Two-sources randomness extractors in finite fields and in elliptic curves

Hortense Boudjou Tchapgnouo, Abdoul A. Ciss, Djiby Sow, D.T. Kolyang

TWO-SOURCES RANDOMNESS EXTRACTORS IN FINITE FIELDS AND IN ELLIPTIC CURVES

Boudjou T. Hortense[1] *Abdoul A. Ciss*[2] *Djiby Sow*[3] *Kolyang*[4]

[1]*High Institute of the Sahel, University of Maroua, Cameroon*
hortense_boudjou@yahoo.fr
[2] *Laboratory of Information Processing and Intelligent Systems, Polytechnic School of Thies, Senegal*
aaciss@ept.sn
[3] *Laboratory of Algebra, Analysis, Cryptography, Algebraic Geometry and Applications, University of Cheikh Anta Diop, Senegal*
sowdjibab@yahoo.fr
[4] *Department of Computer Science, Higher Normal School, University of Maroua*
dtaiwe@yahoo.fr

ABSTRACT

We propose two-sources randomness extractors over finite fields and on elliptic curves that can extract from two sources of information without consideration of other assumptions that the starting algorithmic assumptions with a competitive level of security. These functions have several applications. We propose here a description of a version of a Diffie-Hellman key exchange protocol and key extraction.

Keywords: *Cryptography, key exchange, random deterministic extractors, finite fields, elliptic curves.*

RESUME

Nous proposons des extracteurs d'aléas 2-sources sur les corps finis et sur les courbes elliptiques capables d'extraire à partir de plusieurs sources d'informations sans considération d'autres hypothèses que les hypothèses algorithmiques de départ avec un niveau de sécurité compétitif. Ces fonctions possèdent plusieurs applications. Nous proposons ici une version du protocole d'échange de clé Diffie-Hellman incluant la phase d'extraction.

Mots clés: *Cryptographie, échange de clé, extracteur d'aléa 2-sources, corps finis, courbes elliptiques.*

1. INTRODUCTION

The shared element after a Diffie-Hellman exchange is $g^{ab} \in G$, where G is a cyclic subgroup of a finite field. g^{ab} is indistinguishable from any other element of G under the decisionnal Diffie-Hellman (DDH) assumption [4]. This hypothesis argues that, given two distribution (g^a, g^b, g^{ab}) and (g^a, g^b, g^c) there is no efficient algorithm that can distinguish them. However, the encryption key should be indistinguishable from a random bit string having a uniform distribution. So we could not directly use g^{ab} as an encryption key. It is therefore of adequate arrangements to ensure the indistinguishability of the key such as hash functions, pseudo-random functions or random extractors.

Deterministic random extractor have been introduced in complexity theory by Trevisan and Vadhan [21]. Most of the work on deterministic extractors using exponential sums for their security proof work with simple exponential sums [5, 11–13, 15]. Here, we introduce deterministic random extractors that extract a perfectly random bit string of an element derived from the combination of two separate sources.

More precisely, We propose a deterministic random extractor under the DDH asumption, which maps two multiplicative subgroups of a finite field $\mathbb{F}_{p^n}$ to the set $\{0,1\}^k$, permitting to extract the k-least significant bits of a random element in the product of the two subgroups. We use the double exponential sums to bound the collision probability and give a security proof of our extractor. The same work is performed over two subgroups G_1 and G_2 of points of an elliptic curve defined over a finite field $\mathbb{F}_{p^n}$.

This work is organized as follows: In section 2, We introduce some definitions and results on both the measurement parameters of randomness and exponential sums. Section 3 gives summary of previous work. In section 4 we present and analyze the security of our randomness extractors. In section 5, we give an application of our results, that is a version of Diffie-Hellman key exchange protocol. Section 6 is our conclusion.

2. PRELIMINARIES

This section recalls some definitions and results on the measurement of randomness and the sums of characters. We rely on them to establish the safety of our results. [19].

2.1. Measures of randomness

Definition 2.1. *Collision probability.*

Let $\mathcal{X}$ be a finite set and X an $\mathcal{X}$-valued random variable. The collision probability of X, denoted by $Col(X)$, is the probability $Col(X) = Pr[X = X'] = \sum_{x\in\mathcal{X}} Pr[X = x]^2$.

Definition 2.2. *Statistical distance.*

Let $\mathcal{X}$ be a finite set. If X and Y are $\mathcal{X}$-valued random variables, then the statistical distance $SD(X, Y)$ between X and Y is defined as $SD(X, Y) = \frac{1}{2}\sum_{x\in\mathcal{X}} |Pr[X = x] - Pr[Y = x]|$.

Let $U_{\mathcal{X}}$ be a random variable uniformly distributed on $\mathcal{X}$ and $\delta \leq 1$ a positive real number. Then a random variable X on $\mathcal{X}$ is said to be $\delta - uniform$ if $SD(X, U_{\mathcal{X}}) \leq \delta$.

Lemma 2.1. *Relation between SD and Col(X).*

Let X be a random variable over a finite set $\mathcal{X}$ of size $|\mathcal{X}|$ and $\Delta = SD(X, U_{\mathcal{X}})$ be the statistical distance between X and $U_{\mathcal{X}}$, where $U_{\mathcal{X}}$ is a uniformly distributed random variable over $\mathcal{X}$. Then,

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

To establish this result, we use the following one:

Lemma 2.2. *Let $\mathcal{X}$ be a finite set and $(\alpha_x)_{x\in\mathcal{X}}$ a sequence of real numbers. Then*

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

Proof. This inequality is a direct consequence of the Cauchy-Schwarz inequality below:

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

Hence the result. □

If X is a random variable with values in $\mathcal{X}$, laying $\alpha_x = Pr[X = x]$, since the sum of the probabilities is equal to 1 and as $Col(X) = \sum_{x\in\mathcal{X}} Pr[X = x]^2$ we get:

$$\frac{1}{|\mathcal{X}|} \leq Col(X). \tag{3}$$

Now we can establish the proof of Lemma 2.1.

Proof. If $\Delta = 0$, then the result is immediate.

Assuming $\Delta \neq 0$. Let us define $q_x = |Pr[X = x] - \frac{1}{|\mathcal{X}|}|/2\Delta$, then $\sum_x q_x = 1$. According to Equation 1, we get:

$$\frac{1}{|\mathcal{X}|} \leq \sum_{x\in\mathcal{X}} q_x^2 = \frac{1}{4\Delta^2}\sum_{x\in\mathcal{X}} \left(Pr[X = x] - \frac{1}{|\mathcal{X}|}\right)^2 = \frac{1}{4\Delta^2}\left(\sum_{x\in\mathcal{X}} Pr[X = x]^2 - \frac{1}{|\mathcal{X}|}\right) \leq \frac{1}{4\Delta^2}\left(col(X) - \frac{1}{|\mathcal{X}|}\right)$$

Hence the expected result. □

Definition 2.3. *Deterministic $(\mathcal{Y}, \delta)$-extractor.*

Let $\mathcal{X}$ and $\mathcal{Y}$ be two finite sets. Let Ext be a function Ext : $\mathcal{X} \to \mathcal{Y}$. We say that Ext is a deterministic $(\mathcal{Y}, \delta)$-extractor for $\mathcal{X}$ if $Ext(U_{\mathcal{X}})$ is δ-uniform on $\mathcal{Y}$. That is $SD(Ext(U_{\mathcal{X}}), U_{\mathcal{Y}}) \leq \delta$.

Definition 2.4. *Two-sources extractor.*

Let $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ be finite sets. The function $F : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ is a two-sources extractor if the distribution $F(X, Y)$ is δ-close to the uniform distribution $U_Z \in \mathcal{Z}$ for every uniformly distributed random variables $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$.

2.2. Exponential sums

In this section, we introduce some definitions and results on exponential sums over finite fields and over elliptic curves (see [1, 18, 22]).

2.2.1. Exponential sums over finite fields

Definition 2.5. *Character.*
Let G be an abelian group. A character of G is a homomorphism from $G \to \mathbb{C}^*$. A character is trivial if it is identically 1. We denote the trivial character by $\mathcal{X}_0$ or ψ_0.

Definition 2.6. *Let $\mathbb{F}_q$ be a given finite field. An additive character $\psi : \mathbb{F}_q^+ \to \mathbb{C}$ is a character ψ with $\mathbb{F}_q$ considered as an additive group. A multiplicative character $\mathcal{X} : \mathbb{F}_q^* \to \mathbb{C}$ is a character with $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$ considered as a multiplicative group. We extend $\mathcal{X}$ to $\mathbb{F}_q$ by defining $\mathcal{X}(0) = 1$ if $\mathcal{X}$ is trivial, and $\mathcal{X}(0) = 0$ otherwise. Note that the extended $\mathcal{X}$ still preserves multiplication.*

The main interests of exponential sums is that they allows to construct some characteristic functions and in some cases we know good bounds for them. The use of these characteristic functions can permit to evaluate the size of these sets. We focus on certain character sums, those involving the character e_p define as it follows.

Theorem 2.1. *Multiplicative characters of $\mathbb{F}_p$.*
The multiplicative characters of $\mathbb{F}_p$, where p is a prime, are given by: $\forall x \in \mathbb{F}_p$, $e_p(x) = e^{\frac{2i\pi x}{p}} \in \mathbb{C}^*$.

Theorem 2.2. *Additive characters of $\mathbb{F}_q$.*
Suppose $q = p^r$ where p is prime. The additive characters of $\mathbb{F}_q$ are given by $\psi(x) = e_p(Tr(x))$ where $Tr(x) = x + x^p + ... + x^{p^{n-1}}$ is the trace of x.

Definition 2.7. *Single character sums.*
Let p be a prime number, G a multiplicative subgroup of $\mathbb{F}_p^*$. For all $a \in \mathbb{F}_{p^*}$, let introduce the following notation: $S(a, G) = \sum_{x \in G} e_p(ax)$.

Lemma 2.3. *Let p be a prime number, G a multiplicative subgroup of $\mathbb{F}_p^*$.*

1. *if $a = 0$, $\quad \sum_{x=0}^{p-1} e_p(ax) = p$*
2. *For all $a \in \mathbb{F}_p^*$, $\quad \sum_{x=0}^{p-1} e_p(ax) = 0$*
3. *For all $x_0 \in G$ and all $a \in \mathbb{F}_p^*$, $S(ax_0, G) = S(a, G)$*

Proof. See [24] pp 69 □

Theorem 2.3. *Polya-Vinogradov bound.*
Let p be a prime number, G a multiplicative subgroup of $\mathbb{F}_p^*$. For all $a \in \mathbb{F}_p^*$: $\left| \sum_{x \in G} e_p(ax) \right| \leq \sqrt{p}$

Proof. See [24] pp 70 □

Theorem 2.4. *Winterhof bound.*
Let V be an additive subgroup of $\mathbb{F}_{p^n}$ and let ψ be an additive caracter of $\mathbb{F}_{p^n}$. Then, $\sum_{a \in \mathbb{F}_{p^n}} \left| \sum_{x \in V} \psi(ax) \right| \leq p^n$

Proof. See [23] □

Definition 2.8. *Bilinear character sums.*
Let p be a prime number, G and H be two multiplicative subgroups of $\mathbb{F}_p^*$. For all $a \in \mathbb{F}_{p^*}$, let introduce the following notation: $S(a, (G, H)) = \sum_{x \in G} \sum_{y \in H} e_p(axy)$

Lemma 2.4. *Let p be prime and, G and H two subsets of $\mathbb{F}_p^*$. Then*
$\max_{(n,p)=1} |\sum_{x\in G}\sum_{y\in H}(e_p(nxy))| \leq (p|G||H|)^{\frac{1}{2}}$.

Proof. See [6] (bound (1.4)), [22] pp 142. □

Lemma 2.5. *For any subsets G, H of $\mathbb{F}_{p^n}^*$ and for any complex coefficients α_x, β_y with $|\alpha_x| \leq 1$, $|\beta_y| \leq 1$, the following bound holds, $|\sum_{x\in G}\sum_{y\in H}\alpha_x\beta_y\psi(xy)| \leq (p^n|G||H|)^{\frac{1}{2}}$.*

Proof. See [22] pp 142. □

2.2.2. Exponential sums over points of elliptic curves

Definition 2.9. *Elliptic curves.*

Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_p$ with $p \geq 3$ defined by an affine Weieirstrass equation of the form $y^2 = x^3 + ax + b$ with coefficients $a, b \in \mathbb{F}_p$. It is known that the set $\mathcal{E}(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points of $\mathcal{E}$, with the point at infinity $\mathcal{O}$ as the neutral element, forms an abelian group. The group law operation is denoted by $\oplus$. Every point $\mathrm{P} \neq \mathcal{O} \in \mathcal{E}(\mathbb{F}_p)$ is denote by $\mathrm{P} = (x(\mathrm{P}), y(\mathrm{P}))$. Given an integer n and a point $\mathrm{P} \in \mathcal{E}(\mathbb{F}_p)$, we write $n\mathrm{P}$ for the sum of n copies of P:

$$n\mathrm{P} = \mathrm{P} \oplus \mathrm{P} \oplus \ldots \oplus \mathrm{P}.$$

Definition 2.10. *Bilinear sums over additive character.*

Given two subsets $\mathcal{P}, \mathcal{Q}$ of $\mathcal{E}(\mathbb{F}_p)$, and arbitrary complex functions σ, v supported on $\mathcal{P}$ and $\mathcal{Q}$ we consider the bilinear sums of additive characters.

$$\mathrm{V}_{\sigma,\mathrm{v}}(\psi, \mathcal{P}, \mathcal{Q}) = \sum_{\mathrm{P}\in\mathcal{P}}\sum_{\mathrm{Q}\in\mathcal{Q}}\sigma(\mathrm{P})\mathrm{v}(\mathrm{Q})\psi(x(\mathrm{P} \oplus \mathrm{Q})).$$

Lemma 2.6. *Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{F}_q$ where $q = p^n$, with $n \geq 1$ and let $\sum_{\mathrm{P}\in\mathcal{P}} |\sigma(\mathrm{P})|^2 \leq \mathrm{R}$ and $\sum_{\mathrm{Q}\in\mathcal{Q}} |\mathrm{v}(\mathrm{Q})|^2 \leq \mathrm{T}$. Then, uniformly over all nontrivial additive character ψ of $\mathbb{F}_q$, $|\mathrm{V}_{\sigma,\mathrm{v}}(\psi, \mathcal{P}, \mathcal{Q})| \ll \sqrt{q\mathrm{RT}}$*

Proof. Let $\mathcal{X}$ be the set of group characters on $\mathcal{E}(\mathbb{F}_q)$. We collect the points P and Q with a given sum $S = \mathrm{P} \oplus \mathrm{Q}$ and identify this condition via the character sum over $\mathcal{X}$. This gives

$$\mathrm{V}_{\sigma,\mathrm{v}}(\psi, \mathcal{P}, \mathcal{Q}) = \sum_{S\in\mathcal{E}(\mathbb{F}_q)}\psi(x(S))\sum_{\mathrm{P}\in\mathcal{P}}\sum_{\mathrm{Q}\in\mathcal{Q}}\sigma(\mathrm{P})\mathrm{v}(\mathrm{Q})\frac{1}{\#\mathcal{E}(\mathbb{F}_q)}\sum_{\mathrm{X}\in\mathcal{X}}\mathrm{X}(\mathrm{P} \oplus \mathrm{Q} \ominus S).$$

Therefore

$$\mathrm{V}_{\sigma,\mathrm{v}}(\psi, \mathcal{P}, \mathcal{Q}) = \frac{1}{\#\mathcal{E}(\mathbb{F}_q)}\sum_{\mathrm{X}\in\mathcal{X}}\sum_{S\in\mathcal{E}(\mathbb{F}_q)}\psi(x(S))\overline{\mathrm{X}(S)}\sum_{\mathrm{P}\in\mathcal{P}}\sigma(\mathrm{P})\mathrm{X}(\mathrm{P})\sum_{\mathrm{Q}\in\mathcal{Q}}\mathrm{v}(\mathrm{Q})\mathrm{X}(\mathrm{Q}).$$

The sum over S is $\mathcal{O}(q^{1/2})$, so

$$\mathrm{V}_{\sigma,\mathrm{v}}(\psi, \mathcal{P}, \mathcal{Q})| \ll \frac{q^{1/2}}{\#\mathcal{E}(\mathbb{F}_q)}\sum_{\mathrm{X}\in\mathcal{X}}\left|\sum_{\mathrm{P}\in\mathcal{P}}\sigma(\mathrm{P})\mathrm{X}(\mathrm{P})\right|\left|\sum_{\mathrm{Q}\in\mathcal{Q}}\mathrm{v}(\mathrm{Q})\mathrm{X}(\mathrm{Q})\right|.$$

Then, with the Cauchy inequality we get

$$\left(\sum_{\mathrm{X}\in\mathcal{X}}\left|\sum_{\mathrm{P}\in\mathcal{P}}\sigma(\mathrm{P})\mathrm{X}(\mathrm{P})\right|\left|\sum_{\mathrm{Q}\in\mathcal{Q}}\mathrm{v}(\mathrm{Q})\mathrm{X}(\mathrm{Q})\right|\right)^2 \leq \sum_{\mathrm{X}\in\mathcal{X}}\left|\sum_{\mathrm{P}\in\mathcal{P}}\sigma(\mathrm{P})\mathrm{X}(\mathrm{P})\right|^2\sum_{\mathrm{X}\in\mathcal{X}}\left|\sum_{\mathrm{Q}\in\mathcal{Q}}\mathrm{v}(\mathrm{Q})\mathrm{X}(\mathrm{Q})\right|^2$$
$$\leq \#\mathcal{E}(\mathbb{F}_q)^2\mathrm{RT}$$

since

$$\sum_{\mathrm{X}\in\mathcal{X}}\left|\sum_{\mathrm{P}\in\mathcal{P}}\sigma(\mathrm{P})\mathrm{X}(\mathrm{P})\right|^2 = \sum_{\mathrm{P}_1,\mathrm{P}_2\in\mathcal{P}}\sigma(\mathrm{P}_1)\overline{\sigma(\mathrm{P}_2)}\sum_{\mathrm{X}\in\mathcal{X}}\mathrm{X}(\mathrm{P}_1 \ominus \mathrm{P}_2) = \#\mathcal{E}(\mathbb{F}_q)\sum_{\mathrm{P}\in\mathcal{P}}|\sigma(\mathrm{P})|^2 \leq \#\mathcal{E}(\mathbb{F}_q)\mathrm{R}.$$

Similarly

$$\sum_{\mathrm{X}\in\mathcal{X}}\left|\sum_{\mathrm{Q}\in\mathcal{Q}}\mathrm{v}(\mathrm{Q})\mathrm{X}(\mathrm{Q})\right|^2 \leq \#\mathcal{E}(\mathbb{F}_q)\mathrm{T},$$

and the desired result follows. □

3. SUMMARY OF PREVIOUS WORK

After a Diffie-Hellman key exchange protocol, the honest parties share an element which is indistinguishable from a uniformly distributed element assuming the DDH assumption. However they need a uniformly distributed bits string to perform cryptographic operations as encryption. Thus one needs to extract entropy from the shared element.

Several solutions exist and can be implemented. There are essentially two methods of resolution: the descent method and the character method.

3.1. Descent method and probabilistic solutions

The descent method is based on the random oracle model. The first way, and also the most commonly used, to derive a bits string from a random element is to hash using hash functions. The advantage of this solution is that its implementation is simple. However, most often the solutions of this method are probabilistic. Indeed, in addition to the original source, it is considered an additional input which is uniformly distributed, meaning that it is viewed as a perfect random that, in practice, is difficult to achieve. The additional input is called "seed" and such constructions are named "seeded extractor".

For such extractors with seed of length $\mathcal{O}(\log n)$ bits, together with enumeration over all possible seed values, it is possible to simulate probabilistic algorithm with polynomial overhead, using only a high min-entropy source. On that point of view, the polynomial overhead can be too expensive. More, cryptographic applications prohibit such enumeration.

In 1998, Boneh et *al.* [5] showed that calculating the *k-most significant bits* of a secret is as difficult as calculating the common secret. The authors relied on the *Hidden Number Problem* (HNP). The goal of the HNP is to find a hidden number $s \in \mathbb{Z}_p^*$, when given p a prime, g a generator of $\mathbb{Z}_p^*$ and access to an oracle that on query a returns the k most significant bits of $s.g^a \mod (p)$.

Hästad et *al*. [16] proposed random extractor based on the probabilistic *Leftover Hash Lemma*, capable of removing all of the entropy random source having sufficient min-entropy. This technique and its variants, however, require the use of hash functions and perfect random.

The drawback of these extractors is that they belong to the random oracle model so the indistinguishability cannot be proven under the DDH assumption unless you add a random oracle which in practice is considered to be limitations.

3.2. Character method

The character method is based on the standard model. Another approach, not requiring the consideration of an additional perfect random is to use the deterministic randomness extractors. They are also called "seedless extractors" and do not require any computation. The only constraint is to consider quite large subgroups.

There have been many works constructing such seedless extractors using different techniques.

In 2008, Fouque et *al*. [15] proposed a simple extractor capable of extracting the *k-least significant bits* or the *k-most significant bits* of a strong random element issued to the Diffie-Hellman exchange on a sufficient big subgroup of $\mathbb{Z}_p$. They relied on exponential sums to bound the statistical distance between two variables.

In 2009, Chevalier et *al*. [11] also used exponential sums but bound the collision probability of bits extracted to prove the security of their extractor. Authors used the *Vinogradov inequality* to limit the incomplete character sums. They improved the results of Fouque by providing an extractor capable of extracting up to two times more bits. They also featured extractor on the group of points of an elliptic curve defined over a finite field. However, their work was limited to the finite prime fields.

In 2011, Ciss et *al*. [12] extended the work of Chevalier over finite non-prime fields $\mathbb{F}_{p^n}$ and elliptic curves over $\mathbb{F}_{p^n}$ and more particularly on binary finite fields. They used the *Winterhof inequality* to limit the incomplete character sums.

All those previous works are based on the use of single character sums for their proof. Sometimes a source cannot be able to allow deterministic extraction. So, when seedless extractor from one source is impossible or when the unique source does not have enough min-entropy, it is natural to consider doing so from several independent sources.

Indeed, in the last few years, there where results on constructing extractors for a few independent sources. For example, in 2005, Bourgain [8] showed how to get an extractor for 2 sources relying on bounds coming from arithmetic combinatorics. In 2012, Kasher et *al.* [17] proposed a two-sources extractors in the quantum world, especially against entanglement.

4. OUR CONTRIBUTION

4.1. Randomness extractors in finite fields

We propose and prove the security of a simple deterministic randomness extractor for two subgroups G_1 and G_2 of $\mathbb{F}_q^*$ where $q = p^n$, with p prime and $n \geq 1$. The main theorem of this section states that the k-least significant bits of $x_1 \cdot x_2$, where (x_1, x_2) is a random element in (G_1, G_2), are close to a truly random element in $\{0,1\}^k$. Our approach is from the model based on character sums.

4.1.1. Randomness extraction in $\mathbb{F}_p$

Let $\mathbb{F}_p$ be a finite prime field such that $|p| = m$. Let G_1 and G_2 be two multiplicative subgroups of $\mathbb{F}_p^*$ of order q_1 and q_2 respectively, with $|q_1| = l_1$, $|q_2| = l_2$, the bit-length of q_1 and q_2 respectively. Let U_{G_1} (resp. U_{G_2}) be a random variable uniformly distributed on G_1 (resp.G_2), and k a positive integer less than m.

Definition 4.1. *Extractor f_k on $\mathbb{F}_p$.*
The extractor f_k is defined as the function $f_k : G_1 \times G_2 \longrightarrow \{0,1\}^k, (x_1, x_2) \longmapsto lsb_k(x_1.x_2)$

The following theorem shows that f_k is a good randomness extractor.

Theorem 4.1. *Let U_k be a random variable uniformly distributed on $\{0,1\}^k$. If $\Delta = SD(f_k(U_{G_1}, U_{G_2}), U_k)$ then,*

$$2\Delta \leq 2^{\frac{k+m+\log_2(m)-(l_1+l_2)}{2}}$$

Proof. We introduce the following notation $S(a,(G_1,G_2)) = \sum_{x_1 \in G_1} \sum_{x_2 \in G_2} e_p(ax_1x_2)$. Let us define $K = 2^k$, and $u_0 = \mathrm{msb}_{m-k}(p-1)$. Let us construct the characteristic function, $\mathbf{1}((x_1,x_2),(x_1',x_2'),u) = \frac{1}{p}\sum_{a=0}^{p-1} e_p(a(x_1x_2 - x_1'x_2' - Ku))$ using properties (1) and (2) of Lemma 2.3. Its equal to 1 if $x_1x_2 - x_1'x_2' = Ku \mod (p)$ and 0 otherwise. Therefore, we can evaluate $Col(f_k(U_{G_1}, U_{G_2}))$ where U_{G_1} (resp. U_{G_2}) is uniformly distributed in G_1 (resp. in G_2):

$Col(f_k(U_{G_1}, U_{G_2})) = \frac{1}{(q_1q_2)^2}|\{((x_1,x_2),(x_1',x_2')) \in (G_1,G_2)^2 \exists u \leq u_0, x_1x_2 - x_1'x_2' = Ku \mod (p)\}| =$

$$\frac{1}{(q_1q_2)^2 p} \sum_{(x_1,x_2)\in(G_1,G_2)} \sum_{(x_1',x_2')\in(G_1,G_2)} \sum_{u=0}^{u_0}\sum_{a=0}^{p-1} e_p(a(x_1x_2 - x_1'x_2' - Ku)).$$

Then, we manipulate the sums, separate some terms (a = 0) with the rest.

That is, for $a = 0$,

$$Col(f_k(U_{G_1}, U_{G_2})) = \frac{1}{(q_1q_2)^2 p}\sum_{a=0}^{p-1} \sum_{(x_1,x_2)\in(G_1,G_2)} \sum_{(x_1',x_2')\in(G_1,G_2)} \sum_{u=0}^{u_0} e_p(0) = \frac{u_0+1}{p} \quad (*)$$

For $a \in \mathbb{F}_p^*$,

$$Col(f_k(U_{G_1}, U_{G_2})) = \frac{1}{(q_1q_2)^2 p}\sum_{a=1}^{p-1} \sum_{(x_1,x_2)\in(G_1,G_2)} \sum_{(x_1',x_2')\in(G_1,G_2)} \sum_{u=0}^{u_0} e_p(a(x_1x_2 - x_1'x_2' - Ku))$$

$$= \frac{1}{(q_1q_2)^2 p}\sum_{a=1}^{p-1} \sum_{(x_1,x_2)\in(G_1,G_2)} e_p(ax_1x_2) \sum_{(x_1'x_2')\in(G_1,G_2)} e_p(-ax_1'x_2') \sum_{u=0}^{u_0} e_p(-aKu)$$

$$= \frac{1}{(q_1q_2)^2 p}\sum_{a=1}^{p-1} S(a,(G_1,G_2))S(-a,(G_1,G_2)) \sum_{u=0}^{u_0} e_p(-aKu)$$

$$= \frac{1}{(q_1q_2)^2 p}\sum_{a=1}^{p-1} |S(a,(G_1,G_2))|^2 \sum_{u=0}^{u_0} e_p(-aKu).$$

We inject the result of (*) tin the above result, the collision probability is there equal to:

$$Col(f_k(U_{G_1}, U_{G_2})) = \frac{u_0+1}{p} + \frac{1}{(q_1q_2)^2 p}\sum_{a=1}^{p-1} |S(a,(G_1,G_2))|^2 \sum_{u=0}^{u_0} e_p(-aKu)$$

According to the change of variable ($a' = Ka = 2^k a \mod (p)$, with $\gcd(2,p) = 1$) and the fact that $[0, u_0]$ is an interval, giving a geometric sum on it, We have: $\sum_{a=1}^{p-1}\sum_{u=0}^{u_0} e_p(-aKu) = \sum_{a=1}^{p-1}\sum_{u=0}^{u_0} e_p(-au) = \sum_{a=1}^{p-1} \frac{1-e_p(-a(u_0+1))}{1-e_p(-a)} = \sum_{a=1}^{p-1} \frac{\sin(\frac{\pi a(u_o+1)}{p})}{\sin(\frac{\pi a}{p})} = 2\sum_{a=1}^{\frac{p-1}{2}} \frac{\sin(\frac{\pi a(u_o+1)}{p})}{\sin(\frac{\pi a}{p})} \leq 2\sum_{a=1}^{\frac{p-1}{2}} \frac{1}{\sin(\frac{\pi a}{p})} \leq 2\sum_{a=1}^{\frac{p-1}{2}} |\frac{p}{a}| \leq p\log_2(p)$

Therefore $Col(f_k(U_{G_1}, U_{G_2})) \leq \frac{u_0+1}{p} + \frac{1}{(q_1q_2)^2 p}|S(a,(G_1,G_2))|^2 p\log_2(p) \leq \frac{u_0+1}{p} + \frac{1}{(q_1q_2)^2 p}(pq_1q_2p\log_2(p)) \leq \frac{u_0+1}{p} + \frac{p\log_2(p)}{q_1q_2}$

Using Lemma 2.1 which gives a relation between the statistical distance Δ, of $f_k(U_{G_1}, U_{G_2})$ with the uniform distribution, and the collision probability: $Col(f_k(U_{G_1}, U_{G_2})) = \frac{1+4\Delta^2}{2^k}$, the previous upper bound combined with some manipulations gives:

$$2\Delta \leq \sqrt{2^k.Col(f_k(U_{G_1}, U_{G_2})) - 1} \leq \sqrt{\frac{2^k}{p}} + \sqrt{\frac{2^k p(\log_2(p))}{q_1q_2}} \leq 2^{\frac{k+m+\log_2(m)-(l_1+l_2)}{2}}$$

□

4.1.2. Randomness extraction in $\mathbb{F}_{p^n}$

Consider the finite field $\mathbb{F}_{p^n}$, where p is a m-bits prime and n is a positive integer greater than 1. $\mathbb{F}_{p^n}$ is a n-dimensional vector space over $\mathbb{F}_p$. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. That means, every element x in $\mathbb{F}_{p^n}$ can be represented in the form $x = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n$, where $x_i \in \mathbb{F}_p$. Let G_1 and G_2 be two multiplicative subgroups of $\mathbb{F}_{p^n}^*$ of order q_1 and q_2 respectively, with $|q_1| = l_1$, $|q_2| = l_2$.
Let U_{G_1} (resp. U_{G_2}) be a random variable uniformly distributed on G_1 (resp.G_2), and k be a positive integer less than n.

The theorem here establishes that the $k-$first coefficients in $\mathbb{F}_p$ of a random element of $G_1 \times G_2$ are indistinguishable from a random group element of $\mathbb{F}_p^k$.

Definition 4.2. *Extractor F_k on $\mathbb{F}_{p^n}$.*
We define the function $F_k : G_1 \times G_2 \longrightarrow \mathbb{F}_p^k, (x, x') \longmapsto (x_1x'_1, x_2x'_2, \ldots, x_kx'_k)$.

The theorem below shows that F_k is a good randomness extractor.

Theorem 4.2. *Let U_k be a random variable uniformly distributed on $\mathbb{F}_p^k$. In the terms of the above consideration, if $\Delta = SD(F_k(U_{G_1}, U_{G_2}), U_k)$ then,*

$$\Delta \leq 2^{\frac{km+nm-(l_1+l_2+2)}{2}}.$$

Proof. Let us introduce the notation $T(a,(G_1,G_2)) = \sum_{x\in G_1}\sum_{x'\in G_2} \psi(axx')$. Let $(x,x'),(y,z) \in (G_1,G_2)^2$.

Let us define the following sets:

$R = \{x_{k+1}x'_{k+1}\alpha_{k+1} + x_{k+2}x'_{k+2}\alpha_{k+2} \ldots + x_nx'_n\alpha_n\}$, a subgroup of $\mathbb{F}_{p^n}$

$C = \{((x,x'),(y,z)) \in (G_1,G_2)^2 / \exists r \in R, xx' - yz = r\}$

$|C| = \frac{1}{p^n}\sum_{x\in G_1, x'\in G_2}\sum_{y\in G_1, z\in G_2}\sum_{r\in R}\sum_{a\in\mathbb{F}_{p^n}} \psi(a(xx' - yz - r))$.

We can evaluate the collision probability: $Col(F_k(U_{G_1}, U_{G_2})) = \frac{|C|}{|G_1 \mathrm{x} G_2|^2}$

$= \frac{1}{(q_1q_2)^2p^n}\sum_{(x,x')\in(G_1,G_2)}\sum_{(y,z)\in(G_1,G_2)}\sum_{r\in R}\sum_{a\in\mathbb{F}_{p^n}} \psi(a(xx' - yz - r))$

$= \frac{1}{(q_1q_2)^2p^n}\sum_{a\in\mathbb{F}_{p^n}}\sum_{(x,x')\in(G_1,G_2)} \psi(axx') \sum_{(y,z)\in(G_1,G_2)} \psi(-ayz)\sum_{r\in R}\psi(-ar)$.

Then we manipulate the sums, separate some terms (a = 0) which gives $\frac{1}{p^k}$ with the rest. So for $a \in \mathbb{F}_{p^n}^*$

$Col(F_k(U_{G_1}, U_{G_2})) = \frac{1}{(q_1q_2)^2p^n}\sum_{a\in\mathbb{F}_{p^n}^*}\sum_{(x,x')\in(G_1,G_2)} \psi(axx') \sum_{(y,z)\in(G_1,G_2)} \psi(-ayz)\sum_{r\in R}\psi(-ar)$

Then, for all $a \in \mathbb{F}_{p^n}$

$Col(F_k(U_{G_1}, U_{G_2})) = \frac{1}{p^k} + \frac{1}{(q_1q_2)^2p^n} \sum_{a\in\mathbb{F}^*_{p^n}} \sum_{(x,x')\in(G_1,G_2)} \psi(axx') \sum_{(y,z)\in(G_1,G_2)} \psi(-ayz) \sum_{r\in R} \psi(-ar)$

$= \frac{1}{p^k} + \frac{1}{(q_1q_2)^2p^n} \sum_{a\in\mathbb{F}^*_{p^n}} |T(a,(G_1,G_2))|^2 \sum_{r\in R} \psi(-ar)$

$\leq \frac{1}{p^k} + \frac{p^n(q_1q_2)p^n}{(q_1q_2)^2p^n}$, by Lemma 2.5 and Theorem 2.4

$\leq \frac{1}{p^k} + \frac{p^n}{(q_1q_2)}$.

Therefore, using Lemma 2.1 with some manipulations, we obtain the expected result:

$\Delta \leq \sqrt{\frac{p^{n+k-2}}{q_1q_2}} \leq 2^{\frac{km+nm-(l_1+l_2+2)}{2}}$. □

Corollary 4.1. *Corollary 1.*

Let G_1 and G_2 be two multiplicative subgroups of $\mathbb{F}^*_{2^n}$ of order q_1 (resp.q_2), with $|q_1| = l_1$, $|q_2| = l_2$.
If $e > 1$ and $k > 1$ are two integers such as $k \leq (l_1 + l_2) - 2e - n + 2$ then, F_k is a $((U_{G_1}, U_{G_2}), \frac{1}{2^e})$-deterministic extractor .

Proof. Proof of corollary 4.1

If $k \leq (l_1 + l_2) - 2e - n + 2$,

$\frac{k+n}{2} \leq \frac{l_1+l_2+2}{2} - e$

$2^{\frac{k+n}{2}} \leq 2^{\frac{l_1+l_2+2}{2}} 2^{-e}$

$\sqrt{\frac{p^{n+k}}{4q_1q_2}} \leq 2^{-e}$ □

Corollary 4.2. *Corollary 2.*

Let $p > 2$ a prime such as $|p| = m$.
If $e > 1$ and $k > 1$ are two integers such as $k \leq \frac{(l_1+l_2)-2e-mn+2}{m}$ then, F_k is a $((U_{G_1}, U_{G_2}), 2^{-e})$-deterministic extractor .

4.2. Randomness extraction in elliptic curves

Let p be a prime greater than 5. Let $\mathcal{E}$ be an elliptic curve over the finite field $\mathbb{F}_p$ and let $\mathcal{P}$, $\mathcal{Q}$ be two subgroups of $\mathcal{E}(\mathbb{F}_p)$. Let denote $|\mathcal{P}| = q_1$ and $|\mathcal{Q}| = q_2$. Let $U_\mathcal{P}$ and $U_\mathcal{Q}$ be two random variables uniformly distributed in $\mathcal{P}$ and $\mathcal{Q}$ respectively.

4.2.1. Randomness extractor in $\mathcal{E}(\mathbb{F}_p)$

Definition 4.3. *We define the function* $\mathrm{extract}_k : \mathcal{P} \times \mathcal{Q} \longrightarrow \{0,1\}^k, (\mathrm{P}, \mathrm{Q}) \longmapsto lsb_k(x(\mathrm{P}) \cdot x(\mathrm{Q}))$.

The following theorem shows that $\mathrm{extract}_k$ is a good randomness extractor.

Theorem 4.3. *Let U_k be the uniform distribution in $\{0,1\}^k$. Then,*

$$\Delta(\mathrm{extract}_k(U_\mathcal{P}, U_\mathcal{Q}), U_k) \ll 2^{\frac{k+n+\log_2(n)-(l_1+l_2+2)}{2}}.$$

Proof. Let us define $K = 2^k$, $u_0 = \mathrm{msb}_{m-k}(p-1)$. Let us define the characteristic function $\mathbf{1}((\mathrm{P},\mathrm{Q}),(\mathrm{A},\mathrm{B}),u) = \frac{1}{p}\sum_{\psi\in\Psi} \psi(x(\mathrm{P})x(\mathrm{Q}) - x(\mathrm{A})x(\mathrm{B}) - Ku)$ which is equal to 1 if $\psi = \psi_0$ and to 0, otherwise.

Let us compute the collision probability: $Col(\mathrm{extract}_k(U_\mathcal{P}, U_\mathcal{Q})) = \frac{1}{(q_1q_2)^2p} \sum_{\mathrm{P}\in\mathcal{P}} \sum_{\mathrm{Q}\in\mathcal{Q}} \sum_{\mathrm{A}\in\mathcal{P}} \sum_{\mathrm{B}\in\mathcal{Q}} \sum_{\psi\in\Psi} \sum_{u\leq u_0} \psi(x(\mathrm{P})x(\mathrm{Q}) - x(\mathrm{A})x(\mathrm{B}) - Ku)$. Then we manipulate the sums, separate some terms ($\psi = \psi_0$) with the rest.

So for ($\psi = \psi_0$),

$Col(\mathrm{extract}_k(U_\mathcal{P}, U_\mathcal{Q})) = \frac{1}{(q_1q_2)^2p} \sum_{\psi=\psi_0} \sum_{\mathrm{P}\in\mathcal{P}} \sum_{\mathrm{Q}\in\mathcal{Q}} \sum_{\mathrm{A}\in\mathcal{P}} \sum_{\mathrm{B}\in\mathcal{Q}} \sum_{u\leq u_0} \psi_0(0)$

$= \frac{1}{(q_1q_2)^2p} \sum_{\psi=\psi_0} \sum_{\mathrm{P}\in\mathcal{P}} \sum_{\mathrm{Q}\in\mathcal{Q}} \sum_{\mathrm{A}\in\mathcal{P}} \sum_{\mathrm{B}\in\mathcal{Q}} \sum_{u\leq u_0} e_p(Tr(0))$

$$= \frac{1}{(q_1q_2)^2p} \sum_{\psi=\psi_0} \sum_{\mathrm{P}\in\mathcal{P}} \sum_{\mathrm{Q}\in\mathcal{Q}} \sum_{\mathrm{A}\in\mathcal{P}} \sum_{\mathrm{B}\in\mathcal{Q}} \sum_{u\leq u_0} 1 = \frac{u_0+1}{p}$$

And for $(\psi \neq \psi_0)$, $Col(\mathrm{extract}_k(U_\mathcal{P}, U_\mathcal{Q})) = \frac{1}{(q_1q_2)^2p} \sum_{\psi\neq\psi_0} \sum_{\mathrm{P}\in\mathcal{P}} \sum_{\mathrm{Q}\in\mathcal{Q}} \sum_{\mathrm{A}\in\mathcal{P}} \sum_{\mathrm{B}\in\mathcal{Q}} \sum_{u\leq u_0} \psi(x(\mathrm{P})x(\mathrm{Q}) - x(\mathrm{A})x(\mathrm{B}) - Ku)$.
Then for all ψ,

$$Col(\mathrm{extract}_k(U_\mathcal{P}, U_\mathcal{Q})) = \frac{u_0+1}{p} + \frac{1}{(q_1q_2)^2p} \sum_{\psi\neq\psi_0} \sum_{\mathrm{P}\in\mathcal{P}} \sum_{\mathrm{Q}\in\mathcal{Q}} \sum_{\mathrm{A}\in\mathcal{P}} \sum_{\mathrm{B}\in\mathcal{Q}} \sum_{u\leq u_0} \psi(x(\mathrm{P})x(\mathrm{Q}) - x(\mathrm{A})x(\mathrm{B}) - Ku)$$
$$= \frac{u_0+1}{p} + \frac{1}{(q_1q_2)^2p} \sum_{\psi\neq\psi_0} \sum_{\mathrm{P}\in\mathcal{P}} \sum_{\mathrm{Q}\in\mathcal{Q}} \psi(x(\mathrm{P})x(\mathrm{Q})) \sum_{\mathrm{A}\in\mathcal{P}} \sum_{\mathrm{B}\in\mathcal{Q}} \psi(-x(\mathrm{A})x(\mathrm{B})) \sum_{u\leq u_0} \psi(-Ku)$$
$$= \frac{u_0+1}{p} + \frac{1}{(q_1q_2)^2p} \sum_{\psi\neq\psi_0} |\sum_{\mathrm{P}\in\mathcal{P}} \sum_{\mathrm{Q}\in\mathcal{Q}} \psi(x(\mathrm{P})x(\mathrm{Q}))| |\sum_{\mathrm{A}\in\mathcal{P}} \sum_{\mathrm{B}\in\mathcal{Q}} \psi(-x(\mathrm{A})x(\mathrm{B}))| \sum_{u\leq u_0} \psi(-Ku)$$
$$= \frac{u_0+1}{p} + \frac{1}{(q_1q_2)^2p} \sum_{\psi\neq\psi_0} |\mathrm{V}(\psi, \mathcal{P}, \mathcal{Q})|^2 \sum_{u\leq u_0} \psi(-Ku)$$
$$\leq \frac{1}{p} + \frac{1}{(q_1q_2)^2p} \sum_{\psi\neq\psi_0} q_1q_2p \sum_{u\leq u_0} \psi(-Ku), \quad by \quad Lemma \quad 2.6$$
$$\leq \frac{1}{p} + \frac{1}{(q_1q_2)^2p} pq_1q_2p\log_2(p), \quad since \quad it \quad is \quad shown \quad that \sum_{\psi\neq\psi_0} \sum_{u\leq u_0} \psi(-Ku) \leq p\log_2(p)$$
$$\leq \frac{1}{p} + \frac{1}{(q_1q_2)} p\log_2(p).$$

Therefore, using Lemma 2.1 with some manipulations, we obtain the expected result:
$$\Delta(\mathrm{extract}_k(U_\mathcal{P}, U_\mathcal{Q}), U_k) \ll \sqrt{\frac{2^{k-2}p\log_2(p)}{q_1q_2}} = 2^{\frac{k+n+\log_2(n)-(l_1+l_2+2)}{2}}$$ □

4.2.2. Randomness extractor in $\mathcal{E}(\mathbb{F}_{p^n})$

Definition 4.4. *Let us define the function* $\mathrm{Extract}_k : \mathcal{P} \times \mathcal{Q} \longrightarrow \mathbb{F}_p^k, (\mathrm{P}, \mathrm{Q}) \longmapsto (t_1, t_2, \ldots, t_k)$*, where* $x(\mathrm{P}) \cdot x(\mathrm{Q}) = t_1\alpha_1 + t_2\alpha_2 + \ldots + t_n\alpha_n$.

The theorem below shows that $\mathrm{Extract}_k$ is a good randomness extractor over $\mathcal{E}(\mathbb{F}_{p^n})$.

Theorem 4.4. *Let U_k be the uniform distribution in $\mathbb{F}_p^k$. Then,*

$$\Delta(\mathrm{Extract}_k(U_\mathcal{P}, U_\mathcal{Q}), U_k) \ll 2^{\frac{km+nm-(l_1+l_2+2)}{2}}.$$

Proof. Using Lemma 2.6 and Theorem 2.4, the sketch of the proof is the same as those of Theorem 4.2 □

4.3. Specification: Abstract Data Type

Sort ArrayofBits;

Functions

initialize:		→	ArrayofBits;
createKey:	Integer	→	ArrayofBits;
getKeyLength:	ArrayofBits	→	Integer;
testParameterEntropy	ArrayofBits,Integer	→	Boolean;
lsb-k:	ArrayofBits,Integer	→	ArrayofBits;

Axioms

A1 initialize=[]

A2 createKey(r) = createKey(ConvertToBits(r))

A3 getKeyLength(initialize) = 0

A4 getKeyLength(createKey(r))
= # getKeyLength(createKey(ConvertToBits(r)))

A5 testParameterEntropy(initialize, k)=False

A6 testParameterEntropy(createKey(r), k)= True,
if getKeyLength(createKey(r))$\geq k$

A7 lsb-k(initialize, k)= Error

A8 lsb-k(createKey(r), k)
= lsb-k(createKey(ConvertToBits(r)), k)

5. APPLICATIONS

The ideas behind a randomness extractors is the following one: suppose one got a random variable X with some entropy but which is not uniform. For many areas of computer science, typically for many cryptographic applications, it is required an uniformly random variable for example to use as a secret key. Therefore, one needs to somehow extract the randomness from X to get a uniformly distributed output.

Extractors for multiple sources. Sometimes, extraction from one source is impossible.

There are some solutions in the probabilistic method namely "seeded extractors". These are extractors that receive one source (with min-entropy at least k, for some parameter k) and an independent short input Y, called "seed", that is uniformly distributed. Since the assumption over Y is strong, that is having perfectly random bits is difficult in practice, an alternative is the use of two or more sources. In this setup, a more natural setting is to consider Y with the same length and min-entropy threshold as X.

Moreover, cryptographic protocols require to work on sufficient large sub-groups. The high level of considering multiple sources is to show that if the given l-sources with *min-entropy* $\delta n, \delta > 0$ are over a finite field $\mathbb{F}_q$ that has no large sub-fields (which holds in the case that $\mathbb{F}_q$ is a prime field), then the cumulative distribution will have more *min-entropy*.

Generating keys for cryptographic protocols The interest of studying randomness extractors has several cryptographic applications. Specially, it can apply for the key extraction phase of a key exchange protocol, but also for identity encryption schemes.

The security of cryptographic protocols depends on the ability of honest parties to generate uniformly distributed and private random key. More generally, honest parties work in a non-secure environment set up by an adversary trying to steal the shared secret.

Thus multi-source extractors enable an honest party to sample a string that is (close to) uniform, given multiple sources, the main requirement from each source being to contain some min-entropy.

For example, if one wants to extract a 256-bits, for $n = 1024, e = 80$, one needs a group of seize greater than 2^{756} with Chevalier's et *al.* extractor [11]. With our extractor f_k define in subsection 4.1.1, considering two groups of sizes 2^{724} one can extracts 256-bits. In this case, f_k is an $((U_{G_1}, U_{G_2}), 2^{-80})-$deterministic extractor.

Exemple: key exchange protocol and key extraction from two-sources

Parameters: An elliptic curve group of points $G = \langle P \rangle$; A two-sources randomness extractor $\mathrm{Extract}_k : G \times G \mapsto \{0,1\}^k$;

1. Initial Point exchange

   Alice chooses $a \in \mathbb{Z}_q^*$, sends aP to Bob;

   Bob chooses $b \in \mathbb{Z}_q^*$, sends bP to Alice;

   Alice computes abP and Bob computes baP;

   $R = abP$; (They share and keep secret R)

2. For each session

   Alice chooses $a' \in \mathbb{Z}_q^*$, sends $a'P$ to Bob;

   Bob chooses $b' \in \mathbb{Z}_q^*$, sends $b'P$ to Alice;

   Alice computes $a'b'P$ and Bob computes $b'a'P$;

   $Q = a'b'P$;

   $K = \mathrm{Extract}_k(R, Q) = \mathrm{lsb}_k(x(R) + x(Q))$;

   $R = Q$;

6. CONCLUSION

The problem is: how to ensure the indistinguability of a key session which is a string of bits issue to a shared element after a Diffie-Hellman exchange protocol. Even if the commonly use solution is one of a hash function, the solutions in the standard model are more reliable. We have constructed some two-sources deterministic randomness extractors which perform extraction of random bits string close to the uniform distribution over more than one source of information. These extractors can be used in any finite field or any elliptic curve based protocols. We have also proposed some applications, for example a version of Diffie-Hellman key exchange protocol with key extraction step.

As future work, we intend to generalize the proposed extractors to n-sources, find analogous results for hyperelliptic curves and propose cryptographically secure pseudorandom number generators based on these extractors. Most identity-based protocols calculates the current key of a user from its identity view as a point of an (hyper)elliptic curve . This is, an implementation of a platform of session keys generation using our extractors, and of calculation of a point of a curve using new encoding functions is underway. The goal here is to provide a practical tool for key generation phases of these encryption primitive .

7. REFERENCES

[1] O. Ahmadi, and I. E. Shparlinski. Exponential Sums over Points of Elliptic Curves. arXiv preprint arXiv:1302.4210. (2013)

[2] A. Balog, K. A. Broughan and I. E. Shparlinski. *Sum-Products Estimates with Several Sets and Applications*

[3] M. Bellare and P. Rogaway. *Random oracles are practical : A Paradigm for designing efficient protocols*. In V. Ashby, editor, ACM CCS 93, pages 62-73. ACM Press, Nov. 1993.

[4] D. Boneh. The decision Diffie-Hellman problem. *In Third Algorithmic Number Theory Symposium (ANTS)*, vol.1423 of LNCS. Springer, 1998.

[5] D. Boneh and R. Venkatesan. *Hardness of computing the most significant bits of secret keys in Diffie-Helman and related schemes*. In N. Koblitz, editor, CRYPTO'96, vol. 1109 of LNCS, pages 129-142. Springer, Aug. 1996.

[6] J. Bourgain and M. Z. Garaev. *On a variant of sum-product estimate and explicit exponential sum bounds in prime field*, Math.Proc.Camb.Phil.Soc, 146(2008), 1-21.

[7] J. Bourgain and S. V. Konyagin. *Estimates for the Number of Sums and Products and for Exponential Sums Over Subgroups in Fields of Prime Order*.

[8] J. Bourgain. *More on the sum-product phenomenon in prime fields and its applications*, International Journal of Number Theory, 1:1?2, 2005.

[9] R. Carneti, J. Friedlander, S. Koyagin, M. Larsen, D. Lieman and I. Shparlinski. *On the Statistical Properties of Diffie-Hellman Distributions*. Israel Journal of Mathematics, vol. 120, pages 23-46, 2000.

[10] R. Carnetti, J. Friedlander, and I. Shparlinski. *On Certain Exponential Sums and the Distribution of Diffie-Hellman Triples*. Journal of the London Mathematical Society, 59(2):799-812, 1999.

[11] C. Chevalier, P. Fouque, D. Pointcheval and S. Zimmer. *Optimal Randomness Extraction from a Diffie-Hellman Element, Advances in Cryptology*- Eurocrypt'09, vol. 5479 of LNCS, pages 572-589, Springer-Verlag, 2009

[12] A. A. Ciss and D. Sow. *On Randomness Extraction in Elliptic Curves*. In A. Nitaj and D. Pointcheval, editors. Africacrypt 2011, vol. 6737 of LNCS, pages 290-297. Springer-Verlag, 2011.

[13] W. Diffie, M. Hellman. *New Directions in Cryptography, IEEE Trans- actions On Information Theory*, vol.22, no.6, 644-654, 1976

[14] R. R. Farashahi, I. E. Shparlinski, and J. F. Voloch. *On hashing into elliptic curves*, J.Math.Cryptology, 3, 353-360, 2010

[15] P. A. Fouque, D. Pointcheval, J. Stern, and S. Zimmer. *Hardness of distinguishing the MSB or the LSB of secret keys in Diffie-Hellman schemes*. In M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, editors, ICALP 2006, Part II, vol. 4052 of LNCS, pages 240-251. ACM, 2008.

[16] J. Hästad, R. Impagliazzo, L. Levin, and M. Luby. *A pseudorandom generator from any one-way function*, SIAM Journal on Computing, Vol. 28, no.4, 1364-1396,1999

[17] R. Kasher and J. Kempe. *Two-source Extractors Secure Against Quantum Adversaries*, Theory Of Computing, 8(1)(2012):461-486.

[18] S. V. Koyagin and I. Shparlinski. *Character Sums With Exponential Functions and Their Applications*. Cambridge University Press, Cambridge, 1999.

[19] V. Shoup. *A Computational Introduction to Number Theory and Algebra Cambridge University Press*, Cambridge 2005.

[20] L. Trevisan. *Extractors and pseudorandom generators*. J. ACM 48, 4 (July 2001), 860-879, (2001).

[21] L. Trevisan and S. Vadhan. *Extracting Randomness from Samplable Distributions*, IEEE Symposium on Foundations of Computer Science, 32-42, 2000

[22] I. M. Vinogradov. *An Introduction to the Theory of Numbers* (Pergamon Press, 1955).

[23] A. Winterhof. *Incomplete Additive Character Sums and Applications*. In D. Jungnickel and H. Niederreiter, editors. Finite Fields and Applications, pages 462-474. Springer-Velag 2001.

[24] S. Zimmer. *Mécanismes cryptographiques pour la génération de cléfs et l'authentification*