J. Math. Univ. Tokushima
Vol.39 (2005), 7-21

Maps $R : Z/nZ \longrightarrow Z/n^2Z$ and Some Cryptographic Applications

By
Hiroharu YASUI and Shin-ichi KATAYAMA

Kurayoshi-higashi High School, Kurayoshi, Tottori, 682-0812, JAPAN
and
Department of Mathematical and Natural Sciences, Faculty of Integrated Arts and Sciences, The University of Tokushima, Tokushima 770-8502, JAPAN
e-mail address : hiroharu1979@yahoo.co.jp
: katayama@ias.tokushima-u.ac.jp

(Received September 30, 2005)

Abstract

In his master thesis [8], the first author has studied the RSA signatures with several types of redundancy functions. In this paper, we shall introduce these redundancy functions and investigate arithmetic properties of these redundancy functions and the signatures with these redundancy functions.

2000 Mathematics Subject Classification. Primary 11N45; Secondary 11A07, 94A62

Introduction

The purpose of this paper is to generalize the digital signatures with redundancy functions introduced in [8] and investigate arithmetic properties of these redundancy functions and the signatures with these redundancy functions.

Firstly, we briefly describe the RSA signature scheme. Let n be the product of randomly chosen distinct large primes p and q. Then the message space and the cipher text space for the RSA public-key encryption scheme are both Z/nZ. The RSA signature scheme can be created by reversing the roles of the encryption and the decryption as follows.

We denote Alice's public key and secret key by e and d, respectively. Note that the public key and the secret key satisfy $ed \equiv 1 \ mod \ \varphi(n)$. Here φ is the

Euler's φ function and satisfies $|(Z/nZ)^\times| = \varphi(n)$.
Alice can sign any message $m \in (Z/nZ)^\times$ by applying her secret key d

$$s \equiv m^d \in (Z/nZ)^\times.$$

Bob can check the signature by applying Alice's public key e, i.e.,

$$s^e \equiv m^{de} \equiv m \ mod \ n.$$

We will explain the reason why this is a signature. By raising the randomly looking number to the power e, one may recover the plain text m. Hence s can be considered to the eth root of m and computing eth roots of an integer $m \ mod \ n$ without the knowledge of d is infeasible. Since Alice is the only one who knows d, Bob can verify that Alice must have computed s and thereby signed m. We note that any one who knows Alice's Public key (n, e) can also verify this signature s.

Though the original idea of the RSA signature is the one described as above, there are a number of possible attacks. We explain here some of those attacks.

Firstly, we shall explain the *existential forgery*. Oscar chooses $s \in (Z/nZ)^\times$ and claims that s is a RSA signature of Alice. If $m = s^e \ mod \ n$ is a meaningful text, one believes that Alice has signed m. This is called an *existential forgery*.

Another attack comes from the fact RSA is multiplicative. Let $m_1, m_2 \in (Z/nZ)^\times$ and their signatures are $s_1 \equiv m_1^d \ mod \ n$ and $s_2 \equiv m_2^d \ mod \ n$. Put $m = m_1 m_2 \ mod \ n$. Then

$$s = s_1 s_2 \equiv m_1^d m_2^d = (m_1 m_2)^d \equiv m^d \ mod \ n.$$

Thus s is the signature of the message m. This is called a *multiplicative attack*.

There are two known methods to protect from these attacks. The first one is to use the *hash function h* and the second one is to use the *redundancy function*

$$R : Z/nZ \longrightarrow Z/nZ.$$

In order to protect from the *multiplicative attack*, it is important that the redundancy function R is not multiplicative. Moreover it should be expected R satisfies the following property.

For any $x, y \in Z/nZ$,

$$R(x)R(y) \not\equiv R(z) \ mod \ n \ \text{ for any } z \in Z/nZ.$$

In [1] 11.2.5, a redundancy function based on the binary expansion of x $(0 < x < n)$ was proposed. It seems that two attacks described above no longer work for the signature with this redundancy function, but we could not verify it mathematically.

Thus, instead of these usual redundancy functions $R : Z/nZ \longrightarrow Z/nZ$, the first author introduced other redundancy functions

$$R : Z/nZ \longrightarrow Z/n^2Z$$

and studied the security of the signatures with these new redundancy functions. In the following, we shall introduce these redundancy functions and study the arithmetic properties of these redundancy functions.

1. Redundancy functions R_k and arithmetical properties

In the following, we shall introduce several redundancy functions and investigate the fundamental properties of these redundancy functions.
Let k be any fixed natural number ≥ 2. We shall introduce a redundancy function $R_k : \{0, 1, \cdots, n-1\} \to \{0, 1, \cdots, n^k - 1\}$ by putting

$$R_k : w \mapsto R_k(w) = \overbrace{w \circ w \circ \cdots \circ w}^{k}.$$

Here, for any $0 \leq w < n$, we denote $wn^{k-1} + wn^{k-2} + \cdots + w \ mod \ n^k$ by

$$w \circ w \circ \cdots \circ w.$$

In the following, we shall consider the conditions of (x, y) when $R_k(x)R_k(y) \equiv R_k(z)$ for some z. Firstly, we shall show it is rare to occur $R_2(x)R_2(y) \equiv R_2(z)$. Finally, we shall show that $R_k(x)R_k(y) \not\equiv R_k(z)$ for any $k \geq 3$.

Consider the case when n is any natural number and $k = 2$. It is obvious that $(0 \circ 0)(x \circ x) = 0 \circ 0$ for any $x \in \boldsymbol{Z}/n\boldsymbol{Z}$. Thus, in the following, we shall restrict ourselves to non-trivial cases $0 < x, y < n$.
We call

(x, y) $(1 \leq x, y < n)$ has the *double structure*

if

$$(x \circ x)(y \circ y) \equiv z \circ z \ \ mod \ n^2 \ \text{ for some } z.$$

Then we have the following fundamental lemma.

Lemma 1. *(x, y) has the double structure if and only if*

$$x \cdot y = an + n - a, \quad \textit{with some } a \ (0 < a < n).$$

Proof. Put $x \cdot y = an + b$ $(0 \leq a, b < n)$. Then we have

$$\begin{aligned}(xn + x)(yn + y) &= xy(n^2 + 2n + 1) \\ &= (an + b)(n^2 + 2n + 1) \\ &\equiv (an + b)(2n + 1) \ mod \ n^2 \\ &\equiv (a + 2b)n + b \ \ mod \ n^2.\end{aligned}$$

Then

$$\begin{aligned}(x,y) \text{ has the double structure} &\iff a+2b \equiv b \mod n \\ &\iff a+b \equiv 0 \mod n.\end{aligned}$$

Since $0 < a+b \leq 2n-2$, we have

$$n|(a+b) \iff a+b=n.$$

Thus we have shown

$$(x,y) \text{ has the double structure} \iff a+b=n.$$

Thus we have completed the proof.

Let G be the multiplicative group of residues modulo $n-1$, i.e., $(Z/(n-1)Z)^{\times}$. If any x with $1 \leq x < n$ satisfies $x|n$, then we see that $x \cdot (n/x) = n \equiv 1 \mod (n-1)$. Hence we can define a subset H of G by putting

$$H = \{x \mod n \mid 1 \leq x < n \text{ with } x|n\}.$$

We note that $|G| = \varphi(n-1)$ and $|H| = d(n)-1$, where φ is the Euler's function and d is the divisor function.

Lemma 2. *(x,y) has the double structure if and only if*

$$x \not| n \text{ and } y \equiv x^{-1} \mod (n-1).$$

Proof. From Lemma 1, we know that (x,y) has the double structure if and only if $xy = an+n-a$ with $0 < a < n$. We see $an+n-a = a(n-1)+n \equiv 1 \mod (n-1)$. Thus we know if (x,y) has the double structure, then $y \equiv x^{-1} \mod (n-1)$. Moreover $a \neq 0$ implies $x \not| n$.

Conversely, assume $x \in G-H$ and put $y \equiv x^{-1} \mod (n-1)$ with $0 < y < n$. Then one can write

$$xy = b(n-1)+1 = bn-b+1 = (b-1)n+n-(b-1) \quad \text{with some } 0 \leq b < n.$$

From the assumption $x \notin H$, we see $x \not| n$, i.e., we have $b \neq 0, 1$. Thus we have $0 < b-1 < n$, which means that (x,y) has the double structure. Hence we have shown

$$\begin{aligned}&(x,y) \text{ has the double structure} \\ \iff\ & x \in G-H \text{ and } y \equiv x^{-1} \mod (n-1) \\ \iff\ & x \not| n \text{ and } y \equiv x^{-1} \mod (n-1).\end{aligned}$$

Let $K(n)$ be the number of the pairs (x,y) with $0 < x, y < n$ which have the double structure. Then, from the above lemmas, $K(n)$ equals to the number of

the elements contained in the set $G - H$. Hence we have shown the following theorem.

Theorem 1.

$$K(n) = \varphi(n-1) - d(n) + 1.$$

We note that we can estimate the security of the RSA signature with the redundancy function R_2 from the multiplicative attack by estimating the ratio of the following numbers:

$$\frac{\text{the number of the pairs } (x,y) \text{ which has the double structure}}{\text{the number of all the pairs } (x,y)} = \frac{K(n)}{(n-1)^2}.$$

In the following, we shall show

$$\frac{K(n)}{(n-1)^2} \longrightarrow 0, \quad \text{as } n \longrightarrow \infty.$$

More precisely, we shall show

$$\frac{\log(K(n))}{\log(n-1)} \longrightarrow 1, \quad \text{as } n \longrightarrow \infty.$$

Firstly, we have to estimate $\varphi(n-1)$. It is obvious that for any $n > 2$, $\varphi(n-1) < n-1$. Moreover one can easily show the following:

Lemma 3. (Hatalová and T. Šalát [3]) *For any* $n \geq 4$,

$$\frac{\log 2}{2} \times \frac{n-1}{\log(n-1)} < \varphi(n-1) < n-1$$

Proposition 1. $K(n)$ *satisfies the following inequality*

$$\begin{aligned} K(n) &> \frac{(n-1)\log 2}{2\log(n-1)} - 2\sqrt{n} \\ &> \frac{(n-1)\log 2}{4\log(n-1)} \qquad (n > 11688) \end{aligned}$$

Proof. Firstly we note the smaller one of the divisor a of n must satisfies the inequality $a \leq \sqrt{n}$. Thus we know

$$d(n) - 1 < 2\sqrt{n}.$$

Next, we shall show $\dfrac{(n-1)\log 2}{4\log(n-1)} > 2\sqrt{n} \quad (n > 11688)$.

We define a function $f(n)$ by putting

$$f(n) = \frac{(n-1)\log 2}{4\log(n-1)} - 2\sqrt{n}$$

$$= \frac{(n-1)\log 2 - 8\sqrt{n}\log(n-1)}{4\log(n-1)}.$$

Put

$$g(n) = (n-1)\log 2 - 8\sqrt{n}\log(n-1).$$

Then

$$\begin{aligned} g'(n) &= \log 2 - \frac{4\log(n-1)}{\sqrt{n}} - \frac{8\sqrt{n}}{n-1} \\ &\to \log 2 > 0 \quad (n \to \infty). \end{aligned}$$

Now we can easily verify $f(11687) = -0.00553\cdots, f(11688) = 0.00173\cdots$ and $f'(n) > 0$ for $n > 11688$. Thus we have completed the proof.

From this proposition, for any $n > 11688$, we have

$$\log(K(n)) > \log(n-1) - \log\log(n-1) + \log\log 2 - \log 4.$$

Since it is obvious that $\log(K(n)) < \log(n-1)$, we have shown the security of the RSA signatures with this redundancy function R_2 against the multiplicative attack as follows.

Theorem 2.

$$\lim_{n\to\infty} \frac{\log K(n)}{\log(n-1)^2} = \frac{1}{2}.$$

Finally we shall consider the cases $k > 2$. Assume $0 < x, y < n$ satisfies

$$R_{k+1}(x)R_{k+1}(y) \equiv R_{k+1}(z) \ mod\ n^{k+1} \text{ for some } z\ (0 < z < n).$$

Then, from the fact $R_{k+1}(x) \equiv R_k(x) \ mod\ n^k$, (x, y) also satisfies

$$R_k(x)R_k(y) \equiv R_k(z) \ mod\ n^k.$$

Now we shall show the following lemma.

Lemma 4. *For any $0 < x, y, z < n$, we have*

$$R_3(x)R_3(y) \not\equiv R_3(z) \ mod\ n^3.$$

Proof. Assume, on the contrary

$$R_3(x)R_3(y) \equiv R_3(z) \ mod \ n^3 \text{ for some } z.$$

Then

$$R_2(x)R_2(y) \equiv R_2(z) \ mod \ n^2.$$

Hence, from Lemma 1, x, y satisfies $xy = an + n - a$ with some a $(0 < a < n)$. Therefore

$$\begin{aligned} R_3(x)R_3(y) &= (an+n-a)(n^2+n+1)^2 \equiv (an+n-a)(3n^2+2n+1) \\ &\equiv (n-a+1)n^2 + (n-a)n + n - a \\ &\equiv (n-a+1) \circ (n-a) \circ (n-a) \ mod \ n^3. \end{aligned}$$

We see that $(n-a+1) \circ (n-a) \circ (n-a) \neq z \circ z \circ z$, which completes the proof.

From this lemma and the relations of R_k and R_{k+1} described as above, we see

$$R_k(x)R_k(y) \not\equiv R_k(z) \ mod \ n^k \text{ for any } k \geq 3.$$

Thus we have shown:

Theorem 3.

$$R_k(x)R_k(y) \not\equiv R_k(z) \ mod \ n^k, \ \textit{for any } k \geq 3.$$

Remark 1. If we use the RSA signature with the redundancy function R_3, it takes about 27 times to generate and verify this signature compared to the usual signature. But we think this RSA signature is of interest, because, from this theorem, the multiplicative attack can no longer be applied to this signature.

2. On the structure of $K(n)$ and H

In this section, we shall consider the arithmetic properties of $K(n)$ and H more precisely. Though we don't use this property later, we think it is worth for studying the structure of H here. Firstly, we shall consider the special case $n = 2^r$. Here we shall give a table of the numbers $K(2^r)$ for small r.

r	$(2^r-1)^2$	$K(2^r)$
2	9	0
3	49	3
4	225	4
5	961	25
6	3969	30
7	16129	119
8	65025	120
9	261121	423
10	1046529	590
11	4190209	1925
12	16769025	1716
13	67092481	8177
14	268402689	10570
15	1073676289	26985
16	4294836225	32752
17	17179607041	131053

Table 1: Calculations of the number $K(2^r)$ using UBASIC86

From this table, we see $r|K(2^r)$ for small r. Actually, we can show $K(2^r)$ has the following property.

We shall define the maps σ and σ^{-1} on $K(2^r)$ by putting

$$\sigma = \begin{cases} x \longmapsto 2x & (1 \leq x \leq 2^{r-1}-1) \\ x \longmapsto 2(x-2^{r-1})+1 & (2^{r-1} \leq x \leq 2^r-1) \end{cases}$$

$$\sigma^{-1} = \begin{cases} y \longmapsto \dfrac{y}{2} & (y = 2k, k \in N) \\ y \longmapsto \dfrac{y-1}{2} + 2^{r-1} & (y = 2k+1, k \in N) \end{cases}$$

Since

$$\sigma(x)\sigma^{-1}(y) = xy,$$

we can define a map $\tilde{\sigma}$ on $K(2^r)$, by putting

$$\tilde{\sigma} : (x, y) \longmapsto (\sigma(x), \sigma^{-1}(y)).$$

Example of $\tilde{\sigma}$ for the case $r = 6$.

$$\begin{array}{ccccc} & & \overset{\tilde{\sigma}}{} & & \\ & & (000101, 100110) & \to & (001010, 010011) \\ & \overset{\tilde{\sigma}}{\nearrow} & & & \searrow \tilde{\sigma} \\ (100010, 001101) & & & & (010100, 101001) \\ & \tilde{\sigma} \nwarrow & & \tilde{\sigma} & \swarrow \tilde{\sigma} \\ & & (010001, 011010) & \leftarrow & (101000, 110100) \end{array}$$

In [8], the first author proved this map has the order r using only the elementary argument, i.e., he proved that, for any $0 < d(1) < d(2) \leq r$,

$$\tilde{\sigma}^{d(1)}((x, y)) \neq \tilde{\sigma}^{d(2)}((x, y))$$

and

$$\tilde{\sigma}^{r}((x, y)) = (x, y).$$

In this paper, we shall give another proof based on the structure of the group G. From the definition, we see that, for any $n = 2^r$,

$$H = \{x \bmod n (= 2^r) | 1 \leq x < n \text{ and } x | n\} = \{1, 2, 4, \ldots, 2^{r-1} \bmod 2^r\}.$$

Thus H is the subgroup $\langle 2 \rangle$ of $G = (\boldsymbol{Z}/n\boldsymbol{Z})^{\times}$ for this case $n = 2^r$. We can verify the map $\tilde{\sigma}$ on $K(2^r)$ is nothing but dividing the set $G - H$ into the cossets of H in G. Since $|H|(=$ the order of 2 mod $2^r) = r$, we have shown $r | K(2^r)$.

Let ℓ be a prime. Consider the case $n = \ell^r$. Then, in the same way as above, we see $H = \langle \ell \rangle < G$ and $|H|(=$ the order of ℓ mod $\ell^r) = r$ and $r | K(\ell^r)$.

Conversely, we shall show that $H < G$ implies $n = \ell^r$ for some prime ℓ. Assume $H < G$. Let ℓ be the smallest prime which divides n. From the condition $\ell | n$, we see $\ell \bmod n \in H$. The assumption $H < G$ implies any powers of $\ell \bmod n$ must be contained in H. If n is not the power of primes, then there exist $r > 0$ with $\ell^r | n$ but $\ell^{r+1} \nmid n$ and $\ell^{r+1} < n$. Thus $\ell^{r+1} \bmod n \notin H$, which is the contradiction.

Therefore we have shown the following theorem.

Theorem 4. *With the above notation,*

$$H < G \Longleftrightarrow n = \ell^r \text{ with some prime } \ell.$$

Moreover, we have $r | K(\ell^r)$.

3. Other redundancy functions

In the following, we shall investigate other redundancy functions. Let t be a fixed non-negative integer. We define a redundancy function $R_{(t \circ 1)}$ by putting

$$R_{(to1)} : \{0, 1, \cdots, n-1\} \to \{0, 1, \cdots, n^2 - 1\} \ , \ w \mapsto R_{(to1)}(w) = t \cdot w \circ w.$$

Here we denote $twn + w \ mod \ n^2$ by $tw \circ w$. We shall call

$$(x, y) \text{ has the } (t \circ 1) \textit{ structure}, \text{ if}$$

$$R_{(to1)}(x)R_{(to1)}(y) \equiv R_{(to1)}(z) \ mod \ n^2 \ \text{ for some } z \ (0 < z < n).$$

Let $K_{(to1)}(n)$ be the number of the elements (x, y) which have the $(t \circ 1)$ structure. Let us denote $xy = an + b$ with $0 \leq a, b < n$, then we see

$$R_{(to1)}(x)R_{(to1)}(y) \equiv (an + b)(2tn + 1) \equiv (a + 2tb)n + b \ mod \ n^2.$$

Thus

$$(x, y) \text{ has the } (t \circ 1) \text{ structure} \Longleftrightarrow a + tb \equiv 0 \ mod \ n.$$

Since $0 < a, b < n$, we see

$$a + tb \equiv 0 \ mod \ n \Longleftrightarrow a + tb = n, 2n, \ldots, tn.$$

Thus we can estimate

$$K_{(to1)}(n) \leq tn$$

and

$$\limsup_{n \to \infty} \frac{\log(K_{(to1)}(n))}{\log(n-1)^2} \leq \frac{1}{2} \ \text{ for any fixed } t.$$

We note that the redundancy function R_2 investigated in Section 1 is the special case $R_{(1o1)}$. In general, we have the following weak but generalized results.

Theorem 5. *With the above notation, we have*

$$\limsup_{n \to \infty} \frac{\log(K_{(to1)}(n))}{\log(n-1)^2} \leq \frac{1}{2},$$

In [8], the first author investigated the cases $t = 2$ and 3 more precisely and conjectured that, for any odd n,

$$\lim_{n \to \infty} \frac{\log(K_{(to1)}(n))}{\log(n-1)^2} = \frac{1}{2} \quad \text{for the cases } t = 2 \text{ and } 3.$$

In the later, we shall investigate these results more precisely.

Next, we shall consider the case $t = -1$. Since we defined $R_{(to1)}$ only for non-negative t, we shall modify the definition of the map $R_{(-1o1)}$ as follows

$$R_{(-1o1)} : \{1, \cdots, n-1\} \to \{1, \cdots, n^2 - 1\}\ ,\ w \mapsto R_{(-1o1)}(w) = (n-w) \circ w.$$

We call (x, y) has the $(-1 \circ 1)$ *structure*, if

$$((n-x) \circ x)((n-y) \circ y) \equiv (n-z) \circ z \ mod\ n^2 \ \text{ for some } z\ (0 < z < n).$$

We have

$$((n-x) \circ x)((n-y) \circ y) \equiv xy(-2n+1) \equiv (a-2b)n + b \ mod\ n^2.$$

Combining this congruence relation and the condition $0 \leq a, b < n$, we see that (x, y) has the $(-1 \circ 1)$ structure if and only if

$$a - b \equiv 0 \ mod\ n \Longleftrightarrow a = b.$$

Therefore we have

$$K_{(-1o1)}(n) = \#\{(x, y) | xy = a(n+1)\ (1 \leq a < n)\}.$$

Put $d = (x, n+1)$. Then $1 < d < n+1$ and, for any d, x, y can be written $x = dx_0$ and $y = ((n+1)/d)y_0$ with unique x_0 and y_0, which satisfy

$$(x_0, (n+1)/d) = 1 \text{ and } \ 0 < y_0 < d.$$

Thus we have

$$\begin{aligned} K_{(-1o1)}(n) &= \sum_{d|(n+1),\ 1<d<n+1} \left(\#\{x_0 \mid 1 \leq x_0 < \frac{n+1}{d}, \left(x_0, \frac{n+1}{d}\right) = 1\} \right) \\ &\qquad \times (\#\{y_0 | 1 \leq y_0 < d\}) \\ &= \sum_{d|(n+1)} \varphi\left(\frac{n+1}{d}\right)(d-1) - n \\ &= \sum_{d|(n+1)} \varphi\left(\frac{n+1}{d}\right) d - \sum_{d|(n+1)} \varphi\left(\frac{n+1}{d}\right) - n \\ &= (\varphi * i)(n+1) - 2n - 1. \end{aligned}$$

Here i is the arithmetic function such that $i(k) = k$ for any natural number k, and $*$ is the convolution of the arithmetic functions φ and i. Using the obvious relation $\varphi(x)y \leq xy$, we can roughly estimate

$$\begin{aligned} K_{(-1o1)}(n) &\leq \sum_{d|(n+1)} \varphi(n+1) - 2n - 1 \\ &= d(n+1)\varphi(n+1) - 2n - 1 \\ &\leq 2\sqrt{n+1}(n+1) - 2n - 1. \end{aligned}$$

Hence we can easily show the following theorem.

Theorem 6. *With the above notation, we have*

$$\limsup_{n\to\infty} \frac{\log(K_{(-1\circ 1)}(n))}{\log(n-1)^2} \leq \frac{3}{4}.$$

Next, we shall investigate the case $t = 0$. In the same way as above, we denote

$$K_{(0\circ 1)}(N) = \#\{(x,y) \mid (0 \circ x)(0 \circ y) \equiv (0 \circ z)\}.$$

Writing $xy = an + b$ with $0 \leq a, b < n$, we see (x,y) has the $(0 \circ 1)$ structure if and only if $a = 0$. Thus we see

$$\begin{aligned} K_{(0\circ 1)}(n) &= \#\{x | xy = b \ (1 \leq b < n)\} \\ &= \sum_{1\leq b<n} d(b) \\ &= n\log n + (2\gamma - 1)n + O(\sqrt{n}). \end{aligned}$$

Here γ is the *Euler's constant* defined by

$$\gamma = \lim_{n\to\infty}(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n).$$

Therefore we have the following consequence:

Theorem 7.

$$\lim_{n\to\infty} \frac{\log K_{(0\circ 1)}(n)}{\log(n-1)^2} = \frac{1}{2}.$$

Remark 2. Let (n,e) be the public key system of Alice. Then Alice can divide the plain text into x with $x \leq \sqrt{n}$. Then Alice can define the redundancy function R of usual bit length by putting

$$R : x \mapsto 0 \circ x \ mod \ n.$$

Thus, substituting n to $\sqrt{n}$ in Theorem 7, we can estimate the security of this redundancy function R from the multiplicative attack.

Finally, we will study the redundancy function $K_{(2\circ 1)}(n)$ again. Write $xy = an + b$ with $0 < a, b < n$. Then we know that (x,y) has the $(2 \circ 1)$ structure if and only if $a + 2b = n$ or $2n$. In the following, we shall estimate $K_{(2\circ 1)}(n)$ as follows.

(I) Firstly, we shall treat the case $a + 2b = n$. Then we have

$$\begin{aligned}(2x)(2y) &= 4(an+b)\\ &= 4an + 2(n-a)\\ &= 2(2n-1)a + (2n-1) + 1\\ &\equiv 1 \ mod\ (2n-1).\end{aligned}$$

We note that $0 < 2n-1-2x\ ,\ 2n-1-2y < 2n-1$ and

$$(2n-1-2x)(2n-1-2y) \equiv 1 \ mod\ (2n-1).$$

Since $2x$ is even and $2n-1-2x$ is odd, we see the number of even numbers $0 < 2x < 2n-1$ with $(2x, 2n-1) = 1$ equals to the number of odd numbers $0 < 2y+1 < 2n+1$ with $(2y+1, 2n+1) = 1$. Thus the number of (x, y) with $(2x)(2y) \equiv 1 \ mod\ (2n-1)$ satisfies

$$\#\{(x,y) \mid (2x)(2y) \equiv 1 \ mod\ (2n-1)\} \leq \frac{\varphi(2n-1)}{2}.$$

(II) Next, we shall treat the case $a + 2b = 2n$. Then we have

$$\begin{aligned}2xy &= 2(an+b)\\ &= 2an + (2n-a)\\ &= (2n-1)a + (2n-1) + 1\\ &\equiv 1 \ mod\ (2n-1).\end{aligned}$$

Thus, in the same way as in (I), the number of the pairs (x, y) with $2xy \equiv 1 \ mod\ (2n-1)$ satisfies

$$\#\{(x,y) \mid (2x)y \equiv 1 \ mod\ (2n-1)\} \leq \frac{\varphi(2n-1)}{2}.$$

Thus we have shown $K_{(2\circ 1)}(n) \leq \varphi(2n-1)$ and proved the following theorem.

Theorem 8.

$$K_{(2\circ 1)}(n) \leq \varphi(2n-1) \leq 2(n-1) \ \textit{for any}\ n \geq 2.$$

Moreover, for any $0 < x < n$, we may expect the inverse of $2x \ mod\ (2n-1)$ distributes uniformly in the interval 0 and $2n-1$. Thus we will give the following conjecture:

Conjecture.

$$\lim_{n\to\infty} \frac{K_{(2\circ1)}(n)}{\varphi(2n-1)} = \frac{1}{2}.$$

Here we will give a table of the numbers $K_{(2\circ1)}(n)$ $(n = 2^r)$ for small r which supports this conjecture.

$n = 2^r$	$\varphi(2n-1)$	$\varphi(2n-1)/2$	$K_{(2\circ1)}(n)$
2	6	3	3
3	8	4	4
4	30	15	17
5	36	15	14
6	126	63	75
7	128	64	66
8	432	216	213
9	600	300	286
10	1936	968	999
11	1728	864	924
12	8190	4095	4093
13	10584	5292	5294
14	27000	13500	13699
15	32768	16384	16262
16	131070	65535	65661

Table 2: Calculations of $K_{(2\circ1)}(2^r)$ using UBASIC86

Remark 3. In [8], we have shown that $K_{(3\circ1)}(n)$ satisfies the analogous results as above and formulated similar conjecture for any odd n.

4. Numerical data

In the following, we shall give the numerical data to generate and verify the signature with the redundancy function R_2. We used a text m of the bit length 7.39KB and used the *Timing* of Mathematica 4.1. In the following "Normal" is the time(second) which took to generate and verify the signature s of the text m. "Redundancy" is the time(second) which took to generate and verify the signature of the text $m_1 = R_2(m)$. Let (n, e) be the RSA signature system with $ed \equiv 1 \ mod \ \varphi(n^2)$. Then We know the complexity to sign the normal text m is $O((\log n)^2 \cdot \log d)$, while the complexity to sign the text with R_2 is $O((\log(n^2))^2 \cdot \log d)$. Thus we can expect the time to generate and verify the signature with the redundancy function R_2 takes about $4 \sim 8$ times as the usual one. In practice, it took about $2 \sim 3$ times as follows.

The bit length of p and q	Generation		Verification	
	Normal	Redundancy	Normal	Redundancy
106	0.312(sec.)	0.516	0.313(sec.)	0.469
212	0.531	1.219	0.562	1.266
318	0.781	2.172	0.781	2.156
425	1.156	3.359	1.172	3.328

Table 3: Practical time to generate and verify, using Mathematica 4.1

References

[1] J. A. Buchmann, Introduction to Cryptography, Springer–Verlag, New York, 2001.

[2] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 5th ed., Oxford University Press, Oxford, 1979.

[3] H. Hatalová and T. Šalát, Remarks on two results in the elementary theory of numbers, *Acta Fac. Rer. Natur. Univ. Comenian. Math.* **20** (1969), 113-117.

[4] Y. Kida, User's Manual for UBASIC86 [8.7], Nihon-hyoronsha, Tokyo, 1994.

[5] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, New York, 1997.

[6] D. S. Mitrinović, J. Sándor and B. Cristici, Handbook of Number Theory, Kluwer Academic Publishers, Dordrecht, 1996.

[7] R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, **21**, (1978), 120-126.

[8] H. Yasui, On RSA signatures with redundancy, Master Thesis (2004) Tokushima University (in Japanese).