A post quantum (n, n)-threshold secret sharing scheme using AD cryptosystem

Mahdi Ashrafi Bafghi[*]
Islamic Azad University, Bafgh Branch

Ali Nakhaei Amroudi
Malek Ashtar University of Technology

Abstract

The existing secret sharing schemes either require integer numbers or require DLP (Discrete Logarithm Problem) for verification. In addition, they use secure channel for transmission of secret. In this paper we present a (n, n)-threshold secret sharing scheme using AD cryptosystem through insecure channel in which the floating numbers can be used. The proposed scheme doesn't need DLP for verification. In addition, it is secure against quantum algorithms.

Keywords: Secret Sharing Scheme, Ajtai and Dwork (AD) Cryptosystem, Lattice, Post Quantum Cryptography.
Mathematics Subject Classification [2010]: 94A62, 94A62

1 Introduction

Secret sharing scheme (SSS) is a cryptographic primitive that allows a secret to be shared among a set of participants such that only a qualified subset (or even the whole set) can recover the secret [6]. SSSs are ideal for sensitive and highly important systems such as encryption keys, missile launch codes, numbered bank accounts access control systems, e-voting, authentication protocols and etc [6]. Classical constructions for (k,n)-threshold secret-sharing schemes include the polynomial based Shamir scheme [1], the nonparallel hyper planes-based Blakley scheme [5] and the integer-based Chinese remainder Theorem (CRT) scheme [2]. In fact Blakley and Shamir invented threshold sharing schemes independently [1, 5]. However, the existing schemes either use DLP for verification of secret or require a secure channel for secret transmission. In 1994, Shor discovered a quantum algorithm for solution of DLP [7]. Therefore, SSSs, which use DLP, are not resistant against quantum attacks.

Lattice-based cryptosystems are resistant against quantum attacks. Steinfeld et al. has introduced Lattice-based threshold-changeability for standard Shamir secret-sharing schemes in [8]. They proved the security of their works by lattice reduction techniques but their schemes require secure channel for secret transmission.

The Ajtai and Dwork (AD) cryptosystem is one of the post-quantum cryptosystems [4]. Post-quantum means that they are resistant against quantum attacks. In this paper, we propose a (n,n)-threshold SSS based on the AD cryptosystem. Ajtai and Dwork uses hard

[*] Speaker