Post-Quantum's algorithm is finalist in NIST's Post-Quantum Cryptography competition

Monday 27 July, 2020

Rapid advances mean a sufficiently developed quantum computer will soon break today's public-key cryptography, placing virtually all the world's data at risk. Combined with the threat of nation states such as China and Russia harvesting data today, for decryption in the future, the need to move the world to modern 'quantum-safe' public key cryptography has never been more urgent.

That's why the National Institute for Science and Technology's (NIST) global competition to identify the strongest cryptographic algorithms that can withstand attack by quantum computers has been running for four years already, with the objective of creating a new global standard by 2022.

Today, UK deep tech start-up Post-Quantum announces it has merged its own NIST submission, known as 'NTS-KEM', with the submission led by Professor Daniel Bernstein. The joint candidate, known as 'Classic McEliece', has been selected as one of seven 'finalists' in NIST's third round selection process for public-key cryptography and key establishment. Selection follows a gruelling multi-year period where the world's preeminent cryptographers and hackers have been attempting to crack the algorithm, without success.

NIST's post-quantum standard is necessary because it has been shown that quantum computers can easily factorise large numbers and it is now a matter of time before today's public-key cryptography standards (RSA and Elliptic Curve) are broken. These standards currently protect virtually all the world's data both at rest and in transit across the internet, as well as crypto-currencies such as Bitcoin.

All technical products (browsers, applications, email and communication protocols) will need to transition to NIST's new post-quantum encryption standard as it becomes available from 2022. Post-Quantum is launching its own range of quantum-safe products having recently unveiled its biometric identity authentication service 'Nomidio'.

Importantly, Classic McEliece is the only finalist within the 'code-based' category of the competition, which is significant given NIST intends for the final standard to include a range of cryptographic techniques, widely expected to include code-based. Classic McEliece is ultra-secure whilst offering enhanced performance that even outperforms today's standards.

Andersen Cheng, CEO and Co-Founder at Post-Quantum commented: "*We are pleased to have combined our cryptographic innovations with those of Professor Daniel Bernstein's team to create a single NIST submission. Dan is one of the top cryptographers in the world and together with Professor Kenny Paterson from ETH Zurich, Professors Martin Albrecht and Carlos Cid from Royal Holloway University of London, we are confident our joint efforts will ensure Classic McEliece remains a tour de force for many years to come.*

He continued: *"The entire world needs to upgrade its encryption and we last did that in 1978, when RSA came in. The stakes couldn't be higher with record levels of cyber-attack and heightened nation state activity – if China or Russia is the first to crack RSA then cyber Armageddon will begin."*

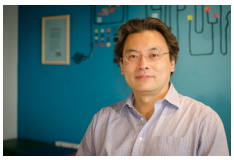
"*This isn't an academic exercise for us, we are already several years down the commercialisation path with real-world quantum-safe products for identity authentication and VPN. If you work for an organisation with intellectual property or critical data with a long shelf life, and you're working from home during lockdown, you should already be using a quantum-safe VPN." Added Cheng.*

Post-Quantum's Classic McEliece algorithm deliberately introduces errors into the encryption process and the outputs are 'never the same', which in effect means quantum computers have 'nowhere to start' when trying to brute-force break the encryption.

This work was pioneered by Post-Quantum Co-Founder Professor Martin Tomlinson of Plymouth University whose background in correcting errors in satellite communications (e.g. removing pixilation from satellite TV) has been transferred into the field of cryptography. Also essential to Post-Quantum's algorithm is third Co-Founder and CTO, CJ Tjhai, a former student of Professor Tomlinson and a specialist in optimising and creating commercially robust software for real world implementations.

"We have already launched our quantum-ready identity solutions under the 'Nomidio' brand for partners

Media:



Related Sectors:

Business & Finance :: Computing & Telecoms ::

Related Keywords:

Post Quantum :: Quantum Computing :: Cryptography :: Classic McEliece :: National Institute For Science And Technology :: NIST :: Cryptosystem ::

Scan Me:

and clients such as Amazon, Avaya and Hitachi. We are also bringing to market a quantum-safe Virtual Private Network (VPN) that companies can buy off-the-shelf to ensure their data crossing the internet is protected from quantum attack. The great risk is that adversaries may steal data today and then, in years to come, use a quantum machine to decrypt it." Added Tjhai. *"Whichever way NIST formalises the eventual standard, our products are engineered for 'crypto agility', so we can simply drop the NIST finalist algorithms in."*

NIST's Post-Quantum Cryptography competition has already been running for almost four years and the original 82 submissions, including multiple submissions from Microsoft, IBM and Intel, have now been whittled down to the seven 'finalists', deemed to be widely applicable algorithms that will be 'ready to go' after the final selection round. Eight 'alternate' algorithms are also still being assessed that may need more time to mature or are tailored for more specific applications.

After this final round concludes NIST expects to standardise one or two algorithms for Encryption and Key Establishment, and another for Digital Signatures.

1. **Public-key encryption:** an encryption scheme based on widely distributed public-keys and private keys known only to the owner. In such a system, any person can encrypt a message using the receiver's public key, but that encrypted message can only be decrypted with the receiver's private key.
2. **Key establishment:** the process of securely providing encryption keys to two parties that wish to encrypt and decrypt messages exchanged between one another.
3. **Digital signatures:** a technique for verifying the authenticity of digital messages helping a receiver to be sure the message originated from a specific sender.

Company Contact:

_

Post-Quantum

E. jbarnes@fireoth.com
W. https://post-quantum.com/

Additional Contact(s):
nward@fireoth.com
zhardman@fireoth.com

View Online

Additional Assets:

Newsroom: Visit our Newsroom for all the latest stories:
https://www.pq.pressat.co.uk