ÉLÉMENT DE PORTFOLIO 01

Création d'entreprise

1 DÉFINITION DE CET ÉLÉMENT

Titre de l'élément : CryptoNext Security

URL de l'élément : `https://www.cryptonext-security.com/`

2 MOTIVATIONS DU CHOIX DE CET ÉLÉMENT

La création de CRYPTONEXT SECURITY atteste du leadership de PolSys sur la cryptographie post-quantique ainsi que sa capacité à valoriser les outils du calcul formel dans le monde économique. Elle montre aussi comment l'équipe a su se saisir des dispositifs de transfert technologique pour mettre en œuvre un cycle complet d'innovation technologique (de la recherche fondamentale jusqu'à l'entrepreneuriat).

3 PRÉSENTATION DE CET ÉLÉMENT

CRYPTONEXT SECURITY est une startup issue de PolSys et créée le 13 juin 2019. Les deux fondateurs sont liés à l'équipe : Jean-Charles Faugère (CTO, temps complet dans la société) en a été le responsable, et Ludovic Perret (CEO, en délégation à temps complet de 2019 à 2022) membre. La cryptographie post-quantique est une composante majeure des recherches de PolSys et la startup repose sur cette expertise (un brevet [2] et un dépôt logiciel relié à MQSOFT [1]).

En 2015, dans le cadre d'une visite organisée par le LIP6, le Ministère des Armées a demandé à PolSys de concevoir une application de messagerie instantanée post-quantique fonctionnant sur des téléphones portables du commerce. Le Ministère des Armées a testé l'application et mené une expérience en conditions réelles en installant l'application sur une centaine de téléphones utilisés sur le terrain par des militaires. Le succès de cette expérience a incité les fondateurs à entamer cette même année un projet de maturation porté par la SATT Lutech, dont CRYPTONEXT SECURITY est l'aboutissement. En 2016, l'institut de normalisation américain NIST a annoncé le lancement d'un processus de sélection de nouveaux standards de cryptographie post-quantique en vue d'une migration des administrations américaines à partir de 2024.

Constatant l'intérêt croissant suscité par la cryptographie post-quantique, les fondateurs de CRYPTONEXT SECURITY ont alors créé la société et ont finalisé une première levée de fonds avec Quantonation (fonds professionnel) en décembre 2019 ainsi qu'avec ses tutelles via la SATT Lutech. En 2021, l'équipe des deux fondateurs a été rejointe par Florent Grosmaitre comme nouveau CEO afin d'accompagner la croissance rapide CRYPTONEXT SECURITY et entraînant le retour de L. Perret dans PolSys en juin 2022.

CRYPTONEXT SECURITY est aujourd'hui présente au campus Cyber à la Défense. L'entreprise était, auparavant accélérée par la BNPP via le programme Plug & Play de Station F, par Wilco (promotion 2019), incubée par Agoranov (avril 2019) et sélectionnée dans le programme Cyber@StationF de Thales à (Cyber@StationF, juin 2019). Pendant le programme Cyber@StationF, CRYPTONEXT SECURITY a été sélectionnée parmi 1000 start-ups comme faisant partie des 40 plus prometteuses. En 2020, CRYPTONEXT SECURITY a été lauréate du prestigieux Concours d'innovation i-Lab et l'un des 10 Grands Prix récompensant des projets exceptionnels qui ont vocation à relever un défi sociétal majeur.

J.-C Faugère et L. Perret ont reçu le premier prix Atos-Fourier (2018) dans le domaine des technologies quantiques pour la création de CryptoNext Security et leurs contributions académiques au post-quantique et nommés, en 2022, par le Magazine Le Point dans les 100 inventeurs de demain.

3.1 Nature de l'activité

L'ordinateur quantique remettant en cause la sécurité des techniques cryptographiques actuelles, CryptoNext Security a pour mission de simplifier la transition des organisations publiques et privées vers de nouvelles normes cryptographiques post-quantiques. Le cœur technologique et le savoir-faire de CryptoNext Security sont une bibliothèque logicielle de cryptographie, qui implémente les deux fonctions fondamentales de la cryptographie à clé publique, l'échange de clés et la signature numérique, en utilisant une cryptographie post-quantique.

La bibliothèque logicielle est destinée à être intégrée dans tous les cas d'usage qui utilisent de la cryptographie à clé publique, en particulier HSM (Hardware Security Module), VPN (Virtual Private network), les solutions de signatures numériques, les solutions métiers (logiciel métier santé, embarqué automobile, ...), les solutions de bureautique (messagerie instantanée, visio-conférence, email, ...).

Le logiciel a déjà été testé par plusieurs clients : le gouvernement français avec la transmission du premier message diplomatique utilisant de la cryptographie post-quantique et des clients du monde de la défense ou de la finance (comme la Banque de France).

CRYPTONEXT SECURITY a collaboré avec l'équipe QI du LIP6 sur deux projets (Européen et régional) qui visent à intégrer la cryptographie post-quantique et la distribution de clé quantique (QKD) dans le cadre de la conception d'un futur réseau Européen de communication quantique.

4 RÉFÉRENCES BIBLIOGRAPHIQUES

[1] Jean-Charles Faugère, Ludovic Perret, and Jocelyn Ryckeghem. Software Toolkit for HFE-based Multivariate Schemes. In *CHES 2019 : International Conference on Cryptographic Hardware and Embedded Systems*, volume 2019 of *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 257–304, Atlanta, United States, August 2019.

[2] Ludovic Perret and Jean-Charles Faugère. Mise en Oeuvre Optimisée du HFE, January 2017.