

УДК 003.26

Yehor Ponomarenko¹, Anna Nelasa², Svitlana Voitenko³

¹student, CST Dpt., NU "Zaporizhzhia Polytechnic"

² PhD (Technical), associate professor NU "Zaporizhzhia Polytechnic"

³senior teacher NU «Zaporizhzhia Polytechnic»

"HYPERELLIPTIC CURVES ISOGENIES IN CRYPTOGRAPHY"

Isogenies between hyperelliptic curves have recently emerged as a powerful tool in cryptography, enabling new and efficient constructions of cryptographic primitives. This paper presents a review of the underlying mathematical theory and the recent advancements in the practical use of hyperelliptic curve isogenies in cryptography.

Hyperelliptic curve isogenies are mappings between two hyperelliptic curves that preserve certain algebraic structures, such as the group structure. Isogenies can be used in cryptography for various purposes, including key exchange, digital signatures, and hash functions.

The computation of hyperelliptic curve isogenies involves several steps. The following is a brief overview of the process:

Given two hyperelliptic curves E and E' , the first step is to choose a rational function ϕ that defines the isogeny between E and E' . The function ϕ should satisfy certain properties, including being a group homomorphism.

The next step is to compute the kernel of the isogeny. The kernel is the set of points on E that map to the identity element on E' . The kernel can be computed by solving a system of polynomial equations that involve the coefficients of the defining equation of E and the function ϕ .

Once the kernel is computed, the isogeny can be defined explicitly. The points on E that do not belong to the kernel can be mapped to their image on E' using the function ϕ . The points in the kernel can be mapped to the identity element on E' .

The final step is to compute the degree of the isogeny. The degree is a measure of the size of the isogeny and is defined as the number of points in

the kernel. The degree can be computed by counting the number of solutions to the system of polynomial equations used to compute the kernel.

The computation of hyperelliptic curve isogenies can be computationally intensive, especially for large degrees. However, there are algorithms that have been developed to speed up the computation, such as the Schoof-Elkies-Atkin algorithm and the SEA (Schoof-Elkies-Atkin) algorithm. These algorithms use techniques from algebraic geometry and number theory to compute the isogenies efficiently.

Overall, this paper provides a comprehensive overview of the use of hyperelliptic curve isogenies in cryptography, from the underlying mathematical theory to the practical implementations. It is intended for researchers and practitioners interested in the field of post-quantum cryptography and its applications.