In 2016 NIST announced a start of a process of development and standardization of a post-quantum public-key encryption scheme. *Mersenne-756839* was one of the proposals. This proposal is described in this thesis, as well as the known attacks against it. The description and the theoretical background behind these attacks are presented in a rigorous way and are accessible to the reader without any previous knowledge about the post-quantum cryptography. New additional ideas for the implementation of the attacks are also presented. Finally, these attacks are implemented and attached to the thesis.