Verification of EA-equivalence for Vectorial Boolean Functions

Lilya Budaghyan, Oleksandr Kazymyrov

Department of Informatics, University of Bergen,
Bergen, Norway
Oleksandr.Kazymyrov@uib.no

July 17, 2012

WAIFI 2012

Outline

1. Basic Definitions
2. Equivalence of Vectorial Functions
3. Verification of Equivalence for Vectorial Boolean Functions

Basic Definitions

Let $\alpha \in \mathbb{F}_{2^n}$ be the root of a primitive polynomial $f(x)$ of degree n over $\mathbb{F}_2$, then

$$\mathbb{F}_{2^n} = \{0, \alpha, \alpha^2, \ldots, \alpha^{2^n-1}\}$$

Any $b \in \mathbb{F}_{2^n}$ has the following representations

- polynomial (binary)
- integer
- logarithmic

Example of Representations

Let $f(x) = x^3 + x + 1$, $n = 3$ and $\alpha = x$ then

log	polynomial	binary	integer
0	0	$(0,0,0)$	0
α	x	$(0,1,0)$	2
α^2	x^2	$(0,0,1)$	4
α^3	$x+1$	$(1,1,0)$	3
α^4	x^2+x	$(0,1,1)$	6
α^5	x^2+x+1	$(1,1,1)$	7
α^6	x^2+1	$(1,0,1)$	5
α^7	1	$(1,0,0)$	1

Basic Definitions

Let n and m be two positive integers. Any function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ is called an (n, m)-function.

(n, m)-functions are used in cryptography as:

- nonlinear combining or filtering functions in the pseudo-random generators (stream ciphers)
- substitution boxes (S-boxes) providing confusion in block ciphers

ANF and Algebraic Degree

The algebraic normal form (ANF) of any (n, m)-function F always exists and is unique:

$$\sum_{I \subseteq \{1,\ldots,n\}} a_I \left(\prod_{i \in I} x_i \right) = \sum_{I \subseteq \{1,\ldots,n\}} a_I x^I, \; a_I \in \mathbb{F}_2^m$$

The algebraic degree of F

$$deg(F) = \max\{|I| \mid a_I \neq 0\}$$

Any (n, n)-function F admits a unique univariate polynomial representation over F_{2^n}, of degree at most $2^n - 1$:

$$F(x) = \sum_{j=0}^{2^n-1} \delta_j x^j, \; \delta_j \in \mathbb{F}_{2^n}.$$

Almost Bent Function

The Walsh transform of an (n, m)-function F at $(u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$

$$\lambda(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) + u \cdot x}$$

where "$\cdot$" are inner products.
Extended Walsh Spectrum

$$\Lambda_F = \{|\lambda(u, v)| \mid (u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^m, v \neq 0\}$$

Function F is called almost bent (AB) if $\Lambda_F \in \{0, 2^{\frac{n+1}{2}}\}$.

Almost Perfect Nonlinear

- F is differentially δ-uniform if equation

$$b = F(x) + F(x+a),\ \forall a \in \mathbb{F}_2^n, \forall b \in \mathbb{F}_2^m, a \neq 0$$

  has at most δ solutions.
- F with $\delta = 2^{n-m}$ is called perfect nonlinear
- An (n, n)-function F is almost perfect nonlinear (APN) if $\delta = 2$
- Since characteristic of field $\mathbb{F}_{2^n}$ is 2, $\delta \geq 2$ and must be even.

Basic Definitions

A function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ is linear if

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

The sum of a linear function and a constant is called an affine function

$$A(x) = L(x) + c, \; c \in \mathbb{F}_{2^m}.$$

Basic Definitions

Matrix representation of an affine function $A(x)$

$$A(x) = M \cdot x \oplus C,$$

where M is $m \times n$ matrix and $C \in \mathbb{F}_2^m$.
All operations are performed in the field $\mathbb{F}_2$. In other words

$$\begin{pmatrix} a_0 \\ a_1 \\ \dots \\ a_{m-1} \end{pmatrix}_x = \begin{pmatrix} k_{0,0} & \cdots & k_{0,n-1} \\ k_{1,0} & \cdots & k_{1,n-1} \\ \vdots & \ddots & \vdots \\ k_{m-1,0} & \cdots & k_{m-1,n-1} \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ x_1 \\ \dots \\ x_{n-1} \end{pmatrix} \oplus \begin{pmatrix} c_0 \\ c_1 \\ \dots \\ c_{m-1} \end{pmatrix}$$

Outline

EA-equivalence

- Two functions F and G are called EA-equivalent if

$$F(x) = A_1 \circ G \circ A_2(x) + L_3(x) = \\ = L_1(G(L_2(x) + c_2)) + L_3(x) + c_1$$

  for some affine permutations $A_1(x) = L_1(x) + c_1$, $A_2(x) = L_2(x) + c_2$ and linear function $L_3(x)$.
- Functions F and G are restricted EA-equivalent if some functions of $\{L_1, L_2, L_3, c_1, c_2\}$ are in $\{0, x\}$. Two special cases
  - linear equivalent: $\{L_3, c_1, c_2\} = \{0, 0, 0\}$
  - affine equivalent: $L_3 = 0$

EA-equivalence

For $F, G : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ another form of representation of EA-equivalence is the matrix form

$$F(x) = M_1 \cdot G(M_2 \cdot x \oplus V_2) \oplus M_3 \cdot x \oplus V_1$$

where elements of $\{M_1, M_2, M_3, V_1, V_2\}$ have dimensions $\{m \times m, n \times n, m \times n, m, n\}$.
Matrices M_i and vectors V_j have a form

$$M = \begin{pmatrix} k_{0,0} & \cdots & k_{0,n-1} \\ k_{1,0} & \cdots & k_{1,n-1} \\ \vdots & \ddots & \vdots \\ k_{m-1,0} & \cdots & k_{m-1,n-1} \end{pmatrix}, \quad V = \begin{pmatrix} v_0 \\ v_1 \\ \cdots \\ v_{m-1} \end{pmatrix}.$$

CCZ-equivalence

Two functions $F(x)$ and $G(x)$ are CCZ-equivalent iff for some affine permutation $\mathcal{L}(x,y) = (L_1(x) + L_2(y), L_3(x) + L_4(y))$

$$F(x) = F_2 \circ F_1^{-1}(x),$$

where F_1 is a permutation and

$$F_1(x) = L_1(x) + L_2 \circ G(x); \quad F_2(x) \quad = L_3(x) + L_4 \circ G(x).$$

If F is CCZ-equivalent to G and $L_2 = const$ (resp. $L_1 = const$) then G (resp. G^{-1}) and F are EA-equivalent.
Invariant characteristics for both equivalences:

- extended Walsh spectrum (nonlinearity, AB)
- δ-uniformity (APN)

Only EA-equivalence preserves algebraic degree.

Outline

Open Problems

1. Verification of EA-equivalence for arbitrary functions.
2. For given functions F and G, find affine permutations A_1, A_2 and a linear function L_3 such that

$$F(x) = A_1 \circ G \circ A_2(x) + L_3(x)$$

Complexity of exhaustive search for $F, G : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$ equals $O\left(2^{3n^2+2n}\right)$. For $n = 6$ the complexity is already 2^{120}.

Open Problems

Alex Biryukov et al. have shown that for permutation G:

- $F(x) = L_1 \circ G \circ L_2 \; (O(n^2 \cdot 2^n))$
- $F(x) = A_1 \circ G \circ A_2 \; (O(n \cdot 2^{2n}))$

The following complexities are not taken into account:

- obtaining the value $F(x)$ for any x;
- computation of $F^{-1}(x)$ and corresponding substitution;
- memory needed for data storage.

Convert Linear Function to Matrix

For linear function $L : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ and $m \times n$ matrix M

$$L(x) = M \cdot x$$

suppose

$$\text{rows}_M(i) = (m_{ij}), \ \forall j \in \{0, 1, \ldots, n-1\};$$
$$\text{cols}_M(i) = (m_{ji}), \ \forall j \in \{0, 1, \ldots, m-1\}.$$

For $x = 2^i, \ i \in \{0, 1, \ldots, n-1\}$

$$2^0 = \begin{pmatrix} 1 \\ 0 \\ \ldots \\ 0 \end{pmatrix} \quad 2^1 = \begin{pmatrix} 0 \\ 1 \\ \ldots \\ 0 \end{pmatrix} \quad 2^{n-1} = \begin{pmatrix} 0 \\ 0 \\ \ldots \\ 1 \end{pmatrix}$$

Convert Linear Function to Matrix

Relation Between Function and Matrix

$$L(2^i) = \mathsf{cols}_M(i),\ \forall i \in \{0, 1, \dots, n-1\}$$

Suppose $L : \mathbb{F}_{2^4} \mapsto \mathbb{F}_{2^4}$, $L(x) = \alpha^4 x + \alpha^3 x^2 + \alpha^{11} x^4 + \alpha^5 x^8$.

$$L(1) = \alpha^4 = z + 1 = (1, 1, 0, 0) = 3$$
$$L(2) = \alpha^6 = z^3 + z^2 = (0, 0, 1, 1) = 12$$
$$L(4) = \alpha^3 = z^3 = (0, 0, 0, 1) = 8$$
$$L(8) = \alpha^{13} = z^3 + z^2 + 1 = (1, 0, 1, 1) = 13$$

$$M = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

$$\boxed{O(n)}$$

Equivalence of $F(x) = M_1 \cdot G(x) \oplus V_1$

Restricted EA-equivalence

$$F(x) = M_1 \cdot G(x) \oplus V_1$$

Let $G(x) = G'(x) \oplus G(0)$ and $F(x) = F'(x) \oplus F(0)$ then

$$F'(x) \oplus F(0) = M_1 \cdot G'(x) \oplus M_1 \cdot G(0) \oplus V_1$$

$$\begin{cases} F(0) = M_1 \cdot G(0) \oplus V_1 \\ F'(x) = M_1 \cdot G'(x) \end{cases}$$

Two different cases

- $\{2^i \mid 0 \leq i \leq m-1\} \subset \mathrm{img}(G')$
- $G'(x)$ is arbitrary

Equivalence of $F(x) = M_1 \cdot G(x) \oplus V_1$

- $\{2^i \mid 0 \leq i \leq m-1\} \subset \mathsf{img}(G')$

$$F'(x) = M_1 \cdot G'(x)$$

$$G'(x_i) = 2^i,\ 0 \leq i \leq m-1$$

$$N = \{x_i \mid G'(x_i) = 2^i,\ 0 \leq i \leq m-1\}$$

$$\boxed{F'(a_i) = \mathsf{cols}_{M_1}(i),\ a_i \in N, i \in \{0, 1, \ldots, m-1\}}$$

Complexity:

Cheking M_1, $\forall x \in \mathbb{F}_2^n$

$$\boxed{O(2^n + m + 2^n) \approx O(2^{n+1})}$$

Finding N

Finding M_1

Equivalence of $F(x) = M_1 \cdot G(x) \oplus V_1$

- $G'(x)$ is arbitrary.

Definition

Let $F'(x)_i$ be ith-bit of $F'(x)$, $u_{G'} = |img(G')|$ and $N_{G'}$ be any subset of $\mathbb{F}_2^n$ such that $|\{G'(a)|a \in N_{G'}\}| = u_{G'}$.

Example

- S-box$_G$ = [0, 8, 1, 2, 8, 1, 3, 5, 2, 2, 0, 1, 5, 11, 13, 2]
- $img(G) = [0, 8, 1, 2, 3, 5, 11, 13]$
- $N_G = [0, 1, 2, 3, 6, 7, 13, 14]$

- $G'(x)$ is arbitrary.

Definition

Let $F'(x)_i$ be ith-bit of $F'(x)$, $u_{G'} = |img(G')|$ and $N_{G'}$ be any subset of $\mathbb{F}_2^n$ such that $|\{G'(a)|a \in N_{G'}\}| = u_{G'}$.

Example

- S-box$_G$ = [0, 8, 1, 2, 8, 1, 3, 5, 2, 2, 0, 1, 5, 11, 13, 2]
- $img(G) = [0, 8, 1, 2, 3, 5, 11, 13]$
- $N_G = [0, 1, 2, 3, 6, 7, 13, 14]$

Equivalence of $F(x) = M_1 \cdot G(x) \oplus V_1$

- $G'(x)$ is arbitrary.

Definition

Let $F'(x)_i$ be ith-bit of $F'(x)$, $u_{G'} = |img(G')|$ and $N_{G'}$ be any subset of $\mathbb{F}_2^n$ such that $|\{G'(a)|a \in N_{G'}\}| = u_{G'}$.

Example

- S-box$_G$ = [0, 8, 1, 2, 8, 1, 3, 5, 2, 2, 0, 1, 5, 11, 13, 2]
- $img(G) = [0, 8, 1, 2, 3, 5, 11, 13]$
- $N_G = [0, 1, 2, 3, 6, 7, 13, 14]$

- $G'(x)$ is arbitrary.

$$F'(x_j)_i = \text{rows}_{M_1}(i) \cdot G'(x_j), \;\; \forall x_j \in N_{G'}, \; 0 \leq j \leq u_{G'} - 1 \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} F'(x_0)_i = \text{rows}_{M_1}(i) \cdot G'(x_0) \\ F'(x_1)_i = \text{rows}_{M_1}(i) \cdot G'(x_1) \\ \dots \\ F'(x_{u_{G'}-1})_i = \text{rows}_{M_1}(i) \cdot G'(x_{u_{G'}-1}) \end{cases} .$$

For $u_{G'} \approx 2^n$ the complexity is equal to

$$\boxed{O\left(m \cdot 2^{2n}\right)}$$

Equivalence of $F(x) = G(x) \oplus M_3 \cdot x \oplus V_1$

Restricted EA-equivalence

$$F(x) = G(x) \oplus M_3 \cdot x \oplus V_1$$

Let $H(x) = F(x) \oplus G(x)$ then

$$H(x) = F(x) \oplus G(x) = M_3 \cdot x \oplus V_1$$
$$H(x) = H'(x) \oplus H(0)$$
$$\begin{cases} V_1 = H(0) \\ H'(x) = M_3 \cdot x \end{cases}$$

For $x = 2^i$, $\forall i = \{0, 1, \ldots, n-1\}$ find M_3 with complexity

$$\boxed{O(n)}$$

Equivalence of $F(x) = G(M_2 \cdot x \oplus V_2)$

Restricted EA-equivalence

$$F(x) = G(M_2 \cdot x \oplus V_2)$$

- G is a permutation. Let $H(x) = G^{-1}(F(x))$

$$H(x) = M_2 \cdot x \oplus V_2$$
$$H(x) = H'(x) + H(0)$$
$$\begin{cases} V_2 = H(0) \\ H'(x) = M_2 \cdot x \end{cases}$$

For $x = 2^i$, $\forall i = \{0, 1, \ldots, n-1\}$ find M_2 with complexity

$$\boxed{O(n)}$$

Equivalence of $F(x) = M_1 \cdot G(x) \oplus M_3 \cdot x \oplus V_1$

Restricted EA-equivalence

$$F(x) = M_1 \cdot G(x) \oplus M_3 \cdot x \oplus V_1$$

Every vectorial Boolean function H admits the form

$$H(x) = H'(x) \oplus L_H(x) \oplus H(0)$$

$$\begin{cases} F'(x) = M_1 \cdot G'(x) \\ L_F(x) = M_1 \cdot L_G(x) \oplus M_3 \cdot x \\ F(0) = M_1 \cdot G(0) \oplus V_1 \end{cases}$$

$\boxed{O\left(2^{n+1}\right)}$

$\{2^i \mid 0 \leq i \leq m-1\} \subset \text{img}(G')$

$\boxed{O\left(m \cdot 2^{2n}\right)}$

$G'(x)$ is arbitrary

Summary Table of Obtained Results

Restricted EA-equivalence	Complexity	G
$F(x) = M_1 \cdot G(x \oplus V_2) \oplus V_1$	$O\left(2^{2n+1}\right)$	†
$F(x) = M_1 \cdot G(x \oplus V_2) \oplus V_1$	$O\left(m \cdot 2^{3n}\right)$	A
$F(x) = G(M_2 \cdot x \oplus V_2) \oplus V_1$	$O\left(n \cdot 2^{m}\right)$	P
$F(x) = G(x \oplus V_2) \oplus M_3 \cdot x \oplus V_1$	$O\left(n \cdot 2^{n}\right)$	A
$F(x) = M_1 \cdot G(x \oplus V_2) \oplus M_3 \cdot x \oplus V_1$	$O\left(2^{2n+1}\right)$	‡
$F(x) = M_1 \cdot G(x \oplus V_2) \oplus M_3 \cdot x \oplus V_1$	$O\left(m \cdot 2^{3n}\right)$	A

† - G is under condition $\{2^i \mid 0 \le i \le m-1\} \subset \mathrm{img}(G')$ where $G'(x) = G(x) \oplus G(0)$.

‡ - G is under condition $\{2^i \mid 0 \le i \le m-1\} \subset \mathrm{img}(G')$ where $G'(x) = G(x) \oplus L_G(x) \oplus G(0)$.

Comparison of the Results

Restricted EA-equivalence	Complexity	$G(x)$
$F(x) = M_1 \cdot G(M_2 \cdot x)$	$O\left(n^2 \cdot 2^n\right)$	P
$F(x) = M_1 \cdot G(M_2 \cdot x \oplus V_2) \oplus V_1$	$O\left(n \cdot 2^{2n}\right)$	P
$F(x) = M_1 \cdot G(x \oplus V_2) \oplus V_1$	$O\left(2^{2n+1}\right)$	†
$F(x) = M_1 \cdot G(x \oplus V_2) \oplus V_1$	$O\left(n \cdot 2^{3n}\right)$	A
$F(x) = G(M_2 \cdot x \oplus V_2) \oplus V_1$	$O\left(n \cdot 2^n\right)$	P
$F(x) = G(x \oplus V_2) \oplus M_3 \cdot x \oplus V_1$	$O\left(n \cdot 2^n\right)$	A
$F(x) = M_1 \cdot G(x \oplus V_2) \oplus M_3 \cdot x \oplus V_1$	$O\left(2^{2n+1}\right)$	‡
$F(x) = M_1 \cdot G(x \oplus V_2) \oplus M_3 \cdot x \oplus V_1$	$O\left(n \cdot 2^{3n}\right)$	A

† - G is under condition $\{2^i \mid 0 \le i \le m-1\} \subset \mathrm{img}(G')$ where $G'(x) = G(x) + G(0)$.

‡ - G is under condition $\{2^i \mid 0 \le i \le m-1\} \subset \mathrm{img}(G')$ where $G'(x) = G(x) \oplus L_G(x) \oplus G(0)$.

References

- A. Biryukov, C. De Canniere, A. Braeken, B. Preneel, A Toolbox for Cryptanalysis: Linear and Affine Equivalence Algorithms, Eurocrypt, LNCS 2656, Springer-Verlag, pp. 3350, 2003.
- C. Carlet, P. Charpin, and V. Zinoviev, "Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems", presented at Des. Codes Cryptography, 1998, pp.125-156.
- C. Carlet, Vectorial Boolean functions for cryptography. In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge.