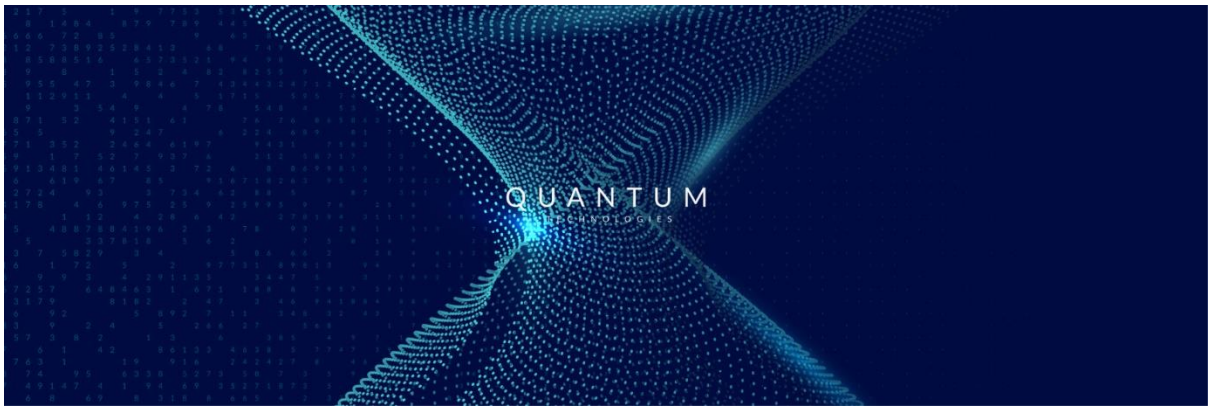
Cryptography Specialists – The Key to a Secure Post-Quantum World

Written by Joshua Bucheli, Researcher und Editor in cooperation with Xenia Bogolomec, Information Security Specialist and CEO of Quant-X Security and Coding, and Peter Kosel, Founder of cyberunity



'Cybersecurity' and 'cryptography' may sound like 21st century tech jargon, but data privacy and encryption are by no means modern inventions.

From the ancient Mesopotamian craftsman who encrypted his recipe for pottery glaze to protect it from competitors to the 20th Century wartime Enigma rotor machine – using ciphers to obscure information from prying eyes (cryptography) is nothing new. Just as ancient is the pastime of trying to 'crack' or 'de-cipher' these codes.

The 21st century has seen this cat and mouse game progress in complexity, and just like Tom and Jerry, both sides have always remained more or less evenly matched. However, as quantum computers begin introducing unprecedented processing power, the game is set to change.

The advent of quantum computers is set to usher in new threats to cybersecurity and new opportunities for job seekers in the field of cryptography.

Whether the entire cybersecurity industry is revolutionised or compromised by the quantum age is a matter of whether or not the right specialists step up in time to help the industry transition to post-quantum encryption.

Post-Quantum Cryptography: A New Age of Cybersecurity

The unmatched computing power of quantum processors will eventually allow computers to crack even the strongest conventional asymmetric encryptions in a matter of minutes, rendering the basis of most cybersecurity systems obsolete, and ushering in the age of 'Post-Quantum Cryptography'.

The following video provides a crash course for those who are interested in delving into the details of how quantum computers break encryptions.

What is important to understand though, is the urgency of this issue. According to Xenia Bogolomec, Information Security Specialist and CEO of Quant-X Security and Coding GmbH:

"If companies want to ensure the future confidentiality of the data they currently send over the internet, then Post-Quantum-Cryptography is a key issue. It will also be crucial when it comes to NFC verifications and electronic passports where private keys are linked to encrypted signatures. These will all need to be made anew when quantum computers enter the stage."

According to experts like Peter Shor and estimates from IBM, quantum-computing related cybersecurity incidents are likely no more than three or four years away.

This post-quantum paradigm shift in computing power will have dramatic impacts on digital integrity. From national security and electronic IDs to intellectual property and High-Tech IT firms, everything and everyone will have to adapt.

As a result, Post-Quantum-Cryptography specialists who can help shape the future of cybersecurity in a post-quantum age are absolutely essential.

Major Developments and Employers in the Field of Post-Quantum-Cryptography

One of the most anticipated developments in the field is NIST's ongoing evaluation of 'quantum-proof' cryptographic methods.

"If this NIST standard comes into force then we are on the right track to securing systems in time for the arrival of quantum computers", says Xenia.

However, regulatory standards are only part of the solution. It will also take 'boots on the ground' in the field of algorithmics, crypto-engineering, and crypto-consulting to help prepare the world for the impending shift towards post-quantum-cryptography.

Individuals interested in such positions would do well to begin their job search by looking to industry leaders in processor development such as Intel, CISCO, AWS, Infineon, IBM, Google, and Microsoft.

Government intelligence agencies are also on the lookout for cryptographers, as evidenced by the BND's recent recruitment campaign, #followtheglitchkarnickel, which is well worth a watch.

Furthermore, organisations like PQ Shield and Almacrypt, and companies like Cybersec Innovation Partners (for those interested in specializing in public-key infrastructure) are ideal places for motivated individuals to find opportunities.

Xenia also invites anyone interested in building a career at the forefront of cybersecurity's nascent post-quantum frontier to apply for positions and projects at her company, Quant-X Security & Coding, as and when they become available.

What Hard Skills Should Post-Quantum-Cryptography Specialists Bring to the Table?

It goes without saying that a general familiarity with cybersecurity concepts is a prerequisite for a career in post-quantum-cryptography. But there are certain skillsets that will set aspiring cryptographers apart from the competition.

For Xenia, the case is clear: when it comes to **algorithmics** the industry needs people with the combined skillset of a computer scientist and a mathematician. "Individuals who are able to apply theoretical principles from these disciplines to machines in practice and implement algorithms in programs are in especially high demand."

For those interested in **crypto-engineering** positions, the ability to implement cryptographic solutions, especially in terms of Identity and Access-Management is essential.

"A crypto-engineer doesn't necessarily need to know how a discrete logarithm is implemented algorithmically. But he or she must know what a public-, private-, and session-key is, which contexts call for which key-lengths, and how a true random value is generated" says Xenia.

Above all, employers want to see that applicants have a good understanding of the foundations of cryptography and that they have the knowledge and skills necessary to help defend against timing- or side-channel attacks.

In addition to these skills, aspiring **crypto-consultants** should also demonstrate the ability to set up, coordinate, and oversee efficient and effective processes of System-Integration.

Advantageous Qualifications and Experience:

University degrees and professional certificates in mathematics, computer science, programming, or engineering lay a good foundation for a career in post-quantum-cryptography.

However, it's practical experience, not certificates or degrees, that will be the deciding factor for candidates, says Xenia.

For positions in **algorithmics,** employers will be looking for individuals who are able to exercise effective quality-control of algorithms. Evidence of strong analytical skills, an ability to collaborate regularly with others, and a demonstrable passion for all things 'crypto' are key.

Attending Post-Quantum-Cryptography Conferences and engaging actively with the community is a great way to gain such experience and demonstrate to employers that one is passionate about cryptography.

People coming from network-centric IT fields who have experience with Multi-Factor-Authentication or building VPN-Modules – Network and Firewall Engineers, Identity-Access-Platform Engineers, or Open VPN Programmers – will stand out for **crypto-engineer** positions.

Something that is still often overlooked is the fact that individuals with experience in **change management** will also be integral to facilitating the transition of systems from conventional to post-quantum encryption.

While knowledge of cryptography is a plus, what is really important for these individuals is that they have experience in **procedural certificate management** and the standard operating procedures of **IT**

migration. They must be able to identify and replace certificates in existing structures and systems, ensuring that they are kept up to date.

Personality (Beyond Technical Know-How):

In terms of personality, different roles will require different interpersonal skills. For example, algorithm-developers will need to be able to work in smaller teams of highly specialized experts.

Crypto-engineers, consultants, and change managers, on the other hand, will be required to interact regularly with a wider range of teams, and will therefore need to exhibit stronger integrative skills.

The way Xenia sees it, "Overall, post-quantum-cryptography is still a highly intellectual field. The selection process focuses more on technical expertise than on personality - at least as far as algorithm-developers are concerned. If we're talking about change managers with IT migration experience, then here, as in many other professions, interpersonal skills are much more of a deciding factor."

In general, those seeking a career in post-quantum-cryptography, whether in algorithmics or in change management, would be well served to emphasize their critical and analytical skills, their patience, and a general passion for tackling complex problems on a daily basis.

After all, guiding humanity into a post-quantum world of cybersecurity is no small feat, and as Peter Kosel, Founder and Talent Community Manager at cyberunity, points out:

"It's vitally important that employers reach out to and get to know the right individuals in time. Waiting for an urgent need to arise before contacting first-rate specialists is like waiting for financial trouble before reaching out to potential customers. It might work, but it is by no means advisable".