Affine equivalence of Boolean functions

Sugata Gangopadhyay

Department of Mathematics, Indian Institute of Technology Roorkee

February 10, 2009

Sugata Gangopadhyay (IITR)

Japan-India Kick-off Meeting

< 6 b

- Let \mathbb{F}_2 be the prime field of characteristic 2.
- Let \mathbb{F}_2^n be the *n*-dimensional vector space over \mathbb{F}_2 .
- A Boolean function *f* on *n* variables is a function from \mathbb{F}_2^n into \mathbb{F}_2 .
- Aleternatively a Boolean function *f* on *n* variables is a function from 𝔽_{2ⁿ} into 𝔽₂, where 𝔽_{2ⁿ} is the *n*-th degree extension of 𝔽₂.
- Let \mathcal{B}_n be the set of all Boolean functions on *n* variables.

• The Boolean functions *f* and *g* are said to be affine equivalent if there exist

$$A \in GL(n, \mathbb{F}_2), b, \lambda \in \mathbb{F}_2^n, \epsilon \in \mathbb{F}_2$$

such that

$$g(x) = f(Ax + b) + \lambda \cdot x + \epsilon,$$

where $\lambda \cdot x$ is the inner product of λ and x. If $\lambda = (\lambda_1, \ldots, \lambda_n)$ and $x = (x_1, \ldots, x_n)$ where $\lambda_i, x_i \in \mathbb{F}_2$ for all $i = 1, \ldots, n$ then we use an inner product defined by $\lambda \cdot x = \lambda_1 x_1 + \ldots + \lambda_n x_n$.

• A Boolean function on 4 variables.

<i>x</i> ₄	<i>x</i> 3	<i>x</i> ₂	<i>x</i> ₁	f
0	0	0	0	0
0	0	0	1	1
0	0	1	0	1
0	0	1	1	1
0	1	0	0	1
0	1	0	1	1
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	0
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

글 🕨 🖌 글

$$f: \{0,1\}^4 \to \{0,1\}$$

A Brief Survey on Affine Equivalence Problem

- O. S. Rothaus. On bent functions. *Journal of Combinatorial Theory, Series A*, 20:300–305, 1976.
- B. Preneel, Analysis and design of cryptographic hash functions, PhD thesis, Katholieke Universiteit Leuven, (1993).
- A. Braeken, Y. Borisov, S. Nikova, B. Preneel. Classification of Boolean Functions of 6 Variables or Less with Respect to Cryptographic Properties. International Colloquium on Automata, Languages and Programming ICALP 2005, *Lecture Notes in Computer Science* Vol. 3580, Springer-Verlag, p. 324-334, 2005.

< 口 > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

- C. Carlet. Two new classes of bent functions. Eurocrypt'93, Lecture Notes in Computer Science Vol. 765 (1994) 77 - 101.
- X. D. Hou, *GL*(*m*, 2) acting on *R*(*r*, *m*)/*R*(*r* − 1, *m*), *Discrete Math.* Vol. 149 (1996), 99-122.
- X. D. Hou, Cubic bent functions, *Discrete Math.* Vol. 189 (1998), 149-161.
- Q. Meng, M. Yang, H. Zhang, Y. Liu. Analysis of affinely equivalent boolean functions, *First International Workshop, BFCA'05* (2005) 105 - 114.

< 口 > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

- We demonstrate that a spectrum consisting of weights of second derivatives of a Boolean function, taken over all distinct 2 dimensional subspaces of its domain, can act as an invariant.
- We provide an algorithm with $O(n2^{2n})$ time complexity to compute this spectrum.

- The derivative of $f \in B_n$ with respect to $a \in \mathbb{F}_2^n$ is defined as the function $D_a f(x) = f(x + a) + f(x)$, for all $x \in \mathbb{F}_2^n$.
- Let V be a 2 dimensional subspace of 𝔽ⁿ₂ and {a, b} be any basis of V. Then the derivative of f ∈ 𝔅_n with respect to V is defined as

$$D_V f(x) = D_b D_a f(x) = f(x + a + b) + f(x + b) + f(x + a) + f(x)$$

for all $x \in \mathbb{F}_2^n$. $D_V f$ is referred to as second derivative of f at V.

 It is to be noted that the value of D_V is independent of the choice of the basis.

- $S(f:a,b) = \sum_{x \in \mathbb{F}_2^n} D_a D_b f(x)$
- S(f) = [S(f : a, b) : {a, b} ∈ Jⁿ₂], where Jⁿ₂ is the set of all distinct bases in ℝⁿ₂ of cardinality 2.
- Suppose f, g ∈ B_n such that S(f) ≠ S(g) then f is not affine equivalent to g.

< 47 ▶

- We show that all the 6 variable bents can be distinguished by using this spectrum.
- We prove that there exist 6 and 8 variable bents that are not affine equivalent to rotation symmetric bents.
- We show that using this spectrum it is possible to partially distinguish bents within the class of *PS_{ap}* type bents.

- Dillon and Dobbertin (2004) have characterized Kasami bent functions.
- Suppose $f(x) = Tr_1^n(\lambda x^k)$ for all $x \in \mathbb{F}_{2^n}$ such that
 - n is not divisible by 3.

k =
$$2^{2d} - 2^d + 1$$
 with $gcd(n, d) = 1, 0 < d < n$.

3 $\lambda \in \mathbb{F}_{2^n}^*$ does not belong to $\{x^3 : x \in \mathbb{F}_{2^n}\}$.

Then *f* is a bent function. Any bent function which can be written in this form is said to be a Kasami bent function.

- It is observed experimentally by Canteaut, Daum, Dobbertin and Leander (2004, 2006) that some Kasami bents are not affine equivalent to Maiorana-MacFarland type bents.
- By considering the second derivative spectrum we prove that no non-quadratic Kasami bent is affine equivalent to Maiorana-MacFarland type bent functions.
- Gangopadhyay S., Sharma D., Sarkar S., Maitra S., On Affine (Non) Equivalence of Bent Functions, Computing, (Springer), (accepted)

A B A A B A

A D M A A A M M