BBS generator using the function $x^2 - 2 \pmod n$

Raúl DURÁN DÍAZ
Departamento de Tratamiento de la Información y Codificación
Instituto de Física Aplicada, CSIC
C/ Serrano 144, E-28006 Madrid, Spain

and

Alberto PEINADO DOMÍNGUEZ
Departamento de Ingeniería de Comunicaciones
ETS Ingeniería de Telecomunicación
Universidad de Málaga
Campus de Teatinos, E-29071 Málaga, Spain

ABSTRACT

A BBS-like generator is discussed for which the quadratic function $F\colon x \mapsto x^2 - 2 \pmod n$, where $n = p \cdot q$ is the product of two distinct primes, is used. The maximal cycle length of the orbits produced by iterating F is obtained and the particular important cases in which p, q are both 1- and 2-safe are analyzed in deeper detail.

Keywords: BBS Generator, Quadratic Functions on Finite Fields, Safe Primes.

1. INTRODUCTION

The BBS Generator [3] is defined by the quadratic function $f\colon \mathbb{Z}_n \to \mathbb{Z}_n$, $f(x) = x^2 \pmod n$ on the set of the quadratic residues of integers modulo n, where n is a Blum integer (*i.e.*, n is the product of two distinct prime numbers both congruent to 3 (mod 4)) as follows: Starting from a seed x_0 and iterating $x_{i+1} \equiv x_i^2 \pmod n$, one obtains a binary sequence $b_i = \text{parity}\,(x_i)$. The cryptographic security of this generator in predicting sequences to the left, *i.e.*, the obstruction in constructing a *previous bit predictor* (*cf.* [7, §12.3.1]) is closely related to the difficulty of factoring n, which has been so far assumed to be a hard problem. Blum, Blum and Shub [3] proved that the BBS Generator is a cryptographically secure pseudo-random bit generator under the quadratic residuosity assumption. From the results in [1], this assumption can be replaced by the hypothesis that factoring Blum integers is a hard problem. The BBS Generator allowed them to introduce a public-key cryptosystem based on the difficulty of taking square roots in $\mathbb{Z}_n^*$. In [9] a stronger result was proved related to the security of the BBS Generator: This generator is cryptographically secure under the assumption that the integer factorization problem is intractable.

In practice, however, two problems arise. As the function $x^2 \pmod n$ provides different orbits depending on the selected initial seed, it is a must

- to determine moduli n producing orbits whose period is exactly known in advance, and
- to determine the seeds x_0 for which this period is obtained.

These problems were addressed and solved in [4], where the authors determine explicitly both a class of moduli $n = p \cdot q$ and the seeds in $\mathbb{Z}_n$ which produce orbits of maximal period for the function $x^2 \pmod n$. They also supply a sharp general upper bound for the period of any orbit.

The function f above does not represent all possible quadratic functions in $\mathbb{Z}_n$ since it is not difficult to see that it is not linearly conjugated to $f_c\colon \mathbb{Z}_p \to \mathbb{Z}_p$, $f_c(x) = x^2 + c$, for $c \neq 0$ (see [6]).

In this communication we face a part of the aforementioned problems for the function $F = f_c$, with $c = -2$. While no theoretical background is offered, the experimental results obtained along with results from other authors (*e.g.*, [8]), seem to confirm that the maximal length cycles are precisely reached in this case.

2. PRELIMINARIES

Let $f\colon X \to X$ be a map on a finite set. The f-orbit

of an element $x \in X$ is defined by

$$O_f(x) = \{f^n(x) \mid n \in \mathbb{N}\},$$

where f^n denotes the n-th iteration of f; for the sake of simplicity we also write $O(x)$ when the function f is understood. Let $h = h(x)$ be the least positive integer for which an integer k exists such that,

(i) $0 \leq k < h$,

(ii) $f^k(x) = f^h(x)$.

The set of elements $f^0(x) = x, f^1(x), \ldots, f^{k-1}(x)$ is called the "tail" $T(x)$ of the orbit and the set of elements $f^k(x), f^{k+1}(x), \ldots, f^{h-1}(x)$ is called the "cycle" $C(x)$ of the orbit, and $l(x) = l_f(x) = h - k$ is the length or the period of the cycle (*cf.* [4, 5]). If $X = \mathbb{Z}_n$ then we usually write $l_n(x)$ instead of $l(x)$.

A very well-known case corresponds to the mapping $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$, $f(x) = x^2$. The orbits of this function whose cycle is of maximal length, have been completely characterized and the prime numbers producing such orbits have been classified. Precisely, we have the following results (see [4]):

(1) If p is odd, the length of the tail of $O(x)$ is at least $v_2(r)$, where r is the order of x in $\mathbb{Z}_p^*$. The tail of $O(x)$ is maximal if and only if x is a quadratic non-residue and, in this case, $k(x) = v_2(p-1)$, where $v_p(e)$ is the multiplicity of the prime number p in the factorization of the integer e.

(2) If $p \equiv 3 \pmod 4$, then

   (a) For every $x \in \mathbb{Z}_p^*$, $x \neq 1$, $l_p(x)$ coincides with the order of 2 in $\mathbb{Z}_r^*$, where r is the order of x or x^2 in $\mathbb{Z}_p^*$, depending on x being a quadratic residue or a quadratic non-residue.

   (b) For every $x \in \mathbb{Z}_p^*$, $l_p(x) \leq \frac{1}{2}(p-3)$.

   (c) If x is a quadratic residue, then the tail of $O(x)$ is empty; if x is a quadratic non-residue, then the tail of $O(x)$ is $\{x\}$.

(3) Let $p = 2p_1 + 1$ be a 1-safe prime number.

   (a) If 2 is a generator of $\mathbb{Z}_{p_1}^*$, then every quadratic residue $x \in \mathbb{Z}_p^*$, $x \neq 1$, produces an orbit of maximal length $l_p(x) = \frac{1}{2}(p-3)$.

   (b) If -2 is a generator of $\mathbb{Z}_{p_1}^*$ but 2 is not a generator of $\mathbb{Z}_{p_1}^*$, then $p_1 \equiv 3 \pmod 4$ and every quadratic residue $x \in \mathbb{Z}_p^*$, $x \neq 1$, produces an orbit of length $l_p(x) = \frac{1}{4}(p-3)$.

   (c) In addition, if $p_1 > 3$ is also safe (*i.e.*, p is 2-safe), then 2 is a generator of $\mathbb{Z}_{p_1}^*$ if and only if $\frac{1}{4}(p_1+1) = \frac{1}{8}(p+1)$ is odd.

Again in [4], the case of a composite modulus $n = p \cdot q$ is considered and the problem of characterizing moduli n, for which the orbits are of maximal length, is analyzed. Let $p = 2p_1 + 1$, $q = 2q_1 + 1$ be two 1-safe prime numbers. Set $n = p \cdot q$. An orbit of the $x^2 \pmod n$ function exists whose cycle has a maximal period equal to $\frac{1}{8}(p-3)(q-3)$, if and only if the following two conditions hold:

(1) Either 2 is a generator of $\mathbb{Z}_{p_1}^*$ and either 2 or -2 is a generator of $\mathbb{Z}_{q_1}^*$, or 2 is a generator of $\mathbb{Z}_{q_1}^*$ and either 2 or -2 is a generator of $\mathbb{Z}_{p_1}^*$.

(2) $\gcd(p_1 - 1, q_1 - 1) = 2$.

These conditions, which determine the maximal period of the cycles, are weaker (*i.e.*, easier to test) than those imposed in [3, Theorem 9]. In particular, they are satisfied if p and q are both 2-safe prime integers with p, $q > 11$ and either $p_1 \equiv 3 \pmod 8$ or $q_1 \equiv 3 \pmod 8$.

In a similar way, our aim is to obtain analogous results for the function F.

3. ORBITS IN $\mathbb{Z}_p$

The upper bounds proved for the orbits of the functions $f_c\colon \mathbb{Z}_p \to \mathbb{Z}_p$, $f_c(x) = x^2 + c$, $c \neq 0$ are not so accurate as those proved for the the function f of the BBS generator. Let $L_p(c)$ be the greatest value of $l_p(x)$ when x runs $\mathbb{Z}_p$; *i.e.*,

$$L_p(c) = \max_{x \in \mathbb{Z}_p} l_p(x).$$

As a particular case of the results proved in [6], we have, assuming $p > 9$, that the following results hold:

If -1 is not a quadratic residue, then $L_p(c)$ is bounded as follows:

(1) $L_p(c) \leq \frac{1}{8}(3p+3)$, if $\frac{1}{4}(p-3)$ is odd.

(2) $L_p(c) \leq \frac{1}{8}(3p-1)$, if $\frac{1}{4}(p-3)$ is even and $-2c$ is a quadratic residue.

(3) $L_p(c) \leq \frac{1}{8}(3p+7)$, if $\frac{1}{4}(p-3)$ is even and $-2c$ is not a quadratic residue.

If -1 is a quadratic residue, then $L_p(c)$ is bounded as follows:

(4) $L_p(c) \leq \frac{1}{8}(3p+5)$, if $\frac{1}{4}(p-1)$ is even.

(5) $L_p(c) \leq \frac{1}{8}(3p+1)$, if $\frac{1}{4}(p-1)$ is odd and $-2c$ is a quadratic residue.

(6) $L_p(c) \leq \frac{1}{8}(3p+9)$, if $\frac{1}{4}(p-1)$ is odd and $-2c$ is not a quadratic residue.

Nevertheless, experimental results show that $L_p(c)$ is bounded by $\frac{1}{4}(p-1)$ (resp. $\frac{1}{4}(p-3)$) if $p \equiv 1 \pmod 4$ (resp. $p \equiv 3 \pmod 4$). For a discussion on these bounds see [6]. Hence, roughly speaking, in the theoretical bounds above the factor 3 should be replaced by 2, thus slimming the factor $\frac{3}{8}$ to $\frac{1}{4}$, but to obtain this improvement has proved to be difficult. In spite of this, it is shown in [2] that these bounds are reached in the particular case of the function $F = f_{-2}$. In addition, computations of the length of all cycles of all functions f_c on the set of prime numbers less than 10^4 show indeed that the maximal cycle length for these functions is precisely attained for $c = -2$; see [6, 8].

Moreover, in the particular case when p is a 1-safe prime, the following more accurate bounds for the function F, have been recently obtained in [2]:

Let $e = order'_d(2)$ be the least integer such that $2^e \equiv \pm 1 \pmod d$ for d odd. Let p be a 1-safe prime, *i.e.*, $p = 2p_1+1$, with p, p_1 odd primes such that either 2 or -2 is a generator of $\mathbb{Z}^*_{p_1}$. Writing $p-1 = 2^\tau \rho$, $p+1 = 2^{\tau'}\rho'$, with both ρ, and ρ' odd, the orbits of the function F verify that:

(1) There exists only one cycle with maximal length $\frac{1}{4}(p-3)$, and each element of it has a dangling tail with precisely one element, *i.e.*, the orbits leading to this cycle have tail lengths no greater than 1.

(2) For each odd proper divisor d of $\frac{1}{4}(p+1)$, there exist cycles of length $order'_d(2)$. Besides, the graph of the function F displays a binary tree of depth $\tau' \geq 2$, hanging off each element of the cycle.

Another interesting particular case occurs when p is 2-safe, *i.e.*, $p = 2p_1+1$, $p_1 = 2p_2+1$, p, p_1, p_2 being odd primes. Now we are led to distinguish two different cases. If $\frac{1}{8}(p+1)$ is odd, then we have for the orbits of F that

(1) There exists only one cycle with maximal length $\frac{1}{4}(p-3)$, and each element of it has a dangling tail with precisely one element, *i.e.*, the orbits leading to this cycle have tail lengths no greater than 1.

(2) For each proper odd divisor d of $\frac{1}{8}(p+1)$, there exist cycles of length $order'_d(2)$. Besides, the graph of the function F displays a binary tree of depth 3 hanging off each element of the cycle.

On the other hand, if $\frac{1}{8}(p+1)$ is even, again for the orbits of F, we have

(3) There exists only one cycle with maximal length $\frac{1}{4}(p-3)$, and each element of it has a dangling tail with precisely one element, *i.e.*, the orbits leading to this cycle have tail lengths no greater than 1.

(4) For each proper odd divisor d of $\frac{1}{16}(p+1)$, there exist cycles of length $order'_d(2)$. Besides, the graph of the function F displays a binary tree of depth 4 hanging off each element of the cycle.

4. ORBITS IN $\mathbb{Z}_n$

Let us begin with the following

Lemma: Let $F(x) = a_0 + a_1 x + \ldots + a_d x^d$ be a polynomial with integer coefficients, $a_i \in \mathbb{Z}$, and let $l_n(x)$ be the period of the cycle of the orbit $O(x)$ with respect to the function $F \pmod n$. If $n = p \cdot q$, and p, q are two relatively prime numbers, then we have

$$\operatorname{lcm}(l_p(x), l_q(x)) = l_n(x).$$

Proof: By the Chinese Remainder Theorem there exists a ring isomorphism

$$\varphi\colon \mathbb{Z}_n \to \mathbb{Z}_p \oplus \mathbb{Z}_q,$$
$$\varphi(x \pmod n) = (x \pmod p, x \pmod q),$$

and we have

$$\varphi \circ F \pmod n = (F \pmod p, F \pmod q) \circ \varphi.$$

Hence

$$\varphi(F^h(x) \pmod n) = (F^h(x) \pmod p, F^h(x) \pmod q),$$

and the result follows from the very definition of $l(x)$. □

Proposition: Let $n = p \cdot q$, where both p and q are 1-safe primes, *i.e.*, $p = 2p_1 + 1$, $q = 2q_1 + 1$. Then, the maximal cycle length of the orbits of the function $F\colon \mathbb{Z}_n \to \mathbb{Z}_n$, $F(x) = x^2 - 2$, is given by,

$$l_n(x) = \frac{(p_1-1)(q_1-1)}{2\gcd(p_1-1, q_1-1)}.$$

Proof: By applying the previous lemma, we have

$$\begin{aligned} l_n(x) &= \operatorname{lcm}(l_p(x), l_q(x)) \\ &= \operatorname{lcm}\left(\frac{p-3}{4}, \frac{q-3}{4}\right) \\ &= \operatorname{lcm}\left(\frac{p_1-1}{2}, \frac{q_1-1}{2}\right) \\ &= \frac{(p_1-1)(q_1-1)}{2\gcd(p_1-1, q_1-1)}. \end{aligned}$$

□

It is more interesting to consider the case where both p and q are 2-safe primes:

Corollary: If p and q are 2-safe primes, then we have

$$l_n(x) = \frac{1}{4}(p_1 - 1)(q_1 - 1) = \frac{1}{16}(p - 3)(q - 3).$$

Proof: In fact, as in the present case we have

$$\gcd(p_1 - 1, q_1 - 1) = 2,$$

the result follows from the previous proposition. □

5. CONCLUDING REMARKS

(1) After the careful research presented here, it is not to be expected that any quadratic function may improve the one used by the BBS cryptosystem, namely, $f(x) = x^2 \pmod n$, in terms of maximal length cycles produced. Besides, these maximal length cycles seem to be generated always using the same value for c, in particular, $c = -2$.

(2) The maximal cycle lengths have been obtained for the function $F = f_{-2}$ and they are at best, half as long as those obtained for the BBS function (see §2 and §4).

(3) It remains as an open issue whether the function $f_c \colon \mathbb{Z}_p \mapsto \mathbb{Z}_p$ admits at least one cycle with length $O(p)$ for almost any c.

6. REFERENCES

[1] W. Alexi, B. Chor, O. Goldreich, C.P. Schnorr, "RSA and Rabin functions: certain parts are as hard as the whole", SIAM J. Comput., Vol. 17, 1988, pp. 194–209.

[2] A.M. Barbancho, J. Cintado, J. Muñoz, A. Peinado, "Sobre la Complejidad Lineal de las secuencias de longitud máxima producidas por el generador de Pollard", preprint.

[3] L. Blum, M. Blum, M. Shub, "A simple unpredictable pseudo-random number generator", SIAM J. Comput., Vol. 15, 1986, pp. 364–383.

[4] L. Hernández Encinas, F. Montoya Vitini, J. Muñoz Masqué, A. Peinado Domínguez, "Maximal periods of orbits of the BBS generator", Proc. 1998 International Conference on Information Security & Cryptology (ICISC'98), Seoul, Korea, 1998, pp. 71–80.

[5] W. Narkiewicz, "Polynomial mappings", Lecture Notes in Math., Vol. 1600, Springer-Verlag, 1995.

[6] A. Peinado, F. Montoya, J. Muñoz, A.J. Yuste, "Maximal periods of x^2+c in $\mathbb{F}_q$", Lecture Notes in Comput. Sci., Vol. 2227, 2001, pp. 219–228.

[7] D.R. Stinson, Cryptography. Theory and Practice, Boca Raton, FL: CRC Press, Inc., 1995.

[8] T. Vasiga, J. Shallit, "On the iteration of certain quadratic maps over $GF(p)$", preprint.

[9] U.V. Vazirani, V.V. Vazirani, "Efficient and secure pseudo-random number generator", in Proc. IEEE 25th Symp. Found. Comput. Sci., 1984, pp. 458–463.