Journal of ELECTRICAL ENGINEERING, VOL. 51, NO. 12/s, 2000, 92–95

CYCLOTOMIC GENERATORS OF ORDER 4

Hana Lichardová — Marek Greško *

Some properties of binary cyclotomic generators of order 4 are discussed. Via estimates of difference parameters there is shown which primes are suitable for designing generators with ideal difference property. For particular generators, statistical properties of generated sequences are tested.

K e y w o r d s: stream cipher, linear complexity, differential analysis, cyclotomic numbers, pattern distribution

2000 *Mathematics Subject Classification*: 94A60,68P25

1 INTRODUCTION

Cyclotomy generators are intended to produce keystreams for stream ciphers [2]. Since the security of a stream cipher depends on the randomness properties of the keystream, it is important to pay attention to a mathematical analysis of the keystream sequence.

We design a keystream generator producing the sequence with large both linear and sphere complexity, and show for which periods it has the ideal difference property.

The designed keystream generator is a so-called *natural stream generator* (NSG). It consists of a counter modulo N (which merely counts cyclically numbers from 0 to $N-1$), and a cryptographic function $F(x)$. If the key of the generator is k (i.e. the counter starts to count from the number k), the generated sequence is $s^\infty = (s_i)_{i=0}^\infty$, where $s_i = F((i+k) \bmod N)$.

Let $N = dt+1$ be a prime. A corresponding *cyclotomic generator of order* d over $GF(q)$ is described by

$$s_i = \left((i+k)^{(N-1)/d} \bmod N\right) \bmod q\,.$$

If $N = 4t+1$, $q = 2$, we have a binary cyclotomic generator of order 4.

In the following four sections we introduce conceptions and relations which will be useful for analyzing some properties of binary NSG based on cyclotomy. For more details in the field, we refer the reader to [1], [2], [4], [5]. Then difference parameters of binary cyclotomic generator of order 4 will be derived. In the last section, results of some statistical tests are presented.

2 PRIMITIVE ROOTS

Given integers $n > 1$, q, we say that d is the *order of* q modulo n, $d = \mathrm{ord}_n(q)$, if d is the least positive integer such that $q^d \equiv 1 \,(\mathrm{mod}\, n)$. Analogously, m is the *negative order of* q modulo n, $m = \mathrm{nord}_n(q)$, if m is the least positive integer such that $q^m \equiv -1 \,(\mathrm{mod}\, n)$.

An integer q is said to be a *primitive root* modulo n (of n), if $\mathrm{ord}_n(q) = \varphi(n)$, where Euler's function $\varphi(n)$ is the number of all positive integers $a < n$ such that $\gcd(a, n) = 1$. For given n, we will take into consideration only primitive roots smaller than n. The classical result by Gauss is that each prime N has exactly $\varphi(N-1)$ primitive roots.

Now we state some properties of primitive roots modulo a prime N. We recommend the proof of the following lemma as a good exercise.

Lemma 1. *Let $N > 4$ is a prime. Then q is a primitive root of N if and only if $\mathrm{nord}_N(q) = (N-1)/2$.*

Lemma 2. *If q is a primitive root of a prime $N > 4$, then q must be quadratic nonresidue modulo N.*

P r o o f . We recall that $q \in Z_N$ is a quadratic residue modulo N if there exists $b \in Z_N^*$ such that $q \equiv b^2 \,(\mathrm{mod}\, N)$. Otherwise it is quadratic nonresidue. Since q is a primitive root of N, $q^{(N-1)/2} \equiv -1 \,(\mathrm{mod}\, N)$. On the other hand, by Fermat's Theorem, $b^{N-1} \equiv 1 \,(\mathrm{mod}\, N)$ for each b. It follows immediately that q cannot be a quadratic residue.

The fact that $q \in Z_N$ is a quadratic residue may be expressed by the Legendre symbol — it is 1 in the case q is a residue, otherwise it is -1.

Lemma 3. *For $q = 2$ and a prime N, there holds the Legendre symbol formula*

$$\left(\frac{2}{N}\right) = (-1)^{(N^2-1)/8},$$

which means that 2 is a quadratic nonresidue only for $N = 8k \pm 3$.

The proof may be found in [5].

The next assertion is a straightforward consequence of the preceeding lemmas.

* Faculty of Electrical Engineering and Information Technology STU, Ilkovičova 3, 812 19 Bratislava 1, Slovak Republic, E-mail: lichardova@kmat.elf.stuba.sk, gresko@ulib.sk

ISSN 1335-3632

Theorem 1. *If 2 is a primitive root of a prime $N > 4$, then N must be of the form $4t \pm 1$ with t odd (such N is called the* o-prime*, in opposite to e-primes with t even).*

We will see in the next section that binary sequences of period N, with 2 being a primitive root of N, are important because of their large linear and sphere complexity.

3 CRYPTOGRAPHIC ASPECTS OF SEQUENCES

We restrict our attention only to two security aspects — the first is the linear and sphere complexity, the second is the difference property. Due to [2], the ideal difference property of the cryptographic function $F(x)$ of a binary generator ensures automatically other security aspects like ideal nonlinearity, ideal autocorrelation property, ideal two-bit pattern distribution property.

3.1 Linear complexity and sphere complexity

Let s^∞ denote the sequence $s_0 s_1 s_2 \ldots$ of period N over a finite field $GF(q)$. The polynomial

$$f(x) = c_0 + c_1 x + \ldots + c_k x^k$$

such that

$$c_0 s_j + c_1 s_{j-1} + \ldots + c_k s_{j-k} = 0, \quad j \geq k\,,$$

is called the *characteristic polynomial* of s^∞. The characteristic polynomial of a given sequence with minimal degree is the *minimal polynomial*. The *linear complexity* of s^∞, denoted by $\mathrm{L}(s^\infty)$, is defined to be a degree of its minimal polynomial. In other words, the linear complexity is the length of the shortest linear feedback shift register that generates the sequence. It should be clear that $\mathrm{L}(s^\infty) \leq N$.

Now consider the space of infinite sequences of period N over $GF(q)$ with Hamming distance d_H defined to be the number of places in one period where two sequences differ. Correspondingly, Hamming weight of s^∞, $\mathrm{WH}(s^\infty)$, is defined to be the number of nonzero elements in one period of s^∞.

Let $O(s^\infty, u) = \{t^\infty : 0 < d_H(s^\infty, t^\infty) \leq u\}$ be a sphere with radius u and center s^∞. The *sphere complexity* is defined by

$$\mathrm{SC}_u(s^\infty) = \min\{\mathrm{L}(t^\infty) : t^\infty \in O(s^\infty, u)\}\,.$$

In other words, the sphere complexity is the minimum of lengths of the shortest linear feedback shift registers that generate the "nearby" sequences.

Theorem 2. *Let $N > 2$ be a prime, and let q be a primitive root modulo N. Then for any nonconstant sequence s^∞ of period N over $GF(q)$,*

1. $\mathrm{L}(s^\infty) = N$ *or* $N - 1$*;*
2. $\mathrm{SC}_u(s^\infty) = N$ *or* $N - 1$ *for* $u < \min\{\mathrm{WH}(s^\infty), N - \mathrm{WH}(s^\infty)\}$*, otherwise it is zero.*

For the proof see [2], §§3.3, 3.4.

This theorem, together with Theorem 1, gives a sufficient assumption on the period of a generator to ensure the largest possible linear and sphere complexity of a generated binary sequence. The algorithm is as follows:

1. Choose a large prime N of the form $4t \pm 1$ with t odd. Check whether 2 is a primitive root of N.
2. Design a binary sequence of period N.

To complete the first step, we may use one of special primes like Stern primes (with t prime), or an o-prime of the form $N = 2p + 1$, where $p = 2t - 1$ is also a prime (Sophie Germain prime). The second step may be done by the NSG with a counter modulo N and an arbitrary nontrivial cryptographic function.

3.2 Differential analysis

Let $C = \{C_0, C_1, \ldots, C_{n-1}\}$ be an ordered partition of Z_N, $w \in Z_N^*$. Numbers

$$d_C(i, j, w) = |C_i \cap (C_j - w)|$$

are called *difference parameters*. In other words, a difference parameter $d_C(i, j, w)$ is the number of solutions (x, y) to the equation

$$x + w = y, \quad (x, y) \in C_i \times C_j\,.$$

Consider now the function

$$F(x)\colon Z_N \to GF(q)\,,$$

and the corresponding ordered partition

$$C_i = \{x \in Z_N : F(x) = p_i\}\,, \quad p_i \in GF(q)\,.$$

Then *differential analysis* of $F(x)$ is the analysis of difference parameters $d_C(i, j, w)$. We say that F has the *ideal difference property* if the values $d_C(i, j, w)$ are approximately the same for all possible triples (i, j, w).

In what follows, we show how difference parameters of cyclotomic generators may be easily estimated by cyclotomic numbers.

4 CYCLOTOMIC NUMBERS

Let $N = dt + 1 > 2$ be a prime and let θ be a fixed primitive root of N. We denote by D_0 the multiplicative subgroup $\langle \theta^d \rangle$, and define *cyclotomic classes* D_i, $i = 0, 1 \ldots d - 1$, by $D_i = \theta^i D_0$. Then $\{D_0, \ldots, D_{d-1}\}$ is the partition of Z_N^*. Let $(l, m)_d$ denote the number of solutions (x, y) to the equation

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

or equivalently

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

The constants $(l, m)_d$ are called *cyclotomic numbers* of order d. Many of their properties may be found in [2]. We now focus on one cryptographically important aspect of cyclotomic numbers — their relation to difference parameters.

Let

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

It takes a diligent reader just a while to show that

- if $ij \neq 0$, then

$$d_C(i,j,\theta^k) = (i-k+N-1, j-k+N-1)_d; \qquad (1)$$

- otherwise

$$\begin{aligned} &0 \leq d_C(0,j,\theta^k) - (-k+N-1, j-k+N-1)_d \leq 1\,,\\ &0 \leq d_C(i,0,\theta^k) - (i-k+N-1, -k+N-1)_d \leq 1\,, \qquad (2)\\ &0 \leq d_C(0,0,\theta^k) - (-k+N-1, -k+N-1)_d \leq 2\,. \end{aligned}$$

Consequently, the difference parameters are almost the same as the cyclotomic numbers. We will use this fact in calculating difference parameters of cyclotomic generators.

Let $N = 4t+1$ be an o-prime. It may be written in the form $N = x^2 + 4y^2$, where $x \equiv 1 \,(\mathrm{mod}\, 4)$ [3]. It is clear that there are at most 16 cyclotomic numbers of order 4. But, thanks to the properties of cyclotomic numbers, the situation is far more simple.

Theorem 3. *For an o-prime $N = x^2 + 4y^2$, $x \equiv 1 \,(\mathrm{mod}\, 4)$, there are at most five distinct cyclotomic numbers of order 4, namely*

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

For the proof, we refer the reader to [3].

Now we have all necessary prerequisites, and are ready to design and analyze binary cyclotomic generators of order 4.

5 CYCLOTOMIC GENERATOR OF ORDER 4

Let $N = 4t+1$ be a large o-prime such that 2 is a primitive root of N. A binary cyclotomic generator of order 4 is defined by the cryptographic function

$$F(x) = \left(x^t \bmod N\right) \bmod 2\,. \qquad (4)$$

Since 2 is a primitive root of N, we can construct cyclotomic classes of order 4 as $D_0 = \left(2^4\right)$, $D_i = 2^i D_0$, $i = 1,2,3$.

Proposition 1. *Let $2^t \bmod N$ is even. Then*

$$F(x) = \begin{cases} 1\,, & \text{if } x \in E_1 = D_0 \cup D_3\,,\\ 0\,, & \text{if } x \in E_0 = D_1 \cup D_2 \cup \{0\}\,. \end{cases}$$

P r o o f . Trivially, $F(0) = 0$. Let $x \in Z_N^*$. Then x belongs to one of the cyclotomic classes, say D_i, i.e. $x = 2^{4l+i}$, $0 \leq l \leq t-1$. Thus we obtain

$$F(x) = \left(2^{4lt+it} \bmod N\right) \bmod 2 = \left(2^{it} \bmod N\right) \bmod 2\,,$$

where we use the fact that $2^{4t} \equiv 1 \,(\mathrm{mod}\, N)$. Now we compute the four cases separately:

- $x \in D_0$: $x^t \equiv 1 \,(\mathrm{mod}\, N)$, thanks to Fermat's Theorem;
- $x \in D_1$: $(x^t \bmod N) = (2^t \bmod N)$, which is even, by the assumption;
- $x \in D_2$: $(x^t \bmod N) = \left(2^{2t} \bmod N\right) = (-1) \bmod N = N-1$, which is even, since N is odd;
- $x \in D_3$: $(x^t \bmod N) = \left(2^{3t} \bmod N\right) = (-2^t) \bmod N$, which is odd, since $2^t \bmod N + (-2^t) \bmod N$ is odd.

If $2^t \bmod N$ is odd, one can proceed analogously to obtain the same result with ordered partition $E_1 = D_0 \cup D_1$, $E_0 = D_2 \cup D_3$.

Theorem 4. *Let N have the binary quadratic form $x^2 + 4y^2$, and set*

$$d_1 = t + \frac{y-1}{2}\,, \quad d_2 = t - \frac{y+1}{2}\,. \qquad (5)$$

Then difference parameters of the cryptographic function $F(x)$ are

$$d_1,\ d_1+1,\ d_1+2,\ d_2,\ d_2+1,\ d_2+2\,. \qquad (6)$$

P r o o f . We give the proof only for the case $2^t \bmod N$ is even; the case with $2^t \bmod N$ odd is left to the reader.

Difference parameters of $F(x)$ are, by definition, the same as difference parameters of the ordered partition $E = \{E_0, E_1\}$. It is easy to check that

$$\begin{aligned} d_E(0,0,\theta^k) &= d_D(1,1,\theta^k) + d_D(1,2,\theta^k)\\ &\quad + d_D(2,1,\theta^k) + d_D(2,2,\theta^k)\,,\\ d_E(0,1,\theta^k) &= d_D(1,0,\theta^k) + d_D(1,3,\theta^k)\\ &\quad + d_D(2,0,\theta^k) + d_D(2,3,\theta^k)\,,\\ d_E(1,0,\theta^k) &= d_D(0,1,\theta^k) + d_D(0,2,\theta^k)\\ &\quad + d_D(3,1,\theta^k) + d_D(3,2,\theta^k)\,,\\ d_E(1,1,\theta^k) &= d_D(0,0,\theta^k) + d_D(0,3,\theta^k)\\ &\quad + d_D(3,0,\theta^k) + d_D(3,3,\theta^k)\,. \end{aligned}$$

Using (1), we get

$$d_E(0,0,\theta^k) = (a-1,a-1) + (a-1,a) + (a,a-1) + (a,a)\,,$$

where $a = (2-k) \bmod 4$. Substituting $a = 0,1,2,3$ and using (3) gives $d_E(0,0,\theta^k) = d_1,\ d_2,\ d_1,\ d_2$, respectively (depending on a).

For the other difference parameters, we have to use estimates (2). Thus we obtain

$$\begin{aligned} d_E(0,1,\theta^k) &= (a-1,a-2) + x_1 + (a-1,a+1)\\ &\quad + (a,a-2) + x_2 + (a,a+1)\,, \end{aligned}$$

where $x_1, x_2 \in \{0,1\}$ are possible differences between difference parameters and cyclotomic numbers. As before, we have that $d_E(0,1,\theta^k) = d_2+1+x_1+x_2,\ d_1+1+x_1+x_2,\ d_2+x_1+x_2,\ d_1+x_1+x_2$. We continue analogously to get $d_E(1,0,\theta^k) = d_2+x_3+x_4,\ d_1+x_3+x_4,\ d_2+$

$1 + x_3 + x_4$, $d_1 + 1 + x_3 + x_4$ with $x_3, x_4 \in \{0, 1\}$, and $d_E(1, 1, \theta^k) = d_1 + x_5 + x_6 + x_7$, $d_2 + x_5 + x_6 + x_7$, $d_1 + x_5 + x_6 + x_7$, $d_2 + x_5 + x_6 + x_7$ with $x_5 \in \{0, 1, 2\}$, $x_6, x_7 \in \{0, 1\}$. To be more precise, we use the following simple facts which represent "conservation rules" between the difference parameters:

$$\sum_{j=0}^{1} d_E(i, j, w) = |E_i|\,, \quad i = 0, 1\,;$$

$$\sum_{i=0}^{1} d_E(i, j, w) = |E_j|\,, \quad j = 0, 1\,;$$

$$\sum_{i,j=0}^{1} d_E(i, j, w) = N\,.$$

Now the assertion of the theorem follows immediately after solving corresponding simple systems of linear equations.

Corollary 1. *The binary cyclotomic generator of order* 4 *defined by (4) has the ideal difference property if and only if we choose* $N = x^2 + 4y^2$ *such that* y *is a small odd integer.*

P r o o f . By (5) and (6), the biggest difference between the difference parameters is $d_1 + 2 - d_1 = y + 2$. Particularly, if $N = x^2 + 4$, the difference parameters are $t - 1$, t, $t + 1$, $t + 2$.

We summarize the obtained results in the following theorem:

Theorem 5. *If we choose* N *to be an o-prime such that 2 is a primitive root of* N*, and the quadratic form of* N *is* x^2+4 *with* $x \equiv 1 \pmod N$*, then the binary cyclotomic generator of order* 4 *defined by (4) has the largest possible linear and sphere complexity, and the ideal difference property.*

The last deal of work is to find some primes recommended by Theorem 5 and to test their statistical properties.

6 STATISTICAL TESTS

We have tested the pattern distribution property (see [2], [6]) for binary sequences generated by cyclotomic generators of order 4 with $N_1 = 64013$, $N_2 = 227533$, $N_3 = 85853$, $N_4 = 76733$, $N_5 = 205213$, $N_6 = 514093$, $N_7 = 727613$, $N_8 = 700573$, $N_9 = 458333$, $N_{10} = 8323229$. By the previous sections, the sequences have the ideal difference property, which implies, as we have mentioned in §3, the ideal two-bit pattern distribution property. Thanks to the construction of generator, the sequences also pass one-bit pattern distribution test, i.e. the number of 1's is approximately the same as the number of 0's. As far as the tests on pattern distribution for patterns of length $k \geq 3$, the results vary depending on N and k. Therefore we have focused on patterns of length 4, according to the standard FIPS 140-1 [7]. This test has been passed by all $N's$ except for N_2 and N_5. Other tests recommended in FIPS 140-1 (the number of occurrences of runs — consecutive 1's or 0's — of given length) have been passed by all N's.

7 FINAL REMARKS

We have shown that binary cyclotomic generators of order 4 have (for a special choice of modul N) some "ideal" properties: large linear and sphere complexity, security against differential attack, randomness. However, there is still a deal of security aspects that we have not touched. It could be a subject for further investigations.

Acknowledgements

We would like to thank Prof. Otokar Grošek for help and useful tips.

References

[1] BIRKHOFF, G.—BARTEE, T. C.: Modern Applied Algebra, McGraw-Hill, New York, 1970. (in Slovak: Alfa 1981)

[2] CUSICK, T. W.—DING, C.—RENVALL, A.: Stream Ciphers and Number Theory, Elsevier, Amsterdam, 1998.

[3] DICKSON, L. E.: Cyclotomy and trinomial congruences, Trans. Amer. Math. Soc. **37** (1935), 363–380.

[4] GROŠEK, O.—PORUBSKÝ, Š.: Cryptography — Algorithms, Methods, Practice (Šifrovanie — Algoritmy, metódy, prax), Grada, 1992. (in Slovak)

[5] KOBLITZ, N.: A Course in Number Theory and Cryptography, Springer-Verlag, New York, 1987.

[6] KNUTH, D. E.: The Art of Computer Programming, vol. 2 Seminumerical Algorithms, Addison-Wesley, 1969.

[7] MENEZES, A.—van OORSCHOT, P.—VANSTONE, S.: Handbook of Applied Cryptography, CRC Press, 1996, (www.cacr.math.uwaterloo.ca/hac).

Received 7 July 2000

Hana Lichardová (1965) received the Ms degree (RNDr) in Mathematics in 1989 from Comenius University, where she also graduated (PhD) in May, 2000. She works as a teaching assistant in the Department of Mathematics, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology

Marek Greško (1977) is a student of computer science at the Faculty of Electrical Engineering and Information Technology of SUT. He received the Bc degree in 1999. His supervisor is Hana Lichardová.