Re-implementation of the Picnic-signaturescheme in Python

Thorsten Knoll

info@thorstenknoll.de

March, 2019

I. Introduction

Post-quantum cryptography, NIST and Picnic

Quantum computers are experiencing fast development and seem to be available within a timeframe of the next few decades. One of their properties will be to break huge parts of modern cryptography. Especially the discrete logarithm and prime-factorisation loose their trapdoor funcionality in regards to the efficient quantum algorithms from Grover and Shor. Therefore the need for new cryptographic algorithms arises, beeing save in regards to the availability of quantum computers. This field of research goes with the name "Post-quantum cryptography" (PQC). The american National Institute of Standards and Technology (NIST) called out a challenge to find the next PQC standards. This challenge is in round two of three at the time of writing this document. 69 submissions from round one were reduced to 26 candidates in round two of the challenge. These 26 candidates got announced by NIST not long ago at the end of january 2019. One of the submissions surviving the first round is the Picnic signaturescheme.

Evaluation and categorization

Learning PQC

Figure 1: Dummy PDF

II. LowMC

III. Picnic

References

[1] Microsoft *Picnic PQC Signatureschene*. 2018