Quantum exponentiation and (twisted) Fibonacci numbers

Medhi Kermaoui*[1]

[1]Cryptology, arithmetic : algebraic methods for better algorithms – Centre Inria de l'Université de Lorraine, Department of Algorithms, Computation, Image and Geometry – France

Résumé

From Shor's algorithm to the computation of isogenies in CSIDH, exponentiation is an extensively used operation in quantum cryptanalysis. Since it is a costly operation, improving its efficiency is crucial. While it has been well studied in the classical case, quantum exponentiation has received less scrutinity. On the one hand, we can adapt classical algorithms, such as Square and Multiply, in the quantum setting, providing "time"-efficient algorithms, but at the cost of a memory
that scales linearly in the exponent. On the other hand, quantum exponentiation can be performed efficiently in mem-
ory, using 0(1) registers, but with worse performance.
This work provides a versatile quantum exponentiation algorithm, which performs well at any memory size, closing
the gap between the previous methods.
Joint work with Xavier Bonnetain and Pierrick Gaudry

*Intervenant