

Macro Roundup Article

Headline: Chinese Researchers Claim to Find Way to Break Encryption Using Quantum Computers

Author(s)	Richard Waters
Publication	Financial Times
Publication Date	January 05, 2023

Tweet: Chinese computer scientists claimed to have used quantum computing to break the RSA algorithm that underpins the vast majority of online encryption. However, the algorithm may not be fast enough to be relevant. @FT

Summary: Computer security experts were struggling this week to assess a startling claim by Chinese researchers that they have found a way to break the [RSA algorithm,] the most common form of online encryption, using the current generation of quantum computers, years before the technology was expected to pose a threat. Peter Shor, the Massachusetts Institute of Technology scientist whose 1994 algorithm proving that a quantum machine could defeat online encryption, noted that the Chinese researchers had “failed to address how fast the algorithm will run”, and said that it was possible it “will still take millions of years”. He said: “In the absence of any analysis showing that it will be faster, I suspect that the most likely scenario is that it’s not much of an improvement.”

Related Articles: nan

Primary Topic: Innovation/Research

Topics: Factoid, Innovation/Research, News article, Productivity, Sell-by Date

Permalink: <https://www.edwardconard.com/macro-roundup/chinese-computer-scientists-claimed-to-have-used-quantum-computing-to-break-the-rsa-algorithm-that-underpins-the-vast-majority-of-online-encryption-however-the-algorithm-may-not-be-fast-enough-to-be?view=detail>