Analysis of pseudo-random number generators based on elliptic curves

Tanja Lange
Technical University of Denmark
Denmark

Igor Shparlinski
Macquarie University
Australia
Overview

- Motivation
- Elliptic curves
- PRNGs from elliptic curves
  - Linear congruential generator
  - EC Power generator
  - Naor-Reingold generator
- Bounds for the power generator
- Koblitz curves
Motivation

- Pseudo-Random Number Generators are good to have
- Study helps to increase trust in EC-DLP
  - bad performance with respect to some measure could be turned into attack.
- Some PRNGs related to

  Discrete Logarithm Problem (DLP)

  Given \( P \) and \( Q = kP \) find \( k \).

- Nice application of character sums, combinatorics, and curves :-)}
**Elliptic Curve**

\[
E : y^2 + (a_1 x + a_3) y = x^3 + a_2 x^2 + a_4 x + a_6, \quad h, f \in \mathbb{F}_q[x]
\]

**Group:** \( E(\mathbb{F}_q) = \{ (x, y) \in \mathbb{F}_q^2 : y^2 + h(x)y = f(x) \} \cup \{ P_\infty \} \)
Elliptic Curve

\[ E : y^2 + (a_1 x + a_3) y = x^3 + a_2 x^2 + a_4 x + a_6, \quad h, f \in \mathbb{F}_q[x] \]

\[ h(x) \]

\[ f(x) \]

**Group:** \( E(\mathbb{F}_q) = \{ (x, y) \in \mathbb{F}_q^2 : y^2 + h(x)y = f(x) \} \cup \{ P_{\infty} \} \)

---

Tanja Lange

Pseudo-random number generators from elliptic curves – p. 4
Elliptic Curve

\[ E : y^2 + (a_1 x + a_3) y = x^3 + a_2 x^2 + a_4 x + a_6, \ h, f \in \mathbb{F}_q[x] \]

**Group:** \( E(\mathbb{F}_q) = \{ (x, y) \in \mathbb{F}_q^2 : y^2 + h(x)y = f(x) \} \cup \{ P_\infty \} \)

over \( \mathbb{R} \)
Elliptic Curve

\[ E : y^2 + (a_1 x + a_3) y = x^3 + a_2 x^2 + a_4 x + a_6, \quad h, f \in \mathbb{F}_q[x] \]

\[ \text{Group: } E(\mathbb{F}_q) = \{ (x, y) \in \mathbb{F}_q^2 : y^2 + h(x)y = f(x) \} \cup \{ P_\infty \} \]
Group Law \((q \text{ odd})\)

\[
E : y^2 = x^3 + a_4x + a_6, \; a_i \in \mathbb{F}_q
\]

\[
= (x_3, y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1),
\]

where

\[
\lambda = \begin{cases} 
(y_2 - y_1)/(x_2 - x_1) & \text{if } x_1 \neq x_2, \\
(3x_1^2 + a_4)/(2y_1) & \text{else}.
\end{cases}
\]

\(\Rightarrow\) consider sequence of points \(P_n \in E(\mathbb{F}_q)\).

Let \(P \in E(\mathbb{F}_q)\) be a point of order \(\ell\), often \(\ell\) is assumed to be a prime.
Group Law \((q \text{ odd})\)

\[
E : y^2 = x^3 + a_4x + a_6, \; a_i \in \mathbb{F}_q
\]

\[
= (x_3, y_3) = \\
= (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1),
\]

where

\[
\lambda = \begin{cases} 
(y_2 - y_1)/(x_2 - x_1) & \text{if } x_1 \neq x_2, \\
(3x_1^2 + a_4)/(2y_1) & \text{else}.
\end{cases}
\]

\[
(x_1, y_1) + (x_2, y_2) = \\
\Rightarrow \text{consider sequence of points } P_n \in E(\mathbb{F}_q).
\]

Let \(P \in E(\mathbb{F}_q)\) be a point of order \(\ell\), often \(\ell\) is assumed to be a prime.
Sequences from points

Map points $P_n = (x_n, y_n) \in \mathbb{F}_q^2$ into $[0, 1) \times [0, 1)$ and request that the discrepancy is small.

If $q = p$ prime then there is a natural map

$$P_n \rightarrow \left( \frac{x_n}{p}, \frac{y_n}{p} \right)$$

(think $\mathbb{F}_p = \{0, 1, \ldots, p - 1\}$).

Some applications use only $x$-coordinate or apply further maps to the coordinate values (e.g. hash functions or the trace map).
Elliptic curve PRNGs I

EC Linear Congruential Generator, EC-LCG: For the “initial value” \( Q_0 \in E(\mathbb{F}_q) \), consider the sequence:

\[
Q_k = P \oplus Q_{k-1} = kP \oplus Q_0, \quad k = 1, 2, \ldots .
\]

Easy to construct following element given two consecutive ones.

Let \( Q_k = (x_k, y_k) \). Use \((x_k)_{k=0}^\infty\), as sequence in \(\mathbb{F}_q\) or normalize to \([0, 1)\) by using an enumeration of the field and dividing by \(q\).

Over \(\mathbb{F}_{2^n}\) the sequence
\[(\text{Tr}(x_0), \text{Tr}(y_0), \text{Tr}(x_1), \text{Tr}(y_1), \text{Tr}(x_2), \text{Tr}(y_2), \text{Tr}(x_3), \ldots\)
was studied.

Period length linked to the number of points on \(E\).
EC Power Generator, **EC-PG**: For an integer $e \geq 2$, consider the sequence (with $Q_0 = P$),

$$Q_k = eQ_{k-1} = e^k P, \quad k = 1, 2, \ldots ,$$

Determining $e$ from $Q_k, Q_{k-1}$ would be solving the DLP. Constructing the following sequence element given longer substrings related to generalized Diffie-Hellman problem.
Elliptic curve PRNGs III

EC Naor-Reingold Generator, EC-NRG:
Given an integer vector \((a_1, \ldots, a_n)\), consider the sequence:

\[ Q_{a,k} = a_1^{k_1} \cdots a_n^{k_n} P, \quad k = 1, 2, \ldots, \]

where \( k = k_1 \ldots k_n \) is the bit representation of \( k \),
\( 0 \leq k \leq 2^n - 1 \).

Example:
n = 4, \( l = 19 \) and \( a = (2, 5, 3, 4) \)

\[
\begin{align*}
 f_{a,0} &= 2^05^03^04^0 P = P, \quad \ldots \\
 f_{a,1} &= 2^05^03^04^1 P = 4P, \quad f_{a,11} = 2^15^03^14^1 P = 24P = 5P \\
 f_{a,2} &= 2^05^03^14^0 P = 3P, \quad f_{a,15} = 2^15^13^14^1 P = 120P = 6P \\
 f_{a,3} &= 2^05^03^14^1 P = 12P
\end{align*}
\]
David Kohel, Igor Shparlinski, 2000:

Let $E/\mathbb{F}_p$ be an elliptic curve and $P \in H \subseteq E(\mathbb{F}_p)$ for some subgroup $H$. Then for any function $f$ nonconstant on $E$ we have

$$\sum_{P \in H} \exp \left( 2\pi i \frac{f(P)}{p} \right) = O(p^{1/2})$$
Results

Florian Hess, T. L., Igor Shparlinski, 2002–2003:

If the order $\ell$ of $P$ is at least $p^{1/2+\varepsilon}$ then all above sequences (EC-LCG, EC-PG, EC-NRG) are reasonably well distributed.

E. g. EC power generator for $E/\mathbb{F}_q$ nonsupersingular, $q = p^r$, $T = \text{ord}_\ell(e)$.

For any integer $\nu \geq 1$, the bound

$$\Delta_e(S_{\text{PG}}) \ll T^{1-(3\nu+2)/2\nu(\nu+2)}\ell(\nu+1)/\nu(\nu+2)q^{1/4(\nu+2)}(\ln p + 1)^r$$

holds for $\Delta$ the discrepancy of the sequence $S_{\text{PG}}$ obtained from the power generator.
Cryptanalysis of the Dual Elliptic Curve Generator, ePrint archive, 190/2006 (29th May).

- Analysis of a variant of the linear congruential generator.
  - $s_0$ random, $Q = aP$, $a$ secret
  - $s_i = x(s_{i-1}P)$
  - $r_i = \text{lsb}_{240}(x(s_i Q))$

- $r_i$ are not uniformly distributed – next bit is predictable without knowing $a$.

- Looks secure when less bits are extracted.
Koblitz curves over $\mathbb{F}_2$

Koblitz curves are subfield curves

$$E_a : Y^2 + XY = X^3 + aX^2 + 1, \quad a = 0, 1.$$  

Consider curve over extension field $\mathbb{F}_{2^n}$.

Frobenius automorphism $\varphi$ of field extension extends to points: $\varphi((x, y)) = (x^2, y^2)$

$$P \in E(\mathbb{F}_{2^n}) \Rightarrow \varphi(P) \in E(\mathbb{F}_{2^n})$$

If $\ell > (\#E_a(\mathbb{F}_{2^n}))^{1/2}$ then $\varphi^\ell(P) \in \langle P \rangle$. Assume this case in the sequel.
Scalar multiplication

Neal Koblitz, Jerome Solinas 1992–1999:
Every integer $m$ allows unique NAF (non-adjacent form) such that

$$mP = \sum \mu_i \varphi^i(P), \mu_i \in \{0, \pm 1\}, \mu_i \mu_{i-1} = 0.$$ 

Hence, obvious use in above method – just use expansion of $e$.
In cryptographic protocols often computation of $mP$ for random $m$ is required.
Faster:

choose random NAF $(\mu_0, \mu_1, \ldots, \mu_{k-1}), \mu_i \in \{0, \pm 1\}, \mu_i \mu_{i-1} = 0$ to save time to compute expansion.
General results on NAF

Bosma, 2001:

\[ M_k = \{(\mu_0, \ldots, \mu_{k-1}) \in \{0, \pm1\}^k \mid \mu_j \mu_{j+1} = 0\} \]

\[ \#M_k = \frac{4}{3} 2^k + O(1). \]
For $k \leq n$ we consider the points

$$P_m = \sum_{j=0}^{k-1} \mu_j \phi^j(P), \quad m = (\mu_0, \ldots, \mu_{k-1}) \in \mathcal{M}_k.$$ 

Let $N_k(Q) = \# \{ m \in \mathcal{M}_k \mid P_m = Q \}$. For good distribution expect $N_k(Q) \sim \#\mathcal{M}_k / \ell$.

T. L., Igor Shparlinski, 2003:

$$N_k(Q) = O\left(\#\mathcal{M}_k / \ell\right)$$
Proof I

Let $1 \leq r \leq k$ and $2^r \leq \ell/8$. Assume that $N_k(Q) \geq \#\mathcal{M}_{k-r} + 1$ solutions. Then there are two distinct vectors

$$m_\nu = (\mu_{\nu,0}, \ldots, \mu_{\nu,k-1}) \in \mathcal{M}_k, \quad \nu = 1, 2,$$

with $P_{m_1} = P_{m_2} = Q$ and such that $m_1$ and $m_2$ agree at the last $k - r$ components. Therefore,

$$\mathcal{O} = P_{m_1} - P_{m_2} = \sum_{i=0}^{r-1} d_i \sigma^i(P),$$

where $d_i = m_{1,i} - m_{2,i}$ and thus $|d_i| \leq 2, i = 0, \ldots, r - 1.$
Proof II

The characteristic polynomial of $E_a$ (and of $\sigma$) is

$$\chi_a(T) = T^2 + (-1)^a T + 2.$$ 

Assume that $\chi_a(T)$ is irreducible (the other case is similar . . . but not too interesting).

Hence $\chi_a(T)$ and

$$F(T) = \sum_{i=0}^{r-1} d_i T^i$$

have a common root in the algebraic closure of $\mathbb{F}_\ell$.

Therefore,

$$\text{Res}(\chi_a, F) \equiv 0 \pmod{\ell}.$$
Proof III

Let \( \tau_1 \) and \( \tau_2 \) be the roots of \( \chi_a \). Then

\[
\text{Res}(\chi_a, F) = F(\tau_1)F(\tau_2)
\]

and \( |\tau_1| = |\tau_2| = \sqrt{2} \).

Bounding \( |F(\tau_j)| \), we get

\[
|\text{Res}(\chi_a, F)| < 2^{r+3} \leq \ell.
\]

Hence, \( \text{Res}(\chi_a, F) = 0 \). – Easy to rule out by looking at the constant coefficient of \( \chi_a \).
Generalizations

Let $\sigma$ be some endomorphism of $E$. Put

$$P_{\sigma,m} = \sum_{j=0}^{k-1} \mu_j \sigma^j(P), \quad m = (\mu_0, \ldots, \mu_{k-1}) \in \mathcal{M}_k.$$ 

We consider the endomorphisms

- **Doubling** $\delta(P) = 2P$ on arbitrary curves $E$ and fields $\mathbb{F}_q$.
- **Frobenius endomorphism** $\varphi(P) = (x^2, y^2)$ on the Koblitz curves $E_{a}/\mathbb{F}_{2^n}$.
- **Complex multiplication** $\psi(x, y) = \left(\frac{x^2-b}{b^2(x-c)}, \frac{y(x^2-2cx+b)}{b^3(x-c)^2}\right)$, where $b = (1 + \sqrt{-7})/2$ and $c = (b - 3)/4$, on $E_{GLV}: y^2 = x^3 - \frac{3}{4}x^2 - 2x - 1$ over $\mathbb{F}_p$ with $p > 3$ and $-7$ quadratic residue modulo $p$. 

Tanja Lange

Pseudo-random number generators from elliptic curves – p. 20
Distribution properties II

The endomorphism $\psi$ on $E_{GLV}$ satisfies the same characteristic polynomial $T^2 - T + 2 = 0$ as the Frobenius endomorphism on $E_1$.

Thus L./Shparlinski 03 generalizes to:
Let $P \in E(\mathbb{F}_q)$ be of prime order $\ell$. Then for any positive integer $k$ and for every point $Q \in E(\mathbb{F}_q)$ the bound

$$N_{\sigma,k}(Q) \ll 2^k \ell^{-1} + 1$$

holds, where $\sigma$ is one of the following endomorphisms:
- $\delta$ for an arbitrary curve $E$,
- $\varphi$ for a Koblitz curve $E = E_a$, $a = 0, 1$,
- $\psi$ for the GLV curve $E = E_{GLV}$.
Example: $\mathbb{F}_q = \mathbb{F}_{p^n}$ with $n > 1$

Fix basis $\omega_1, \ldots, \omega_n$ of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ and a set $J \subseteq \{1, \ldots, n\}$.

For fixed $c = (c_j)_{j \in J}$ with $c_j \in \mathbb{F}_p$ let $T_{\sigma,k}(J, c)$ be the number of $m \in M_k$ for which

$$x(P_{\sigma,m}) = \sum_{i=1}^{n} a_i \omega_i$$

and $a_j = c_j$ for every $j \in J$.

I.e. $T_{\sigma,k}(J, c)$ counts how often a fixed pattern is obtained in the $x$-coordinate of the points $P_{\sigma,m}$.

Expect:

$$T_{\sigma,k}(J, c) \sim \frac{\#M_k}{p \#J}.$$
Example: $F_q = F_{p^n}$ with $n > 1$

The bound

$$\max_{\mathcal{J}, c} \left| T_{\sigma,k}(\mathcal{J}, c) - \frac{\#\mathcal{M}_k}{p \#\mathcal{J}} \right| \ll \#\mathcal{M}_k (p^{n/4\nu + 1/2\nu} + 2^{-k/2\nu} p^{n(\nu+1)/4\nu^2})$$

holds with fixed integer $\nu \geq \frac{n \log p}{2k}$, where $\sigma$ is one of the following endomorphisms:

- $\delta$ for an arbitrary curve $E$,
- $\varphi$ for a Koblitz curve $E = E_a$, $a = 0, 1$.

Special case $\ell = q^{1+o(1)}$ and $k = \lfloor \log q \rfloor$: for any fixed $\alpha < 1/16$ the components on any $s \leq \alpha n$ positions are uniformly distributed.
The End!