Publications Mathematicae Debrecen | **Year: 2022** | **Vol.: 100** | **Fasc.: Suppl.**

Title: Provably secure identity-based remote password registration

Author(s): Csanád Bertók, Andrea Huszti, Szabolcs Kovács and Norbert Oláh

One of the most significant challenges is the secure user authentication. If it becomes breached, confidentiality and integrity of the data or services may be compromised. The most widespread solution for entity authentication is the passwordbased scheme. It is easy to use and deploy. During password registration typically users create or activate their account along with their password through their verification email, and service providers are authenticated based on their Secure Sockets Layer / Transport Layer Security (SSL/TLS) certificate. We propose a certificate-less secure blind registration protocol (CLS-BPR) which is a password registration scheme based on identity-based cryptography, i.e., both the user and the service provider are authenticated by their short-lived identity-based secret key. For secure storage a bilinear map with a salt is applied, therefore in case of an offline attack the adversary is forced to calculate a computationally expensive bilinear map for each password candidate and salt that slows down the attack. New adversarial model with new secure password registration scheme are introduced. We show that the proposed protocol is based on the assumptions that solving the Bilinear Diffie–Hellman problem is computationally infeasible, the bilinear map is a one-way function, Mac is existentially unforgeable under an adaptive chosen-message attack, where the bilinear map is considered in the generic bilinear group model and the hash functions are supposed as random oracles.