

CryptoNext Security raises 11M€ to reinforce leadership in Post-Quantum Cryptography Remediation solutions and accelerate international expansion

- CryptoNext Security announces it has today secured 11M€ funding for the industrialization of its Quantum Safe Remediation Solutions and its international expansion. The funding round is led by AVP (AXA Venture Partners) and Quantonation with participation from Auriga Cyber Ventures
- Founded in 2019 after 20 years+ of academic research, CryptoNext Security develops Post Quantum Cryptography software solutions to manage the quantum threat and migrate IT/OT infrastructures to quantum safe.
- CryptoNext Security has pioneered and demonstrated clear leadership in both standardization bodies and achievement of global companies Quantum Safe roadmap partnership projects.

Paris – November, 30th, 2023

CryptoNext Security, pioneering a new era in quantum computer resistant cryptography remediation technology and management solutions, today announces it has raised 11 Million euros funding round, led by AVP (AXA Venture Partners) and Quantonation, with participation from Auriga Cyber Ventures.

CryptoNext Security, founded in 2019 by Jean-Charles Faugère after over 20 years of leadership in post-quantum cryptography academic research and spin-off from Inria, CNRS and Sorbonne University prestigious laboratories, has its headquarters based in Paris, France.

The advent of Quantum Computer opens great opportunities through huge computing capabilities to tackle inaccessible problem solving until now. It also comes with a new major threat for our cybersecurity through its capacity to « break » the public-key cryptosystems that secure today's internet and IT infrastructures as well as IoT and embedded systems communications.

Such quantum threat and its remediation is the rising emergency for today, considering:

- Already existing « Harvest now/Decrypt later » attacks where state or private organizations have started to collect massive amounts of data in order to decrypt them later as soon as a powerful enough quantum computer will be available (impact on long-life sensitive data)
- Migration of technical infrastructures and applications towards quantum resistance full operational capacity typically is counted in years.
- Products life cycle from design to end of operations most frequently exceeds 15-20 years as observed in the Industrial IoT space.

This has led in the US the National Institute for Standards & Technology (NIST) to initiate from 2016, a new competition to define new standards for cryptography able to resist to quantum computer attacks. NIST unveiled on July 2022, the first post-quantum cryptography (PQC) standard algorithms selected and its partner body National Cybersecurity Center of Excellence (NCCoE) launched a "Migration to PQC" initiative with 20 of the most influent companies including CryptoNext Security as a selected member.

The depth and width of the migration challenge on cybersecurity of IT, OT/IoT and Embedded systems defines a new paradigm for crypto-agile remediation and operations management solutions, which CryptoNext has been intensively working on over the last years, with its global customers in multiple vertical markets such as Government, Defense, Finance or Critical Infrastructures as well as technology partners.

These have fostered CryptoNext's vision and products portfolio with the launch of CryptoNext Quantum Safe Remediation Suite (C-QSR). C-QSR is a multi-layer software solution that includes latest releases of newly-defined international, US and European standards, whether at the level of cryptographic algorithms library and cryptographic protocols and objects such as certificates, with embedded configurable crypto-agility and hybridization, as recommended by the security agencies. On top of these, C-QSR brings a comprehensive set of cryptography integration tools and application plugins for network and security infrastructure, secure messaging, IT server, proxies and connectors as well as crypto-agile management.

"With our investors support, we are now well positioned for growth through our innovative products portfolio and global operations expansion" declared Florent Grosmaître, CEO of CryptoNext Security. «Our solutions are currently successfully deployed at global end-users, service providers, equipment manufacturers and software vendors for multiple use cases end-to-end security. We are proud to be a trusted advisor and aim at providing our customer partners with a guarantee of expertise, mastery and timing for post-quantum cybersecurity deployment at controlled costs in this context where time for migration is now critical."

Francois Robinet, Managing partner at AVP (AXA Venture Partners): *"AVP is proud and very excited to support CryptoNext Security in its mission to pioneer quantum-resistant cybersecurity solutions. The threat on encryption protocols arising from quantum computing is huge and therefore the quantum-resistant solutions market is big. Moreover, although the exact timing for the emergence of quantum computers is still uncertain, the market for post quantum cryptography is already there. As digital threats evolve, CryptoNext's innovative approach aligns seamlessly with our commitment to investing in cutting-edge technologies that address critical challenges. We have been very impressed by CryptoNext's team and CryptoNext's leadership and are very happy to support the company in its journey and its potential to reshape the landscape of post-quantum cryptography. We are also very happy to co-invest alongside Quantonation, the market leader in investment in quantum computing technologies and Auriga Cyber Venture, the specialist in cybersecurity investments."*

Olivier Tonneau, Partner at Quantonation declared that *"As the leading investor in the Quantum Technologies space, we were very impressed with the level of expertise and recognition that CryptoNext has reached since our first investment in the company back in 2020. We are now entering an exciting phase of deployment of CryptoNext's technology roadmap with a list of first-class customers and are confident that their leadership will pave the way for growth"*.

William Lecat, Investment Director at Auriga Cyber Ventures insisted that *"As an investment fund specializing in cybersecurity, we have identified that the quantum threat will have a systemic impact on security, and that all organizations will have to migrate their IT/OT infrastructure to quantum safe in the next few years. We were impressed by CryptoNext Security's in-depth technical expertise and are excited about the solutions they are bringing to market to help organizations migrate efficiently to quantum safe."*

About CryptoNext Security

CryptoNext Security, based in Paris, founded in 2019 after more than 20 years of academic research. CryptoNext Security is a software vendor specializing in quantum computer resistant cryptography (PQC: post-quantum cryptography). CryptoNext offers its leading C-QSR Quantum Safe Remediation software suite including its world reference library Quantum Safe Library (C-QSL) with the latest updates of US NIST standard and EU recommended PQC algorithms optimized implementation and extended security modules as well as full set of upper-layer crypto-agile, full PQC hybridization-ready integration tools, application plugins and management modules, for end-user enterprises and integrators, to help them in their migration and operations in the era of post-quantum cybersecurity.

For more information, www.cryptonext-security.com

Contact: Christian d'Orival, Chief Revenue Officer, christian.d-orival@cryptonext-security.com.

About AVP (AXA Venture Partners)

AVP (AXA Venture Partners) is a global venture capital firm specializing in high-growth, technology-enabled companies, managing \$1.3 billion in assets across four investment strategies: Venture, Growth, Late Stage, and Fund of Funds. Since its establishment in 2016, AVP has invested in more than 60 technology companies in Venture and Growth stages in the US and Europe.

With offices in New York, London, and Paris, AVP supports companies in expanding internationally and provides portfolio companies with tailored business development opportunities to further accelerate their growth. AVP operates under AXA IM- Alts, the alternative investment business unit of AXA IM.

For more information, visit www.axavp.com

Contact: Sébastien Loubry, Partner Business development (sebastien@axavp.com)

About Quantonation

Quantonation Ventures is the leading VC dedicated to Quantum Technologies. Quantonation invests globally, targeting early-stage companies in Quantum Computing, Quantum communication and security and Quantum sensing areas. Quantonation aims to support their transition to marketable products for the industry. Quantonation is headquartered in Paris, France.

For more information, visit: www.quantonation.com

Contact: Eleonore de Rose, Audacia communication director (eleonore.derose@audacia.fr)

About Auriga Cyber Ventures

Launched in 2021, Auriga Cyber Ventures is a French early-stage investment fund 100% dedicated to European cybersecurity startups. Initiated by cyber entrepreneurs and Auriga Partners – a management company that has been pioneering VC in France since 1998 – it leverages a network of investors of more than 80 cyber specialists to deliver high value support to its portfolio. The fund aims at supporting the emergence of the future European cybersecurity champions.

For more information: visit www.aurigacyberventures.com

Contacts: Geoffroy Rosset, Partner (rosset@aurigapartners.com) / William Lecat, Investment director (lecat@aurigapartners.com)