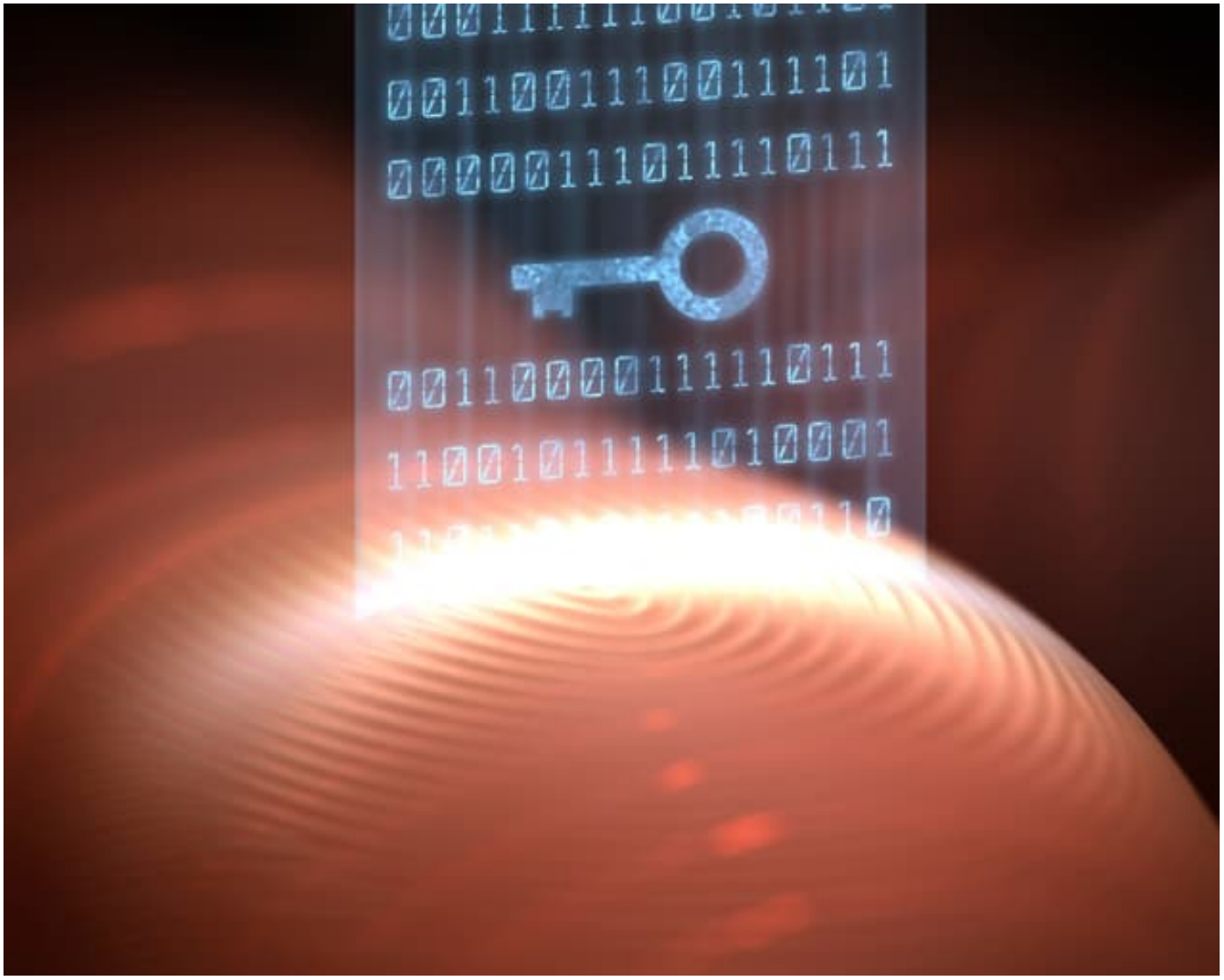
physicsworld

CRYPTOGRAPHY | NEWS

NIST selects four 'post-quantum' encryption standards

20 Jul 2022



The US institute has selected four algorithms that will be developed to protect data from a future quantum computer attack (Courtesy: iStock/ktsimage)

The US National Institute of Standards and Technology (NIST) has selected four algorithms that will be developed as post-quantum encryption standards to protect data from a future quantum computer attack. The announcement follows a six-year competition, with NIST now calling on institutions to investigate how to best apply the standards.

Once fully developed, quantum computers are considered ideal candidates for calculating complex processes. On the other hand, they could also be used for malicious activities, such as hacking currently encrypted information. This could put data – such as governmental documents or company secrets – at risk.

For this reason, in 2016 NIST launched an open competition in post-quantum cryptography where researchers from all over the world could submit their algorithms to be considered as a future standard. Several rounds shortlisted the candidates and allowed for further tweaking of the proposed protocols.

More to come

Now NIST has announced four winners. Post-quantum cryptography is designed for two main tasks. The first is general encryption that protects information exchanged across a public network. Here NIST selected the CRYSTALS-Kyber algorithm that uses comparatively small encryption keys that two parties can exchange easily and has a high speed of operation.

The second task concerns digital signatures and is used for identity authentication. Three algorithms were selected: CRYSTALS-Dilithium, FALCON and SPHINCS+. The first two are preferred due to their efficiency, while SPHINCS+ uses a different mathematical approach from the other three winners.

NIST says that institutes should now begin to upgrade to post-quantum cryptography, stressing a "collect-now decrypt-later" approach, which means implementing post-quantum cryptography before the creation of large-scale quantum computers. NIST also announced four other algorithms that are still under consideration as standards. The winners of that round will be announced at a later date.

Martijn Boerkamp is a science journalist based in the Netherlands