Randomness Extraction in finite fields $\mathbb{F}_{p^n}$

No Author Given

No Institute Given

Abstract. Many technics for randomness extraction over finite fields was proposed by various authors such as Fouque *et al.* and Carneti *et al.*. At eurocrypt'09, these previous works was improved by Chevalier *et al.*, over a finite field $\mathbb{F}_p$, where p is a prime. But their papers don't study the case where the field is not prime such as binary fields. In this paper, we present a deterministic extractor for a multiplicative subgroup of $\mathbb{F}_{p^n}^*$, where p is a prime. In particular, we show that the k-first $\mathbb{F}_2$-coefficients of a random element in a subgroup of $\mathbb{F}_{2^n}^*$ are indistinguishable from a random bit-string of the same length. Hence, under the Decisional Diffie-Hellman assumption over binary fields, one can deterministically derive a uniformly random bit-string from a Diffie-Hellman key exchange in the standard model. Over $\mathbb{F}_p$, Chevalier *et al.* use the "Polya-Vinogradov inequality" to bound incomplete character sums but over $\mathbb{F}_{p^n}^*$ we use "Winterhof inequality" to bound incomplete character sums. Our proposition is a good deterministic extractor even if the length of its output is less than those one can have with the leftover hash lemma and universal hash functions. Our extractor can be used in any cryptographic protocol or encryption schemes.

Keywords: Finite fields, Polya-Vinogradov inequality, Winterhof inequality, exponential sums, incomplete character sums, Deterministic extractor, Decisional Diffie-Hellman, random bit-string, key exchange, leftover hash lemma.

1 Introduction

In many cryptographic protocols and cryptographic schemes, it is necessary to be able to derive a random bit-string from a random element in a group. This is the case for Diffie-Hellman key exchange [8] which is the most famous protocol that allows parties to agree on a common random element in a cyclic subgroup H of a group G, generated by an element g of prime order q. The security of the Diffie-Hellman exchange relies on the Diffie-Hellman assumption (DDH) [2], which states that there is no efficient algorithm that can distinguish the two distributions (g^a, g^b, g^{ab}) and (g^a, g^b, g^c) in G^3, where $1 \leq a, b, c \leq q$ are chosen at random. Under the DDH assumption, one can agree on a random private element. Hence, one has to derive a random-looking bit-string from this random element. Different approaches were proposed to solve this problem.

One classical way to transform a random group-element to a random-looking bit-string is to apply a hash function to the Diffie-Hellman group-element but

the indistinguishability is proved under the random oracle model [1]. An alternative method to hash functions, secure under the standard model, is to use a randomness extractor.

In 1998, Boneh *et al.* propose in [4], to extract the least or the most significant bits of the Diffie-Hellman element.

In 1999, Håstad *et al.*, [12], via the Leftover Hash Lemma, propose a probabilistic randomness extractor that can extract entropy from any random source which has sufficient min-entropy. This technic, with its variants [10, 12], requires the use of hash or pseudorandom functions and an extra perfect randomness, which is a lack for practical use.

In 2000, Carneti *et al.* [5] show that, in a statistical sense, the k most significant bits of g^{xy} is indistinguishable from a random bit-string of length k, given the k most significant bits of g^x and g^y. But, in 2001, Boneh *et al.* observe that this technic cannot be used in practice because in most protocols, the adversary learns all of g^x and g^y.

In 2008, Fouque *et al.* show in [9], under the DDH assumption that k least significant bits or the most significant bits of a random element in a subgroup of $\mathbb{Z}_p^*$ are indistinguishable from a random bit-string of the same length. To prove this, the authors bound the statistical distance by evaluating the L_1 norm, using exponential sums.

In 2009, at Eurocrypt, Chevalier *et al.* [6] study a quite simple deterministic extractor from random Diffie-Hellman elements defined over a prime order multiplicative subgroup G of $\mathbb{Z}_p^*$ and over the group of points of an elliptic curve. They upper-bound the L_2 norm and use some classical results on exponential sums to prove their results. They improve at the same time the results in [9]. But their works include only prime fields.

In this paper, we extend the above result of Chevalier *et al.* to non prime finite fields: $\mathbb{F}_{p^n}$, with a prime p and a positive integer n greater than 1. The extension of the work of Chevalier *et al.* on elliptic curves over non prime finite fields was already done in [7]. Here, we present a quite simple deterministic extractor, denoted Ext_k for a multiplicative subgroup G of a finite field $\mathbb{F}_{p^n}$. In particular for binary finite fields $\mathbb{F}_{2^n}$, we show under the DDH assumption that the k-first $\mathbb{F}_2$-coefficients (the k least significant bits) of a random group-element in a subgroup of $\mathbb{F}_{2^n}^*$, are indistinguishable from a random bit-string of the same length. This approach is somewhat similar to those of [7] for deterministic randomness extractor in elliptic curves. Over $\mathbb{F}_p$, Chevalier *et al.* use the "Polya-Vinogradov inequality" to bound incomplete character sums [14] but over $\mathbb{F}_{p^n}^*$ we use "Winterhof inequality" to bound incomplete character sums [20].

The paper is organized as follows : In section 1, we recall some definitions and results about randomness extraction and character sums. In section 2, we present and give an analysis of our extractor. We finish by giving a natural application of our extractor to the Diffie-Hellman key exchange in $\mathbb{F}_{2^n}^*$.

2 Preliminaries

In this section, we introduce some definitions and results about entropy and randomness extraction.

2.1 Deterministic extractor

Definition 1 (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*

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

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

Definition 2 (Statistical distance). *Let S be a finite set. If X and Y are S-valued random variables, then the statistical distance $\Delta(X, Y)$ between X and Y is defined as*

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

Definition 3. *Let U_S be a random variable uniformly distributed on S and $\delta \leq 1$ a positive real number. Then a random variable X on S is said to be δ-uniform if*

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

Lemma 1. *Let S be a finite set and let $(\alpha_x)_{x \in S}$ be a sequence of real numbers. Then,*

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

Proof. This inequality is a direct consequence of Cauchy-Schwartz inequality:

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

The result can be deduced easily.

Corollary 1. *If X is an S-valued random variable then*

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

Lemma 2. *Let X be a random variable over a finite set S of size $|S|$ and $\epsilon = \Delta(X, U_S)$ be the statistical distance between X and U_S, where U_S is a uniformly distributed random variable over S. Then,*

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

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

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

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

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

The lemma can be deduced easily.

Definition 4. *Let S and T be two finite sets. Let* Ext *be a function* $\mathrm{Ext} : S \longrightarrow T$*. We say that* Ext *is a deterministic (T, δ)-extractor for S if* $\mathrm{Ext}(U_S)$ *is δ-uniform on T. That is*

$$\Delta(\mathrm{Ext}(U_S), U_T) \leq \delta.$$

For more information on extractors, see [16, 18].

2.2 Character sums

In the following, we recall some fundamental results on character sums. We denote by e_p the character on $\mathbb{F}_p$ such that, for all $y \in \mathbb{F}_p$, $e_p(y) = e^{\frac{2i\pi y}{p}} \in \mathbb{C}^*$, and by ψ the additive character in $\mathbb{F}_{p^n}$ such that for all $x \in \mathbb{F}_{p^n}$, $\psi(x) = e_p(\mathrm{Tr}(x))$ where $\mathrm{Tr}(x) = x + x^p + \ldots + x^{p^{n-1}}$ is the trace of $x \in \mathbb{F}_{p^n}$ to F_p.

Lemma 3. *Let ψ be an additive character of $\mathbb{F}_{p^n}$ and let G be a multiplicative subgroup of $\mathbb{F}_{p^n}^*$. Consider the following Gauss sum $T(a, G) = \sum_{x\in G} \psi(ax)$. Then,*

$$\max_{a\in\mathbb{F}_{p^n}^*} |T(a, G)| \leq \sqrt{p^n}.$$

Proof. See [14] or [17].

Lemma 4. *Let V be an additive subgroup of $\mathbb{F}_{p^n}$ et let ψ be an additive character of $\mathbb{F}_{p^n}$. Then,*

$$\sum_{y\in\mathbb{F}_{p^n}} \left|\sum_{z\in V} \psi(yz)\right| \leq p^n.$$

Proof. See [20] for the proof.

For more details on character sums see [14, 15].

2.3 Leftover Hash Lemma

In this subsection, we recall the Leftover Hash Lemma [13, 12]. It is the most famous randomness extractor but it requires the use of universal hash functions.

Definition 5 (Guessing probability).
Let X be a random variable taking values on a set $\mathcal{V}$ of size N, the guessing probability $\gamma(X)$ of X is defined to be $\gamma(X) = \max\{P[X = v] : v \in \mathcal{V}\}$.

Definition 6 (Universal hash function families). *Let $\mathcal{H} = \{h_i\}_i$ be a family of efficiently computable hash functions $h_i : \{0,1\}^n \longrightarrow \{0,1\}^k$, for $i \in \{0,1\}^d$. We say that $\mathcal{H}$ is a universal hash function family if for every $x \neq y$ in $\{0,1\}^n$,*

$$\mathrm{Pr}_{i\in\{0,1\}^d}[h_i(x) = h_i(y)] \leq 1/2^k.$$

Theorem 1 (Leftover Hash Lemma). *Let $\mathcal{H}$ be a universal hash function family from $\{0,1\}^n$ to $\{0,1\}^k$, keyed by $i \in \{0,1\}^d$. Let i denote a random variable with uniform distribution over $\{0,1\}^d$, let U_k be a random variable uniformly distributed in $\{0,1\}^k$, and let A be a random variable taking values in $\{0,1\}^n$, with i and A mutually independent. Let $\gamma = \gamma(A)$, then*

$$\Delta(\langle i, h_i(A)\rangle, \langle i, U_k\rangle) \leq \frac{\sqrt{2^k\gamma}}{2}.$$

Proof. See [19]

The Leftover Hash Lemma extracts nearly all of the entropy available whatever the randomness sources are, but it needs to invest few additional truly random bits. To circumvent this problem, we propose a deterministic extractor which is not optimal.

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

In this section, we propose and prove the security of a simple deterministic randomness extractor for a subgroup G of $\mathbb{F}_{p^n}$. The main theorem of this section states that the k-first coefficients of a random element in G are close to a truly random group-element in $\mathbb{F}_p^k$. Our approach is somewhat similar to those in [7] related to randomness extraction in elliptic curves defined over $\mathbb{F}_{p^n}$. In fact, we use the Gaussian exponential sums to bound the statistical distance.

Consider the finite field $\mathbb{F}_{p^n}$, where p is prime and n is a positive integer. Then $\mathbb{F}_{p^n}$ 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 $x_i \in \mathbb{F}_{p^n}$. Let G be a subgroup of $\mathbb{F}_{p^n}$. The extractor Ext_k, for a given random element x of G, outputs the k-first $\mathbb{F}_p$-coefficients of x.

Definition 7. *Let $G \subset \mathbb{F}_{p^n}^*$ be a multiplicative subgroup of order q and let k be a positive integer less than n. The extractor* Ext_k *is defined as a function*

$$\begin{aligned} \mathrm{Ext}_k : G &\longrightarrow \mathbb{F}_p^k \\ x &\longmapsto (x_1, x_2, \ldots, x_k), \end{aligned}$$

where x is represented as $x = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n$.

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

Theorem 2. *Let $G \subset \mathbb{F}_{p^n}^*$ be a multiplicative subgroup of order q. Then*

$$\Delta(\mathrm{Ext}_k(U_G), U_{\mathbb{F}_q^k}) \leq \frac{\sqrt{p^{(n+k)}}}{2q},$$

where $1 < k < n$ is a positive integer, U_G is a random variable uniformly distributed in G and $U_{\mathbb{F}_p^k}$ is the uniform distribution in $\mathbb{F}_p^k$.

Proof. Let us define the sets

$$M = \{(x_{k+1}\alpha_{k+1} + x_{k+2}\alpha_{k+2} + \ldots + x_n\alpha_n), x_i \in \mathbb{F}_p\} \subset \mathbb{F}_{p^n},$$

and

$$A = \{(x, y) \in G^2 / \exists m \in M, x - y = m\}.$$

Let us construct the characteristic function

$$\mathbf{1}_{(x,y,m)} = \frac{1}{p^n} \times \sum_{a \in \mathbb{F}_q} \psi(a(x - y - m)),$$

which is equal to 1 if $x - y = m$ and 0 otherwise. Then the size of the set A is given by

$$|A| = \frac{1}{p^n} \times \sum_{x \in G} \sum_{y \in G} \sum_{m \in M} \sum_{a \in \mathbb{F}_p^n} \psi(a(x - y - m)).$$

Therefore,

$$\begin{aligned}
\mathrm{Col}(\mathrm{Ext}_k(U_G)) &= \frac{|A|}{|G|^2} = \frac{|A|}{q^2} \\
&= \frac{1}{q^2 \times p^n} \times \sum_{x\in G}\sum_{y\in G}\sum_{m\in M}\sum_{a\in\mathbb{F}_p^n} \psi(a(x-y-m)) \\
&= \frac{1}{p^k} + \frac{1}{q^2 \times p^n} \times \sum_{x\in G}\sum_{y\in G}\sum_{m\in M}\sum_{a\in\mathbb{F}_{p^n}^*} \psi(a(x-y-m)) \\
&= \frac{1}{p^k} + \frac{1}{q^2 \times p^n} \times \sum_{a\in\mathbb{F}_{p^n}^*} \left(\sum_{x\in G}\psi(ax)\right)\left(\sum_{y\in G}\psi(-ay)\right)\sum_{m\in M}\psi(-am) \\
&= \frac{1}{p^k} + \frac{1}{q^2 \times p^n} \times \sum_{a\in\mathbb{F}_{p^n}^*} T(a,G).T(-a,G)\sum_{m\in M}\psi(-am) \\
&\leq \frac{1}{p^k} + \frac{1}{q^2 \times p^n} \times R^2 \times \sum_{a\in\mathbb{F}_{p^n}^*} \left|\sum_{m\in M}\psi(-am)\right|,
\end{aligned}$$

where $R = \max_{a\in\mathbb{F}_{p^n}^*} |T(a,G)|$ ..

Since

- $R \leq \sqrt{p^n}$, by Lemma 3,
- and $\sum_{a\in\mathbb{F}_{p^n}^*} \left|\sum_{m\in M}\psi(-am)\right| \leq p^n$, by Lemma 4,

we have the following inequalities:

$$\mathrm{Col}(\mathrm{Ext}_k(U_G)) \leq \frac{1}{p^k} + \frac{p^n}{q^2}.$$

Therefore,

$$\frac{1 + 4\Delta^2(Ext_k(U_G), U_{\mathbb{F}_p^k})}{p^k} \leq \frac{1}{p^k} + \frac{p^n}{q^2}.$$

Hence,

$$\Delta(\mathrm{Ext}_k(U_G), U_{\mathbb{F}_p^k}) \leq \frac{\sqrt{p^{(n+k)}}}{2q}.$$

For non binary field, we have the following corollary.

Corollary 2. *Let $p > 2$ be a prime and let $G \subset \mathbb{F}_{p^n}^*$ be a multiplicative subgroup of order q with $|q| = r$ and $|p| = m$. If $e > 1$ is a positive integer and $k > 1$ is a positive integer such that*

$$k \leq \frac{2r - 2e - mn}{m},$$

then Ext_k is a $(U_G, \frac{1}{2^e})$ deterministic randomness extractor.

Proof. Since $k \leq \frac{2r-2e-mn}{m}$, we have

$$\frac{m(n+k)}{2} \leq r-e \Longleftrightarrow 2^{\frac{m(n+k)}{2}} \leq 2^r \times 2^{-e} \Longleftrightarrow \frac{2^{\frac{m(n+k)}{2}}}{2 \times 2^{r-1}} \leq 2^{-e} \Longleftrightarrow \frac{p^{\frac{(n+k)}{2}}}{2q} \leq 2^{-e}.$$

Hence $\Delta(\mathrm{ext}_k(U_G), U_{\mathbb{F}_p^k}) \leq 2^{-e}$.

For binary fields, we obtain the following lemma.

Lemma 5. *Let $G \subset \mathbb{F}_{2^n}^*$ be a multiplicative subgroup of order q with $|q| = r$. If $e > 1$ is a positive integer and and $k > 1$ is a positive integer such that*

$$k \leq 2r - 2e - n,$$

then Ext_k *is a* $(U_G, \frac{1}{2^e})$ *deterministic randomness extractor.*

Proof. We have

$$k \leq 2t - 2e - n \Leftrightarrow 2^{\frac{(n+k)}{2}} \leq 2^r 2^{-e}.$$

Since $p = 2$ and $2^{r-1} \leq q < 2^r$, we deduce that $p^{\frac{(n+k)}{2}} \leq \frac{2^r}{2^e}$. Therefore,

$$\frac{\sqrt{p^{n+k}}}{2 \times 2^{r-1}} \leq \frac{1}{2^e} \Longleftrightarrow \frac{\sqrt{p^{n+k}}}{2q} \leq \frac{1}{2^e}.$$

Remark 1. We have the same results as above if the extractor Ext_k outputs the k-last $\mathbb{F}_p$-coefficients of a given random element in a multiplicative subgroup G of $\mathbb{F}_{p^n}^*$.

4 Applications

Our extractor can extract entropy from any random element in a group G. Hence, an obvious application of the extractor Ext_k is key derivation from a random Diffie-Hellman element in a DDH group $G \subset \mathbb{F}_{2^n}^*$. After a Diffie-Hellman key exchange, parties agree on a common random element in G which is indistinguishable from a uniformly distributed element in G, under the DDH assumption. However, it does not suffice since they want a uniformly distributed bit-string for symmetric schemes. Thus, one have to extract the entropy from this random Diffie-Hellman element by means of a randomness extractor.

For example, suppose that we want a 256-bits symmetric key from a random Diffie-Hellman key exchange is a subgroup G of $\mathbb{F}_{2^n}$ with a security bound of $2^{-e} = 2^{-80}$ as in the Leftover Hash Lemma. Then, one has to take the prime $n = 811$ and consider a subgroup G of prime order q with $|q| = r = 615$. We obtain exactly a perfectly random 256-bit string with the security bound 2^{-80}. Note that the subgroup G has only q elements with $2^{615} \leq q < 2^{616}$.

As in [10] for prime field, the large q is the main drawback here for non prime field because q is greater than $\sqrt{p^n}$.

In the following table we give the size of $q = |G|$,(with $p = 2$ and $e = 80$) knowing the size n(= prime) of the field $\mathbb{F}_{2^n}$ and k (the length of the output of the extractor).

k (key)\\n (prime)	521	811	1021	1153
128	$\|q\| = 404$	$\|q\| = 549$	$\|q\| = 654$	$\|q\| = 720$
192	$\|q\| = 432$	$\|q\| = 581$	$\|q\| = 686$	$\|q\| = 752$
224	$\|q\| = 448$	$\|q\| = 597$	$\|q\| = 702$	$\|q\| = 768$
256	$\|q\| = 468$	$\|q\| = 615$	$\|q\| = 718$	$\|q\| = 783$

Conclusion

This paper extends the study of the existence of randomness extractors for a subgroup G of a finite prime field $\mathbb{Z}_p$ to a field of the form $\mathbb{F}_{p^n}$ where p is a prime and $n > 1$ an integer. The extractor denoted by Ext_k, for a given random element in a subgroup G of $\mathbb{F}_{p^n}$, outputs k-first (resp. k-last) $\mathbb{F}_p$-coefficients of this element. Our extractor works for any finite field $\mathbb{F}_{p^n}$ where the DDH assumption holds. Hence, we show that if q is large we can derive random bit-string. In general, they can be used in any cryptographic protocol which requires to extract a random bit-string from a random group-element.

As in Fouque *et al.* [10] for prime field, the large q is the main drawback here for non prime field because q is grater than $\sqrt{p^n}$. Hence, as further work it will be interesting to improve the bound proposed in this paper.

References

1. 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.
2. D. Boneh. *The decision Diffie-Hellman problem.* In Third Algorithmic Number Theory Symposium (ANTS), vol.1423 of LNCS. Springer, 1998
3. D. Boneh and I. Shparlinski. *On the unpredictability of bits of the elliptic curve Diffie-Hellman scheme.* In J. Kilian, editor, CRYPTO 2001, vol. 2139 of LNCS, pages 201-212. Springer, Aug. 2001.
4. D. Boneh and R. Venkatesan. *Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes.* In N. Koblitz, editor, CRYPTO'96, vol. 1109 of LNCS, pages 129-142. Springer, Aug. 1996.
5. 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.
6. 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
7. 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.
8. W. Diffie, M. Hellman, *New Directions in Cryptography*, IEEE Transactions On Information Theory, vol.22, no.6, 644-654, 1976
9. 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.

10. P. A. Fouque, D. Pointcheval, S. Zimmer. *HMAC is a good randomness extractor and applications to TLS*. In M. Abe and V. D. Gligor, editors, ASIACCS, pages 21-32. ACM, 2008.
11. Y. Dodis, R. Gennaro, J. Håstad, H. Krawczyk, and T. Rabin, *Randomness extraction and key derivation using the CBC, cascade and HMAC modes*. In Matthew K. Franklin, editor, Advances in Cryptology - CRYPTO 2004, volume 3150 of *LNCS*, pages 494-510. Springer 2004
12. R. Genaro, H. Krawczyk, and T. Rabin. *Secure Hashed Diffie-Hellman on non-DDH groups*. In C. Cachin and J. Camenisch, editors, *Eurocrypt 2004*, volume 3027 of *LNCS*, pages 361-381. Springer, May 2004.
13. J. Håstad, 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
14. S. V. Koyagin and I. Shparlinski. *Character Sums With Exponential Functions and Their Applications*. Cambridge University Press, Cambridge, 1999.
15. R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, 1997.
16. R. Shaltiel, *Recent Developments in Explicit Constructions of Extractors*, Bulletin of the EATCS 77 (2002), 67–95; 2002
17. I. Shparlinski. *Bounds of Gauss Sums in Finite Fields*. Proceedings of the American Mathmatical Society, vol 132, pages 2817-2824. AMS 2004.
18. L. Trevisan and S. Vadhan, *Extracting Randomness from Samplable Distributions*, IEEE Symposium on Foundations of Computer Science, 32–42, 2000
19. V. Shoup *A Computational Introduction to Number Theory and Algebra* Cambridge University Press, Cambridge 2005.
20. 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.