Cryptanalysis of the Quadratic Generator

Domingo Gomez, Jaime Gutierrez, Alvar Ibeas

Faculty of Sciences,
University of Cantabria,
Santander E–39071, Spain
jaime.gutierrez@unican.es

Abstract. Let p be a prime and let a and c be integers modulo p. The quadratic congruential generator (QCG) is a sequence (v_n) of pseudo-random numbers defined by the relation $v_{n+1} \equiv av_n^2 + c \bmod p$. We show that if sufficiently many of the most significant bits of several consecutive values v_n of the QCG are given, one can recover in polynomial time the initial value v_0 (even in the case where the coefficient c is unknown), provided that the initial value v_0 does not lie in a certain small subset of exceptional values.

1 Introduction

For a prime p, denote by $\mathbb{F}_p$ the field of p elements and always assume that it is represented by the set $\{0, 1, \ldots, p-1\}$. Accordingly, sometimes, where obvious, we treat elements of $\mathbb{F}_p$ as integer numbers in the above range.

For fixed $a \in \mathbb{F}_p^*$, $c \in \mathbb{F}_p$, the *quadratic generator* (v_n) of elements of $\mathbb{F}_p$ is given by the recurrence relation

$$v_{n+1} \equiv av_n^2 + c \bmod p \qquad n = 0, 1, \ldots, \tag{1}$$

where v_0 is the *initial value*.

We refer to the coefficients a and c as the *multiplier* and *shift*, respectively. This generator has many interesting applications in cryptography, see [4, 14–17, 9].

In the cryptographic setting, the initial value v_0 and the constants a and c are assumed to be the secret key, and we want to use the output of the generator as a stream cipher. Of course, if several consecutive values v_n are revealed, it is easy to find v_0, a and c. So in this setting, we output only the most significant bits of each v_n in the hope that this makes the resulting output sequence difficult to predict. The paper [3], shows that not too many bits can be output at each stage: the quadratic generator is unfortunately polynomial time predictable if sufficiently many bits of its consecutive elements are revealed, so long as a small number of secret keys are excluded. However, some of the results in that paper only hold after excluding a small set of a, see [3, Theorem 3]. If this small set is not excluded, the algorithm for finding the secret information may fail. An optimist might hope that by deliberately choosing a to lie in this excluded

set, one can generate cryptographically stronger sequences. This paper aims to show that this strategy is unlikely to succeed. Namely we introduce some modifications and additions to the method of [3] which allow us to attack the generators no matter how the value of a is chosen. In fact, our idea is similar to the approach in paper [2]. We demonstrate our approach in the special cases when a and c are public and when c is secret and a is public. This last case was not considered in the mentioned paper. But we believe that the extra strength of the result we obtain makes this situation of interest in its own right. We also believe this approach can be extended to the case when both a and c are secret [3, Theorem 5].

Assume that the sequence (v_n) is not known but, for some n, some approximations w_j are given. We show that if a and c are public or if a is public and c secret the values v_{n+j} and a can be recovered from this information in polynomial time if the approximations w_j are sufficiently good and if a certain small set of initial values v_0 are excluded. (The results in [3] exclude a small set of a in addition to values of v_0, and so in this sense our result here is stronger.)

The remainder of the paper is structured as follows.

We start with a short outline of some basic facts about lattices in Section 2.1 and polynomial in congruences Section 2.2. In Section 3 we consider the cases of quadratic generator with known multiplier and shift in Subsection 3.1 and with known multiplier and unknown shift in Subsection 3.2. Finally, Section 4 makes some final comments and poses several open questions.

Acknowledgment. This work is partially supported by Spanish Ministry of Science grant MTM2004-07086.

2 Lattices and Polynomials

2.1 Background on Lattices

Here we collect several well-known facts about lattices which form the background to our algorithms.

We review several related results and definitions on lattices which can be found in [5]. For more details and more recent references, we also recommend consulting [1, 6, 7, 11–13].

Let $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_s\}$ be a set of linearly independent vectors in $\mathbb{R}^r$. The set

$$\mathcal{L} = \{\boldsymbol{z} \ : \ \boldsymbol{z} = c_1\boldsymbol{b}_1 + \ldots + c_s\boldsymbol{b}_s, \quad c_1, \ldots, c_s \in \mathbb{Z}\}$$

is called an *s-dimensional lattice* with *basis* $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_s\}$. If $s = r$, the lattice L is of *full rank*.

To each lattice $\mathcal{L}$ one can naturally associate its *volume*

$$\mathrm{vol}\,(\mathcal{L}) = \left(\det\left(\langle \boldsymbol{b}_i, \boldsymbol{b}_j\rangle\right)_{i,j=1}^{s}\right)^{1/2},$$

where $\langle \boldsymbol{a}, \boldsymbol{b}\rangle$ denotes the inner product. This definition does not depend on the choice of the basis $\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_s\}$.

For a vector $\boldsymbol{u}$, let $\|\boldsymbol{u}\|$ denote its *Euclidean norm*. The famous Minkowski theorem, see Theorem 5.3.6 in Section 5.3 of [5], gives the upper bound

$$\min\{\|\boldsymbol{z}\|:\ \boldsymbol{z} \in \mathcal{L} \setminus \{\mathbf{0}\}\} \le s^{1/2} \operatorname{vol}(\mathcal{L})^{1/s} \tag{2}$$

on the shortest nonzero vector in any s-dimensional lattice $\mathcal{L}$ in terms of its volume. In fact, $s^{1/2}$ can be replaced by the *Hermite constant* $\gamma_s^{1/2}$, for which we have

$$\frac{1}{2\pi e} s + o(s) \le \gamma_s \le \frac{1.744}{2\pi e} s + o(s), \qquad s \to \infty.$$

The Minkowski bound (2) motivates a natural question: how to find the shortest vector in a lattice. The celebrated *LLL algorithm* of Lenstra, Lenstra and Lovász [10] provides a desirable solution in practice, and the problem is known to be solvable in deterministic polynomial time (polynomial in the bit-size of the basis of $\mathcal{L}$), provided that the dimension of $\mathcal{L}$ is fixed (see Kannan [8, Section 3], for example). The lattices in this paper are of fixed dimension. (Note that there are several indications that the shortest vector problem is **NP**-complete when the dimension grows.)

In fact, in this paper we consider only very special lattices. Namely, only lattices which are consisting of integer solutions $\boldsymbol{x} = (x_0, \dots, x_{s-1}) \in \mathbb{Z}^s$ of the system of congruences

$$\sum_{i=0}^{s-1} a_{ij} x_i \equiv 0 \bmod q_j, \qquad j = 1, \dots, m,$$

modulo some integers $q_1, \dots, q_m$. Typically (although not always) the volume of such a lattice is the product $Q = q_1 \dots q_m$. Moreover, all the aforementioned algorithms, when applied to such a lattice, become polynomial in $\log Q$.

2.2 Polynomial congruences

Our second basic tool is essentially the theorem of Lagrange which asserts that a non-zero univariate polynomial of degree N over any field has no more than N zeros in this field.

The polynomials we consider belong to a certain family of functions parametrised by small vectors in a certain lattice, thus the size of the family can be kept under control.

Now we present a technical result for later use. The following lemma is an adaptation of an argument in the paper [2]:

Lemma 1. *Let $p > 5$ be a prime and let α be a nonzero integer modulo p. Then the bivariate congruence*

$$\alpha x \equiv y \bmod p,$$

with $\gcd(x, y) = 1$, $|x| < p^{1/3}$ and $|y| < p^{1/3}$ has at most two integer solutions (x, y).

Proof. Suppose that (x, y) and (x', y') are two solutions. Then $xy' \equiv yx' \bmod p$ and since both xy' and yx' have absolute value at most $p^{2/3}$ we find that $xy' = yx'$. But since $\gcd(x, y) = \gcd(x', y') = 1$ we now obtain the thesis.

3 Predicting the Quadratic Generator

Throughout the paper the term polynomial time means polynomial in $\log p$. Our results involve another parameter Δ which measures how well the values w_j approximate the terms v_{n+j}. This parameter is assumed to vary independently of p subject to satisfying the inequality $\Delta < p$ (and is not involved in the complexity estimates of our algorithms.)

More precisely, we say that w is a Δ-*approximation* to u if $|w - u| \le \Delta$. In all of our results, the case where Δ grows like a fixed power p^δ where $0 < \delta < 1$ corresponds to the situation where a positive proportion δ of the least significant bits of terms of the output sequence remain hidden.

To simplify the notation, we assume that $n = 0$ from now on.

3.1 Predicting the Quadratic generator with known multiplier and shift

We can formulate the main result in this subsection.

Theorem 1. *Let p be a prime number and let Δ be an integer such that $p > \Delta \ge 1$. For any $a \in \mathbb{F}_p^*$ and $c \in \mathbb{F}_p$, there exists a set $\mathcal{U}(\Delta; a, c) \subseteq \mathbb{F}_p$ of cardinality $\#\mathcal{U}(\Delta; a, c) = O(\Delta^4)$ with the following property. There exists an algorithm which, when given a, c and Δ-approximations w_0, w_1 to two consecutive values v_0, v_1 produced by the quadratic generator (1), where $v_0 \notin \mathcal{U}(\Delta; a, c)$, returns the value of v_0 in deterministic polynomial time.*

Proof. The theorem is trivial when $\Delta^4 \ge p$ and we assume that $\Delta^4 < p$. We fix $a, c \in \mathbb{F}_p$ and we assume that $v_0 \in \mathbb{F}_p$ is chosen so as not to lie in a certain subset $\mathcal{U}(\Delta; a, c)$ of $\mathbb{F}_p^*$ of cardinality $O(\Delta^4)$. As its definition is fairly complicated we define it gradually.

Let $\varepsilon_j := v_j - w_j$, $j = 0, 1$. From $v_1 \equiv a v_0^2 + c \bmod p$, we obtain

$$w_1 + \varepsilon_1 - a(w_0 + \varepsilon_0)^2 - c \equiv 0 \bmod p.$$

Writing

$$A \equiv (w_1 - a w_0^2 - c) \bmod p, \qquad B_1 \equiv -2 a w_0 \Delta \bmod p,$$
$$B_2 \equiv \Delta \bmod p, \qquad C \equiv -a\Delta^2 \bmod p,$$

we obtain

$$A\Delta^2 + B_1 \Delta \varepsilon_0 + B_2 \Delta \varepsilon_1 + C\varepsilon_0^2 \equiv 0 \bmod p. \tag{3}$$

Therefore the lattice $\mathcal{L}$ consisting of integer solutions

$$\boldsymbol{x} = (x_0, x_1, x_2, x_3) \in \mathbb{Z}^4$$

of the system of congruences

$$A x_0 + B_1 x_1 + B_2 x_2 + C x_3 \equiv 0 \bmod p,$$
$$x_0 \equiv 0 \bmod \Delta^2,$$
$$x_1 \equiv x_2 \equiv 0 \bmod \Delta,$$

contains a vector

$$\boldsymbol{e} = \left(\Delta^2 e_0, \Delta e_1, \Delta e_2, e_3\right) = \left(\Delta^2, \Delta\varepsilon_0, \Delta\varepsilon_1, \varepsilon_0^2\right).$$

We have

$$e_0 = 1, \qquad |e_1|, |e_2| \le \Delta, \qquad |e_3| \le \Delta^2,$$

thus

$$\|\boldsymbol{e}\| \le \left(4\Delta^4\right)^{1/2} = 2\Delta^2.$$

Let $\boldsymbol{f} = \left(\Delta^2 f_0, \Delta f_1, \Delta f_2, f_3\right)$ be a shortest nonzero vector in $\mathcal{L}$. So, $\|\boldsymbol{f}\| \le \|\boldsymbol{e}\| \le 2\Delta^2$. We have

$$|f_0| \le 2, \qquad |f_1|, |f_2| \le 2\Delta, \qquad |f_3| \le 2\Delta^2.$$

Note that we may compute $\boldsymbol{f}$ in polynomial time from the information we are given. The vector $\boldsymbol{d} = f_0\boldsymbol{e} - e_0\boldsymbol{f} = (0, \Delta d_1, \Delta d_2, d_3) \in \mathcal{L}$ and has first component 0. We might hope that $\boldsymbol{e}$ and $\boldsymbol{f}$ are always parallel. If not, we claim that $d_1 = 0$ unless v_0 belongs to the set $\mathcal{V}(\Delta; a, c)$ which we define below.

Using the definition of $\mathcal{L}$, we find that

$$-2aw_0 d_1 + d_2 - ad_3 \equiv 0 \bmod p, \tag{4}$$

where $d_i = e_i f_0 - f_i$, and thus $|d_i| \le 2|e_i| + |f_i|$ for $i = 1, 2, 3$. Hence

$$|d_1|, |d_2| \le 4\Delta, \qquad |d_3| \le 4\Delta^2. \tag{5}$$

Substituting $w_i = v_i - \varepsilon_i$, $i = 0, 1$, into the congruence (4), we find the following congruence

$$-2ad_1 v_0 \equiv E \bmod p,$$

where

$$E = a\left(-2d_1\varepsilon_0 + d_3\right) - d_2.$$

We define $\mathcal{U}(\Delta; a, c)$ as the set a values v_0 that satisfy some congruence of the form (4) with $d_1 \not\equiv 0 \bmod p$. The bounds (5) imply that d_1 can take only $O(\Delta)$ distinct values. Moreover, E can take $O(\Delta^3)$ distinct values (because $2d_1\varepsilon_0 - d_3 = O(\Delta^2)$ and $d_2 = O(\Delta)$). Since $d_1 \not\equiv 0 \bmod p$, this means that $\#\mathcal{U}(\Delta; a, c) = O(\Delta^4)$.

So, we can assume that $v_0 \notin \mathcal{U}(\Delta; a, c)$. The bound (5) on $|d_1|$ and this assumption imply

$$d_1 = 0 \quad \text{and} \quad -d_2 + ad_3 \equiv 0 \bmod p.$$

We distinguish two cases: $f_0 \neq 0$ and $f_0 = 0$ and analyze them separately.

Predicting the generator when $f_0 \neq 0$. Since $d_1 = 0$ we have $f_0\varepsilon_0 - f_1 \equiv 0 \bmod p$. The bound on $|f_1|$ shows that $\varepsilon_0 = f_1/f_0$ and so we may compute the secret information ε_0.

Predicting the generator when $f_0 = 0$. In this case we have $\boldsymbol{d} = \boldsymbol{f} = (0, 0, \Delta f_2, f_3)$ verifying $f_2 \equiv a f_3 \bmod p$. It is easy to see that $f_3 \not\equiv 0 \bmod p$. Otherwise would contradict the fact that $\boldsymbol{f}$ is a nonzero vector. Hence $f_3 a \equiv f_2 \bmod p$ and so we may write

$$sa \equiv r \bmod p, \text{ where } r = f_2/\gcd(f_2, f_3) \text{ and } s = f_3/\gcd(f_2, f_3).$$

Note that r and s are coprime,

$$|r| \le 2\Delta, \qquad |s| \le 2\Delta^2. \tag{6}$$

Moreover we know explicitly r and s since we have computed $\boldsymbol{f}$.

From the congruence (3) we derive

$$\underbrace{rw_0^2 - sw_1 + sc} + \underbrace{2rw_0}\,\varepsilon_0 - s\varepsilon_1 + r\varepsilon_0^2 \equiv 0 \bmod p$$

We now consider a new lattice: the lattice $\mathcal{L}'$ consisting of solutions $\boldsymbol{x} = (x_0, x_1, x_2) \in \mathbb{Z}^3$ of the congruences

$$\mathcal{L}' : \begin{cases} (rw_0^2 + sc - sw_1)\Delta^{-3} x_0 + 2rw_0\Delta^{-2} x_1 + x_2 \equiv 0 \bmod p \\ x_0 \equiv 0 \bmod \Delta^3 \\ x_1 \equiv 0 \bmod \Delta^2 \end{cases} \tag{7}$$

It is easy to check that the lattice (7) contains the vector

$$\boldsymbol{e'} = \left(\Delta^3, \Delta^2\varepsilon_0, r\varepsilon_0^2 - s\varepsilon_1)\right).$$

Thus the Euclidean norm $\|\boldsymbol{e'}\|$ of $\boldsymbol{e'}$ satisfies the inequality

$$\|\boldsymbol{e'}\| \le \sqrt{\Delta^6 + \Delta^6 + 16\Delta^6} = 3\sqrt{2}\Delta^3.$$

Again, we now show that all short vectors in $\mathcal{L}'$ are parallel to $\boldsymbol{e'}$ unless v_0 belongs to the set $\mathcal{V}'(\Delta; a, b)$ which we define below.

Assume, for a contradiction, that there is another vector

$$\boldsymbol{f'} = (\Delta^3 f_0', \Delta^2 f_1', f_2') \in \mathcal{L}'$$

with $\|\boldsymbol{f'}\| \le \|\boldsymbol{e'}\| \le 3\sqrt{2}\Delta^3$ which is not parallel to $\boldsymbol{e'}$. The vector $\boldsymbol{d'} \in \mathcal{L}'$ defined by

$$\boldsymbol{d'} = \boldsymbol{f'} - f_0'\boldsymbol{e'} = (0, \Delta^2 d_1', d_2').$$

verifies:

$$|d_1'| \le 9\Delta, \qquad |d_2'| \le 21\Delta^3. \tag{8}$$

Using the first congruence in (7), we find that

$$2rw_0 d_1' + d_2' \equiv 0 \bmod p. \tag{9}$$

If $d_1' \equiv 0 \bmod p$, then using bounds (8) we obtain $d_1' = d_2' = 0$. This implies that vectors $\boldsymbol{e'}$ and $\boldsymbol{f'}$ are parallel which it is a contradiction.

Substituting $w_0 = v_0 - \varepsilon_0$ in the congruence (9)

$$2rv_0d_1' \equiv E' \bmod p, \tag{10}$$

where $E' \equiv 2r\varepsilon_0 d_1' - d_2' \bmod p$. We define $\mathcal{V}'(\Delta; a, c)$ the set of values v_0 that satisfy some congruence of the form (10) with $d_1' \not\equiv 0 \bmod p$. Since $d_1' \not\equiv 0 \bmod p$, the congruence (10) can be satisfied for at most 1 values of v_0 once r, d_1' and E' have been chosen. By bounds (6) we can apply Lemma 1 then there are at most 2 choices for r. There are $O(\Delta^3)$ choices for E' since $|E'| \leq 42\Delta^3$. Hence there are only $O(\Delta^4)$ values of v_0 that satisfy some congruence of the form (10) where the d_i' and E' satisfy the appropriate bounds. This means that $\#\mathcal{V}'(\Delta; a, c) = O(\Delta^4)$. So all short vectors in $\mathcal{L}'$ are parallel to $\boldsymbol{e'}$ whenever $v_0 \notin \mathcal{V}'(\Delta; a, b)$.

Finally, we apply a deterministic polynomial time algorithm for the shortest vector problem in a finite dimensional lattice to find a shortest nonzero vector $\boldsymbol{f'}$ in $\mathcal{L}'$, and this vector must be parallel to $\boldsymbol{e'}$. We recover $\boldsymbol{e'}$ by using the fact that $\boldsymbol{e'} = \boldsymbol{f'}/f_0'$. This gives us ε_0 which is used to calculate v_0.

Defining

$$\mathcal{U}(\Delta; a, b) = \mathcal{V}(\Delta; a, b) \cup \mathcal{V}'(\Delta; a, b)$$

which concludes the proof.

As we said in the introduction section [3, Theorem 3] excludes a small set of values of a.

3.2 Predicting the Quadratic generator with known multiplier and unknown shift

In this subsection we consider the problem of breaking the quadratic generator given a and approximations to three consecutive values. We prove the following result:

Theorem 2. *Let p be a prime number and let Δ be an integer such that $p > \Delta \geq 1$. For any $a \in \mathbb{F}_p^*$ and $c \in \mathbb{F}_p$, there exists a set $\mathcal{U}(\Delta; a, c) \subseteq \mathbb{F}_p$ of cardinality $\#\mathcal{U}(\Delta; a, c) = O(\Delta^5)$ with the following property: there exists an algorithm which, when given a and Δ-approximations w_i, $i = 0, 1, 2$ to three consecutive values v_0, v_1, v_2 produced by the quadratic generator (1), where $v_0 \notin \mathcal{U}(\Delta; a, c)$, recovers v_0 and c in deterministic polynomial time.*

Proof. We can assume that $\Delta^5 < p$ and that $v_0 \in \mathbb{F}_p$ is chosen so as not to lie in a certain subset $\mathcal{U}(\Delta; a, c)$ of $\mathbb{F}_p^*$ of cardinality $O(\Delta^5)$. As its definition is fairly complicated we define it gradually. By hypothesis, we have:

$$v_i = w_i + \varepsilon_i,\ |\varepsilon_i| \leq \Delta,\ i = 0, 1, 2\ , \quad \text{and} \quad av_i^2 + c \equiv v_{i+1} \bmod p,\ i = 0, 1.$$

So, we obtain the following equation that involves the known parameters a, w_i and with the desired information ε_i:

$$(aw_0^2 - w_1 - aw_1^2 + w_2) + 2aw_0 \underbrace{\varepsilon_0} - (1+2aw_1) \underbrace{\varepsilon_1} + \underbrace{\varepsilon_2} + a \underbrace{(\varepsilon_0^2 - \varepsilon_1^2)} \equiv 0 \bmod p \tag{11}$$

Then, the vector $(1, \varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_0^2 - \varepsilon_1^2)$ satisfies the congruence (11) with known coefficients. In order to handle a vector with norm-balanced components, we write:

$$(aw_0^2 - w_1 - aw_1^2 + w_2) \underbrace{\Delta^2} + 2aw_0\Delta \underbrace{\Delta\varepsilon_0} - (1 + 2aw_1)\Delta \underbrace{\Delta\varepsilon_1} + \\ + \Delta \underbrace{\Delta\varepsilon_2} + a\Delta^2 \underbrace{(\varepsilon_0^2 - \varepsilon_1^2)} \equiv 0 \bmod p.$$

So, the $\boldsymbol{e} := (\Delta^2, \Delta\varepsilon_0, \Delta\varepsilon_1, \Delta\varepsilon_2, \varepsilon_0^2 - \varepsilon_1^2)$ lies in the lattice $\mathcal{L}$ consisting of $(x_0, x_1, x_2, x_3, x_4) \in \mathbb{Z}^5$ verifying:

$$\mathcal{L} : \begin{cases} (aw_0^2 - w_1 - aw_1^2 + w_2)x_0 + 2aw_0\Delta x_1 - (1 + 2aw_1)\Delta x_2 + \\ \qquad + \Delta x_3 + a\Delta^2 x_4 \equiv 0 \bmod p, \\ x_0 \equiv 0 \bmod \Delta^2, \\ x_1, x_2, x_3 \equiv 0 \bmod \Delta. \end{cases}$$

Also, we have $\|\boldsymbol{e}\| < 3\Delta^2$. We can compute on polynomial time a shortest vector $\boldsymbol{f}$ in the lattice $\mathcal{L}$:

$$\begin{aligned} \boldsymbol{f} =: (\Delta^2 f_0, \Delta f_1, \Delta f_2, \Delta f_3, f_4), \quad \|\boldsymbol{f}\| < 3\Delta^2, \\ |f_0| < 3, \ |f_1|, |f_2|, |f_3| < 3\Delta, \ |f_4| < 3\Delta^2. \end{aligned} \tag{12}$$

We hope that $\boldsymbol{e}$ and $\boldsymbol{f}$ are always parallel, that this

$$\boldsymbol{d} := f_0\boldsymbol{e} - \boldsymbol{f} = (0, \Delta d_1, \Delta d_2, \Delta d_3, d_4) \in \mathcal{L}$$

is the null vector. If not, we claim that $d_1 = d_2 = 0$ unless v_0 belongs to the set $\mathcal{V}(\Delta; a, c)$ which we define below. Substituting in (11) we derive

$$2aw_0 d_1 - (1 + 2aw_1)d_2 + d_3 + ad_4 \equiv 0 \bmod p,$$

and using the bounds in (12)

$$|d_1|, |d_2|, |d_3| < 6\Delta, |d_4| < 9\Delta^2 \tag{13}$$

Now, plugin $w_i = v_i - \varepsilon_i, i = 0, 1$ in the above congruence, we get

$$2a(v_0 - \varepsilon_0)d_1 - (1 + 2a(v_1 - \varepsilon_1))d_2 + d_3 + ad_4 \equiv 0 \bmod p.$$

Substituting $v_1 \equiv av_0^2 + c \bmod p$ in the above congruence we obtain:

$$2ad_1v_0 - 2ad_1\varepsilon_0 - d_2 - 2ad_2(av_0^2 + c) + 2ad_2\varepsilon_1 + d_3 + ad_4 \equiv 0 \bmod p.$$

Then, $P(v_0) \equiv 0 \bmod p$ with

$$P(T) = -2a^2d_2T^2 + 2ad_1T - 2ad_1\varepsilon_0 - d_2 - 2ad_2c + 2ad_2\varepsilon_1 + d_3 + ad_4.$$

Let's define the first piece of the exceptional set $\mathcal{V}(\Delta; a, c)$ as the set of elements $v_0 \in \mathbb{F}_p$ such that there exist integers $d_1, d_2, d_3, d_4, \varepsilon_0, \varepsilon_1$ satifying:

$$d_1d_2 \not\equiv 0 \bmod p \quad \text{and} \quad P(v_0) \equiv 0 \bmod p.$$

The bounds in (13) imply that the number of elements in $\mathcal{V}(\Delta; a, c)$ is $O(\Delta^5)$, because in the equation:

$$-2a^2d_2v_0^2 + 2ad_1v_0 + 2ad_2c + d_2 - d_3 \equiv a(2d_2\varepsilon_1 - 2d_1\varepsilon_0 + d_4) \bmod p,$$

there may exist less than $O(\Delta^2)$ possibilities for the right term. On the other hand, in the left term, there may appear $O(\Delta^3)$ different (always nonconstant) polynomials.

Whenever $v_0 \notin \mathcal{V}(\Delta; a, c)$, it must be $d_1 = d_2 = 0$, because of the bounds for these integers, see again (13).

Once under this assumption, we look at the first coefficient of the vector $\boldsymbol{f}$. If $f_0 \neq 0$, we can easily recover:

$$\varepsilon_0 = f_1(f_0)^{-1},\ \varepsilon_1 = f_2(f_0)^{-1},\ \text{(as identities in } \mathbb{Z}).$$

We concentrate the study when $f_0 = 0$. Then, $\boldsymbol{d} = (0, 0, \Delta d_2, \Delta d_3, d_4)$ with

$$d_3 + ad_4 = f_3 + af_4 \equiv 0 \bmod p$$

It is easy to see that $f_4 \not\equiv 0 \bmod p$, otherwise $\boldsymbol{f}$ is the null vector. We compute integers r, s, with $\gcd(r, s) = 1$, and $|r| < 3\Delta$, $|s| < 3\Delta$, such that:

$$a \equiv rs^{-1} \bmod p$$

By Lemma 1, the possibilities for these integers do not vary as we consider different aproximations, but remain fixed for the parameters a, p, Δ. Now, we change equation (11):

$$\begin{aligned}&(rw_0^2 - sw_1 - rw_1^2 + sw_2) + 2rw_0\varepsilon_0 - (s + 2rw_1)\varepsilon_1 + s\varepsilon_2 + r(\varepsilon_0^2 - \varepsilon_1^2) \equiv 0 \bmod p.\\ &(rw_0^2 - sw_1 - rw_1^2 + sw_2) + 2w_0r\underbrace{\varepsilon_0} - 2w_1r\underbrace{\varepsilon_1} + \underbrace{s(\varepsilon_2 - \varepsilon_1) + r(\varepsilon_0^2 - \varepsilon_1^2)} \equiv 0 \bmod p.\end{aligned} \tag{14}$$

Finally,

$$\begin{aligned}(rw_0^2 - sw_1 - rw_1^2 + sw_2)\underbrace{\Delta^3} + \ 2w_0r\Delta\underbrace{\Delta^2\varepsilon_0} - 2w_1r\Delta\underbrace{\Delta^2\varepsilon_1} \ +\\ +\Delta^3\underbrace{s(\varepsilon_2 - \varepsilon_1) + r(\varepsilon_0^2 - \varepsilon_1^2)} \equiv 0 \bmod p.\end{aligned}$$

So, the vector $\boldsymbol{e}' := (\Delta^3, \Delta^2\varepsilon_0, \Delta^2\varepsilon_1, s(\varepsilon_2 - \varepsilon_1) + r(\varepsilon_0^2 - \varepsilon_1^2))$ lies in the lattice:

$$\mathcal{L}' : \begin{cases} (rw_0^2 - sw_1 - rw_1^2 + sw_2)x_0 + 2rw_0\Delta x_1 - 2rw_1\Delta x_2 + \Delta^3 x_3 \equiv 0 \bmod p \\ x_0 \equiv 0 \bmod \Delta^2 \\ x_1, x_2 \equiv 0 \bmod \Delta^2 \end{cases}$$

Again, we now show that all short vectors in $\mathcal{L}'$ are parallel to $\boldsymbol{e'}$ unless v_0 belongs to the set $\mathcal{V}'(\Delta; a, b)$ which we define below.

Assume, for a contradiction, that there is another vector. We compute on polynomial time a vector $\boldsymbol{f'}$ with minimum norm in $\mathcal{L}'$.

$$\boldsymbol{f'} = (\Delta^3 f'_0, \Delta^2 f'_1, \Delta^2 f'_2, f'_3),\ \|\boldsymbol{f'}\| < 13\Delta^3$$

$$|f'_0| < 13,\ |f'_1|, |f'_2| < 13\Delta,\ |f'_3| < 13\Delta^3 \tag{15}$$

The vector $\boldsymbol{d'} := f'_0\boldsymbol{e'} - \boldsymbol{f'} =: (0, \Delta^2 d'_1, \Delta^2 d'_2, d'_3)$ is also in the lattice $\mathcal{L}'$. We can bound its coefficients by (15):

$$|d'_1|, |d'_2| < 26\Delta,\ |d'_3| < 169\Delta^3. \tag{16}$$

Now, by (14), we find that

$$2w_0 r d'_1 - 2w_1 r d'_2 + d'_3 \equiv 0 \bmod p \tag{17}$$

Substituting $w_0 = v_i - \varepsilon_i$ in the congruence (17) we derive

$$2(v_0 - \varepsilon_0) r d'_1 - 2(a v_0^2 + c - \varepsilon_1) r d'_2 + d'_3 \equiv 0 \bmod p. \tag{18}$$

Then, $P'(v_0) \equiv 0 \bmod p$ with

$$P'(T) := -2ard'_2 T^2 + 2rd'_1 T - 2rd'_1\varepsilon_0 - 2rd'_2 c + 2rd'_2\varepsilon_1 + d'_3.$$

We define $\mathcal{V}'(\Delta; a, c)$ the set of elements $v_0 \in \mathbb{F}_p$ such that there exist integers $d'_1, d'_2, d'_3, \varepsilon_0, \varepsilon_1, r, s$ with the appropriate bounds verifying:

$$d'_1 d'_2 \not\equiv 0 \bmod p \quad \text{and} \quad P'(v_0) \equiv 0 \bmod p.$$

By the bounds in the integers $d'_1, d'_2, d'_3, \varepsilon_0, \varepsilon_1, r, s$, we have that $\#\mathcal{V}'(\Delta; a, c) = O(\Delta^5)$, because in the equation:

$$-2ard'_2 v_0^2 + 2rd'_1 v_0 + 2rd'_2 c \equiv 2rd'_1\varepsilon_0 - 2rd'_2\varepsilon_1 - d'_3 \bmod p,$$

there are $O(\Delta^3)$ options for the right side, and $O(\Delta^2)$ different (and nonconstant) polynomials in v_0 for the left one.

Now, if $v_0 \notin \mathcal{V}'(\Delta; a, c)$, it must be $d'_1 \equiv d'_2 \equiv 0 \bmod p$, then using bounds (16) we obtain $d'_1 = d'_2 = d'_3 = 0$. This implies that vectors $\boldsymbol{e'}$ and $\boldsymbol{f'}$ are parallel which it is a contradiction. So, $\boldsymbol{e'}$ and $\boldsymbol{f'}$ are parallel vectors.

Once again, if we have $f'_0 \not\equiv 0 \bmod p$, we recover easily the approximation errors and the orginal values. Now, if $f'_0 \equiv 0 \Rightarrow f'_0 = 0$, we would have $\boldsymbol{f'} = (0, 0, 0, 0')$ which it is a contradiction.

We just must define $\mathcal{U}(\Delta; a, c) := \mathcal{V}(\Delta; a, c) \cup \mathcal{V}'(\Delta; a, c)$ to comple the proof.

4 Remarks and Open Questions

Obviously our Theorem 1 is nontrivial only for $\Delta = O(p^{1/4})$ and Theorem 2 only for $\Delta = O(p^{1/5})$. Thus increasing the size of the admissible values of Δ (even at the cost of considering more consecutive approximations) is interesting.

One can presumably obtain a very similar result in the dual case, where c is given but the multiplier a is unknown.

As we have mentioned several other results about predictability of nonlinear generators have recently been obtained in [3]. However, they are somewhat weaker than the present result because each of them excludes a certain small exceptional set of pairs of parameters (a, c). In particular the Theorem 5 of [3] when both multiplier and shift are secret. We believe that the approach of this work may help to eliminate this drawback. Certainly this question deserves further study.

We do not know how to predict the quadratic (and other generators considered in [3]) in the case when the modulus p is secret as well. We remark that in the case of the linear congruential generator a heuristic approach to this problem has been proposed in [6]. However it is not clear how to extend this (even just heuristically) to the case of nonlinear generators.

References

1. M. Ajtai, R. Kumar and D. Sivakumar, 'A sieve algorithm for the shortest lattice vector problem', *Proc. 33rd ACM Symp. on Theory of Comput. (STOC 2001)*, Association for Computing Machinery, 2001, 601–610.
2. S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, 'Predicting the inversive generator', *Proc. 9th IMA Intern. Conf on Cryptography and Coding*, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, **2898** (2003), 264–275.
3. S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, 'Predicting nonlinear pseudorandom number generators', *Math. Computation*, **74** (2005), 1471-1494.
4. E. F. Brickell and A. M. Odlyzko, 'Cryptanalysis: A survey of recent results', *Contemp. Cryptology*, IEEE Press, NY, 1992, 501–540.
5. M. Grötschel, L. Lovász and A. Schrijver, *Geometric algorithms and combinatorial optimization*, Springer-Verlag, Berlin, 1993.
6. A. Joux and J. Stern, 'Lattice reduction: A toolbox for the cryptanalyst', *J. Cryptology*, **11** (1998), 161–185.
7. R. Kannan, 'Algorithmic geometry of numbers', *Annual Review of Comp. Sci.*, **2** (1987), 231–267.
8. R. Kannan, 'Minkowski's convex body theorem and integer programming', *Math. Oper. Res.*, **12** (1987), 415–440.
9. J. C. Lagarias, 'Pseudorandom number generators in cryptography and number theory', *Proc. Symp. in Appl. Math.*, Amer. Math. Soc., Providence, RI, **42** (1990), 115–143.
10. A. K. Lenstra, H. W. Lenstra and L. Lovász, 'Factoring polynomials with rational coefficients', *Mathematische Annalen*, **261** (1982), 515–534.
11. D. Micciancio and S. Goldwasser, *Complexity of lattice problems*, Kluwer Acad. Publ., 2002.

12. P. Q. Nguyen and J. Stern, 'Lattice reduction in cryptology: An update', in: W. Bosma (Ed), *Proc. ANTS-IV, Lect. Notes in Comp. Sci. Vol. 1838*, Springer-Verlag, Berlin, 2000, 85–112.
13. P. Q. Nguyen and J. Stern, 'The two faces of lattices in cryptology', in: J.H. Silverman (Ed), *Cryptography and Lattices Lect. Notes in Comp. Sci. Vol. 2146* , Springer-Verlag, Berlin, 2001, 146–180.
14. H. Niederreiter, 'New developments in uniform pseudorandom number and vector generation', in: H. Niederreiter and P.J. Shiue (Eds), *Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing, Lect. Notes in Statistics Vol. 106*, Springer-Verlag, Berlin, 1995, 87–120.
15. H. Niederreiter, 'Design and analysis of nonlinear pseudorandom number generators', in G.I. Schueller and P. D. Spanos (Eds) *Monte Carlo Simulation*, A.A. Balkema Publishers, Rotterdam, 2001, 3–9.
16. H. Niederreiter and I. E. Shparlinski, 'Recent advances in the theory of nonlinear pseudorandom number generators', in: K.-T. Fang, F.J. Hickernell and H. Niederreiter (Eds), *Proc. Conf. on Monte Carlo and Quasi-Monte Carlo Methods, 2000*, Springer-Verlag, Berlin, 2002, 86–102.
17. H. Niederreiter and I. E. Shparlinski, 'Dynamical systems generated by rational functions', in: Marc Fossorier, Tom Høholdt and Alain Poli (Eds), *Applied Algebra, Algebraic Algorithms and Error Correcting Codes – AAECC-15, Lect. Notes in Comp. Sci. Vol. 2643*, Springer-Verlag, Berlin, 2003, 6–17.