HED: Crypto Researchers Crunch to Protect Data for Quantum Computing Era

By Aaron Ricadela

Computers based on quantum physics are poised to open vistas in medicine, manufacturing, and finance, exploiting subatomic properties to run massive numbers of calculations simultaneously. Yet these emerging quantum computers' staggering power to weigh possibilities could also render today's data-protecting encryption schemes lame within a decade or two, touching off a race to keep business and government data safe.

Internet encryption standards such as the widely used RSA algorithm and others rely on complicated math that taxes the ability of classical computers to reverse-engineer certain equations in realistic time frames. That cipher-cracking could prove easy for future quantum computers, which increase their processing power exponentially as they add more miniature quantum bits. Experts are advising businesses to start paying attention to developments now and assessing their risk.

"There's a threat now even if a quantum computer hasn't been built," says Dustin Moody, a mathematician at the National Institute of Standards and Technology leading its Post-Quantum Cryptography program. Since governments and hackers could collect information now to decrypt later with a quantum computer, and many organizations require data be kept secret for years, "businesses that have quantum computing on their radar and start planning will do a lot better than those trying to put out a fire in two years," he says.

NIST's Post-Quantum Cryptography program aims to evaluate, stress-test, and ultimately publish by 2025 a new set of online encryption schemes that quantum computers can't break. By early June NIST plans to announce 10 to 13 data encryption algorithms that qualify for a third round of the program, winnowing down the 26 candidates it ratified at the beginning of last year. A final group of security schemes considered safe from attacks by quantum computers could lead to government and private sector adoption internationally, according to Moody.

Today's widely used public-key cryptography systems safeguard e-commerce, internet banking, telecom networks, e-mail, blockchain, and more. They rely on computers' inability in a reasonable time to find the two factors of extremely large prime numbers—as in the widely used RSA algorithm—or to compute logarithms and find intersecting points on a curve—as in Diffie-Hellman key exchange or elliptic curve cryptography. Quantum computers likely won't contain enough qubits to crack those until about 2030. But businesses and technology vendors are working now to make sure data stays safe in the future.

"The real thing we're worried about is if quantum computers come out before we can fully retool," says Daniel Southern, an information security senior manager at Oracle, who is tracking the progress of the Post-Quantum Cryptography program and has commented on submissions[**[CHECK]].** Global companies will ultimately adopt these standards for data encryption, and products including databases, business applications, productivity software, phones, and laptops will need to run them. "It doesn't matter which flag you're flying, you're using NIST cryptography," he says.

SUBHED: Exponential Increases

Quantum computers store and process information in a fundamentally different way than traditional machines whose bits consist of strings of zeros and ones. The quantum computers being tested by tech companies, universities, government labs, and startups exploit properties of quantum mechanical behavior to store information in microscopic qubits. Microwave pulses push qubits into states of quantum uncertainty so they hold information in two states—zero and one—simultaneously until they're measured, a phenomenon called superposition. Qubits can also be "entangled" with one another according to the laws of quantum physics, creating circuits that aid their calculations. The result is a system that can explore many computational paths at once, adding computing power exponentially according to the number of qubits. That means a system with 100 qubits could store 2 to the 100th power number of values—more than the number of atoms on Earth.

The result could be that the resolution of an airplane design model doesn't have to get fuzzier as objects increase in size, or financial portfolio analyses that encompass many more market variables. Drug design software could model every atom in a molecule. That fine grain is beyond today's computers for even a common drug such as penicillin, according to a Boston Consulting Group report last year on the economic potential of quantum computing. Global firms could realize an additional $2 billion to $5 billion in annual operating income by 2024 by applying quantum computing to supply chain and financial portfolio optimization, vehicle design, and drug discovery, BCG writes. The impact could accelerate to $25 billion to $50 billion annually within 10 to 20 years.

Private industry is jumping in. Goldman Sachs is working with a California quantum computing startup on reducing the time it takes to value portfolios of options. Volkswagen last fall demonstrated using a quantum computer to instantly calculate routes for nine buses through Lisbon for the WebSummit conference. In Germany, chemical company BASF invested in a startup spun out of Harvard University that's developing software for quantum computers.

The search for quantum advantage is also fueling an influx of government funding. The U.S. government is committing $1.2 billion to increase quantum computing research and establish a federal advisory committee on the field, and may commit

more to build a quantum-safe network among the country's national labs. The European Union is spending €1 billion ($1.1 billion) over 20 years on quantum computing research, including on encryption of its telephone and data transmission networks. China has spent $400 million on a national quantum computing lab, and is developing an alternative security technique called quantum encryption, which differs from the mathematical approaches favored by NIST. Japan is also investing in post-quantum cryptography.

SUBHEAD: Still Safe—For Now

So far, public key encryption is still secure. It's unclear whether a practical quantum computer with enough processing power will be built that's capable of breaking today's internet encryption schemes. Such a system would need to contain millions of qubits, according to experts. Today's state of the art: less than 100. In addition, quantum machines generally operate at extremely cold temperatures—minus 273 Celsius, or near absolute zero and colder than outer space. Quibits also need to be heavily isolated from outside interference such as radio waves or vibrations.

Quantum computers could pose a threat to public-key cryptography within 10 to 20 years, according to a survey of 22 quantum computing experts surveyed last year by the Global Risk Institute, which studies threats and trends in the finance industry from new technologies.

Successors to today's encryption schemes will likely fall into three general categories designed to thwart quantum computing's code-breaking advantages, according to NIST's Moody. One is the mathematical construction of lattices—like the structure of a honeycomb or crystal, but with hundreds or a thousand dimensions, with all points in the lattice represented by an integer, and infinite space between them. It's exceedingly hard to find points on the lattice from an arbitrary location without possessing the secret key.

Another set of candidate algorithms use code-based cryptography, which introduces noise and interference to obscure information on the recipient's end of a message. A third family of algorithms for digital signatures, called multivariate cryptography, rests on the difficulty of reverse-engineering quadratic functions **[[CHECK]]** that form a parabola.

These new algorithms would need to not only thwart attacks by future quantum computers but also run on servers, phones, and smaller industrial internet devices without slowing performance, Moody notes. Whereas current RSA and elliptical curve keys contain 200 to 300 bits, post-quantum algorithms could contain 1,000 to 2,000 bytes. "Some of these internet protocols are going to have to deal with much larger key sizes," says Moody. "It's likely they won't be immediate drop-in."

Businesses can prepare now by becoming knowledgeable about the latest developments in post-quantum cryptography and conducting a “quantum risk assessment” that looks at which public and symmetric key algorithms their company uses which would potentially need to be replaced, says Moody. He also recommends companies start evaluating products with quantum-safe features and asking their technology vendors about awareness and plans, but eschew development of their own quantum-safe algorithms until industry standards are defined. Businesses should also make sure a manager is responsible for quantum security plans and the CEO is aware.

Oracle, in addition to attending conferences and commenting on **[[CHECK]]** NIST’s post-quantum program, has funded research to identify business software applications that could benefit from quantum-computing speedups.