Improved criteria on the resistance against differential attacks

Anne Canteaut and Joëlle Roué

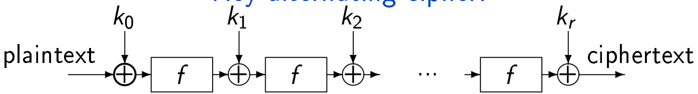
Inria Paris-Rocquencourt, Project team SECRET

March 27, 2014

Overview

Substitution-permutation networks

Key-alternating cipher:



Let m and t be two positive integers.

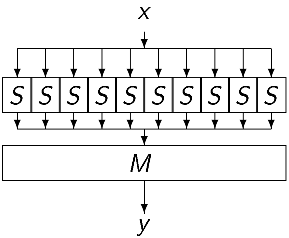
Notation

$\mathrm{SPN}(m, t, S, M)$ defined over $\mathbb{F}_2^{mt}$:

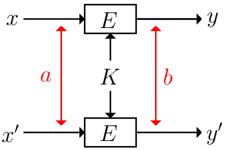
Substitution function:
t copies of a permutation S of $\mathbb{F}_2^m$;

Diffusion function:
a linear permutation M of $\mathbb{F}_2^{mt}$.

$\mathrm{SPN}(m, 10, S, M)$:



Differential cryptanalysis [Biham-Shamir 90]



Attack: Find a, b such that, for almost all keys K,

$$\Pr_x[E_K(x+a)+E_K(x)=b] \gg \frac{1}{2^n-1}.$$

Security criterion

$$\max_{a\neq 0, b\neq 0} \Pr_x[E_K(x+a)+E_K(x)=b] \text{ should be small for all } K.$$

Notation

Let $(E_k)_k$ be an iterated cipher with r rounds.

- The *probability of an r-round differential* (a, b) *for a fixed key k* is

$$\mathrm{DP}_r^{E_k}(a, b) = \mathrm{Pr}_X[E_k(X) + E_k(X + a) = b];$$

- The *expected probability of an r-round differential* (a, b) is

$$\mathrm{EDP}_r^{E}(a, b) = 2^{-\kappa} \sum_{k \in \mathbb{F}_2^{\kappa}} \mathrm{Pr}_X[E_k(X) + E_k(X + a) = b];$$

- The *maximum expected probability for r rounds* is

$$\mathrm{MEDP}_r^{E} = \max_{a \neq 0, b} \mathrm{EDP}_r^{E}(a, b).$$

Differential uniformity

Let S be a function from $\mathbb{F}_2^m$ into $\mathbb{F}_2^m$. For any a and b in $\mathbb{F}_2^m$,

$$\delta(a,b) = |\{x \in \mathbb{F}_2^m, S(x+a) + S(x) = b\}| \ .$$

- The *differential uniformity* of S is

$$\delta(S) = \max_{a \neq 0, b} \delta(a,b);$$

- The *differential spectrum* of S is the multi-set $\{\delta(a,b),\ a \in \mathbb{F}_2^m \setminus \{0\}, b \in \mathbb{F}_2^m\}$.

Sboxes with the same differential spectrum

Definition

Two permutations S and S' of $\mathbb{F}_2^m$ are *affinely equivalent* if there exist two affine permutations of $\mathbb{F}_2^m$ A_1 and A_2 such that $S' = A_2 \circ S \circ A_1$.

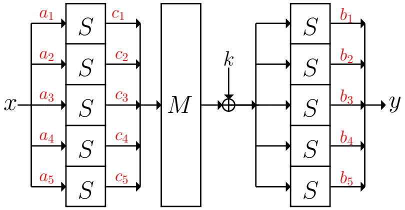
If S and S' are affinely equivalent, they satisfy

$$\delta_{S'}(a,b) = \delta_S(L_1(a), L_2^{-1}(b)),\ \forall a,b \in \mathbb{F}_2^m \ ,$$

where L_1 and L_2 correspond to the linear parts of A_1 and A_2.

Differential probability of a two-round characteristic

Let $a = (a_1, \dots, a_t)$, $b = (b_1, \dots, b_t)$ and $c = (c_1, \dots, c_t)$ be nonzero elements of $(\mathbb{F}_2^m)^t$.



$$\mathrm{ECP}_2(a, M(c), b) \leq \left(\frac{\delta(S)}{2^m}\right)^{wt(c)} \left(\frac{\delta(S)}{2^m}\right)^{wt(M(c))} .$$

Branch number

Let M be a permutation of $(\mathbb{F}_2^m)^t$. We associate to M the code $\mathcal{C}_M$ of length $2t$ and size 2^t over $\mathbb{F}_2^m$ defined by

$$\mathcal{C}_M = \{(c, M(c)),\ c \in (\mathbb{F}_2^m)^t\}\ .$$

The *branch number d* of M is the minimum distance of $\mathcal{C}_M$.

Singleton's bound:

The minimum distance d of the code $\mathcal{C}_M$ satisfies

$$d = \min_{c \neq 0} wt(c, M(c)) \leq t + 1,$$

with equality for MDS codes (Maximum Distance Separable).

AES-128 [Daemen-Rijmen 98], [FIPS PUB 197]

- Key-alternating block cipher;
- Block size: 128 bits;
- Key size: 128 bits;
- 10 rounds;
- Round-permutation: concatenation of 4 SPN(8, 4, S, M);

▶ $S(x) = L \circ \psi^{-1}\left(\psi(x)^{254}\right)$
where ψ is an isomorphism from $\mathbb{F}_2^8$ into the field $\mathbb{F}_{2^8}$ and L is an affine permutation of $\mathbb{F}_2^8$;

▶ M is a linear permutation of $\left(\mathbb{F}_2^8\right)^4$ with branch number 5.

$$\Rightarrow \max_{a,c,b} \mathrm{ECP}_2\left(a, M(c), b\right) \le 2^{-6\times 5}.$$

Characteristics vs. differentials

But we need to estimate the value of

$$\mathrm{EDP}_2(a,b) = \sum_{c \in \mathbb{F}_2^{mt}} \mathrm{ECP}_2(a, M(c), b).$$

Let $(E_k)_k$ be a block cipher of the form $\mathrm{SPN}(m,t,S,M)$ where M is a linear permutation with branch number d. We have:

$$\mathrm{MEDP}_2^E \leq \left(\frac{\delta(S)}{2^m}\right)^{d-1}.$$

FSE 2003 bound (for differentials): [Chun *et al.* 03], [Park *et al.* 03]

Let $(E_k)_k$ be a block cipher of the form $\mathrm{SPN}(m, t, S, M)$ where M is a linear permutation with branch number d. Then,

$$\mathrm{MEDP}_2^E \leq 2^{-md} \max\left(\max_{a \in (\mathbb{F}_2^m)^*} \sum_{\gamma \in (\mathbb{F}_2^m)^*} \delta(a,\gamma)^d, \max_{b \in (\mathbb{F}_2^m)^*} \sum_{\gamma \in (\mathbb{F}_2^m)^*} \delta(\gamma,b)^d \right).$$

Difference table

$$\max\left(\max_{a\in(\mathbb{F}_2^m)^*}\sum_{\gamma\in(\mathbb{F}_2^m)^*}\delta(a,\gamma)^d,\ \max_{b\in(\mathbb{F}_2^m)^*}\sum_{\gamma\in(\mathbb{F}_2^m)^*}\delta(\gamma,b)^d\right)$$

	$\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$	$\begin{pmatrix}0\\0\\1\\1\end{pmatrix}$	$\begin{pmatrix}0\\1\\0\\1\end{pmatrix}$	$\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$	$\begin{pmatrix}0\\0\\1\\0\end{pmatrix}$	$\begin{pmatrix}0\\1\\1\\0\end{pmatrix}$	$\begin{pmatrix}1\\0\\1\\0\end{pmatrix}$	$\begin{pmatrix}1\\1\\0\\1\end{pmatrix}$	$\begin{pmatrix}0\\1\\0\\0\end{pmatrix}$	$\begin{pmatrix}1\\1\\0\\0\end{pmatrix}$	$\begin{pmatrix}0\\1\\1\\1\end{pmatrix}$	$\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$	$\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$	$\begin{pmatrix}1\\0\\1\\1\end{pmatrix}$	$\begin{pmatrix}1\\1\\1\\0\end{pmatrix}$
$(0,0,0,1)$	4	0	0	0	0	2	0	2	0	0	2	2	0	2	2
$(0,0,1,1)$	0	0	0	0	2	0	2	0	0	2	2	0	2	2	4
$(0,1,0,1)$	0	0	0	2	0	2	0	0	2	2	0	2	2	4	0
$(1,1,1,1)$	0	0	2	0	2	0	0	2	2	0	2	2	4	0	0
$(0,0,1,0)$	0	2	0	2	0	0	2	2	0	2	2	4	0	0	0
$(0,1,1,0)$	2	0	2	0	0	2	2	0	2	2	4	0	0	0	0
$(1,0,1,0)$	0	2	0	0	2	2	0	2	2	4	0	0	0	0	2
$(1,1,0,1)$	2	0	0	2	2	0	2	2	4	0	0	0	0	2	0
$(0,1,0,0)$	0	0	2	2	0	2	2	4	0	0	0	0	2	0	2
$(1,1,0,0)$	0	2	2	0	2	2	4	0	0	0	0	2	0	2	0
$(0,1,1,1)$	2	2	0	2	2	4	0	0	0	0	2	0	2	0	0
$(1,0,0,1)$	2	0	2	2	4	0	0	0	0	2	0	2	0	0	2
$(1,0,0,0)$	0	2	2	4	0	0	0	0	2	0	2	0	0	2	2
$(1,0,1,1)$	2	2	4	0	0	0	0	2	0	2	0	0	2	2	0
$(1,1,1,0)$	2	4	0	0	0	0	2	0	2	0	0	2	2	0	2

Results for AES

FSE 2003 bound for AES:

$$\mathrm{MEDP}_2 \leq 79 \times 2^{-34}.$$

Exact value for AES with the naive Sbox (i.e. the inverse function $\psi^{-1}\left(\psi(x)^{254}\right)$):

$$\mathrm{MEDP}_2 = 79 \times 2^{-34}.$$

Exact value for AES [Keliher-Sui 07]:

$$\mathrm{MEDP}_2 = 53 \times 2^{-34}.$$

New bound on MEDP_2

Notation:

A block cipher $(E_k)_k$ is denoted by $\mathrm{SPN}_F(m, t, S, M)$ if it is a Substitution-Permutation Network over $(\mathbb{F}_{2^m})^t$ where:

- S is a permutation of $\mathbb{F}_{2^m}$;
- M is an $\mathbb{F}_{2^m}$-linear permutation of $(\mathbb{F}_{2^m})^t$.

New bound:

Let d be the branch number of M and

$$\mathcal{B}(\mu) := \max_{1 \le u < d} \quad \max_{a,b,\lambda \in \mathbb{F}^*_{2^m}} \sum_{\gamma \in \mathbb{F}^*_{2^m}} \delta(a,\gamma)^u \delta(\gamma\lambda + \mu, b)^{d-u}, \quad \mu \in \mathbb{F}_{2^m}.$$

Then,

$$\mathrm{MEDP}_2 \le 2^{-md} \max_{\mu \in \mathbb{F}_{2^m}} \mathcal{B}(\mu).$$

Difference table

$$\sum_{\gamma \in \mathbb{F}_{2^m}^*} \delta(a, \gamma)^{u} \delta(\gamma, b)^{d-u}.$$

	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
1	4	0	0	0	0	2	0	2	0	0	2	2	0	2	2
α	0	0	0	0	2	0	2	0	0	2	2	0	2	2	4
α^2	0	0	0	2	0	2	0	0	2	2	0	2	2	4	0
α^3	0	0	2	0	2	0	0	2	2	0	2	2	4	0	0
α^4	0	2	0	2	0	0	2	2	0	2	2	4	0	0	0
α^5	2	0	2	0	0	2	2	0	2	2	4	0	0	0	0
α^6	0	2	0	0	2	2	0	2	2	4	0	0	0	0	2
α^7	2	0	0	2	2	0	2	2	4	0	0	0	0	2	0
α^8	0	0	2	2	0	2	2	4	0	0	0	0	2	0	2
α^9	0	2	2	0	2	2	4	0	0	0	0	2	0	2	0
α^{10}	2	2	0	2	2	4	0	0	0	0	2	0	2	0	0
α^{11}	2	0	2	2	4	0	0	0	0	2	0	2	0	0	2
α^{12}	0	2	2	4	0	0	0	0	2	0	2	0	0	2	2
α^{13}	2	2	4	0	0	0	0	2	0	2	0	0	2	2	0
α^{14}	2	4	0	0	0	0	2	0	2	0	0	2	2	0	2

Difference table

$$\sum_{\gamma \in \mathbb{F}_{2^m}^*} \delta(a, \gamma)^u \delta(\gamma, b)^{d-u}.$$

	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
1	4	0	0	0	0	2	0	2	0	0	2	2	0	2	2
α	0	0	0	0	2	0	2	0	0	2	2	0	2	2	4
α^2	0	0	0	2	0	2	0	0	2	2	0	2	2	4	0
α^3	0	0	2	0	2	0	0	2	2	0	2	2	4	0	0
α^4	0	2	0	2	0	0	2	2	0	2	2	4	0	0	0
α^5	2	0	2	0	0	2	2	0	2	2	4	0	0	0	0
α^6	0	2	0	0	2	2	0	2	2	4	0	0	0	0	2
α^7	2	0	0	2	2	0	2	2	4	0	0	0	0	2	0
α^8	0	0	2	2	0	2	2	4	0	0	0	0	2	0	2
α^9	0	2	2	0	2	2	4	0	0	0	0	2	0	2	0
α^{10}	2	2	0	2	2	4	0	0	0	0	2	0	2	0	0
α^{11}	2	0	2	2	4	0	0	0	0	2	0	2	0	0	2
α^{12}	0	2	2	4	0	0	0	0	2	0	2	0	0	2	2
α^{13}	2	2	4	0	0	0	0	2	0	2	0	0	2	2	0
α^{14}	2	4	0	0	0	0	2	0	2	0	0	2	2	0	2

Difference table

$$\mathcal{B}(\mu) = \max_{1 \leq u < d} \max_{a, b, \lambda \in \mathbb{F}_{2^m}^*} \sum_{\gamma \in \mathbb{F}_{2^m}^*} \delta(a, \gamma)^u \delta(\gamma\lambda + \mu, b)^{d-u}.$$

	1	α	$α^2$	$α^3$	$α^4$	$α^5$	$α^6$	$α^7$	$α^8$	$α^9$	$α^{10}$	$α^{11}$	$α^{12}$	$α^{13}$	$α^{14}$
1	4	0	0	0	0	2	0	2	0	0	2	2	0	2	2
α	0	0	0	0	2	0	2	0	0	2	2	0	2	2	4
$α^2$	0	0	0	2	0	2	0	0	2	2	0	2	2	4	0
$α^3$	0	0	2	0	2	0	0	2	2	0	2	2	4	0	0
$α^4$	0	2	0	2	0	0	2	2	0	2	2	4	0	0	0
$α^5$	2	0	2	0	0	2	2	0	2	2	4	0	0	0	0
$α^6$	0	2	0	0	2	2	0	2	2	4	0	0	0	0	2
$α^7$	2	0	0	2	2	0	2	2	4	0	0	0	0	2	0
$α^8$	0	0	2	2	0	2	2	4	0	0	0	0	2	0	2
$α^9$	0	2	2	0	2	2	4	0	0	0	0	2	0	2	0
$α^{10}$	2	2	0	2	2	4	0	0	0	0	2	0	2	0	0
$α^{11}$	2	0	2	2	4	0	0	0	0	2	0	2	0	0	2
$α^{12}$	0	2	2	4	0	0	0	0	2	0	2	0	0	2	2
$α^{13}$	2	2	4	0	0	0	0	2	0	2	0	0	2	2	0
$α^{14}$	2	4	0	0	0	0	2	0	2	0	0	2	2	0	2

New bound on MEDP_2

Let $(E_k)_k$ be a block cipher of the form $\mathrm{SPN}_F(m, t, S, M)$ where M has branch number d.
Let

$$\mathcal{B}(\mu) := \max_{1 \leq u < d} \quad \max_{a,b,\lambda \in \mathbb{F}_{2^m}^*} \sum_{\gamma \in \mathbb{F}_{2^m}^*} \delta(a, \gamma)^u \delta(\gamma\lambda + \mu, b)^{d-u}, \quad \mu \in \mathbb{F}_{2^m}.$$

Then,

$$\mathrm{MEDP}_2 \leq 2^{-md} \max_{\mu \in \mathbb{F}_{2^m}} \mathcal{B}(\mu).$$

Result for AES:

$$\mathrm{MEDP}_2 \leq 55.5 \times 2^{-34}.$$

Optimality of the new bound

Theorem

This bound is smaller or equal to the FSE 2003 bound, with equality if S is an involution.

Theorem

Let S be a permutation of $\mathbb{F}_{2^m}$ and t be any integer with $t \leq 2^{m-1}$. Then, there exists a linear diffusion layer M over $(\mathbb{F}_{2^m})^t$ such that $\mathcal{C}_M$ is MDS and the cipher $\mathrm{SPN}_F(m, t, S, M)$ satisfies

$$\mathrm{MEDP}_2^E \geq 2^{-m(t+1)}\mathcal{B}(0).$$

Examples

$\mathrm{SPN}(4, 4, S_6, M)$, where S_6 can be used in the cipher Prince [Borghoff *et al.*, 12]:

- for any $\mathbb{F}_2$-linear permutation M of $\mathbb{F}_2^{16}$ with $d = 5$, FSE 2003 bound gives:
$$\mathrm{MEDP}_2^E \leq 34 \times 2^{-14};$$
- for any M linear over $\mathbb{F}_{2^4}$ with $d = 5$, where $\mathbb{F}_{2^4}$ is identified with $\mathbb{F}_2^4$ by $\{1, \alpha, \alpha^2, \alpha^3\}$, α a root of $X^4 + X^3 + X^2 + X + 1$:
$$\mathrm{MEDP}_2^E \leq 33 \times 2^{-14};$$
- there exists M' linear over $\mathbb{F}_{2^4}$ with $d = 5$, where $\mathbb{F}_{2^4}$ is identified with $\mathbb{F}_2^4$ by $\{1, \beta, \beta^2, \beta^3\}$, β a root of $X^4 + X + 1$, such that:
$$\mathrm{MEDP}_2^E = 34 \times 2^{-14}.$$