On the distribution of the elliptic curve power generator

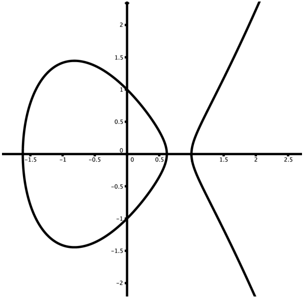
László Mérai

Eötvös Loránd University
Budapest

26. 06. 2012.

Elliptic curves

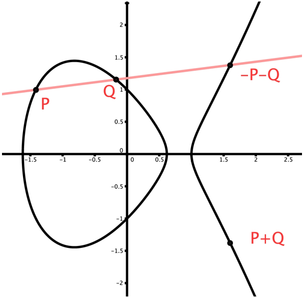
$$\mathcal{E}(\mathbb{F}_q) = \{(x, y) : y^2 = x^3 + a_1 x + a_2\} \cup \{\infty\}, \quad a_1, a_2 \in \mathbb{F}_q$$



$(\mathcal{E}(\mathbb{F}_p), +)$ is an Abelian group.

Elliptic curves

$$\mathcal{E}(\mathbb{F}_q) = \{(x,y) : y^2 = x^3 + a_1 x + a_2\} \cup \{\infty\}, \quad a_1, a_2 \in \mathbb{F}_q$$



$(\mathcal{E}(\mathbb{F}_p), +)$ is an Abelian group.

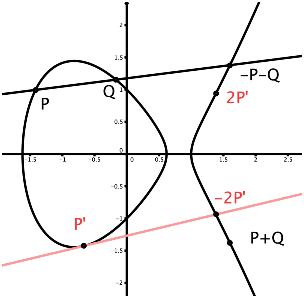
Adding: $(x_P, y_P) + (x_Q, y_Q)$:

$$x = \left(\frac{y_P - y_Q}{x_P - x_Q}\right)^2 - x_P - x_Q$$

$$y = y_P + \frac{y_P - y_Q}{x_P - x_Q}(x_P - x)$$

Elliptic curves

$$\mathcal{E}(\mathbb{F}_q) = \{(x, y) : y^2 = x^3 + a_1 x + a_2\} \cup \{\infty\}, \quad a_1, a_2 \in \mathbb{F}_q$$



$(\mathcal{E}(\mathbb{F}_p), +)$ is an Abelian group.

Adding: $(x_P, y_P) + (x_Q, y_Q)$:

$$x = \left(\frac{y_P - y_Q}{x_P - x_Q}\right)^2 - x_P - x_Q$$

$$y = y_P + \frac{y_P - y_Q}{x_P - x_Q}(x_P - x)$$

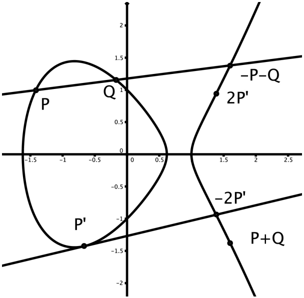
Doubling: $2(x_{P'}, y_{P'})$:

$$x = \left(\frac{3x_{P'}^2 + A}{2z_{P'}}\right)^2 - 2x_{P'}$$

$$y = y_P + \frac{3x_{P'}^2 + A}{2z_{P'}}(x_{P'} - x) - y_{P'}$$

Elliptic curves

$$\mathcal{E}(\mathbb{F}_q) = \{(x, y) : y^2 = x^3 + a_1 x + a_2\} \cup \{\infty\}, \quad a_1, a_2 \in \mathbb{F}_q$$

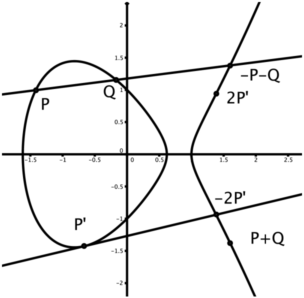


Applications:

- Public key cryptosystem
- Digital signature
- Generating pseudorandom sequences, . . .

Elliptic curves

$$\mathcal{E}(\mathbb{F}_q) = \{(x, y) : y^2 = x^3 + a_1 x + a_2\} \cup \{\infty\}, \quad a_1, a_2 \in \mathbb{F}_q$$



Applications:

- Public key cryptosystem
- Digital signature
- Generating pseudorandom sequences, ...

Discrete logarithm problem: given $P, nP \in \mathcal{E}(\mathbb{F}_p)$ find n!

Sequences generated by elliptic curve

Let $P_n \in \mathcal{E}(\mathbb{F}_q)$ be a sequence of points.

We study the distribution of points $P_n = (x_n, y_n)$, $(x_n, y_n \in \mathbb{F}_q)$

Sequences generated by elliptic curve

Let $P_n \in \mathcal{E}(\mathbb{F}_q)$ be a sequence of points.

We study the distribution of points $P_n = (x_n, y_n)$, $(x_n, y_n \in \mathbb{F}_q)$

Importance:

- We may get a good pseudorandom generator.
- Helps us to trust the hardness of discrete logarithm problem.

Sequences generated by elliptic curve

Let $P_n \in \mathcal{E}(\mathbb{F}_q)$ be a sequence of points.

We study the distribution of points $P_n = (x_n, y_n)$, $(x_n, y_n \in \mathbb{F}_q)$

Importance:

- We may get a good pseudorandom generator.
- Helps us to trust the hardness of discrete logarithm problem.
  A negative result would help us to attack this problem.

Pseudorandomness of sequences - Discrepancy

Let $(u_n) \subset [0,1)$ be a sequence.
For a positive integer s, the discrepancy $D_s(N)$ of the points

$$(u_n, \dots, u_{n+s-1}), \quad n = 1, \dots, N$$

is defined by

$$D_s(N) = \sup_{B \subseteq [0,1)^s} \left| \frac{N(B)}{N} - |B| \right|,$$

where $N(B)$ is the number of points which hit the box

$$B = [a_1, b_1) \times \cdots \times [a_s, b_s)$$

and the supremum is taken over all such boxes B.

Pseudorandomness of sequences - Discrepancy

Let $(u_n) \subset [0,1)$ be a sequence.
For a positive integer s, the discrepancy $D_s(N)$ of the points

$$(u_n, \dots, u_{n+s-1}), \quad n = 1, \dots, N$$

is defined by

$$D_s(N) = \sup_{B \subseteq [0,1)^s} \left| \frac{N(B)}{N} - |B| \right|,$$

where $N(B)$ is the number of points which hit the box

$$B = [a_1, b_1) \times \cdots \times [a_s, b_s)$$

and the supremum is taken over all such boxes B.

We can apply the discrepancy to the sequence $\frac{x_n}{p}$ where
$P_n = (x_n, y_n) \in \mathcal{E}(\mathbb{F}_p)$

Pseudorandomness of sequences - Measures of pseudorandomness

Let $E_N = (e_1, \ldots, e_N) \in \{+1, -1\}^N$ binary sequence.
The well-distribution measure $W(E_N)$ is

$$W(E_N) = \max_{a,b,t} \left| \sum_{j=1}^{t} e_{a+jb} \right|$$

Pseudorandomness of sequences - Measures of pseudorandomness

Let $E_N = (e_1, \ldots, e_N) \in \{+1, -1\}^N$ binary sequence.
The well-distribution measure $W(E_N)$ is

$$W(E_N) = \max_{a,b,t} \left| \sum_{j=1}^{t} e_{a+jb} \right|$$

The correlation measure $C_\ell(E_N)$ of order ℓ is

$$C_\ell(E_N) = \max_{M,d_1,\ldots,d_\ell} \left| \sum_{n=1}^{M} e_{n+d_1} \ldots e_{n+d_\ell} \right|$$

Pseudorandomness of sequences - Measures of pseudorandomness

Let $E_N = (e_1, \dots, e_N) \in \{+1, -1\}^N$ binary sequence.
The well-distribution measure $W(E_N)$ is

$$W(E_N) = \max_{a,b,t} \left| \sum_{j=1}^{t} e_{a+jb} \right|$$

The correlation measure $C_\ell(E_N)$ of order ℓ is

$$C_\ell(E_N) = \max_{M,d_1,\dots,d_\ell} \left| \sum_{n=1}^{M} e_{n+d_1} \dots e_{n+d_\ell} \right|$$

We can apply this measures by transforming P_n to a binary sequence:

- $P_n = (x_n, y_n) \mapsto \begin{cases} +1, & \text{if } x_n \in \{0, 1, \dots, \frac{p-1}{2}\} \\ -1, & \text{otherwise} \end{cases}$
- $P_n = (x_n, y_n) \mapsto \left(\frac{x_n}{p}\right)$, (Here $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.)

Sequences generated by elliptic curve

Elliptic curve linear congruential generator, EC-LCG:

Let $P, P_0 \in \mathcal{E}(\mathbb{F}_q)$ and the sequence U_n ($n \in \mathbb{N}$) generated by the rule

$$U_n = U_{n-1} + P = nP + P_0$$

Sequences generated by elliptic curve

Elliptic curve linear congruential generator, EC-LCG:

Let $P, P_0 \in \mathcal{E}(\mathbb{F}_q)$ and the sequence U_n ($n \in \mathbb{N}$) generated by the rule

$$U_n = U_{n-1} + P = nP + P_0$$

- Given consecutive elements U_n, U_{n+1} one can easily compute P.
- We can consider the sequence $f(U_n) \in \mathbb{F}_q$ with secret $f \in \mathbb{F}_q(\mathcal{E})$.
- Due to the simple structure, the generator is well-understood.

Sequences generated by elliptic curve

Elliptic curve linear congruential generator, EC-LCG:

Let $P, P_0 \in \mathcal{E}(\mathbb{F}_q)$ and the sequence U_n ($n \in \mathbb{N}$) generated by the rule

$$U_n = U_{n-1} + P = nP + P_0$$

- Given consecutive elements U_n, U_{n+1} one can easily compute P.
- We can consider the sequence $f(U_n) \in \mathbb{F}_q$ with secret $f \in \mathbb{F}_q(\mathcal{E})$.
- Due to the simple structure, the generator is well-understood.

Elliptic curve power generator, EC-PG:

Let $Q \in \mathcal{E}(\mathbb{F}_q)$ and fix an integer e. The sequence W_n ($n \in \mathbb{N}$) generated by the rule

$$W_n = eW_{n-1} = e^n Q$$

Sequences generated by elliptic curve

Elliptic curve linear congruential generator, EC-LCG:

Let $P, P_0 \in \mathcal{E}(\mathbb{F}_q)$ and the sequence U_n ($n \in \mathbb{N}$) generated by the rule

$$U_n = U_{n-1} + P = nP + P_0$$

- Given consecutive elements U_n, U_{n+1} one can easily compute P.
- We can consider the sequence $f(U_n) \in \mathbb{F}_q$ with secret $f \in \mathbb{F}_q(\mathcal{E})$.
- Due to the simple structure, the generator is well-understood.

Elliptic curve power generator, EC-PG:

Let $Q \in \mathcal{E}(\mathbb{F}_q)$ and fix an integer e. The sequence W_n ($n \in \mathbb{N}$) generated by the rule

$$W_n = eW_{n-1} = e^n Q$$

- To compute e from consecutive elements W_n, W_{n+1} one may need to solve the *discrete logarithm problem*.
- To compute an element W_n from the some previous ones one may need to solve the *Diffie-Helmann problem*.

Elliptic curve linear congruential generator, EC-LCG

Discrepancy bounds:

- Hess, Shparlinski: Let $u_n = \frac{x(nG)}{p} \in [0,1)$.
  Then the discrepancy of $(u_{n+1}, \ldots, u_{n+s})$ is
  $D_s(t) \ll t^{-1} p^{1/2+\varepsilon}$, (Here t is the order of G.)

Elliptic curve linear congruential generator, EC-LCG

Discrepancy bounds:

- Hess, Shparlinski: Let $u_n = \frac{x(nG)}{p} \in [0, 1)$.
  Then the discrepancy of $(u_{n+1}, \ldots, u_{n+s})$ is
  $D_s(t) \ll t^{-1} p^{1/2+\varepsilon}$, (Here t is the order of G.)

Bounds on the pseudorandom measures of binary case:

- Chen; Mérai: Let $e_n = \left(\frac{f(nG)}{p}\right) \in \{+1, -1\}$, then
  $W(E_N), C_\ell(E_N) \ll p^{1/2+\varepsilon}$.

Elliptic curve linear congruential generator, EC-LCG

Discrepancy bounds:

- Hess, Shparlinski: Let $u_n = \frac{x(nG)}{p} \in [0, 1)$.

  Then the discrepancy of $(u_{n+1}, \ldots, u_{n+s})$ is

  $D_s(t) \ll t^{-1} p^{1/2+\varepsilon}$, (Here t is the order of G.)

Bounds on the pseudorandom measures of binary case:

- Chen; Mérai: Let $e_n = \left(\frac{f(nG)}{p}\right) \in \{+1, -1\}$, then

  $W(E_N), C_\ell(E_N) \ll p^{1/2+\varepsilon}$.

- Liu, Wang, Zhand; Mérai:

  Let $e_n = \begin{cases} +1, & \text{if } f(nG) \in \{0, 1, \ldots, \frac{p-1}{2}\} \\ -1, & \text{otherwise} \end{cases}$, then

  $W(E_N), C_\ell(E_N) \ll p^{1/2+\varepsilon}$.

Elliptic curve power generator, EC-PG

Discrepancy bound:

- Banks, Friedlander, Garaev, Shparlinski: Let $u_n = \frac{x(e^n G)}{p} \in [0, 1)$. Then its discrepancy:

$$D_1(N) \ll N^{-2/3} T^{5/9} p^{1/18+\varepsilon}$$

Here T is the multiplicative order of e modulo $|G|$.

Elliptic curve power generator, EC-PG

Discrepancy bound:

- Banks, Friedlander, Garaev, Shparlinski: Let $u_n = \frac{x(e^n G)}{p} \in [0, 1)$.

  Then its discrepancy:

  $$D_1(N) \ll N^{-2/3} T^{5/9} p^{1/18+\varepsilon}$$

  Here T is the multiplicative order of e modulo $|G|$.

Remarks:
There are no non-trivial bound on discrepancy even of $\left(\frac{x(e^n G)}{p}, \frac{x(e^{n+1} G)}{p}\right)$!

Except for some trivial examples, e.g. $e = 2$.

Elliptic curve power generator, EC-PG

Discrepancy bound:

- Main result: Let $u_n = \frac{f(e^n G)}{p}$ for an $f \in \mathbb{F}_p(\mathcal{E})$.

  Then

$$D_1(N) \ll \deg f \; N^{-2/3} T^{5/9} p^{1/18+\varepsilon}$$

Elliptic curve power generator, EC-PG

Discrepancy bound:

- Main result: Let $u_n = \frac{f(e^n G)}{p}$ for an $f \in \mathbb{F}_p(\mathcal{E})$.

  Then

$$D_1(N) \ll \deg f \; N^{-2/3} T^{5/9} p^{1/18+\varepsilon}$$

Remarks:
Discrepancy bound on $\left(\frac{f(e^n G)}{p}, \frac{f(e^{n+1} G)}{p}, \ldots, \frac{f(e^{n+s-1} G)}{p}\right)$ can be also given just small e:

$$D_s(N) \ll \deg f \; e^{2(s-1)} N^{-2/3} T^{5/9} p^{1/18+\varepsilon}$$

Exponential sums over elliptic curves

The discrepancy bounds immediately follow from exponential sum estimates.

- Kohel, Shparlinski: Let $\mathcal{H} \le \mathcal{E}(\mathbb{F}_q)$ and ψ be an additive character of $\mathbb{F}_q$. If f is not constant, then
$$\sum_{Q \in \mathcal{H}} \psi(f(Q)) \le 2 \deg f \, q^{1/2}$$

Exponential sums over elliptic curves

The discrepancy bounds immediately follow from exponential sum estimates.

- Kohel, Shparlinski: Let $\mathcal{H} \le \mathcal{E}(\mathbb{F}_q)$ and ψ be an additive character of $\mathbb{F}_q$. If f is not constant, then
$$\sum_{Q \in \mathcal{H}} \psi(f(Q)) \le 2 \deg f \; q^{1/2}$$
- Lange, Shparlinski: Let $\mathcal{H} \le \mathcal{E}(\mathbb{F}_q)$ and ψ be an additive character of $\mathbb{F}_q$. If $1 \le d_1 < \cdots < d_s \le D$, then
$$\sum_{Q \in \mathcal{H}} \psi\left(\sum_{i=1}^{s} c_i x(d_i Q)\right) \ll s\, D^2 q^{1/2}$$

Exponential sums over elliptic curves

The discrepancy bounds immediately follow from exponential sum estimates.

- Kohel, Shparlinski: Let $\mathcal{H} \le \mathcal{E}(\mathbb{F}_q)$ and ψ be an additive character of $\mathbb{F}_q$. If f is not constant, then
$$\sum_{Q \in \mathcal{H}} \psi(f(Q)) \le 2 \deg f \, q^{1/2}$$
- Lange, Shparlinski: Let $\mathcal{H} \le \mathcal{E}(\mathbb{F}_q)$ and ψ be an additive character of $\mathbb{F}_q$. If $1 \le d_1 < \cdots < d_s \le D$, then
$$\sum_{Q \in \mathcal{H}} \psi\left(\sum_{i=1}^{s} c_i x(d_i Q)\right) \ll s\, D^2 q^{1/2}$$
- Banks, Friedlander, Garaev, Shparlinski: Let $Q \in \mathcal{E}(\mathbb{F}_p)$ and e be an integer of order T modulo $|G|$, then
$$\sum_{n=1}^{N} e_p(x(e^n Q)) \ll N^{1/3} T^{5/9} p^{1/18+\varepsilon}$$

Exponential sums over elliptic curves

- A new bound: Let $\mathcal{H} \leq \mathcal{E}(\mathbb{F}_q)$, ψ be an additive character of $\mathbb{F}_q$. If $f \in \mathbb{F}_q(\mathcal{E})$ is not constant and $1 \leq d_1 < \cdots < d_s \leq D$, then

$$\sum_{Q \in \mathcal{H}} \psi\left(\sum_{i=1}^{s} c_i f(d_i Q)\right) \ll s \deg f \; D^2 q^{1/2}$$

Exponential sums over elliptic curves

Let

$$F(Q) = \sum_{i=1}^{s} c_i f(d_i Q)$$

Exponential sums over elliptic curves

Let

$$F(Q) = \sum_{i=1}^{s} c_i f(d_i Q)$$

In order to prove the theorem it is enough to show:

- $F(Q)$ is not constant. It can be shown that there is at least one pole:

Exponential sums over elliptic curves

Let

$$F(Q) = \sum_{i=1}^{s} c_i f(d_i Q)$$

In order to prove the theorem it is enough to show:

- $F(Q)$ is not constant. It can be shown that there is at least one pole:
- $\deg F \leq s \deg f \; D^2$

Exponential sums over elliptic curves

Let

$$F(Q) = \sum_{i=1}^{s} c_i f(d_i Q)$$

In order to prove the theorem it is enough to show:

- $F(Q)$ is not constant. It can be shown that there is at least one pole:

  We can order the poles of $f(d_i Q)$ by their orders, and there is an (almost) unique maximum element.

- $\deg F \leq s \deg f \; D^2$

Thank you!