Boolean Functions for stream ciphers

Anne Canteaut

INRIA-Rocquencourt
projet CODES
Anne.Canteaut@inria.fr
http://www-rocq.inria.fr/codes/Anne.Canteaut/

ECRYPT summer school - May 2007

Outline

- Basic properties of Boolean functions for LFSR-based generators
- Other representations of Boolean functions
- Correlation attacks and related criteria
- Distance to affine functions and Walsh transform
- Algebraic attacks and related criteria
- Some practical constructions

Basic properties of Boolean functions for LFSR-based generators

Definition. A Boolean function of n variables is a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2$.

Truth table of a Boolean function.

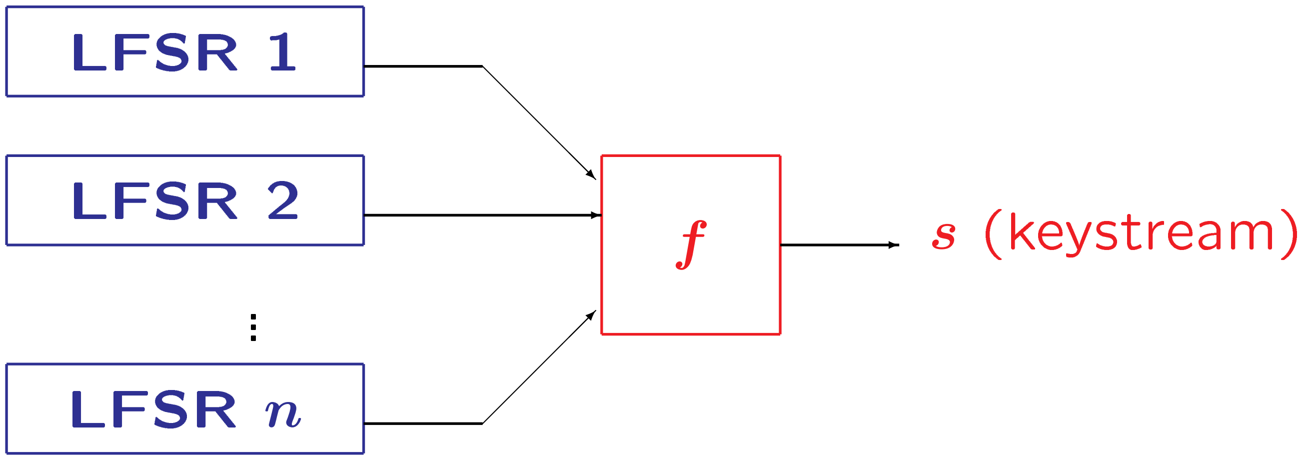
x_1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1
x_3	0	0	0	0	1	1	1	1
$f(x_1, x_2, x_3)$	0	1	0	0	0	1	1	1

Hamming weight of a Boolean function.

The Hamming weight of a Boolean function f, $wt(f)$, is the Hamming weight of its value vector.

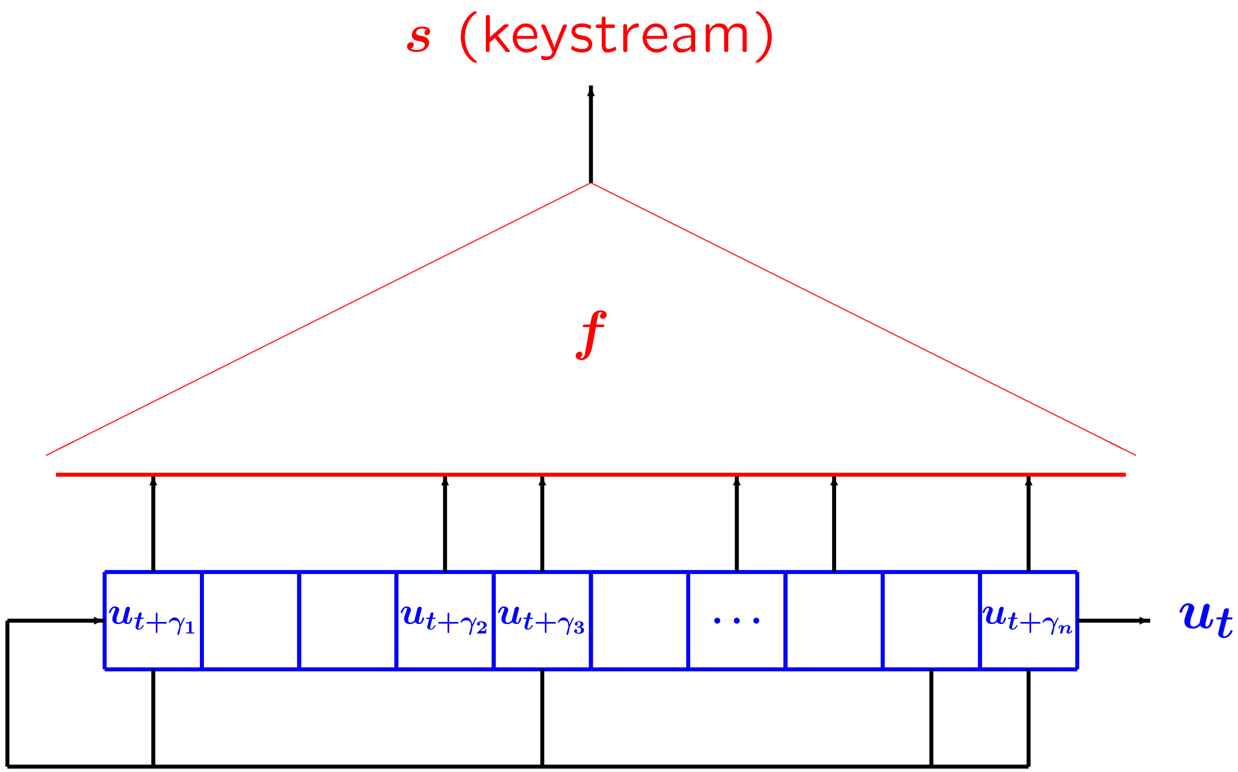
A function of n variables is balanced if and only if $wt(f) = 2^{n-1}$.

Combination generator



where f is a balanced Boolean function of n variables.

Filter generator



$$\forall t \geq 0, \quad s_t = f(u_{t+\gamma_1}, u_{t+\gamma_2}, \ldots, u_{t+\gamma_n})$$

Algebraic normal form (ANF)

Monomials in $\mathbf{F}_2[x_1, \ldots, x_n]/(x_1^2 + x_1, \ldots, x_n^2 + x_n)$:

$$\{x^u, \ \ u \in \mathbf{F}_2^n\} \text{ where } x^u = \prod_{i=1}^{n} x_i^{u_i}.$$

Example: $x^{1011} = x_1 x_3 x_4$.

Proposition.
Any Boolean function of n variables has a unique polynomial representation in $\mathbf{F}_2[x_1, \ldots, x_n]/(x_1^2 + x_1, \ldots, x_n^2 + x_n)$:

$$f(x_1, \ldots, x_n) = \sum_{u \in \mathbf{F}_2^n} a_u x^u, \ \ a_u \in \mathbf{F}_2.$$

Moreover, the coefficients of the ANF and the values of f satisfy:

$$a_u = \bigoplus_{x \preceq u} f(x) \text{ and } f(u) = \bigoplus_{x \preceq u} a_x,$$

where $x \preceq y$ if and only if $x_i \leq y_i$ for all $1 \leq i \leq n$.

Computing the ANF

x_1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1
x_3	0	0	0	0	1	1	1	1
$f(x_1, x_2, x_3)$	0	1	0	0	0	1	1	1

$$a_{000} = f(000) = 0$$
$$a_{100} = f(100) \oplus f(000) = 1$$
$$a_{010} = f(010) \oplus f(000) = 0$$
$$a_{110} = f(110) \oplus f(010) \oplus f(100) \oplus f(000) = 1$$
$$a_{001} = f(001) \oplus f(000) = 0$$
$$a_{101} = f(101) \oplus f(001) \oplus f(100) \oplus f(000) = 0$$
$$a_{011} = f(011) \oplus f(001) \oplus f(010) \oplus f(000) = 1$$
$$a_{111} = \bigoplus_{x \in \mathbb{F}_2^3} f(x) = wt(f) \bmod 2 = 0$$

$$f = x_1 + x_1 x_2 + x_2 x_3.$$

Degree and linear complexity

Definition.
The degree of a Boolean function is the degree of the largest monomial in its ANF.

Proposition. The weight of an n-variable function f is odd if and only if $\deg f = n$.

Degree and linear complexity of the combination generator.

Proposition. [Rueppel - Staffelbach 87]
For n LFSRs with primitive feedback polynomials and distinct lengths, the linear complexity of the keystream sequence generated by the combination of these LFSR by f is

$$\Lambda = f(L_1, \ldots, L_n)$$

where f is evaluated over integers.

Example: Geffe generator (1973)

$$f(x_1, x_2, x_3) = x_1 + x_1x_2 + x_2x_3. \Longrightarrow \Lambda = L_1 + L_1L_2 + L_2L_3.$$

Degree and linear complexity (2)

Degree and linear complexity of the filter generator.

Proposition. [Key76, Rueppel 86]
The linear complexity Λ of the keystream sequence generated by an LFSR of length L filtered by f satisfies

$$\Lambda \leq \sum_{i=0}^{\deg f} \binom{L}{i}.$$

Moreover, if L is a large prime,

$$\Lambda \geq \binom{L}{\deg f}$$

for most filtering functions.

Degree and basic algebraic attacks

Communication Theory of Secrecy Systems (1949), page 711.

"Using functional notation we have for enciphering $\boldsymbol{E = f(K, M)}$.

Given (or assuming) $\boldsymbol{M = m_1, m_2, \ldots, m_s}$ and $\boldsymbol{E = e_1, e_2, \ldots, e_s}$, the cryptanalyst can set up equations for the different key elements $\boldsymbol{k_1, k_2, \ldots, k_r}$ (namely the enciphering equations).

$$\begin{aligned} e_1 &= f_1(m_1, m_2, \ldots, m_s; k_1, \ldots, k_r) \\ e_2 &= f_2(m_1, m_2, \ldots, m_s; k_1, \ldots, k_r) \\ &\vdots \\ e_s &= f_s(m_1, m_2, \ldots, m_s; k_1, \ldots, k_r) \end{aligned}$$

All is known, we assume, except the $\boldsymbol{k_i}$. Each of these equations should therefore be complex in the $\boldsymbol{k_i}$, and involve many of them. Otherwise the enemy can solve the simple ones and then the more complex ones by substitution."

Shannon's attack on LFSR-based stream ciphers

Set up the enciphering equations:

$$\begin{cases} s_0 & = & f(x_0, \ldots, x_{L-1}) \\ s_1 & = & f \circ \mathcal{L}(x_0, \ldots, x_{L-1}) \\ & & \\ s_t & = & f \circ \mathcal{L}^t(x_0, \ldots, x_{L-1}) \end{cases}$$

System of equations with L variables of degree $d = \deg(f)$.

$\Longrightarrow$ Solve the system by linearization

$$\sum_{i=1}^{d} \binom{n}{i} \simeq \frac{L^d}{d!} \text{ keystream bits}$$

Time complexity: L^{3d} operations .

Other representations of Boolean functions

Reed-Muller codes

Definition. [Reed 54], [Muller54]

The Reed-Muller code of length 2^n and order r, $RM(r,n)$, is the linear code formed by the value vectors of all Boolean functions of n variables and degree at most r.

Proposition. $RM(r,n)$ has minimum distance 2^{n-r}.

Complexity of a Boolean function [Wegener 87]

$C_\Omega(f)$ = smallest number of gates of a circuit computing f, whose gates belong to Ω.

Usually, $\Omega = \mathcal{B}_2$, set of Boolean functions of 2 variables.

For Programmable Logic-Arrays, $\Omega = (\wedge, \vee, \neg)$.

Example.

- $x_1x_2 + x_1x_3 + x_1x_4 + x_1x_5 + x_2x_3 + x_2x_4 + x_2x_5 + x_3x_4 + x_3x_5$ $+x_4x_5$ — 19 gates.

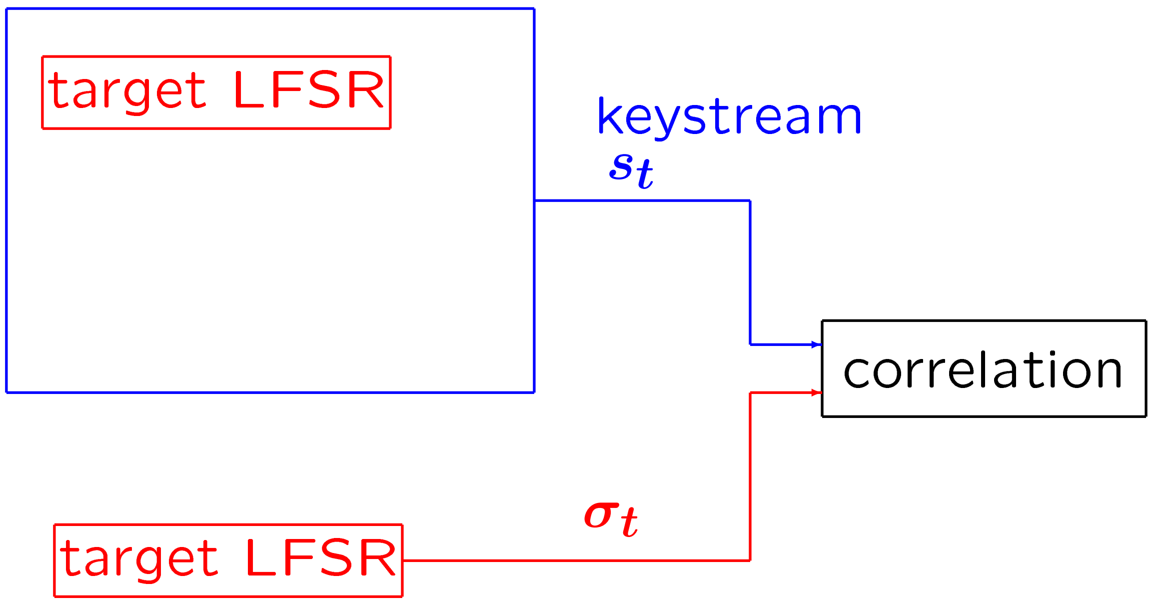
- $[(z + x_4)(z + x_5) + z] + [y(x_1 + x_3) + x_1]$ with $z = y + x_3$ and $y = x_1 + x_2$ — 10 gates

The Shannon effect [Shannon 49], [Lupanov 70]

For all $n \geq 9$, "almost all" Boolean functions of n variables have complexity $C_{\mathcal{B}_2}$ greater than $2^n/n$.

Correlation attacks and related criteria

Correlation attack [Siegenthaler 85]

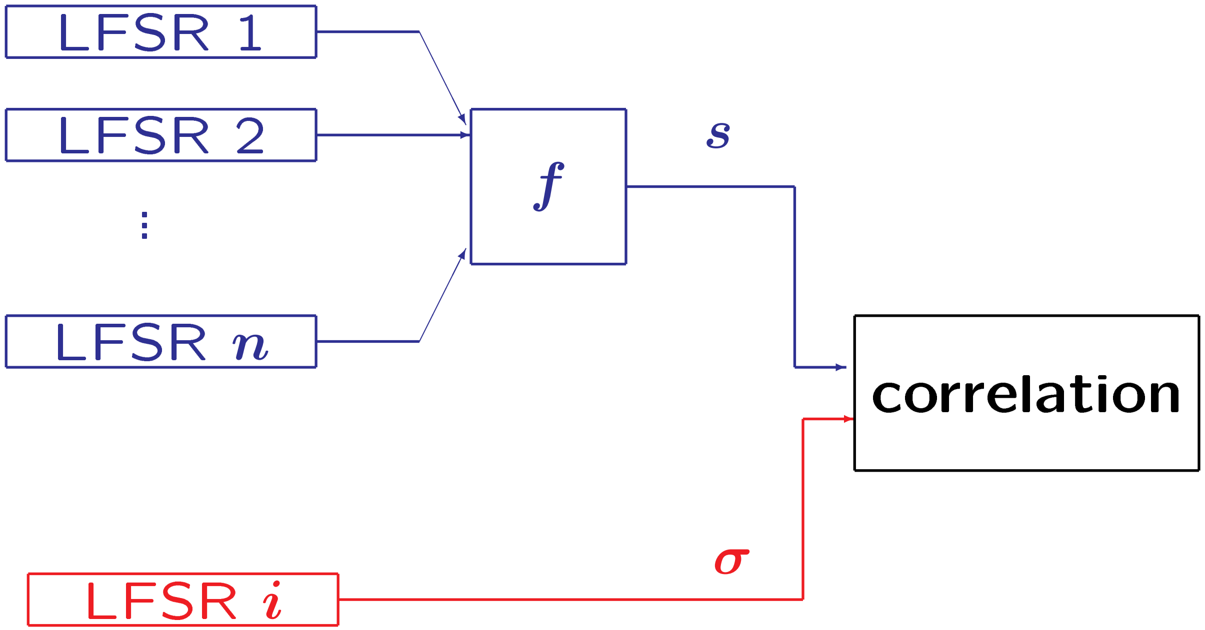


$$\text{where } p = \Pr[s_t \neq \sigma_t] \neq \frac{1}{2} \,.$$

Problem:

Recover the initial state of the target register from the knowledge of some keystream bits.

Correlation attack on a combination generator



with $\Pr[f(x_1, \ldots, x_n) \neq x_i] = P[s_t \neq \sigma_t] \neq \frac{1}{2}$.

Correlation-immune functions

$$\Pr[f(X_1,\ldots,X_n)=1|X_i=1]=\Pr[f(X_1,\ldots,X_n)=1|X_i=0]\ .$$

In terms of Hamming distance

	$x \in \mathbf{F}_2^n, x_i=0$	$x \in \mathbf{F}_2^n, x_i=1$
f	f_1	f_2
$x \mapsto x_i$	0 0 . . . 0 0	1 1 . . . 1 1
$f+x_i$	f_1	f_2+1

f correlation-immune: $wt(f_1)=wt(f_2)$.

$$\Longleftrightarrow d(f,x_i)=wt(f_1)+wt(f_2+1)=wt(f_1)+(2^{n-1}-wt(f_2))=2^{n-1}\ .$$

Correlation-immunity of order t [Siegenthaler 84]

Definition. A Boolean function f of n variables is t-th order correlation-immune if, for any subset $T \subset \{1, \dots, n\}$, $|T| = t$, for any $a \in \mathbf{F}_2^t$,

$$\Pr[f(X_1, \dots, X_n) = 1 | \forall i \in T, X_i = a_i] = \Pr[f(X_1, \dots, X_n) = 1] .$$

Proposition. [Xiao-Massey88]
f is t-th order correlation-immune if and only if
for all $\alpha \in \mathbf{F}_2^n$ with $1 \leq wt(\alpha) \leq t$, $d(f, \alpha \cdot x) = 2^{n-1}$.

Definition. A t-resilient function is a balanced t-th order correlation-immune function.

$\Longrightarrow$ The correlation-immunity order of a combining function must be high.

Degree of a correlation-immune function

Theorem. [Siegenthaler 84]
Let f be a Boolean function of n variables. Then, its correlation-immunity order t satisfies

$$\deg(f) + t \leq n$$

Moreover, if f is balanced,

$$\deg(f) + t \leq n - 1$$

Distance to affine functions and Walsh transform

Walsh transform of a Boolean function

Imbalance of a Boolean function.

For any Boolean function f of n variables

$$\mathcal{F}(f) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)} = 2^n - 2wt(f).$$

Linear functions of n variables.

$$\varphi_a : x \longmapsto a \cdot x$$

Walsh transform of a function f of n variables

$$\begin{array}{ccl} \mathbf{F}_2^n & \longrightarrow & \mathbf{C} \\ a & \longmapsto & \mathcal{F}(f + \varphi_a) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x) + a \cdot x} \end{array}$$

Computing the Walsh transform

f	0	1	0	0	0	1	1	1
$(f_1 + f_2, f_1 - f_2)$	0	2	1	1	0	0	-1	-1
$(f_3 + f_4, f_3 - f_4, f_5 + f_6, f_5 - f_6)$	1	3	-1	1	-1	-1	1	1
Fourier transform $\hat{f}$	4	-2	0	-2	-2	0	2	0
Walsh transform $= 2^n \delta_0 - 2\hat{f}$	0	4	0	4	4	0	-4	0

Some basic properties of the Walsh transform

Lemma:

$$\sum_{x \in \mathbf{F}_2^n} (-1)^{a \cdot x} = \begin{cases} 2^n & \text{if } a = 0 \\ 0 & \text{otherwise} \end{cases}.$$

Proposition. The Walsh transform is an involution (up to a multiplicative constant).

$$\begin{aligned} \sum_{a \in \mathbf{F}_2^n} \mathcal{F}(f + \varphi_a)(-1)^{a \cdot x} &= \sum_{u \in \mathbf{F}_2^n} \sum_{a \in \mathbf{F}_2^n} (-1)^{f(u) + a \cdot u + a \cdot x} \\ &= \sum_{u \in \mathbf{F}_2^n} (-1)^{f(u)} \sum_{a \in \mathbf{F}_2^n} (-1)^{a \cdot (x+u)} \\ &= 2^n (-1)^{f(x)} \end{aligned}$$

Parseval equality.

$$\sum_{a \in \mathbf{F}_2^n} \mathcal{F}^2(f + \varphi_a) = 2^{2n}.$$

Divisibility of the Walsh coefficients

Proposition.

For any $\boldsymbol{a} \in \mathbf{F}_2^n$,

$$\mathcal{F}(f + \varphi_a) \equiv \mathcal{F}(f) \bmod 2^{\lceil \frac{n}{\deg f} \rceil + 1}.$$

In particular,

$$\begin{aligned} \mathcal{F}(f + \varphi_a) &\equiv 2 \bmod 4 \text{ if } \deg f = n \\ &\equiv 0 \bmod 4 \text{ if } \deg f < n. \end{aligned}$$

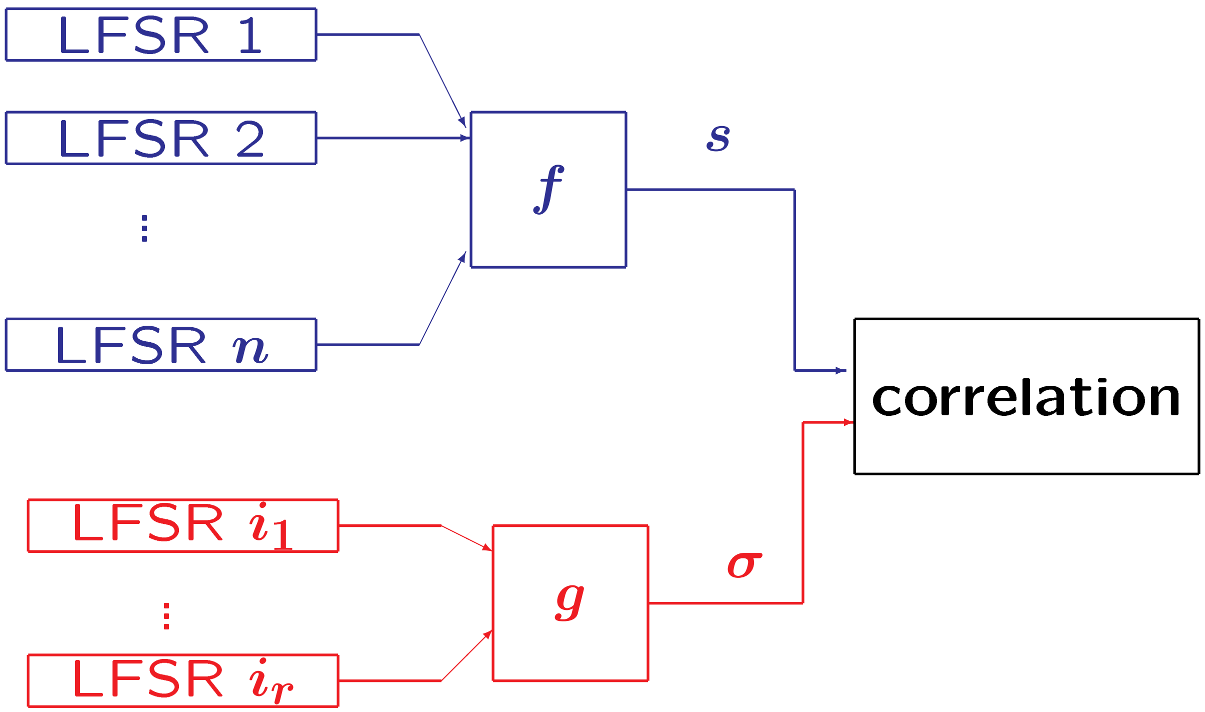
Nonlinearity of a Boolean function

Nonlinearity of $f : \mathbf{F}_2^n \longrightarrow \mathbf{F}_2$:

Hamming distance of f to $RM(1,n) = \{\varphi_a + \varepsilon,\ a \in \mathbf{F}_2^n,\ \varepsilon \in \mathbf{F}_2\}$.

$$2^{n-1} - \frac{1}{2}\mathcal{L}(f) \qquad \text{where } \mathcal{L}(f) = \max_a |\mathcal{F}(f + \varphi_a)| \ .$$

Generalization of Siegenthaler's attack



where g is an r-variable function such that

$$p_g = \Pr[f(x_1, \ldots, x_r, x_{r+1}, \ldots, x_n) = g(x_1, \ldots, x_r)] > \frac{1}{2}.$$

Approximation of f by a function of fewer variables
[Zhang-Chan 00][C.-Trabbia 00][C. 02]

Proposition.

$$\max_{g \in \mathcal{B}oo\ell_r} \left| p_g - \frac{1}{2} \right| \leq \frac{1}{2^{n+1}} \left(\sum_{\lambda \in \mathbf{F}_2^r} \mathcal{F}^2(f + \varphi_{\lambda,0}) \right)^{1/2}$$

In particular:

- For f balanced,

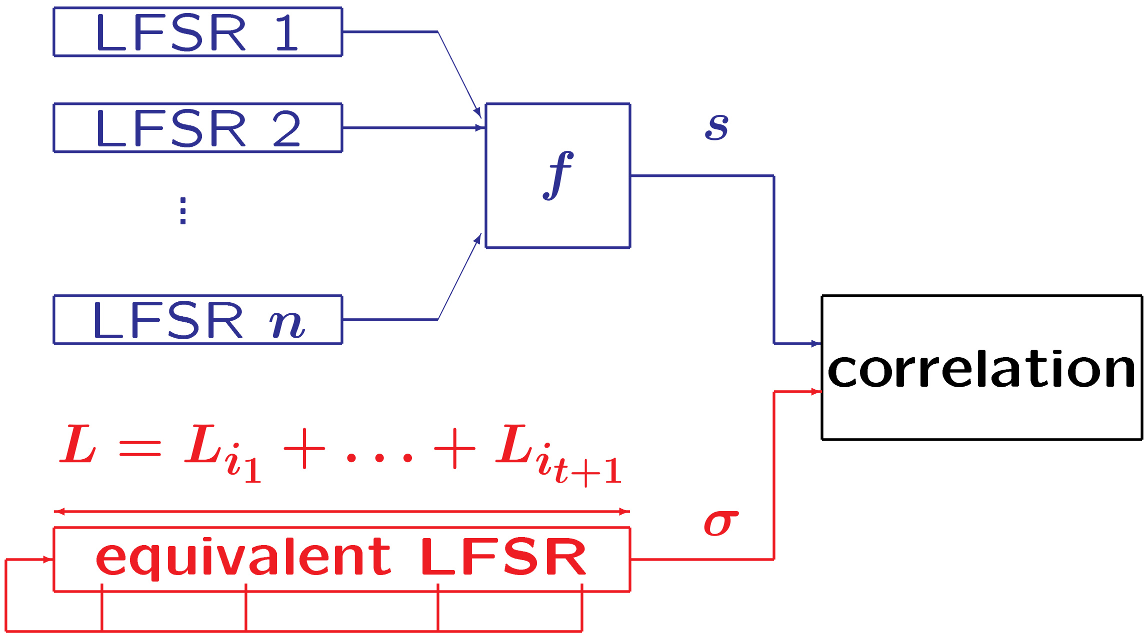
$$p_g = \frac{1}{2} \text{ for any } g \text{ depending on } t \text{ variables}$$

if and only if f is t-resilient.

- The best approximation of a t-resilient function f by a function of $(t+1)$ variables is affine: $g = x_{i_1} + \ldots + x_{i_{t+1}} + \varepsilon$.

- $\max_g \left| p_g - \frac{1}{2} \right| \leq 2^{\frac{r}{2}-n-1} \mathcal{L}(f)$.

Generalization of Siegenthaler's attack



$$\Pr[s_t \neq \sigma_t] - \frac{1}{2} = \Pr[f(x_1, \ldots, x_n) \neq x_1 + \ldots + x_{t+1})] - \frac{1}{2}$$
$$= \frac{1}{2^{n+1}} \mathcal{F}(f + \varphi_v)$$

where v is the vector which equals 1 on its first $(t+1)$ coordinates.

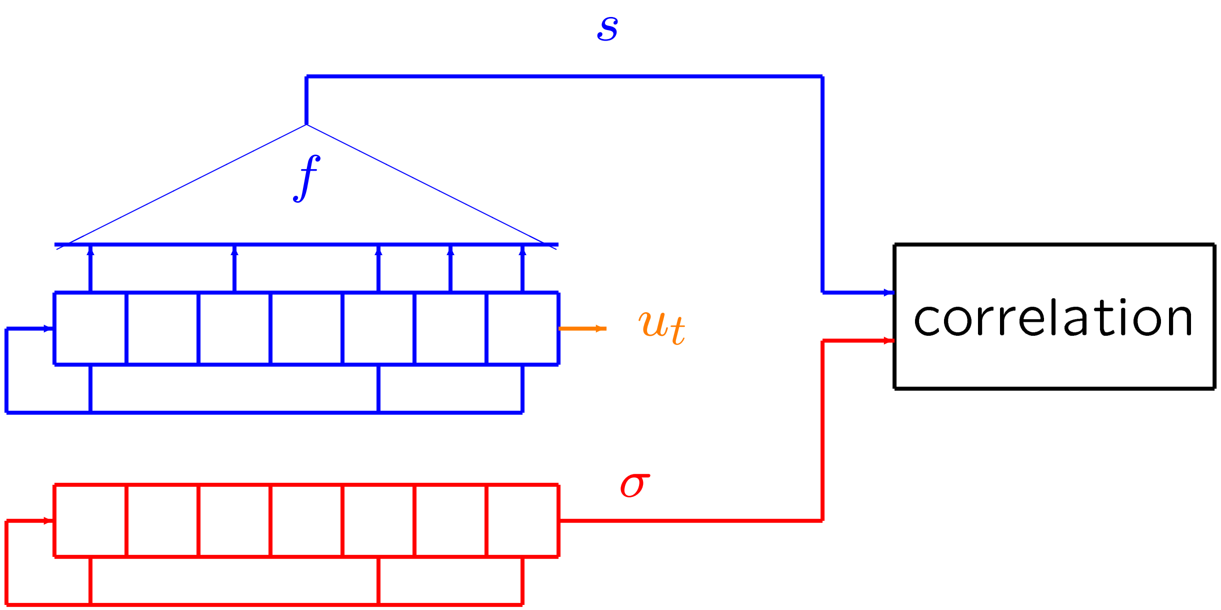
Correlation attack on a filter generator

Let $a \in \mathbf{F}_2^n$ which minimizes

$$p_a = \Pr[f(x_1, \dots, x_n) \neq \varphi_a] = \Pr[s_t \neq \sigma_t]$$

where $\sigma_t = \varphi_a(u_{t+\gamma_1}, \dots, u_{t+\gamma_n})$.

The sequence σ is produced by an LFSR with the same feedback polynomial but with initial state $\varphi_a(u_{t+\gamma_1}, \dots, u_{t+\gamma_n}),\ \ 0 \leq t < L$.



Boolean functions with a high nonlinearity (1)

Proposition.

$$2^{\frac{n}{2}} \leq \min_{f \in \mathcal{B}ool_n} \mathcal{L}(f) \leq 2^{\frac{n+1}{2}}$$

where the lower bound is tight if and only if n is even and f is bent.

Some properties of bent functions. [Rothaus 76][Dillon 74]

Let f be a bent function of n variables.

- $\forall a \in \mathbf{F}_2^n,\ \ \mathcal{F}(f + \varphi_a) = \pm 2^{\frac{n}{2}}$. In particular, f is not balanced.
- $\deg f \leq \frac{n}{2}$.

Quadratic functions.

For n odd, $n = 2t + 1$

$$x_1 x_2 + x_3 x_4 + \ldots + x_{2t-1} x_{2t} + x_{2t+1}$$

satisfies $\mathcal{L}(f) = 2^{\frac{n+1}{2}}$. Moreover, f is balanced and

$$\forall a \in \mathbf{F}_2^n,\ \ \mathcal{F}(f + \varphi_a) \in \{0, \pm 2^{\frac{n+1}{2}}\}.$$

Boolean functions with a high nonlinearity (2)

n	$\min_{f \in \mathcal{B}ool_n} \mathcal{L}(f)$	
5	8	[Berlekamp-Welch 72]
7	16	[Mykkelveit 80]
9	24, 26, 28, 30	[Kavut-Maitra-Yücel 06]
11	46-60	
13	92-120	
15	182-216	[Paterson-Wiedemann 83]

Open problem. Find the highest possible nonlinearity for a Boolean function of n variables, where n is odd and $n \geq 9$.
(Covering radius of $RM(1, n)$)

Balanced Boolean functions with a high nonlinearity

Proposition. [Dobbertin 94]

For balanced functions f of n variables, n even,

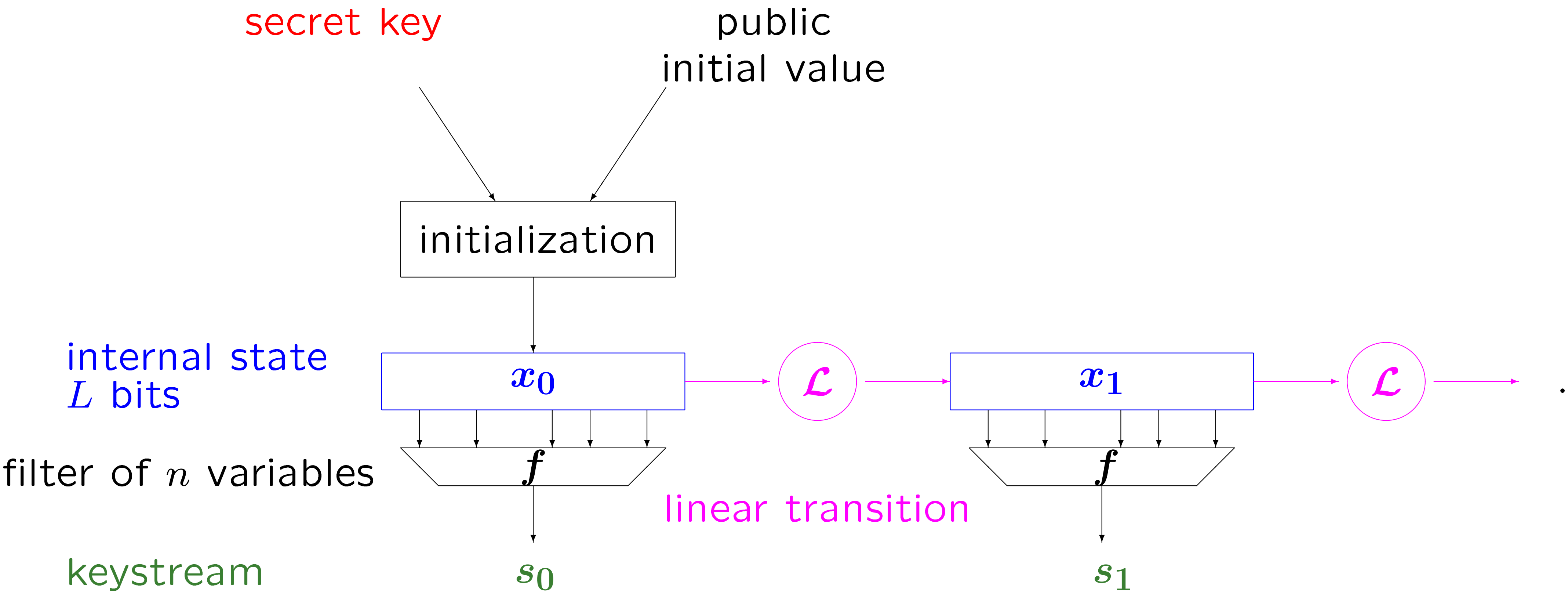
$$2^{\frac{n}{2}} + 4 \leq \min_{f \in \mathcal{B}al_n} \mathcal{L}(f) \leq 2^{\frac{n}{2}} + \min_{g \in \mathcal{B}al_{\frac{n}{2}}} \mathcal{L}(g)$$

n	$\min_{f \in \mathcal{B}al_n} \mathcal{L}(f)$
4	8
5	8
6	12
7	16
8	20, 24
9	24, 28, 32
10	36, 40

Open problem. Find the highest possible nonlinearity for a balanced Boolean function of n variables, where n is even and $n \geq 8$.

Algebraic attacks and related criteria

Stream cipher with a linear transition function



Algebraic attacks [Courtois-Meier 03]

Let $AN(f) = \{g,\ g(x)f(x) = 0 \text{ for all } x \in \mathbf{F}_2^n\}$.

Let $g \in AN(f)$, i.e., such that $g(x)f(x) = 0$ for all x.

$$g(x_t)f(x_t) = g(x_t)s_t = 0$$

$$\Longrightarrow g \circ \mathcal{L}^t(x_0) = 0 \text{ if } s_t = 1 \ .$$

Let $h \in AN(1+f)$, i.e, such that $h(x)(1+f(x)) = 0$ for all $x \in \mathbf{F}_2^n$.

$$h(x_t)(1+f(x_t)) = h(x_t)(1+s_t) = 0$$

$$\Longrightarrow h \circ \mathcal{L}^t(x_0) = 0 \text{ if } s_t = 0 \ .$$

Algebraic system with L variables of degree

$$d = \min\{\deg(g), g \in AN(f) \cup AN(1+f), g \neq 0\} \ .$$

Complexity of the attack

$AI(f)$ = algebraic immunity of the filtering function f
$AI(f) = \min\{\deg(g),\ g \in AN(f) \cup AN(1+f),\ g \neq 0\}$.

Required number of keystream bits:

$$N \geq \frac{2L^{AI(f)}}{AI(f)!(A_0^{AI(f)} + A_1^{AI(f)})}$$

Number of operations:

$$\left(\sum_{i=0}^{AI(f)} \binom{L}{i}\right)^{\omega} \simeq L^{AI(f)\omega} \text{ where } \omega \simeq 2.37$$

Existence of $g \in AN(f)$ with $\deg g \leq d$

x such that $f(x) = 1$ $[wt(f)]$

$$\begin{array}{r|c|}
\cline{2-2}
1 & \\
x_1 & \\
\vdots & \\
x_n & RM^f(d,n) \\
x_1x_2 & \\
\vdots & \\
x_{n-1}x_n & \\
\cline{2-2}
\end{array}$$

all monomials of degree $\leq d$ $\left[\sum_{i=0}^{d}\binom{n}{i}\right]$

$$\dim\{g \in AN(f), \deg g \leq d\} = \sum_{i=0}^{d}\binom{n}{i} - \operatorname{rank}\left(RM^f(d,n)\right) \; .$$

Proposition. There exists $g \neq 0$ in $AN(f)$ with $\deg g \leq d$ if

$$wt(f) < \sum_{i=0}^{d}\binom{n}{i} \; .$$

Bounds on the algebraic immunity
[Courtois-Meier 03][Dalai-Gupta-Maitra 04]

Proposition.
Let f be a Boolean function of n variables. If $AI(f) \geq d$, then

$$\sum_{i=0}^{d} \binom{n}{i} \leq wt(f) \leq 2^n - \sum_{i=0}^{d} \binom{n}{i}$$

Corollary. For any f of n variables,

$$AI(f) \leq \left\lceil \frac{n}{2} \right\rceil .$$

Moreover, if f has optimal AI, then

- if n is odd, $wt(f) = 2^{n-1}$
- if n is even,

$$2^{n-1} - \frac{1}{2}\binom{n}{n/2} \leq wt(f) \leq 2^{n-1} + \frac{1}{2}\binom{n}{n/2} .$$

Algebraic immunity and nonlinearity [Dalai-Gupta-Maitra 04]

Proposition. Let f be a function of n variables. If f has algebraic immunity at least d, then

$$\mathcal{NL}(f) \geq \sum_{i=0}^{d-2} \binom{n}{i}.$$

Most notably, if f has optimal algebraic immunity, then

$$\mathcal{NL}(f) \geq \begin{cases} 2^{n-1} - \binom{n}{\frac{n-1}{2}} & \text{if } n \text{ is odd} \\ 2^{n-1} - \frac{1}{2}\binom{n}{\frac{n}{2}} - \binom{n}{\frac{n}{2}-1} & \text{if } n \text{ is even} \end{cases}$$

The converse does not hold! (e.g. bent functions of degree 2).

Some practical constructions

Symmetric functions [C.-Videau05]

Definition. A Boolean function is symmetric if its output is invariant under any permutation of its inputs.
$\Longleftrightarrow$ The output only depends on the Hamming weight of the input vector.

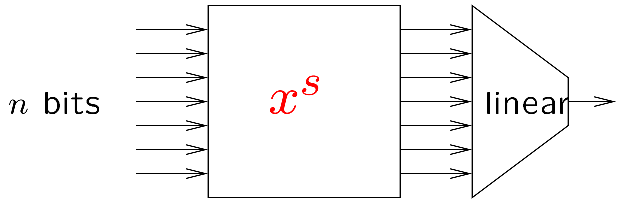
Implementation.

- A symmetric function of n variables can be represented by a vector of $(n+1)$ bits.
- complexity: $\mathcal{O}(n)$.

Related problems.

- Only a few balanced functions (except those having linear structures).
- Highly nonlinear functions are (close to) quadratic functions.

Components of power functions



$$S_\lambda : x \longmapsto \mathrm{Tr}(\lambda x^s) \text{ over } \mathbf{F}_{2^n}, \quad \lambda \in \mathbf{F}_{2^n}^*$$

Proposition. The Hamming weight of S_λ is divisible by $\gcd(s, 2^n - 1)$.
In particular:

- S_λ is balanced if and only if $\gcd(s, 2^n - 1) = 1$.
- If S_λ is bent, then $\gcd(s, 2^n - 1) > 1$
  and s is coprime either with $(2^{\frac{n}{2}} - 1)$ or with $(2^{\frac{n}{2}} + 1)$.

Balanced components of power functions

- For odd n:

$$\mathcal{L}(S_\lambda) \geq 2^{\frac{n+1}{2}}$$

with equality for almost bent (AB) functions [Chabaud-Vaudenay94].

- For even n: it is conjectured that

$$\mathcal{L}(S_\lambda) \geq 2^{\frac{n}{2}+1}$$

Known AB power functions $S : x \mapsto x^s$ over $\mathbf{F}_{2^n}$ with $n = 2t + 1$

	exponents s	
quadratic	$2^i + 1$ with $\gcd(i, n) = 1$, $1 \leq i \leq t$	[Gold 68],[Nyberg 93]
Kasami	$2^{2i} - 2^i + 1$ with $\gcd(i, n) = 1$ $2 \leq i \leq t$	[Kasami 71]
Welch	$2^t + 3$	[Dobbertin 98] [C.-Charpin-Dobbertin 00]
Niho	$2^t + 2^{\frac{t}{2}} - 1$ if t is even $2^t + 2^{\frac{3t+1}{2}} - 1$ if t is odd	[Dobbertin 98] [Xiang-Hollmann 01]

Known power permutations $S : x \mapsto x^s$ over $\mathbf{F}_{2^n}$, n even, with the highest nonlinearity

$2^i + 1,\ \gcd(i,n) = 2$	$n \equiv 2 \bmod 4$	[Gold 68]
$2^{2i} - 2^i + 1,\ \gcd(i,n) = 2$	$n \equiv 2 \bmod 4$	[Kasami 71]
$\sum_{i=0}^{n/2} 2^{ik},\ \gcd(k,n) = 1$	$n \equiv 0 \bmod 4$	[Dobbertin 98]
$2^{\frac{n}{2}} + 2^{\frac{n+2}{4}} + 1$	$n \equiv 2 \bmod 4$	[Cusick-Dobbertin 95]
$2^{\frac{n}{2}} + 2^{\frac{n}{2}-1} + 1$	$n \equiv 2 \bmod 4$	[Cusick-Dobbertin 95]
$2^{\frac{n}{2}} + 2^{\frac{n}{4}} + 1$	$n \equiv 4 \bmod 8$	[Dobbertin 98]
$2^{n-1} - 1$		[Lachaud-Wolfmann 90]

Conclusions

Paradox for hardware-oriented ciphers:

Every Boolean function having a strong algebraic structure is weak.
The implementation complexity of almost all n-variable Boolean functions is greater than $2^n/n$.

$\longrightarrow$ search for suboptimal functions regarding both the resistance to known attacks and the implementation complexity.