JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **22**, No. 4, December 2009

ON SECURE BINARY SEQUENCES GENERATED BY A FUNCTION $f(x) = x + (g(x)^2 \vee C) \mod 2^n$

Min Surp Rhee*

Abstract. Invertible transformations over n-bit words are essential ingredients in many cryptographic constructions. When n is large (e.g., $n = 64$) such invertible transformations are usually represented as a composition of simpler operations such as linear functions, S-P networks, Feistel structures and T-functions. Among them we will study T-functions which are probably invertible transformation and are very useful in stream ciphers. In this paper we will show that $f(x) = x + (g(x)^2 \vee C) \mod 2^n$ is a permutation with a single cycle of length 2^n if both the least significant bit and the third significant bit in the constant C are 1, where $g(x)$ is a T-function.

1. Introduction

Let $\mathbb{B}^n = \{(x_{n-1}, x_{n-2}, \cdots, x_1, x_0) | x_i \in \mathbb{B}\}$ be the set of all n-tuples of elements in $\mathbb{B}$, where $\mathbb{B} = \{0, 1\}$. Then an element of $\mathbb{B}$ is called a **bit** and an element of $\mathbb{B}^n$ is called an n-**bit word**. An element x of $\mathbb{B}^n$ can be represented as $([x]_{n-1}, [x]_{n-2}, \cdots, [x]_1, [x]_0)$, where $[x]_{i-1}$ is the i-th component from the right end of x. In particular, the first component $[x]_0$ of x is called the **least bit** of x. It is often useful to express an n-bit word x as an element $\sum_{i=0}^{n-1} [x]_i 2^i$ of $\mathbb{Z}_{2^n}$. In this expression every element x of $\mathbb{B}^n$ is considered as an element of $\mathbb{Z}_{2^n}$ and the set $\mathbb{B}^n$ as the set $\mathbb{Z}_{2^n}$, where $\mathbb{Z}_{2^n}$ is the congruence ring modulo 2^n. For example, an element $(0, 1, 1, 0, 1, 0, 0, 1)$ of $\mathbb{B}^8$ is considered as an element 105 in $\mathbb{Z}_{2^8} = \mathbb{Z}_{256}$. In this paper we consider the following binary operations defined on $\mathbb{B}^n$ in Definition 1.1.

Received October 05, 2009; Revised November 06, 2009; Accepted November 11, 2009.

2000 Mathematics Subject Classification: Primary 94A60.

Key words and phrases: T-function, n-bit words, period, a single cycle property, cryptographic scheme.

*The present research was conducted by the research fund of Dankook University in 2008.

DEFINITION 1.1. For any n-bit words $x = (x_{n-1}, x_{n-2}, \cdots, x_0)$ and $y = (y_{n-1}, y_{n-2}, \cdots, y_0)$ of $\mathbb{B}^n$, we define the following :

(1) $x \pm y$ and xy are defined as $x \pm y \mod 2^n$ and $xy \mod 2^n$, respectively.

(2) $x \oplus y$ is defined as $(z_{n-1}, z_{n-2}, \cdots, z_0)$, where $z_i = 0$ if $x_i = y_i$ and $z_i = 1$ if $x_i \neq y_i$.

(3) $x \vee y$ is defined as $(z_{n-1}, z_{n-2}, \cdots, z_0)$, where $z_i = 0$ if $x_i = y_i = 0$ and $z_i = 1$ otherwise.

(4) $x \wedge y$ is defined as $(z_{n-1}, z_{n-2}, \cdots, z_0)$, where $z_i = 1$ if $x_i = y_i = 1$ and $z_i = 0$ otherwise.

A function $f : \mathbb{B}^n \to \mathbb{B}^n$ is said to be a $\mathbf{T}-$**function**(short for a triangular function) if the k-th bit of an n-bit word $f(x)$ depends only on the first k bits of an n-bit word x. In particular a function $f : \mathbb{B}^n \to \mathbb{B}^n$ is said to be a **parameter** if the k-th bit of an n-bit word $f(x)$ depends only on the first $k-1$ bits of an n-bit word x.

EXAMPLE 1.2. *Let* $f(x) = x + (x^2 \vee 1)$. *If* $x = \sum_{i=0}^{n-1} [x]_i 2^i$, *then* $x^2 = [x]_0 + ([x]_1^2 + [x]_0[x]_1)2^2 + \cdots$, *and we have*

$$[f(x)]_0 = [x]_0 + [x]_0 \vee 1$$
$$[f(x)]_1 = [x]_1$$
$$[f(x)]_2 = [x]_2 + [x]_1 + [x]_0[x]_1$$
$$\vdots$$
$$[f(x)]_i = [x]_i + \alpha_i, \ \ \textit{with } \alpha_i \textit{ as a function of } [x]_0, \cdots, [x]_{i-1}$$
$$\vdots$$

Hence $f(x)$ *is a T-function. For any given word* $f(x)$ *we can find* $[x]_0, [x]_1, \cdots, [x]_{n-1}$ *in order. Therefore* $f(x)$ *is an invertible T-function.*

Let $a_0, a_1, \cdots, a_n, \cdots$ be a sequence of numbers(or words) in $\mathbb{Z}_{2^n}$. If there is the least positive integer r such that $a_{i+r} = a_i$ for each nonnegative integer i, then the sequence $a_0, a_1, \cdots, a_n, \cdots$ is called to have a **cycle of length** r. In general $a_i, a_{i+1}, \cdots, a_{i+r-1}$ is called a **cycle of length** r for each i.

Now, for any function $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$, let's define $f^i : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ by

$$f^i(x) = \begin{cases} x & \text{if } i = 0 \\ f(f^{i-1}(x)) & \text{if } i \geq 1 \end{cases}$$

Note that if f is a bijective T-function then so does f^i for each i. An element(or word) α of $\mathbb{Z}_{2^n}$ is said to have a **cycle of length** r in f if r

is the least positive integer such that $f^r(\alpha) = \alpha$. From the definition of a cycle of length r, if a word α has a cycle of period r and $\alpha_i = f^i(\alpha)$, then α generates a cycle $\alpha = \alpha_0, \alpha_1, \cdots, \alpha_{r-1}$ of length r. Also, in this case every $\alpha_i (0 \leq i \leq r-1)$ has a cycle of length r. In particular, a word which has a cycle of length 1 is called **a fixed word**. That is, an element α of $\mathbb{Z}_{2^n}$ in f is a fixed word if $f(\alpha) = \alpha$. Also, f is said to have **a single cycle property** if there is a word which has a cycle of length 2^n for every positive integer n. In this case every word of $\mathbb{Z}_{2^n}$ has a cycle of length 2^n.

Consider a sequence of words

$$\alpha_0 = f^0(\alpha) = \alpha,\ \alpha_1 = f(\alpha), \cdots, \alpha_i = f^i(\alpha), \cdots, \alpha_m = f^m(\alpha), \cdots$$

where a word α of $\mathbb{Z}_{2^n}$ has a cycle of length r in f. Then the r words

$$\alpha_0 = f^0(\alpha) = \alpha,\ \alpha_1 = f(\alpha), \cdots, \alpha_i = f^i(\alpha), \cdots, \alpha_{r-1} = f^{r-1}(\alpha)$$

is repeated in the sequence $\alpha_0, \alpha_1, \cdots, \alpha_n, \cdots$. Since we may think a word as n bits, we may consider that a word α of $\mathbb{Z}_{2^n}$ which has a cycle of length r in f generates a binary sequence of period $n \cdot 2^r$. Hence a T-function f that has a single cycle property generates a binary sequence of period $n \cdot 2^n$, which is the longest period in f. This sequence may be considered as a secure sequence.

EXAMPLE 1.3. *Let $f(x) = 2x^2 + x$ be a function on $\mathbb{Z}_{16}$. Then $f(0) = 0$ and $f(8) = 8$ imply that 0 and 8 are fixed words in f. Note $f(2) = 10$ and $f(10) = 2$. Hence 2 is a word which has a cycle of length 2. Note $f(1) = 3, f^2(3) = 5, \cdots, f^8(15) = 1$. Hence 1 is a word which has a cycle of length 8. Hence a word 1 in $\mathbb{Z}_{16}$ generates a binary sequence of period $8 \cdot 4$ in f. That is, '1 3 5 7 9 11 13 15' is a sequence of words, which may be represented as a binary sequence*

0001 0011 0101 0111 1001 1011 1101 1111

Note every word of a cycle $\{1, 3, 5, \cdots, 15\}$ has a cycle of length 8. Also, by a simple calculation we know that a function $f(x) = x+1$ in $\mathbb{Z}_{16}$ has a single cycle property.

The following three propositions can be easily proved. The proof may be found in [2].

PROPOSITION 1.4. *If a function $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ has a single cycle property, then $\mathbb{Z}_{2^n} = \{f^i(x) | i \in \mathbb{Z}_{2^n}\}$ for each $x \in \mathbb{Z}_{2^n}$. In particular, $\mathbb{Z}_{2^n} = \{f^i(0) | i \in \mathbb{Z}_{2^n}\}$. Consequently, f is an invertible function on $\mathbb{Z}_{2^n}$.*

Proposition 1.5. *Let f be an invertible T-function on $\mathbb{Z}_{2^n}$. Then for each cycle in f of length l on $\mathbb{Z}_{2^k}$, there are either two cycles of length l or one cycle of length $2l$ on $\mathbb{Z}_{2^{k+1}}$. Consequently, every cycle in f on $\mathbb{Z}_{2^n}$ is of length 2^i for some $i \leq n$.*

Proposition 1.6. *A function $f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ has a single cycle property if and only if $f^{2^{n-1}}(0) = 2^{n-1}$ mod 2^n and $f^{2^n}(0) = 0$ mod 2^n.*

It is well known that the function $f(x) = x(2x + 1) \bmod 2^n$ is used in RC6, which is one of 5 candidate algorithms that was chosen in the second test of AES(advanced encryption standard). But the number of fixed words in f is $2^{[\frac{n+1}{2}]}$, where $[x]$ is the greatest integer which is not greater than $[x]$, and the number of words of period 2 in f is $2^{[\frac{n}{2}]}$ if n is even and 0 if n is odd. Hence this function is very unsuitable for PRNG(pseudo random number generator). In this sense a function which has a single cycle property is important for PRNG. Let $C \in \mathbb{Z}_{2^n}$ be a given constant. Then the function f defined by $f(x) = x + (x^2 \vee C)$ mod 2^n is invertible if the least significant bit of C is 1. Furthermore, f has a single cycle property if both the least significant bit and the third significant bit of C are 1[2]. In the next section we generalize this fact.

2. Main Theorem

Throughout this section, we are given constant $C \in \mathbb{Z}_{2^n}$ and assume that g is a T-function on $\mathbb{Z}_{2^n}$ and f is a function defined by $f(x) = x + (g(x)^2 \vee C) \mod 2^n$. In this section we show that f has a single cycle property if both the least significant bit and the third significant bit of C are 1. Our main theorem is described in Theorem 2.1 below :

Theorem 2.1. *Let $f(x) = x + (g(x)^2 \vee C) \mod 2^n$ be a function, where $g(x)$ is a bijective T-function. Then :*

(1) If $[C]_0 = 1$, then $f(x)$ is invertible.

(2) If $[C]_0 = [C]_2 = 1$, then $f(x)$ has a single cycle property.

Now, we will prove Theorem 2.1 by using a series of propositions.

Proposition 2.2. *Let $f(x) = x + (g(x)^2 \vee C) \mod 2^n$ be a function, where $g(x)$ is a T-function. Then :*

(1) If $[C]_0 = 1$, then $f(x)$ is invertible.

(2) If $g(x)$ is a parameter, then $f(x)$ is invertible.

(3) If $f(x)$ is invertible and $[g(x)]_0 = [x]_0 + [D]_0$ with D as a constant, then $[C]_0 = 1$.

Proof. (1) Note that $[f(x)]_0 = [x+(g(x)^2 \vee C)]_0 = [x]_0+[g(x)^2 \vee C]_0 = [x]_0 + 1$, and $[f(x)]_i = [x + (g(x)^2 \vee C)]_i = [x]_i + [g(x)^2 \vee C]_i = [x]_i + \gamma$ for every $i = 1, 2, \cdots, n$, where γ is a parameter as shown in Example 1.2. Hence $f(x)$ is invertible.

(2) The assertion immediately follows from (1).

(3) If $[C]_0 = 0$, then $[f(x)]_0 = [x]_0 + [x]_0 + [D]_0 = [D]_0$. Hence f is not invertible. Hence $[C]_0 = 1$. □

Let z_i be the probability of $'0'$ in bit i of x^2 for a random x in $\mathbb{Z}_{2^n}$. That is, $z_i = \frac{1}{2^n}\big|\{x \in \mathbb{Z}_{2^n} : [x^2]_i = 0\}\big|$. It is easy to show that $z_i = \frac{1}{2^{i+1}}\big|\{x \in \mathbb{Z}_{2^{i+1}} : [x^2]_i = 0\}\big|$. Then we will show the value of z_i in the next proposition.

PROPOSITION 2.3. *From the above notation we get* $z_0 = \frac{1}{2}, z_1 = 1$ *and* $z_i = \frac{1}{2}(1 + 2^{-[\frac{i}{2}]})$ *for every integer* $i \geq 2$.

Proof. By the definition of z_i we easily get $z_0 = \frac{1}{2}$ and $z_1 = 1$. Let's directly calculate z_2 and z_3 as follows :

$$z_2 = \frac{1}{2^3}\Big|\{x \in \mathbb{Z}_{2^3} : [x^2]_2 = 0\}\Big| = \frac{6}{2^3} = \frac{1}{2}(1 + 2^{-1}) = \frac{1}{2}\left(1 + 2^{-[\frac{2}{2}]}\right),$$
$$z_3 = \frac{1}{2^4}\Big|\{x \in \mathbb{Z}_{2^4} : [x^2]_3 = 0\}\Big| = \frac{12}{2^4} = \frac{1}{2}(1 + 2^{-1}) = \frac{1}{2}\left(1 + 2^{-[\frac{3}{2}]}\right)$$

Hence $z_i = \frac{1}{2}\big(1 + 2^{-[\frac{i}{2}]}\big)$ holds for $i = 2$ and $i = 3$. Let's assume $z_k = \frac{1}{2}\big(1 + 2^{-i}\big)$ for $k = 2i$ and $k = 2i + 1$. Now, we will show $z_k = \frac{1}{2}\big(1 + 2^{-(i+1)}\big)$ for $k = 2i + 2$ and $k = 2i + 3$. Note

$$\begin{aligned}\big|\{2x \in \mathbb{Z}_{2^{2i+3}} : [4x^2]_{2i+2} = 0\}\big| &= \big|\{x \in \mathbb{Z}_{2^{2i+2}} : [x^2]_{2i} = 0\}\big| \\ &= 2^{2i+2} \cdot z_{2i} \\ &= 2^{2i+1}(1 + 2^{-i})\end{aligned}$$

and

$$\begin{aligned}\big|\{2x + 1 \in \mathbb{Z}_{2^{2i+3}} : [(2x + 1)^2]_{2i+2} = 0\}\big| &= \big|\{x \in \mathbb{Z}_{2^{2i+2}} : [x^2 + x]_{2i} = 0\}\big| \\ &= 2^{2i+1}\end{aligned}$$

since $[x^2]_{2i}$ is independent of $[x]_{2i}$. Hence we get

$$\begin{aligned} z_{2i+2} &= \frac{1}{2^{2i+3}}\big|\{x \in \mathbb{Z}_{2^{2i+3}} : [x^2]_{2i+2} = 0\}\big| \\ &= \frac{1}{2^{2i+3}}\{\big|\{2x \in \mathbb{Z}_{2^{2i+3}} : [4x^2]_{2i+2} = 0\}\big| \\ &\quad + \big|\{2x+1 \in \mathbb{Z}_{2^{2i+3}} : [(2x+1)^2]_{2i+2} = 0\}\big|\} \\ &= \frac{1}{2^{2i+3}}\{2^{2i+1}(1+2^{-i}) + 2^{2i+1}\} \\ &= \frac{1}{2}\big(1+2^{-i-1}\big). \end{aligned}$$

Similarly we get

$$\begin{aligned} z_{2i+3} &= \frac{1}{2^{2i+4}}\big|\{x \in \mathbb{Z}_{2^{2i+4}} : [x^2]_{2i+3} = 0\}\big| \\ &= \frac{1}{2^{2i+4}}\{\big|\{2x \in \mathbb{Z}_{2^{2i+4}} : [4x^2]_{2i+3} = 0\}| \\ &\quad + |\{2x+1 \in \mathbb{Z}_{2^{2i+4}} : [(2x+1)^2]_{2i+3} = 0\}|\} \\ &= \frac{1}{2^{2i+4}}\{2^{2i+2}(1+2^{-i}) + 2^{2i+2}\} \\ &= \frac{1}{2}\big(1+2^{-i-1}\big). \end{aligned}$$

Therefore Proposition 2.3 holds. □

Proposition 2.4. *If* $\sigma = \sum_{j=0}^{2^{n-1}-1} (j^2 \vee C)$ *mod* 2^n, *then* $[\sigma]_{n-1} = 1$.

Proof. Note that

$$x \vee 2^i = \begin{cases} x & : [x]_i = 1 \\ x + 2^i & : [x]_i = 0 \end{cases} \quad \text{and} \quad j^2 \vee C = j^2 + \sum_{i:[C]_i=1 \wedge [j^2]_i=0} 2^i.$$

Hence we get

$$\sigma = \sum_{j=0}^{2^{n-1}-1} (j^2 \vee C) \bmod 2^n = \sum_{j=0}^{2^{n-1}-1} j^2 + 2^{n-1} \sum_{j:[C]_j=1} 2^j z_j \bmod 2^n.$$

Since $\frac{1}{6}\{2^{2n-1} + 2^{2n-2}\} = 2^{2n-3} \equiv 0 \bmod 2^n$ for all $n \geq 3$, we get

$$\begin{aligned}\sum_{j=0}^{2^{n-1}-1} j^2 &= \frac{1}{6}(2^{n-1} - 1)2^{n-1}(2^n - 1)\\ &= \frac{1}{6}\{2^{3n-2} - 2^{2n-1} - 2^{2n-2} + 2^{n-1}\}\\ &\equiv \frac{1}{6}\{2^{3n-2} + 2^{n-1}\} \bmod 2^n.\end{aligned}$$

So $\sigma \equiv \frac{1}{6}\{2^{3n-2} + 2^{n-1}\} + 2^{n-1} \sum_{j:[C]_j=1} 2^j z_j \bmod 2^n$. Note that

$$\begin{aligned}\frac{4^n}{3} = \frac{1}{3}(3+1)^n &\equiv \left[\binom{n}{n} + \binom{n}{n-1} + \cdots + \binom{n}{1}\right] + \frac{1}{3} \bmod 2\\ &\equiv \binom{n}{n} + \binom{n}{n-1} + \cdots + \binom{n}{0} - \binom{n}{0} + \frac{1}{3} \bmod 2\\ &\equiv (1+1)^n - 1 + \frac{1}{3} \bmod 2\\ &\equiv \frac{4}{3} \bmod 2.\end{aligned}$$

Hence we get

$$\begin{aligned}[\sigma]_{n-1} &\equiv \frac{1}{6}\{2^{2n-1} + 1\} + \sum_{j:[C]_j=1} 2^j z_j \bmod 2\\ &\equiv \frac{4^{n-1}}{3} + \frac{1}{6} + \frac{1}{2} + 1 \bmod 2\\ &\equiv 1 \bmod 2.\end{aligned}$$

Therefore, Proposition 2.4 holds. □

PROPOSITION 2.5. *Theorem 2.1 (2) holds.*

Proof. Suppose that $[C]_0 = [C]_2 = 1$. We show that f has a single cycle modulo 2^3. Since $g(x)^2$ is one of $0, 1$ and 4 modulo 8, $f(x) = x + (g(x)^2 \vee C) = x + C \bmod 2^3$. Hence f has a single cycle modulo 2^3. Now, by induction we show that f has a single cycle modulo 2^n. Note that the length of every cycle in any T-permutation is of the form 2^k for some nonnegative integer k. Hence it suffices to show $[f^{2^{n-1}}(x)]_n = [x]_{n-1} + 1$ to prove that the length of a cycle is 2^n. We will show this by induction. Now, let's assume that f has only one cycle for $n-1$. Consider the following sequence :

$$\begin{aligned}
&x_0,\\
&x_1 = f(x_0) = x_0 + (g(x_0)^2 \vee C),\\
&x_2 = f(x_1) = x_1 + (g(x_1)^2 \vee C) = x_0 + (g(x_0)^2 \vee C) + (g(x_1)^2 \vee C)\\
&\quad\vdots\\
&x_{2^{n-1}} = f(x_{2^{n-1}-1}) = x_0 + \sum_{i=0}^{2^{n-1}-1} (g(x_i)^2 \vee C)
\end{aligned}$$

Then $\{x_i \bmod 2^{n-1} \mid i = 0, 1, 2, \cdots, 2^{n-1}-1\}$ is just a permutation $\mathbb{Z}_{2^{n-1}} = \{0, 1, 2, \cdots, 2^{n-1}-1\}$. That is

$$\{x_i \bmod 2^{n-1} \mid i = 0, 1, 2, \cdots, 2^{n-1}-1\} = \mathbb{Z}_{2^{n-1}}.$$

Since $[g(x)^2]_{n-1}$ does not depend on $[x]_{n-1}$, the set $\{g(x_i)^2 \bmod 2^{n-1} \mid i = 0, 1, 2, \cdots, 2^{n-1}-1\}$ is the same as $\{(x_i \bmod 2^{n-1})^2 \bmod 2^n \mid i = 0, 1, 2, \cdots, 2^{n-1}-1\}$. So we get $f^{2^{n-1}}(0) \bmod 2^n = \sum_{j=0}^{2^{n-1}-1} (j^2 \vee C) \bmod 2^n$. Hence it follows from Proposition 2.4 that $[\sigma]_{n-1} = f^{2^{n-1}}(0) \bmod 2^n = \sum_{j=0}^{2^{n-1}-1} (j^2 \vee C) \bmod 2^n$. That is, $[f^{2^{n-1}}(x)]_n = [x]_{n-1} + 1$. Therefore, by Proposition 1.6 has a single cycle modulo 2^n. □

It follows from above main theorem that we get various secure binary sequences of a period $n \cdot 2^n$ depending on a choice of $g(x)$. As a special case of Theorem 2.1 when $g(x) = x$, we consider the function f whose properties are well stated in the following corollary.

COROLLARY 2.6. *Let $f(x) = x + (x^2 \vee C)$ mod 2^n be a function. Then :*

(1) f is invertible if and only if $[C]_0 = 1$,

(2) f has a single cycle property if and only if $[C]_0 = [C]_2 = 1$.

Proof. (1) To show $[C]_0 = 1$, assume $[C]_0 = 0$. Then $[f(x)]_0 = [x]_0 + [x]_0 = 0$, and f is not invertible. Hence $[C]_0 = 1$. The converse of this follows from Proposition 2.2.

(2) If $[C]_0 = [C]_2 = 1$, then it follows from Proposition 2.5 that f has a single cycle property. Conversely, suppose that f has a single cycle property. Then by (1) $[C]_0 = 1$. To show $[C]_2 = 1$, assume $[C]_2 = 0$. Then $C \equiv 1 \bmod 8$ or $C \equiv 3 \bmod 8$. In both cases $f(x) = x + (x^2 \vee 1) \bmod 2^n$ and $f(x) = x + (x^2 \vee 3) \bmod 2^n$, we get $f^4(0) = 0$ from direct

calculation. So f does not have a single cycle property, which is a contradiction. Hence $[C]_2 = 1$. Therefore Corollary 2.6 holds. □

References

[1] Jin Hong, Dong Hoon Lee, Yongjin Yeom and Daewan Han, *A New Class of Single Cycle T-functions*, FSE 2005, LNCS 3557, 68-82, 2005.

[2] A Kilmov and A. Shamir, *A New Class of Invertible Mappings*, CHES 2002, LNCS 2523, 470-483, 2003.

[3] A Kilmov and A. Shamir, *Cryptographic Applications of T-Functions*, SAC 2003, LNCS 3006, 248-261, 2004.

[4] A Kilmov and A. Shamir, *New Cryptographic Primitives Based on Multiword T-Functions*, FSE 2004, LNCS 3017, 1-15, 2004.

[5] M.S Rhee, *On a characterization of T-functions with one cycle property*, J. of the Chungcheong Math. Soc. **21** (2008), no. 2, 259-268.

[6] R. Rivert, M. Robshaw, R. Sidney and Y. L. Yin, *The RC6 block cipher*, Available from http://www.rsa.com/rsalabs/rc6/.

*

Department of Mathematics
Dankook University
Cheonan 330-714, Republic of Korea
E-mail: msrhee@dankook.ac.kr