_2x_3x_7 + x_0x_2x_3 + x_0x_2x_4x_5x_7 + x_0x_2x_4x_6x_7 + x_0x_2x_4x_7 + \\
&x_0x_2x_4 + x_0x_2x_5x_6x_7 + x_0x_2x_5x_6 + x_0x_2x_5x_7 + x_0x_2 + x_0x_3x_4x_5x_7 + x_0x_3x_4x_5 + x_0x_3x_4x_6 + \\
&x_0x_3x_5x_6 + x_0x_3x_5x_7 + x_0x_3 + x_0x_4x_5x_6x_7 + x_0x_4x_5x_7 + x_0x_4x_6 + x_0x_4 + x_0x_5x_6x_7 + x_0x_5x_7 + \\
&x_0x_5 + x_0x_6 + x_1x_2x_3x_4x_6 + x_1x_2x_3x_4x_7 + x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_3x_6x_7 + x_1x_2x_4x_6x_7 + \\
&x_1x_2x_4x_6 + x_1x_2x_4x_7 + x_1x_2x_5x_6x_7 + x_1x_2x_6x_7 + x_1x_2x_6 + x_1x_2x_7 + x_1x_3x_4x_5 + x_1x_3x_4x_6x_7 + \\
&x_1x_3x_4x_6 + x_1x_3x_4x_7 + x_1x_3x_5x_6 + x_1x_3x_5 + x_1x_3 + x_1x_4x_5x_6x_7 + x_1x_4x_5x_7 + x_1x_4x_5 + x_1x_4x_6 + \\
&x_1x_4x_7 + x_1x_5x_6x_7 + x_1x_6x_7 + x_1x_7 + x_2x_3x_4 + x_2x_3x_5x_6 + x_2x_3x_5x_7 + x_2x_3x_5 + x_2x_3x_6x_7 + \\
&x_2x_3x_7 + x_2x_4x_5x_6 + x_2x_4x_5x_7 + x_2x_4x_5 + x_2x_5x_6x_7 + x_2x_5 + x_2x_6x_7 + x_2x_6 + x_2x_7 + x_3x_4x_5x_7 + \\
&x_3x_4x_6x_7 + x_3x_4 + x_3x_5x_6x_7 + x_3x_6x_7 + x_3x_6 + x_3 + x_4x_5x_6x_7 + x_4x_5x_7 + x_4x_5 + x_4x_6x_7 + x_6x_7 + x_6
\end{aligned}
$$

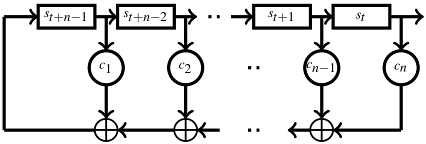
Example on $\mathbb{F}_2^8$

$$F(x_0,x_1,x_2,x_3,x_4,x_5,x_6,x_7) = x_0x_1x_2x_3x_4 + x_0x_1x_2x_3x_7 + x_0x_1x_2x_4x_6 + x_0x_1x_2x_4x_7 + x_0x_1x_2x_5x_7 + x_0x_1x_2x_6x_7 + x_0x_1x_2x_6 + x_0x_1x_2 + x_0x_1x_3x_4x_6 + x_0x_1x_3x_5x_7 + x_0x_1x_3x_5 + x_0x_1x_3x_6x_7 + x_0x_1x_4x_5x_6 + x_0x_1x_4x_6x_7 + x_0x_1x_4x_6 + x_0x_1x_5x_6x_7 + x_0x_1x_5x_6 + x_0x_1x_5x_7 + x_0x_1x_6x_7 + x_0x_1 + x_0x_2x_3x_4x_5 + x_0x_2x_3x_4x_6 + x_0x_2x_3x_5x_6 + x_0x_2x_3x_6x_7 + x_0x_2x_3x_6 + x_0x_2x_3x_7 + x_0x_2x_3 + x_0x_2x_4x_5x_7 + x_0x_2x_4x_6x_7 + x_0x_2x_4x_7 + x_0x_2x_4 + x_0x_2x_5x_6x_7 + x_0x_2x_5x_6 + x_0x_2x_5x_7 + x_0x_2 + x_0x_3x_4x_5x_7 + x_0x_3x_4x_5 + x_0x_3x_4x_6 + x_0x_3x_5x_6 + x_0x_3x_5x_7 + x_0x_3 + x_0x_4x_5x_6x_7 + x_0x_4x_5x_7 + x_0x_4x_6 + x_0x_4 + x_0x_5x_6x_7 + x_0x_5x_7 + x_0x_5 + x_0x_6 + x_1x_2x_3x_4x_6 + x_1x_2x_3x_4x_7 + x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_3x_6x_7 + x_1x_2x_4x_6x_7 + x_1x_2x_4x_6 + x_1x_2x_4x_7 + x_1x_2x_5x_6x_7 + x_1x_2x_6x_7 + x_1x_2x_6 + x_1x_2x_7 + x_1x_3x_4x_5 + x_1x_3x_4x_6x_7 + x_1x_3x_4x_6 + x_1x_3x_4x_7 + x_1x_3x_5x_6 + x_1x_3x_5 + x_1x_3 + x_1x_4x_5x_6x_7 + x_1x_4x_5x_7 + x_1x_4x_5 + x_1x_4x_6 + x_1x_4x_7 + x_1x_5x_6x_7 + x_1x_6x_7 + x_1x_7 + x_2x_3x_4 + x_2x_3x_5x_6 + x_2x_3x_5x_7 + x_2x_3x_5 + x_2x_3x_6x_7 + x_2x_3x_7 + x_2x_4x_5x_6 + x_2x_4x_5x_7 + x_2x_4x_5 + x_2x_5x_6x_7 + x_2x_5 + x_2x_6x_7 + x_2x_6 + x_2x_7 + x_3x_4x_5x_7 + x_3x_4x_6x_7 + x_3x_4 + x_3x_5x_6x_7 + x_3x_6x_7 + x_3x_6 + x_3 + x_4x_5x_6x_7 + x_4x_5x_7 + x_4x_5 + x_4x_6x_7 + x_6x_7 + x_6$$

- $\mathsf{AI}(F) = 4$
- $\mathsf{NL}(F) = 112$ (bound 120 for $n = 8$)

LFSR over a Finite Field

- α : root of the primitive characteristic polynomial in $\mathbb{F}_{2^n}$
- Identify the n-bit words with elements of $\mathbb{F}_{2^n}$ with the dual basis of $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$

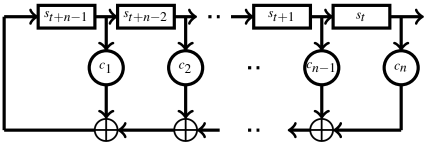


Proposition

The state of the LFSR at time $(t+1)$ is the state of the LFSR at time t multiplied by α.

LFSR over a Finite Field

- α : root of the primitive characteristic polynomial in $\mathbb{F}_{2^n}$
- Identify the n-bit words with elements of $\mathbb{F}_{2^n}$ with the dual basis of $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$



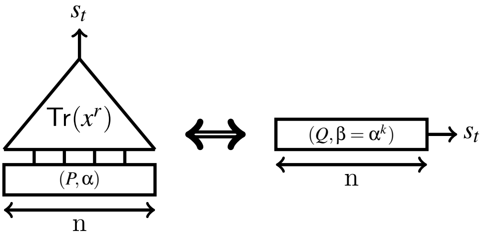
Proposition

The state of the LFSR at time $(t+1)$ is the state of the LFSR at time t multiplied by α.

For all t, $X_t = X_0 \alpha^t$

Monomial equivalence [RonCid10,CanRot16]

$F(x) = \mathsf{Tr}(x^r)$, with $\gcd(r, 2^n - 1) = 1$:
Let k be such that $rk \equiv 1 \mod (2^n - 1)$.



Example on $\mathbb{F}_2^8$

$F(x_0,x_1,x_2,x_3,x_4,x_5,x_6,x_7) =$
$x_0x_1x_2x_3x_4 + x_0x_1x_2x_3x_7 + x_0x_1x_2x_4x_6 + x_0x_1x_2x_4x_7 + x_0x_1x_2x_5x_7 + x_0x_1x_2x_6x_7 + x_0x_1x_2x_6 +$
$x_0x_1x_2 + x_0x_1x_3x_4x_6 + x_0x_1x_3x_5x_7 + x_0x_1x_3x_5 + x_0x_1x_3x_6x_7 + x_0x_1x_4x_5x_6 + x_0x_1x_4x_6x_7 +$
$x_0x_1x_4x_6 + x_0x_1x_5x_6x_7 + x_0x_1x_5x_6 + x_0x_1x_5x_7 + x_0x_1x_6x_7 + x_0x_1 + x_0x_2x_3x_4x_5 + x_0x_2x_3x_4x_6 +$
$x_0x_2x_3x_5x_6 + x_0x_2x_3x_6x_7 + x_0x_2x_3x_6 + x_0x_2x_3x_7 + x_0x_2x_3 + x_0x_2x_4x_5x_7 + x_0x_2x_4x_6x_7 + x_0x_2x_4x_7 +$
$x_0x_2x_4 + x_0x_2x_5x_6x_7 + x_0x_2x_5x_6 + x_0x_2x_5x_7 + x_0x_2 + x_0x_3x_4x_5x_7 + x_0x_3x_4x_5 + x_0x_3x_4x_6 +$
$x_0x_3x_5x_6 + x_0x_3x_5x_7 + x_0x_3 + x_0x_4x_5x_6x_7 + x_0x_4x_5x_7 + x_0x_4x_6 + x_0x_4 + x_0x_5x_6x_7 + x_0x_5x_7 +$
$x_0x_5 + x_0x_6 + x_1x_2x_3x_4x_6 + x_1x_2x_3x_4x_7 + x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_3x_6x_7 + x_1x_2x_4x_6x_7 +$
$x_1x_2x_4x_6 + x_1x_2x_4x_7 + x_1x_2x_5x_6x_7 + x_1x_2x_6x_7 + x_1x_2x_6 + x_1x_2x_7 + x_1x_3x_4x_5 + x_1x_3x_4x_6x_7 +$
$x_1x_3x_4x_6 + x_1x_3x_4x_7 + x_1x_3x_5x_6 + x_1x_3x_5 + x_1x_3 + x_1x_4x_5x_6x_7 + x_1x_4x_5x_7 + x_1x_4x_5 + x_1x_4x_6 +$
$x_1x_4x_7 + x_1x_5x_6x_7 + x_1x_6x_7 + x_1x_7 + x_2x_3x_4 + x_2x_3x_5x_6 + x_2x_3x_5x_7 + x_2x_3x_5 + x_2x_3x_6x_7 +$
$x_2x_3x_7 + x_2x_4x_5x_6 + x_2x_4x_5x_7 + x_2x_4x_5 + x_2x_5x_6x_7 + x_2x_5 + x_2x_6x_7 + x_2x_6 + x_2x_7 + x_3x_4x_5x_7 +$
$x_3x_4x_6x_7 + x_3x_4 + x_3x_5x_6x_7 + x_3x_6x_7 + x_3x_6 + x_3 + x_4x_5x_6x_7 + x_4x_5x_7 + x_4x_5 + x_4x_6x_7 + x_6x_7 + x_6$

- $\mathsf{AI}(F) = 4$
- $\mathsf{NL}(F) = 112$ (bound 120 for $n = 8$)
- $F(X) = \mathsf{Tr}(X^{143}) + \mathsf{Tr}(X)$

Trace representation

$$f(x) = \sum_{u \in \mathbb{F}_2^n} a_u x^u$$

Cyclotomic class of k:

$$C(k) = \{k, 2k, 4k, 8k, \ldots\},\ n_k = \mathrm{Card}(C(k))$$

$$F(X) = \sum_{k \in \Gamma} \mathsf{Tr}(\lambda_k X^k)$$

where Γ is the set of all representatives of the cyclotomic classes and $\lambda_k \in \mathbb{F}_2^{n_k}$.

Trace representation

$$f(x) = \sum_{u \in \mathbb{F}_2^n} a_u x^u$$

Cyclotomic class of k:

$$C(k) = \{k, 2k, 4k, 8k, \ldots\},\ n_k = \mathrm{Card}(C(k))$$

$$F(X) = \sum_{k \in \Gamma} \mathsf{Tr}(\lambda_k X^k)$$

where Γ is the set of all representatives of the cyclotomic classes and $\lambda_k \in \mathbb{F}_2^{n_k}$.

$$\Lambda = \sum_{k \in \Gamma, \lambda_k \neq 0} n_k$$

where Λ is the linear complexity of the output sequence [Blahut83,Massey94].

Algebraic attack [Blahut83]

$$F(X) = G(X) + \mathsf{Tr}(\lambda_k X^k)$$

$$\begin{aligned}
s_0 &= F(X_0) = G(X_0) + \mathsf{Tr}(\lambda_k X_0^k) \\
s_1 &= F(\alpha X_0) = G(\alpha X_0) + \mathsf{Tr}(\lambda_k \alpha^k X_0^k) \\
&\dots \\
s_n &= F(\alpha^n X_0) = G(\alpha^n X_0) + \mathsf{Tr}(\lambda_k \alpha^{kn} X_0^k)
\end{aligned}$$

Algebraic attack [Blahut83]

$$F(X) = G(X) + \mathsf{Tr}(\lambda_k X^k)$$

$$\begin{aligned} s_0 &= F(X_0) = G(X_0) + \mathsf{Tr}(\lambda_k X_0^k) \\ s_1 &= F(\alpha X_0) = G(\alpha X_0) + \mathsf{Tr}(\lambda_k \alpha^k X_0^k) \\ &\dots \\ s_n &= F(\alpha^n X_0) = G(\alpha^n X_0) + \mathsf{Tr}(\lambda_k \alpha^{kn} X_0^k) \end{aligned}$$

P_{α^k}: minimal polynomial of α^k:

$$\sum_{i=0}^{n} c_i G(\alpha^i X_0) = \sum_{i=0}^{n} c_i s_i$$

Example on $\mathbb{F}_2^8$

$$F(X) = \mathsf{Tr}(X^{143}) + \mathsf{Tr}(X)$$

- $\mathsf{AI}(F) = 4$
- $\mathsf{NL}(F) = 112$ (bound 120 for $n = 8$)...

$$\Lambda = 16$$

Example on $\mathbb{F}_2^8$

$$F(X) = \mathsf{Tr}(X^{143}) + \mathsf{Tr}(X)$$

- $\mathsf{AI}(F) = 4$
- $\mathsf{NL}(F) = 112$ (bound 120 for $n = 8$)...

$$\Lambda = 16$$

Rainer A. Rueppel,
Analysis and Design of Stream Ciphers,
Book, Springer Verlag, 1986.

$\rightarrow$ For most of the functions of degree d, $\Lambda = \binom{n}{d}$

Outline

Multivariate representation

- Number of monomials in the ANF?
- Algebraic Immunity restricted to a vector space:

  Claude Carlet, Pierrick Méaux and Yann Rotella,
  Boolean functions with restricted inputs, application to the FLIP cipher,
  IACR Transactions on Symmetric Cryptology 2017.

- Dimension on the vector space of annihilators.

Univariate representation

Guang Gong, Sondre Rønjom, Tor Helleseth and Honggang Hu,
Fast Dicrete Fourier Spectra Attacks on Stream Ciphers,
IEEE Transactions on Information Theory 2011.

Spectral Immuniy:
$\mathbf{s} = (s_t)_{t \leq 0}$ of period $T | (2^n - 1)$, then

$$\mathsf{SI}(\mathbf{s}) = \min_{\mathbf{b}} \{\Lambda(b) | \mathbf{b} \cdot \mathbf{s} = \mathbf{0} \text{ or } \mathbf{b} \cdot (\mathbf{s} + \mathbf{1}) = \mathbf{0}\}$$

Boolean functions $\Leftrightarrow$ Periodic sequences:

Sparse annihilators of a given function, with few monomials in the univariate representation

Univariate representation

Tor Helleseth and Sondre Rønjom,
Simplifying Algebraic Attacks with Univariate Analysis,
IEEE Transactions on Information Theory 2011.

$$\mathsf{SI}(F) \leq \sum_{i=1}^{\mathsf{AI}(F)} \binom{n}{i}$$

Sondre Rønjom,
Powers of Subfield Polynomials and Algebraic Attacks on Word-Based Stream Ciphers,
eprint 495, 2015.

→ Cryptanalysis of Welsh-Gong family of stream ciphers.

Univariate representation

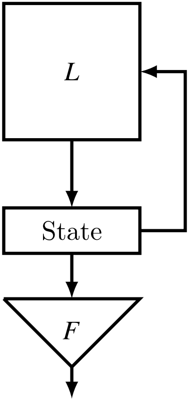
Jingjing Wang, Kefei Chen and Shixiong Zhu,
Annihilators of Fast Dicrete Fourier Spectra Attacks,
IWSEC 2012.

Di Wu, Wenfeng Qi and Huajin Chen,
On the spectral immunity of periodic sequences restricted to binary annihilators,
DCC 2016.

- $\mathsf{SI}(F) \leq 2^{n-1}$ if n is odd, tight;
- $\mathsf{SI}(F) \leq 2^{n-1} + \frac{n}{2}$ if n is even, not always tight;
- $\mathsf{AI}(F) \leq \lceil n/2 \rceil$.

Problem

Bad interaction between f and L.



Conclusion

Multivariate	Univariate
AI	SI
Resiliency	
NL	

Conclusion

Multivariate	Univariate
Generalized AI [MJSC16]	SI
Resiliency	
NL	

Conclusion

Multivariate	Univariate
Generalized AI [MJSC16]	Generalized SI ?
Resiliency	
NL	

Conclusion

Multivariate	Univariate
Generalized AI [MJSC16]	Generalized SI ?
Resiliency	$F(X) \simeq H(X^k)$, $\gcd(k, 2^n - 1) > 1$
NL	GNL [GongYousssef01]

Anne Canteaut and Yann Rotella,
Attacks against Filter Generator Exploiting Monomial Mappings,
FSE 2016.

Thank You
Questions & Comments