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

Title: Arithmetic on generalized Hessian curves using compression function and its applications to the isogeny-based cryptography

Author(s): Michał Wroński and Tomasz Kijko

In this paper, we present formulas for differential addition and doubling using the compression function $f_{GH,2}(P) = x_P + y_P$ of degree 2 on a generalized Hessian curve $E_{GH} : x^3 + y^3 + a = dxy$, where $P = (x_P, y_P)$. We use in this context elementary algebra methods. Moreover, we also present formulas for 2, 3-isogeny, and general ℓ-isogeny evaluation, using this function. It is worth noting that for the compression function $f_{GH,2}$, such formulas have not been presented before. On the other hand, we also use elementary algebra methods for obtaining differential addition and doubling formulas using the compression function $f_{GH,6}(P) = x_P y_P$ of degree 6, and we present formulas for 2 and general ℓ-isogeny evaluation using this function.