PREDICTING MASKED LINEAR PSEUDORANDOM NUMBER GENERATORS OVER FINITE FIELDS

JAIME GUTIERREZ, ÁLVAR IBEAS, DOMINGO GÓMEZ-PEREZ,
AND IGOR E. SHPARLINSKI

Abstract. We study the security of the linear generator over a finite field. It is shown that the seed of a linear generator can be deduced from partial information of a short sequence of consecutive outputs of such generators.

1. Introduction

Let p be a prime number and $\mathbb{F}_p$ be the finite field of p elements. We identify the elements of $\mathbb{F}_p$ with the integer numbers in the range $\{0, \dots, p-1\}$. Given a polynomial $f(X) \in \mathbb{F}_p[X]$, we define the polynomial congruential generator (u_n) of elements of $\mathbb{F}_p$ by the recurrence relation,

$$u_{n+1} = f(u_n), \quad n = 0, 1, \dots,$$

where $u_0 \in \mathbb{F}_p$ is the initial value or seed.

One of the most popular polynomial congruential generators is the so-called *linear congruential generators*, given by the polynomial $f(X) = aX + b$. Indeed, it is still useful in many applications and is a part of many standard computer software libraries. However, they cannot be used in situations where unpredictability is required (for example, in many cryptographic scenarios) because of their coarse lattice structure. To overcome this deficiency, hiding some bits of the output has been proposed, but unfortunately this setup is not secure either and the same lattice structure has been the reason of many powerful attacks, see [4, 5, 6, 10, 11, 12].

If we consider polynomials $f(X)$ of higher degree over residue rings, then the generators become hard to predict when many bits are discarded and the residue ring has sufficiently many elements as it is shown in [3, 9, 14]. On the other hand, if too many bits are revealed at each stage then these type of generators are unfortunately polynomial time predictable if sufficiently many bits of their consecutive elements are given, see [1, 2, 7, 8] and references therein. As a result, in order to achieve the desired level security with this type of generators one has unfortunately sacrifice the efficiency.

Another different approach is to work in extensions of finite fields of small characteristic which offer a different way of "hidding" some information about the elements of the sequence (u_n) by discrding some of their coordinates in fixed basis over the ground field. Moreover, such finite fields are easy to implement and operations are very efficient compared to other fields or residue rings.

Unfortunately, the main result of this paper shows that linear congruential generators over such extensions, even after hiding some of the information about each output can be predicted in polynomial time and thus remain insecure.

We structure the paper as follows. In Section 2, we start with a short outline of the background needed to understand the rest paper. The algorithm that we want to present is divided in two stages, which are given in Section 3 and Section 4. Finally, in Section 5 we present some conclusions and open questions.

2. Preparations

Let $q = p^s$, where s is a positive integer and p is a prime number and let $\mathbb{F}_q$ be the finite field of q elements. We recall that $\mathbb{F}_q$ can be considered as a linear space over $\mathbb{F}_p$, see [13] for a background on finite fields.

We define the *linear generator over a finite field* as the sequence (u_n) defined by the following recurrence,

$$u_{n+1} = au_n + b, \quad a, b \in \mathbb{F}_q,\ a \neq 0,\ n = 0,\ 1, \ldots \tag{1}$$

However, we assume this sequence is not directly used, only part of each element of (u_n) is known to the attacker whose goal is, after observing several outputs, to continue to generate the same sequence.

More precisely, given a basic $(\gamma_1, \ldots, \gamma_s)$ of $\mathbb{F}_q$ over $\mathbb{F}_p$, we recall that every element $\alpha \in \mathbb{F}_q$ can be expressed as a unique linear combination

$$\alpha = c_1\gamma_1 + \cdots + c_s\gamma_s, \qquad c_1, \ldots, c_s \in \mathbb{F}_p,$$

where $(c_1, \ldots, c_s)$ are called the *coefficients of* α *in the basis* $(\gamma_1, \ldots, \gamma_s)$.

We suppose that the basis $(\gamma_1, \ldots, \gamma_s)$ is fixed and known.

Definition 1. *Given a set $\mathcal{I} \subseteq \{1, \ldots, s\}$ and two elements $\alpha,\ \beta \in \mathbb{F}_q$ we say that β is an $\mathcal{I}$-approximation of α if the coefficients of α and β differ only at the positions $i \in \mathcal{I}$.*

Given a set $\mathcal{I} \subseteq \{1, \ldots, s\}$, we also denote,

$$\mathcal{L}(\mathcal{I}) = \left\{ \sum_{i \in \mathcal{I}} c_i \gamma_i \mid c_i \in \mathbb{F}_p, \ \forall i \in \mathcal{I} \right\}. \tag{2}$$

Thus if β is an $\mathcal{I}$-approximation of α if and only if $\beta - \alpha \in \mathcal{L}(\mathcal{I})$.

We show how to recover the elements of the sequence (u_n) given by (1) from several $\mathcal{I}$-approximations.

We assume that the coefficients a and b of the equation (1) are known. However, we do not assume that the set $\mathcal{I}$ is known, so our algorithm works in two stages:

- recovering the set $\mathcal{I}$;
- recovering the initial value u_0.

Throughout the paper a polynomial time algorithm means with complexity $(\log q)^{O(1)}$.

3. Recovering the set $\mathcal{I}$

First we show that for almost all $s+1$ consecutive $\mathcal{I}$-approximations $w_0, w_1, \ldots, w_s$ to $u_0, u_1, \ldots, u_s$ one can find the set $\mathcal{I}$.

Theorem 2. *There exists a polynomial time algorithm that, given $s+1$ consecutive $\mathcal{I}$-approximations w_i to u_i, $i = 0, \ldots, s$ for some set $\mathcal{I} \subseteq \{1, \ldots, s\}$ of cardinality $k = \sharp\mathcal{I}$ and an integer $j \in \{1, \ldots, s\}$, decides correctly whether $j \in \mathcal{I}$, provided that*

$$(\varepsilon_0, \ldots, \varepsilon_s) \notin \mathcal{E}(a, b, \mathcal{I}), \qquad \text{where } \varepsilon_i = u_i - w_i, \ i = 0, \ldots, s,$$

and $\mathcal{E}(a, b, \mathcal{I}) \subset \mathbb{F}_q^{s+1}$ is a certain set of cardinality

$$\sharp\mathcal{E}(a, b, \mathcal{I}) = p^{k(s+1)-1}$$

that depends only on a, b and $\mathcal{I}$.

Proof. We start with the case $b = 0$, then we consider the general case.

Since, $a \in \mathbb{F}_q$ so we know that

$$a_0 + a_1 a + \cdots + a_s a^s = 0$$

where $a_0, \ldots, a_s \in \mathbb{F}_p$ are not all zeros. It is clear that if $b = 0$ then $u_n = a^n u_0$, which implies

$$a_0 u_0 + a_1 u_1 + \cdots + a_s u_s = 0.$$

Recalling the definition of $\varepsilon_0, \ldots, \varepsilon_s$, we obtain

$$a_0 \varepsilon_0 + \ldots + a_s \varepsilon_s = w$$

where

$$w = -a_0 w_0 - \ldots - a_s w_s.$$

Clearly $w \in \mathcal{L}(\mathcal{I})$. We now expand w in the basis $(\gamma_1, \dots, \gamma_s)$.

$$w = \sum_{i=1}^{s} \gamma_i d_i$$

If $d_j \neq 0$, then the algorithm outputs $j \in \mathcal{I}$ and in this case it is always correct.

If $d_j = 0$, then the algorithm outputs $j \notin \mathcal{I}$, which is correct unless $(\varepsilon_0, \varepsilon_1, \dots \varepsilon_s) \in \mathcal{E}(a, b, \mathcal{I})$ where

$$\mathcal{E}(a, b, \mathcal{I}) = \left\{ (x_0, \dots, x_s) \in \mathcal{L}(\mathcal{I})^{s+1} \mid \sum_{i=0}^{s} a_i x_i = \sum_{i \in \mathcal{I} \setminus \{j\}} \gamma_i d_i \right\}.$$

Clearly, $\sharp\mathcal{E}(a, b, \mathcal{I}) = p^{k(s+1)-1}$ which completes the proof in the case $b = 0$.

For $b \neq 0$, we consider the sequence $v_n = u_n - b(a^n - 1)(a-1)^{-1}$. This sequence satisfies $v_n = a^n u_0$ so our previous argument applies to v_n, which concludes the proof. □

Clearly if the "noise" sequence ε_i, $i = 0, 1, \dots$ is uniformly distributed in $\mathcal{L}(\mathcal{I})$ then the algorithm of Theorem 2 is correct with probability $1 - 1/p \geq 1/2$. So applying it with $\mathcal{I}$ approximations to m tuples $(u_h, \dots, u_{h+s})$, $h = 0, \dots, m-1$, and making a majority decision on whether $j \in \mathcal{I}$ we obtain an probabilistic algorithm, polynomial in m and $\log q$, with exponentially small probability of wrong output.

4. Recovering the initial value u_0

We now assume that we are given t consecutive $\mathcal{I}$-approximations with a known set $\mathcal{I}$. We first study the case $t > 2$ and then the case $t = 2$.

Theorem 3. *There exists a polynomial time algorithm that given a set $\mathcal{I} \subseteq \{1, \dots, s\}$ of cardinality $k = \sharp\mathcal{I}$ and $t > 2$ consecutive $\mathcal{I}$-approximations w_i to u_i, $i = 0, \dots, t-1$, finds u_0 correctly, provided $a \notin \mathcal{F}(\mathcal{I})$, for a certain set $\mathcal{F}(\mathcal{I}) \subset \mathbb{F}_q$ of cardinality*

$$\sharp\mathcal{F}(\mathcal{I}) < 2p^{d_t} + \binom{k}{t-2} p^{2k-t+2},$$

where d_t is the largest divisor d of s with $d < t$, that depends only on $\mathcal{I}$

Proof. Without loss of generality, we can suppose that

$$\mathcal{I} = \{1, \dots, k\},$$

that is, the components of $u_i - w_i$, $i = 0, \dots, t-1$, are zeroes except maybe at the first k positions.

As before we define $\varepsilon_i = u_i - w_i$, $i = 0, \dots, t-1$. Using the Equation (1) we derive the following system of linear equations

$$a\varepsilon_i - \varepsilon_{i+1} = e_i, \qquad i = 0, \dots, t-2, \tag{3}$$

where

$$e_i = w_{i+1} - (b + aw_i), \qquad i = 0, \dots, t-2,$$

We also recall that $\varepsilon_0, \dots, \varepsilon_{t-1} \in \mathcal{L}(\mathcal{I})$. Thus (3) leads to a system of $s(t-1)$ linear equations for kt unknowns of the expansion of $\varepsilon_0, \dots, \varepsilon_{t-1}$ in the basis $(\gamma_1, \dots, \gamma_s)$.

This is system is certainly consistent and if it has a unique solution than in polynomial time we can find $\varepsilon_0, \dots, \varepsilon_{t-1}$ and then $u_0 = w_0 + \varepsilon_0$.

However this fails if the system (3) has more than one solution. Now, we show that this implies that $a \in \mathcal{F}_1 \cup \mathcal{F}_2$, where

$$\mathcal{F}_1 = \left\{a \in \mathbb{F}_q \mid a\alpha = \beta,\ 0 < w(\alpha) \le k - t + 2,\ w(\beta) \le k\right\},$$
$$\mathcal{F}_2 = \left\{a \in \mathbb{F}_q \mid F(a) = 0,\ F(X) \in \mathbb{F}_p[X]^*,\ \deg F \le t-1\right\}.$$

Assuming that the system of equations (3) besides $(\varepsilon_0, \dots, \varepsilon_{t-1})$ has another solution $(\widetilde{\varepsilon}_0, \dots, \widetilde{\varepsilon}_{t-1})$ then

$$d_i = \varepsilon_i - \widetilde{\varepsilon}_i \in \mathcal{L}(\mathcal{I}), \qquad i = 0, \dots, t-1,$$

is a nontrivial solution of the following linear system of equations:

$$ay_j - y_{j+1} = 0, \qquad j = 0, \dots, t-2. \tag{4}$$

We see from (4) that if $(d_0, \dots, d_{t-1})$ is a nonzero vector then all components are nonzero elements of $\mathcal{L}(\mathcal{I})$, that is

$$d_i \neq 0, \qquad i = 0, \dots, t-1. \tag{5}$$

We consider the linear subspace over $\mathbb{F}_p$ generated by $d_0, \dots, d_{t-1}$. We consider the following two cases:

- Suppose that $d_0, \dots, d_{t-1}$ are linearly independent over $\mathbb{F}_p$, then by Gaussian elimination, we know that there exists a nonzero element α, which is a linear combination of $d_0, \dots, d_{t-2}$ and $\beta \in \mathcal{L}(\mathcal{I})$ with $w(\alpha) \le k - (t-2)$, and $a\alpha = \beta$. This means that $a \in \mathcal{F}_1$.
- Suppose that $d_0, \dots, d_{t-1}$ are linearly dependent over $\mathbb{F}_p$. We now see that there exits $j \in \{1, \dots, t-1\}$ such that

  $$d_j = c_0 d_0 + c_1 d_1 + \cdots + c_{j-1} d_{j-1}$$

  with $c_0, c_1, \dots, c_{j-1} \in \mathbb{F}_p$. By (4) and (5) it is equivalent to the relations

  $$a^j = c_0 + c_1 a + \cdots + c_{j-1} a^{j-1}.$$

  Thus in that case $a \in \mathcal{F}_2$.

For the cardinality of $\mathcal{F}_1$ we immediately get

$$\sharp\mathcal{F}_1 \le \binom{k}{t-2} p^{2k-t+2}. \tag{6}$$

To estimate $\sharp\mathcal{F}_2$ we note any $a \in \mathcal{F}_2$ is a root of an irreducible polynomial of degree at most t over $\mathbb{F}_p$. Since we also have $a \in \mathbb{F}_{p^s}$, from the well-known properties of irreducible polynomials over finite fields (see [13], for example) we derive

$$\prod_{a\in\mathcal{F}_2} (X-a) \;\Big|\; \prod_{\substack{j\mid s\\ j<t}} \left(X^{p^j} - a\right).$$

Therefore

$$\sharp\mathcal{F}_2 \le \sum_{\substack{j\mid s\\ j<t}} p^j \le \sum_{j=1}^{d_t} p^j \le 2p^{d_t}. \tag{7}$$

Combining (6) and (7) we conclude the proof. □

Using the trivial estimate $d_t \le t-1$ we immediately see that the cardinality of the set $\mathcal{F}(\mathcal{I})$ of Theorem 3 satisfies

$$\sharp\mathcal{F}(\mathcal{I}) < 2p^{t-1} + \binom{k}{t-2} p^{2k-t+2}.$$

Thus, if the number of approximation can be optimised then with $t = k+1$ we derive:

Corollary 1. *There exists a polynomial time algorithm that given a set $\mathcal{I} \subseteq \{1,\ldots,s\}$ of cardinality $k = \sharp\mathcal{I}$ and $t = k+1$ consecutive $\mathcal{I}$-approximations w_i to u_i, $i = 0,\ldots,k$, finds u_0 correctly, provided $a \notin \mathcal{F}(\mathcal{I})$, for a certain set $\mathcal{F}(\mathcal{I}) \subset \mathbb{F}_q$ of cardinality*

$$\sharp\mathcal{F}(\mathcal{I}) < (k+2)p^{k+1}$$

that depends only on $\mathcal{I}$.

Finally, we notice that although the conditions of Theorem 3 requires $t \ge 3$ approximations, a nontrivial result is also possible in the case $t = 2$.

Theorem 4. *There exists a polynomial time algorithm that given a set $\mathcal{I} \subseteq \{1,\ldots,s\}$ of cardinality $k = \sharp\mathcal{I}$ and $t = 2$ consecutive $\mathcal{I}$-approximations w_i to u_i, $i = 0,\ldots,t-1$, finds u_0 correctly provided $a \notin \mathcal{F}(\mathcal{I})$, where $\mathcal{F}(\mathcal{I}) \subset \mathbb{F}_q$ is a certain set of cardinality $\sharp\mathcal{F}(\mathcal{I}) < p^{2k}$ that depends only on $\mathcal{I}$.*

Proof. The proof is a verbatim of that of Theorem 3, except that we note there is only one case: d_0, d_1 are always linearly independent. □

5. Comments and Open Problems

We note that the result of Corollary 1 is nontrivial for the values of k with, say, $k < s - c_0 \log s / \log p$ for any constant $c_0 > 1$. Extending this result to large values of k, say, up to $k \le s - c_0$ with some constant c_0 is an interesting open question.

In our argument it is necessary that the positions where the approximations differ from the correct values are always the same. Eliminating this condition, that is, recovering u_0 from some approximations w_i to u_i, $i = 0, \dots, t-1$, in Hamming metrics is another challenging problem.

References

[1] S. R. Blackburn, D. Gómez-Perez, J. Gutierrez and I. E. Shparlinski, 'Predicting the inversive generator', *Lect. Notes in Comp. Sci.*, vol. 2898, Springer-Verlag, Berlin, 2003, 264–275.

[2] S. R. Blackburn, D. Gómez-Perez, J. Gutierrez and I. E. Shparlinski, 'Predicting nonlinear pseudorandom number generators', *Math. Comp.*, **74** (2005), 1471–1494.

[3] L. Blum, M. Blum and M. Shub, 'A simple unpredictable pseudo-random number generator', *SIAM J. Comp.*, **15** (1986), 364–383.

[4] J. Boyar, 'Inferring sequences produced by pseudo-random number generators', *J. ACM*, **36** (1989), 129–141

[5] J. Boyar, 'Inferring sequences produces by a linear congruential generator missing low–order bits', *J. Cryptology* **1** (1989) 177–184.

[6] S. Contini and I. E. Shparlinski, 'On Stern's attack against secret truncated linear congruential generators', *Lect. Notes in Comp. Sci.*, vol. 3574, Springer-Verlag, Berlin, 2005, 52–60.

[7] D. Gómez-Perez, J. Gutierrez and Á. Ibeas, 'Attacking the Pollard generator', *IEEE Trans. Inform. Theory*, **52** (2006), 5518–5523.

[8] J. Gutierrez and Á. Ibeas 'Inferring sequences produced by a linear congruential generator on elliptic curves missing high-order bits', *Designs, Codes and Cryptography*, **41** (2007), 199–212.

[9] M. Herrmann and A. May, 'Attacking power generators using unravelled linearization: When do we output too much?', *Lecture Notes in Computer Science*, vol. 5912, Springer-Verlag, Berlin, 2009, 487–504.

[10] A. Joux and J. Stern, 'Lattice reduction: A toolbox for the cryptanalyst', *J. Cryptology*, **11** (1998), 161–185.

[11] D. E. Knuth, 'Deciphering a linear congruential encryption', *IEEE Trans. Inf. Theory* **31** (1985), 49–52.

[12] H. Krawczyk, 'How to predict congruential generators', *J. Algorithms*, **13** (1992), 527–545.

[13] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.

[14] R. Steinfeld, J. Pieprzyk and H. Wang, 'On the provable security of an efficient RSA-based pseudorandom generator', *Lecture Notes in Computer Science*, vol. 4284, Springer-Verlag, Berlin, 2006, 194–209..

Department of Applied Mathematics and Computer Science, University of Cantabria, E-39071 Santander, Spain
E-mail address: jaime.gutierrez@unican.es

Department of Applied Mathematics and Computer Science, University of Cantabria, E-39071 Santander, Spain
E-mail address: alvar.ibeas@unican.es

Department of Applied Mathematics and Computer Science, University of Cantabria, E-39071 Santander, Spain
E-mail address: domingo.gomez@unican.es

Department of Computing, Macquarie Univ., Sydney, NSW 2109, Australia
E-mail address: Igor.Shparlinski@mq.edu.au