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

Title: Application of Velusqrt algorithm to Huff's curves

Author(s): Michał Wroński

In 2020 Bernstein, De Feo, Leroux, and Smith presented a new odd-degree ℓ-isogeny computation method called Velusqrt. This method has complexity $\tilde{O}(\sqrt{\ell})$, compared to the complexity of $\tilde{O}(\ell)$ of the classical Vélu method. In this paper, the application of the Velusqrt method to Huff's curves is presented. It is shown how to compute odd-degree isogeny on Huff's curves using the Velusqrt algorithm and x-line arithmetic for different compression functions, especially for degree 4 compression function $f_{4,x^2} = x^2$.