Binary Cyclotomic Generators

Cunsheng Ding*

Department of Mathematics
University of Turku
Fin-20500 Turku, Finland

cding@ra.abo.fi

Abstract. In this paper a number of binary cyclotomic generators based on cyclotomy are described. A number of cryptographic properties of the generators are controlled. A general approach to control the linear complexity and its stability for periodic sequences over any field is shown. Two bridges between number theory and stream ciphers have been established, and the relations between the design and analysis of some stream ciphers and some number-theoretic problems are shown. A number of cryptographic ideas are pointed out.

1 Introduction

The word *cyclotomy* means "circle-division" and refers to the problem of dividing the circumference of the unit circle into a given number, n, of arcs of equal lengths [19]. Our interest in the theory of cyclotomy has stemmed from the rather remarkable fact that the cyclotomic numbers represent actually the difference property and the nonlinearity of some cryptographic functions from residue rings Z_p's to some abelian groups. The DSC and ADSC generators described in [11] are actually the cyclotomic generators of order 2. In this paper we describe some keystream generators based on the theory of cyclotomies modulo a prime p, a square of a prime, and the product of two distinct primes. These generators are all special natural sequence generators of Figure 1 [11], where a cryptographic function $f(x)$, which is a mapping from a residue ring Z_N to an abelian group $(G, +)$, applies to the register of the modulo N ring counter. In the upper part of Figure 1, i.e., the modulo N ring counter, the $\sum_N$ denotes the integer addition modulo N, the symbol i denotes the content of the register of the counter which is updated with each clock. Thus, the register of the ring counter outputs cycles through the elements $0, 1, ..., N$ of the residue ring Z_N. That is, if the register of the counter has value i at time t, then its value at time $t+1$ is $(i+1)$ mod N, here and hereafter the x mod N is defined to be the least positive integer congruent to x modulo N. The semi-infinite sequence z^∞, i.e., the output sequence of the

* Supported partly by the Academy of Finland under Project 11281.

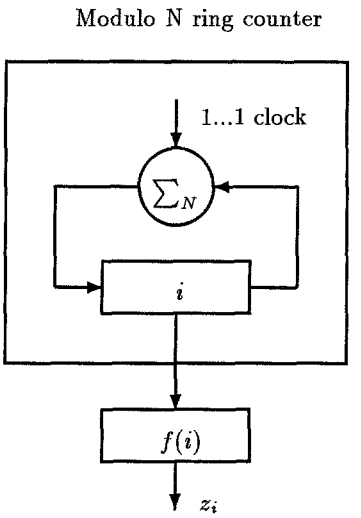

Fig. 1. The natural sequence generator

NSG, is defined by $z_i = f(i + i_0 \bmod N)$, where i_0 is the initial value of the register of the ring counter which is the key of the generator. The cryptographic function $f(x)$ and the modulus N are assumed not to be secret parameters of the generator.

For the binary natural sequence generator the following cryptographic analyses are equivalent:

1. differential analysis of the cryptographic function $f(x)$;
2. nonlinearity analysis of the cryptographic function $f(x)$;
3. autocorrelation analysis of the cryptographic function $f(x)$;
4. autocorrelation analysis of the output sequence;
5. two-bit pattern distribution analysis of the output sequence;
6. stability analysis of the mutual information $I(i;\ z_i z_{i+t-1})$, here and hereafter z^∞ denotes the output sequence of the NSG.
7. transdensity analysis of the additive stream cipher system with this NSG as the keystream generator by which we mean the analysis of the probability of agreement between two encryption resp. decryption transformations specified by two encryption resp. decryption keys [11].

By equivalence we mean one analysis results in another analysis.

We now prove the equivalences between the above seven analyses and show that an ideal difference property of the cryptographic function $f(x)$, by which we mean that the difference parameters defined below are approximately the same, ensures automatically an ideal nonlinearity of the cryptographic function $f(x)$, an ideal autocorrelation property of $f(x)$, an ideal autocorrelation property of the output sequence z^∞, an ideal two-bit pattern distribution property of

the output sequence z^{∞}, and an ideal balance between the mutual information $I(i;\ z_i z_{i+t-1})$ for all possible $(z_i, z_{i+t-1}) \in Z_2 \times Z_2$, where t is arbitrary. In what follows Z_N denotes the residue ring modulo an integer N.

Consider now the NSG of Figure 1. Assume that $(G,+)$ is the abelian group over which the keystream sequence is constructed, and $|G| = n$. For each $i \in G$ let $C_i = \{x \in Z_N : f(x) = i\}$. The ordered set $\{C_0, C_1, \cdots, C_{n-1}\}$ is called the *characteristic class*. For any ordered partition $\{C_0, C_1, \cdots, C_{n-1}\}$ of Z_N, there exists a function $f(x)$ with this partition as its characteristic class. The differential analysis of the system is the analysis of the following *difference parameters*:

$$d_f(i,j;w) = |C_i \cap (C_j + w)|, (i,j) \in G \times G,\ w \in Z_N.$$

There are some elementary facts about these difference parameters [11], which represent some conservations between the difference parameters.

To see why the analysis of the difference parameters can be regarded as a kind of differential analyses, we take $(G,+) = (Z_2,+)$. Consider the input pairs (x,y) such that $x - y = a$, and consider the difference of the corresponding output pairs. Then we have the following expressions

$$\begin{aligned} \frac{|\{(x,y): f(x)-f(y)=1,\ x-y=a\}|}{|\{(x,y): x-y=a\}|} &= \frac{d_f(0,1;a)}{N} + \frac{d_f(1,0;a)}{N} \\ \frac{|\{(x,y): f(x)-f(y)=0,\ x-y=a\}|}{|\{(x,y): x-y=a\}|} &= \frac{d_f(0,0;a)}{N} + \frac{d_f(1,1;a)}{N}, \end{aligned}$$

These two expressions show that the difference parameters can be regarded as partial differentials or directional differentials of the function $f(x)$.

In what follows we prove the equivalences between the above seven analyses for the binary NSG (natural sequence generator).

Equivalence between differential and nonlinearity analyses: The nonlinearity analysis of the cryptographic function $f(x)$ refers to the analysis of the probability $p(f(x+a) - f(x) = b)$. It can be easily seen

$$\begin{aligned} Np(f(x) - f(y) = 1) &= d_f(0,1;a) + d_f(1,0;a), \\ Np(f(x) - f(y) = 0) &= d_f(0,0;a) + d_f(1,1;a) \end{aligned} \tag{1}$$

and

$$\begin{aligned} 2d_f(0,0;-a) &= |C_0| - |C_1| + Np(f(x+a) - f(x) = 0), \\ 2d_f(1,1;-a) &= |C_1| - |C_0| + Np(f(x+a) - f(x) = 0), \\ 2d_f(1,0;-a) &= 2d_f(0,1;-a) = N - Np(f(x+a) - f(x) = 0). \end{aligned} \tag{2}$$

Then formulae (1) and (2) show the equivalence.

Equivalence between differential and autocorrelation analyses: The autocorrelation analysis of $f(x)$ refers to the analysis of the autocorrelation function

$$C_f(a) = \frac{1}{N} \sum_{x \in Z_N} (-1)^{f(x+a)-f(x)}.$$

It is easily verified

$$NC_f(a) = N - 4d_f(1, 0; a) \tag{3}$$

and

$$\begin{aligned} 4d_f(0, 0; a) &= 4|C_0| - N + NC_f(a), \\ 4d_f(1, 1; a) &= 4|C_1| - N + NC_f(a), \\ 4d_f(1, 0; a) &= 4d_f(0, 1; a) = N - NC_f(a). \end{aligned} \tag{4}$$

Combining formulae (3) and (4) proves the equivalence between differential analysis and autocorrelation analysis of $f(x)$.

The autocorrelation analysis of the output binary sequence z^∞ refers to the analysis of the autocorrelation function

$$C_z(a) = \frac{1}{N} \sum_{i \in Z_N} (-1)^{z_{i+a}-z_i}.$$

Apparently by the definition of the NSG we have

$$C_z(a) = C_f(a), \quad \text{for each } a.$$

Thus, the above formulae (3) and (4) are also true we replace $C_f(a)$ with $C_z(a)$. This fact shows the equivalence between the differential analysis and the autocorrelation analysis of the output sequence z^∞.

Equivalence between differential and two-bit pattern distribution analyses: The two-bit pattern distribution analysis of z^∞ is concerned with how the two-bit patterns are distributed in a circle of length N in the sequence. For each fixed t with $0 < t \leq N - 1$ the vector (z_i, z_{i+t}) takes on elements of $Z_2 \times Z_2$ when i runs from 0 to $N-1$. Let $n[(z_i, z_{i+t}) = (a, b)]$ denote the number of times with which the vector (z_i, z_{i+t}) takes on $(a, b) \in Z_2 \times Z_2$ when i runs from 0 to $N - 1$. Then we have obviously

$$n[(z_i, z_{i+t}) = (a, b)] = d_f(a, b; -t). \tag{5}$$

Thus, for the binary NSG each difference parameter represents in fact the number times a two-bit pattern appears in a circle of length N of the binary output sequence z^∞.

Equivalence between differential and mutual information analyses: Given two bits z_i and z_{i+t} of the output sequence of the binary NSG. It is cryptographically interesting to know how much information these two bits gives to the value of the register of the counter in the binary NSG at the time the output bit z_i was produced. It is easy to verify

$$I(i; z_i z_{i+t}) = \log_2 N - \log_2 d_f(z_i, z_{i+t}; -t) \cdot \text{ bits} \tag{6}$$

and

$$d_f(z_i, z_{i+t}; -t) = N 2^{-I(i; z_i z_{i+t})}, \tag{7}$$

where the mutual information $I(i; z_i z_{i+t})$ is measured in bits. Formulae (6) and (7) show clearly the equivalence. In addition they show that the difference parameters are in fact a measure of uncertainty.

Equivalence between differential and transdensity analysis: In a cipher system it is possible for two keys to determine the same encryption (resp. decryption) transformation. Even if the two transformation are distinct, it is cryptographically interesting to know the the probability of agreement between the two transformations. The control of this probability of agreement can prevent a cipher from any key approximation attack, that is, to use one key to decrypt the message encrypted by another key. Let E_k (resp. D_k) denote the encryption (resp. decryption) transformation specified by the key k. The analysis of the density (briefly, transdensity analysis) of a cipher system refers to the analysis of the probability of agreement $p(E_k(m) = E_{k'}(m))$, where m can be confined on plaintext blocks or without restriction [11].

For the additive binary stream cipher with the binary NSG as its keystream generator this probability can be expressed easily as

$$p(E_k = E_{k'}) = C_z(k - k' \bmod N) = C_f(k - k' \bmod N), \tag{8}$$

because of the additive structure of the additive stream cipher and the fact that the keystream sequences specified by all keys are shift versions of each other. Thus, the equivalence follows easily from formula (8).

So far we have proved the equivalences between differential and other six analyses. Thus, the equivalences among the seven analyses follows.

In addition, there is no tradeoff between all the above seven aspects and the linear complexity and its stability aspects for this generator (we will see this fact in later sections). This means that it is possible to design the NSG so that it has not only an ideal property for all the seven aspects in the usual senses, but also a large linear complexity and ideal linear complexity stability for the output sequence. It is because of these facts and that every periodic sequence can be produced by the natural sequence generator that the generator was called a natural one [11].

Formulae 1–8 clearly show that to ensure an ideal property for all the seven aspects, it suffices to control the difference property of the cryptographic function

$f(x)$. Thus, in what follows we will concentrate on the control of the difference property of $f(x)$, of the linear complexity, and of the sphere complexity of the output sequence of each specific NSG.

2 Cyclotomy and its cryptographic importance

The motivation of the investigation of cyclotomic numbers is related to the outstanding Waring problem, difference sets, and the solution of equations over finite fields [7, 9, 17]. Cyclotomic numbers invented by Gauss turn out to be quite valuable in the design and analysis of some keystream generators.

Let $N = df + 1$, be a odd prime and let θ be a fixed primitive element of Z_N. Denoting the multiplicative subgroup (θ^d) as D_0, we see that the coset decomposition of Z_N^* with respect to the subgroup D_0 is then

$$Z_N^* = \cup_{i=0}^{d-1} D_i,$$

where $D_i = \theta^i D_0$ for $0 \leq i \leq d-1$. The coset D_l is called the *index class* l [3] or *cyclotomic class* l [19]. Let $(l, m)_d$ denote the number of solutions (x, y) of the equation

$$1 = x - y, \quad (x, y) \in D_l \times D_m,$$

which were called *cyclotomic numbers* [2, 3, 8, 12], or equivalently,

$$(l, m)_d = |D_l \cap (D_m + 1)|.$$

Apparently, there are at most d^2 distinct cyclotomic numbers of order d and these numbers depend not only on N, d, l, m, but also on which of the $\phi(N-1)$ primitive elements of Z_N is chosen.

There are some elementary cyclotomic facts which are very important to our cryptographic applications, because they indicate several kinds of conservations between the cyclotomic numbers. They are the theoretical bases of the need of keeping the stability of local nonlinearities of some cryptographic functions.

We now see the meaning of the cyclotomic numbers from another viewpoint. From the definition we know the set $\{(l, m)_d : l = 0, 1, \cdots, d-1\}$ represents how the set $D_m + 1$ is distributed among the cyclotomic classes. Note

$$|D_l \cap (D_m + \theta^k)| = |D_{l+N-1-k} \cap (D_{m+N-1-k} + 1)|$$

for each k, we see that the d sets of numbers $\{(l, m)_d : l = 0, 1, \cdots, d-1\}$ for $m = 0, 1, \cdots, d-1$, represents also the distribution of the elements of any set $D_m + w$ with $w \neq 0$.

As seen above, cyclotomic numbers represent in fact the difference property of the partitions $\{D_0, D_1, \cdots, D_{d-1}\}$. So they should have connections with difference sets. Actually, the investigation of residue difference sets is the main motivation of the calculation of cyclotomic numbers [3, 19]. Now we see the cryptographic importance of cyclotomy.

Let the symbols as before. What we want to do now is to construct cryptographic functions from Z_N to an abelian group $(G,+)$ of d elements, where $G=\{g_0,g_1,\cdots,g_{d-1}\}$. Let

$$C_0=D_0\cup\{0\},\quad C_i=D_i,\ i=1,\cdots,d-1.$$

Without concerning the implementation problem, we define a function from Z_N to $(G,+)$ as: $f(x)=g_i$ iff $x\in C_i$.

If $i\cdot j\neq 0$, then we have

$$d_f(g_i,g_j;\theta^k)=(i+N-1-k,j+N-1-k)_d.$$

On the other hand, we have

$$d_f(g_0,g_0;\theta^k)=|(D_{N-1-k}\cup\{0\})\cap(D_{N-1-k}\cup\{0\}+1)|.$$

It follows that

$$0\le d_f(g_0,g_0;\theta^k)-(N-1-k,N-1-k)_d\le 2.$$

Similarly, we have

$$0\le d_f(g_0,g_1;\theta^k)-(N-1-k,N-k)_d\le 1.$$

and

$$0\le d_f(g_1,g_0;\theta^k)-(N-k,N-1-k)_d\le 1.$$

Thus, we arrive at the conclusion that the difference parameters are almost the same as the cyclotomic numbers.

3 A basic theorem and main bridge

Before describing some binary cyclotomic generators, we introduce the sphere complexities and show why it is necessary to control the sphere complexity for those cyclotomic sequences described later.

Let x and y be finite sequences of length n over $GF(q)$, $\mathrm{WH}(x)$ denote the Hamming weight, and $d_H(x,y)=\mathrm{WH}(x-y)$, the Hamming distance between x and y. Let $O(x,y)=\{y:\ 0<d_H(x,y)\le u\}$ be the sphere without center x. The *sphere complexity* [10] is defined by

$$\mathrm{SC}_u(x)=\min_{y\in O(x,u)}L(y).$$

here and hereafter $L(x)$ denotes the linear complexity or linear span of x.

Similarly, let s^∞ be a sequence of period N (not necessarily least period) over $GF(q)$. The sphere complexity [10] of periodic sequences is defined by

$$\mathrm{SC}_u(s^\infty)=\min_{0<v\le u}\left[\min_{\mathrm{WH}(t^N)=v,per(t^\infty)=N}L(s^\infty+t^\infty)\right],$$

where $per(t^\infty) = N$ denotes that t^∞ has a period N, and $t^N = t_0 t_1 ... t_{N-1}$.

That the control of the sphere complexity of keystream sequences for additive synchronous stream ciphers is cryptographically necessary follows from the fact that there is a polynomial-time algorithm which determines a LFSR with approximately the same output as the original keystream sequence, provided that the linear complexity of the keystream sequence has a bad stability. This algorithm can be roughly described as follows.

If the sphere complexity $\mathrm{SC}_k(s^\infty) = l$ of the binary semi-infinite sequence s^∞ is small for some very small integer k, then theoretically the sequence s^∞ can be written as

$$s^\infty = t^\infty + w^\infty,$$

where s^∞, t^∞ and w^∞ all have a period N with respect to which the sphere complexity is concerned, and $L(t^\infty) = l$, and the Hamming weight $\mathrm{WH}(w^N) \leq k$. The task of this polynomial-time algorithm is to construct a LFSR of length l which produces the sequence t^∞ or another LFSR which outputs a sequence with the probability of agreement with the original sequence s^∞ no less than $1 - k/N$.

Suppose that a cryptanalyst gets a piece of the sequence s^∞, say S. Then the piece must be written as $S = T + W$, where T and W are the corresponding pieces of the periodic sequence t^∞ and w^∞ respectively. Since the k is very small, with a very high probability, which depends on the length of S and the pattern distribution of s^∞, it holds $S = T$. In this case if the length of S is large than $2l$, then applying the Berlekamp-Massey algorithm [14] to S will give an LFSR which produces the sequence t^∞ with the probability of agreement with s^∞ being no less than $1 - k/N$.

If $S \neq T$, the Hamming weight of $S - T$ must be very small since k is very small. Then by changing a few bits in S the cryptanalyst gets T. However, he/she does not know the actual sequence $S - T$. But he/she can first get a number of sequences S_i by changing only one bit in the ith position of S for all i, in this way he/she gets m modified versions of S, where m is the length of S. Then apply the Berlekamp-Massey algorithm to each modified version to get a LFSR. After that use these LFSRs to decipher a long piece of ciphertext. If one LFSR has a probability of correct decipherment no less than $1 - k/N$, then the cryptanalyst accept this LFSR for approximating the original keystream generator. Otherwise changing two bits each time in S gives $m(m-1)/2$ modified versions of S, then apply the Berlekamp-Massey algorithm to these modified version to see whether an acceptable LFSR is obtained. If not, try to modify three bits to get $m(m-1)(m-2)/6$ versions, and apply the Berlekamp-Massey algorithm to the modified versions again. Since k is very small, the cryptanalyst must get an acceptable LFSR after repeating the procedure a number of times. Since the complexity of the Berlekamp-Massey algorithm is of order $O(m^2)$, where m is the length of the input sequence, the complexity of this approximation algorithm must be polynomial. The smaller the k, the less the complexity of this approximation algorithm. This algorithm clearly shows the importance of the

sphere complexity. It is quite clear that if $\mathrm{SC}_6(s^\infty) = l$ is small, with the above algorithm a cryptanalyst must succeed in get a LFSR with the probability of agreement with the original generator larger or equal to $1 - 6/N$.

We describe the above algorithm here in order to show the cryptographic necessity of controlling the sphere complexity for our binary cyclotomic sequences for additive stream ciphering. The necessity of controlling the linear complexity of keystreams for additive stream ciphering follows from the efficient Berlekamp-Massey algorithm. After having shown the need for controlling the linear and sphere complexity for cyclotomic sequences, we now prove some theorems which will be needed when we control these complexities for those sequences.

Basic Theorem 1 *Let $N = p_1^{e_1} \cdots p_t^{e_t}$, where $p_1, \cdots, p_t$ are t pairwise distinct primes, q a positive integer such that $\gcd(q, N) = 1$. Then for each nonconstant sequence s^∞ of period N over $GF(q)$, we have*

1. $L(s^\infty) \geq \max\{ord_{p_1}(q), \cdots, ord_{p_t}(q)\}$;
2. $SC_k(s^\infty) \geq \max\{ord_{p_1}(q), \cdots, ord_{p_t}(q)\}$, *if* $k < \min\{\mathrm{WH}(s^N), N - \mathrm{WH}(s^N)\}$,

here and hereafter $L(s^\infty)$ and $SC_k(s^\infty)$ denote the linear and sphere complexity of the sequence respectively, $\mathrm{WH}(x)$ the Hamming weight of x, and $s^N = s_0 s_1 \cdots s_{N-1}$.

Proof: Let K be a field of characteristic p, the n a positive integer not divisible by p, and ξ a primitive nth root of unity over K, the nth cyclotomic polynomial is defined by

$$Q_n(x) = \prod_{s=1, \gcd(s,n)=1}^{n} (x - \xi^s).$$

To prove the theorem, we need the following properties of the cyclotomic polynomial (see Lidl and Niederreiter [13] for proof).

1. $Q_n(x)$ is independent of the choice of ξ.
2. $\deg(Q_n(x)) = \phi(n)$.
3. The coefficients of $Q_n(x)$ belong to the prime subfield of K.
4. $x^n - 1 = \prod_{d|n} Q_d(x)$.
5. If $K = \mathrm{GF}(q)$ with $\gcd(q, n) = 1$, then Q_n factors into $\phi(n)/d$ distinct monic irreducible polynomials in $K[x]$ of the same degree d, where d is the least positive integer such that $q^d = 1 \bmod n$, i.e., d is the order (or exponent) of q modulo n, denoted as $ord(q)$ modulo n or $ord_n(q)$.

It is easily seen that $ord_{p^k}(a) \geq ord_p(a)$ for any prime p and any positive integer a with $\gcd(a, p) = 1$. By assumptions and the above basic property 5 the polynomial $x^n - 1$ is equal to the product of $\phi(n)/d$ distinct monic irreducible polynomials over $GF(q)[x]$ of the same degree d, where d is the least positive integer such that $q^d = 1 \bmod n$, i.e., d is the order (or exponent) of q modulo

n. Since the minimum polynomial of each sequence of period N over $GF(q)$ divides $x^N - 1$ and $x^N - 1 = \prod_{n|N} Q_n(x)$, we consider the orders $ord_n(q)$ for each possible divisor n of N.

If n divides N, there are integers $h_{i_1}, ..., h_{i_s}$, where $1 \leq h_{i_j} \leq e_{i_j}$ for $1 \leq j \leq s$ and $1 \leq s \leq t$, such that $n = p_{i_1}^{e_{i_1}} \cdots p_{i_s}^{e_{i_s}}$. By the Chinese Remainder Theorem and the above conclusions

$$\begin{aligned} ord_n(q) &= \text{lcm}\{ord_{p_1^{e_1}}(q), \cdots, ord_{p_t^{e_t}}(q)\} \\ &\geq \max\{ord_{p_1^{e_1}}(q), \cdots, ord_{p_t^{e_t}}(q)\} \\ &\geq \min\{ord_{p_1}(q), \cdots, ord_{p_t}(q)\}. \end{aligned}$$

Thus, the conclusions of this theorem follow. QED

One can see that the above lower bound is optimal. If $t = 1$ and $e_1 = 1$, then we have the general lower bound for sequences of a prime period. If $t = 1$, then it gives a lower bound for the linear complexity and sphere complexity of sequences with period being a prime power. Most of the theorems and corollaries in the paper are special cases of the above basic theorem, that is why we call it a basic theorem. We say that it is a bridge between number theory and stream ciphers because it makes a clear connections between the linear and sphere complexity of sequences and quite a number of number-theoretic problems such as primes of special forms (e.g., Sophie German primes, Stern primes, twin primes) and their distributions, primality testing, primitive roots and their distributions, and primitivity testing. Some of these connections will be made clear in Sections 4–7.

This basic theorem shows that it is usually quite easy to control the global linear and sphere complexities. However, it seems fairly difficult to control the local linear and sphere complexities. It is worthy to note that here we use the speciality of period to control the linear and sphere complexities, while some cryptographic functions are traditionally used to control the global linear complexity in the literature. Thus, we stress the importance of period.

4 Cyclotomic generator of order $2k$

Binary sequences with prime period are cryptographically attractive due to the following theorems about the linear and sphere complexities, which follow easily from Basic Theorem 1.

Theorem 1. *If N is prime, then for any nonconstant sequence s^∞ of period N over $GF(2)$ and over $GF(2^s \bmod N)$ with $\gcd(s, N-1) = 1$ and with $2^s \bmod N$ being a power of a prime,*

1. $L(s^\infty) \geq ord_N(2)$;
2. $SC_k(s^\infty) = \begin{cases} ord_N(2), & \text{if } k < \min\{\text{WH}(s^N), N - \text{WH}(s^N)\}; \\ 0, & \text{otherwise.} \end{cases}$

Proof: Setting $t = 1$ and $e_1 = 1$ in Basic Theorem 1 proves the theorem. QED

Theorem 2. *If $N = 4t + 1$ is prime and t is a odd prime, then for any nonconstant sequence s^∞ of period N over $GF(2)$ and over $GF(2^s \bmod N)$ with $\gcd(s, N-1) = 1$ and with $2^s \bmod N$ being a power of a prime,*

1. $L(s^\infty) = N$ *or* $N - 1$;
2. $SC_k(s^\infty) = \begin{cases} N \text{ or } N-1, & \text{if } k < \min\{\mathrm{WH}(s^N), N - \mathrm{WH}(s^N)\}; \\ 0, & \text{otherwise.} \end{cases}$

Proof: Recall that a is a primitive root modulo an integer N if and only if $\mathrm{ord}_N(a) = \phi(N)$, where $\phi(x)$ is the Euler function. Since both $N = 4t + 1$ and t are primes, it is seen that 2 is a primitive root of N. Then the conclusion of this theorem follows from Theorem 1. QED

Theorem 3. *Let $N = 4t - 1$ be a prime with t odd. If $(N-1)/2$ is prime (i.e., it is a Sophie Germain prime), then for any nonconstant sequence s^∞ of period N over $GF(2)$ and over $GF(2^s \bmod N)$ with $\gcd(s, N-1) = 1$ and with $2^s \bmod N$ being a power of a prime,*

1. $L(s^\infty) = N$ *or* $N - 1$;
2. $SC_k(s^\infty) = \begin{cases} N \text{ or } N-1, & \text{if } k < \min\{\mathrm{WH}(s^N), N - \mathrm{WH}(s^N)\}; \\ 0, & \text{otherwise.} \end{cases}$

Proof: By the special form of the prime N it is easy to see that 2 is a primitive root modulo N. Then the conclusion of this theorem follows from Theorem 1. QED

Theorem 4. *Let $N = 4t + 1$ be a prime with t odd and $t = t_1 t_2$, where t_1 and t_2 are primes. If*

$$2^{2t_1} \not\equiv -1 \bmod N, \quad 2^{2t_2} \not\equiv -1 \bmod N,$$

then for any nonconstant sequence s^∞ of period N over $GF(2^s \bmod N)$ (especially over $GF(2)$) with $\gcd(s, N-1) = 1$ and with $2^s \bmod N$ being a power of a prime,

1. $L(s^\infty) = N$ *or* $N - 1$;
2. $SC_k(s^\infty) = \begin{cases} N \text{ or } N-1, & \text{if } k < \min\{\mathrm{WH}(s^N), N - \mathrm{WH}(s^N)\}; \\ 0, & \text{otherwise.} \end{cases}$

Proof: Note that $\mathrm{ord}_N(2)$ divides $\phi(N) = N - 1 = 4t_1 t_2$ and that t_1 and t_2 are primes. It then follows by the two inequalities in the assumptions of the theorem that the order of 2 must be equal to $N - 1$. Combining this fact and Theorem 1 proves the theorem. QED

Theorem 5. *Let $N = 4t - 1$ be a prime with t odd and $2t - 1 = t_1 t_2$, where t_1 and t_2 are primes. If*

$$2^{t_1} \not\equiv -1 \bmod N, \quad 2^{t_2} \not\equiv -1 \bmod N,$$

then for any nonzero sequence s^∞ of period N over $GF(2)$ and over $GF(2^s \bmod N)$ with $\gcd(s, N-1) = 1$ and with $2^s \bmod N$ being a power of a prime,

1. $L(s^\infty) = N$ *or* $N-1$;
2. $SC_k(s^\infty) = \begin{cases} N \text{ or } N-1, & \text{if } k < \min\{\mathrm{WH}(s^N), N - \mathrm{WH}(s^N)\}; \\ 0, & \text{otherwise.} \end{cases}$

Proof: With the same arguments as in Theorem 4 we see that the order of 2 modulo N is $N-1$. Combing this fact and Theorem 1 yields the conclusion of this Theorem. QED

After having proved the above theorems, which are needed to control the linear complexity and sphere complexity of the cyclotomic sequences of order $2k$, we now describe the binary cyclotomic generator of order $2k$. Let prime $N = 2kf + 1$, and $D_0, D_1, \cdots, D_{2k-1}$ be the cyclotomic classes of order $2k$ defined as before. If we choose the mapping

$$H(x) = (i^{(N-1)/2k} \bmod N) \bmod 2$$

as the cryptographic function for the NSG of Figure 1, then we have the *binary cyclotomic generator of order* $2k$.

It is not difficult to verify that each difference parameter of the above cryptographic function $H(x)$ for the binary cyclotomic generator of order $2k$ can be expressed as the sum of k^2 cyclotomic numbers of order $2k$. Thus, if the cyclotomic numbers of order $2k$ have an ideal stability, the formulae in Section 1 show that we have an ideal property for the seven aspects described in Section 1 if k is small enough. Even if the cyclotomic numbers of order $2k$ are stable to an ideal extent, the largeness of the k may lead to a relatively bad difference property of the cryptographic function. Thus, only those generators derived from small k are cryptographically attractive.

Theorems 1–5 clearly show how to control the linear complexity and its stability for the output sequence of the binary cyclotomic generator of order $2k$. By Theorem 1, to control the linear complexity and its stability of the output sequences of the binary cyclotomic generators, it suffices to choose the prime N such that $\mathrm{ord}_N(2)$ is large enough. The best choices for the primes are Sophie Germain primes, i.e., primes p such that $2p+1$ is also a prime, and Stern primes, i.e., primes $p = 4t + 1$ with t also prime.

If $k = 1$, then it is called the *binary cyclotomic generator* of order 2. The binary cyclotomic generators of order 2 can be further classified into DSC (difference set characterized) and ADSC (almost difference set characterized) generators which correspond the cases $N = -1 \bmod 4$ and $N = 1 \bmod 4$, respectively [11]. In the case $k = 1$ the output sequence of the DSC and ADSC generators are the 0-1 version of the Legendre sequences with a slight modification of the values for $\left(\frac{pi}{p}\right)$ for $i = 0, 1, \cdots$, and a proper choosing of the prime p.

A DSC generator with a Sophie Germain prime has the following cryptographic attributes: its output sequences have maximum linear complexity by Theorem 3; best autocorrelation property by the formula for cyclotomic numbers of order 2 or the difference set property of the set $f^{-1}(1)$ and formula (3), where $f(x) = (x^{(N-1)/2} \bmod N) \bmod 2$; best linear complexity stability by Theorem 3; the cryptographic function $f(x)$ has best nonlinearity with respect to

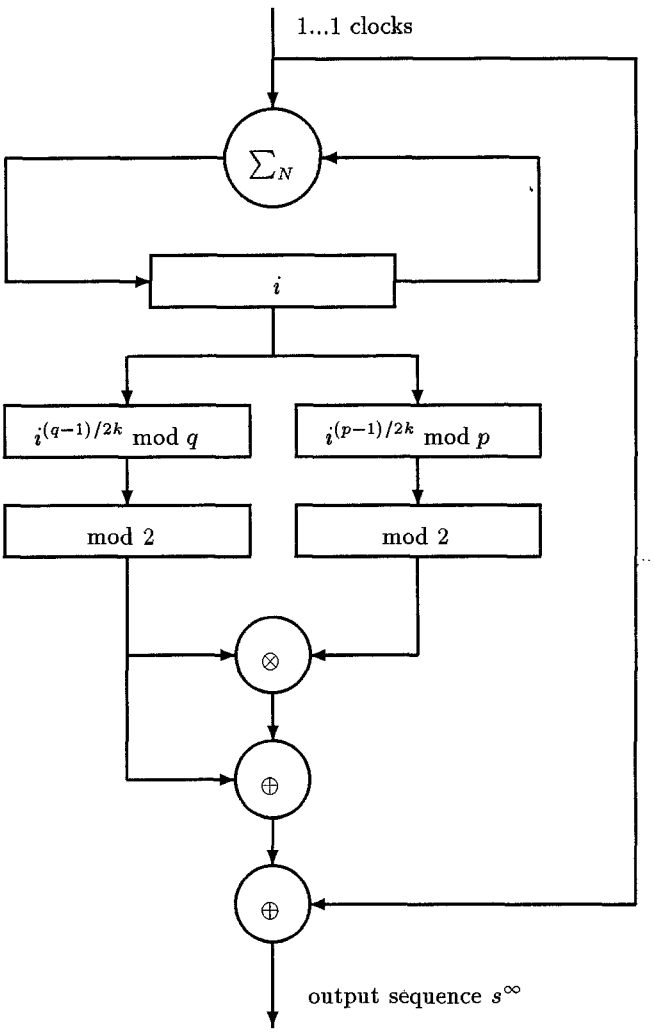

Fig. 2. The two-prime generator of order $2k$ including the twin-prime generator

the additions of Z_N and Z_2 by the difference set property of $f^{-1}(1)$ and formula (1). The ADSC generator with a Stern prime has almost the same cryptographic attributes.

5 Two-prime cyclotomic generator of order 2

Let p and q be two distinct odd primes with $\gcd(p-1, q-1) = 2$, and

$$R = \{0\}, \quad P = \{p, 2p, \cdots, (q-1)p\}, \quad Q = \{q, 2q, \cdots, (p-1)q\}.$$

Furthermore, let g be a fixed common primitive root of both primes p and q, $d = \gcd(p-1, q-1)$ and $de = (p-1)(q-1)$. Then it is proved in [21] there exits an integer x such that

$$Z_{pq}^* = \{g^s x^i : s = 0, 1, \cdots, e-1;\ i = 0, 1, \cdots, d-1\}.$$

The set Z_{pq}^* is also called the reduced residue system modulo $N = pq$. In Whiteman's generalized cyclotomy the *index class* or *cyclotomic class* D_i consists of e numbers and is defined by

$$D_i = \{g^s x^i : s = 0, 1, \cdots, e-1\}$$

and the generalized cyclotomic number $(i, j)_d$ by

$$(i, j)_d = |(D_i + 1) \cap D_j|.$$

There are d cyclotomic classes $D_0, \cdots, D_{d-1}$, which form a partition of Z_{pq}^*.

We now analyze the relation between the difference property of the partition of Z_{pq}^* and the generalized cyclotomic numbers. It is obvious that $x \in Z_{pq}^*$. Assume that the order of x modulo N is m. Then $m \geq d$. Let $w \in Z_{pq}^*$. Then there must exist two integers s and t with $0 \leq s \leq e-1$, $0 \leq t \leq d-1$ such that $w = g^s x^t$. Because $x^d = g^u$ for some fixed u such that $0 \leq u \leq d-1$, the difference parameter can be expressed as

$$\begin{aligned} d(i, j; w) &= |(D_i + g^s x^t) \cap (D_j)|,\ 0 \leq i,\ j \leq d-1;\ w \in Z_N^*, \\ &= |(D_{(m-t+i) \bmod d} + 1) \cap D_{(m-t+j) \bmod d}| \\ &= ((m-t+i) \bmod d, (m-t+j) \bmod d)_d. \end{aligned}$$

This means that for each $(i, j; w)$ with $0 \leq i, j \leq d-1$, $w \in Z_{pq}^*$, the difference parameter $d(i, j; w)$ is in fact one cyclotomic number. We will discuss the case for $w \notin Z_{pq}^*$ later.

As seen above, the index classes $D_0, \cdots, D_{d-1}$ is a partition of Z_N^*. Since

$$R = \{0\},\quad P = \{p, 2p, \cdots, (q-1)p\},\quad Q = \{q, 2q, \cdots, (p-1)q\},$$

the sets $D_0, \cdots, D_{d-1}$; R; P; Q form a partition of Z_N. To extend the partition of Z_N^* to Z_N, we have to study the difference property between the above sets. The following conclusions have been proven or are implied in [21]:

1. For any $r \in P \cup Q$, it holds

$$d(0, 1; r) = |(D_0 + r) \cap D_1| = (p-1)(q-1)/d^2. \tag{9}$$

2. For any $r \in P \cup Q$ and any $1 \leq k \leq d-1$, it holds

$$d(0, k; r) = |(D_0 + r) \cap D_k| = (p-1)(q-1)/d^2.$$

3. Let symbols as before, then

$$\begin{aligned} d(0, 0; r) &= |(D_0 + r) \cap D_0| \\ &= \begin{cases} (p-1)(q-1-d)/d^2, & r \in P, r \notin Q; \\ (q-1)(p-1-d)/d^2, & r \in Q, r \notin P. \end{cases} \end{aligned}$$

Since $x \in Z_N^*$ and $x = g^u$ for some u with $0 \le u \le d-1$, for each r we have

$$\begin{aligned} d(i,j;r) &= |(D_i + r) \cap D_j| \\ &= |x^{d-i}(D_i + r) \cap x^{d-i} D_j| \\ &= d(0, (j+d-i) \bmod d; x^{d-i} r \bmod N). \end{aligned}$$

If $r \in P$ (or Q), then $x^{d-i} \in P$ (or Q).

For the partition $D_0, \cdots, D_{d-1}$ of Z_N^* and $w \neq 0$, combining the above results we obtain

$$d(i,j;w) = \begin{cases} (p-1)(q-1)/d^2, & i \neq j,\ w \in P \cup Q; \\ (p-1)(q-1-d)/d^2, & i = j,\ w \in P,\ w \notin Q; \\ (q-1)(p-1-d)/d^2, & i = j,\ w \in Q,\ w \notin P; \\ (i',j')_d \text{ for some } (i',j'), \text{ otherwise.} \end{cases}$$

In order to put the elements of R, P, Q to some of the D_i's to get a partition of Z_N with good difference property, we need the following result proved by Whiteman [21]:

$$|D_0 \cap (Q + r)| = (p-1)/d; \quad \text{If } r \notin Q \cap R.$$

To design the two-prime cyclotomic generator of order 2, we need functions from Z_{pq} to Z_2 with good nonlinearity with respect to the additions of the two rings. Due to the inspiration of Whiteman's result, we now consider the characteristic function of the partition $\{R \cup Q \cup D_0,\ P \cup D_1\} = \{C_0, C_1\}$ of Z_{pq}. In what follows in this section we assume that $d = \gcd(p-1, q-1) = 2$. To analyze the function, we need the generalized cyclotomic numbers of order 2 obtained by Whiteman [21].

Let symbols as before. If ff' is even, we have $(0,0) = (1,0) = (1,1)$ and two different cyclotomic numbers

$$(0,0) = \frac{(p-2)(q-2)+1}{4}, \quad (0,1) = \frac{(p-2)(q-2)-3}{4}. \tag{10}$$

If ff' is odd, we have $(0,1) = (1,0) = (1,1)$ and

$$(0,0) = \frac{(p-2)(q-2)+3}{4}, \quad (0,1) = \frac{(p-2)(q-2)-1}{4}. \tag{11}$$

We now analyze the difference property of the partition $\{C_0, C_1\}$ of Z_{pq}. Note that

$$d_C(0,0;r) = |[(R+r) \cup (Q+r) \cup (D_0+r)] \cap [R \cup Q \cup D_0]|.$$

Setting

$$a(0,0;r) = |(Q+r) \cap Q| + |(Q+r) \cap D_0| + |(D_0+r) \cap Q| + |(D_0+r) \cap D_0|,$$

we can prove

$$0 \le d_C(0,0;r) - a(0,0,r) \le 2.$$

So our task now is to estimate the $a(0,0;r)$ with $r \neq 0$. One simple fact is

$$|(Q+r) \cap Q| = \begin{cases} p-2, & r \in Q; \\ 0, & r \in P \cup Z_{pq}^*; \end{cases}$$

Note that if $r \in P$, then it is possible to have $Q + r \subset D_0$. Thus, for each r we have the following two apparent facts:

$$0 \leq |(Q+r) \cap D_0| \leq p-1;$$
$$0 \leq |Q \cap (D_0+r)| \leq p-1.$$

It follows that

$$|(D_0+r) \cup D_0| \leq a(0,0;r) \leq 3p-4+|(D_0+r) \cup D_0|.$$

Setting

$$B = \max\{\frac{(p-2)(q-2)+3}{4}, \frac{(p-1)(q-3)}{4}, \frac{(p-3)(q-1)}{4}\}$$

and

$$C = \min\{\frac{(p-2)(q-2)-3}{4}, \frac{(p-1)(q-3)}{4}, \frac{(p-3)(q-1)}{4}\},$$

we get

$$C \leq a(0,0;r) \leq 3p-4+B,$$

and therefore

$$C \leq d_C(0,0;r) \leq 3p-2+B.$$

We can similarly prove that for each $r \neq 0$, it holds

$$C \leq d_C(1,1;r) \leq 3q-4+B.$$

In what follows we analyze $d_C(1,0;r)$ and $d_C(0,1;r)$. By definition we have

$$\begin{aligned} d_C(1,0;r) &= |(C_1+r) \cap C_0| = |[(P+r) \cup (D_1+r)] \cap (R \cup Q \cup D_0)| \\ &= |(P+r) \cap R| + |(P+r) \cap Q| + |(P+r) \cap D_0| \\ &\quad + |(D_1+r) \cap R| + |(D_1+r) \cap Q| + |(D_1+r) \cap D_0|. \end{aligned}$$

If $r \in P$, then by formula (9) we have

$$|(D_1+r) \cap D_0| = (p-1)(q-1)/4.$$

In addition we have apparently

$$|(P+r) \cap Q| = |(P+r) \cap D_0| = |(D_1+r) \cap R| = 0$$
$$|(P+r) \cap R| = 1, \ 0 \leq |(D_1+r) \cap Q| \leq p-1.$$

Hence, we obtain in the case $r \in P$

$$1 + \frac{(p-1)(q-1)}{4} \leq d_C(1,0;r) \leq \frac{(p-1)(q-1)}{4} + p.$$

If $r \in Q$, we can similarly prove

$$\frac{(p-1)(q-1)}{4} \leq d_C(1,0;r) \leq \frac{(p-1)(q-1)}{4} + q - 1.$$

If $r \in Z_{pq}^* \setminus P \cup Q \cup R$, then by the formulae (10) and (11) we get

$$\frac{(p-2)(q-2)-3}{4} \leq |(D_1 + r) \cap D_0| \frac{(p-2)(q-2)+3}{4}.$$

In addition we have apparently

$$\begin{aligned}
&|(P+r) \cap R| = 0 \\
&0 \leq |(P+r) \cap Q| \leq \min\{p-1, q-1\} \\
&0 \leq |(P+r) \cap D_0| \leq q-1 \\
&0 \leq |(D_1+r) \cap Q| \leq p-1 \\
&0 \leq |(D_1+r) \cap R| \leq 1.
\end{aligned}$$

It follows in this case that

$$\begin{aligned}
\tfrac{(p-2)(q-2)-3}{4} &\leq d_C(1,0;r) \\
&\leq \tfrac{(p-1)(q-1)}{4} + \min\{p-1, q-1\} + \tfrac{3}{4}(p+q) + \tfrac{1}{2}.
\end{aligned}$$

Combining the results for the three cases, we obtain

$$\frac{(p-2)(q-2)-3}{4} \leq d_C(1,0;r) \leq \frac{(p-1)(q-1)}{4} + E,$$

where

$$E = \max\{p, q-1, \min\{p-1, q-1\} + \frac{3}{4}(p+q) + \frac{1}{2}\}.$$

Similarly, one can prove

$$\frac{(p-2)(q-2)-3}{4} \leq d_C(0,1;r) \leq \frac{(p-1)(q-1)}{4} + E,$$

Summarizing the above analysis, we obtain the difference property of the above cryptographic function $F_C(x)$, as described by the following theorem.

Theorem 6. *Let*

$$a = \frac{(p-2)(q-2)-3}{4}, \quad d = \frac{(p-1)(q-1)}{4},$$

$$b = \max\{\frac{(p-2)(q-2)+3}{4}, \frac{(p-1)(q-3)}{4}, \frac{(p-3)(q-1)}{4}\}$$

and

$$c = \min\{\frac{(p-2)(q-2)-3}{4}, \frac{(p-1)(q-3)}{4}, \frac{(p-3)(q-1)}{4}\}.$$

then we have

$$\begin{aligned} c \le d_C(0,0;r) &\le 3p-2+b, \\ c \le d_C(1,1;r) &\le 3q-4+b, \\ a \le d_C(1,0;r) &\le d+E, \\ a \le d_C(0,1;r) &\le d+E, \end{aligned}$$

for each $r \not\equiv 0 \bmod N$, *where*

$$E = max\{p, q-1, \min\{p-1, q-1\} + \frac{3}{4}(p+q) + \frac{1}{2}\}.$$

This theorem tells us that if $|p-q|$ is small enough, the cryptographic function $F_C(x)$ has an ideal difference property. Thus, the other six aspects are automatically ensured due to our formulae in Section 1. In this case, the facts that $|C_0| = (p-1)(q-1)/2 + q$ and $|C_1| = (p-1)(q-1)/2 + p - 1$, show that the function has also good balance. It is called a cyclotomic generator because the difference property and the nonlinearity of the above cryptographic function depend on the generalized cyclotomy developed by Whitman.

It is not difficult to see that the characteristic function of the partition $\{C_0, C_1\}$ can be expressed by

$$F_C(j) = \begin{cases} 1, & j \in R \cup Q; \\ 0, & j \in P; \\ (1 + (\frac{j}{p})(\frac{j}{q}))/2, & \text{otherwise.} \end{cases}$$

With this cryptographic function the binary two-prime cyclotomic generator of order 2 is depicted in Figure 2, where p and q are distinct odd primes and $k = 1$, the $\otimes$ and $\oplus$ denote bit multiplication and bit-XOR operations, and the other parts have the same meanings as those of Figure 1.

On the other hand, the two primes should be chosen properly for the purpose of controlling the linear complexity and the linear complexity stability of the output sequence. In fact we have generally the following result, which is a special case of Basic Theorem 1.

Theorem 7. *Let* $N = rs$ *be a product of two distinct primes,* u *an integer with* $\gcd(u, N) = 1$. *Then for any nonconstant sequence* s^∞ *of period* N *over* $GF(u)$, *it holds*

1. $L(s^\infty) \geq \min\{ord_r(u), ord_s(u)\}$;
2. $SC_k(s^\infty) \geq \min\{ord_r(u), ord_s(u)\}$, *if* $k < \min\{\mathrm{WH}(s^N), N - \mathrm{WH}(s^N)\}$,

where $SC_k(s^\infty)$ *denotes the sphere complexity of the sequence,* $\mathrm{WH}(s^N)$ *the Hamming weight of the finite sequence,* $ord_r(u)$ *the order of* u *modulo* r.

Proof: Setting $t = 2$ and $e_1 = e_2 = 1$ in Basic Theorem 1 proves this theorem. QED

As consequences of the above theorem, we have the following corollaries:

Corollary 8. *Let* $r = 4t_1 + 1$, $s = 4t_2 + 1$, $r \neq s$. *If* r, s, t_1 *and* t_2 *are odd primes, then for any nonconstant binary sequence of period* $N = rs$,

1. $L(s^\infty) \geq \min\{r - 1, s - 1\}$
2. $SC_k(s^\infty) \geq \min\{r - 1, s - 1\}$, *if* $k < \min\{\mathrm{WH}(s^N), N - \mathrm{WH}(s^N)\}$.

Proof: Note that the proof of Theorem 2 shows that $\mathrm{ord}_r(2) = r-1$ and $\mathrm{ord}_s(2) = s - 1$, that is, 2 is a primitive root of both r and s. Combing these two facts and Theorem 7 proves this corollary. QED

Corollary 9. *Let* $r = 4r_1 - 1$, $s = 4s_1 - 1$, $(r - 1)/2$ *and* $(s - 1)/2$ *are all odd primes. If* $r > 5$ *and* $s > 5$, *then for each nonconstant binary sequence* s^∞ *of period* $N = rs$, *we have*

1. $L(s^\infty) \geq \min\{r - 1, s - 1\}$;
2. $SC_k(s^\infty) \geq \min\{r - 1, s - 1\}$; *if* $k < \min\{\mathrm{WH}(s^N), N - \mathrm{WH}(s^N)\}$.

Proof: The Proof of Theorem 3 shows that 2 is a common primitive root of r and s. Combining this and Theorem 7 yields the conclusion of this corollary. QED

Corollary 10. *Let* $r = 4r_1 + 1$, $s = 4s_1 - 1$. *If* $r, r_1, s, (s - 1)/2$ *all odd primes, then for each nonconstant binary sequence* s^∞ *of period* $N = rs$, *we have*

1. $L(s^\infty) \geq \min\{r - 1, s - 1\}$;
2. $SC_k(s^\infty) \geq \min\{r - 1, s - 1\}$; *if* $k < \min\{\mathrm{WH}(s^N), N - \mathrm{WH}(s^N)\}$.

Proof: The proofs of Theorems 2 and 3 show that 2 is common primitive root of both r and s. Combing this and Theorem 7 proves this corollary. QED

The above theorem and its three corollaries clearly show how to control the linear complexity and its stability for the output sequence of the binary two-prime generator of order 2.

Summarizing the above results, we see that the parameters should be chosen such that

1. p and q both are large enough with $\gcd(p - 1, q - 1) = 2$;
2. $|p - q|$ is small enough, compared with pq;
3. $\mathrm{ord}_p(2)$ and $\mathrm{ord}_q(2)$ both are large enough.

It should be made clear that the special properties of the primes p and q determine partly the quadratic partition of the primes, and thus contributes to the stability of the cyclotomic numbers, and consequently to the difference property and other six aspects described in Section 1.

Generally speaking, the two-prime generator is more flexible, due to the fact that we have much freedom to select the primes.

The best choices for the p and q are the twin primes. They ensures the best difference property and nonlinearity of the cryptographic function according to generalized cyclotomic numbers of order 2 (see [21]). In this case the output sequence of generator is the characteristic sequence of the twin-prime difference set with parameters $(N, h, \lambda) = (p(p+2), (N-1)/2, (N-3)/4)$ (see [21]). Note

$$n = h - \lambda = \begin{cases} (2t+1)^2, & \text{if } p = 4t+1; \\ 4t^2, & \text{if } p = 4t-1. \end{cases}$$

It follows from [11] that the linear complexity of the output sequence is N or $N-1$, provided that $p = 4t+1$. If $p = 4t+1$, then $N+2 = 4(t+1)-1$. It follows that p and $p+2$ has no common primitive root 2 if $p = 4t+1$. Nevertheless, the output sequence has best linear complexity.

If $p = 4t-1$, it is possible for p and $p+2$ to have common primitive root 2. Assume that they have common primitive root 2, then by Theorem 7 we have

1. $L(z^\infty) \geq p-1$;
2. $SC_k(z^\infty) \geq p-1$, if $k < \min\{\mathrm{WH}(z^N), N - \mathrm{WH}(z^\infty)\}$.

Because the cryptographic function is the characteristic function of a twin-prime difference set, all the seven aspects described in Section 1 are optimal.

The output sequence of the two-prime cyclotomic generator of order 2 is an extension of 0-1 version of the Jacobi sequence in the sense that the values at the special sets Q, P and R are modified. In addition, the condition that $\gcd(p-1, q-1) = 2$ is essential to the generator. It is because of this condition that the generalized cyclotomic numbers of order 2 ensure an ideal difference property of the cryptographic function. Without this condition it cannot be called a cyclotomic generator.

6 Two-prime generator of order 4

To design cryptographic functions from Z_{pq} to Z_4, we follow the same approach as in the foregoing sections. Let $p = 4f+1$ and $q = 4f'+1$ with $\gcd(f, f') = 1$. Then $d = \gcd(p-1, q-1) = 4$ and $e = 4ff'$. Define the function

$$F(j) = \begin{cases} 1, \ j \in \{0, q, 2q, \cdots, (p-1)q\}; \\ 0, \ j \in \{p, 2p, \cdots, (q-1)p\}; \\ ((j^{(q-1)/4} \bmod q) \bmod 2) \oplus ((j^{(p-1)/4} \bmod p) \bmod 2) \oplus 1, \ j \in Z_{pq}^*. \end{cases}$$

With this $F(x)$ we describe a generator based on the generalized cyclotomy of order 4, as depicted in Figure 2 with $k = 2$.

If we define the function $F^*(x)$ from Z_{pq}^* to Z_2 by

$$F^*(j) = ((j^{(q-1)/4} \bmod q) \bmod 2) \oplus ((j^{(p-1)/4} \bmod p) \bmod 2) \oplus 1, \ j \in Z_{pq}^*.$$

Then it is easy to know that $F^*(x)$ has characteristic set $C_1 = D_i \cup D_j \cup Q$, where $Q = \{0, q, 2q, \cdots, (p-1)q\}$, D_i and D_j are two of the four generalized cyclotomic classes developed by Whitman [21]. Thus, an ideal stability of the generalized cyclotomic numbers of order 4 ensures an ideal difference property and nonlinearity of the above function $F(x)$.

Fortunately, the generalized cyclotomic numbers of order four have an ideal stability [21]. Thus, it follows from the formulae in Section 1 and the relation between cyclotomic numbers and the difference parameters described in Section 2 that we have ensured an ideal property for all the seven aspects described in Section 1.

The control of the linear complexity and its stability for the output sequence of the binary two-prime cyclotomic generator of order 4 is the same as that of order 2. By Theorems 6 and 7 the parameters should be chosen such that

1. p and q both are large enough with $\gcd(p-1, q-1) = 4$;
2. $|p-q|$ is small enough, compared with pq;
3. $\mathrm{ord}_p(2)$ and $\mathrm{ord}_q(2)$ both are large enough.

7 Prime-square generator

Sequences with period of the square of a odd prime are cryptographically attractive due to the following theorems about their linear complexity and linear complexity stability which follow easily from Basic Theorem 1.

Theorem 11. *Let r be a odd prime, $N = r^e$ and q an integer with $\gcd(q, N) = 1$. Then for any nonconstant sequence of period N over GF(q),*

1. $L(s^\infty) \geq ord_r(q)$;
2. $SC_k(s^\infty) \geq ord_r(q)$, *if* $k < \min\{\mathrm{WH}(s^N), N - \mathrm{WH}(s^N)\}$.

Proof: Setting $t = 1$ in Basic Theorem 1 proves this theorem. QED

Theorem 12. *Let r be a odd prime, $N = r^2$ and q a primitive root modulo r and r^2 does not divides $q^{r-1} - 1$, then for any nonzero sequence of period N over GF(q),*

1. $L(s^\infty)$ *must be equal to one of* $\{\sqrt{N}, \sqrt{N}-1, N-\sqrt{N}, N-\sqrt{N}+1, N-1, N\}$;
2. $SC_k(s^\infty) \geq \sqrt{N} - 1$, *if* $k < \min\{\mathrm{WH}(s^N), N - \mathrm{WH}(s^N)\}$.

Proof: Since q is a primitive root of r and r^2 does not divides $q^{r-1} - 1$ by assumptions, it is known that q must be a primitive root of r^2 (for proof, see [1]). Thus, by the basic properties of cyclotomic polynomial presented in the proof of Basic Theorem 1 we know that the cyclotomic polynomials $Q_r(x)$ and $Q_{r^2}(x)$

are irreducible over $GF(q)$. Again from the properties of cyclotomic polynomials it follows

$$x^N - 1 = (x-1)Q_r(x)Q_{r^2}(x).$$

Note that $\deg(Q_r(x)) = r-1$ and $\deg(Q_{r^2}(x)) = r(r-1)$ since q is a common primitive root of r and r^2. Combining these fact and the fact that the minimum polynomial of each sequence of period N over $GF(q)$ divides $x^N - 1$ proves this theorem. QED

Thus, the best primes p for binary sequences of period p^2 are the non-Wieferich primes with base q, i.e., those described by the above theorem, which is related to the *Fermat quotient* and some other number-theoretic problems. We prove these two theorems here because we need them to control the linear and sphere complexities of the output sequences of the prime-square generator.

If we choose one of the following functions

$$F_C(x) = \begin{cases} 1, & x \in R; \\ (x^{p(p-1)/2} \bmod p^2) \bmod 2, & \text{otherwise} \end{cases}$$

and

$$F_C(x) = \begin{cases} 0, & x \in R; \\ (x^{p(p-1)/2} \bmod p^2) \bmod 2, & \text{otherwise} \end{cases}$$

for the cryptographic function of Figure 1, where $N = p^2$, then we have the binary prime-square cyclotomic generator.

To describe the difference property of the above two cryptographic functions, we give a brief introduction to the cyclotomic numbers modulo p^2. Let p be a odd prime. By the Chinese Remainder Theorem there is a common primitive root α modulo both p and p^2. Setting $D_0 = (\alpha^2)$, a multiplicative subgroup of $Z_{p^2}^*$, and $D_1 = \alpha D_0$. Then the cyclotomic numbers of order 2 modulo p^2 are defined by

$$(l,m)_2 = |D_l \cap (D_m + 1)|, \ 0 \le l, m \le 1.$$

We need the following theorem, which was conjectured by the author and proved by D. Pei [16], to ensure an ideal property for all the seven aspects described in Section 1.

Theorem 13. *Let symbols as before. If* $p = 3 \bmod 4$, *we have*

$$(0,1) = (0,0) = (1,1) = \frac{p(p-3)}{4}, \ (1,0) = \frac{p(p-3)}{4} + p.$$

If $p = 1 \bmod 4$, *we have*

$$(0,1) = (1,0) = (1,1) = \frac{p(p-1)}{4}, \ (0,0) = \frac{p(p-1)}{4} - p.$$

Let $\{C_0, C_1\}$ be the characteristic class of the above function $F_C(x)$, then similar to Section 2 it is easily verified that the difference parameters of the above function are approximately the same as the four cyclotomic numbers defined for the modulus $N = p^2$. Thus, an ideal difference property and therefore an ideal property for the other six aspects are ensured by the formulae described in Section 1.

8 Behind the cyclotomic generators

There are several cryptographic ideas behind the construction of these cyclotomic generators. The first one is the order of choosing the design parameters for the generator. Contrary to the traditional approach, we first control the period of the output sequence. This will automatically ensure the linear complexity and its stability aspects only with the condition that the sequence is not a constant sequence. Then we choose the cryptographic function for other purposes. This approach is intended to avoid unnecessary tradeoffs.

The second cryptographic idea behind the design and analysis of cyclotomic generators is the idea of introducing good partners, in order to get a stable system. In particular, we search for pairs of period and finite field so that it is easy to control the linear complexity and its stability for those sequences over those fields with corresponding partner periods. This has been shown clearly by the theorems and corollaries concerning linear and sphere complexities. We say that such pairs work in harmony with respect to the aspects of linear complexity and its stability. For example, some Mersenne and Fermat primes are not good partners of the field $GF(2)$, since it is difficult to control the linear complexity and its stability for binary sequences with period of some Fermat and Mersenne primes. This is because that the order of 2 modulo these primes is quite small. From Basic Theorem 1 and its corollaries it is rational to use $\mathrm{ord}_N(q)$ as a measure on the partnership between an positive integer N and an integer q with respect to the linear and sphere complexity aspects when designing sequences of period N over $GF(q)$, where $\gcd(N, q) = 1$. We say that q and N are the *best partners* when q is a primitive root modulo N.

Another kind of partnership is to find an integer r which is a power of prime such that $\mathrm{lcm}\{\mathrm{ord}_{p_1}(r), \cdots, \mathrm{ord}_{p_h}(r)\}$ is large enough when designing sequences of period $N = p_1 \cdots p_h$ over $GF(r)$, where $p_1, \cdots, p_h$ are distinct primes (see Basic Theorem 1). We say that r is a *best common partner* of $p_1, \cdots, p_h$ if r is a common primitive root of these primes.

The third cryptographic idea is to use some techniques of ensuring "good + bad = good". With a simple argument each cryptographic function employed in the generators described in the foregoing sections can be expressed as

$$F(x) = H(G(x)),$$

where $G(x)$ is a mapping from Z_N to U which is a subgroup of the group $(Z_N^*, \cdot)$ with order d, and $H(x)$ a mapping from U to Z_d. The nonlinearity of $G(x)$ with respect to $(Z_N, +)$ and $(U, \cdot)$ is determined mainly by the (generalized)

cyclotomic numbers of order d, which usually have an ideal stability; while the function $H(x)$ is almost linear (or with good linearity) with respect to $(U, \cdot)$ and $(Z_d, +)$. Thus, it is clear that one cryptographic idea behind the cyclotomic generators is

"GOOD + BAD = GOOD".

The fourth cryptographic idea is to use cryptographic functions $f(x)$ from an abelian group $(G_1, +)$ to another abelian group $(G_2, +)$ such that $|G_2|$ does not divide $|G_1|$. We say that such a function is *linearly non-approximatable*, since there is no linear mapping other than the zero constant function from $(G_1, +)$ to $(G_2, +)$. This technique makes any linear approximation attack with respect to the two operations out of sense. It should be pointed out that the nonlinearity definition based on the minimum correlation (measured in probability of agreement, or distance [15] between a function and all affine functions) is not rational in many cases. This definition makes no sense for the above cryptographic functions.

The fifth cryptographic idea is to make use of the relativity about nonlinearity and linearity. It is a common fact that the nonlinearity and linearity are relative to the operations considered, and that both linear components and nonlinear components should be employed in many cipher systems. To find out some cryptographic functions with good nonlinearity with respect to some operations, one may try to find some linear cryptographic function with respect to some other operations and use them in the context of the former operations. This is to say that bad things in one sense may be good ones in another sense, and one way to get goodness is to use badness in a proper way and proper context. To illustrate this philosophy, we first take the corresponding function $G(x) = x^{(p-1)/d} \bmod p$ used to construct the cyclotomic generator of order $2k$. Then $G(x)$ is linear with respect to $(Z_p^*, \cdot)$ and $(U, \cdot)$, where U is the multiplicative subgroup of Z_p^* with order d. But $G(x)$ has ideal nonlinearity with respect to $(Z_p, +)$ and $(U, +)$ if we define $G(0)$ to be any fixed element of U. And we use $G(x)$ in the context of the later pair of operations exactly. The same idea has been used for other generators.

To illustrate the relativity of linearity and nonlinearity, we prove the following theorem.

Theorem 14. *For every nonzero linear function $L(x)$ from $F = GF(q^m)$ to $K = GF(q)$ with respect to the additions of the two fields, its nonlinearity with respect to $(F^*, \times)$ and $(K, +)$ is optimal, as described by*

$$p(L(x) - L(x/\alpha) = b) = p(L(x(1-\alpha^{-1})) = b) = \begin{cases} \frac{q^{m-1}-1}{q^m-1}, & \text{if } b = 0, \\ \frac{q^{m-1}}{q^m-1}, & \text{if } b \neq 0, \end{cases}$$

which holds for $\alpha \in F$ with $\alpha \neq 1$, and each $b \in K$.

Proof: For any nontrivial linear mapping $L(x)$from F to K the kernel $L^{-1}(0)$ is an Abelian subgroup of $(F, +)$ and thus $L(x)$ takes on each element of K equally

likely, that is, q^{m-1} times. Confining the linear mapping on $F^* = F \setminus \{0\}$ and using the above fact proves the theorem. QED

This theorem clearly shows the cryptographic importance of linear functions from $F = GF(q^m)$ to $K = GF(q)$ with respect to the additions of the two fields, especially the trace functions. Actually all the cryptographic functions for the cyclotomic generators are composition functions of linear functions with respect to different pairs of operations. It may be possible to employ this idea to design some block ciphers.

9 Some related number-theoretic problems

In the paper at least two bridges between some number-theoretic problems and the design and analysis of the natural sequence generator have been established. These bridges may play an important role in the interactions between number theory and stream ciphers, and particularly in the design and analysis of the cyclotomic generators described in this paper.

The first one is the bridge supported by Basic Theorem 1 and the theorems and corollaries concerning linear and sphere complexities. The reason for calling it a bridge has already made clear in Section 3. Obviously, there are more results which can be derived from Basic Theorem 1. If we go across this bridge from the stream cipher side, we shall encounter at least the following two basic number-theoretic problems when we are designing sequences of period N over $GF(q)$ with ideal linear and sphere complexities (see Basic Theorem 1).

Basic Problem 1 *Find large positive integers N's and positive integers q's which are powers of primes such that*

1. $\gcd(N, q) = 1$;
2. *For any factor n of N, $ord_n(q) = \phi(n)$.*

Basic Problem 2 *Find large positive integers N's and positive integers q's which are powers of primes such that*

1. $\gcd(N, q) = 1$;
2. *N has a few factors;*
3. *For any factor n of N, $ord_n(q)$, a factor of $\phi(n)$, is as large as possible.*

Attacking these two basic problems and many of its subproblems and variants will involve many, if not most, number-theoretic problems. Among them are the searching for special primes, such as Fermat primes, Mersenne primes, Stern primes, prime repunits, and twin primes, the distribution of special primes, primitivity testing, the distribution of primitive roots. These facts have already been shown clearly by all the theorems concerning the linear and sphere complexities proved in this paper. We need special primes for these generators, and have to know whether they exist. And if they exist, we have to know how to find large special primes.

We need not only twin primes for our twin-prime generator, but also special twin primes. The most interesting twin primes are those having a common primitive root 2 (the best common partner of the twins). However, some twins have, others don't. Problems as to which twins have the common primitive root 2 and how to find them are naturally important to the design of the twin-prime generators. By introducing sexes to twin we can solve one cryptographic problem for the twin-prime generator.

Let $(p, p+2)$ be a pair of twin primes and $p = \Xi(p) \bmod 4$, where $\Xi(p) = \pm 1$. Then we call $\Xi(p)$ the *sex characteristic* of the twins. If the twins $(p, p+2) = (4t-1, 4t+1)$ for some t, then we say that the twins have the same sex; otherwise, we say that they have different sexes.

In the above definitions, we say that twin primes $(p, p+2)$ have same sex, because in the expression of the form $4u \pm 1$, the u's for both p and $p+2$ are the same, and have therefore the same parity, if $p = 4t - 1$. If $p = 4t + 1$, then $p + 2 = 4(t + 1) - 1$ and t and $t + 1$ have different parities. That is why we call them twins with different sexes. This discussion has also proved the following property of twins.

Theorem (The Sex Principle of Twins *) If the smaller of the twins has sex characteristic* -1*, then the twins have the same sex; otherwise, they have different sexes.*

Theorem 15. *If* p *and* $p + 2$ *have the same sex, then it is possible for them to have common primitive root* 2 *(a common best partner); otherwise, they never have.*

Proof: With the help of the Law of Quadratic Reciprocity it is easy to see that a necessary condition for 2 to be a primitive root of a prime N is $N = 8k \pm 3$ for some k. Combining this fact and the definition of sexes proves the theorem. QED

Thus, the cryptographic importance of classifying twin primes into two classes according to their sexes for the design of the twin-prime generator clearly follows from the above theorem. Before searching for twins with the same sex, we have to know the distribution of the two classes. Solving this problem and searching for twin primes with the same sex are important design problems for the twin-prime generator.

The second bridge we set up when we design these cyclotomic generators is supported by the relations between the difference parameters of the cryptographic function $f(x)$, and the nonlinearity measure, the autocorrelation functions, mutual information, and two-bit pattern distributions, as described by the formulae in Section 1.

At one side of the second bridge are the autocorrelation property, the two-digit pattern distribution property of the output sequences, and the difference property and nonlinearity of the cryptographic functions of the NSG; while at the other side are cyclotomy-related problems and the Riemann Hypothesis for Curves over Finite Fields, which was proven to be true by Weil in 1948 [20].

We call it another bridge between number theory and stream ciphers because it makes a clear connection between the above set of cryptographic problems and the set of number-theoretic problems.

Related to cyclotomic numbers and their stability are the quadratic partition of primes and of some integers, the theory of quadratic forms, genus theory, class field theory, residue difference sets, group character, and character sums. In what follows we give a brief explanation to why these problems are related to the design of the cyclotomic generators. It is a pity that we cannot show here how some of these problems are related to the design and analysis of the cyclotomic generators since doing so must involve quite a number of number-theoretic concepts. However, pointing out some relations between design problems of cyclotomic generators and a number of number-theoretic problems might be helpful for those who are interested in these generators. Let us begin with the stability of cyclotomic numbers.

We now consider the binary cyclotomic generator of order 4 in Section 4. Let $N = 4f+1$ be a chosen prime for the generator. Let $N = x^2+4y^2$, $x = 1 \bmod 4$, here y is two valued, depending on the choice of the primitive root [8]. There are five possible different cyclotomic numbers in the case f even; i.e., (0,0), (1,3)=(2,3)=(1,2), (1,1)=(0,3), (2,2)=(0,2), (3,3)=(0,1) and

$$\begin{aligned}
(0,0) &= (p-11-6x)/16,\\
(0,1) &= (p-3+2x+8y)/16,\\
(0,2) &= (p-3+2x)/16,\\
(0,3) &= (p-3+2x-8y)/16,\\
(1,2) &= (p+1-2x)/16.
\end{aligned}$$

For the case f odd, there are at most five distinct cyclotomic numbers, which are

$$\begin{aligned}
(0,0) = (2,2) = (2,0) &= (p-7+2x)/16,\\
(0,1) = (1,3) = (3,2) &= (p+1+2x-8y)/16,\\
(1,2) = (0,3) = (3,1) &= (p+1+2x+8y)/16,\\
(0,2) &= (p+1-6x)/16,\\
\text{the rest} &= (p-3-2x)/16,
\end{aligned}$$

where $p = x^2+4y^2$ and $x = 1 \bmod 4$.

Although these formulas show a roughly ideal stability of cyclotomic numbers of order 4, the actual stability depends on the quadratic partition $p = x^2 + 4y^2$ and $x = 1 \bmod 4$. If there is a big difference between $|x|$ and $|y|$, then there is a considerable difference between the cyclotomic numbers. And it is not difficult to give examples to show there do exist primes such that there is a considerable difference between x^2 and y^2 in their quadratic partitions. Thus, choosing large special primes to ensure better stability of cyclotomic numbers is cryptographically necessary.

There are two approaches to do this. The first approach is to use traditional methods to get first large primes. Then use some special algorithm to get the partition and see whether it results in an ideal stability of cyclotomic numbers. This special algorithm should be related to classical problems about quadratic partitions such as the number of solutions of such a quadratic partition. Another approach is to consider directly for given n the set

$$\{x^2 + ny^2 : x, y \in Z\}.$$

If there are infinitely many primes in the set, we can search for the primes which give an ideal stability of cyclotomic numbers. With this approach the first problem we have to solve is whether there are infinite many primes in the above set. The Dirichlet theorem about primes in arithmetic progression does not help here. However, with some results from class field theory we can get a positive answer for each n [5].

If one has a quick look at each set of cyclotomic formulae known today, one will find that they have the same form. Behind this uniformity of all cyclotomic numbers is the Riemann Hypothesis for Curves over Finite Fields, which can be described as follows.

Riemann Hypothesis for Curves over Finite Fields: Suppose that $F(x, y)$ is a polynomial of total degree d, with coefficients in $GF(q)$ and with N zeros $(x, y) \in GF(q) \times GF(q)$. Suppose that $F(x, y)$ is absolutely irreducible, i.e., irreducible not only over $GF(q)$, but also over every algebraic extension thereof. Then

$$|N - q| \leq 2g\sqrt{q} + c_1(d),$$

where g is the genus of the curve $F(x, y) = 0$ and $c_1(d)$ is a constant depending on d.

This theorem, proven by Weil [20], not only indicates the uniformity of the form of cyclotomic formulae, but also can be used to set up bounds for pattern distributions in the output sequences of the cyclotomic generators. With the Weil Theorem one can see some cryptographic meanings of the genus of curves. For details about the Weil Theorem, the reader is referred to [18]. Since cyclotomic numbers are related to characters and character sums [8, 9, 12], the cyclotomic generators are naturally related to character and character sums. In fact many of the cryptographic functions $f(x)$ employed here are group characters.

One part of the design and analysis of these cyclotomic generators is to solve the following basic problem at the number-theory side of the second bridge.

Basic Problem 3 *Let N be a positive integer, and Z_N denote the residue ring modulo N. Find partitions $\{C_0, C_1\}$ of Z_N, i.e.,*

$$C_0 \cap C_1 = \Phi, \ C_0 \cup C_1 = Z_N,$$

such that

$$\begin{aligned} &|C_0| \approx N/2, \ |C_1| \approx N/2, \\ &|C_i \cap (C_j + r)| \approx N/4 \end{aligned} \tag{12}$$

for each nonzero r of Z_N, and each $i, j \in Z_2 = \{0, 1\}$. Here and hereafter $A \approx B$ means that $A = B \pm O(B^e)$ for some e with $0 \le e \le \frac{1}{2}$.

For our cryptographic application we hope that $A \approx B$ means that A is as near to B as possible. But for the flexibility of the solutions of the above basic problem, we give such a definition of $A \approx B$.

The characteristic function of a partition $\{C_0, C_1\}$ of Z_N satisfying (12) ensures that it has an ideal difference property, and therefore an ideal property for the other six aspects described in Section 1. But to ensure an ideal pattern distribution property for various pattern lengths is to solve the following more general basic problem.

Basic Problem 4 *Let $C = \{C_0, C_1\}$ be a partition of Z_N, $r_0, r_1, \cdots, r_{s-1}$ be s pairwise distinct elements of Z_N, and*

$$D_{i_0 \cdots i_{s-1}}(r_0, \cdots, r_{s-1}) = \cap_{k=0}^{s-1}(C_{i_k} + r_k),$$
$$d_{i_0 \cdots i_{s-1}}(r_0, \cdots, r_{s-1}) = |\cap_{k=0}^{s-1}(C_{i_k} + r_k)|,$$

where $i_0, \cdots, i_{s-1} \in Z_2$. Then $\{C_{i_0 \cdots i_{s-1}}(r_0, \cdots, r_{s-1}) : i_0, \cdots, i_{s-1} \in Z_2\}$ forms a partition of Z_N.

Find partitions $\{C_0, C_1\}$ of Z_N such that

$$d_{i_0 \cdots i_{t-1}}(r_0, \cdots, r_{t-1}) \approx \frac{N}{2^t} \tag{13}$$

holds for each t with $1 \le t \le \lfloor \log_2 N \rfloor$, and for each set of pairwise distinct elements $r_0, \cdots, r_{s-1}$ of Z_N.

The conditions here include those of Basic Problem 3. They ensure that the output sequence of the NSG employing the characteristic function of the partition has an ideal pattern distribution for each pattern with length t satisfying $1 \le t \le \lfloor \log_2 N \rfloor$, and also an ideal mutual information stability $I(i; z_{i_1} z_{i_2} \cdots z_{i_t})$. It is noted that these *higher order difference parameters* $D_{i_0 \cdots i_{s-1}}(r_0, \cdots, r_{s-1})$ are exactly measures on patterns distributions of binary sequences.

One class of solutions to Basic Problem 3 is those partitions $C = \{C_0, C_1\}$ of Z_N such that C_0 is a residue difference set of Z_N with $|C_1| \approx |C_0|$. However, difference sets exist only for those $N = 3 \bmod 4$. For $N = 1 \bmod 4$ there may exist some partitions $\{C_0, C_1\}$ of Z_N with almost the same difference property. These are partitions $\{C_0, C_1\}$ of Z_N with C_1 being an almost difference set.

Let N be a odd number, and $D = \{d_1, \cdots, d_k\}$ a subset of an abelian group $(G, +)$. If for each of half of the nonzero elements a's of Z_N, the equation

$$d_i - d_j = a$$

has exactly λ solutions (d_i, d_j) with d_i and d_j in D, and for each of the other half exactly $\lambda + 1$ solutions, we call D an (N, k, λ) *almost difference set* (briefly, a.d. set).

It is easy to see that N must be of the form $4t + 1$ if Z_N has an (N, k, λ) difference set. Almost difference sets are not easy to find. The cyclotomic numbers

of order 2 show that the quadratic residues modulo a prime $N = 1 \bmod 4$ form an $(N, (N-1)/2, (N-5)/4)$ a.d. set. For the biquadratic residues we have the following conclusion.

Theorem 16. *Let a prime $N = 4t+1 = x^2 + 4y^2$ with $x = 1 \bmod 4$ and t being odd. Then the biquadratic residues modulo N form an $(N, t, (t-3)/4)$ a.d. set if and only if $x = 5$ or -3.*

Proof: By the formulae for cyclotomic numbers of order 4 presented in this section and the definition of a.d. sets we see that the biquadratic residues modulo N form an $(N, t, (t-3)/4)$ a.d. set if and only if

$$(0,0) - (1,1) = \frac{2x-7}{16} + \frac{3+2x}{16} = \frac{1}{4} = \pm 1,$$

which is equivalent to $x = 5$ or 3. This proves the theorem. QED

For other power residues it is not difficult to see whether they form a.d. sets by employing the cyclotomic numbers of various orders. In general, it is not easy to find a.d. residue sets. It is noted that difference sets and almost difference sets are employed in the cyclotomic generator of order 2 and in the twin-prime generator. So they are closely related to cyclotomic generators.

Another solution to Basic Problem 3 is to make use of power residues and cyclotomic numbers generally, as done in the foregoing sections. One advantage of the sets of power residues is that they form multiplicative groups, and this makes the implementation problem of characteristic functions of the corresponding partitions simple. There may exist other solutions to Basic Problem 3, which remains to be investigated.

The condition (12) can only give a very rough guarantee for other conditions in (13). The cyclotomic numbers and the Weil Theorem seem to indicate that partitions based on power residues give ideal solutions to Basic Problem 4. In fact we can set up bounds of order $N \pm O(\sqrt{N})$ for these higher order difference parameters $D_{i_0 \cdots i_{s-1}}(r_0, \cdots, r_{s-1})$ for $s \geq 3$ based on the Weil Theorem when N is a prime, but the bounds becomes more and more looser with the increase of s though the bounds remain in order $N \pm O(\sqrt{N})$.

We pointed out a number of number-theoretic problems here, since they are essential to the design and analysis of cyclotomic generators. For other type of generators there may be other related number-theoretic problems, such as the class numbers for imaginary quadratic fields which are related to properties of some number-theoretic generator [4].

10 Concluding remarks

Since we have controlled the difference property of the cryptographic functions and the linear and sphere complexities of the output sequences of the binary cyclotomic generators, the formulae in Section 1 and theorems and corollaries regarding the linear and sphere complexities show that these generators have the following properties:

1. the cryptographic function $f(x)$ has an ideal difference property;
2. the cryptographic function $f(x)$ has an ideal nonlinearity with respect to the additions of Z_N and Z_2;
3. the cryptographic function $f(x)$ has an ideal autocorrelation property;
4. the affine approximation of $f(x)$ with respect to $(Z_N, +)$ and $(Z_2, +)$ makes no sense, since there are only two trivial affine functions from Z_N to Z_2 for odd N;
5. the output sequence has an ideal autocorrelation property;
6. the output sequence has an ideal two-bit pattern distribution property;
7. the output sequence has ideal linear complexity and linear complexity stability;
8. the mutual information $I(i;\ z_i z_{i+t-1})$ has an ideal stability, here z^∞ denotes the output sequence of the NSG; and
9. the additive stream cipher system with this NSG as the keystream generator has an ideal density of encryption (resp. decryption) transformations, i.e., the probability of agreement between two encryption (resp. decryption) transformations specified by two keys is approximately 1/2.

In fact we can calculate exact values of measures (such as autocorrelation values, the mutual information) for the above aspects based on the formulae in Section 1 if we have formulae for the difference parameters. For example measures for the above aspects for the cyclotomic generator of order 2 can be expressed exactly in terms of N, the modulus for the modulo N ring counter. If we have bounds for the difference parameters, then using the formulae in Section 1 gives bounds for measures on the above aspects.

In addition, the Weil Theorem and the formulae of cyclotomic numbers seem to indicate that the output sequences of these cyclotomic generators have an ideal distribution property for any pattern with length $1 \leq l \leq \lfloor \log_2 N \rfloor$.

In this paper we consider only some binary cyclotomic generators. It is possible to extend the results for binary cyclotomic generators to cyclotomic generators over other fields. For the linear complexity and sphere complexity of periodic sequences over other fields we have similar results.

The performances of these cyclotomic generators are basically of the same order, since they are all based on the exponentiation-modulo-N operation. It seems that these generators are not fast, but with a fast exponentiation algorithm it is possible to get a reasonable performance if the moduli are not too large. For the time being moduli having about 64 bits seems enough for the generators. Though the generators are not fast, they might have an ideal security. Thus, trading performance for security might be possible.

Finally we mention that some related work about some randomness aspects of the Legendre and Jacobi sequences was done by Damgård [6].

Acknowledgment: I would like to thank Arto Salomaa for several discussions on this topic with me, and the reviewers for helpful comments.

References

1. T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, 1976.
2. L. D. Baumert and H. Fredricksen, *The Cyclotomic Number of Order Eighteen with Applications to Difference Sets*, Math. Comp. 21, 1967, pp. 204-219.
3. L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics, vol. 182, Springer-Verlag, 1971.
4. T. W. Cusick, *Properties of the X^2 mod N generator*, to appear in IEEE Trans. Inform. Theory, 1995.
5. D. A. Cox, *Primes of the Form x^2+ny^2: Fermat, Class Field Theory, and Complex Multiplication*, John Wiley & Sons, 1989.
6. I. Damgård, *On the Randomness of Legendre and Jacobi Sequences*, Advances in Cryptology: Crypto'88, S. Goldwasser (Ed.), LNCS 403, Springer-Verlag, 1990, pp. 163-172.
7. J.-M. Deshouillers, *Waring's Problem and the Circle-Method*, in Number Theory and Applications, R. A. Mollin Eds., Kluwer Academic Publishers, 1989, pp. 37-44.
8. L. E. Dickson, *Cyclotomy, Higher Congruences, and Waring's Problem*, Amer. J. Math. 57, 1935, pp. 391-424, pp. 463-474.
9. L. E. Dickson, *Solution of Waring's Problem*, Amer. J. Math. 58, 1936, pp. 530-535.
10. C. Ding, G. Xiao, and W. Shan, *The Stability Theory of Stream Ciphers*, LNCS 561, Springer-Verlag, 1991.
11. C. Ding, *The Differential Cryptanalysis and Design of the Natural Stream Ciphers*, Fast Software Encryption: Proc. of the 1993 Cambridge Security Workshop, R. Anderson (Ed.), LNCS 809, Springer-Verlag, 1994, pp. 101-115.
12. E. Lehmer, *On the Number of Solutions of $u^k + D = w^2$ mod p*, Pacific J. Math. 5, 1955, pp. 103-118.
13. R. Lidl, H. Niederreiter, *Finite Fields*, in Encyclopedia of Mathematics and Its Applications, vol. 20, Addison-Wesley, 1983.
14. J. L. Massey, *Shift-Register Synthesis and BCH Decoding*, IEEE Trans. Inform. Theory, vol. IT-15, January, 1969, pp. 122-127.
15. W. Meier, O. Staffelbach, *Nonlinearity Criteria for Cryptographic Functions*, LNCS 434, Advances in Cryptology, Springer-Verlag, 1990, pp. 549-562.
16. D. Pei, *Personal communications*, Jan. 1994.
17. S. Pillai. *On Waring's Problem*, I. Ind. Math. Soc. 2, 1933, pp. 16-44.
18. W. M. Schmidt, *Equations over Finite Fields: An Elementary Approach*, Lecture Notes in Mathematics, vol. 536, Springer-Verlag, 1976.
19. T. Storer, *Cyclotomy and Difference Sets*, Marham, Chicago, 1967.
20. A. Weil, *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Actualités Sci. Ind. No. 1041.
21. A. L. Whiteman, *A Family of Difference Sets*, Illinois J. Math. 6, 1962, pp. 107-121.