Generalized Boolean Bent Functions

Laurent Poinsot and Sami Harari

Laboratoire S.I.S.
Institut des Sciences de l'Ingénieur
Université Sud Toulon-Var
France

INDOCRYPT 2004
5th International Conference on Cryptology in India
December 20-22, 2004
Chennai (Madras), India

Outline of this talk

- Back to Basics
- On Fixed-Point Free Involutions of $\mathbb{F}_2^m$
- Generalized Perfect NonLinearity
- Fourier Characterization
- Construction of a Generalized Boolean Bent Function
- Conclusion

Back to Basics (I/IV)

Dual Group and Characters

Let G be a finite Abelian group of exponent E.
The *dual group* of G is

$$\widehat{G} = Hom(G, U_E)$$

where U_E is the multiplicative group of E^{th} roots of the unity in $\mathbb{C}$.

Property

$\widehat{G}$ is isomorphic to G .

Notation

χ_G^α is the image of $\alpha \in G$ by such an isomorphism.

Example

If $G = \mathbb{F}_2^m$, we have $\chi_G^\alpha(x) = (-1)^{\alpha . x}$.

Back to Basics (II/IV)

Fourier Transform

Let $f : G \longrightarrow \mathbb{C}$.

The *Fourier transform* of f defined by

$$\widehat{f}(\alpha) = \sum_{x \in G} f(x) \chi_G^{\alpha}(x) \ .$$

Parseval Equation

$$\boxed{\frac{1}{|G|} \sum_{\alpha \in G} |\widehat{f}(\alpha)|^2 = \sum_{x \in G} |f(x)|^2 \ .}$$

Back to Basics (III/IV)

Perfect NonLinearity

Let $f : G_1 \longrightarrow G_2$.

- The *derivative* of f in direction $\alpha \in G_1$ is

$$d_\alpha f : x \in G_1 \mapsto f(x+\alpha) - f(x) \ .$$

- f is *balanced* if for each $\beta \in G_2$

$$|\{x \in G_1 | f(x) = \beta\}| = \frac{|G_1|}{|G_2|} \ .$$

- f is perfect nonlinear (*pnl*) if for each nonzero $\alpha \in G_1$

$d_\alpha f$ is balanced.

Back to Basics (IV/IV)

Fourier Characterization

Theorem

$f : G_1 \longrightarrow G_2$ is *pnl* if and only if for each nonezero $\beta \in G_2$ the Fourier transform of the complex-valued function $f^{(\beta)} = \chi_{G_2}^{\beta} \circ f$ has constant magnitude $\sqrt{|G_1|}$.

On Fixed-Point Free Involutions of $\mathbb{F}_2^m$ (I/III)

Definitions and First Results

Let $\sigma \in S(\mathbb{F}_2^m)$.
σ is a fixed-point free involution (*fpfi*) if

$$\text{for all } x \in \mathbb{F}_2^m,\ \sigma x \neq x \text{ and } \sigma^2 x = x.$$

The set of all *fpfi* is a conjugacy class of $S(\mathbb{F}_2^m)$. Its cardinality is then

$$\frac{2^m!}{2^{m-1}!2^{2^{m-1}}}\ .$$

Example
Let α be a nonzero element of $\mathbb{F}_2^m$. The translation $\sigma_\alpha : x \in \mathbb{F}_2^m \mapsto x \oplus \alpha \in \mathbb{F}_2^m$ is an *fpfi*.

On Fixed-Point Free Involutions of $\mathbb{F}_2^m$ (II/III)

Maximal Group of fpfi

Let $G \subset S(\mathbb{F}_2^m)$ be a subgroup such that all nonidentity element of G is a *fpfi*. G is called a *maximal group of involutions* (*mgi*) of $\mathbb{F}_2^m$ if $|G| = 2^m$.

Such a *mgi* is Abelian.

Examples

- The group of all translations $T(\mathbb{F}_2^m) = \{\sigma_\alpha\}_{\alpha \in \mathbb{F}_2^m}$ is a *mgi*.
- Let $\pi \in S(\mathbb{F}_2^m)$. $G_\pi = \pi T(\mathbb{F}_2^m)\pi^{-1}$ is a *mgi*.

On Fixed-Point Free Involutions of $\mathbb{F}_2^m$ (III/III)

Maximal Group of fpfi

Property

A *mgi* G acts regularly on $\mathbb{F}_2^m$.

In other terms, for each $x \in \mathbb{F}_2^m$, the *orbital function*

$$\phi_x : \sigma \in G \longrightarrow \sigma x \in \mathbb{F}_2^m$$

is one-to-one.

Generalized Perfect NonLinearity

Let $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$ and G be a *mgi* of $\mathbb{F}_2^m$.
The *derivative* of f in direction $\sigma \in G$ is the function

$$D_\sigma f : x \in \mathbb{F}_2^m \mapsto f(\sigma x) \oplus f(x) \in \mathbb{F}_2^n \ .$$

Definition

f is said G-*pnl* if for each nonidentity $\sigma \in G$

$$D_\sigma f \text{ is balanced.}$$

Proposition

f is $T(\mathbb{F}_2^m)$-*pnl* if and only if f is *pnl* in the traditional way.

Fourier Characterization (I/IV)

G-**"Convolutional product"** of two real-valued functions f and g defined on $\mathbb{F}_2^m$ (where G is a *mgi* of $\mathbb{F}_2^m$)

$$f \boxtimes g(\sigma) = \sum_{x \in \mathbb{F}_2^m} f(x) g(\sigma x) \ .$$

Fourier Characterization (II/IV)

The Fourier Transform of the G-convolutional product is

$$\boxed{f \widehat{\boxtimes} g(\sigma) = \frac{1}{2^m} \sum_{x \in \mathbb{F}_2^m} \widehat{f_x}(\sigma) \widehat{g_x}(\sigma) \ .}$$

where $f_x : G \longrightarrow \mathbb{R}$ defined by $f_x(\sigma) = f(\sigma x)$.

Fourier Characterization (III/IV)

New Theorem
Let G be a *mgi* of $\mathbb{F}_2^m$ and $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$.

f is G-*pnl* if and only if for each $\sigma \in G$ and for each nonzero $\beta \in \mathbb{F}_2^n$

$$\sum_{x \in \mathbb{F}_2^m} (\widehat{f_x^{(\beta)}}(\sigma))^2 = 2^{2m} \ .$$

Fourier Characterization (IV/IV)

New Theorem

Let G be a *mgi* of $\mathbb{F}_2^m$ and $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$.

f is G-*pnl* if and only if for each $x \in \mathbb{F}_2^m$, $f_x : \sigma \in G \mapsto f(\sigma x) \in \mathbb{F}_2^n$ is *pnl* in traditional way which is equivalent to the fact that for each $x \in \mathbb{F}_2^m$, for each nonzero $\beta \in \mathbb{F}_2^n$ and for all $\sigma \in G$

$$\boxed{|\widehat{f_x^{(\beta)}}(\sigma)| = 2^{\frac{m}{2}}\ .}$$

Construction of a Generalized Boolean Bent Function (I/II)

Let $\pi \in S(\mathbb{F}_2^m)$ and $G_\pi = \pi T(\mathbb{F}_2^m)\pi^{-1}$. Let $g : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$ be a (classical) perfect nonlinear function.

We define

$$f : x \in \mathbb{F}_2^m \mapsto f(x) = g(\pi^{-1}x) \in \mathbb{F}_2^n \ .$$

Proposition
The function f previously defined is G_π-perfect nonlinear.

Construction of a Generalized Boolean Bent Function (II/II)

Proof

Let σ be a nonidentity element of G_π and $\beta \in \mathbb{F}_2^n$.

$$
\begin{aligned}
|\{x \in \mathbb{F}_2^m | f(\sigma x) \oplus f(x) = \beta\}| &= |\{x \in \mathbb{F}_2^m | f(\pi \sigma_\alpha \pi^{-1} x) \oplus f(x) = \beta\}| \\
&= |\{y \in \mathbb{F}_2^m | f(\pi \sigma_\alpha y) \oplus f(\pi y) = \beta\}| \\
&\quad (\textit{by the change of variable } y = \pi^{-1} x) \\
&= |\{y \in \mathbb{F}_2^m | g(\sigma_\alpha y) \oplus g(y) = \beta\}| \\
&= |\{y \in \mathbb{F}_2^m | g(\alpha \oplus y) \oplus g(y) = \beta\}| \\
&= 2^{m-n} (\textit{by perfect nonlinearity of } g).
\end{aligned}
$$

Conclusion (I/II)

Summary

- Generalization of the notion of Perfect Nonlinearity in the boolean case by considering groups of involutions rather than simple translations.

- Characterization with the Fourier transform that leads to generalized boolean bent functions.

- Characterization by the distance to a set of “affine” functions.

- Construction of a G-Perfect NonLinear function in the case where G is a conjugate group of $T(\mathbb{F}_2^m)$.

Conclusion (II/II)

Further Works

- Let G be a *mgi* of $\mathbb{F}_2^m$. Is G be conjugate to $T(\mathbb{F}_2^m)$?

- If it is not the case we should construct a G-perfect nonlinear function for G non conjugate to $T(\mathbb{F}_2^m)$.

- Study of links with hyper-bent functions.
  Indeed $f : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_2$ is hyper-bent if for all d co-prime with $2^m - 1$, $x \mapsto f(x^d)$ is bent.