A Method of Constructing Highly Nonlinear Balanced Boolean Functions

Baha Güçlü DÜNDAR, Faruk GÖLOĞLU, Ali DOĞANAKSOY and Zülfükar SAYGI

Cryptography Program

Graduate School of Applied Mathematics

Middle East Technical University

Outline

1. Preliminaries

2. Constructing highly nonlinear balanced Boolean functions

3. Cryptographic properties of the construction

1. Preliminaries

1.1. Boolean Functions

– $GF(2)$: finite field with binary values.

– $GF(2)^n$: vector space of binary n-tuples over $GF(2)$ with respect to addition $\oplus$ and scalar multiplication.

– A *Boolean function* is an $GF(2)$ valued function defined on $GF(2)^n$.

– *Weight of the function* f:

$$w(f) = \sum_{\alpha \in GF(2)^n} f(\alpha).$$

Properties:

– f is called *balanced* if $w(f) = 2^{n-1}$.

– Support of f:

$$Supp(f) = \{x \in GF(2)^n | f(x) = 1\}.$$

– Algebraic Normal Form of a Boolean function:

$$f(x) = \bigoplus_{u \in GF(2)^n} a_u x^u = \bigoplus_{u \in GF(2)^n} a_u (\prod x^{u_1} \cdots x^{u_n})$$

– *Affine functions* are of the form:

$$f(x_1, \ldots, x_n) = a_0 \oplus a_1 x_1 \oplus \cdots \oplus a_n x_n,$$

for all a_i in $GF(2)$ and $i = 0, \ldots, n$.

Properties Cnt'd:

- Any nonconstant affine function is balanced.

- An affine Boolean function is called a *linear function* if $a_0 = 0$.

- For each Boolean function f on $GF(2)^n$, the function $W_f : GF(2)^n \to \mathbb{R}$ defined by:

$$W_f(a) = \sum_{x \in GF(2)^n} (-1)^{f(x)+a \cdot x}$$

  is called the *Walsh transform of f*, for $a \in GF(2)^n$.

- Nonlinearity N_f of f in terms of Walsh transform:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{a \in GF(2)^n} \{|W_f(a)|\}$$

1.2. Bent Functions

- *Bent functions* is a family of Boolean functions with maximal distance to the set of affine functions.

- They exist only for even n.

- A Boolean function f is called bent if $W_f(a) = \pm 2^{\frac{n}{2}}$, ($i.e.$, $N_f = 2^{n-1} - 2^{\frac{n}{2}-1}$)

- Weight of bent functions can take two values: $w(f) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$.

1.3. Normal Boolean Functions

Definition 1. *A Boolean function f is called* normal, *if restriction of f to an $\lceil n/2 \rceil$-dimensional affine subspace is constant.*

Fact 1 *(Dobbertin:[3]) Let f be a normal bent function, which is constant on an affine subspace $V \subseteq GF(2)^n$ with $dim(V) = \frac{n}{2}$. Then f is balanced on each proper coset of V.*

Definition 2. *A Boolean function f is called k-*normal, *if there exists a k-dimensional flat on which f is constant.*

Properties:

– For $n \leq 7$, all Boolean functions are $\lfloor n/2 \rfloor$-normal (Dubuc:[4]).

– Canteaut et. al. verified that there exist non-normal bent functions defined on $GF(2)^{10}$ (Canteaut:[1]).

– Direct sum of normal and non-normal bent function produces non-normal bent function (Carlet et. al.:[2]).

1.4. Correlation Immunity of a Boolean Function

– Boolean functions are said to be *correlation immune of order* m, if distribution of their truth table is unaltered while fixing any m inputs (Siegenthaler:[5]).

– (Siegenthaler's Inequality,[5]) Let f be a Boolean function defined on $GF(2)^n$ with algebraic degree d, then $d \leq n - m$ with $m < n$.

– Balanced Boolean functions with correlation immunity m is called *m-resilient functions*.

– (Characterization of correlation immune functions, Xiao-Massey: [6]) A Boolean function f defined on $GF(2)^n$ is correlation immune of order m if $W_f(\alpha) = 0$ for all $\alpha \in GF(2)^n$ such that $1 \leq w(\alpha) \leq m$.

1.5. Autocorrelation Function of a Boolean Function

– *The autocorrelation function* of f with the shift α:

$$\Delta_f(\alpha) = \sum_x (-1)^{f(x)+f(x+\alpha)}.$$

– *Absolute indicator of* f [7]:

$$\Delta(f) = max_{\alpha \in GF(2)^n} \Delta_f(\alpha).$$

Proposition 1. *Let* f *be any Boolean function with algebraic degree* d *on* $GF(2)^n$*. Then,* $\Delta_f(s)$ *is a multiple of* $2^{\lceil \frac{n}{d} \rceil + 1}$ *if* $d \neq 1$*.*

Remark 1. We have the following:

– Boolean functions having algebraic degree less than n, have autocorrelation function a multiple of 8. In particular, autocorrelation function of a balanced Boolean functions is a multiple of 8.

– Absolute indicator of any quadratic Boolean function with an even number of variables is divisible by $2^{\frac{n}{2}+1}$.(1)

2. Constructing Highly Nonlinear Balanced Boolean Functions

– In most cryptosystems, desired properties of Boolean functions are balance, high nonlinearity, correlation immunity, and good propagation characteristics.

– Upper bound on nonlinearity of balanced Boolean functions is theoretically $2^{n-1} - 2^{\frac{n}{2}-1} - 2$, but for $n \geq 8$, finding balanced Boolean functions defined on $GF(2)^n$ achieving that nonlinearity value is a challenge.

– Some constructions of highly nonlinear balanced Boolean functions exist (having nonlinearity strictly smaller than $2^{n-1} - 2^{\frac{n}{2}-1} - 2$) in literature.

Dobbertin's Conjecture:

H. Dobbertin conjectured in [3] that the nonlinearity of balanced Boolean function defined on $GF(2)^n$ cannot exceed $2^{n-1} - 2^{\frac{n}{2}} + N_\theta$ where N_θ denote the maximum achievable nonlinearity of a balanced Boolean function θ defined on $GF(2)^{\frac{n}{2}}$.

Dobbertin's Construction:

Proposition 2. *([3]) Let* $U = GF(2)^{\frac{n}{2}}$ *and* $V = U^2$*. Let* f *be a normal bent function on* V*. Without loss of generality* $f(x, \mathbf{0}) = 0$ *for all* $x \in U$*. Furthermore let a balanced function* $h : U \to GF(2)$ *be given. Set for* $x, y \in U$

$$g(x, y) = \begin{cases} f(x, y), \textit{if } y \neq \mathbf{0} \\ h(x), \quad \textit{otherwise.} \end{cases}$$

Then g *is balanced and we have*

$$W_g(a, b) = \begin{cases} W_f(a, b) + W_h(a), \textit{if } a \neq \mathbf{0} \\ 0, \qquad\qquad\qquad\qquad \textit{otherwise.} \end{cases}$$

It follows that

$$N_g = 2^{n-1} - 2^{n/2} + N_h.$$

2.1. Our Modification

Theorem 2. *Let $U = GF(2)^{\frac{n}{2}}$ and $V = U^2$. Let f be a normal bent function on V. That is without loss of generality $f(x, \mathbf{0}) = 0$ for all $x \in U$. Furthermore let $h : U \to GF(2)$ with $w(h) = 2^{n/2-1} - c$ and $p : V \to GF(2)$ with $w(p) = c$, $p(x, \mathbf{0}) = 0$ for all $x \in U$ and $Supp(p) \cap Supp(f) = \emptyset$ be given. Set for $x, y \in U$*

$$g(x, y) = \begin{cases} f(x, y) + p(x, y), & \text{if } y \neq \mathbf{0} \\ h(x), & \text{otherwise.} \end{cases}$$

Then g is balanced and we have

$$W_g(a, b) = \begin{cases} W_f(a, b) + W_h(a) + \delta(a, b), & \text{if } a \neq \mathbf{0} \\ 2c + \delta(\mathbf{0}, b), & \text{otherwise} \end{cases}$$

where the real-valued function $\delta(a, b) = 2 \sum_{(x,y) \in Supp(p)} (-1)^{a \cdot x + b \cdot y + 1}$.

Remarks:

- If one chooses $w(p) = c = 0$, that is h to be balanced, then our construction coincides with the Dobbertin's construction [3].

- If we alter bits of f merely on the restriction to proper cosets of A, in other words $h(x) = 0$, Walsh transform of g can be expressed as:

$$W_g(a, b) = W_f(a, b) + \delta(a, b).$$

Examples:

For $n = 8$, we have chosen a normal bent function f on $GF(2)^8$ with $f(x, 0) = 0$ for all $x \in GF(2)^4$. Then we have constructed balanced Boolean functions g as below:

1. Let h be any bent function on $GF(2)^4$ with $w(h) = 6$ and p be any function satisfying the conditions in our construction,
2. Let h be a function on $GF(2)^4$ with $w(h) = 7$ and $N_h = 5$ and p be any function satisfying the conditions in our construction;

with nonlinearity 116.

3. Cryptographic Properties of the Construction

$\mathcal{B}_n$: the set of balanced Boolean functions on $GF(2)^n$ modified from normal bent functions by changing $2^{\frac{n}{2}-1}$ bits.

Proposition 3. *All functions in $\mathcal{B}_n$ are 0-resilient.*

Proposition 4. *Absolute indicator of functions in $\mathcal{B}_n$ is at most $2^{\frac{n}{2}+1}$.(1)*

Corollary 1. *By combining Remark 1 and Proposition 4, we have the fact that autocorrelation function of quadratic functions in $\mathcal{B}_n$ takes three values $0, \pm 2^{\frac{n}{2}+1}$ and so their absolute indicator is $2^{\frac{n}{2}+1}$.*

Hans Dobbertin (1952-2006)

We extend our condolences to all who appreciate his works.

Questions and Comments

References

1. Canteaut, A., Daum, M., Leander, G., and Dobbertin, H. Normal and nonnormal bent functions. In *Proceedings of the 2003 International Workshop on Coding and Cryptography (WCC 2003)* (2003), pp. 91–100.
2. Carlet, C., Dobbertin, H., and Leander, G. Normal extension of bent functions. *IEEE Transactions on Information Theory 50*, 11 (2004), 2880–2885.
3. Dobbertin, H. Construction of bent functions and balanced Boolean functions with high nonlinearity. In *Fast Software Encryption (Workshop on Cryptographic Algorithms, Leuven 1994* (1995), no. 1008 in Lecture Notes in Computer Science, Springer-Verlag, pp. 61–74.
4. Dubuc, S. *Etude des propriétés de dégénérescence et de normalité des fonctions Booleénnes et construction de fonctions q-aires parfaitement non-linéaires.* PhD thesis, Université de Caen, 2001.
5. Siegenthaler, T. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory IT-30*, 5 (1984), 776–780.
6. Xiao, G.-Z., and Massey, J. L. A spectral characterization of correlation immune combining functions. *IEEE Transactions on Information Theory IT 34*, 3 (1988), 569–571.
7. Zhang, X. M., and Zheng, Y. GAC- The criterion for global avalanche characteristics of cryptographic functions. *Journal of Universal Computer Science 1*, 5 (1995), 316–333.