AXA VENTURE PARTNERS

Insights

# AVP Investment thesis CryptoNext Security

December 2023

New York - London - Paris

www.axavp.com

AXA VENTURE PARTNERS

# What is the opportunity behind the post-quantum cryptography market?

Even if the timing is still uncertain (3, 5 or even 10 years), it is absolutely inevitable: quantum computers will be able to break current encryption protocols, enabling malicious actors to gain access to confidential data and not only putting the whole internet at risk, but also threatening many industries and major aspects of the economy. This threat of data leaks is major and has a systemic impact on cybersecurity and concerns all organizations which will have – rather sooner than later – the need to migrate their IT/OT infrastructure to quantum-safe systems. Post-quantum cryptography therefore involves solving more difficult mathematical problems that resist quantum computing.

According to a study from BCG, the time needed to conduct a transition plan before Q-Day – the date on which the quantum computer will break public keys – is getting shorter and shorter. It is estimated that the quantum computer will break current public key protocols by 2030, leaving a window of 3 to 8 years to drive the transition to a quantum-proof infrastructure, during which most organizations will need to evolve their current cryptography to PQC standards.

But, in addition, even if this may not happen before 10 years, what we might perceive as a rather far, somewhat futuristic concern is, in fact, pretty urgent. Organizations (nation-states, criminal organizations, hedge funds) are already starting to collect encrypted data today, especially in critical areas: governments, defense, banks, healthcare and energy companies. This is what is commonly called the "harvest now, decrypt later" risk: cyber attackers could already harvest sensitive data that will be still valid in 3, 5 or 10 years from now to decrypt it later with the power of a quantum computer in their hands. That is super important to understand: some encrypted data have a very short lifetime (bank transaction data for example), but other has a lifetime of several decades (health-related, defense and national security data among others)

So, data must be encrypted in a "quantum computer resistant" way NOW!

Standardization and regulatory activities are essential to drive industry adoption of post-quantum cryptography (PQC). New standard algorithms are currently being defined in the US, with a major milestone achieved in December 2022 with the passage of the Quantum Computing Cybersecurity Preparedness Act. The National Institute of Standards and Technology (NIST) is leading efforts to standardize PQC algorithms by holding competitions to evaluate various new encryption methods. Currently, four algorithms - CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON and SPHINCS+ - have been shortlisted for their resistance to quantum attacks, each excelling in different applications such as securing data in transit, at rest or for authentication purposes. Last August, NIST unveiled the first draft standards and is expected to finalize the draft PQC standards by 2024, with the aim of having the economy fully protected against quantum attacks by 2031.

As a result, some of the world's largest and most influential technology and security companies along with smaller, specialized actors have engaged into different categories of quantum-resistant technology, from cryptographic inventorying to remediation suites. One of those disrupting companies that help organizations achieve this transition towards post-quantum cryptography is CryptoNext Security.

AXA VENTURE PARTNERS

# Why are we excited about investing in CryptoNext Security?

CryptoNext Security was founded in 2019 and is based in Paris. It provides cryptographic protocols, libraries and standards that will make organizations' IT infrastructures resilient against quantum computers. Its solution, CryptoNext Remediation Suite (C-QSR), is an effective, simple and sustainable integrated multi-layer migration solution for applications, data & infrastructure with ultimate PQ security and performance at all levels: algorithms, protocols, tools and applications, with long-term agility and evolution in mind.

As discussed previously, time-to-market is right because the threat "harvest now, decrypt later" needs to be addressed now, and the addressable market is large. But, above all, CryptoNext Security is well positioned and led by an exceptional team, recognized globally for their scientific excellence. The company is a spin-off from INRIA, CNRS and Sorbonne University, based on 20 years of academic research. It is headed by Florent Grosmaître, a graduate of HEC Paris, Arts et Métiers engineer and serial entrepreneur. Florent has extensive experience in international business development, having notably worked as a partner and executive director of healthcare tech company Actibase, which was sold to French market leader Evolucare Technologies after a period of successful restructuring. He supports the company's vision and implements and strategy, inspired by Jean-Charles Faugère, CTO and founder.

Jean-Charles' background is impressive and unique in its kind. With a PhD in Computer Science and a degree from ENS Paris, the "School of Nobel Prices", he is a pioneer in the area of quantum-safe cryptography. In particular, he is recognized by his peers for having developed efficient algorithms and high-performance software for assessing the security of a wide variety of quantum-safe cryptosystems. Before founding CryptoNext Security, Jean-Charles was a research director at INRIA. The expert calls we conducted as part of our due diligence unanimously confirmed Jean-Charles' impressive reputation and worldwide recognition for his expertise in cryptography. Together, and with a team of 8 other FTEs, CryptoNext Security has been able to build a quantum-safe multi-layer remediation suite, addressing multiple use cases and positioning itself as one of the industry's leading players.

Indeed, CryptoNext Security won numerous awards for proven scientific excellence, including being selected in the final round of the NIST competition in the US. What's more, they have successfully led strategic pilots with some of the world's largest public and private organizations. During some of our reference calls, Cryptonext's solution was recognized as the "most fluid hybrid solution on the market with the most comprehensive library of PQ algos", as well as being "easy to use and highly adaptable on both hardware and software". Customers also highlighted the aspect of sovereignty - another very important aspect of Cryptonext's competitive advantages, as one of the only European players most advanced in this specific and niche field, with a rare pool of talent.

With AVP as a significant shareholder, CryptoNext Security will benefit from AVP unique corporate network and AXA, in Europe and the US. We are very confident in CryptoNext Security's ability to establish itself as a leader in its category, and to conquer a global booming multi-billion market thanks to its ambitious and talented team. We are delighted to co-invest in this round with Quantonation, known for its expertise in the quantum computing industry, which was an early investor in the company and confirmed its confidence by co-leading the round with us and Auriga Cyber Ventures. We look forward to participating in the development of cryptographic standards

AXA VENTURE PARTNERS

for enterprises, and to helping them to smoothly transit their information systems towards a quantum-proof (not too distant) future.

We invest in great entrepreneurs.

We support outstanding companies.


New York - London - Paris

www.axavp.com