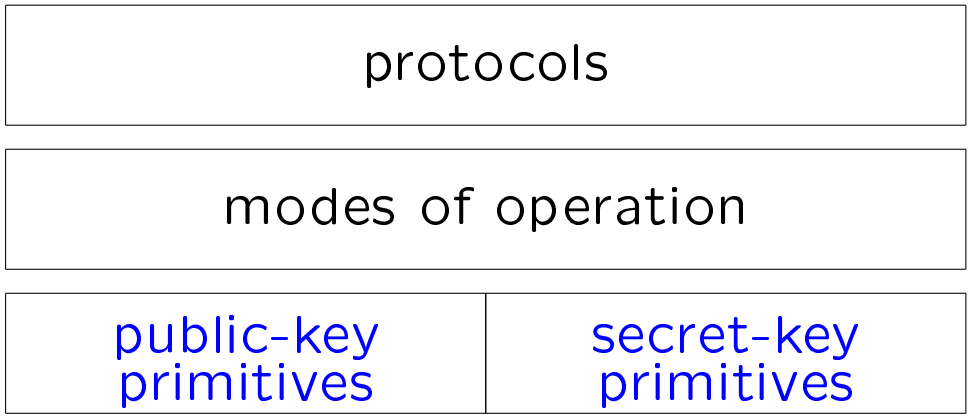
Analysis and design of symmetric ciphers

Anne Canteaut

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

September 15, 2006

Overview of the situation



High-level layers: security proofs in some models (random oracle model, ideal cipher model . . .).

Low-level layer: very fragile situation.

Nessie portfolio of recommended cryptographic primitives (Feb. 2003) :

« **Stream ciphers and pseudorandom number generators:** *the Nessie portfolio in this category is empty.* »

Secret-key vs. public-key ciphers

algorithms for achieving confidentiality

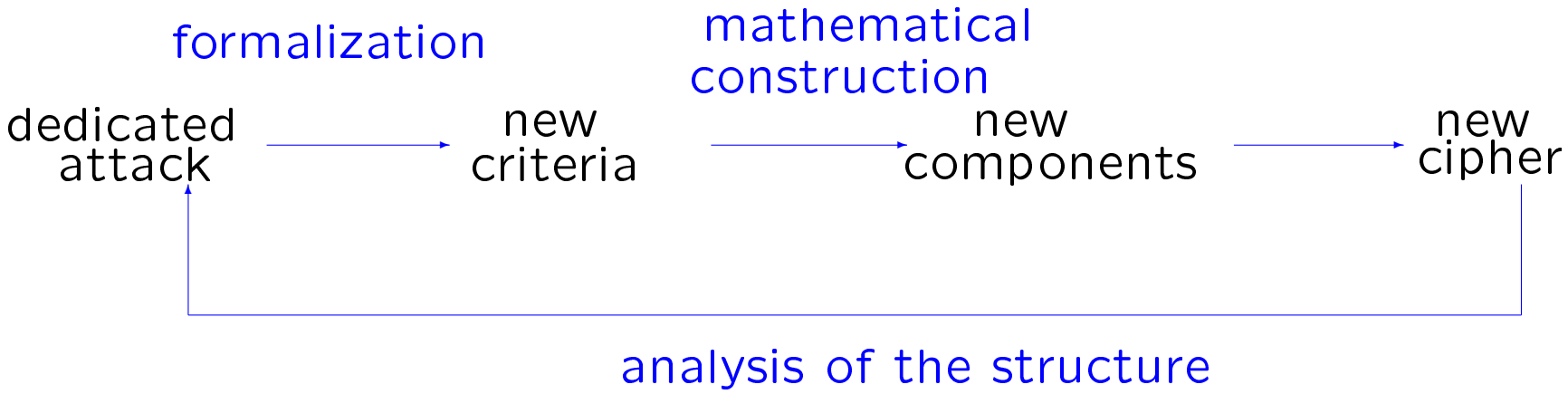
public-key (asymmetric)	**secret-key (symmetric)**
RSA, elliptic curves	AES, DES
no key exchange	key exchange
RSA-OAEP: { 24 Kcycles/Byte 484 Kcycles/Byte	AES-CTR: 30 cycles/Byte Sosemanuk: 6.5 cycles/Byte

In practice: the session key is transmitted with a public-key cipher and the data are enciphered by a secret-key algorithm.

$\longrightarrow$ Pressing demand for secure and fast algorithms dedicated to low-cost devices: E0 (Bluetooth), A5/1 (GSM), Kasumi (UMTS)...

The game

Problem. Design a secure and efficient cipher



Approach.

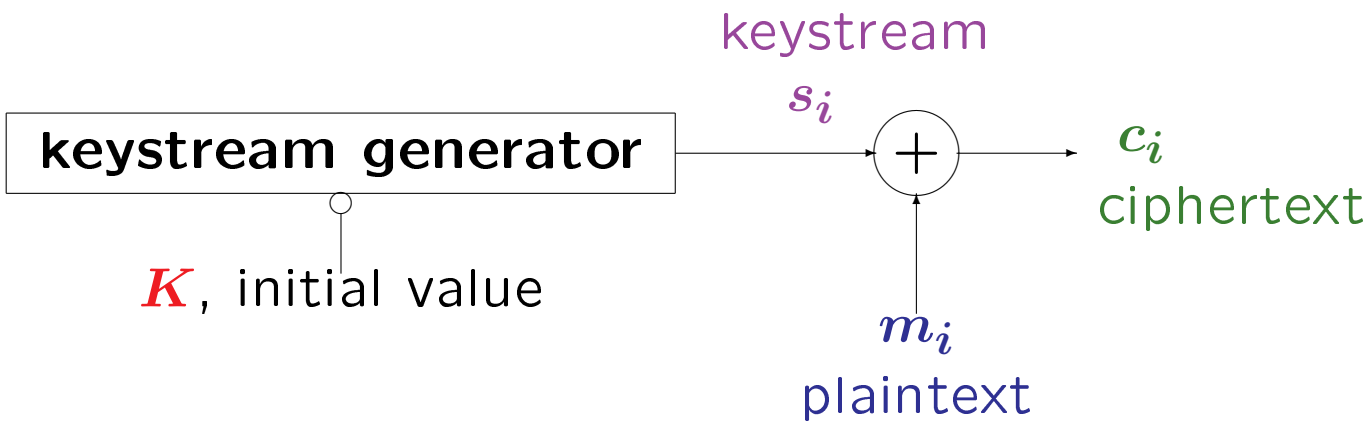
- Consider all aspects together, from the most theoretical ones to the very practical ones.
- The very particular building-blocks achieving optimal resistance and optimal implementation may introduce unintended weaknesses.

Outline

1. **Stream ciphers**
   - Some security criteria for the filtering function (distinguishing attacks, correlation attacks,...)
   - Construction of appropriate filtering functions
2. **Block ciphers**
   - Some security criteria for the S-boxes
   - Optimal S-boxes for linear and differential cryptanalysis
   - Weaknesses induced by optimal S-boxes

Stream ciphers

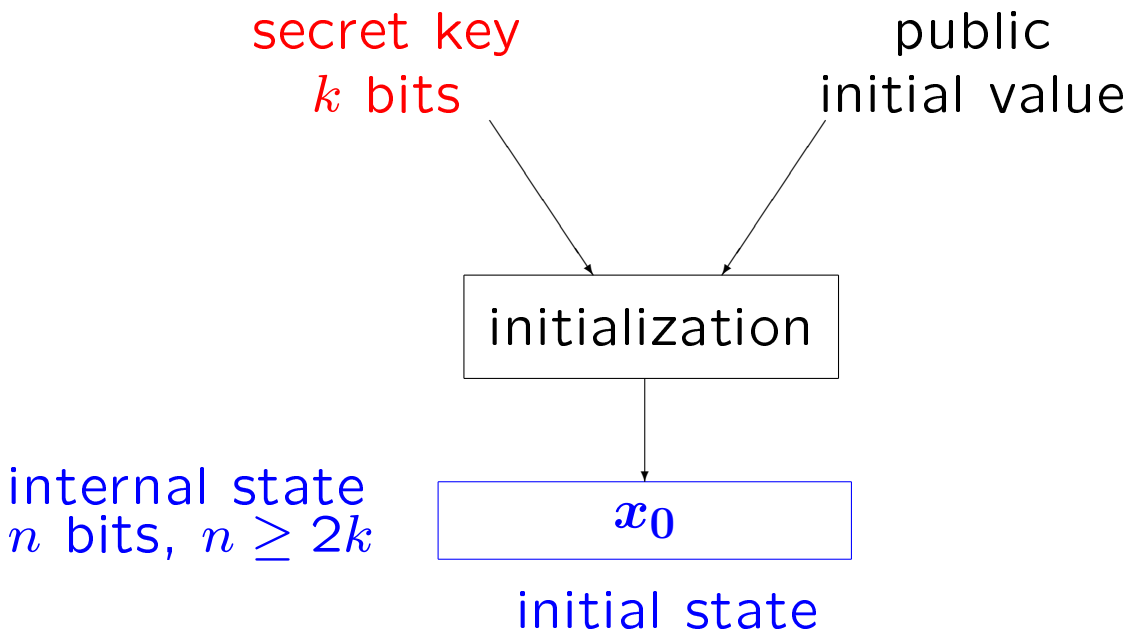
Additive synchronous stream ciphers



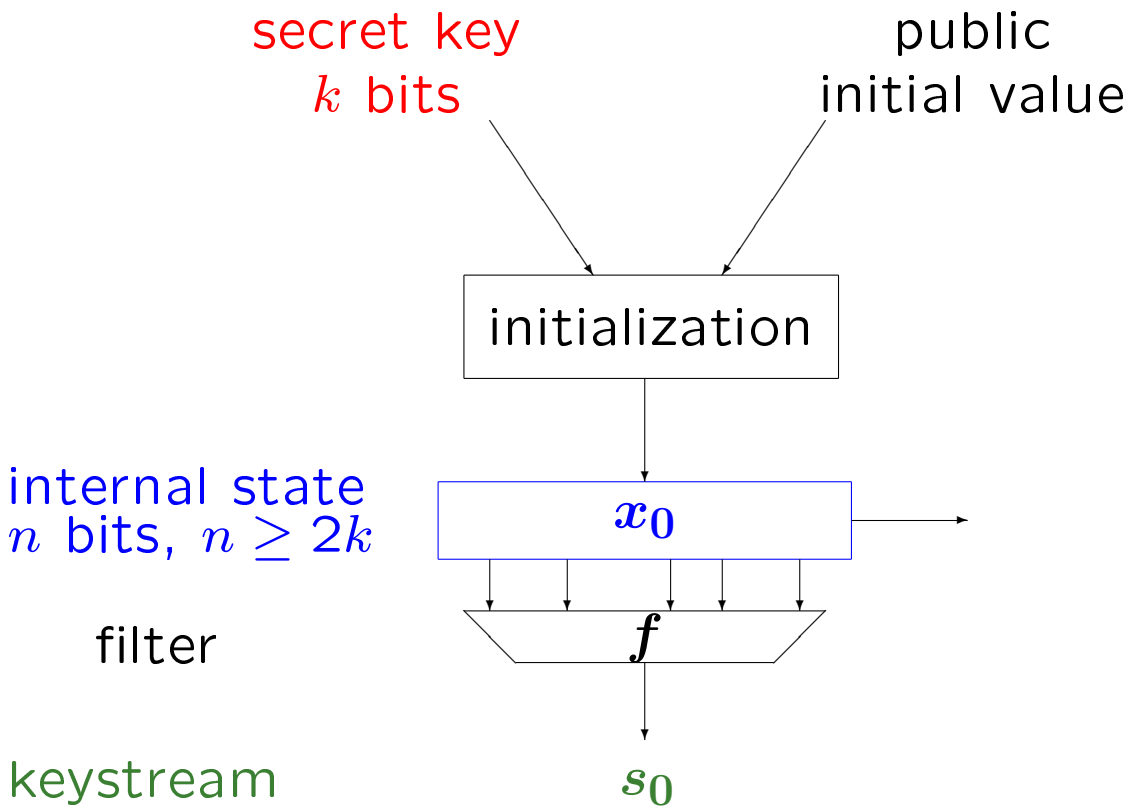
Known-plaintext attacks:

- Key-recovery attacks: recover the secret-key from N keystream bits;
- Initial state-recovery attacks: recover the initial state from N keystream bits;
- Distinguishing attacks: distinguish N keystream bits from a random sequence.

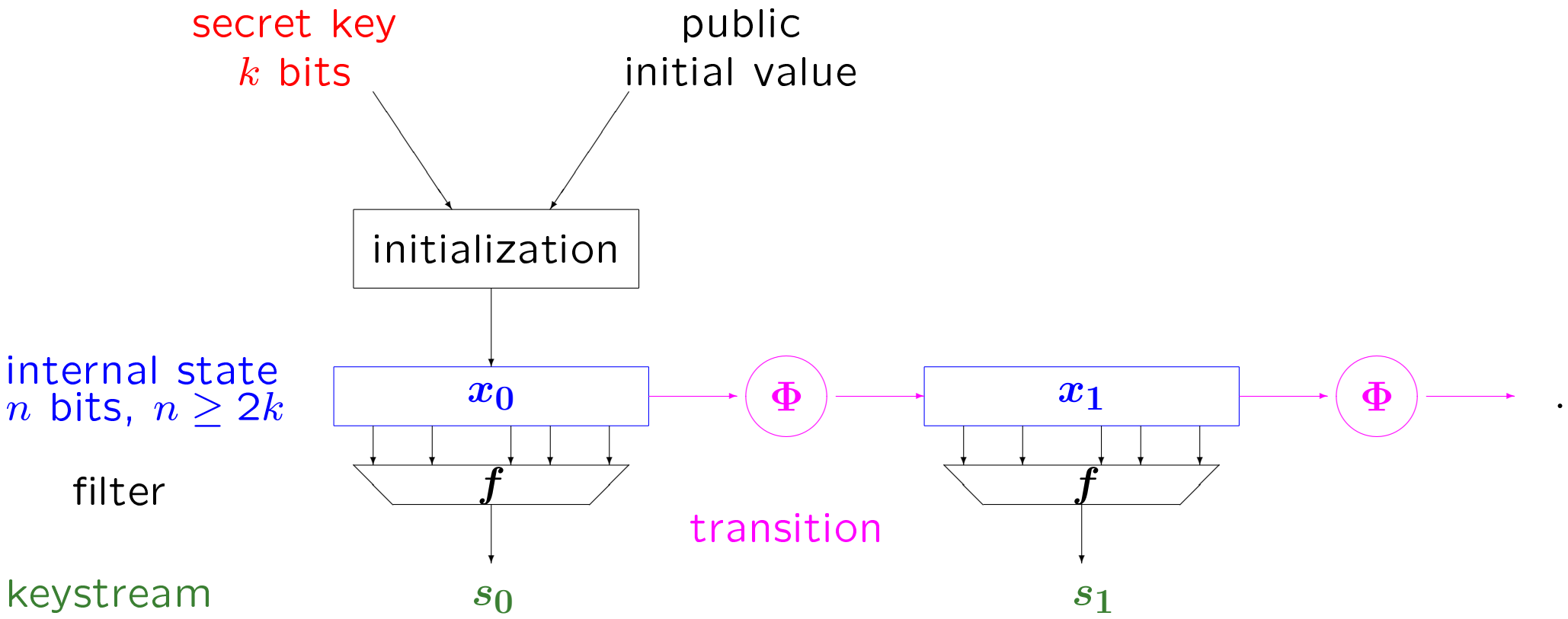
General design



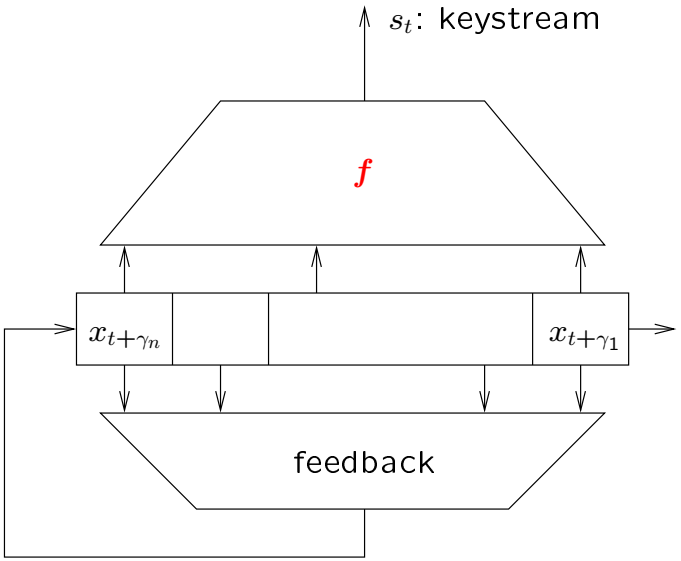
General design



General design



Augmented function of a filtered shift register



$$s_t = f(x_{t+\gamma_1}, x_{t+\gamma_2}, \ldots, x_{t+\gamma_n})$$

Attack principle. Exploit a bias in the distribution of $(s_t, s_{t+\tau})$, $t \geq 0$, for a fixed τ.

Proposition. [Golic 96][C. 06] $(s_{t+\gamma_1}, \ldots, s_{t+\gamma_n})$ is uniformly distributed **if and only if**

$$f(x_1, \ldots, x_n) = x_1 + g(x_2, \ldots, x_n)$$

$$\text{or } f(x_1, \ldots, x_n) = g(x_1, \ldots, x_{n-1}) + x_n \ .$$

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 spectrum of $f : \mathbf{F}_2^n \to \mathbf{F}_2$

$$\left\{ \mathcal{F}(f + \varphi_a) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)+a \cdot x}, \ a \in \mathbf{F}_2^n \right\}$$

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

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

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

Distinguisher based on sparse parity-check relations

[Molland-Helleseth 04], [Englund-Johansson 04], [Leveiller *et al.* 02]

For LFSR-based generators.

- Search for a parity-check relation of weight w for the LFSR:
  $x_t + x_{t+\tau_1} + \ldots + x_{t+\tau_{w-1}} = 0, \ \forall t.$
- Distinguish the distribution of $(s_t, s_{t+\tau_1}, \ldots, s_{t+\tau_{w-1}})$ from the uniform distribution.

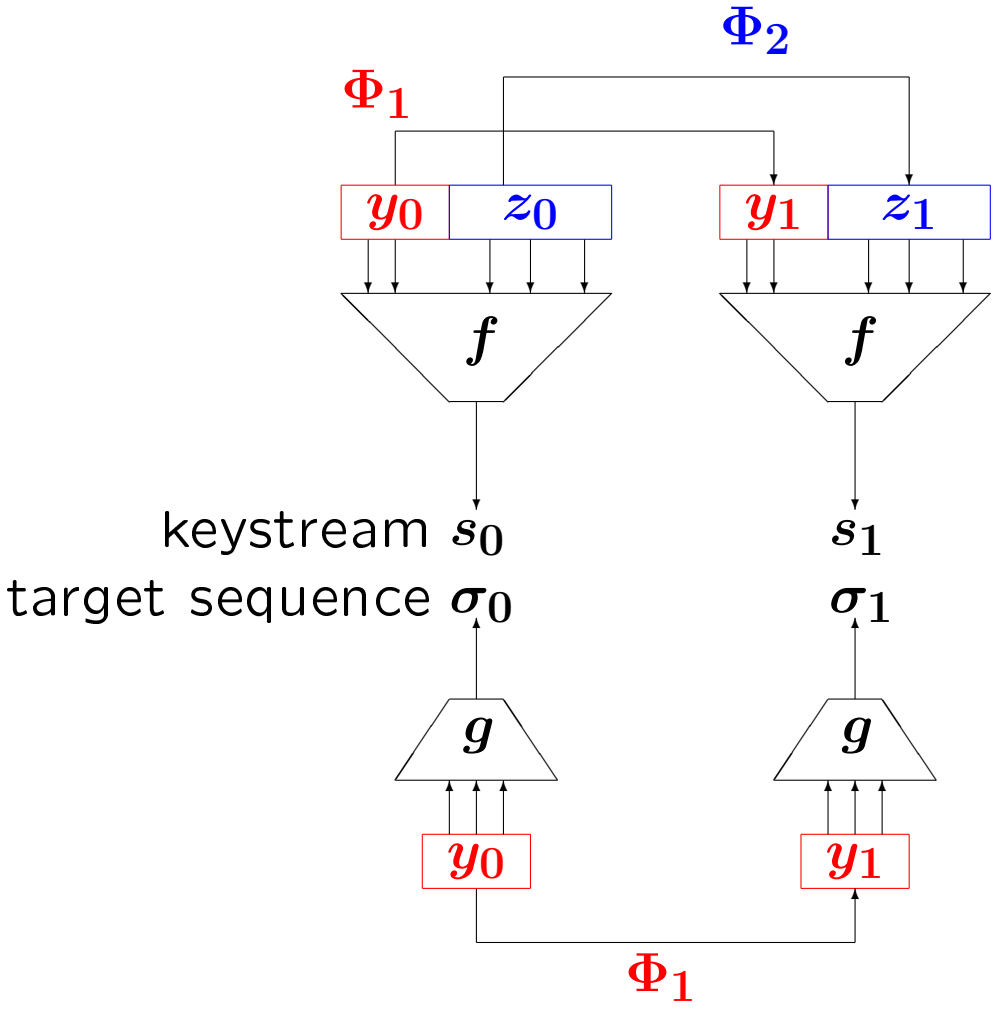
Complexity.

$$\text{time complexity} = \frac{w}{\Delta_w^2} \qquad \text{data complexity} = \frac{1}{\Delta_w^2} + \tau_{w-1}$$

$$\text{with } \Delta_w = 2^{-wn} \sum_{\lambda \in \mathbf{F}_2^n} \mathcal{F}^w(f + \varphi_\lambda).$$

Reverse-engineering techniques [C.-Filiol00][Cluzeau 04]

Correlation attack [Siegenthaler 85]



where g is a function such that

$$p_g = \Pr_{Y,Z}[f(Y,Z) = g(Y)] > \frac{1}{2}.$$

Approximation of f by a function of fewer variables

[Zhang-Chan 00][C.-Trabbia 00][C. 02]

Proposition. Let $V \subset \mathbf{F}_2^n$ and $g : V \longrightarrow \mathbf{F}_2$.

$$\max_{g \in \mathcal{B}ool_V} \left| p_g - \frac{1}{2} \right| \leq \frac{1}{2^{n+1}} \left(\sum_{\lambda \in V} \mathcal{F}^2(f + \varphi_\lambda) \right)^{1/2}$$

In particular:

- For any V of dimension ℓ,

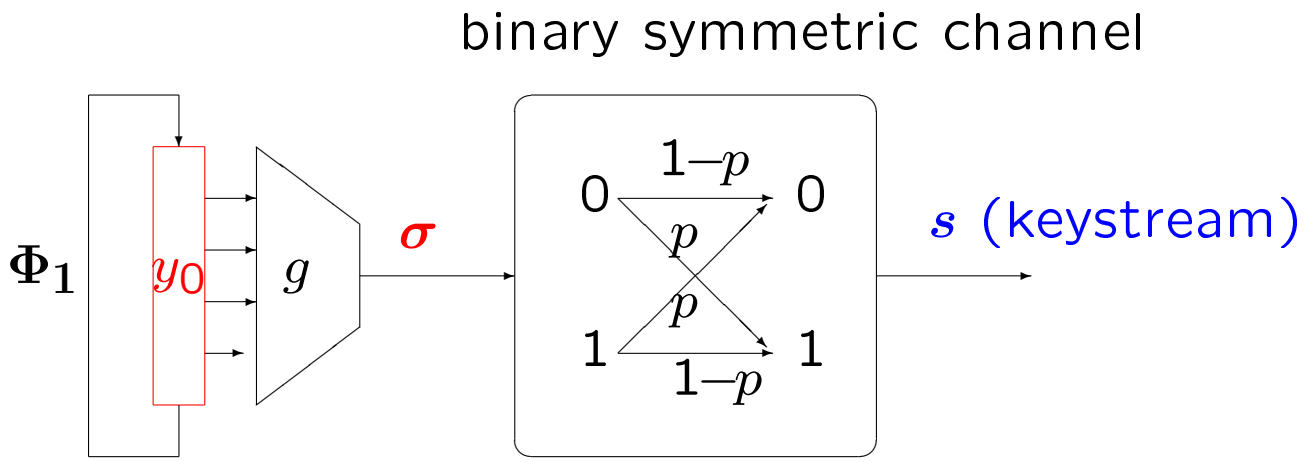
$$\max_g \left| p_g - \frac{1}{2} \right| \leq 2^{\frac{\ell}{2} - n - 1} \mathcal{L}(f).$$

- 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.

Correlation attack as a decoding problem [Meier-Staffelbach 88]



Error probability:

$$\forall t \geq 0,\ \Pr[s_t \neq \sigma_t] = 1 - p_g < \frac{1}{2}$$

$(\sigma_t)_{t<N}$ belongs to the code of length N and size 2^ℓ defined by Φ_1 and g.

Iterative decoding using parity-check equations of weight w

[Meier-Staffelbach 88], [C.-Trabbia 00]

- Find some multiples of weight w of the feedback polynomial.
- Exploit the parity-check relations for decoding the received word with an iterative decoding algorithm (variant of Gallager's algorithm).

$$\textbf{Number of keystream bits: } \propto \left(\frac{1}{2\varepsilon}\right)^{\frac{2(w-2)}{w-1}} 2^{\frac{\ell}{w-1}}.$$

$$\textbf{Precomputation } \simeq \frac{N^{w-2}}{(w-2)!} \qquad \textbf{Decoding } \propto \left(\frac{1}{2\varepsilon}\right)^{\frac{2w(w-2)}{w-1}} 2^{\frac{\ell}{w-1}}.$$

For $w = 4$:

$\ell = 40$, $p = 0.44$, $N = 400\ 000$ keystream bits.
Precomputation: 9 h, decoding: 1.5 h.

$\ell = 60$, $p = 0.4$, $N = 900\ 000$ keystream bits, 2^{38} operations.

Search for appropriate filtering functions

Security criteria.

- balancedness;
- nonlinearity;
- w-th power moments of the Walsh spectrum for small w;
- algebraic-immunity.

Highest possible nonlinearity.

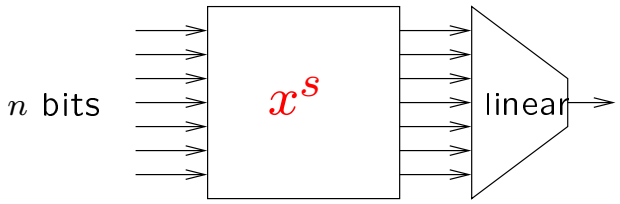
$$2^{\frac{n}{2}} \leq \min_{f \in \mathcal{B}ool_n} \mathcal{L}(f) \leq 2^{\frac{n+1}{2}}$$

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

Implementation constraints.

- symmetric functions [C.-Videau05];
- components of power functions.

Components of power functions



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

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.

- For even n: it is conjectured that

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

Proposition. For $\lambda \neq 0$,

$$\sum_{\mu \in \mathbf{F}_2^n} \mathcal{F}^3(S_\lambda + \varphi_\mu) = 2^{2n+1} + 2^{2n}(\delta_1 - 2)$$

$$\sum_{\mu \in \mathbf{F}_2^n} \mathcal{F}^4(S_\lambda + \varphi_\mu) = 2^{3n+1} + 2^{2n} \sum_{c \in \mathbf{F}_2^n} \delta_c(\delta_c - 2)$$

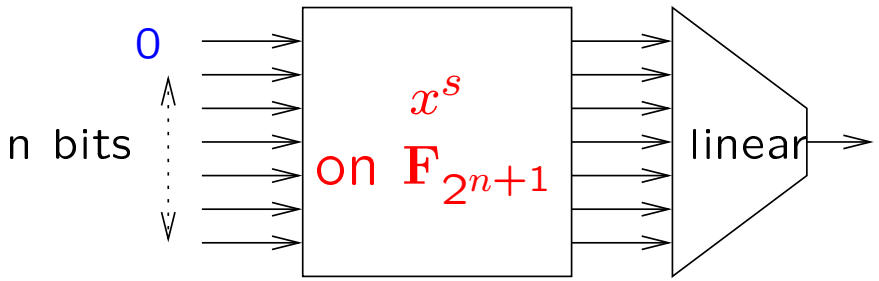
with $\delta_c = |\{x \in \mathbf{F}_{2^n},\ (x+1)^s + x^s = c\}|$.

Restrictions of a bent function

Proposition. [C.-Carlet-Charpin-Fontaine 01]

f is a bent function of n variables, n even, if and only if for any hyperplane H, the restrictions of f to H and $\overline{H}$ are such that their Walsh spectra are $\{0, \pm 2^{\frac{n}{2}}\}$ and

$$\mathcal{F}(f_H + \varphi_\lambda) \neq \mathcal{F}(f_{\overline{H}} + \varphi_\lambda), \ \forall \lambda \in \mathbf{F}_2^{n-1} \ .$$



Power functions with bent components

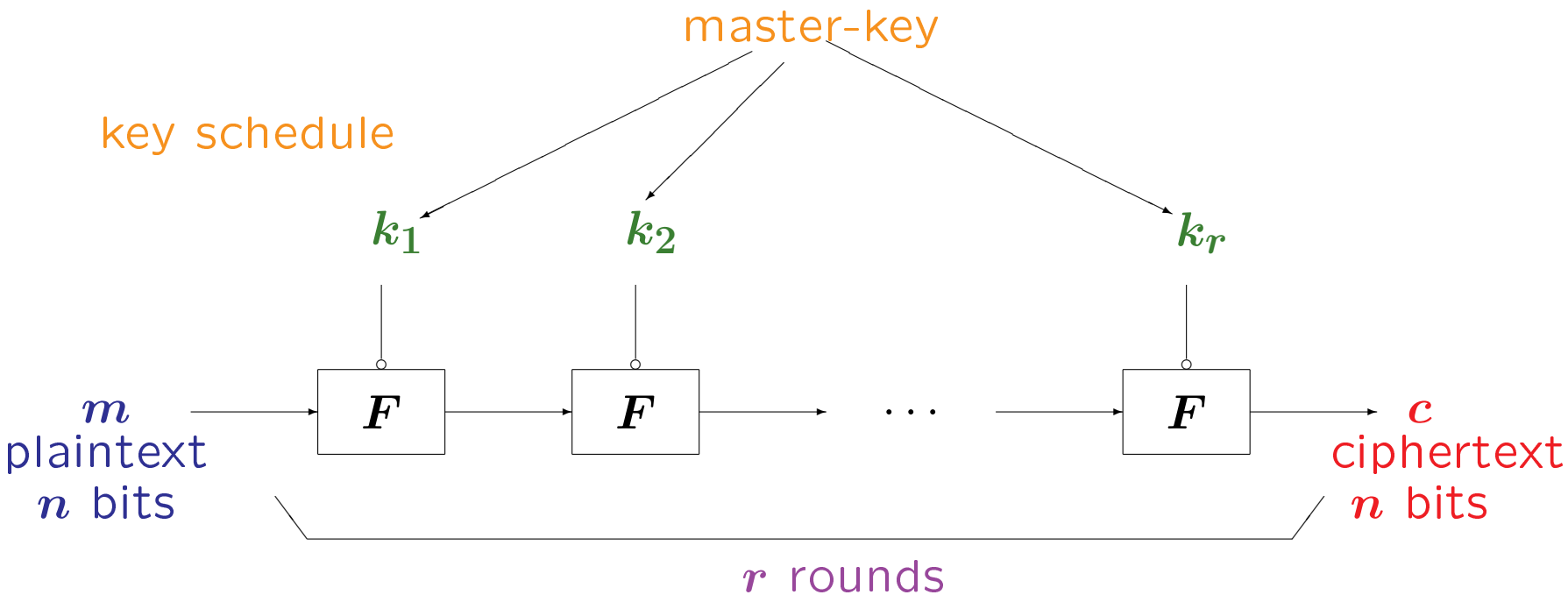
Problem. Find all integers s such that there exists $\lambda \in \mathbf{F}_{2^n}$ for which

$$x \longmapsto \mathrm{Tr}(\lambda x^s) \text{ is bent .}$$

$\mathcal{PS}_{ap}$	$a(2^{\frac{n}{2}}-1)$	$\gcd(a,2^{\frac{n}{2}}+1)=1$	[Dillon74] [Lachaud-Wolfmann90]
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n)=1$	[Dillon-Dobbertin04]
Maiorana -McFarland	2^i+1	$\frac{n}{\gcd(n,i)}$ even	[Gold68]
	$(2^{\frac{n}{4}}+1)^2$	$n \equiv 0 \bmod 4$	[Leander05]
	$2^{\frac{n}{3}}+2^{\frac{n}{6}}+1$	$n \equiv 0 \bmod 6$	[C-Charpin-Kyureghyan 06]

Block ciphers

Iterated block ciphers

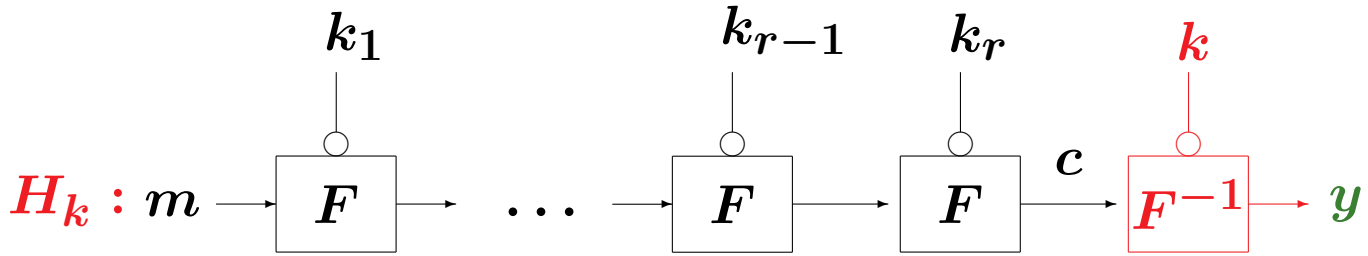


where the round function F_k is a permutation of $\mathbf{F}_2^n$ for all $k \in \mathcal{K}$

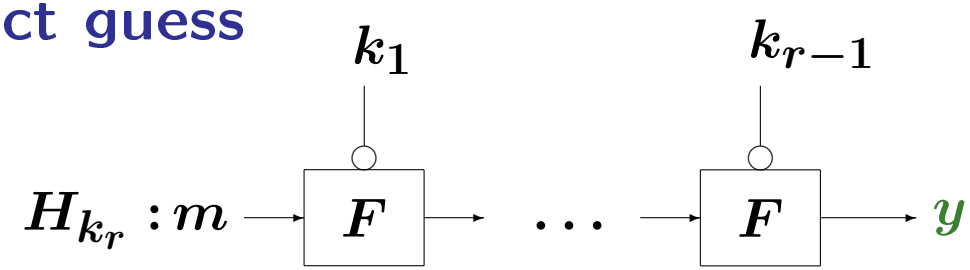
Last-round attack

Principle. Exploit a distinguisher for the reduced cipher, i.e., for $(r-1)$ rounds.

k: candidate for k_r



Correct guess



Wrong guess

$\simeq$ random permutation (hypothesis of wrong-key randomization)

Differential cryptanalysis [Biham-Shamir 91]

Principle. Exploit a bias in the distribution of a derivative of the reduced cipher

$$D_a G_k : x \longmapsto G_k(x+a) + G_k(x)$$

Security criterion for the round function

$$\delta_F = \max_{a,b \neq 0} \#\{X \in \mathrm{F}_2^n,\ F(X+a) + F(X) = b\} \text{ must be small.}$$

Proposition. [Nyberg-Knudsen 92]

For any $F : \mathrm{F}_2^n \longrightarrow \mathrm{F}_2^n$, $\delta_F \geq 2$.

In case of equality, F is **almost perfect nonlinear (APN)**.

Linear cryptanalysis [Matsui 93] [Gilbert-Chassé 91]

Principle. Exploit an affine approximation of the reduced cipher.

Security criterion for the round function

$$\mathcal{L}(F) = \max_{a,b \neq 0} \left| \sum_{x \in \mathbf{F}_2^n} (-1)^{b \cdot F(x) + a \cdot x} \right| \quad \text{must be small.}$$

Proposition. [Sidelnikov 71] [Chabaud-Vaudenay 94]

For any function $F : \mathbf{F}_2^n \longrightarrow \mathbf{F}_2^n$,

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

In case of equality, F is **almost bent (AB)** (n odd).

3-rd and 4-th power moments of S-boxes

Let $F : \mathbf{F}_2^n \longrightarrow \mathbf{F}_2^n$ and $F_\lambda : x \longmapsto \lambda \cdot F(x)$, $\lambda \neq 0$.

Theorem.

$$\sum_{\lambda \in \mathbf{F}_2^n \setminus \{0\}} \sum_{\mu \in \mathbf{F}_2^n} \mathcal{F}^3(F_\lambda + \varphi_\mu) = 2^{2n+1}(2^n - 1) + 2^{2n} D_0(F)$$

$$\sum_{\lambda \in \mathbf{F}_2^n \setminus \{0\}} \sum_{\mu \in \mathbf{F}_2^n} \mathcal{F}^4(F_\lambda + \varphi_\mu) = 2^{3n+1}(2^n - 1) + 2^{2n} D(F)$$

where

$$D_0(F) = |(a,b),\ a,b \in \mathbf{F}_2^n \setminus \{0\},\ a \neq b,\ D_a D_b F(0) = 0\}|$$
$$D(F) = |(a,b,x),\ a,b \in \mathbf{F}_2^n \setminus \{0\},\ x \in \mathbf{F}_2^n,\ a \neq b,\ D_a D_b F(x) = 0\}|$$

Corollary. [Berger - C. - Charpin - Laigle-Chapuy 06]

$$\sum_{\lambda \in \mathbf{F}_2^n \setminus \{0\}} \sum_{\mu \in \mathbf{F}_2^n} \mathcal{F}^4(F_\lambda + \varphi_\mu) \geq 2^{3n+1}(2^n - 1)$$

with equality if and only if F is APN.

Link between APN and AB properties

Theorem. [C.-Charpin-Dobbertin 99]

Let $F : \mathbf{F}_2^n \longrightarrow \mathbf{F}_2^n$, and

$$D(F) = |(a,b,x),\ a,b \in \mathbf{F}_2^n \setminus \{0\}, x \in \mathbf{F}_2^n, a \neq b,\ D_a D_b F(x) = 0\}| \ .$$

(i)

$$D(F) \leq (2^n - 1)\left(\mathcal{L}^2(F) - 2^{n+1}\right)$$

with equality if and only if all $\mathcal{F}(F_\lambda + \varphi_\mu)$ are in $\{0, \pm\mathcal{L}(F)\}$.

(ii) If all nonzero Walsh coefficients are such that $|\mathcal{F}(F_\lambda + \varphi_\mu)| \geq L_0$, then

$$D(F) \geq (2^n - 1)\left(L_0^2 - 2^{n+1}\right) \ ,$$

with equality if and only if all $\mathcal{F}(F_\lambda + \varphi_\mu)$ are in $\{0, \pm L_0\}$.

Corollary. [Chabaud-Vaudenay94]

Let $F : \mathbf{F}_2^n \longrightarrow \mathbf{F}_2^n$, n odd. If F is AB, then F is APN.

Link between APN and AB properties (2)

Corollary. [C.-Charpin-Dobbertin 99]

Let $F : \mathbf{F}_2^n \longrightarrow \mathbf{F}_2^n$, n odd.

F is AB **if and only if** F is APN and all its Walsh coefficients are divisible by $2^{\frac{n+1}{2}}$.

For power functions: the divisibility of the Walsh coefficients can be computed by McEliece theorem.

Theorem. Let $S : x \longmapsto x^s$ over $\mathbf{F}_{2^n}$, n odd.

S is AB if and only if S is APN and for all integers u, $0 \leq u \leq 2^n - 1$,

$$w_2(us \bmod (2^n - 1)) \leq w_2(u) + \frac{n-1}{2} .$$

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]

Optimal functions for even n

Resistance to linear attacks.

Conjecture. For any $S : x \longmapsto x^s$ over $\mathbf{F}_{2^n}$, n even,

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

Theorem. The conjecture holds if $\gcd(s,2^n-1) > 1$.
Moreover, if $\mathcal{L}(S) = 2^{\frac{n}{2}+1}$, then $\gcd(s,2^n-1) = 3$ and

$$\mathcal{F}(S_\lambda) = \begin{cases} (-1)^{\frac{n}{2}+1} 2^{\frac{n}{2}+1} & \text{if } \lambda \in \{x^3, x \in \mathbf{F}_{2^n}^\star\} \\ (-1)^{\frac{n}{2}} 2^{\frac{n}{2}} & \text{if } \lambda \notin \{x^3, x \in \mathbf{F}_{2^n}^\star\} \end{cases}.$$

Resistance to differential attacks.

There is no APN power permutations.

Open problem. Find an APN permutation over $\mathbf{F}_{2^n}$, n even.

Differentially 4-uniform power permutations for even n

n	s	$w_2(s)$	s^{-1}	$w_2(s^{-1})$	$\mathcal{L}(S)$	divisibility	
$n = 12$	73	3	731	7	128	6	
	2047	11	2047	11	128	2	inverse
$n = 14$	5	2	3277	7	256	8	$\mathcal{Q}(2)$
	17	2	2893	7	256	8	$\mathcal{Q}(4)$
	65	2	2773	7	256	8	$\mathcal{Q}(6)$
	13	3	1339	7	256	8	$\mathcal{K}(2)$
	241	5	205	5	256	8	$\mathcal{K}(4)$
	319	7	979	7	256	8	$\mathcal{K}(6)$
	8191	13	8191	13	256	2	inverse
$n = 16$	32767	15	32767	15	512	2	inverse

Divisibility and higher-order differential attacks

Principle. [Knudsen 95]

Find a subspace $V \subset \mathbf{F}_2^n$ such that the reduced cipher G_k satisfies

$$\sum_{v \in V} G_k(x+v) = 0, \ \forall x.$$

Any V with $\dim V > \deg G_k$ satisfies this property.

Problem. Determine the degree of the reduced cipher, i.e., improve

$$\deg G_k \leq (\deg F_k)^{r-1}$$

Theorem. [C. - Videau 02]

If the Walsh coefficients of F are all divisible by 2^ℓ, then

$$\deg(F' \circ F) \leq \deg(F') + n - \ell \ .$$

For instance, if F is AB, then

$$\deg(F' \circ F) \leq \deg(F') + \frac{n-1}{2}.$$

Power permutations over $\mathbf{F}_{2^8}$

s	$w_2(s)$	s^{-1}	$w_2(s^{-1})$	$\delta(S)$	quadratic relations	$\mathcal{L}(S)$	
7	3	37	3	6	24	64	
11	3	29	4	10	24	64	
13	3	59	5	12	16	64	$\mathcal{K}(2)$
19	3	47	5	16	24	48	Niho
23	4	61	5	16	20	64	Niho
31	5	91	5	16	36	32	$\mathcal{K}(4)$
43	4	43	4	30	28	96	
53	4	53	4	16	18	64	Niho
127	7	127	7	4	39	32	inv.

All power permutations over $\mathbf{F}_{2^8}$ have quadratic relations between their inputs and outputs.

For $\mathbf{10 \leq n \leq 16}$, $x \longmapsto x^{53}$ does not have any quadratic relations.

Conclusions

What is provably secure is probably not. (L. Knudsen)

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.

- define relevant criteria related to hardware implementation;
- design efficient algorithms for constructing suboptimal functions;
- find appropriate mathematical tools for studying suboptimal functions.