Meet PQShield, creating quantum-secure cryptography to protect from quantum attacks

As part of our quick fire questions series – or QFQs – we spoke to Dr Ali El Kaafarani, CEO of PQShield about cutting-edge cryptographic technologies, quantum attacks and the art of explaining the quantum threat to non-technical leaders.

Temps de lecture : minute

---

20 December 2022

Quantum computing poses a once-in-a-generation threat to information security. That's because, with exponentially higher processing power than today's most powerful computers, quantum machines will be able to smash through the public-key encryption methods used to protect almost all sensitive data today. We co-designed the new NIST standards for public-key cryptography that will be used for decades to come to provide protection for all sensitive data.

Tell me about the business - what it is, what it aims to achieve, who you work with, how you reach customers and so on?

PQShield is creating cutting-edge cryptographic technologies to power the security layer of the world's leading organisations, bridging the gap between academic theory and commercial practice.

Our team has collectively spent decades developing the research, designing the solutions and setting the cryptography standards for the

coming quantum era. Our researchers and advisory board contributed to all of the first international PQC NIST standards announced in July 2022.

Team PQShield have also led multiple projects for RISC-V (e.g. TRNG, AES-ISE, etc.) and contributed to the Internet Engineering Task Force (IETF), GlobalPlatform and World Economic Forum (WEF) to name but a few.

PQShield's products include solutions for hardware, software, and protocols. They're amongst the world's most comprehensive quantum-ready solutions, and are already being used by industry leaders like Microchip and Raytheon, amongst others

How has the business evolved since its launch? When was this?

When I realised the devastating impact a quantum attack could have, I knew it was too severe to ignore.

I founded PQShield in 2018 with the support of the University of Oxford's venture arm; Innovate UK; and a world-class roster of academic advisors.

Since then, companies and government bodies have started paying more and more attention to the quantum threat. We've secured funding from top venture capital firms, including Lee Fixel's Addition and our team of leading academics, researchers and engineers continues to grow.

Tell us about the working culture at PQShield?

When you're building a business from scratch, hard work is inevitable and it can be easy to let it dominate your life. That's especially true when you're wrapped up in what you're doing.

Our team is made up of world-class mathematicians and engineers who are all really passionate about their research, and this passion and hard work is key to success, but it's equally important to always have perspective and balance. I have two young children, and I know just how important this is - it's something we encourage across the whole team.

How are you funded?

PQShield has attracted the attention of *leading investors in the US and Europe*.

In July 2020, we emerged from stealth as a spin-out from the University of Oxford's Mathematical Institute with £5.5M in seed funding from Kindred Capital, Crane Venture Partners and Oxford Sciences Enterprise, and Innovate UK. In January 2022, we raised £15.5M in Series A funding led by Addition.

What has been your biggest challenge so far and how have you overcome this?

In the early days, one of our biggest challenges was explaining to non-technical leaders why they should care about the quantum threat. Since a super-powerful quantum computer isn't yet in production, it was difficult for them to understand why the quantum threat should be considered an urgent business priority.

This is where explaining the "harvest now, decrypt later" challenge really made a difference.

Since those early days, we've seen a big shift in mindset. Many more leaders now understand the threat and want to put defences in place today.

The White House, national security agencies and *even the UN* have helped. In recent months, they have all been making noise about the quantum threat and encouraging governments and industry to prepare the way for new encryption standards.

How does PQShield answer an unmet need?

We've developed quantum-secure cryptography that protects devices and sensitive data from quantum attack. Today's encryption cannot do this.

Our cryptographic algorithms are built on complex mathematical problems that are extremely difficult to solve, even for a powerful quantum computer.

What's in store for the future?

Industries that use or manufacture highly-sensitive software or hardware - like defence, semiconductors and financial services - are already responding to the quantum threat.

Many others are likely to follow in future, especially as governments mandate standards based on NIST's recently announced candidates.

Also, our R&D team is breaking ground in cryptography research and we will continue to share our innovations with the wider cryptography community and our customers as well.

What one piece of advice would you give other founders or future founders?

Understand and lean into your customers' pain-points. And when looking for investors, choose one that truly understands both your technology and vision.

And finally, a more personal question! What’s your daily routine and the rules you’re living by at the moment?

I am changing my daily routine to improve my work/life balance, especially post-pandemic, and sports are becoming a bigger part of it!

Dr Ali El Kaafarani, is the CEO of *PQShield* and Oxford Mathematical Institute research fellow.

Article by Dr Ali El Kaafarani