PAPER *Special Section on Cryptography and Information Security*

Quadratic Equations from APN Power Functions*

Jung Hee CHEON†, ***Member and*** **Dong Hoon LEE**††, ***Nonmember***

SUMMARY We develop several tools to derive quadratic equations from algebraic S-boxes and to prove their linear independence. By applying them to all known *almost perfect nonlinear* (APN) power functions and the inverse function, we can estimate the resistance against algebraic attacks. As a result, we can show that APN functions have different resistance against algebraic attacks, and especially S-boxes with Gold or Kasami exponents have very weak resistance.

key words: *algebraic attack, quadratic equations, almost perfect nonlinear (APN), linear independence, nonlinearity.*

1. Introduction

After they were proposed by Courtois in 2002 [7], algebraic attacks became one of the most powerful attack on stream ciphers [15]. The attacks can be also applied to block ciphers when they use some weak S-boxes [9]. Algebraic attacks consist of two steps: The first one is to find a system of multivariate equations having secret key bits as variables. The next is to compute the secret key by solving the system. There are a few techniques for solving a system of multivariate equations such as linearization, XL algorithms and Gröbner basis [2], [8], [10].

Recently, some stream ciphers [13], [21] as well as block ciphers uses S-boxes as nonlinear components. Our main interest is to establish a system of multivariate equations from S-boxes. In [9], Courtois and Pieprzyk proposed an algebraic attack on AES [1] by exploiting algebraic properties of S-boxes: They considered the S-box $y = 1/x$ as a quadratic equation $xy = 1$ in x and y, and obtain additional quadratic equations by multiplying appropriate monomials. More precisely, they obtain 23 quadratic equations with a total of 81 distinct terms from the S-box of AES and show that the equations are linearly independent by simulation.

In this paper, we give theoretical approaches to obtain *linearly independent* multivariate equations from algebraic S-boxes. We develop a few tools to prove *linear independence* of multivariate equations. First, for a vector Boolean function $F(x, y) : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, all nonzero components of $F(x, y)$ are linearly independent if $F(x, g(x))$ has m linearly independent components for some vector Boolean function $g : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Second, linear independence of multivariate equations is *invariant* under an invertible transformation of inputs and an invertible affine transformation of outputs. We also introduce several methods to derive quadratic equations from given algebraic S-boxes by applying multiplications, compositions, and substitutions.

By applying these tools, we can derive $5n - 1$ quadratic equations from the inverse function $y = 1/x$ in $\mathbb{F}_{2^n}$ (or its affine transformation) and show that they are linearly independent for any positive integer n. Further we apply them to all known *almost perfect nonlinear* (APN) power functions [11]. Note that 'APN' functions are the S-boxes with the best resistance against differential cryptanalysis [3], [4]. Our analysis shows, however, that they require different numbers of new variables to obtain the same number of linear independent equations and so have different resistance against algebraic attacks. More precisely, Gold or Kasami power functions have weaker resistance and Welch or Niho power functions have better resistance than the inverse or Dobbertin power functions against algebraic attacks.

In Section 2, we introduce some preliminaries on APN and resistance against algebraic attacks. In Section 3, we propose some auxiliary lemmas used to show the linear independence of multivariate equations. In Section 4, we discuss a few methods to derive quadratic equations from a given function. Using these tools, we prove the linear independence of quadratic equations induced from APN power functions in Section 5. As an application, we deal with the resistance of S-boxes made by APN power functions and compare them in Section 6.

2. Preliminaries

2.1 Notations

Let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements. A function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ is called a vector Boolean function. When $m = 1$, it is merely called a Boolean function.

Let $\mathbb{F}_2^n$ be an n-dimensional vector space over $\mathbb{F}_2$. If we fix a basis $\{\omega_0, \cdots, \omega_{n-1}\}$ of $\mathbb{F}_{2^n}$, then there is a natural isomorphism ϕ such that

$$\phi : \mathbb{F}_{2^n} \to \mathbb{F}_2^n, \quad \sum a_i\omega_i \mapsto (a_0, \cdots, a_{n-1}).$$

†The author is with the Faculty of Seoul National University, Korea

††The author is working for National Security Research Institute as a senior researcher

*A part of this paper was published in FSE 2004 [6]

Consider of a univariate monomial x^d over $\mathbb{F}_{2^n}$. Let $d = \sum d_i 2^i$ be a binary representation of d. We call the weight of d by the number of nonzero d_i, denoted $wt(d)$. If $x = \sum x_i \omega_i$ for a fixed basis, then

$$\begin{aligned} x^d &= \prod_{d_j=1} \left(\sum_{i=0}^{n-1} x_i \omega_i^{2^j} \right) \\ &= \sum_{i=0}^{n-1} f_i(x_0, \cdots, x_{n-1}) \omega_i \end{aligned}$$

for Boolean functions f_i with n variables of degree $wt(d)$. Thus x^d can be regarded as a vector Boolean function via the isomorphism ϕ.

We define the algebraic degree of a monomial x^d by the degree of component functions as a vector Boolean function. Therefore every quadratic monomial can be represented as $x^{2^i+2^j}$ for distinct i and j.

2.2 Almost Perfect Nonlinear Power Functions

Definition 1. *A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called a* almost perfect nonlinear *(APN) if each equation*

$$F(x+a) - F(x) = b \quad \text{for } a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}$$

has at most two solutions $x \in \mathbb{F}_{2^n}$.

That is, APN functions are the S-boxes with the best resistance against differential cryptanalysis. It was conjectured that all APN *power functions* are classified as in Table 1 and Table 2 [11], [12].

Table 1 APN power functions x^d on $\mathbb{F}_{2^n}$ where $n = 2m+1$

Types	Exponents
Gold	$d = 2^k + 1$, $\gcd(k,n) = 1$ $(1 \le k \le m)$
Kasami	$d = 2^{2k} - 2^k + 1$, $\gcd(k,n) = 1$ $(2 \le k \le m)$
Dobbertin	$d = 2^{4s} + 2^{3s} + 2^{2s} + 2^s - 1$ if $n = 5s$
Welch	$d = 2^m + 3$
Niho	$d = \begin{cases} 2^m + 2^{m/2} - 1, & \text{if } m \text{ is even} \\ 2^m + 2^{(3m+1)/2} - 1, & \text{if } m \text{ is odd} \end{cases}$
Inverse	$d = -1$

Table 2 APN power functions x^d on $\mathbb{F}_{2^n}$ where n is even

Types	Exponents
Gold	$d = 2^k + 1$, $\gcd(k,n) = 1$ $(1 \le k < n/2)$
Kasami	$d = 2^{2k} - 2^k + 1$, $\gcd(k,n) = 1$ $(2 \le k \le n/2)$
Dobbertin	$d = 2^{4s} + 2^{3s} + 2^{2s} + 2^s - 1$ if $n = 5s$

The resistance against linear cryptanalysis is measured by *nonlinearity* and the functions with maximal nonlinearity are said to be *maximally nonlinear*. It was proved that a maximally nonlinear function is APN if n is odd [11]. Especially, Gold and Kasami exponents are proved to be *maximally nonlinear* and Welch and Niho exponents are conjectured to be maximally nonlinear. Therefore the APN functions are considered as good candidates of S-boxes of block ciphers.

2.3 Algebraic Attacks on Block Ciphers

The algebraic attack is to make algebraic equations relating the initial key bits and the output bits, and find the initial key by solving the equations. Courtois *et al.* introduced a computational method to solve overdefined systems of polynomial equations called the XL algorithm [8]. Later, their method is applied to block ciphers [9]. However, it is shown that the XL algorithm is a redundant variant of F_4 algorithm that computes Gröbner basis of the ideal generated by corresponding equations [2] and its time complexity is not subexponential [10].

However, it does not imply that the *algebraic* attacks are not practical. The approaches using Gröbner basis are still hopeful. To solve a system of equations during algebraic attacks (using variants of linearization method or Gröbner basis), we need many equations with only small number of variables. Our main interest is to see how many *linearly independent* quadratic equations can be derived from a given S-box.

3. Auxiliary Lemmas

Definition 2. *Given Boolean functions $f_1, \ldots, f_m$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, they are said to be linearly independent over $\mathbb{F}_2$ if they are linearly independent as multivariate polynomials, or equivalently if $\sum_{i=1}^m a_i f_i(x) = 0$ for all $x \in \mathbb{F}_2^n$ with $a_1, \ldots, a_m \in \mathbb{F}_2$ implies $a_1 = \cdots = a_m = 0$.*

Lemma 1. *Consider two vector Boolean functions $F(x,y) : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ and $g : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. If $F(x, g(x))$ has m linearly independent components, so does $F(x,y)$ in $\mathbb{F}_2[x_1, \ldots, x_n, y_1, \ldots, y_n]$.*

Proof. Suppose that

$$F(x,y) = (f_1(x,y), \ldots, f_m(x,y))$$

has m linearly dependent components, *i.e.* there are not-all-zero $a_1, \ldots, a_m \in \mathbb{F}_2$ such that $\sum_{i=1}^m a_i f_i(x,y) = 0$. Then we have $\sum_{i=1}^m a_i f_i(x, g(x)) = 0$, which implies that $f_i(x, g(x))$'s are linearly dependent. It contradicts that $F(x, g(x))$ has m linearly independent components. Therefore $F(x,y)$ should have m linearly independent components. □

Now we show that linear independence is invariant under invertible transformations of inputs and invertible affine transformations of outputs.

Lemma 2. *Let $T : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an invertible transformation. A vector Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ has m linearly independent components over $\mathbb{F}_2$ if and only if so does $F \circ T$.*

Proof. Let $F(x) = (f_1(x), \ldots, f_m(x))$ for $x \in \mathbb{F}_2^n$. Assume $a_1, \ldots, a_m \in \mathbb{F}_2$ satisfies $\sum_{i=1}^m a_i f_i(Tx) =$

0 for all $x \in \mathbb{F}_2^n$. Since T is invertible, we have $\sum_{i=1}^m a_i f_i(y) = 0$ for all $y \in F_2^n$. Since F has m linearly independent components, we have $a_1 = \cdots = a_m = 0$, which implies the independence of m components of $F \circ T$. The converse follows from the invertibility of T. □

Lemma 3. *Let $S : \mathbb{F}_2^m \to \mathbb{F}_2^m$ be an invertible affine linear transformation. A vector Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ has m linearly independent components over $\mathbb{F}_2$ if and only if so does $S \circ F$. Further it holds for any affine transformation S if there exists $x_0 \in \mathbb{F}_2^n$ such that $F(x_0) = 0$.*

Proof. Let $S(x) = (s_1(x), \ldots, s_m(x))$ where $s_i(x) = \sum_{j=1}^m p_{ij} x_j + c_i$ for $p_{ij} \in \mathbb{F}_2$ and $c_i \in \mathbb{F}_2$. For $F = (f_1, \ldots, f_m)$, we have $S \circ F = (g_1, \ldots, g_m)$ such that $g_i = \sum_{j=1}^m p_{ij} f_j + c_i$. If there are not-all-zero $a_1, \ldots, a_m \in \mathbb{F}_2$ satisfying $\sum_{i=1}^m a_i g_i(x) = 0$, we have

$$\sum_{i=1}^m a_i \{\sum_{j=1}^m p_{ij} f_j(x) + c_i\}$$
$$= \sum_{j=1}^m \{\sum_{i=1}^m a_i p_{ij}\} f_j(x) + \sum_{i=1}^m a_i c_i = 0$$

for all $x \in \mathbb{F}_2^n$. Note that $\sum_{i=1}^m a_i c_i = 0$ if either S is linear or there exists an element $x_0 \in \mathbb{F}_{2^m}$ such that $F(x_0) = 0$. Since $f_1, \ldots, f_m$ are linearly independent, $\sum_{i=1}^m a_i p_{ij} = 0$ for all j, which implies $a_1 = \cdots = a_m = 0$ from the invertibility of the matrix (p_{ij}). Hence m components of F should be linearly independent. The converse is the same. □

Remark that if the inverse image of 0 for F is empty, Lemma 3 does not hold for an affine transformation S. For example, $F : \mathbb{F}_2^2 \to \mathbb{F}_2^3 : (x_1, x_2) \mapsto (x_1 + 1, x_2 + 1, x_1 + x_2 + 1)$ has 3 linearly independent components, but after the affine transformation $S : \mathbb{F}_2^3 \to \mathbb{F}_2^3 : (x, y, z) \mapsto (x + 1, y + 1, z + 1)$ is taken to F, $S \circ F = (x_1, x_2, x_1 + x_2)$ is not linearly independent anymore.

We also recall some useful lemmas.

Lemma 4. *Any permutation $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ has n linearly independent components.*

Proof. This is a binary version of Corollary 7.39 in [17]. □

Lemma 5. *Consider a vector Boolean function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$. If the nonlinearity of F is non-zero, F has m linearly independent components.*

Proof. This follows from the definition of nonlinearity of vector Boolean functions [20]. □

4. Obtaining Independent Quadratic Equations

From now on, we consider a polynomial over a finite field. If we fix a basis, this polynomial can be regarded as multivariate equations. Unless confused, we will consider a polynomial as multivariate equations without specifying a basis.

When we are given m quadratic equations from $F(x) = 0$, we can consider the following methods to get more quadratic equations:

1. Multiplication by linear or quadratic equations.
2. Composition with quadratic equations.
3. Substitution of quadratic terms by new variables.

4.1 Multiplications

In order to get more quadratic equations from given algebraic equations, we firstly consider multiplications of given equations by a linear monomial or a quadratic monomial.

We introduce some notation to classify exponents of monomials. We denote by a *run* a consecutive ones in the binary representation of an exponent. A point and a punctured run denote a run of length one and a run with one zero inside it, respectively. Since exponents are defined modulo $2^n - 1$ and a multiplication by two is the same with its circular shift, we consider the most significant bit is connected to the least significant bit.

Lemma 6. *A monomial x^d over $\mathbb{F}_{2^n}$ multiplied by a linear or quadratic monomial has degree at most two if and only if d has at most two runs or one point plus one punctured run.*

Proof. Let $x^d x^a = x^m$ where $1 \le wt(a), wt(m) \le 2$. That is, $d = m - a \mod 2^n - 1$. Without loss of generality, we assume that the least significant bit of a is one. We also assume that there is no position in which both a and m have one since this case can be reduced to smaller weight cases.

First we consider the case $wt(a) = 1$, that is, $a = 1$. If $m = 2^i$ for $i > 0$, $d = 2^{i-1} + \cdots + 2 + 1$ has only one run. If $m = 2^i + 2^j$ for $i > j > 0$, $d = 2^i + 2^{j-1} + \cdots + 1$ has one point plus one run.

Next we consider the case $wt(a) = 2$, that is, $a = 2^k + 1$ for $k > 0$. Assume $m = 2^i$ for $i > 0$, then d has one run or one punctured run as follows:

$$d = \begin{cases} 2^{i-1} + \cdots + 2^{k+1} + 2^{k-1} + \cdots + 2^0 & \text{if } i > k+1, \\ 2^{k-1} + \cdots + 2^0 & \text{if } i = k+1, \\ 2^{n-1} + \cdots + 2^k + 2^{i-1} + \cdots + 2^1 & \text{if } i \le k. \end{cases}$$

Assume $m = 2^i + 2^j$ with $i > j > 0$, d has one point plus one punctured run or at most two runs as follows:

$$d = \begin{cases} 2^i + 2^{j-1} + \cdots + 2^{k+1} + 2^{k-1} + \cdots + 2^0 & \text{if } j > k+1, \\ 2^i + 2^{k-1} + \cdots + 2^0 & \text{if } j = k+1, \\ 2^{i-1} + \cdots + 2^k + 2^{j-1} + \cdots + 2^0 & \text{if } i > k \geq j, \\ 2^{n-1} + \cdots + 2^k + 2^i + 2^{j-1} + \cdots + 2^1 & \text{if } k \geq i > j. \end{cases}$$

The converse is trivial. □

When a multiplier is linear or quadratic, we have more detailed results as follows:

Lemma 7. *Suppose that $n > 2$ and $k \geq 1$. Assume that the weight of d is at most two. The product x^m of two monomials x^{2^k+1} and x^d is linear or quadratic only in the following cases:*

1. *If $d = 1$, then $m = \begin{cases} 4 & \text{if } k = 1, \\ 2^k + 2 & \text{if } k \neq 1. \end{cases}$*
2. *If $d = 2^k$, then $m = 1 + 2^{k+1}$.*
3. *If $d = 3$, then $m = \begin{cases} 2^3 & \text{if } k = 2, \\ 2^k + 2^2 & \text{if } k \neq 2. \end{cases}$*
4. *If $d = 2^s + 1$ and if $k = 1$, then $m = \begin{cases} 2^3 & \text{if } s = 2, \\ 2^s + 2^2 & \text{if } s \neq 2. \end{cases}$*
5. *If $d = 2^k + 1$, then $m = 2^{k+1} + 2$.*
6. *If $d = 2^{k+1} + 2^k$, then $m = 2^{k+2} + 1$.*

Proof. It is sufficient to check the weight of $m = 2^k + 1 + d \mod (2^n - 1)$, since $x^{2^n-1} = 1$. Assume that $w(d) = 1$, i.e $d = 2^l$ for some $l < n$. Then m becomes $1 + 2^k + 2^l < (2^n - 1)$. Unless two of $\{0, k, l\}$ are equal, x^m is cubic. This covers first two cases of the lemma.

Assume that $w(d) = 2$, i.e $d = 2^l + 2^s$ for some $l < s < n$. Then m becomes $1+2^k+2^l+2^s < (2^n-1)$. If all of $\{0, k, l, s\}$ are distinct, then x^m is quartic. Hence at least two of them are equal, especially $l = 0$ or $l = k$ since $0 < k$. If $l = 0$ then

$$m = \begin{cases} 2^k + 2^2 & \text{if } s = 1, \text{ (Case 3)} \\ 2^s + 2^2 & \text{if } k = 1, \text{ (Case 4)} \\ 2^{k+1} + 2 & \text{if } s = k. \text{ (Case 5)} \end{cases}$$

If $l = k$ then s should be $k+1$ (Case 6). This completes the proof. □

4.2 Composition

Given an equation $y = x^d$, we can get $y^{d_1} = x^{dd_1}$ by composing with X^{d_1}. The equation is linear or quadratic if both of d_1 and $d_2 = dd_1$ have weight ≤ 2. That is, if d is congruent to d_2/d_1 modulo $2^n - 1$ and $wt(d_i) \leq 2$, we can get a quadratic equation by composition. For example, there are 66 values among $2^8 - 2 = 254$ exponents (resp. 49 values among $2^7 - 2 = 126$ exponents) which are represented as a ratio of integers of weight two, when $n = 8$ (resp. $n = 7$).

Note that we may consider only the case $wt(d_1) = 2$ because the composition gives only dependent equations when $wt(d_1) = 1$.

4.3 Substitution

Assume d is congruent to d_2/d_1 modulo $2^n - 1$ for d_1 and d_2 with $wt(d_i) \leq 2$. If X^{d_1} is a permutation, we can replace x by z^{d_1} by adopting a new variable z. Then we get more quadratic equations as follows:

$$\begin{cases} x = z^{d_1}, \\ y = z^{d_2}. \end{cases}$$

If d is congruent to $d = d_1 d_2$ and $wt(d_1) = 2$, then we can substitute x^{d_1} by z to get the following quadratic equations:

$$\begin{cases} z = x^{d_1}, \\ y = z^{d_2}. \end{cases}$$

In these processes, we should be careful for adding new variables. If a substitution by adopting a new variable gives too many new monomials, it does not reduce the complexity of algebraic attacks. For example, we can always obtain n more equations by adopting a new variable, but it may require additional n^2 monomials, which is not preferable.

5. Almost Perfect Nonlinear Power Functions

In this section, we investigate the linear independence of quadratic equations induced from the inverse function and APN power functions.

5.1 Inverse Exponents

First, we note that the inverse function $y = 1/x$ is equivalent to $xy = 1$ except when $x = 0$. If we fix a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, we can obtain n equations from $xy = 1$. When the identity 1 is represented by $\sum_{i=1}^n a_i\beta_i$, $a_i \in \{0, 1\}$ for a basis $\beta = \{\beta_1, \beta_2, \ldots, \beta_n\}$, $xy = 1$ gives n equations of the form $f_i(x_1, \ldots, x_n, y_1, \ldots, y_n) = a_i$, where f_i is the sum of monomials of the form $x_j y_k$. This equation is compatible with $y = 1/x$ if and only if $a_i = 0$. Hence if the basis contains 1 *i.e.* 1 has weight one when represented by the basis, then the number of equations from $y = 1/x$ is $n - 1$. When we consider the inverse power function, we assume that 1 is contained in the basis.

We count the number of linearly independent multivariate quadratic equations from $xy - 1 = 0$. A composition of $xy - 1 = 0$ with any quadratic equation gives an equation of degree larger than two. Thus we only consider a multiplication by a linear or quadratic equation:

1. The original equation: $F(x, y) = xy - 1$
2. Multiplied by x: $G_0(x, y) = x^2y - x$
3. Multiplied by x^3: $G_1(x, y) = x^4y - x^3$
4. Multiplied by y: $H_0(x, y) = xy^2 - y$

5. Multiplied by y^3: $H_1(x,y) = xy^4 - y^3$

The types and the numbers of distinct monomials that appear in the equations from F, G, and H are given in Table 3.

Table 3 The type and the number of distinct monomials from the inverse function

Eq.	XY	XX	YY	X	Y	#
F	O	–	–	–	–	n^2
G_0	O	–	–	O	–	n^2+n
H_0	O	–	–	–	O	n^2+n
G_1	O	O	–	O	–	$\frac{n(3n+1)}{2}$
H_1	O	–	O	–	O	$\frac{n(3n+1)}{2}$

In Table 3, we denote the type of monomials of x_iy_j for $0 \le i,j < n$ by XY. Similarly XX, YY, X and Y represent monomials x_ix_j, y_iy_j, x_k, and y_k for $0 \le i < j < n$ and $0 \le k < n$, respectively. The marks O (–, resp.) are used to indicate that monomials of the type given in the first entry of each column may (does not, resp.) appear in the equation. For example, the equation F does not contain any monomials except monomials of type x_iy_j for each $1 \le i,j < n$. The last column denotes the maximum number of distinct monomials that can appear in the equation.

Theorem 1. *All the above $5n$ quadratic equations induced from the inverse function are linearly independent.*

Proof. In order to show that all components produced by the above polynomials are linearly independent, it is better to look at the matrix form. Each row corresponds to the equations from $G = (G_0, G_1)$, $H = (H_0, H_1)$, and F.

$$\begin{pmatrix} M_1 & 0 & M_2 & 0 \\ 0 & M_3 & M_4 & 0 \\ 0 & 0 & M_5 & M_6 \end{pmatrix} \begin{pmatrix} x_ix_j \\ y_iy_j \\ x_iy_j \\ 1 \end{pmatrix} = 0,$$

where each M_i represents a nonzero binary matrix and each monomial in the column vector represents all monomials of similar forms (For example, x_ix_j represents all x_ix_j for $1 \le i,j \le n$.).

First we can easily see that $F(x,y)$ has n linearly independent components by Lemma 1 and Lemma 4 since $F(x,y) = xy - 1$ is a permutation for any nonzero y. Thus it is enough to show that each rank of M_1 and M_3 is $2n$ respectively. $M_1(x_ix_j)$ can be written in the more precise form:

$$M_1(x_ix_j) = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} x_i \\ x_ix_j \end{pmatrix},$$

where x_i represents $x_1, x_2, \ldots, x_n$ and x_ix_j represents all x_ix_j's with $1 \le i < j \le n$. Since $(A\ B)$ represents the coefficients of the term x in G_0, A is the identity matrix of size n and $B = 0$. Since $(C\ D)$ represents the coefficients of the term $-x^3$ in G_1, we can write $-x^3 = C(x_i) + D(x_ix_k)$. Since $C(x_i)$ is a linear function over $\mathbb{F}_2^n$, the nonlinearity of $D(x_ix_k)$ is equal to that of x^3. Therefore $D(x_ix_k)$ has n linearly independent components by Lemma 5, and so the rank of D is n. This implies that the rank of M_1 is $2n$. We can show that the rank of M_3 is also $2n$ by the similar argument. □

5.2 Gold Exponents

When $\gcd(k,n) = 1$ and $k < n/2$, 2^k+1 is called a Gold exponent [14]. Note that any quadratic monomial can be changed into a Gold power function by an affine transformation. Since the original equation consists of x^{2^k+1} and y, we can multiply only by monomials of type x^d or $x^{d_1}y^{d_2}$. In the first case, x^d should be linear so that we have $d = 1$ or $d = 2^k$ by Lemma 7. In the second case, $x^{2^k+1+d_1}$, y^{d_2}, x^{d_1}, and y^{1+d_2} should be linear so that $(d_1, d_2) = (1,1)$. For composition case, if d is 2^s, the product produces only dependent equations on the original equations. Thus the weight of d should be two. Then $m = (2^k+1)(1+2^l) = 1 + 2^l + 2^k + 2^{k+l}$ and x^m can be quadratic only if $l = k = 1$.

Hence from $y = x^{2^k+1}$, we can obtain the following multivariate quadratic equations.

1. The original equation: $F_1(x,y) = x^{2^k+1} - y$
2. Multiplied by linear equations: $F_2(x,y) = x^{2^k+2} - xy$ and $F_3(x,y) = x^{2^{k+1}+1} - x^{2^k}y$
3. Multiplied by $x^{d_1}y^{d_2}$: $F_4(x,y) = x^4y - xy^2$ only for $k = 1$
4. Composition with X^d: $F_5(x,y) = x^9 - y^3$ only for $k = 1$.

The types of distinct monomials in the equations from F_i for $1 \le i \le 5$ are summarized in Table 4.

Table 4 The types of distinct monomials from a Gold power function

When $k = 1$

Eq.	XY	XX	YY	X	Y	#
F_1	–	O	–	–	O	$\frac{n(n+1)}{2}$
F_2	O	–	–	O	–	n^2+n
F_3	O	O	–	–	–	$\frac{n(3n-1)}{2}$
F_4	O	–	–	–	–	n^2
F_5	–	O	O	–	–	$n(n-1)$

When $k > 1$

Eq.	XY	XX	YY	X	Y	#
F_1	–	O	–	–	O	$\frac{n(n+1)}{2}$
F_2	O	O	–	–	–	$\frac{n(3n-1)}{2}$
F_3	O	O	–	–	–	$\frac{n(3n-1)}{2}$

Theorem 2. *All the above $5n$ quadratic equations induced from a Gold function are linearly independent.*

Proof. We will use the matrix arguments similar to the inverse function. First, we assume that $k = 1$. We may write all $5n$ equations as the following matrix form. Each row corresponds to the equations from F_2, F_1, F_3, F_5 and F_4.

$$\begin{pmatrix} M_1 & 0 & 0 & 0 & M_2 \\ M_3 & M_4 & M_5 & 0 & 0 \\ M_6 & 0 & M_7 & 0 & M_8 \\ M_9 & M_{10} & M_{11} & M_{12} & 0 \\ 0 & 0 & 0 & 0 & M_{13} \end{pmatrix} \begin{pmatrix} x_i \\ y_i \\ x_i x_j \\ y_i y_j \\ x_i y_j \end{pmatrix} = 0,$$

where each M_i is a non-zero binary matrix.

Each of M_1, M_4, M_7, M_{12}, and M_{13} in diagonal block represents the coefficients of monomials in x^4, $-y$, x^5, y^3, and $F_4 = x^4y - xy^2$, respectively. Here x^4 and $-y$ are permutations, and x^5, y^3, and $F_4(x, ax^3) = (1-a)x^7$ for $a \neq 1$ have nonzero nonlinearity by [5]. Therefore, each of them has n linearly independent components and so each of the matrices has rank n. Thus the whole coefficient matrix has rank $5n$ and all components of the equations are linearly independent.

Next, assume that $k > 1$. Each row corresponds to the equations from F_1, F_2, and F_3.

$$\begin{pmatrix} M_1 & M_2 & M_3 & 0 \\ 0 & M_4 & M_5 & M_6 \\ 0 & M_7 & M_8 & M_9 \end{pmatrix} \begin{pmatrix} y_i \\ x_i \\ x_i x_k \\ x_i y_j \end{pmatrix} = 0,$$

where each M_i is a non-zero binary matrix.

Since M_1 represents the coefficients of monomials in $-y$, it is invertible. Thus we are enough to show that all components of F_2 and F_3 are linearly independent. Consider $F(x, y) = (F_2(x, y), F_3(x, y))$. By letting $g(x) = x^{2^k+1}+x$, we have $F(x, g(x)) = (x^2, x^{2^k+1})$. If $F(x, g(x))$ is linearly dependent, there exist nonzero c_1 and c_2 such that $\mathrm{Trace}(c_1x^2 + c_2x^{2^k+1}) = 0$ since both of x^2 and x^{2^k+1} have n linearly independent components [5]. Thus the nonlinearity of $c_2^{-1}c_1x^2 + x^{2^k+1}$ is zero, but this is a contradiction with $\gcd(k, n) = 1$. Therefore $F(x, g(x))$ has $2n$ linearly independent components by Lemma 1, and so all components of (F_2, F_3) are linearly independent. □

5.3 Kasami Exponents

When $\gcd(n, k) = 1$ and $1 < k < n/2$, $d = 2^{2k} - 2^k + 1$ is called a Kasami exponent [16]. Although Kasami exponent has the weight $k + 1$, we can express it as a ratio of two elements of weight 2 if $\gcd(2^k+1, 2^n-1) = 1$.†

$$d = \frac{2^{3k} + 1}{2^k + 1}.$$

Thus z^{2^k+1} is a permutation. So we can obtain the following quadratic equations by substituting $x = z^{2^k+1}$.

1. Substitution $x = z^{2^k+1}$
   a. $F_1(x, y, z) = x - z^{2^k+1}$
   b. $F_2(x, y, z) = y - z^{2^{3k}+1}$
2. Modification of 1.(a)
   a. $F_3(x, z) = xz - z^{2^k+2}$
   b. $F_4(x, z) = xz^{2^k} - z^{2^{k+1}+1}$
3. Modification of 1.(b)
   a. $F_5(y, z) = yz - z^{2^{3k}+2}$
   b. $F_6(y, z) = yz^{2^{3k}} - z^{2^{3k+1}+1}$

Further we can obtain another linearly independent quadratic equation by applying composition by $2^k + 1$.

4. $F_7(x, y) : y^{2^k+1} - x^{2^{3k}+1}$

However we cannot obtain any quadratic equation by multiplying $x^{d_1}y^{d_2}$ to F_3. If the product $x^{d_1+1+2^{3k}}y^{d_2} - x^{d_1}y^{d_2+1+2^k}$ is quadratic then all x^{d_1}, y^{d_2}, $x^{d_1+1+2^{3k}}$, and $y^{d_2+1+2^k}$ should be linear monomials. This contradicts Lemma 7.

The types of distinct monomials in the equations from F_i for $1 \le i \le 7$ are summarized in Table 5.

Table 5 The types of distinct monomials from Kasami power functions

Eq.	XZ	YZ	XX	YY	ZZ	X	Y
F_1	–	–	–	–	O	O	–
F_2	–	–	–	–	O	–	O
F_3	O	–	–	–	O	–	–
F_4	O	–	–	–	O	–	–
F_5	–	O	–	–	O	–	–
F_6	–	O	–	–	O	–	–
F_7	–	–	O	O	–	–	–

Theorem 3. *The $6n$ quadratic equations induced from F_i for $i = 1, 2, 3, 4, 5, 7$ are linearly independent. Moveover if $k < n/4$, then all the $7n$ equations are linearly independent.*

Proof. Since y^{2^k+1} is nonlinear, n equations from F_7 are linearly independent. In particular, XX and YY type of monomials are appeared only in F_7. Hence it is enough to show that other equations are linearly independent.

We will use matrix arguments. From Table 5, we may write $6n$ equations from F_i for $i = 1, \cdots, 6$ as the following matrix form.

$$\begin{pmatrix} M_1 & 0 & 0 & 0 & M_2 \\ 0 & M_3 & 0 & 0 & M_4 \\ 0 & 0 & M_5 & 0 & M_6 \\ 0 & 0 & M_7 & 0 & M_8 \\ 0 & 0 & 0 & M_9 & M_{10} \\ 0 & 0 & 0 & M_{11} & M_{12} \end{pmatrix} \begin{pmatrix} x_i \\ y_i \\ x_i z_j \\ y_i z_j \\ z_i z_j \end{pmatrix} = 0.$$

†Since $\gcd(n, k) = 1$, n should be odd.

Since M_1 and M_3 corresponds to x and y, they are identity matrices. We will show that the rank of (M_5, M_7) is $2n$. It corresponds to (xz, xz^{2^k}) and in F_3 and F_4 respectively. Let $G(x,z) = (xz, xz^{2^k})$. Consider $G(z^2, z) = (z^2, z^{2^k+1})$. Then it is linearly independent by the same argument of inverse function. Hence the rank of (M_5, M_7) is $2n$ by Lemma 1.

Next, consider (M_9, M_{11}) which corresponds to $(yz, yz^{2^{3k}})$ in F_5 and F_6 respectively. Let $H(y,z) = (yz, yz^{2^{3k}})$. If we take $g(z) = z^{2^k}$, then $H(g(z), z) = (z^{2^k+1}, z^{2^{3k}+2^k})$. The first term is nonlinear, hence the rank of M_9 is n. Moreover all $2n$ equations are assured to be linearly independent when $k < n/4$ by [5]. □

5.4 Welch Exponents

When $n = 2m+1$, $d = 2^m + 3$ is called a Welch exponent. Recently it is proved that the Welch power functions are almost perfect nonlinear [11], but it is still remained to be a conjecture that they are maximally nonlinear [19].

We cannot obtain any quadratic equation by composition methods except $m = 2$.

Lemma 8. *Assume that $m \geq 2$. For $1 \leq l \leq 2m$, $(2^m+3)(2^l+1) \mod (2^n-1)$ cannot have the weight at most 2 except when $m = 2$ and $l = 3$.*

Proof. Let s be the product of $(2^m+3)(2^l+1) = 2^{m+l} + 2^{l+1} + 2^l + 2^m + 2 + 1$. It is easy to show that s has the weight at least 3 for any m and l except $m = l+1$ by hand calculations.

If $m = l+1$, then $s \equiv 2^{m+2} + 2^{m+1} + 2^m + 4 < 2^n - 1$. Hence s has the weight 4 when $m > 2$. For $m = 2$, $s \equiv 1 \mod 2^n - 1$ and Welch function can be modified as $y^9 = x$ by composition methods. □

Therefore, it is sufficient to consider multiplications and substitutions to get quadratic equations except when $m = 2$.

1. Multiplication by x: $F_1(x,y) = yx - x^{2^m+4}$
2. Substitution by $z = x^3$[†]
   a. $F_2(x,y,z) = z - x^3$
   b. $F_3(x,y,z) = y - x^{2^m} z$
3. Modification of 2.(a)
   a. $F_4(x,z) = zx - x^4$
   b. $F_5(x,z) = zx^2 - x^5$
   c. $F_6(x,z) = z^2x - zx^4$
   d. $F_7(x,z) = z^3 - x^9$
4. Modification of 2.(b)
   a. $F_8(x,y,z) = yz - x^{2^m} z^2$
   b. $F_9(x,y,z) = yx^{2^m} - x^{2^{m+1}} z$
5. Composition when $m = 2$: $F_{10}(x,y) = y^9 - x$

The types of distinct monomials in the equations from F_i for $1 \leq i \leq 10$ are summarized in Table 6.

Table 6 The types of distinct monomials from a Welch power function

When $m > 2$

Eq.	XY	XZ	YZ	XX	YY	ZZ	X	Y	Z
F_1	O	–	–	O	–	–	–	–	–
F_2	–	–	–	O	–	–	–	–	O
F_3	–	O	–	–	–	–	–	O	–
F_4	–	O	–	–	–	–	O	–	–
F_5	–	O	–	O	–	–	–	–	–
F_6	–	O	–	–	–	–	–	–	–
F_7	–	–	–	O	–	O	–	–	–
F_8	–	O	O	–	–	–	–	–	–
F_9	O	–	O	–	–	–	–	–	–

When $m = 2$

Eq.	XY	XZ	YZ	XX	YY	ZZ	X	Y	Z
F_1	O	–	–	–	–	–	O	–	–
F_2	–	–	–	O	–	–	–	–	O
F_3	–	O	–	–	–	–	–	O	–
F_4	–	O	–	–	–	–	O	–	–
F_5	–	O	–	O	–	–	–	–	–
F_6	–	O	–	–	–	–	–	–	–
F_7	–	–	–	O	–	O	–	–	–
F_8	–	O	O	–	–	–	–	–	–
F_9	O	–	O	–	–	–	–	–	–
F_{10}	–	–	–	–	O	–	O	–	–

Theorem 4. *All the above $10n$ equations induced from a Welch power function are linearly independent.*

Proof. Only (F_1, F_9) contains XY type of monomials, (yx, yx^{2^m}), which are linearly independent by similar arguments of previous section. Thus $2n$ equations induced from (F_1, F_9) are linearly independent regardless of other equations.

Similarly, only (F_2, F_3, F_7, F_{10}) contains (Z, Y, ZZ, YY) type of monomials, respectively. The corresponding functions are (z, y, z^3, y^9), each of which is a permutation. Therefore it is enough to show that other $4n$ equations are linearly independent.

We may write $4n$ equations as the following matrix form. Each row corresponds to F_4, F_5, F_6, and F_8.

$$\begin{pmatrix} M_1 & 0 & M_2 & 0 & 0 \\ 0 & M_3 & M_4 & 0 & 0 \\ 0 & 0 & M_5 & 0 & 0 \\ 0 & 0 & 0 & M_6 & M_7 \end{pmatrix} \begin{pmatrix} x_i \\ x_i x_j \\ x_i z_j \\ y_i z_j \end{pmatrix} = 0.$$

Each of M_1, M_3, M_5, M_6 represents the coefficients of

[†]We may consider a substitution $z = x^{2^m+2}$ to obtain two equations $z = x^{2^m+2}$ and $y = xz$. But these two equations yield smaller number of multivariate equations than the above two equations by $z = x^3$ (Refer to Section 5.2 for Gold power function). Hence we do not consider this substitution.

monomials in $x^4, x^5, z^2x - zx^4, yz$. (M_1, M_3) has the rank $2n$ since each component is a permutation and its nonzero linear combination is nonlinear. The third and forth terms are easily shown to be linearly independent by Lemma 1. □

5.5 Niho Exponents

When $n = 2m+1$, let $m' = m/2$ if m is even, and $m' = (3m+1)/2$ otherwise. $d = 2^m + 2^{m'} - 1$ is called a Niho exponent. From a Niho power function $y = x^{2^m+2^{m'}-1}$, we can obtain quadratic equations by multiplying x:

$$F(x, y) = yx - x^{2^m+2^{m'}}.$$

Since $F(x, 0) = -x^{2^m+2^{m'}}$ is nonlinear [5], $F(x, y)$ has n linearly independent equations.

5.6 Dobbertin Exponents

When $n = 5s$, $d = 2^{4s} + 2^{3s} + 2^{2s} + 2^s - 1$ is called a Dobbertin exponent [11]. A Dobbertin exponent has the weight $s + 3$. The equation can be changed into $(yx^2)^{2^s-1} = 1$. That is, we have

$$F(x, y) = y^{2^s} x^{2^{s+1}} - yx^2.$$

Note that F is a composition of G and H: $G(t) = t^{2^s} - t$ and $H(x, y) = yx^2$. Since $H(x, 1)$ is a permutation, $H(x, 1)$ and so $H(x, y)$ have n linear independent equations by Lemma 1. Since G is an affine transformation and the inverse image of 0 by H is non-empty, F has also n linear independent equations by Lemma 3.

6. Application to Algebraic Attacks

In [9], Courtois and Pieprzyk defined the resistance against algebraic attacks as follows:

Definition 3. *Let r be the number of equations and t the number of monomials in the r equations. Then we define $\Gamma_1 = ((t-r)/n)^{\lceil (t-r)/n \rceil}$ and $\Gamma_2 = (t/n)^{\lceil t/r \rceil}$ as the resistances of the system of equations against algebraic attacks (RAA).*

The definitions of Γ_1 and Γ_2 are from Asiacrypt 2002 and the e-print version of attacks respectively in [9]. In the preliminary version of [9], two algorithms, so called *eXtended Sparse Linearization* (XSL) algorithms, for algebraic attacks against block ciphers are proposed. The first is to consider only cipher itself whatever the key schedule is, and so requires more known plaintexts. (This one is later published in Asiacrypt 2002.) The second is to utilize the key schedule and so requires less known plaintexts. As shown in Table 7, one is not always superior to the other with respect to time complexity.

Although these quantities may not be exact measures of algebraic attacks, it is true that they reflect a difficulty of solving multivariate equations in some sense. Since there are no standard measures to estimate the resistance, we will use these quantities to compare the resistance of S-boxes against algebraic attacks.

Table 7 Comparison of RAA for APN Functions and the inverse function ($*$ denotes the smallest complexity for the given type of exponents.)

When n is even

Exponent	# of rel.	# of term	(Γ_1, Γ_2) for $n = 8$
Inverse	$n-1$	n^2	$(2^{22.66}, 2^{30.0})$
	$2n-1$	n^2+n	$(2^{22.66}, 2^{15.85})$
	$3n-1$	n^2+2n	$(2^{22.66}, 2^{13.29})*$
	$4n-1$	$3n(n+1)/2$	$(2^{32.66}, 2^{15.02})$
	$5n-1$	$2n^2+n$	$(2^{46.80}, 2^{16.35})$
Gold ($k=1$)	n	$n(n+1)/2$	$(2^{7.23}, 2^{10.85})*$
	$2n$	n^2	$(2^{15.51}, 2^{12.0})$
	$3n$	$n(3n-1)/2$	$(2^{27.79}, 2^{14.09})$
	$4n$	$n(3n+1)/2$	$(2^{27.79}, 2^{14.58})$
	$5n$	$2n^2$	$(2^{38.05}, 2^{16.0})$
Gold ($k>1$)	n	$n(n+1)/2$	$(2^{7.23}, 2^{10.85})*$
	$3n$	$n(3n+1)/2$	$(2^{32.48}, 2^{18.22})$
Kasami	n	$(n^2+n)/2$	$(2^{7.23}, 2^{10.85})$
	$2n$	$(n^2+3n)/2$	$(2^{7.23}, 2^{7.37})*$
	$3n$	$(3n^2+n)/2$	$(2^{32.48}, 2^{18.22})$
	$4n$	$(3n^2+3n)/2$	$(2^{32.48}, 2^{15.02})$
Dobbertin	n	n^2	–

When n is odd

Exponent	# of rel.	# of term	(Γ_1, Γ_2) for $n = 7$
Inverse	$n-1$	n^2	$(2^{18.33}, 2^{25.27})$
	$2n-1$	n^2+n	$(2^{18.33}, 2^{15.00})$
	$3n-1$	n^2+2n	$(2^{18.33}, 2^{12.68})*$
	$4n-1$	$3n(n+1)/2$	$(2^{27.23}, 2^{14.34})$
	$5n-1$	$2n^2+n$	$(2^{36.77}, 2^{15.63})$
Gold ($k=1$)	n	$n(n+1)/2$	$(2^{4.75}, 2^{8.00})*$
	$2n$	n^2	$(2^{11.61}, 2^{11.23})$
	$3n$	$n(3n-1)/2$	$(2^{19.65}, 2^{13.29})$
	$4n$	$n(3n+1)/2$	$(2^{19.65}, 2^{10.38})$
	$5n$	$2n^2$	$(2^{28.53}, 2^{11.42})$
Gold ($k>1$)	n	$n(n+1)/2$	$(2^{4.75}, 2^{8.00})*$
	$3n$	$n(3n+1)/2$	$(2^{24.00}, 2^{13.84})$
Kasami	n	$(n^2+n)/2$	$(2^{4.75}, 2^{8.0})$
	$2n$	$(n^2+3n)/2$	$(2^{4.75}, 2^{6.97})*$
	$3n$	$(3n^2+n)/2$	$(2^{24.0}, 2^{13.83})$
	$4n$	$(3n^2+3n)/2$	$(2^{24.0}, 2^{10.75})$
Dobbertin	n	n^2	–
Welch ($m>1$)	n	$n(3n-1)/2$	$(2^{28.53}, 2^{33.22})$
	$2n$	$3n(n+1)/2$	$(2^{33.22}, 2^{21.51})$
	$5n$	$n(3n+5)/2$	$(2^{24.0}, 2^{11.10})*$
Niho	n	$(3n^2-n)/2$	$(2^{28.53}, 2^{33.22})$

Table 7 shows the comparison of the resistance of APN functions and the inverse function against algebraic attacks. From the table, we can see that the power

functions with Gold exponents and Kasami exponents have very weak resistance against algebraic attacks in both measures. The power function with Welch exponents and Niho exponents have better resistance than the inverse function.

Acknowledgement

This work was supported by Korea Research Foundation Grant (KRF-2004-003-C00034).

References

[1] Advanced Encryption Standards, `http://csrc.nist.gov/CryptoToolkit/aes/`

[2] G. Ars, J.-C. Faugère, H. Imai, M. Kawazoe, and M. Sugita, "Comparison Between XL and Gröbner Basis Algorithms," *Proc. of Asiacrypt 2004*, LNCS 3329, Springer-Verlag, pp. 338-353, 2004.

[3] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," *Journal of Cryptology*, Vol. 4, pp. 3-72, 1991.

[4] E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.

[5] J. Cheon and S. Chee, "Nonlinearity of Boolean Functions and Hyperelliptic Curves," *SIAM J. on Discrete Math*, Vol. 16, No. 3, pp. 354-365, 2003.

[6] J. Cheon and D.H. Lee, "Resistence of S-boxes against Algebraic Attacks," *Proc. of FSE 2004*, LNCS 3017, Springer-Verlag, pp. 83-93, 2004.

[7] N. Courtois, "Higher Order Correlation Attacks, XL Algorithm and Cryptanalysis of Toyocrypt," *Proc. of ICISC 2002*, LNCS 2587, Springer-Verlag, pp. 182-199, 2002. An updated version is available at http://eprint.iacr.org/2002/087/

[8] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, "Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations," *Proc. of Eurocrypt 2000*, LNCS 1807, Springer-Verlag, pp. 392-407, 2000.

[9] N. Courtois and J. Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations," *Proc. of Asiacrypt 2002*, LNCS 2501, Springer-Verlag, pp. 267-287, 2002. The preliminary version is available at http://eprint.iacr.org/2002/044.

[10] C. Diem, "The XL-Algorithms and a Conjecture from Commutative Algebra," *Proc. of Asiacrypt 2004*, LNCS 3329, Springer-Verlag, pp. 323-337, 2004.

[11] H. Dobbertin, "Almost Perfect Nonlinear Power Functions on $GF(2^n)$: The Welch Case," *IEEE Trans. Inform. Theory*, Vol. 45, No. 4, pp. 1271-1275, 1999.

[12] H. Dobbertin, "Almost Perfect Nonlinear Power Functions on $GF(2^n)$: A New Case for n Divisbible by 5," *Proc. of the Fifth Conference on Finite Fields and Applications*, Augsburg 1999, Springer-Verlag, pp. 113-121, 2001.

[13] P. Ekdahl and T. Johansson, "A New Version of the Stream Cipher SNOW," *Proc. of SAC 2002*, LNCS 2595, Springer-Verlag, pp. 47-61, 2002. Submitted to ISO/IEC FCD 18033-4, IT Security techniques - Encryption algorithms - Part 4: Stream ciphers, 2004.

[14] R. Gold, "Maximal Recursive Sequences with 3-valued Recursive Cross-correlation Functions," *IEEE Trans. Inform. Theory*, Vol. IT-14, pp. 154-156, 1968.

[15] P. Haukes and G. Rose, "Rewriting Variables: The Complexity of Fast Algebraic Attacks on Stream Ciphers," *Proc. of Crypto 2004*, LNCS 3152, Springer-Verlag, pp. 390-406, 2004.

[16] T. Kasami, "The Weight Enumerators for Several Classes of Subcodes of the Second Order Binary Reed-Muller Codes," *Infor. Contr.*, Vol. 18, pp. 369-394, 1971.

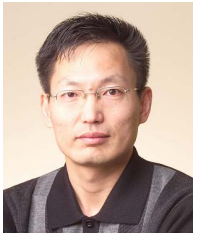
[17] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and Its Applications, Vol. 20, Cambridge University Press, 1983.

[18] M. Matsui, "Linear Cryptanalysis Method for DES cipher," *Proc. of Eurocrypt'93*, LNCS 765, Springer-Verlag, pp. 386-397, 1993.

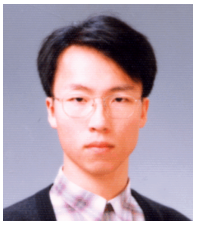
[19] Y. Niho, "Multi-valued cross-correlation functions between two maximal linear recursive sequences," Ph.D. dissertation, 1972.

[20] K. Nyberg, "On the construction of highly nonlinear permutations," *Proc. of Eurocrypt'92*, LNCS 658, Springer-Verlag, pp. 92–98, 1993.

[21] D. Watanabe, S. Furuya, H. Yoshida, K. Takaragi, and B. Preneel, "A New Key Stream Generator MUGI," *Proc. of FSE 2002*, LNCS 2365, Springer-Verlag, pp. 179-194, 2002.



Jung Hee Cheon received his B.S., M.S., and Ph.D. degrees in mathematics from Korea Advanced Institute of Science and Technology (KAIST) in 1991, 1993, and 1997, respectively. For three years from 1997, he worked for Electronics and Telecommunication s Research Institute (ETRI). In 2000 he held postdoc position in Brown university working with J. Silverman. After working as an assistant professor in Information and Communications University (ICU) for two years, he joined to Seoul National University (SNU) in 2003. His research interests include elliptic curve cryptography, Non-abelian group cryptography, Boolean functions, and cryptographic protocols.



Dong Hoon Lee received his the B.S. degree in mathematical education from Seoul National University in 1994. He also received the M.S. and the Ph. D degrees in mathematics from Korea Advanced Institute of Science and Technology(KAIST) in 1996 and 2000 respectively. From 2000 to 2002, he had worked at Cryptography & Network Security Center of Future systems Inc. Since 2002 he has been with National Security Research Institute(NSRI) as a senior research member. His interests include number theory, cryptography, and cryptanalysis.