BitMint: Secure and efficient transition journey to Quantum-Resistant Cryptography

Project Partner Search Form

☒ I offer my expertise to participate as a Partner in a Horizon Europe Project

☐ I am planning to coordinate a project and I am looking for Project Partners

TOPICS OF INTEREST

HORIZON-CL3-2024-CS-01-02: Post-Quantum Cryptography Transition

PARTNER INFORMATION

Description of the Legal Entity

☐ Higher Education	☐ Research Institution	☐ Public Administration
☒ Industry /SME	☐ NGO	☐ Other: ***Please specify***

Description of the (Research) Team

BitMint builds a **crypto-agility strategy**, with a **Quantum Emergency Recovery {QER] capability**, that is ready to kick-in in case of a catastrophic scenario (e.g. an adversary breached the cryptographic system and cause a collapse). It will make it possible to rely on the NIST standard when it is announced (if desired), but not to be based ONLY on NIST.

Ensuring long-term resilience against quantum threats requires **crypto agility**, e.g.,

(i) the ability to easily switch cryptographic methods as ciphers in use are breached;

(ii) Shifting the control from cipher developer to the user itself, who knows better the level of security required for each piece of information. Unlike the current situation in which users are "locked" to one cipher, they should be able to choose less or more security, based on the level of confidentiality/sensitivity of the data transmitted.

This concept of crypto agility is of utmost importance, because we don't ever want to be back in the same situation we are now where we have mathematical algorithms that are being compromised.

Therefore, it's a MUST to make, at least critical applications, - crypto agile, so organisations have a "**life-boat" in case of an emergency**, and can rotate between different solutions.

It will enable deploying all relevant available solutions - PQC (NIST/ETSI), Pattern Devoid Cryptography (Trans Vernam Ciphers) and potentially QKD when it is ripe for deployment, and effectively continuously and smoothly modernizing and updating their cryptographic ecosystem.

BitMint: Secure and efficient transition journey to Quantum-Resistant Cryptography

We have a family of solutions that are based on Pattern Devoid Cryptography, with **mathematical proof of efficacy**.

- In January 2024, a respectable **London publisher** is coming out with a new thoroughly **vetted peer-reviewed** book –'Biometrics and Cryptography'. A leading chapter in the book -

'Pattern-Devoid Cryptography', authored by OUR chief technology officer, professor Gideon Samid, PhD, Eng.

https://www.intechopen.com/online-first/pattern-devoid-cryptography

Earlier,

- **The World Economic Forum [WEF]** acknowledges OUR concepts: "Randomness: The Fix for Today's Broken Security", authored by our CTO, and by a physicist from the German 22Bn€ Innogy corporation.

https://www.weforum.org/agenda/2017/11/what-a-100-year-old-idea-can-teach-us-about-cybersecurity

These solutions help to establish crypto-agility throughout the EU quantum-resistant journey, with technologies that build simplicity, flexibility, and automation as well as ability to self-control the rate of security, into the EU quantum-resistant transformation roadmap.

Expertise of the Team Leader

Prof. Gideon Samid, PhD, PE is a recognized innovator (41 issued patents), active in cyber and material sciences, developer of the new cryptographic pathway: Trans-Vernam, Quantum-Resistant ciphers. Worked in Israeli security apparatus, and at NASA, graduated from the Technion -- Israel Institute of Technology

Potential role in the project

☒ Research ☐ Training

☐ Dissemination ☐ Other: ***Please specify***

Already experience as a	Coordinator	☐ YES	☐ NO
	Partner	☐ YES	☐ NO
	Expert Evaluator	☒ YES	☐ NO

CONTACT DETAILS

Contact Person: Amnon Samid
Organization: BitMint
City: Tel-Aviv/Sderot
Country: Israel
Phone: +972544200400
Email: amnon@BitMint.com
Organization Website: https://www.bitmintalk.com/
Contact Person Webpage: https://www.linkedin.com/in/amnon-samid-3057418/

Date: 16 September 2024

Elaboration

BitMint: Secure and efficient transition journey to Quantum-Resistant Cryptography – BRIEF abstract

We aim to join a consortium that is preparing to submit a proposal in response to **HORIZON-CL3-2024-CS-01-02: Post-Quantum Cryptography Transition.**

We believe that what our small company has to offer could be an important added value to any consortium submitting to this call, with different approach that is mathematically proven, and will complement any PQC (like NIST), and will strengthened EU cybersecurity capacities and European Union sovereignty in digital technologies, aligning with the recommended hybrid approach, combining recognized standard like NIST or future ETSI standards, that are based on complexity theory with no mathematical proof, with what we propose - a Pattern-Devoid Cryptography with mathematical proof of efficacy.

A brief elaboration: what are the options:

- Quantum key distribution [QKD] utilizes the unique properties of quantum mechanical systems to generate and distribute cryptographic keying material using special purpose technology .
  - QKD is not mature enough .
- Quantum cryptography [QC] uses the same physics principles and similar technology to communicate over a dedicated communications link .
- Post Quantum Cryptography [PQC], like NIST's published standards of 13th August 2024 – derive their security through mathematical complexity, but are not based on a mathematical proof, meaning they are NOT Quantum-Proof Cryptography .

The "weak link" of the last two is that it is born in the bosom of a complex algorithm, and it will die when this algorithm surrenders to AI Cryptanalysis, or to smarter mathematicians armed with quantum computers. The greater the mathematical complexity, the greater the chance for an extended mathematical imagination to find a mathematical shortcut associated with quantum computing and stealthily crack the complexity cipher.

So, what else is there? - -(=what we propose as add-on to any proposal) -

🔷Pattern-Devoid Cryptography provide means with mathematical proof of efficacy for assuring the confidentiality, integrity, and authentication of data stored or in transit - even against a potential future quantum computer.

🔷Crypto-agility: Ensuring long-term resilience against quantum threats requires crypto agility, e.g. the ability to easily switch cryptographic methods as ciphers in use are breached, and shifting the control from cipher developer/issuer to the user itself .

🔷 Quantum Emergency Recovery [QER]: It is advised to prepare a super-secured cryptography, that is NOT complexity based - to be kicked in, should the need arise. You may feel duty bound to consider Quantum Emergency Recovery [QER], so you are able to recover fast from a catastrophic cyber collapse.

- Smart countries will not rely ONLY on complexity-based solutions (like NIST's PQC) with NO mathematical proof, BUT also on Pattern-Devoid Cryptography with mathematical proof of efficacy.

It also makes sense to ask **why should Europe rely on an American standard, which does not and cannot have a mathematical proof**, instead of deploying a quantum resistant cryptography that has a mathematical proof, so there will not even be a shadow of fear that the Americans (or others) will be able to integrate there a 'back door', nor breaching it with smart team and strong computers.

The above challenges are exactly where our approach fits in.

Contact: amnon@BitMint.com