Quantum Heists and the Future of Digital Privacy

Cameron Myers

November 7 2023

Ever since the inception of the idea of quantum computing, its potential in the minds of the public grew to legendary heights. This is not unfounded, as the impressive capabilities of quantum computing is in fact astounding, but the main source of concern is its capability to break modern encryption and thus leak everyone's embarrassing internet secrets. Almost as concerning is the possibility of many fraudulent charges on your bank account every time you use your credit card, as malicious actors would be able to use quantum computers to see any transaction and break the encryption used to protect your card information. In this paper I will discuss the prospects and perils of quantum computing and see just how safe your embarrassing Harry Potter fanfiction (and your credit card) is from the threat of quantum hackers.

First I will establish why quantum computing is a real threat to the future of digital privacy. Nearly all current encryption methods, such as RSA, are the same. Why? Because it's incredibly effective. Prime factors make up numbers, and creating very large numbers with prime factors is fairly easy. For example, take two relatively large prime numbers and multiply them together: $211 \times 67 = 14{,}137$. This is computationally trivial this way and can be done with a simple calculator, but if I were to reverse the process and ask, "what prime factors make 14,137?" the answer is not obvious. The best way our current computers have to solve this is to guess prime factors and multiply them together until

they get a match, making it a much more time consuming task of guess and check. This asymmetry is the basis of RSA encryption, which is the method used to protect most personal information currently, except they use numbers with hundreds of digits, rendering the factorization task virtually impossible with current classical computing power. In other words, it's a fast and simple algorithm that is currently very hard to break. However, quantum computers have extra capabilities that allow this process to be sped up significantly. This is done with an algorithm called Shor's Algorithm which can be used to great advantage using a property of qubits known as superposition.

Classical bits have two states: 1 or 0. When computing with qubits, superposition allows these bits to be both 1 *and* 0. In other words, a qubit could be 1 or 0 or anywhere in between. In its default state, it has a 50% chance of being determined 1 and 50% being 0. But how does this relate to factoring numbers? Let's explore this with an example using modular arithmetic. Lets take powers of 2: 2, 4, 8, 16, 32... and take them modulo 5 (I will denote this with normal fraction notation, as modulo is just the remainder of an operation of division) shown in the table 1. As you can see, these values are periodic. They repeat after intervals of 4, which is indicative of the prime factor 2 since other prime factors will have different periods (for example, the prime factor 11 would have a period of 1, as all powers of 11 mod 5 is 1). Qubits can take advantage of this fact since these periods give us clues on which number we could be working towards. This is where superposition comes in.

Take a single qubit, which can be represented as $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, where ψ is the "value" of the qubit and you can think of α as the "amount" that the qubit is 0 and β the "amount" it is 1. In the case of the default value mentioned earlier, this would make $\alpha = 0.5$ and $\beta = 0.5$, the constraint being that these coefficients must add to 1. So every time this system makes a calculation, it

uses information about that calculation to move these parameters closer to 0 or 1 using constructive and destructive interference across the wavefunction of all qubits. This means that it can process in different parts of the wavefunction simultaneously, or if you're into science fiction, across different parallel realities using the many worlds interpretation of quantum mechanics! This is a simplification of Shor's algorithm and how it works, but basically it can use information about its guesses, like these periodicities, to orchestrate interference across the full range of qubits to boost the probability of the correct outcome. If you're inclined to think like a classical computer, this would be kind of like an iterative algorithm, where each guess tunes the parameters for optimization, except the guessing and tuning are happening at the same time, in a sense. This algorithm can be used with classical computers, though the exponential growth of parallel processing required would make it obsolete, as it would be more efficient to just run a guess and check with the large numbers used for RSA encryption.

Now that we have established that quantum mechanics is overpowered, we should accept the fact that digital privacy will soon be a thing of the past. You may as well come clean and tell everyone about your dubious search history before the quantum bandits leak it to your friends and family... okay perhaps now I should discuss some of its shortcomings. The first is that qubits are very finicky and also hard to build. So your average person will not have access to these machines any time soon. Even if they did, current processes require many of the qubits be dedicated to error correction schemes, because qubits are very sensitive to their environment. Only the remaining qubits, called physical qubits, can be used for computation. As a result, current estimations on breaking 256-bit encryption within one day would require 13 million qubits![2] So rest easy as your secrets are safe. For now.

However, technology tends to advance quickly. Although the biggest uni-

Table 1: Powers of 2, modulo 5

Cycle	2^n	$= 2^n$	$2^n \bmod 5$	$= 2^n \bmod 5$
Cycle 1 (for $n = 1$ to 4)				
	2^1	2	$\frac{2}{5}$	2
	2^2	4	$\frac{4}{5}$	4
	2^3	8	$\frac{8}{5}$	3
	2^4	16	$\frac{16}{5}$	1
Cycle 2 (for $n = 5$ to 8)				
	2^5	32	$\frac{32}{5}$	2
	2^6	64	$\frac{64}{5}$	4
	2^7	128	$\frac{128}{5}$	3
	2^8	256	$\frac{256}{5}$	1
Cycle 3 (for $n = 9$ to 12)				
	2^9	512	$\frac{512}{5}$	2
	2^{10}	1024	$\frac{1024}{5}$	4
	2^{11}	2048	$\frac{2048}{5}$	3
	2^{12}	4096	$\frac{4096}{5}$	1

versal quantum computer is only just over 400 qubits, IBM plans to release its 1121-qubit chip within 2023. They collaborate with UC Berkeley and are quite confident that "quantum computers will soon surpass classical computers in practical tasks"[1]. Eventually, RSA encryption may no longer be effective. Thankfully there are many math wizards working on different encryption algorithms that will be resistant to quantum computing. The premise of this is simple, just create another algorithm that is easy to encode one way but difficult to decode that does not have an exploitative underlying pattern like the periodicity in RSA encryption. While this is quite easy, the difficulty lies in creating an encryption algorithm like this that doesn't require long keys (you can think of keys as the prime factors 67 and 211 from our first example). If the keys are not simple, then encryption takes a long time. This may seem trivial, but if you're texting your significant other and your message takes 5 minutes to encrypt and decrypt this process would make convenient text messages not so convenient. Plus, we all know how quickly your partner gets mad when you don't text them back within 5 minutes.

To conclude this discussion, I will quickly summarize my thoughts. Despite quantum mechanic's possible access to the multiverse, we are still able to keep its capability to break encryption at bay with advancements in encryption methods. We are not in immediate danger of RSA encryption being broken. By the time the technology catches up, we should be able to find an algorithm that is both resistant to quantum trickery and fairly simple to encrypt and decrypt data. Although quantum cryptography's capacity for superseding current security measures can not be ignored, we aren't in immediate danger and quantum resistant algorithms have time to be perfected. This means that your bank account and embarrassing emails will likely be secure by the time quantum computers are powerful enough to break current encryption protocols.

References

[1] Mohit Pandey. *IBM makes the best quantum computer open to public*. June 2023. URL: https://analyticsindiamag.com/ibm-makes-the-best-quantum-computer-open-to-public/#:~:text=IBM%20is%20set%20to%20release,Condor%20chip%2C%20later%20this%20year.&text=IBM%20in%20collaboration%20with%20UC,classical%20computers%20in%20practical%20tasks..

[2] Mark Webber et al. "The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime". In: *AVS Quantum Science* 4.1 (Jan. 2022), p. 013801. ISSN: 2639-0213. DOI: 10.1116/5.0073075. eprint: https://pubs.aip.org/avs/aqs/article-pdf/doi/10.1116/5.0073075/16493244/013801_1_online.pdf. URL: https://doi.org/10.1116/5.0073075.