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

Title: Using GeMSS128 in a ring signature scheme

Author(s): Viliam Hromada and Daniela Leščinská

In this paper, we investigate the possibility of using the multivariate GeMSS signature scheme as the building block of a ring signature scheme. Namely, we determine a set of parameters which provide 128-bit level of security for different numbers of ring's participants. We also provide performance measurements and compare this ring signature scheme with a similar one which uses the Rainbow signature scheme as its building block instead.