Post Quantum Cryptography

Students

Isaac Würth

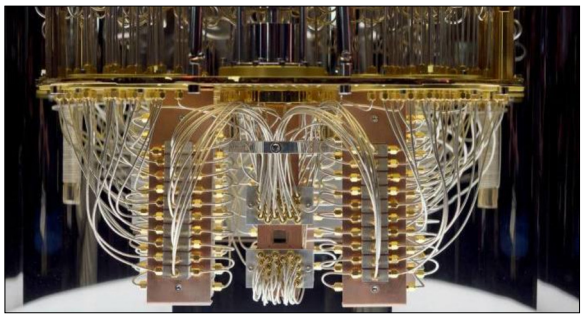
Marco Zanetti

Definition of Task: Quantum computers are becoming a reality in the industrial sector. With the quantum cloud from IBM putting quantum computing resources within reach of everyone with an internet connection. The computing power of these machines is starting to surpass their conventional counterparts and they are opening up new opportunities for solving problems unfeasible on traditional computers like the quick calculation of incredibly hard mathematical equations. One of these mathematical problems, of which they can reduce the calculating time, is the so called factorization problem. The issue with this is, the impossibility to efficiently factorize large numbers on conventional computers has been the foundation of modern cryptographic algorithms like RSA and ECC.

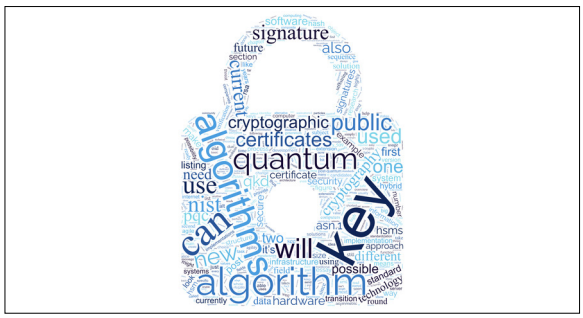
Objective: The goal of this essay is to provide an overview over what is currently being done to prepare the IT infrastructure for the coming quantum threat. This is done by showcasing the most pressing issues of post quantum cryptography and some relating topics. We show how the issue of broken cryptography is being handled at the moment, and which technologies can help to increase the security with the advent of efficient quantum computers.

Result: During the writing and research of this thesis, we were able to show that quantum computers are taking shape, and already have surpassed their conventional counterparts in certain use cases. The standardization process of the algorithms, lead by NIST is coming towards an end in early 2022, they aim to release a rough draft in the first half of next year. Furthermore, the standardization procedure will continue, yielding quantum safe algorithms. But the change of one cryptographic algorithm to another cannot be performed without adequate tools and preparation. This is where we show how the idea of hybrid certificates can help to tie us over this period of change. It enables us to use old and new algorithms side by side until the infrastructure as been adapted to the new algorithms, phasing out the deprecated ones. As we can see, the cryptographic landscape is about to change, and the chances are high that it will be more fluid in the future.
Our recommendation, for companies of any scale, is to start cataloguing their infrastructure. It is crucial to know your assets and have a clear understanding of ones own architecture. Be this physical assets, software or the used cyphers. Only then, you will be able to prepare for the transition to a post quantum cryptography architecture. While the transition does not need to start immediately, it is advisable to keep a close eye on releases by NIST. Once standards and guidelines have been published, which should happen in a timely manner, it will be important to evaluate possible solutions and to start planning the future transition to post quantum cryptography. It is thus crucial to create a tailored solution for every company. Our essay gives solutions applicable to different use cases.

An IBM quantum computer
https://csferrie.medium.com



Wordcloud
Own presentment



A hybrid and composite certificate
Own presentment

Examiner
Prof. Dr. Nathalie Weiler

Subject Area
Security

Project Partner
Credit Suisse, Zürich, ZH