conferenceseries.com

World Congress on QUANTUM PHYSICS

September 27-28, 2023 | Webinar

Rank AGS identification scheme and signature scheme

Vaishnavi Nagaraja
Rank AGS Identification Scheme and Signature Scheme, Malaysia

The identification protocol is a type of zero-knowledge proof. One party (the prover) needs to prove his identity to another party (the verifier) without revealing the secret key to the verifier. One can apply the Fiat–Shamir transformation to convert an identification scheme into a signature scheme which can be used for achieving security purposes and cryptographic purposes, especially for authentication. In this paper, we recall an identification protocol, namely the RankID scheme, and show that the scheme is incorrect and insecure. Then, we proposed a more natural approach to construct the rank version of the AGS identification protocol and show that our construction overcomes the security flaws in the RankID scheme. Our proposal achieves better results when comparing the public key size, secret key size, and signature size with the existing identification schemes, such as Rank RVDC and Rank CVE schemes. Our proposal also achieves 90%, 50%, and 96% reduction for the signature size, secret key size, and public key size when compared to the Rank CVE signature scheme.

Biography

Vaishnavi Nagaraja currently is a current third-semester PhD student at UPM, Malaysia. This is her first paper which has been published in MDPI. Her expertise is mathematical cryptography which focuses on code-based cryptography.