Lattice-based post-quantum cryptography compared to conventional cryptography methods

Master-Thesis

Author:

Indrajitsinh Slonaki

Course of Study:

Information and Electrical Engineering

Submitted on:

01.09.2022

Supervisors:

Prof. Dr.-Ing.Habil. Andreas Ahrens

Dipl. -Ing Mr. Uwe Starke

The main objective of this thesis is to compare classical cryptography with lattice-based cryptography through practical observation. The thesis required the formulation of strong arguments as to why conventional cryptography should be replaced with lattice-based cryptography.

Challenges to classical cryptography

The cryptography methods in use today are robust enough that classical computers are not able to break them. It would take the classical computer years to do so.

The strength of old cryptography methods will be put to the test with the rise of quantum computers. These computers are capable of breaking today‘s methods with remarkable speed.

Results

To break any algorithm, certain attacks are required. A computer‘s ability to break an algorithm also depends on the speed of the computer. Therefore, it is a matter of how many operations can be run by a computer and how many possible operations are needed to break the algorithm. Running DES on the classical computer gives 3089150.33 in one second and the 56-bit key size has 2^{56}= 7.2057594e+16 keys. The formula is key size/operation per second:

$$\frac{2^{56}}{3089150.33} = 23326023773.6$$

result in years is 740 years.
Table 1 shows the total time required to break RSA and AES algorithms with classical computers as well with Quantum computers.

Algorithm	Classical Computer	Quantum Computer
RSA	3×10^{14} years	8 hours
AES	1.0×10^{24} years	6 months

Table 1. Break time of AES and RSA

Comparison

The development of Quantum computers is growing rapidly. Quantum computers will likely be put on the market by 2023 to 2025.

Lattice-based cryptography is considered very fast and quantum-safe. The hardness of Lattice-based cryptography is based on the selected bases in the lattice field instead of Factoring or discrete logarithm problems. Quantum computers are fast enough to solve this problem, but until now there is no algorithm that has been developed to break lattice-based algorithm using Quantum computers.

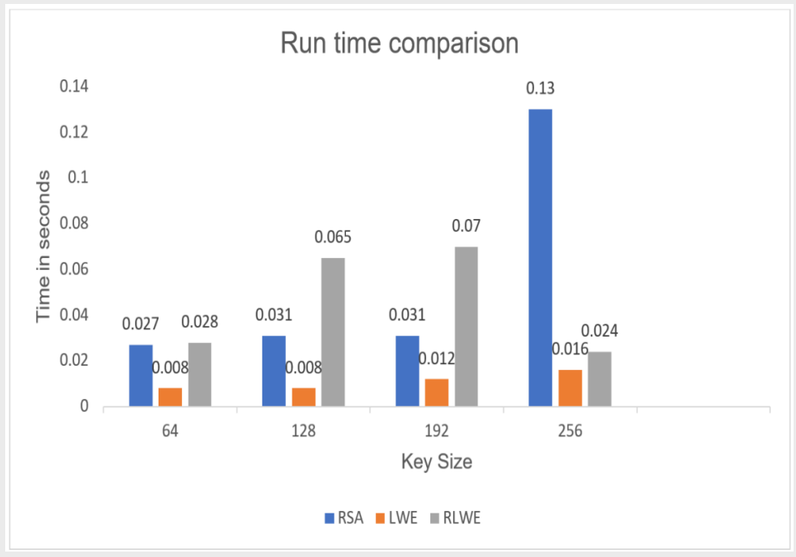

Figure 2. speed comparison

On a classical computer, I used different algorithms at different key sizes and measured the run time so I may compare them to each other.

As per the result stated in figure 2, Lattice based cryptography is faster than asymmetric cryptography.

Lattice-based cryptography is the best alternative against a quantum computer.

Fakultät für Ingenieurwissenschaften
Bereich Elektrotechnik und Informatik

www.fiw.hs-wismar.de