Algebraic Immunity of Some Cryptographic Boolean Functions

Yassir Nawaz and Guang Gong
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, ON, N2L 3G1, CANADA
ynawaz@engmail.uwaterloo.ca, g.gong@ece.uwaterloo.ca

ABSTRACT

In this paper we investigate the algebraic immunity of some well known cryptographic functions to determine their resistance to algebraic attacks. Experimental results for single trace term functions, hyper-bent functions and Welch-Gong transformations are presented. We also prove that the degree of the inverse function in n variables can be reduced to $n/2$ by multiplying it with a quadratic function.

1. INTRODUCTION

Algebraic attacks have recently gained importance as an effective cryptanalytic technique against block and stream ciphers[1]-[5]. Ciphers such as LILI and Toyocrypt have been successfully broken using algebraic attacks [4]. These are also the most promising attacks against AES (Advanced Encryption Standard) so far [5]. These attacks reduce the cipher into a system of nonlinear multivariate equations which can then be solved by linearization or other methods i.e. XL algorithm or Grobner bases algorithm. The success of the attack depends on the keystream available and the effort required for solving the system of multivariate equations. The number of all monomial terms in n variables of degree $< d$ are $\sum_{i=0}^{d} \binom{n}{i}$, which is the number of equations required for a solvable linearized system. Therefore the complexity of the algebraic attack depends on n as well as d. This means that for a given n, lower the degree d of the Boolean function or S-Box in the cipher, the faster the attack. Courtois recently showed that even if the degree of the Boolean function f is high, it can be multiplied by a well chosen function g such that the degree of the product is much lower than degree of f [4]. Therefore if such g exists for a Boolean function used in the cipher then the complexity of the attack can be reduced substantially and the function is considered to be cryptographically weak.

2. ALGEBRAIC IMMUNITY OF CRYPTOGRAPHIC FUNCTIONS

In this section we study the resistance of some well known cryptographic functions to algebraic attacks. It is proved in [4] that if f is any Boolean function $f : \mathrm{F}_{2^n} \rightarrow \mathrm{F}_2$, then for any pair of integers (d, e) such that $d+e \geq n$, there is a Boolean function $g \neq 0$ of degree at most d such that $f \cdot g$ is of degree at most e. Let us denote the degree of a function f as $deg(f)$, then we say that f has *algebraic immunity* if there does not exist a multiplier g such that:

a) $d + e < n$
b) $e < deg(f)$

If there exists some multiplier g such that a) and b) are true, then we say that g is a low degree approximation of f. It is of interest to find the Boolean functions which satisfy the desired cryptographic properties and also have algebraic immunity. In this paper we examine three classes of cryptographic functions: Functions represented by a single trace term in polynomial form, hyper-bent functions and Welch-Gong transformations.

2.2 Inverse Function

The AES (Advanced Encryption Standard) S-box is composed of the inverse function in finite field F_{2^8}. This type of S-box mappings can be decomposed into monomial trace functions as follows:

Let $\{\alpha_0, ..., \alpha_{n-1}\}$ and $\{\beta_0, ..., \beta_{n-1}\}$ be the dual basis of $GF(2^n)$. Then $F(x)$ can be represented as $F(x) = \sum_{j=0}^{n-1} Tr_1^n(\beta_j x^{-2^i})\alpha_j$, $x \neq 0$, where $Tr(x)$ is a trace function from $\mathrm{F}_{2^n} \rightarrow \mathrm{F}_2$. Thus each component function $f_j(x) = Tr_1^n(\beta_j x^{-2^i})$ can be considered as a Boolean function in n variables. Note that f_j has degree $n-1$, the maximal degree for a balanced Boolean function and $Tr_1^n(\beta_j x^{-2^i}) = Tr_1^n(\beta_j^{2^i} x^{-1})$. We establish the following result:

Theorem 1: Let $n = 2m$, $d = 1 + 2^m$, $f(x) = Tr_1^n(\beta x^{-1})$, $\beta \in \mathrm{F}_{2^n}$ and $g(x) = Tr_1^m(\eta x^d)$, $\eta \in \mathrm{F}_{2^m}$. Then

$$f(x)g(x) = a + \sum_{i=1}^{m-1} Tr_1^n(\zeta_i x^{r_i}), \qquad (1)$$

where $a = Tr_1^n(\beta^{2^{m-1}}\eta)$, $\zeta_i = \beta^{2^{i-1}}\eta$, and $r_i = 1 + \sum_{j=i}^{m-1} 2^j, i = 1, \cdot\cdot, m-1$.

The consequence of Theorem 1 is that there always exists a quadratic function g such that $deg(f \cdot g) = n/2$.

In order to prove Theorem 1 we need the following lemma.

Lemma 1: Let $r = 2^{n-1} - 1 = 1 + 2 + \cdots + 2^{n-2}$, $d_i = d + r2^{m+i}$. Then

$$d_i = (1 + \sum_{j=i}^{m-1} 2^j)2^m, i = 1, \cdot\cdot, m-1 \tag{2}$$

and

$$H(d_i) = m - i + 1, d_i = r_i 2^m, i = 1, \cdot\cdot, m-1, \tag{3}$$

where $H(d_i)$ represents the Hamming weight of d_i, i.e. the number of nonzero coefficients in the binary representation of d_i.

Proof: The above result can be established by examining the binary representation of d_i.

	$2m-1$				m			1	0
$r2^{m+1}$	1	$\cdot\cdot$	1	0	1	1	$\cdot\cdot$	1	1
d	0	$\cdot\cdot$	0	0	1	0	$\cdot\cdot$	0	1
$d + r2^{m+1}$	1	$\cdot\cdot$	1	1	1	0	$\cdot\cdot$	0	0

Then $H(d + r2^{m+1}) = m$.

	$2m-1$					m			1	0
$r2^{m+2}$	1	$\cdot\cdot$	1	0	1	1	1	$\cdot\cdot$	1	1
d	0	$\cdot\cdot$	0	0	0	1	0	$\cdot\cdot$	0	1
$d + r2^{m+2}$	1	$\cdot\cdot$	1	1	0	1	0	$\cdot\cdot$	0	0

So $H(d + r2^{m+2}) = m - 1$. In general,

	$2m-1$					$\leftarrow i-1 \rightarrow$	m		0
$r2^{m+i}$	1	$\cdot\cdot$	1	0	1	$\cdot\cdot$	1	1	$\cdot\cdot$	1
d	0	$\cdot\cdot$	0	0	0	$\cdot\cdot$	0	1	$\cdot\cdot$	1
$d + r2^{m+i}$	1	$\cdot\cdot$	1	1	0	$\cdot\cdot$	0	1	$\cdot\cdot$	0
			$\leftarrow m-i \rightarrow$							

Therefore $H(d + r2^{m+i}) = m - i + 1$, $1 \leq i \leq m-1$. Also we consider,

	$2m-1$			m			1	0
$r2^m$	1	$\cdot\cdot$	1	1	1	$\cdot\cdot$	0	1
d	0	$\cdot\cdot$	0	1	0	$\cdot\cdot$	0	1
$d + r2^m$	1	$\cdot\cdot$	0	0	0	$\cdot\cdot$	0	0

$\Rightarrow 2^m + d = 2^n \equiv 1 \bmod 2^n - 1$

□

Proof of Theorem 1:

$$\begin{aligned} f(x) &= Tr_1^n(\beta x^{-1}) \\ &= Tr_1^n(\beta x^{2r}) \\ &= Tr_1^n(\beta^{2^{n-1}} x^r)(Trace function property). \end{aligned} \tag{4}$$

Also $g(x) = Tr_1^m(\eta x^d)$.
Now consider the product,

$$\begin{aligned} \beta^{2^{n-1+m}} x^{r2^m} \eta x^d &= \beta^{2^{m-1}} \eta x^{r2^m + d} \\ &= \beta^{2^{m-1}} \eta, \end{aligned} \tag{5}$$

since $x^{2^j(2^m r + d)} = 1, x \neq 0$.
Now we can write

$$\sum_{j=0}^{n-1} \beta^{2^{m-1+j}} \eta^{2^j} = Tr_1^n(\beta^{2^{m-1}} \eta) = a. \tag{6}$$

To derive the second term in equation 1 we consider the following product

$$\begin{aligned} (\beta^{2^n - 1} x^r)^{2^{m+i}} \eta x^d &= \beta^{2^{m-1+i}} \eta x^{r2^{m+i} + d} \\ &= \beta^{2^{m-1+i}} \eta x^{r_i 2^m} (Lemma 1). \end{aligned}$$

This implies that

$$Tr_1^n(\beta^{2^{m-1+i}} \eta x^{r_i 2^m}) = Tr_1^n(\beta^{2^{i-1}} \eta x^{r_i}), \tag{7}$$

where, $(\beta^{2^{m-1+i}} \eta)^{2^m} = \beta^{2^i} \eta$ and $(\eta^{2^m} = \eta)$.
The proof of Theorem 1 is due to equations 6 and 7.

□

Theorem 1 proves that the degree of the multiplier g is independent of n and the ratio $(d+e)/n$ decreases as n increases. This indicates some algebraic weakness in these functions. Note that component functions of AES S-box belong to this category of functions. In the following we also consider all monomial trace functions of degree $d < n - 1$, where $9 \leq n \leq 16$. Table 1 shows some cases where $deg(f \cdot g)$ is significantly smaller than $deg(f)$. We only considered the monomial trace functions as multipliers in our analysis but there may exist other multipliers which can reduce the degree of $f \cdot g$ even further.

2.2 Hyperbent Functions

A bent function is a function from $\mathrm{F}_2^{\mathrm{n}} \rightarrow \mathrm{F}_2$ whose Hadamard transform has constant magnitude, i.e.,

$$\hat{f}(\lambda) = \sum_{x \in \mathrm{F}_{2^{\mathrm{n}}}} (-1)^{Tr(\lambda x) + f(x)} = \pm\sqrt{2^n}, \forall \lambda \in \mathrm{F}_{2^{\mathrm{n}}}$$

where n is even and we write $n = 2m$. A bent function is called a hyper-bent function[7] if,

n	$f, (0 \leq i \leq n-1)$	$deg(f)$	d	e
9	$Tr_1^n(x^{255\times 2^i})$	8	3	4
10	$Tr_1^n(x^{511\times 2^i})$	9	3	5
11	$Tr_1^n(x^{1023\times 2^i})$	10	3	5
12	$Tr_1^n(x^{2047\times 2^i})$	11	3	5
13	$Tr_1^n(x^{4095\times 2^i})$	12	3	6
14	$Tr_1^n(x^{8191\times 2^i})$	13	5	6
15	$Tr_1^n(x^{15295\times 2^i})$	12	5	5
15	$Tr_1^n(x^{15855\times 2^i})$	12	5	5
16	$Tr_1^n(x^{32255\times 2^i})$	14	4	6
16	$Tr_1^n(x^{32767\times 2^i})$	15	4	6

Table 1. Low degree approximations of single trace term functions

$$\hat{f}(\lambda, c) = \pm 2^m, \forall \lambda \in \mathrm{F}_{2^n}, c : 0 < c < 2^n - 1,$$

$gcd(c, 2^n - 1) = 1$, where

$$\hat{f}(\lambda, c) = \sum_{x \in \mathrm{F}_{2^n}} (-1)^{Tr(\lambda x^c) + f(x)}.$$

Hyper-bent functions are important cryptographic functions as they have the maximum nonlinearity (minimum distance from all affine functions). A hyper-bent function f in n variables has degree $d = n/2$ where n is even. We have used the algorithm given in [6] to test hyper-bent functions for algebraic immunity. Our exhaustive search shows that all hyper-bent functions in 6 variables($n = 6$ and $d = 3$) have algebraic immunity i.e. there does not exist a multiplier g such that $deg(f \cdot g) < 3$. However our results for $n = 8$ and $n = 10$ show that for about 10 percent of the hyper-bent functions $deg(f \cdot g) = d - 1$. We conjecture that the degree of $f \cdot g$ can be reduced below $d - 1$ for hyperbent functions.

2.3 Welch-Gong Transformations

Let $n \neq 0 \bmod 3$, $n = 3k - 1$, α a primitive element of F_{2^n}, and $t(x) = x + x^{q_1} + x^{q_2} + x^{q_3} + x^{q_4}$, $x \in \mathrm{F}_{2^n}$, where the $q_i's$ are given by

$n = 3k - 1$	$q_1 = 2^k + 1$ $q_2 = 2^{2k-1} + 2^{k-1} + 1$ $q_3 = 2^{2k-1} - 2^{k-1} + 1$ $q_4 = 2^{2k-1} + 2^k - 1$
$n = 3k - 2$	$q_1 = 2^{k-1} + 1$ $q_2 = 2^{2k-2} + 2^{k-1} + 1$ $q_3 = 2^{2k-2} - 2^{k-1} + 1$ $q_4 = 2^{2k-1} + 2^{k-1} + 1$

The function defined by

$$f(x) = Tr_1^n(t(x+1)+1), x \in \mathrm{F}_{2^n}$$

n	$deg(f)$	No. of WG functions	No. of WG functions with low degree approx	d	e
7	4	18	0	-	-
8	4	16	1	3	3
10	5	60	2	4	4
11	5	176	0	-	-
13	6	631	0	-	-

Table 2. Low degree approximations of WG tranformations

is called the Welch-Gong(WG) transformation. WG transformations have important cryptographic properties suitable for use in stream ciphers. They are balanced with high linear complexity and are first order resilient. The degree of a welch-Gong function in n variables is $\lceil n/3 \rceil + 1$. We tested all WG functions in n variables where $7 \leq n \leq 13$. The results are shown in Table 2. We also checked a few WG functions in 14 variables and found no low degree approximations. According to [8] the probability that a function in n variables has low degree approximations decreases as n increases. Therefore we believe that the probability that a WG function in 11 or more variables ($n \geq 11$) has a low degree approximation is very small.

3. CONCLUSION

In this paper we have investigated three types of cryptographic functions to determine their resistance to algebraic attacks. We have proved that balanced single trace term functions with maximum degree (i.e. $n - 1$ where the functions is in n variables) have some algebraic weakness. Inverse functions belong to this category of functions. We also provided the examples of some algebraically weak single trace term functions in Table 1. Our experimental results for hyper-bent functions and Welch-Gong transformations show that for large values of n these functions have good algebraic immunity.

REFERENCES

[1] N.Courtois, Algebraic Attacks on Combiners with Memory ans Several Outputs, *Cryptology ePrint Archive, Report 2003/125*,http://eprint.iacr.org/, 2003

[2] Frederik Armknecht, On the Existence of low-degree Equations for Algebraic Attacks, *Cryptology ePrint Archive, Report 2004/185*, http://eprint.iacr.org/, 2004

[3] Philip Hawkes and Gregory G. Rose,Rewriting Variables: the Complexity of Fast Algebraic Attacks on Stream Ciphers, *Cryptology ePrint Archive, Report 2004/081*,http://eprint.iacr.org/, 2004,

[4] N.Courtois, Fast Algebraic Attacks on Stream Ciphers with Linear Feedback, *Advances in Cryptology-CRYPTO 2003*, volume LNCS 2729, pp. 176-194. Springer-Verlag, 2003

[5] N.Courtois and Pieprzyk J., Cryptanalysis of Block Ciphers with Overdefined Systems of Equations, *Advances in Cryptology-ASIACRYPT 2002*, volume LNCS 2501. Springer-Verlag, 2002.

[6] G.Gong, On Existence and Invariant of Algebraic Attakcs, *Technical report CORR2004-16, Centre for Applied Cryptographic Research, University of Waterloo*, Available at http://www.cacr.math.uwaterloo.ca/

[7] A.M.Yousef and G.Gong, Hyper-bent Functions, *Advances in Cryptology, EUROCRYPT-2001*, volume LNCS 2045, pp.406-419. Springer-Verlag, 2001

[8] W. Meier, E. Pasalic, and C. Carlet, Algebraic Attacks and Decomposition of Boolean Functions, *Advances in Cryptology EUROCRYPT-2004*, volume LNCS 3027, pp.474-491. Springer-Verlag, 2004