Quantum Computing and its Implications on Digital Security*

Jakob Waibel
Stuttgart Media University, Stuttgart
(Dated: April 20, 2022)

Quantum computing has been gaining more and more relevance in recent times and is often rather seen as a threat than a blessing by society. This paper aims to inform readers about the topic on a high-level to be able to join the discussion about the future relevance of quantum computing. First, this paper will explain the basics of quantum computing and dive into types of quantum computers including ion traps, nuclear magnetic resonance quantum computers and quantum computers based on Josephson junctions. Afterwards, the effects of quantum computing algorithms, especially Shor's and Grover's algorithm on current security mechanisms are discussed, rounding off by explaining approaches on how to achieve post quantum security.

I. INTRODUCTION

Since Paul Benioffs and Richard Feynman's talks on quantum computing held at the first conference on the physics of computation, quantum computing has become a large research area. Quantum computing has become even so large, that it has become more and more difficult to understand the basics of it and its implications on the future of computing. This work will introduce the reader to the basics of quantum computing from a computer scientists perspective. Hence it is important to look at the implications on digital security, especially cryptography.

II. RELATED WORK

Prashant writes about the limitations of classical computers and how quantum computers can be realized [11]. Their explanations on different realizations of quantum computers introduce the reader to several related research areas on a high level.

Bone and Castro provide examples of the workings of Shor's and Grover's algorithm in their overview of quantum computing [2].

Vedral and Planio explain ion trap quantum computers in their paper about the fundamentals of quantum computing [14].

Martinis and Osborne write about Josephson junctions [7] and how the Josephson effect can be used to create a quantum computer utilizing superconductors.

Mavroeidis et al. introduce the reader to present cryptography algorithms, how they are vulnerable to quantum computers and their main topic, post quantum security [9].

The largest number factorized on a quantum computer so far using Shor's algorithm was the number 21. Martìn-Lòpez et al. write about how they achieved this breakthrough in their paper [8].

Micciancio and Regev introduce the topic of lattice-based cryptography [10], which is believed to be a post-quantum secure method by multiplying matrices instead of primes.

III. QUANTUM COMPUTERS

Quantum computers utilize qubits to represent information. Instead of working with classical bits representing 1s and 0s, quantum computers utilize qubits, which can represent various combinations of 1s and 0s at the same time. This effect of qubits representing multiple states at the same time is called superposition. To put qubits into superposition, researchers manipulate qubits in different ways. As quantum computing is based on quantum mechanics and hence has to obey to the same laws, a measurement determines the state of a qubit. Once qubits are measured, their quantum state immediately collapses to either 1 or 0 and its state of superposition is lost.

Quantum entanglement is a phenomenon which causes particles to link so that their state cannot be described independently anymore. This results in those entangled qubits having a similar quantum state at all times. If the state of one of those entangled qubits changes, the other one will instantaneously change its state as well. This improves the processing speed of quantum computers. As Alamira Jouman Hajjar puts it in her Article on AIMultiple [1], one qubit will reveal information about all the qubits said qubit is entangled with. This entanglement allows quantum computers to increase their computational power exponentially, rather than linearly as regular computers. According to an article in IEEE Spectrum [13], a quantum computer equipped with 300 qubits could represent more states than there are atoms in the observable universe.

The quantum behaviour of qubits is determined to decay. This effect is known as the scientific term "decoherence". It describes the quantum state as being extremely fragile. The slightest disturbance can cause a qubit to collapse and hence lose its state of superposition. These disturbances can be caused by vibrations, change of temperatures or related external influences. Disturbances are

*Electronic address: mail@jakobwaibel.com

also referred to as "noise" in quantum computer terminology. Decoherence is the reason why qubits are held in extremly protected environments, often refrigerators or vacuum chambers. To compensate for noise, thousands of standard qubits will be needed to create a reliable qubit, referred to as a "logical" qubit. A logical qubit has a long enough coherence time to be used for quantum logic gates. Essentially, logical qubits are a group of regular qubits referred to as a singular qubit in computation, which have more stable characteristics than regular qubits.

To get a sense of how far development of quantum computers has come, according to Siobhan Roberts in MIT Technology Review [12], the most qubits used in a quantum computer, as of November 17, 2021 are 256 regular qubits in a quantum computer by the Boston startup QuEra Computing.

Since the first proposals revolving around quantum computers by Yuri Manin in 1980 and Richard Feynman in 1981, the term "quantum supremacy" is used to denote the point at which a quantum computer can complete a mathematical calculation that is beyond reach of even the most powerful supercomputers. It is unclear how many qubits will be needed to achieve superposition. This results from the fact that research results in new algorihtms and hardware improvements to boost the performance of classical (super)computers.

Potential applications for quantum computers exceed cryptography. Some potential applications include the simulation of quantum systems, machine learning, computational biology, generative chemistry and optimization problems.

IV. REALIZATIONS OF QUANTUM COMPUTERS

There are different approaches on how to realize machines utilizing quantum effects for computing known as quantum computers. Those different approaches have different advantantages and challenges. Some of those realizations, especially the ones important with regards to digital security, are summarized in the following:

A. Ion Traps

Vedral and Plenio describe the workings of the ion trap in their paper [14, p.12-13] as follows. They state that the ion trap quantum computer represents qubits in energy states and in vibrational modes between ions. In a linear ion trap, currents in electrodes generate a time dependent electric field. Ions then move through this potential and for some currents and ion masses, the ions get trapped in the field. The equilibrium is caused by the force from the electric field generated by the electrodes and the electrostatic repulsion of the ions. The ions form a string seperated by only a few wavelengths of light. The distance of a few wavelengths is sufficient to operate each ion with a different laser. A challenge the researchers are faced with when trying to realize an ion trap is the mechanical degree of freedom the ions have. In general, the ions are trapped at their position but they are in fact not resting but oscillating around their equilibrium position. The ions then get cooled by using laser cooling to reduce the movement of the ions in their current position. This process is able to cool down the ions near 0 Kelvin. At this point, the only movement left would be the movement caused by the quantum mechanical uncertainty priciple. So far, it is not possible to cool a whole string of ions to near 0 Kelvin, although several attempts cooling down a single ion and two ions succeeded.

As mentioned by Prashant in his paper [11, p.20], it has been possible to evaluate Fourier transforms using the ion trap quantum computer. This achievment lead to Shor's factoring algorithm, which is based on performing Fourier transforms.

In 2018, Nicolai Friis et al. controllably entangled 20 trapped ions as they describe in their paper [4].

B. Nuclear Magnetic Resonance

As explained in the article by Gershenfeld [5, p.66-71], a nuclear magnetic resonance (NMR) quantum computer consists of a capsule filled with a liquid and a nuclear magnetic resonance spectrometer which is a machine used to analyze the molecular structure of a material by measuring the interaction of nuclear spins when placed in a strong magnetic field. Each molecule in the liquid represents a quantum memory register. NMR based quantum computers can compute by sending radio signals to the sample using the NMR machine and evaluating the response. In an NMR quantum computer, qubits are represented as spin states of the atoms in the molecules. In contrast to the ion trap quantum computer, a measurement is performed on a statistical ensemble of molecules instead of a single isolated one.

Initially, as mentioned above, the NMR based quantum computer used atoms in a liquid sample as qubits which is known as liquid state NMR (LSNMR). Since solid state NMRs (SSNMR) emerged, SSNMR is usually preferred in terms of performing quantum computation.

Solid state NMRs differ from LSNMRs in that SSNMRs provide a sample in solid state. This has many advantages such as being able to work using lower temperatures as well as the more precise localization of qubits using crystal structures. In SSNMRs, qubits can be measured individually, same as in the ion trap, instead of having to measure an ensemble of molecules as in LSNMRs.

NMRs have been succesfully used in quantum computing, as they can solve non-polynomial problems in a polynomial time. According to Gershenfeld [5, p.69], the first successful computation on a NMR quantum com-

puter was to execute a search using Grover's algorithm, which will be covered in the respective chapter.

C. Josephson Junctions

As Martinis and Osborne explain in their paper [7, p.3-6], the Josephson effect is a phenomenon that occurs when two superconductors are seperated by some barrier or restriction between them, which is thin enough that electrons can tunnel through the barrier using quantum-mechanics. This tunneling produces a current, known as supercurrent, that flows continuosly without any voltage applied. Said current is used to create a non-linear inductance. Wendin and Shumeiko mention [15, p.727] many ways to realize qubits in quantum computers based on Josephson junctions. The simplest of which is to realize qubits in Josepshon junctions by comparing energy levels of josepshon energy to the normal charging energy. The Josephson energy is the kinetic energy of tunneling electrons in the system.

Martinis and Osborne state [7, p.3] that Josephson junction quantum computers are especially interesting because superconductors could provide long coherence times and because increasing the number of qubits should be straightforward.

Qubits in Josephson junction quantum computers are controlled electrically which results in them being interesting for future developments.

V. CHALLENGES IN QUANTUM COMPUTING

As of 2021, there are some challenges researchers face in the current state of quantum computing which can be derived from the earlier sections:

- Often, as e.g. in the Josephson junction quantum computer, extremely low temperatures are required. These have to be achieved at a reasonable cost. Using e.g. laser cooling is one approach in quantum computing. The concept of laser cooling was proposed by Steven Chu, Claude-Cohen-Tannoudji and William D. Phillips who got awarded the Nobel prize for their research in the develoment of methods to cool and trap atoms with laser light.

- Quantum algorithms have probabilistic characteristics. This implies that in a single operation a quantum computer returns multiple solutions, each of those solutions with an assigned probability, where only one can be correct. Figuring out the correct answer reduces the potential speed of quantum computers.

- Qubits are prone to errors earlier introduced as noise. Noise can be caused e.g. by heat or noise in the environment. As in classical computing, noise can lead to bit-flips. There are approaches in "quantum error correction" to deal with these errors. One of those approaches is to use the "bit flip code" in which a total of 3 qubits are needed to result in 1 correct bit using quantum entanglement.

- Increasing the number of qubits in a processor is fundamental. The more qubits in a processor, the more logical qubits can be used. More qubits also lead to less errors since methods for error correction can be used more effectively.

- Decoherence leads to qubits retaining their quantum state only for a short period of time. According to Mavroeidis [9, p.3] The longest time qubits remained in superposition so far was set by Australian researchers at the University of New South Wales. Their qubits remained in superposition for a total of 35 seconds.

VI. QUANTUM COMPUTING ALGORITHMS AND THEIR EFFECTS ON CURRENT SECURITY MECHANISMS

As discussed earlier, quantum computers could eventually reach the state of quantum superiority, in which the quantum computer can perform tasks no regular computer could ever compute. This implies that the quantum computer could also solve problems which a regular computer could not solve so far. Some of the problems that can be solved and which security mechanisms are affected will be discussed in this following section.

A. Shor's algorithm

Shor's algorithm is a quantum computer algorithm developed by Peter Shor in 1994. Essentially, it can find the prime factors of an integer in the complexity class BQP, which is defined as the class of decision problems solvable by a quantum computer in polynomial time with an error probability of at most $\frac{1}{3}$ for all instances. Shor's algorithm is nearly exponentially faster than the general number field sieve, which is the most efficient known classical factoring algorithm. The efficiency of the quantum Fourier transform which, as earlier discussed, can be caluclated using e.g. an ion trap quantum computer, is responsible for the efficiency of Shor's algorithm. The algorithm is generally capable to break current public-key cryptography mechanisms as RSA or the Diffie-Hellman key exchange if the quantum computer could operate with little noise. That these algorithms could be vulnerable was already stated by Kirsch in 2015 [6, p.6].

Bone and Castro [2, p.6-9] describe the workings of Shor's algorithm as follows. First, a memory register is placed into a superposition of all its possible states. Think of all possible permutations of n bits existing in parallel. A calculation performed with Shor's algorithm

can be thought of as computations done in parallel for every permutation generated before. They then describe the mathematics performed on the registers:

- N describes the integer to be factorized
- X is a random number in range $1 < X < N - 1$
- X is raised to one of the permutations generated earlier.
- The remainder of this operation is placed in a second register. The first register contains the permutation.

After performing these operations on all permutations, it is noticable that the contents of the second register repeat e.g. for $N = 15$ the repeating sequence would be $1, 2, 4, 8, 1, 2, 4....$ Now the frequency of repetition can be calculated by using a complex operation on the second register and looking at the contents which causes the results from every permutation to interfere. A possible prime factor can then be calculated by using the frequency of repetition f:

$$FactorP = X^{\frac{f}{2}} - 1 \tag{1}$$

The interference that provides f will lead to the correct answer with a high probability as incorrect answers cancel each other out when interfering. This cannot be guaranteed. Checking that the resulting number is correct can be achieved by performing a simple multiplication. Repeating the process for different random values X has then a high chance of revealing all prime factors.

So far, the largest number factorized using Shor's algorithm is the number 21 factored back in 2012 by Martín-López et al. [8]. The integer 35 was attempted in 2019 on an IBM Q System One, but the algorithm failed.

B. Grover's algorithm

Grover's algorithm, devised by Lov Grover in 1996, refers to a quantum algorithm for performing unstructered search. The analogous problem in classical computing has $O(N)$ complexity. Grover's algorithm achieves the same goal in $O(\sqrt{N})$. In contrast to Shor's algorithm providing exponential speedup, Grover's algorithm only provides quadratic speedup.

As Mavroeidis et al. [9, p.4] state in their paper, Grover's algorithm can be utilized to find a collision in a hash function in $O(\sqrt{N})$ as searching for a collision is comparable to performing an unsorted search. Additionally, Grover's algorithm can be used to improve a lot of brute-force attacks targeting symmetric cryptography. Brassard proved [3] that it is possible to combine Grover's algorithm with the birthday paradox, also known as a quantum birthday attack, which leads to finding collisions with a complexity of $O(N^{\frac{1}{3}})$. As a result, many of current, rather weak, hashing algorithms are disqualified for use in the quantum era. However, as of 2021, both SHA-2 and SHA-3 with longer outputs remain quantum resistant as even Grover's algorithm does not make it feasible to find a collision when the keys are too long.

VII. POST QUANTUM CRYPTOGRAPHY

Post Quantum Cryptography describes algorithms that are secure against quantum computing and conventional computers. To make sure that an algorithm is quantum secure, there are generally two approaches:

A. Improve Current Security Mechanisms

Improving current security mechanisms by increasing the key length from 128 bits to 256 bits squares the number of possible permutations a quantum computer has to search using Grover's algorithm. The speedup Grover's algorithm provdides is not efficient enough to crack this key in a feasible amount of time.

B. Developing Quantum Secure Algorithms

Another approach would be to develop new algorithms using more complex trapdoor functions even quantum computers could not possibly crack in a feasible amount of time. Researchers are working in areas like lattice-based cryptography, supersingular isogeny key exchange or hash-based cryptography. One of these approaches is described in the following:

1. Lattice-based Cryptography

Lattice-based Cryptography is a form of public-key cryptography that avoids the weaknesses of RSA and related security mechanisms. Rather than multiplying primes, lattice-based encryption schemes involve multiplying matrices. As Micciancio and Regev mention in their paper [10, p.2], lattice-based cryptographic mechanisms are based on the presumed hardness of lattice problems. It is belived but not proven that lattice-based cryptography cannot be cracked by a quantum computer since the frequency finding technique, which is used in Shor's algorithm, cannot be used in lattice-based problems.

VIII. CONCLUSION

As described before, Shor's algorithm, as well as Grover's algorithm will presumably force computer scientists to improve current standards to provide information security across areas. The second approach mentioned in this paper is developing new, quantum-secure

algorithms, like lattice-based cryptography. Even the speedups quantum-computers provide do not make it feasible to crack these algorithms. It is not known yet, which type of quantum computer will prevail. Ion traps, Nuclear Magnetic Resonance and Josepshon junctions are some of the most promising approaches. In current systems like the IBM Q System One, Josephson junctions are used in their superconducting quantum computer. If this approach will prevail is unclear, since quantum entanglement in this type of processor is not possible as of 2021. Quantum computers, as current records depict, are not powerful enough to form a threat to security mechanisms by now, since way more qubits are needed to perform operations on large enough numbers and preserve the state of superposition long enough. To conclude, it should be said that quantum computing should be seen as an opportunity for overdue improvement, not as a threat to digital security.

[1] AIMultiple. Quantum entanglement: What it is & why it is important. `https://research.aimultiple.com/quantum-computing-entanglement/`, 2021.

[2] Bone and Castro. A brief history of quantum computing. 2017.

[3] Brassard, HØyer, and Tapp. Quantum cryptanalysis of hash and claw-free functions. *Lecture Notes in Computer Science*, page 163–169, 1998.

[4] Nicolai Friis, Oliver Marty, Christine Maier, Cornelius Hempel, Milan Holzäpfel, Petar Jurcevic, Martin B. Plenio, Marcus Huber, Christian Roos, Rainer Blatt, and Ben Lanyon. Observation of entangled states of a fully controlled 20-qubit system. *Phys. Rev. X*, 2018.

[5] Gershenfeld and Chuang. Quantum computing with molecules. *Scientific American*, 278:66–71, 1998.

[6] Kirsch and Chow. Quantum computing: The risk to existing encryption methods. 2015.

[7] Martinis and Osborne. Superconducting qubits and the physics of josephson junctions. 2004.

[8] Martín-López, Laing, Lawson, Alvarez, Zhou, and O'Brien. Experimental realisation of shor's quantum factoring algorithm using qubit recycling. *Nature Photonics*, 2011.

[9] Mavroeidis, Vishi, Zych, and Jøsang. The impact of quantum computing on present cryptography. *CoRR*, 2018.

[10] Micciancio and Regev. Lattice-based cryptography. 2009.

[11] Prashant. A study on the basics of quantum computing. 2005.

[12] MIT Technology Review. This new startup has built a record-breaking 256-qubit quantum computer. `https://www.technologyreview.com/2021/11/17/1040243/quantum-computer-256-bit-startup/`, 2021.

[13] IEEE Spectrum. How many qubits are needed for quantum supremacy? `https://spectrum.ieee.org/qubit-supremacy`, 2020.

[14] Vedral and Plenio. Basics of quantum computation. *Progress in Quantum Electronics*, 22(1):1–39, Jan 2008.

[15] Wendin and Shumeiko. Quantum bits with josephson junctions. *Fizika Nizkikh Temperatur (Kharkov)*, pages 957–981, 2007.