Towards Solving the Post-Quantum Computing Challenge

Frank W. Holliday, on the 16th of November 2017

Post-quantum computing era comes nearby. The question is not if, the real question is when reliable quantum computing will be reality. My assessment is on this real question: Just in a few years. This disruptive technology will vanish all of our current established asymmetric cryptographic standards in a sudden. But where is the Marshall's plan to prevent this scenario and will be mastering this challenge? Why we should take this challenge seriously?

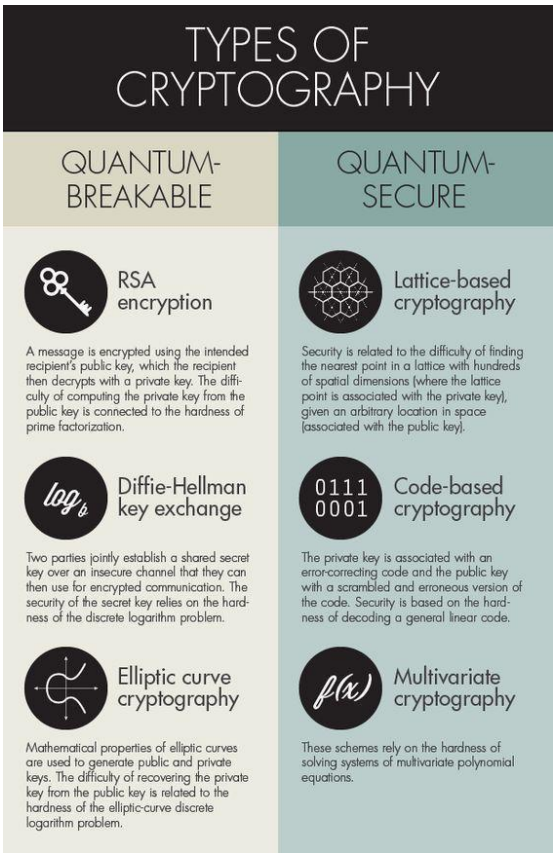
Well, just keep in mind for instance the ip4 to ip6 transition is now lasting over two decades.
I doubt that we can spend this patience for the post-quantum computing challenge.

If non-democratic nations like China will win this race first (China might already possesses sufficient working quantum computing), we (the democratic nations) shall have some big problems keeping our vital secrets sustainably secure. And this is the real political implication we are faced to.

Therefore here are my thoughts towards a solution for this challenge.

First of all we have to **stop** with **the myth no. 1**:
Only quantum cryptography will be suitable in the post-quantum computing era.

That isn't true. A lot of cryptographic schemes for encryption can be constructed, on which even quantum computers (QC) need thousands of years for decryption. This kind of encryption schemes are called to be quantum computing resistant (QCR) or quantum computing secure (QCS). Therefore we don't need to change to quantum based cryptography necessarily to face this challenge. This nice infographic posted by Chuck Brooks at LinkedIn let us see the challenge right:



Secondly we have to **stop** with **myth no. 2**:
We have a long time till quantum computing is ready.

That isn't true either. Just keep in mind that all the internet traffic which is encrypted by the common currently asymmetric crypto standards can be recorded and will be decrypted with less effort when quantum computing is ready (possibly just in a few years and that is an optimistic assessment, the pessimistic assessment is one nation has already sufficient QC working). As far as the current perception about quantum computing resistance shows the symmetric cryptographic standards are QCR which are based on pure sufficiently enriched algorithmic construction like AES-256 and upwards. What means even QC cannot decrypt these kinds of encryption on brute-force base within a realistic time period. But if you think a Perfect Forward Secrecy (PFS) appliance for encrypted internet traffic does protect against the recording threat is unfortunately negative. Cause the current standardized key exchange protocols (needed to compute on both sides the never in the case of PFS over the communication channel exchanged symmetric encryption key) currently all utilize non-QCR asymmetric cryptography.

Thirdly we have to **stop** with **myth no. 3**:
There is no feasible master plan to take this challenge.

Well, what can we do about the worst-case InfoSec scenario of vanished crypto standards accomplished by the disruptive technology QC?

To find an answer for the myth no. 3 I had the luck to read a white paper of the German Institute Fraunhofer SIT located in Darmstadt (Germany). Really I appreciate these people there. In my opinion they are one of the best open-minded, pragmatic cryptologists of the world. So have a look to their white paper at:
https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Practical.PostQuantum.Cryptography_WP_FraunhoferSIT.pdf?_=1503992279

In this white paper you can find the **answers to all of the above noticed three myths**.

This white paper points out nothing else then a **feasible master plan** to cope the challenge as follows:

Step 1: In a fast-track operation we have to establish one or two of the QC resistant key exchange schemes described there as additional cryptographic key exchange standards. Even when the new standardized schemes will turn out later on to be weak according further research we are used to the transition and can supply stronger schemes then. If we don't react fast the whole recorded internet traffic till the transition will be accomplished is at risk to be compromised with less effort by QC.

Step 2: Manufactures have to provide implementations of the new standards as soon as possible to the market.

Step 3: Applicators have to utilize these new standards in combination with the PFS appliance to ensure further internet traffic which is now QCR.

Step 4: Deprecate after a transitional period of one decade all the key exchange protocols which are not QCR.

But this is **not the whole story** of what has to be started urgently. The same procedure needs to be done for all the current **public-key signature** and **public-key encryption** standards, which are based on trivial prime factors or discrete logarithm or certain geometric items of elliptic curves puzzles. In consequence our whole current **certificate standardization (X.509)** is involved based on those puzzles and it **needs to be redesigned and to be re-standardized on the base of QCR cryptographic schemes!**

Yes, indeed, there is a lot to do and we have to start urgently and we have to hurry up for a completion in time.

By the way blockchainers:

It is also a tough challenge for all the blockchains currently set into the wilderness of the cyberspace, too.

This includes especially the current implemented approaches of digital money. They all necessarily need to be designed on QCR base to keep some kind of sustainability.

What reveals the real disadvantage in the kind of those digital objects (besides the lot of energy wasting mining and checking the chain of trust) without Breaking the Chain of Trust: There is no mercy to those kind of digital objects, which are massively spread into the wilderness of the cyberspace possessing critical design flaws.

I will be discussing the implications of the blockchain concept in my next article of the Think Food Series.

About the Author

Frank W. Holliday, CISSP & ISO/IEC 27001 Lead Auditor, has over 15 years of information security, IT audit and compliance experience. He is an IT veteran covering over 35 years of experience on a diversity of IT work fields like embedded systems programing, software product development, system administration, software quality management and finally has found his particular interest in information security. He holds a German master degree in communications engineering and is a member of the German Association of Computer Science (Gesellschaft für Informatik e.V./ GI) and is attached to the GI's workgroup SECMGT (Information Security Management). He also is taking part in the task force ISM of the German registered association TeleTrusT.