Publicationes Mathematicae Debrecen **Year: 2022** **Vol.: 100** **Fasc.: Suppl.**

Title: A provable M-of-N signature scheme based on the BDHI-type assumption in the random oracle model

Author(s): Mariusz Jurkiewicz

We describe a new group-based M-of-N multisignature scheme (i.e., a protocol which allows a group of signers to produce joint signature on a common message), based on an asymmetric pairing of Type 3. The idea of the scheme is such that there are arbitrary number of signing parties with independent keys that sign the same message. Unlike the regular digital signature schemes, the signing algorithm is split into two separated stages, namely making pre-signatures and generating final aggregate signature. The security analysis is conducted in the `euf-cma` model, where the security of the scheme is reduced to the computational hardness of solving the bilinear Diffie– Hellman inversion problem. The reduction is made in the random oracle model.