

A new arbitrated signing scheme based on BFHP

ABSTRACT

Digital signing is commonly used in any electronic authentication. It preserves data integrity while maintaining non-repudiation value for signer and verifier involved. As digital world strives towards paperless operation, a derivative of digital signing known as arbitrated digital signing fills the need to use a trusted third party (TTP) to monitor the signing and verification process. In this paper, a new arbitrated digital signing scheme based on Bivariate Function Hard Problem (BFHP) is discussed.

Keyword: Bivariate function hard problem; Digital signing scheme