Title: Cryptonext Security closes a First Pre-Seed Round of Financing

Date: 13th March, 2020

CryptoNext Security (**CNS**) who provides the next generation security software to protect data against the quantum threat, announced today that it has closed a pre-seed round of financing with a strategic public institute and a leading deep-tech venture capital.

Quantum computers are a cyber-security time bomb. Data can be already stored and will be decrypted once a powerful-enough quantum computer is available. The last announcement of Google on quantum supremacy is yet another major milestone towards building such large quantum computers. The trend is clear and organizations must start now to protect their infrastructure against the quantum threat. Based on 20 years of academic research, CryptoNext's security software permits right now to circumvent the quantum threat.

Standardization for quantum-resistant technologies is intense and world-wide. In view of the quantum threat to security, the US Standard body NIST started in 2017 a process to renew current public-key standards with quantum-resistant algorithms. The reference algorithms will be published within 2022 and adopted by the US administration by 2024. The algorithms selected by NIST will likely become international standards. China has a similar process and reference quantum-resistant algorithms will be published in 2020. At the EU level, ETSI is playing a central role in the integration of new quantum-resistant algorithms into security protocols (such as VPN, …). **CNS** is very active in these processes by proposing algorithms to the NIST and Chinese competitions and contributing to ETSI.

Participating in the round are Quantonation (lead) and SATT Lutech (Technology Transfer Unit from Sorbonne University). This round of funding will be used to hire software engineers and support the first commercial deployments of CryptoNext Security's quantum-resistant cryptographic library. The first customers currently testing the software come from secure messaging, blockchain and digital signature segments.

CryptoNext Security founders (Jean-Charles Faugère, CTO, Ludovic Perret, CEO, and Frédéric Urvoy de Portzamparc, COO) said, *"Besides financing, the closing of this pre-seed materializes strategic alliances for CryptoNext Security. Quantonation is a leading investor in the area of deep physics and is currently building a strong and dynamic ecosystem around quantum computing. CryptoNext Security is a spin-off from Sorbonne University and INRIA. We are very glad that our institutes are now associated to CryptoNext Security via the investment of SATT Lutech."*

Olivier Tonneau, partner at Quantonation, said "*At Quantonation, we are delighted to invest in a world-class team in terms of Post-Quantum cryptography. With new data encryption standards being defined and first clients being already deployed, we believe the market is huge and Cryptonext Security has the potential to become a world leader.*"

SATT Lutech's President, Jacques Pinget, said *"Cryptonext is at the start of a great entrepreneurial adventure, at the beginning of future huge market needs. We are proud of being part of this pre-seed round, allowing years of public research to provide solutions to meet one of the biggest challenges of ICT industry."*

Lucas Ravaux - Deputy Director, Research and Innovation department, from Sorbonne University *"Sorbonne University, Inria and CNRS are proudly supporting the take-off of one of their most talented and promising spin-off in deeptech. Cryptonext team, whose academic excellence has been widely recognized, is now ready to take a next step by tackling a great societal challenge: bringing security in a post-quantum world."*

Notes to Editors:

For more information : contact@cryptonext-security.com.

About Cryptonext Security

CryptoNext Security is a spin-off from from Sorbonne University and INRIA. Based on 20 years of academic research, **CNS** provides quantum-resistant cryptographic software technologies to help all companies protect right now their products and themselves against the quantum threat. Field-proven since 2016 over smartphones, CryptoNext Security's library is now available for security chipsets, common computers, and servers, delivering classical and quantum resistance with optimized performances.

In 2018, the **CNS** founders have been awarded by the first Atos-Fourier Prize on quantum technologies for their contributions to quantum-resistant cryptography. CryptoNext Security has been created in June 2019, currently incubated at Agoranov and accelerated by Cyber@StationF and Wilco. In October 2019, CryptoNext Security has been selected in the first edition of Future40, the 40 most promising startups of StationF (the biggest European startup campus).

For more information and news visit www.cryptonext-security.com.

Cryptonext's Security founding team : Jean-Charles Faugère, Frédéric de Portzamparc and Ludovic Perret.

About Quantonation

Quantonation is the first early stage VC fund dedicated to Quantum Technologies and Deep Physics. Fields such as materials design, high performance computation, cybersecurity, or ultra-precise sensing are now driven by innovation based on these disruptive technologies. Quantonation aims at supporting their transition into commercially available products for the industry. Quantonation is headquartered in Paris, France with investments all over the world. For more information and news visit www.quantonation.com.

About SATT Lutech

Lutech promotes the emergence of innovations with economic and / or societal potential.

Lutech detects, protects, develops and markets the skills, creations and research results from its establishments: Sorbonne University, CNRS, Technological University of Compiègne, National Museum of Natural History, National School of Industrial Creation, University Panthéon-Assas.
Lutech has the capacity to invest in the development of proofs of concept and / or prototypes to support innovative projects towards the market. Lutech is also responsible for transferring these projects to existing companies (large groups, mid-caps and SMEs) or through the creation of companies. These structures will then be able to finalize development at lower risk and put these innovations on the market. For more information, visit www.sattlutech.com