

Quantum Hacking Coming Sooner than Expected

New estimates suggest that some crypto-security systems may soon become vulnerable to quantum-powered break-ins.

By **Michael Schirber**

Quantum computers promise to solve important scientific problems, but they could also be used to crack data security systems. Researchers have performed a new analysis of this threat and have concluded that such quantum-hacking ability may come sooner than previously expected [1]. The team estimates that 500,000 quantum bits (qubits) are needed to crack the most common crypto-security system used today, which is a reduction by a factor of 20 below prior estimates. The implication is that a wide-range of institutions—including government agencies, commercial companies, and cryptocurrency providers—need to rapidly update their cybersecurity to the latest “quantum-resistant” codes.

“Quantum technologies have been thought of as ‘over a decade

away’ for a long time,” says Stephanie Simmons, a quantum researcher from Simon Fraser University in Canada, who was not involved in the new research. But large-scale quantum computers may become available in a few years, she says. One of these machines may become available in a few years, she says, and that possibility has implications for how society protects sensitive infrastructure, such as satellite control systems, power grids, and financial institutions.

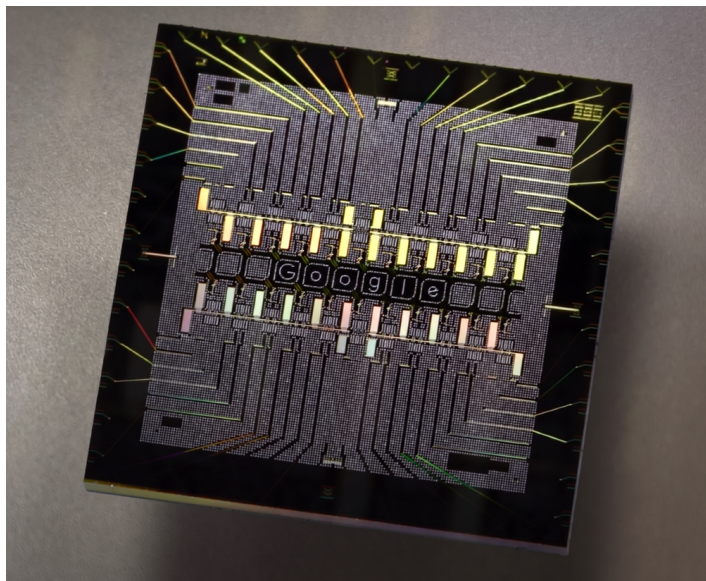
A common perception is that digital cryptography relies on the difficulty of factoring large integers, but today roughly 90% of crypto-schemes are based on solving a complicated polynomial equation, called an elliptic curve equation. Elliptic curve cryptography is used in software authentication, web security, and electronic passport protection, for example. It also provides a way to validate financial transactions for cryptocurrencies, such as Bitcoin and Ethereum. A classical computer would need a billion years or more to break into an elliptic-curve-secured system. The new work by Ryan Babbush of Google Quantum AI in California and colleagues explores how a quantum computer could do it in a much shorter time.

Current quantum computers are too small and too error prone to break elliptic curve cryptography. But researchers have developed quantum-hacking algorithms that could be run on some future quantum computer. These algorithms can be thought of as circuit diagrams that map out the various connections between qubits and the structures, called gates, that perform operations on them. For a particular algorithm, researchers can infer the necessary computing resources. Estimates based on previous algorithms suggested that hacking current crypto-security systems would require millions of qubits and many millions of gates.



Quantum breach. In the near future, hackers might be able to use quantum computers to unlock crypto-security systems.

Credit: [tadamichi/stock.adobe.com](#)



Master key. If they continue to grow in size, quantum computers have the potential to break math-based codes that protect many types of sensitive information.

Credit: Google Quantum AI

Babbush and colleagues have reevaluated these estimates by analyzing a hacking algorithm they developed and by accounting for recent improvements in quantum error correction. They did not reveal the details of their algorithm for security reasons but instead provided a “zero-knowledge proof” that verified its efficacy. (However, a cryptographer was able to use this limited information to fill in the missing details and construct a full algorithm, which has now been posted online [2].)

By the team’s estimates, the hacking algorithm could be run on a superconducting quantum computer having around 500,000 qubits and roughly 80 million gates. This number specifies “physical” qubits, of which only a small number perform logical operations—the rest help correct errors. The operation could take less than 10 minutes, a time short enough that it might pose a risk to certain cryptocurrency transactions that involve short-term public sharing of secret codes.

A separate qubit estimate was recently made by a team of scientists from Oratomic, a quantum computing company in

California. These researchers considered a quantum computer whose qubits are single atoms, a type that generates fewer errors but which is slower than a superconducting quantum computer. With this architecture, they estimate that a quantum hack could be accomplished with 26,000 physical qubits but would take several days [3].

The results “seem reasonable to me, even if all the details haven’t quite been nailed down yet,” says quantum-information expert Scott Aaronson from University of Texas at Austin. He says that the improved algorithms appear to shorten the timeline until a cryptographically relevant quantum computer becomes available.

The moment when such a computer arrives—sometimes called Q-Day—depends not only on algorithms but also on hardware, which continues to improve. Quantum computers can now have more than 1000 qubits, and their error rates are coming down (see [Viewpoint: Plugging Leaks in Quantum Computing](#)).

To mitigate this threat, data-security specialists have developed quantum-resistant security systems. This so-called post-quantum cryptography uses math that is believed to be too hard for even quantum computers to solve. Babbush and colleagues urge all data managers to migrate to post-quantum cryptography “without delay.”

Simmons agrees that this work should be “a wake-up call” to those in the data-security industry. Quantum capabilities are rapidly improving, she says, and some advances may be kept secret. “The publicly known state of the art is unlikely to be the actual state of the art.”

Michael Schirber is a Corresponding Editor for *Physics Magazine* based in Lyon, France.

REFERENCES

1. R. Babbush *et al.*, “Securing elliptic curve cryptocurrencies against quantum vulnerabilities: Resource estimates and mitigations,” *PRX Quantum* **7**, 031001 (2026).
2. A. Schrottenloher, “Optimized point addition circuits for elliptic curve discrete logarithms,” [arXiv:2606.02235](#).
3. M. Cain *et al.*, “Shor’s algorithm is possible with as few as 10,000 reconfigurable atomic qubits,” [arXiv:2603.28627](#).