Periodic sequences in design criteria of post-quantum cryptoschemes on algebras

N.A. Moldovyan

Abstract

Two design criteria of the post-quantum signature schemes are considered, which take into account properties of the periodic functions defined on the base of the public parameters of the cryptoschems. The used computationally difficult problem represents so called hidden discrete logarithm problem that is connected with using exponentiation operation in a hidden cyclic group of prime order q. The first criterion relates to the known candidates for post-quantum signature schemes based on the hidden logarithm problem and is formulated as practical intractibility of the task of composing a periodic function taking on the values in frame of a fixed finite cyclic group, which contains a reriod depending on the value of a discrete logarithm x. However, this criterion does not contradict the development of cryptosystems that allow the construction of periodic functions containing a period of length x, if the values of these functions lie in a sufficiently large number of different groups.

In the second advanced criterion of post-quantum security the period length is fixed to the value q, therefore the potentially possible future quantum algorithms for finding the period length of the periodic functions in finite algebras will not breake the signature scheme. Algebraic supports of the post-quantum public-key cryptoschemes based on the hidden logarithm problem, the technique of implementing the above two criteria and signature schemes based on them are presented.

N. A. Moldovyan

Saint Petersburg Electrotechnical University "LETI"
ul. Professora Popova 5, 197376 St. Petersburg, Russian Federation
E–mail: nmold@mail.ru