# Cryptology ePrint Archive: Report 2011/582

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

*Abdoul Aziz Ciss*

**Abstract:** Many technics for randomness extraction over finite fields was proposed by various authors such as Fouque \emph{et al.} and Carneti \emph{et al.}. At eurocrypt'09, these previous works was improved by Chevalier \emph{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 \emph{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.

**Category / 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

**Date:** received 27 Oct 2011, last revised 5 Jan 2012

**Contact author:** abdoul ciss at ucad edu sn