manuscript No.
(will be inserted by the editor)

On the Linear Complexity of the Naor-Reingold Sequence with Elliptic curves

Marcos Cruz · Domingo Gomez · Daniel Sadornil

Received: date / Accepted: date

Abstract The Naor-Reingold sequences with elliptic curves are used in cryptography due to their large linear complexity. Here we provide a new bound on the linear complexity of these sequences. Our result improves the previous one obtained by I.E. Shparlinski and J.H. Silverman and holds in more cases.

Keywords Naor-Reingold pseudo-random function · linear complexity · elliptic curves

1 Introduction

In this paper we provide a bound for the linear complexity of the Naor-Reingold sequences in elliptic curves. The original sequence was presented in Naor and Reingold (2004) as a primitive for cryptographic protocols. In Shparlinski (2000b), the author introduced analog sequences based on elliptic curves.

For a prime p, we denote by $\mathbb{F}_p$ the field with p elements. The elements of $\mathbb{F}_p$ will be identified with the set of integers $\{0, \ldots, p-1\}$.

Let E be an *elliptic curve* over $\mathbb{F}_p$, that is a rational curve given by the following Weierstrass equation

$$Y^2 = X^3 + aX + b, \qquad A,\ B \in \mathbb{F}_p, \qquad 4A^3 + 27B^2 \neq 0.$$

It is well-known that points of the curve over $\mathbb{F}_p$, including the special point O at infinity, have a group structure with an appropriate composition rule where O is the neutral element.

Let G be a point of the curve E with prime order l. We introduce the auxiliary function $\varphi_{\mathbf{a}}(x) := a_0^{x_0} \cdots a_{n-1}^{x_{n-1}} \in \mathbb{F}_l^*$ where $x = \sum_{i=0}^{n-1} x_i 2^i$ is the binary representation of x.

Departamento de Matemáticas Estadística y Computación
Universidad de Cantabria
Av. Los Castros s/n
E-39005 Santander
E-mail: marcos.cruz@unican.es

Then, each vector $\mathbf{a} = (a_0, \ldots, a_{n-1}) \in (\mathbb{F}_l^*)^n$ defines a finite sequence in the subgroup $\langle G \rangle$ as follows,

$$f_{\mathbf{a}}(x) := \varphi_{\mathbf{a}}(x)G.$$

The *Naor-Reingold Elliptic sequence* is defined as,

$$u_k = X(f_{\mathbf{a}}(k)), \qquad k = 0,\ 1, \ldots 2^n - 1. \tag{1}$$

where $X(P)$ is the abscissa of $P \in E$.

Note that we have required that the order of G is prime, which is not necessary for the definition of the sequence, but the results in the prime case are the basis for the results in the composite case.

It has been shown that, if the decisional Diffie-Hellman assumption holds, then in general the index k is not enough to compute in polynomial time u_k, even if an attacker performs polynomially many queries to a random oracle (Naor and Reingold 2004, Theorem 4.1). Bound on the distribution of the Naor-Reingold sequence is given in Shparlinski (2000a) and the article Ibeas (2008) investigates its period.

We recall that the *linear complexity* of an N-element sequence:

$$f(x), \qquad x = 0, \ldots, N-1$$

is the order L of the shortest linear recurrence

$$f(x+L) = c_{L-1}f(x+L-1) + \cdots + c_1 f(x+1) + c_0 f(x), \qquad x = 0, \ldots, N-L-1.$$

The linear complexity of the Naor-Reingold Elliptic sequence has been studied in Silverman and Shparlinski (2001). We cite the main result, in order to keep the paper self-contained.

Theorem 1 *Suppose that $\gamma > 0$ and n are chosen to satisfy*

$$n \geq (2+\gamma)\log l.$$

For any $\delta > 0$ and sufficiently large l, the linear complexity $L_{\mathbf{a}}$ of the sequence $(X(f_{\mathbf{a}}(k)))_{k=0}^{2^n-1}$ satisfies:

$$L_{\mathbf{a}} \geq \min\left(l^{1/3-\delta}, \frac{l^{(\gamma-3\delta)}}{\log^2 l}\right)$$

for all but at most $O((l-1)^{n-\delta})$ vectors $\mathbf{a} \in (\mathbb{F}_l^*)^n$.

This result provides lower bounds for it, assuming that the dimension n of the parameter $\mathbf{a}$ is bigger than $2\log l$. We obtain a lower bound for the linear complexity that is nontrivial even when $n \sim 4\log l/3$.

2 Preliminaries

Throughout the paper the implied constants in the symbols 'O' and '$\gg$' are absolute, and log denotes the binary logarithm. Using the techniques in Friedlander et al (2000), it is straightforward to prove the following:

Lemma 1 *Let $\mathcal{K}$, $\mathcal{H} \subseteq \mathbb{F}_l^*$ be a set of cardinality $\#\mathcal{K} = K$ and $\#\mathcal{H} = h$, respectively. Using the following notation,*

$$L_r(\mathcal{K}, \mathcal{H}) = \#\{(k, y) \in \mathcal{K} \times \mathcal{H} \mid rk = y\},$$

there exists $r \in \mathbb{F}_l^*$ such that $L_r(\mathcal{K}, h) \geq Kh/l$.

For convenience, we denote

$$L_r(\mathcal{K}, h) = \#\{(k, y) \in \mathcal{K} \times \mathbb{F}_l^* \mid rk = y,\ 0 < y < h\},$$

when $\mathcal{H} = \{0 < y < h\}$. The following results appeared in a stronger version in Silverman and Shparlinski (2001).

Lemma 2 *For any integer $n > 2$ and $0 < \Delta < 1$ for all except at most $O(\Delta(l-1)^n)$ vectors $\mathbf{a} \in (\mathbb{F}_l^*)^n$, the Naor-Reingold elliptic sequence contains at least $\Delta 2^{n-2}$ distinct elements.*

Lemma 3 *Fix integers $1 \leq d_0 < d_1, \ldots, < d_L \leq h < p$ and fix elements $c_0, \ldots,\ c_L \in \mathbb{F}_p$ with $c_L \neq 0$. For any point $Q \in E$, consider the following $\mathbb{F}_p-$linear combination of abscissas of multiples of Q,*

$$\mathcal{L}(Q) = c_0 X(d_0 Q) + c_1 X(d_1 Q) + \ldots + c_L X(d_L Q).$$

Then, there are at most $2(L+1)h^2$ points $Q \in E$ such that $\mathcal{L}(Q) = 0$.

Many properties of the linear complexity have been studied by several authors. We will also use Lemma 2 from Shparlinski (2000a).

Lemma 4 *Consider a finite sequence $(f(x))_{x=0}^{N-1}$ in a field $\mathbb{K}$, with linear complexity L. Then, for any integers $M \geq 1,\ h \geq 1,$ and $0 \leq e_0, \ldots, e_L \leq h$ there are some elements $c_0, \ldots, c_L \in \mathbb{K}$ (not all zero) such that*

$$\sum_{i=0}^{L} c_i f(Mb + e_i) = 0$$

for any integer b with $0 \leq Mk + h \leq N - 1$.

3 Linear complexity bound

We are ready to prove the main result of the article. The combination of the technique developed in Shparlinski (2000a), Silverman and Shparlinski (2001) with Lemma 1 yields a nontrivial result even in the case $n \sim (4/3 + \gamma)\log l$. Furthermore, this bound improves the one provided in Silverman and Shparlinski (2001).

Theorem 2 *For $\gamma > 0$ and $0 < \delta < 1$ such that*

$$n > (4/3 + \gamma) \log l + 4. \tag{2}$$

The linear complexity $L_{\mathbf{a}}$ of the sequence $(X(f_{\mathbf{a}}(k)))_{k=0}^{2^n-1}$ satisfies:

$$L_{\mathbf{a}} \geq \min \left(l^{(\gamma/3-\delta)} 2^{-7}, l^{(1/3-\delta)} \right)$$

for all but at most $O((l-1)^{n-\delta})$ vectors $\mathbf{a} \in (\mathbb{F}_l^*)^n$.

Proof First of all, we define

$$s = \min \left(\lfloor n/2 \rfloor, \lfloor (1-\delta) \log l \rfloor \right), \qquad h = \lfloor 2^{(n-2s-1)/3} l^{1/3} \rfloor.$$

For any $\mathbf{a} = (a_0, \ldots, a_{n-1})$, we denote,

$$\mathbf{a}^- = (a_0, \ldots,\ a_{s-1}), \qquad \mathbf{a}^+ = (a_s, \ldots,\ a_{n-1}).$$

Let $\mathcal{A}$ be the set of vectors such that each of the Naor-Reingold elliptic sequences defined by vectors $\mathbf{a}^-$ and $\mathbf{a}^+$ generate at least $2^{s-2} l^{-\delta}$ and $2^{n-s-2} l^{-\delta}$ distinct elements, respectively. Using Lemma 2, we have that $\#\mathcal{A} = (l-1)^n + O(l^{n-\delta})$.

We show that the bound holds for any vector $\mathbf{a} \in \mathcal{A}$. Let us consider the set

$$\mathcal{K} = \{ a_0^{x_0} \ldots a_{s-1}^{x_{s-1}} \mid x_0, \ldots, x_{s-1} \in \{0,1\} \} = \varphi_a[0, 2^s - 1].$$

The cardinality of this set is at least $2^{s-2} l^{-\delta}$, for $\mathbf{a} \in \mathcal{A}$. By Lemma 1, there exists $r \in \mathbb{F}_l^*$ such that $L_r(\mathcal{K}, h) \geq 2^{(n+s-7)/3} / l^{2/3+\delta}$.

If $L_r(\mathcal{K}, h) > L_{\mathbf{a}}$, we choose $d_1, \ldots,\ d_{L_{\mathbf{a}}} \in \mathcal{K}$ and such that $0 \leq y_i := d_i r < h$. Let $0 \leq e_0 < \cdots < e_{L_{\mathbf{a}}} < 2^s$ be the integers such that $\varphi_{\mathbf{a}}(e_i) = d_i$. Using Lemma 4, we derive

$$\sum_{i=0}^{L_{\mathbf{a}}} c_i X(f_{\mathbf{a}}(2^s b + e_i)) = 0$$

for $0 \leq b < 2^{n-s} - 1$. Let $m := r^{-1} \in \mathbb{F}_l^*$. We have that

$$f_{\mathbf{a}}(2^s b + e_i) = m \varphi_a(2^s b) r \varphi_a(e_i) G = y_i \left(m \varphi_a(2^s b) G \right),$$

where $b = \sum_{j=0}^{n-s-1} b_j 2^j$. Now, as $\mathbf{a} \in \mathcal{A}$, this linear combination

$$\mathcal{L}(Q) = c_0 X(y_0 Q) + c_1 X(d_1 Q) + \ldots + c_L X(y_L Q)$$

is zero for the points $m \varphi_{a^+}(b) G$, which are at least $2^{n-s-2} l^{-\delta}$, because $\mathbf{a} \in\ \mathcal{A}$. This is a contradiction with Lemma 3, because it will imply

$$2^{2(n-2s-1)/3} l^{2/3} L_{\mathbf{a}} \geq 2^{n-s-3} l^{-\delta}$$

and that is impossible. Therefore, $L_{\mathbf{a}} \geq L_r(\mathcal{K}, h)$ and the result follows.

Acknowledgements This article was partially supported by the Spanish Ministry of Science, projects AYA2007-68058-C03-02, MTM2007-67088 and MTM2007-62799.

References

Friedlander J, Hansen J, Shparlinski I (2000) On character sums with exponential functions. Mathematika 47:75–85

Ibeas Á (2008) On the period of the Naor-Reingold sequence. Information Processing Letters 108(5):304–307

Naor M, Reingold O (2004) Number-theoretic constructions of efficient pseudo-random functions. J ACM 51(2):231–262 (electronic)

Shparlinski I (2000a) Linear complexity of the naor-reingold pseudo-random function. Information Processing Letters 76:95–99

Shparlinski IE (2000b) On the Naor-Reingold pseudo-random function from elliptic curves. Appl Algebra Engrg Comm Comput 11(1):27–34, DOI 10.1007/s002000000023, URL http://dx.doi.org/10.1007/s002000000023

Silverman J, Shparlinski I (2001) On the linear complexity of the naor reingold pseudo-random function from elliptic curves. Designs, Codes and Cryptography 24(3):279–289