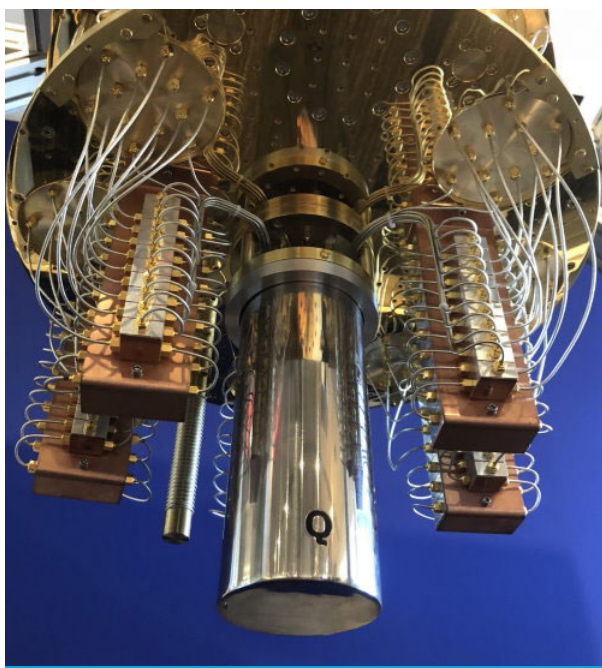BITS&CHIPS

🔍 SUBSCRIBE

HEADLINE

CWI and Radboud help IBM to develop quantum-proof cryptography

Paul van Gerven

27 August

Together with several partners, among which the Centrum Wiskunde & Informatica (CWI) and the Radboud University, IBM Research has developed quantum-safe algorithms for securing data. The so-called Crystals suite, containing a secure key encapsulation mechanism and a digital signature algorithm, has been open-sourced and submitted to the National Institute of Standards and Technology (NIST) for standardization. In addition, IBM plans to make quantum-safe cryptography services available on its cloud quantum computing platform, called IBM Q, and to start offering a 'quantum risk assessment' to customers.

Credit: IBM Research

Related