Improved criteria on the resistance against differential attacks

Anne Canteaut and Joëlle Roué

Inria Paris-Rocquencourt, Project team SECRET

March 27, 2014
Overview

1. Introduction to differential cryptanalysis

2. Classical criteria for substitution-permutation networks

3. New criteria on the resistance against differential attacks
1. Introduction to differential cryptanalysis

2. Classical criteria for substitution-permutation networks

3. New criteria on the resistance against differential attacks
Key-alternating cipher:

Let $m$ and $t$ be two positive integers.

**Notation**

$\text{SPN}(m, t, S, M)$ 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 $\mathbb{F}_2^{mt}$.
**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
  \[
  \text{DP}_r^{E_k}(a, b) = \Pr_x[E_k(X) + E_k(X + a) = b];
  \]

- The expected probability of an \(r\)-round differential \((a, b)\) is
  \[
  \text{EDP}_r^{E_k}(a, b) = 2^{-\kappa} \sum_{k \in \mathbb{F}_2^\kappa} \Pr_x[E_k(X) + E_k(X + a) = b];
  \]

- The maximum expected probability for \(r\) rounds is
  \[
  \text{MEDP}_r^E = \max_{a \neq 0, b} \text{EDP}_r^{E_k}(a, b).
  \]
1 Introduction to differential cryptanalysis

2 Classical criteria for substitution-permutation networks

3 New criteria on the resistance against differential attacks
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 $A_2$. 


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

\[
\text{ECP}_2(a, M(c), b) \leq \left( \frac{\delta(S)}{2^m} \right)^{\text{wt}(c)} \left( \frac{\delta(S)}{2^m} \right)^{\text{wt}(M(c))}.
\]
Branch number

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

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

The branch number $d$ of $M$ is the minimum distance of $C_M$.

Singleton’s bound:

The minimum distance $d$ of the code $C_M$ satisfies

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

with equality for MDS codes (Maximum Distance Separable).
Key-alternating block cipher;
- Block size: 128 bits;
- Key size: 128 bits;
- 10 rounds;
- Round-permutation: concatenation of 4 SPN(8, 4, S, M);

\[ S(x) = L \circ \psi^{-1} (\psi(x)^{254}) \]
where \( \psi \) 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 \( (\mathbb{F}_2^8)^4 \) with branch number 5.

\[ \Rightarrow \max_{a,c,b} \text{ECP}_2 (a, M(c), b) \leq 2^{-6 \times 5}. \]
But we need to estimate the value of

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

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

\[ \text{MEDP}_2^E \leq \left( \frac{\delta(S)}{2^m} \right)^{d-1}. \]
FSE 2003 bound (for differentials): [Chun et al. 03], [Park et al. 03]

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

\[
\text{MEDP}_2^E \leq 2^{-md} \max_{a \in (\mathbb{F}_2^m)^*} \left( \max_{\gamma \in (\mathbb{F}_2^m)^*} \sum_{\delta(a, \gamma)^d} , \max_{b \in (\mathbb{F}_2^m)^*} \sum_{\gamma \in (\mathbb{F}_2^m)^*} \delta(\gamma, b)^d \right).
\]
### Difference table

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

<table>
<thead>
<tr>
<th></th>
<th>(0,0,0,0)</th>
<th>(0,0,0,1)</th>
<th>(0,0,1,0)</th>
<th>(0,0,1,1)</th>
<th>(0,1,0,0)</th>
<th>(0,1,0,1)</th>
<th>(0,1,1,0)</th>
<th>(0,1,1,1)</th>
<th>(1,0,0,0)</th>
<th>(1,0,0,1)</th>
<th>(1,0,1,0)</th>
<th>(1,0,1,1)</th>
<th>(1,1,0,0)</th>
<th>(1,1,0,1)</th>
<th>(1,1,1,0)</th>
<th>(1,1,1,1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0,0,0)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(0,0,1)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(1,0,0)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(1,0,1)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(0,1,0)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(0,1,1)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(1,0,0)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(1,0,1)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(0,1,0)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(0,1,1)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(1,0,0)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(1,0,1)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(0,1,0)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(0,1,1)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(1,0,0)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(1,0,1)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(0,1,0)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(0,1,1)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(1,0,0)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(1,0,1)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(0,1,0)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(0,1,1)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(1,0,0)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(1,0,1)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(0,1,0)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(0,1,1)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(1,0,0)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(1,0,1)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(0,1,0)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(0,1,1)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(1,0,0)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>(1,0,1)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

15/22
Results for AES

FSE 2003 bound for AES:

\[ \text{MEDP}_2 \leq 79 \times 2^{-34}. \]

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

\[ \text{MEDP}_2 = 79 \times 2^{-34}. \]

Exact value for AES [Keliher-Sui 07]:

\[ \text{MEDP}_2 = 53 \times 2^{-34}. \]
1. Introduction to differential cryptanalysis

2. Classical criteria for substitution-permutation networks

3. New criteria on the resistance against differential attacks
New bound on MEDP\(_2\)

**Notation:**
A block cipher \((E_k)_k\) is denoted by \(\text{SPN}_F(m, t, S, M)\) 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
\[
\mathcal{B}(\mu) := \max_{1 \leq u < d} \max_{a, b, \lambda \in \mathbb{F}_{2^m}^*} \sum_{\gamma \in \mathbb{F}_{2^m}^*} \delta(a, \gamma)^u \delta(\gamma \lambda + \mu, b)^{d-u}, \quad \mu \in \mathbb{F}_{2^m}.
\]

Then,
\[
\text{MEDP}_2 \leq 2^{-md} \max_{\mu \in \mathbb{F}_{2^m}} \mathcal{B}(\mu).
\]
Introduction to differential cryptanalysis
Classical criteria for substitution-permutation networks
New criteria on the resistance against differential attacks

Difference table

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

<table>
<thead>
<tr>
<th>( \alpha^i )</th>
<th>1</th>
<th>( \alpha )</th>
<th>( \alpha^2 )</th>
<th>( \alpha^3 )</th>
<th>( \alpha^4 )</th>
<th>( \alpha^5 )</th>
<th>( \alpha^6 )</th>
<th>( \alpha^7 )</th>
<th>( \alpha^8 )</th>
<th>( \alpha^9 )</th>
<th>( \alpha^{10} )</th>
<th>( \alpha^{11} )</th>
<th>( \alpha^{12} )</th>
<th>( \alpha^{13} )</th>
<th>( \alpha^{14} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>( \alpha )</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>( \alpha^2 )</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( \alpha^3 )</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( \alpha^4 )</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( \alpha^5 )</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( \alpha^6 )</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>( \alpha^7 )</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>( \alpha^8 )</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>( \alpha^9 )</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>( \alpha^{10} )</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>( \alpha^{11} )</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>( \alpha^{12} )</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>( \alpha^{13} )</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>( \alpha^{14} )</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
Introduction to differential cryptanalysis
Classical criteria for substitution-permutation networks
New criteria on the resistance against differential attacks

Difference table

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

<table>
<thead>
<tr>
<th></th>
<th>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</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4 0 0</td>
</tr>
<tr>
<td>α</td>
<td>0 0 0</td>
</tr>
<tr>
<td>α^2</td>
<td>0 0 0</td>
</tr>
<tr>
<td>α^3</td>
<td>0 0 2</td>
</tr>
<tr>
<td>α^4</td>
<td>0 2 0</td>
</tr>
<tr>
<td>α^5</td>
<td>2 0 2</td>
</tr>
<tr>
<td>α^6</td>
<td>0 2 0</td>
</tr>
<tr>
<td>α^7</td>
<td>2 0 0</td>
</tr>
<tr>
<td>α^8</td>
<td>0 2 0</td>
</tr>
<tr>
<td>α^9</td>
<td>0 2 2</td>
</tr>
<tr>
<td>α^10</td>
<td>2 2 0</td>
</tr>
<tr>
<td>α^11</td>
<td>2 0 2</td>
</tr>
<tr>
<td>α^12</td>
<td>0 2 2</td>
</tr>
<tr>
<td>α^13</td>
<td>2 2 4</td>
</tr>
<tr>
<td>α^14</td>
<td>2 4 0</td>
</tr>
</tbody>
</table>
Introduction to differential cryptanalysis
Classical criteria for substitution-permutation networks
New criteria on the resistance against differential attacks

**Difference table**

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

<table>
<thead>
<tr>
<th></th>
<th>$1$</th>
<th>$\alpha$</th>
<th>$\alpha^2$</th>
<th>$\alpha^3$</th>
<th>$\alpha^4$</th>
<th>$\alpha^5$</th>
<th>$\alpha^6$</th>
<th>$\alpha^7$</th>
<th>$\alpha^8$</th>
<th>$\alpha^9$</th>
<th>$\alpha^{10}$</th>
<th>$\alpha^{11}$</th>
<th>$\alpha^{12}$</th>
<th>$\alpha^{13}$</th>
<th>$\alpha^{14}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1$</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>$\alpha^2$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>$\alpha^3$</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\alpha^4$</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\alpha^5$</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\alpha^6$</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>$\alpha^7$</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>$\alpha^8$</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>$\alpha^9$</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>$\alpha^{10}$</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\alpha^{11}$</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>$\alpha^{12}$</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$\alpha^{13}$</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>$\alpha^{14}$</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>
New bound on \( \text{MEDP}_2 \)

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

Let

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

Then,

\[
\text{MEDP}_2 \leq 2^{-md} \max_{\mu \in \mathbb{F}_{2^m}} B(\mu).
\]

Result for AES:

\[
\text{MEDP}_2 \leq 55.5 \times 2^{-34}.
\]
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 \( C_M \) is MDS and the cipher \( \text{SPN}_F(m, t, S, M) \) satisfies

\[
\text{MEDP}_2^E \geq 2^{-m(t+1)}B(0).
\]
Examples

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

- for any \(F_2\)-linear permutation \(M\) of \(F_{16}^2\) with \(d = 5\), FSE 2003 bound gives:
  \[
  \text{MEDP}_{E}^F \leq 34 \times 2^{-14};
  \]

- for any \(M\) linear over \(F_{24}\) with \(d = 5\), where \(F_{24}\) is identified with \(F_4\) by \(\{1, \alpha, \alpha^2, \alpha^3\}\), \(\alpha\) a root of \(X^4 + X^3 + X^2 + X + 1\):
  \[
  \text{MEDP}_{E}^F \leq 33 \times 2^{-14};
  \]

- there exists \(M'\) linear over \(F_{24}\) with \(d = 5\), where \(F_{24}\) is identified with \(F_4\) by \(\{1, \beta, \beta^2, \beta^3\}\), \(\beta\) a root of \(X^4 + X + 1\), such that:
  \[
  \text{MEDP}_{E}^F = 34 \times 2^{-14}.
  \]