Quantum Computing and Cryptography
Why You Need to Pay Attention
Table of Contents

Quantum Computing Basics .................................................. 3
VMware Perspective ................................................................. 4
  Can quantum computers be built – at interesting scales? ........ 4
  What technologies are being used to build quantum computers? 5
  What is quantum supremacy? ................................................. 6
  How much better could quantum computers be – and on what types of problems? 6
  Are there problems and/or algorithms where quantum computers could do better than $\sqrt{N}$ speedup? ........... 7
  What are the implications for cryptography? ......................... 9
  Are there quantum-resistant crypto schemes? ....................... 10
Recommendations: What actions should you take now? .......... 11
Conclusion .................................................................................. 12
Quantum Computing may allow scientists to solve some very complex problems, such as the atomic scale modeling of chemical processes – but it may also increase the vulnerability of certain types of cryptography that our industry relies on. As the race to build quantum computer prototypes intensifies, VMware is taking early steps to prepare for the transition to new crypto schemes that are resistant to such attacks.

Why should we start now even before we know if quantum computers of a useful scale will be a reality – let alone when that will happen and what the new crypto standards will be? We need to start now because crypto transitions are lengthy.

If we wait for all the answers, we will be too late.
Quantum Computing Basics

Quantum computing (QC) builds on the quantum mechanical view of atomic-scale systems and especially on three of its properties:\(^1\):

- The description of nature is essentially probabilistic.
- It is not possible to know the values of all of the properties of a system at the same time. Those properties that are not known with precision must be described by probabilities.
- Measuring devices are essentially classical devices and measure classical properties.

In classical computing, we compute on bits that are either zero or one. That means that a register of \( n \) bits can represent one of \( 2^n \) values. For example, a 3-bit register can have one of eight values: 000, 001, 010, 011, 100, 101, 110 or 111.

In quantum computing, information is stored and manipulated in qubits that exist in a continuum representing the probabilities of being zero or one (until they are measured or otherwise disrupted). A register of \( n \) qubits that are entangled with each other can represent \( 2^n \) distinct probability distributions. For example, a 3-qubit register can simultaneously model the probabilities of each of the eight states that a 3-bit classical register could represent.

So, in some limited respects, the quantum register is \( 2^n \) times more expressive than the classical register. In the earliest days of quantum computing this generated considerable excitement with some pundits erroneously suggesting that one could solve complex puzzles that have \( 2^n \) possible answers by simultaneously testing all of the answers and magically selecting the right one.

---

\(^1\) These are simplified/paraphrased from the so-called Copenhagen interpretation.
For example, a crypto challenge could be solved by trying all of the possible keys. It would have meant that a quantum computer could perform $2^n$ computations using the same number of operations (though these would be quantum operations) used by a classical computer performing a single computation.

The catch, of course, comes from the second and third of the quantum mechanical properties. When we measure the state of a qubit it will collapse to a classical value. For example, in the case of our 3-qubit register, we will only be able to extract one of the eight classical values, which is far less exciting than some had hoped.

On the positive side, the probability of any one value being extracted is determined by the qubit’s quantum state just prior to being measured. That is still quite exciting from a computational (and crypto) perspective since we can perform a series of quantum computational steps on the register prior to measuring it. If we are clever in how we go about things, then we can take on some interesting challenges.

VMware Perspective

Can quantum computers be built – at interesting scales?

Although we don’t yet know for sure, things look very promising. The really interesting scale for practical problems is believed to be ~2000 qubits. After two decades of slow progress, the pace has sped up tremendously over the past few years with researchers claiming to have hit the 50-qubit milestone in late 2017 and 70-qubit chips being announced only a few months later.

The challenge in building practical QCs is noise, which, amongst other things, causes qubits to lose their coherence, i.e., their state collapses. So, one challenge is to build qubits that retain their coherence for long enough to perform a useful number of operations on them with an acceptably low rate of errors. Another challenge is to build entangled qubits/registers in which noise doesn’t scale linearly (or worse) with the number of qubits.

On the optimistic side, it is theoretically possible to apply error correction schemes to quantum computing. So, the challenge is not to eliminate noise/errors, but to get the error rate small enough that the gain from error correction is less than its cost.

On the pessimistic side, some argue that real-world physics will preclude the realization of quantum computers, i.e., that physics at the atomic scale is fundamentally too noisy, even in the presence of error correcting schemes. This argument has been losing credibility, especially now that the 50-qubit milestone has been attained, but it is still possible that researchers will run into the atomic scale equivalent of a brick wall. Even if that happens, the technologies being developed may be useful to implement the quantum equivalent of the analog computers that were developed in the 1950’s and 1960’s, i.e., systems that could be configured to perform a wide range of simulations in the analog domain.

**What technologies are being used to build quantum computers?**

For a long time to come, QCs are likely to be custom accelerators attached to classical computers, in much the same way that floating point and graphics processors were initially introduced. Furthermore, a number of QC hardware developers are deploying their systems as cloud-based offerings, making them accessible to a wide range of users.

Since all forms of matter (and interactions with light/energy) exhibit quantum behavior at an atomic scale, many types of materials and approaches are being pursued, including:

- **SUPERCONDUCTING MATERIALS**
  Used to create customized chips that are cooled to millikelvin temperatures. This is the most promising near-term approach since it leverages traditional semiconductor manufacturing.

- **QUANTUM DOTS**
  Can also leverage silicon-based manufacturing.

- **TOPOLOGICAL QUBITS**
  Believed to be fundamentally more resistant to noise.

- **TRAPPED IONS**
  Single electrons and photons.

- **QUANTUM ANNEALING**
  The use of quantum properties to search for the global minimum of a function. This approach may be more akin to analog computation than those above.
What is quantum supremacy?

Supremacy is the term used to express the notion that a QC should be able to compute everything that a classical computer can, and also be able to solve problems that are not practical for classical computers, e.g., by requiring far fewer operations. Such a QC is at least as good in all cases and much better in some. In the very near term, researchers hope to use ~70 qubit prototypes to “bring evidence” that their work is on the path to quantum supremacy. Of course, this only speaks to the number of operations and not their cost or speed, i.e., it might never be the case that a quantum computer will economically outperform a classical computer on the problems that are already within our reach today.

How much better could quantum computers be – and on what types of problems?

Although QC’s are not the nirvana some once hoped, the development of a handful of key algorithms makes it clear that, if ~2000 qubit QC’s can be built, they will allow us to take on problems that are beyond the reach of classical computers. One class of applications that is of this scale is the atomic (or sub-atomic) simulation/modeling of physical systems, e.g., in chemical engineering and materials science. QC’s may also be used to take on problems related to virtual phenomena, for example high fidelity modeling of financial systems/economies or the training of extremely large Deep Neural Networks (DNN’s).

One QC algorithm with broad applicability is Grover’s algorithm, which is loosely related to searching a database (or table) of \( n \) entries for a single entry that matches a key. A classical computer, which must check every entry, will require on the order of \( n \) steps. Of course, if we had the mythical computer some had hoped for, we would be able to check all of the entries in parallel, i.e., in a single step. While not as magical, a QC using Grover’s algorithm can complete the search in \( \sqrt{n} \) steps which, for large \( n \) is an enormous improvement. Better yet, a wide range of interesting problems can be transformed into problems addressable through this algorithm.

\[
\sum_{x_i} |x_i\rangle
\]

\[\begin{align*}
    \text{Oracle:} & \quad -\alpha_m |x_m\rangle + \alpha_b \sum_{x_i \neq x_m} |x_i\rangle \\
    \text{Amplification:} & \quad (2A + \alpha_m) |x_m\rangle + (2A - \alpha_m) \sum_{x_i \neq x_m} |x_i\rangle \\
    \text{repeat } \theta(\sqrt{n}) \text{ times}
\end{align*}\]

Grover diffusion operator applied \( k \) times, each iteration moving \( 1/\sqrt{n} \) amplitude.

---

Figgatt et al., Complete 3-Qubit Grover Search on a Programmable Quantum Computer.
To put the benefit of $\sqrt{n}$ speedup in perspective, brute force search of a table with a billion entries would take order $2^{30}$ steps with a classical computer, but only $2^{15}$ steps (plus error correction, etc.) with a quantum computer. Since today’s largest classical computers can undertake such searches, this example might not justify building a quantum computer. But what if the problem is a “little” bigger, e.g., a table with $2^{64}$ entries? Brute force attacks on problems of that scale are well beyond the reach of classical computers, making quantum computers attractive even if they are burdened with a high cost and latency per operation.

Something to keep in mind though is that brute force isn’t usually required to search large tables, i.e., we typically find that they are sparse in ways that classical systems can leverage and/or that heuristics can be used to wrangle them down to a manageable size. Similarly, although training extremely large deep neural nets (DNN’s) might someday exceed the capacity of classical computation, researchers are finding ways to prune those networks to reduce the degree of computation that is required.

Are there problems and/or algorithms where quantum computers could do better than $\sqrt{n}$ speedup?

Yes, there are. In a remarkable irony of nature, one such algorithm addresses factoring, a problem that has been so highly resistant to attack by classical algorithms that it is the basis for public key cryptography. Shor’s algorithm can be used to factor an integer $n$, which can be represented with $\log(n)$ bits, using on the order of $\log(n)^2$ quantum operations. This is amazingly better than the best known classical factoring algorithms which require an (almost) exponential number of operations.

To gain some intuition around Shor’s algorithm, let’s go back to thinking about the mythical quantum computer that could solve factoring problems by simultaneously trying all of the possible answers. The catch precluding its realization is that, prior to measurement, the answers would all be superimposed on (and entangled with) each other within the $\log(n)$-qubit registers, i.e., they would all be screaming out for attention at the time of collapse and we would be unlikely to measure the “right” answer.
But what if we could apply quantum operations in some way that causes the answers that are not “right” to cancel each other out – thereby increasing the probability of the “right” answer being revealed by our measurement? It turns out that the Quantum Fourier Transform (QFT) algorithm can do just that for certain types of problems, i.e., those that have an underlying periodicity to them.

Shor found enough structure in the factoring problem to effectively reduce it to solving such a problem. The QFT does not solve the factoring problem in its entirety, but reduces it to a point where a more tractable, though still large, number of “educated guesses” can be applied to find the answer. So, in theory, a combination of quantum and classical computing can be used to achieve a dramatic reduction in the complexity of factoring.

If Shor’s algorithm can slay the factoring dragon and Grover’s algorithm can yield quadratic gains at large, then there is cause to hope (or fear, depending on one’s perspective) that other quantum algorithms of equal importance remain to be discovered. On the other hand, those algorithms were discovered in 1994 and 1996, respectively, and remain the high water marks of the space. While 20 years is the blink of an eye in terms of mathematics, the sparseness of high-impact results is disconcerting to many quantum computing advocates.

What are the implications for cryptography?

Asymmetric cryptography systems, e.g., public keys systems such as RSA that are a cornerstone of web commerce, may be subject to attack by future quantum computers of ~2000 qubits. Their security depends on the difficulty of solving mathematical problems, such as integer factorization or computing discrete logarithms, that are very hard for classical computers but that are vulnerable to Shor’s algorithm.

Symmetric/shared key cryptographic schemes, such as AES, and hashing/signature schemes, such as SHA, are also at risk, though from a different source. They are not vulnerable to Shor’s algorithm but Grover’s algorithm still poses a challenge. Although Grover’s $\sqrt{n}$ speedup is huge for most problems, crypto systems can offset that speedup by doubling the length of their keys (which squares the number of operations required). Reconfiguring existing symmetric key systems in this way is an inconvenience but not out of reach. With sufficient and timely investment, shared key systems with longer keys may be made safe until QCs with very large numbers of qubits can be built – or a quantum algorithm that creates new vulnerabilities is discovered. Nonetheless, finding and addressing all of the places where these schemes are in use will be a significant challenge.

The NSA has provided guidance related to the near-term evolution of cryptographic systems. For symmetric systems, the guidance amounts to recommendations around the use of longer keys. For asymmetric/public key systems, the guidance is also to adopt longer keys, but with the caveat that this is only a stop-gap measure to counter early generations of quantum computers. Those systems will eventually need to be replaced.

Are there quantum-resistant crypto schemes?

Yes. Some approaches to asymmetric/public key encryption are believed to be fundamentally resistant to speedups enabled by quantum computing. Researchers are working diligently to reduce these mathematical approaches to practical algorithms that can replace RSA. Parallel work, led by the National Institute of Standards and Technology (NIST), has begun to select amongst them and create new crypto standards. Work in this space is sometimes referred to as *post-quantum cryptography*.

An outstanding question is how enduringly hard the mathematical problems underlying the new standards will prove to be, i.e., could a scheme believed to be quantum-resistant suddenly come under attack as a result of an algorithmic discovery? When factoring was chosen as the basis for RSA, it represented a problem that had been worked on for hundreds of years. That provided empirical reasons to believe that the problem was hard and that the pace of improvement would be slow. It is not yet clear what the basis will be for claiming that a new standard will have similar endurance. It is entirely possible that the initial post-quantum standards will not be nearly as long-lived as RSA has been.

Major families of post quantum cryptography under consideration for new NIST standards.
Recommendations:
What actions should you take now?

Quantum computers capable of cracking classical cryptography are not believed to be in use today. It is quite possible, however, that they will come into use in the next 5-10 years and that some of them will be made widely available via cloud-based services.

Given that migration to new crypto schemes can take over a decade, customers should not sit idle while the standards process works its way to completion. Now is the time for VMware, its partners, and its customers to begin work on quantum readiness by:

• Creating an inventory of cryptography and hashing algorithms/libraries used in your services.

• Instituting a timetable for the adoption of the NSA’s interim guidance regarding key lengths and hash function output sizes.

• Incorporating crypto agility into services, i.e., the ability to update the crypto algorithms, protocols, and key lengths used by deployed software.

• Investigating the modernization and crypto agility plans of the suppliers of third party and/or open source software.

• Taking steps to ensure that access to long term customer data (e.g., archival backups, medical records, other data-at-rest, etc.) cannot be obtained by a patient adversary who collects encrypted data/traffic today with an eye to using QCs to decrypt it in the future.

VMware has recently launched a quantum readiness initiative, which we are in the process of extending to other industry players including, of course, members of the Dell Technologies family, such as RSA.
Conclusion

There has been a dramatic acceleration in the rate of progress towards the realization of quantum computers which, in turn, has implications for cryptography.

Given the lengthy lead time associated with crypto migration, customers should start now on their journey to quantum readiness. It is especially important to start now on transitioning your software to be crypto agile so that it will be easier to substitute new crypto algorithms in the future.

VMware has initiated its own internal quantum readiness effort and is partnering with other industry players to create readiness roadmaps, tools, etc. We are living in interesting times!