2-source Randomness Extractors for Elliptic Curves

Abdoul Aziz Ciss

Laboratoire de Traitement de l'Information et Systèmes Intelligents
École Polytechnique de Thiès, Sénégal
aaciss@ept.sn

Workshop FAST – Bordeaux

Randomness Extractors

Definition

A randomness extractor for a group G is a function which converts a random element of G into a uniformly random bit-string of fixed length.

Applications

- Key derivation
- Encryption, signatures
- Construction of cryptographically secure pseudorandom numbers generator
- Error correcting codes

Statistical distance

Let X and Y be S-valued random variables, where S is a finite set. The statistical distance $\Delta(X,Y)$ between X and Y is

$$\Delta(X,Y) = \frac{1}{2}\sum_{s\in S} |\Pr[X=s] - \Pr[Y=s]|$$

Let U_S be a random variable uniformly distributed on S. Then a random variable X on S is said to be ε-uniform if

$$\Delta(X,U_S) \leq \varepsilon$$

Extractor

Let S and T be two finite sets. A (T, ε)-extractor is a function

$$Ext : S \longrightarrow T$$

such that for every distribution X on S, the distribution $Ext(X)$ is ε-close to the uniform distribution on T. That is

$$\Delta(Ext(X), U_T) \leq \varepsilon,$$

where U_T is the uniform distribution on T

Two-source extractor

Let R, S and T be finite sets. The function $Ext : R \times S \longrightarrow T$ is a two-source extractor if the distribution $Ext(X_1, X_2)$ is ε-close to the uniform distribution U_T for every uniformly distributed random variables X_1 in R and X_2 in S. That is,

$$\Delta(Ext(X_1, X_2), U_T) \leq \varepsilon,$$

Collision probability

Let S be a finite set and X be an S-valued random variable. The collision probability of X, denoted by $Col(X)$, is the probability

$$Col(X) = \sum_{s \in S} \Pr[X = s]^2$$

If X and X' are identically distributed random variables on S, the collision probability of X is interpreted as $Col(X) = \Pr[X = X']$

Collision probability

Lemma

Let S be a finite set and let $(\alpha_x)_{x\in S}$ be a sequence of real numbers. Then,

$$\frac{(\sum_{x\in S}|\alpha_x|)^2}{|S|} \leq \sum_{x\in S}\alpha_x^2. \tag{1}$$

This inequality is a direct consequence of Cauchy-Schwarz inequality:

$$\sum_{x\in S}|\alpha_x| = \sum_{x\in S}|\alpha_x|.1 \leq \sqrt{\sum_{x\in S}\alpha_x^2}\sqrt{\sum_{x\in S}1^2} \leq \sqrt{|S|}\sqrt{\sum_{x\in S}\alpha_x^2}.$$

If X is an S-valued random variable and if we consider that $\alpha_x = \Pr[X = x]$, then

$$\frac{1}{|S|} \leq Col(X), \tag{2}$$

Relation btw Δ and Col

Lemma

Let X be a random variable over a finite S of size $|S|$ and $\delta = \Delta(X, U_S)$ be the statistical distance between X and U_S, the uniformly distributed random variable over S. Then,

$$Col(X) \geq \frac{1 + 4\delta^2}{|S|}$$

Relation btw Δ and Col

Proof. If $\delta = 0$, then the result is an easy consequence of Equation 2. Let suppose that $\delta \neq 0$ and define

$$q_x = |\Pr[X = x] - 1/|S||/2\delta.$$

Then $\sum_x q_x = 1$ and by Equation 1, we have

$$\frac{1}{|S|} \leq \sum_{x \in S} q_x^2 = \sum_{x \in S} \frac{(\Pr[X = x] - 1/|S|)^2}{4\delta^2} = \frac{1}{4\delta^2}\left(\sum_{x \in S} \Pr[X = x]^2 - 1/|S|\right)$$
$$\leq \frac{1}{4\delta^2}(Col(X) - 1/|S|).$$

The lemma can be deduced easily.

Character sums

Definition

Let G be a commutative group. A character χ of G is a homomorphism

$$\chi : G \longrightarrow \mathbb{C}^*.$$

$\hat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$ is a multiplicative group with neutral element χ_0, the character defined by $\chi_0(x) = 1, \forall\, x \in G$.

If G is a cyclic group of order r, then $\chi(x)^r = \chi(x^r) = \chi(1) = 1$.
If $x \in G$, then $\chi(x) \in \mu_r$, the subgroup of $\mathbb{C}^*$ of r^{th} of unity.

Character sums

If $\chi \in \hat{G}$, then the inverse of χ in $\hat{G}$ is the conjugate character $\bar{\chi}$ of χ defined by $\bar{\chi}(x) = \overline{\chi(x)}$

Proposition

Let $K = \mathbb{F}_q$, with $q = p^n$ and let F be an n-variables polynomial with coefficients in K. If φ is a non-trivial additive character of K, then the number of solution of the equation $F = 0$ is given by

$$N = q^{-1} \sum_{y,x} y\varphi(F(x_1, x_2, \ldots, x_n)),$$

where the summation is extended to all points $(y, x_1, \ldots, x_n)$ of K^{n+1}

Character sums over prime fields

Let e_p be the character on $\mathbb{F}_p$ such that, for all $x \in \mathbb{F}_p$

$$e_p(x) = e^{\frac{2i\pi x}{p}} \in \mathbb{C}^*.$$

Let $S(a, G) = \sum_{x \in G} e_p(ax)$, then

$$M = \max_a(|S(a, G)|) \leq \sqrt{p}.$$

If I is an interval of integers, it's well known that

$$\sum_{x \in \mathbb{F}_p^*} \left| \sum_{a \in I} e_p(ax) \right| \leq p \log_2(p).$$

Character sums over $\mathbb{F}_q$

We denote by ψ the additive character in $\mathbb{F}_q$ such that for all $z \in \mathbb{F}_q$, $\psi(z) = e_p(\mathrm{Tr}(x))$. Let G be a subgroup of $\mathbb{F}_q$ and let introduce the following Gauss sum

$$T(a, G) = \sum_{x \in G} \psi(ax).$$

Then,

$$\max_{a \in \mathbb{F}_q^*} |T(a, G)| \leq q^{1/2}.$$

If V is an additive subgroup of $\mathbb{F}_q$ and if ψ is an additive character of $\mathbb{F}_q$, then,

$$\sum_{y \in \mathbb{F}_q} \left| \sum_{z \in V} \psi(yz) \right| \leq q.$$

Character sums over elliptic curves

Let E be an elliptic curve defined over $\mathbb{F}_q$. For a point $P \neq \mathcal{O}$ on E we write $P = (\mathrm{x}(P), \mathrm{y}(P))$. Let ψ be a nonprincipal additive character of $\mathbb{F}_q$ and let $\mathcal{P}$ and $\mathcal{Q}$ be two subsets of $E(\mathbb{F}_q)$. For arbitrary complex functions $\rho(P)$ and $\vartheta(Q)$ supported on $\mathcal{P}$ and $\mathcal{Q}$ we consider the bilinear sums of additive type:

$$V_{\rho,\vartheta}(\psi, \mathcal{P}, \mathcal{Q}) = \sum_{P\in\mathcal{P}} \sum_{Q\in\mathcal{Q}} \rho(P)\vartheta(Q)\psi(\mathrm{x}(P \oplus Q)).$$

Let

$$\sum_{P\in\mathcal{P}} |\rho(P)|^2 \leq R \quad \text{and} \quad \sum_{Q\in\mathcal{Q}} |\vartheta(Q)|^2 \leq T.$$

Then, uniformly over all nontrivial additive character ψ of $\mathbb{F}_q$,

$$|V_{\rho,\vartheta}(\psi, \mathcal{P}, \mathcal{Q})| \ll \sqrt{qRT}.$$

2-source randomness extractors for $E(\mathbb{F}_p)$

Definition

Let E be an elliptic curve defined a finite field $\mathbb{F}_q$, with $q = p$ a prime greater than 5, and let $\mathcal{P}$ and $\mathcal{Q}$ be two subgroups of $E(\mathbb{F}_q)$ with $\#\mathcal{P} = r$ and $\#\mathcal{Q} = t$. Define the function

$$\begin{aligned} Ext_1 : \mathcal{P} \times \mathcal{Q} &\longrightarrow \{0,1\}^k \\ (P, Q) &\longmapsto \mathrm{lsb}_k(\mathrm{x}(P \oplus Q)) \end{aligned}$$

2-source randomness extractors for $E(\mathbb{F}_p)$

Theorem

Let E be an elliptic curve defined over $\mathbb{F}_p$ and let $\mathcal{P}$ and $\mathcal{Q}$ be two subgroups of $E(\mathbb{F}_p)$, with $\#\mathcal{P} = r$ and $\#\mathcal{Q} = t$. Let $U_{\mathcal{P}}$ and $U_{\mathcal{Q}}$ be two random variables uniformly distributed in $\mathcal{P}$ and $\mathcal{Q}$ respectively and let U_k be the uniform distribution in $\{0,1\}^k$. Then,

$$\Delta(Ext_1(U_{\mathcal{P}}, U_{\mathcal{Q}}), U_k) \ll \sqrt{\frac{2^{k-1} p \log(p)}{rt}}$$

2-source randomness extractors for $E(\mathbb{F}_p)$

Corollary

Let m and l be the bit size of r and t respectively and let e be a positive integer. If k is a positive integer such that

$$k \leq m + l - (n + 2e + \log_2(n) + 1),$$

then Ext_1 is a $(k, O(2^{-e}))$-deterministic extractor for $\mathcal{P} \times \mathcal{Q}$.

Application to the Unified Model KE

Symetric key size	**Bit size of** p	**Bit size of** $\#\mathcal{P}$ **:** $|m|_2$
$|k|_2 = 64$: DES-64	521	378
	384	309
	256	245
$|k|_2 = 128$: AES-128	521	410
	384	340
$|k|_2 = 256$: AES-256	521	474

Table: Parameters for $Ext_1(Z_e, Z_s)$ at the 80-bit security level

2-source randomness extractors for $E(\mathbb{F}_{p^n})$, with $p > 5$

Definition

Let E be an elliptic curve defined over the finite field $\mathbb{F}_{p^n}$, where p is a prime greater than 5 and $n > 1$. Consider two subgroups $\mathcal{P}$ and $\mathcal{Q}$ of $E(\mathbb{F}_q)$. Define the function

$$\begin{aligned} Ext_2 : \mathcal{P} \times \mathcal{Q} &\longrightarrow \mathbb{F}_p^k \\ (P, Q) &\longmapsto (x_1, x_2, \ldots, x_k) \end{aligned}$$

where $\mathrm{x}(P \oplus Q) = (x_1, x_2, \ldots, x_k, x_{k+1}, \ldots, x_n)$. In other words, the function Ext_2 output the k first $\mathbb{F}_p$-coefficients of the abscissa of the point $P \oplus Q$.

2-source randomness extractors for $E(\mathbb{F}_{p^n})$, with $p > 5$

Theorem

Let E be an elliptic curve defined over $\mathbb{F}_{p^n}$ and let $\mathcal{P}$ and $\mathcal{Q}$ be two subgroup of $E(\mathbb{F}_{p^n})$ with $\#\mathcal{P} = r$ and $\#\mathcal{Q} = t$. Denote by $U_{\mathcal{P}}$ and $U_{\mathcal{Q}}$ two random variables uniformly distributed on $\mathcal{P}$ and $\mathcal{Q}$ respectively. Then,

$$\Delta(Ext_2(U_{\mathcal{P}}, U_{\mathcal{Q}}), U_{\mathbb{F}_p^k}) \ll \sqrt{\frac{p^{n+k}}{4rt}}$$

Future work

1. Generalization of Ext_1 and Ext_2

$$Ext_1 : \mathcal{P}_1 \times \mathcal{P}_2 \times \ldots \times \mathcal{P}_s \longrightarrow \{0,1\}^k$$
$$(P_1, P_2, \ldots, P_s) \longmapsto \mathrm{lsb}_k(\mathrm{x}(P_1 \oplus P_2 \oplus \ldots \oplus P_s))$$

$$Ext_2 : \mathcal{P}_1 \times \mathcal{P}_2 \times \ldots \times \mathcal{P}_s \longrightarrow \mathbb{F}_p^k$$
$$(P_1, P_2, \ldots, P_s) \longmapsto \mathcal{D}_k(\mathrm{x}(P_1 \oplus P_2 \oplus \ldots \oplus P_s))$$

2. Construct good pseudorandom number generators with Ext_1 and Ext_2

Thank you for your attention