Can Quantum Computers break RSA encryption: An analysis by GQI in partnership with the NATO Innovation Fund

A comprehensive analysis of the current state of quantum computing and key factors that will determine the threat to RSA encryption standards.

MIAMI, FL, UNITED STATES, December 6, 2024 /EINPresswire.com/ -- Global Quantum Intelligence, LLC (GQI), the leading quantum technology research and advisory firm, today published a report titled "Road to Shor Era Quantum Computing" in partnership with the NATO Innovation Fund (NIF).

Read the full report at www.global-qi.com/reports

In partnership with

NIF

THE ROAD TO SHOR ERA QUANTUM COMPUTING — GQI Global Quantum Intelligence

IN PARTNERSHIP WITH

NIF

OUTLOOK REPORT

Dec 2024

The full report is available on our website

The report provides a comprehensive analysis of the current state of quantum computing and identifies the key factors that will determine the emergence of a dominant design able to break RSA 2048 encryption standards.
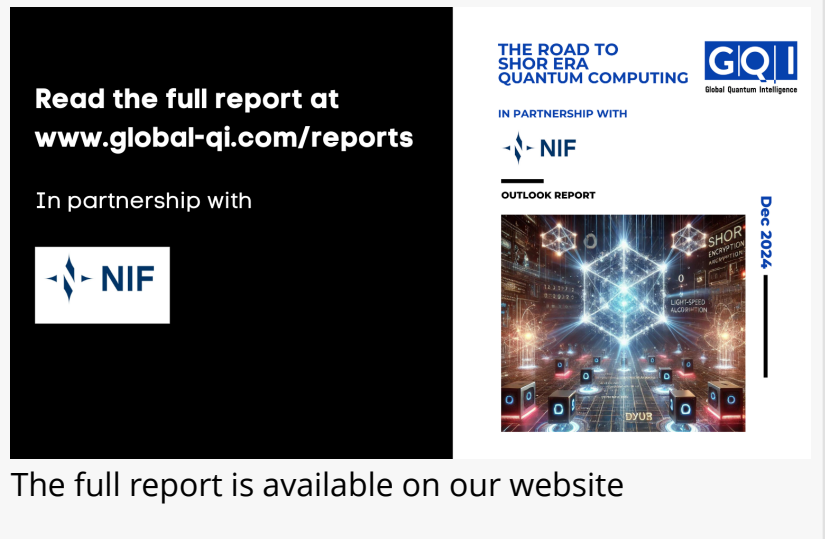
> Working with NIF, our approach was to challenge QC developers to extend their usual hardware roadmaps all the way to a system able to break RSA 2048; a cryptographically relevant quantum computer."
>
> *Dr. David Shaw*

"The history of conventional digital technology shows us that once a dominant design emerges, it is hard to displace," said André M. König, CEO of GQI. "Our report provides a roadmap for quantum computing companies to develop technologies that have the potential to become the dominant design and safeguard our future; before a threat emerges that will put our national security at risk."

Working with NIF, GQI challenged QC developers to extend their usual hardware roadmaps all the way to a system able to break RSA 2048, a cryptographically relevant quantum computer (CRQC). Forcing the large system view brought crucial scaling challenges clearly into focus. A million qubits is not a large scale machine, if surface code error correction is the sole scaling factor.

The report highlights the importance of various qubit platforms, approaches to QEC, and the true cost of scaling towards a dominant design for quantum computing. One key question is if modules are part of a scalable strategy and how key performance indicators, such as 2Q gate fidelity but also speed of operations as well as measurement with realistic code cycle and an effective logical cycle perform. Crucially, to achieve modular scaling, couplers or interconnects that can coherently connect modules are required. That technology has been neglected in far too many product roadmaps.

"Really there are two quite different overall high level architectures out there. Some players are building-out monolithic arrays of qubits, with scalable modules, but ultimately a monolithic array. Others are pursuing some variation of Distributed Quantum Computing, either pure photon based, or matter qubits plus photons. Leave your classical analogies on the shelf they are unhelpful. This is a pure quantum-on-quantum battle that you need to get your head round the differences.," said Dr. David Shaw, Chief Analyst at GQI.

GQI & NIF identifies 7 initial quantum computing vendors with roadmaps towards this goal and provides a deep analysis of their hardware. The report also discusses the investment landscape and the potential for major mergers and acquisitions in the sector.

The full report is available for download at https://www.global-qi.com/product-page/road-to-shor-era-quantum-computing

About GQI

GQI is a leading quantum technology research and advisory firm. We provide our clients with the insights, expertise and tools they need to make informed decisions about quantum technology. Our team of experts has deep experience in quantum physics, computer science, and business. We are committed to helping our clients succeed in the quantum computing revolution. Don't gamble. Know.

André M. König
Global Quantum Intelligence, LLC
info@global-qi.com
Visit us on social media:
X
LinkedIn

---

in today's world. Please see our Editorial Guidelines for more information.