APN functions and S-boxes

Lilya Budaghyan

Department of Informatics
University of Bergen
Norway

Norsk Kryptoseminar 2011
Bergen, Norway
Vectorial Boolean functions: \( F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m \) for \( n \) and \( m \) positive integer.

S-boxes are vectorial Boolean functions used in block ciphers to provide confusion.

Attacks on block ciphers and resp. properties of S-boxes:

- Linear attack – Nonlinearity
- Differential attack – Differential uniformity
- Algebraic attack – Existence of multivariate equations
- Higher order differential attack – Algebraic degree
- Interpolation attack – Univariate polynomial degree
For any positive integer $n$ the unique univariate representation of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$:

$$F(x) = \sum_{i=0}^{2^n-1} c_i x^i, \quad c_i \in \mathbb{F}_{2^n}.$$ 

Binary expansion of an integer $k$, $0 \leq k < 2^n$: $k = \sum_{s=0}^{n-1} 2^s k_s$, where $k_s \in \{0, 1\}$.  

2-weight of $k$: $w_2(k) = \sum_{s=0}^{n-1} k_s$.  

Algebraic degree of $F$:

$$d^\circ(F) = \max_{0 \leq i \leq 2^n - 1} w_2(i) \text{ subject to } c_i \neq 0.$$ 

S-boxes should have high univariate polynomial degree and high $d^\circ(F)$. 

Lilya Budaghyan  
APN functions and S-boxes
Nonlinearity

Trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$: $\text{tr}_n(x) = \sum_{i=0}^{n-1} x^{2^i}$.

Walsh coefficients of $F$:

$$\lambda_F(u, v) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{tr}_n(vF(x) + ux)}, \quad u, v \in \mathbb{F}_{2^n}, v \neq 0.$$

Walsh spectrum of $F$: $\Lambda_F = \{ \lambda_F(u, v) : u \in \mathbb{F}_{2^n}, v \in \mathbb{F}_{2^n}^* \}$.

Extended Walsh spectrum of $F$:

$$\Lambda'_F = \{|\lambda_F(u, v)| : u \in \mathbb{F}_{2^n}, v \in \mathbb{F}_{2^n}^* \}.$$

Nonlinearity of $F$: $N(F) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in \Lambda'_F} \lambda$.

The higher is nonlinearity the better is the resistance to linear attack.

$F$ is almost bent (AB) if $\Lambda_F = \{0, \pm 2^{\frac{n+1}{2}} \}$. 
Differential uniformity

$F$ is differentially $\delta$-uniform if

$$F(x + a) - F(x) = b, \quad \forall a \in \mathbb{F}_2^{*n}, \quad \forall b \in \mathbb{F}_{2^n},$$

has at most $\delta$ solutions.

The smaller is $\delta$ the better is the resistance to differential attack.

- $F$ is almost perfect nonlinear (APN) if $\delta = 2$.
- $F$ is AB $\implies$ $F$ is APN.
- $n$ is odd and $F$ is quadratic APN $\implies$ $F$ is AB.
- Algebraic degree of AB function is at most $(n + 1)/2$ and it exists for $n$ odd only.
The graph of a function $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ is the set

$$G_F = \{ (x, F(x)) : x \in \mathbb{F}_{2^n} \} \subset \mathbb{F}_{2^n}^2.$$ 

$F$ and $F'$ are CCZ-equivalent if

$$\mathcal{L}(G_F) = G_{F'},$$

for some affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n}^2$.

CCZ-equivalence preserves:

- differential uniformity
- nonlinearity
- APNness, ABness
- resistance to algebraic attack

Lilya Budaghyan
APN functions and S-boxes
**EA-equivalence and Inverses of Permutations**

*F* and *F′* are *extended affine equivalent* (EA-equivalent) if

\[ F' = A_1 \circ F \circ A_2 + A. \]

for some affine permutations *A*_1 and *A*_2 and some affine function *A*.

EA-equivalence and inverse transformation are particular cases of CCZ-equivalence.

**EA-equivalence preserves:**
- differential uniformity
- nonlinearity
- resistance to algebraic attack
- algebraic degree
Known APN power functions $x^d$ on $\mathbb{F}_{2^n}$ (up to equiv.)

<table>
<thead>
<tr>
<th>Functions</th>
<th>Exponents $d$</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gold</td>
<td>$2^i + 1$</td>
<td>$\gcd(i, n) = 1, 1 \leq i &lt; n/2$</td>
</tr>
<tr>
<td>Kasami</td>
<td>$2^{2i} - 2^i + 1$</td>
<td>$\gcd(i, n) = 1, 2 \leq i &lt; n/2$</td>
</tr>
<tr>
<td>Welch</td>
<td>$2^m + 3$</td>
<td>$n = 2m + 1$</td>
</tr>
<tr>
<td>Niho</td>
<td>$2^m + 2^{\frac{m}{2}} - 1, \ m \ even$</td>
<td>$n = 2m + 1$</td>
</tr>
<tr>
<td></td>
<td>$2^m + 2^{\frac{3m+1}{2}} - 1, \ m \ odd$</td>
<td></td>
</tr>
<tr>
<td>Inverse</td>
<td>$2^{2m} - 1$</td>
<td>$n = 2m + 1$</td>
</tr>
<tr>
<td>Dobbertin</td>
<td>$2^{4m} + 2^{3m} + 2^{2m} + 2^m - 1$</td>
<td>$n = 5m$</td>
</tr>
</tbody>
</table>

Gold, Kasami functions (with $n$ odd) and Welch, Niho functions are also AB. For $n$ even inverse functions are differentially 4-uniform, and it is used as S-box in AES with $n = 8$. 

Lilya Budaghyan  APN functions and S-boxes
The first families of APN polynomials EA-inequivalent to power functions

\[ x^{2^i+1} + (x^{2^i} + x + \text{tr}_n(1) + 1)\text{tr}_n(x^{2^i+1} + x\text{tr}_n(1)) \]

with \( \text{gcd}(i, n) = 1, \ n \geq 4 \). It is AB for \( n \) odd.

It is by construction CCZ-equivalent to Gold functions (2005).

This proves that CCZ-equivalence is more general than EA-equivalence with taking the inverse of permutations.

For \( n = 5 \) it is AB function EA-inequivalent to any permutation which disproved the conjecture of 1998.
Problems Related to CCZ-equivalence

Do there exist AB functions CCZ-inequivalent to permutations?

Are there APN polyn. CCZ-eq. to other known APN power functions but EA-ineq. to them?

Is there more general equivalence preserving nonlinearity and dif. uniformity?

Are the known power APN functions CCZ-inequivalent to each other? (solved partly)

Do there exist APN polynomials CCZ-inequivalent to power functions? (solved)
Known APN polynomials CCZ-inequivalent to power functions

(i) \(x^{2s+1} + cx^{2ik+2tk+s}, \ n = pk, \ p = 3, 4;\)

(ii) \(x^3 + c^{-1} \text{tr}_n(c^3 x^9);\)

(iii) \(x^3 + c^{-1} \text{tr}_n^3(c^3 x^9 + c^6 x^{18})^i, \ n = 3k, \ i = 1, 2;\)

(iv) \(x(x^{2i} + x^{2n/2} + cx^{2i+n/2}) + x^{2i}(c^{2n/2} x^{2n/2} + bx^{2i+n/2}) + x^{2i+n/2+2n/2}, \ n \text{ even};\)

(v) \(bx^{2s+1} + b^{2n/2} x^{(2s+1)2n/2} + cx^{2n/2+1} + \sum_{i=1}^{n/2-1} r_i x^{2i(2n/2+1)}, \ n \text{ even}, \ n/2 \text{ odd};\)

(vi) \(c^{2k} x^{2-k+2k+s} + cx^{2s+1} + bx^{2-k+1} + dc^{2k+1} x^{2k+s+2s}, \ n = 3k.\)

Functions (i)-(vi) are quadratic over \(\mathbb{F}_{2^n}\) and they are AB when \(n\) is odd. All have Gold like Walsh spectra.
Only one known example of APN polynomial CCZ-ineq. to quadratics and to power functions (\(n=6\)).

Many unclassified quadratic APN polynomials for \(6 \leq n \leq 12\).

Only one known example of quadratic APN polynomial with Walsh spectrum different from gold (\(n = 6\)).

CCZ-classification is finished for:
- APN functions with \(n \leq 5\) (there are only power functions).
- quadratic APN functions for \(n = 6\) (there are 13)!
Existence of APN Permutations for $n$ Even

Big APN problem (solved in 2009):
Do APN permutations exist for $n$ even?

- no for quadratics,
- no for $F \in \mathbb{F}_{2^4}[x]$ if $n/2$ is even,
- no for $F \in \mathbb{F}_{2^{n/2}}[x]$,
- there is an APN permutation for $n = 6$ CCZ-eq. to quadratics!

Still big APN problem:
Do APN permutations exist for $n \geq 8$ even?
Let $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^m}$.

- $F$ is bent if $\Lambda_F = \{ \pm 2^n \}$.
- $F$ is perfect nonlinear (PN) if $\delta = 2^{n-m}$.
  \[ F \text{ is PN} \iff F \text{ is bent.} \]
- PN functions exist only for $n$ even and $m \leq n/2$.

For Boolean functions (case $m = 1$) and for all bent functions CCZ-equivalence coincides with EA-equivalence.
Characterization of APN and AB functions

Let $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ and $a, b \in \mathbb{F}_{2^n}$, define $\gamma_F : \mathbb{F}_{2^n}^2 \rightarrow \mathbb{F}_2$ as

$$
\gamma_F(a, b) = \begin{cases} 
1 & \text{if } a \neq 0 \text{ and } F(x + a) + F(x) = b \text{ has solutions,} \\
0 & \text{otherwise.}
\end{cases}
$$

Then (Carlet, Charpin, Zinoviev, 1998)

- $F$ is APN if and only if $\gamma_F$ has weight $2^{2n-1} - 2^{n-1}$;
- $F$ is AB if and only if $\gamma_F$ is bent;
- if $F$ is APN then the function $b \rightarrow \gamma_F(a, b)$ is balanced for any $a \neq 0$;
- if $F$ is an APN permutation then the function $a \rightarrow \gamma_F(a, b)$ is balanced for any $b \neq 0$. 
If $F$ and $F'$ are CCZ-equivalent then $\gamma_{F'} = \gamma_F \circ \mathcal{L}$ for some affine permutation $\mathcal{L}$ of $\mathbb{F}_2^{2n}$.

If $F$ and $F'$ are EA-equivalent then
$$
\gamma_{F'}(a, b) = \gamma_F(A_2(a) + A_2(0), A_1^{-1}(A(a) + b + A(0) + A_1(0)))
$$
for some affine permutations $A_1$, $A_2$ and an affine function $A$.

All affine invariants for $\gamma_F$ are CCZ-invariants for $F$.

$\gamma_F$ is determined for all known families of APN functions except (vi) and Dobbertin functions B., Carlet, Helleseth, ITW’2011.

For nonquadratic AB cases found $\gamma_F$ potentially provide new bent functions.