Journal of Systems Science and Complexity
24(1): 186-194

A PAIRING-BASED PUBLICLY VERIFIABLE SECRET SHARING SCHEME

Wu, Tsu-Yang; Tseng, Yuh-Min

Abstract

A publicly verifiable secret sharing (PVSS) scheme is a verifiable secret sharing scheme with the special property that anyone is able to verify the shares whether they are correctly distributed by a dealer. PVSS plays an important role in many applications such as electronic voting, payment systems with revocable anonymity, and key escrow. Up to now, all PVSS schemes are based on the traditional public-key systems. Recently, the pairing-based cryptography has received much attention from cryptographic researchers. Many pairing-based schemes and protocols have been proposed. However, no PVSS scheme using bilinear pairings is proposed. This paper presents the first pairing-based PVSS scheme. In the random oracle model and under the bilinear Diffie-Hellman assumption, the authors prove that the proposed scheme is a secure PVSS scheme.

Key words：Bilinear pairing; Cryptography; Random oracle model; Secret sharing