AN OVERVIEW OF DISCRETE LOG AND TRACE BASED PUBLIC KEY CRYPTOGRAPHY ON FINITE FIELDS

Ersan Akyıldız[1]

[1] *Institute of Applied Mathematics and Department of Mathematics, METU, Ankara, TURKEY*

Abstract

The Discrete Logarithm Problem (DLP), that is computing x, given $y = \alpha^x$ and $(\alpha) = G \subset \mathbb{F}_q^*$, based Public Key Cryptosystem (PKC) have been studied since the late 1970s. Such development of PKC was possible because of the trapdoor function $f : \mathbb{Z}_l \to G = (\alpha) \subset \mathbb{F}_q^*$, $f(m) = \alpha^m$ is a group homomorphism. Due to this fact we have: Diffie Hellman (DH) type key exchange, ElGamal type message encryption, and Nyberg-Rueppel type digital signature protocols. The cryptosystems based on the trapdoor $f(m) = \alpha^m$ are well understood and complete. However, there is another trapdoor function $f : \mathbb{Z}_l \to G$, $f(m) \to Tr(\alpha^m)$, where $G = (\alpha) \subset \mathbb{F}_{q^k}^*$, $k \geq 2$, which needs more atention from researchers from a cryptographic protocols point of view. In the above mentioned case, although f is computable, it is not clear how to produce protocols such as Difie Hellman type key exchange, ElGamal type message encryption, and Nyberg-Rueppel type digital signature algorithm, in general. It would be better, of course if we can find a more efficient algorithm than repeated squaring and trace to compute $f(m) = Tr(\alpha^m)$ together with these protocols. In the literature we see some works for a more efficient algorithm to compute $f(m) = Tr(\alpha^m)$ and not wondering about the protocols. We also see some works dealing with an efficient algorithm to compute $Tr(\alpha^m)$ as well as discussing the cryptographic protocols. In this review paper, we are going to discuss the state of art on the subject.

[1]ersan@metu.edu.tr