Quantum Computing and Its Effect on Cryptography

Ahmed Muharram, King Fahd Model Language School

Abstract

Programmable computers have been around for more than 7 decades. They have almost reached their maximum potential because computer parts are becoming too small. More than two decades ago, researchers theorized the first quantum computer: a computer that uses different mechanics than digital computers and is way faster than them. This unimaginable power might lead to breaking current cryptography algorithms, which led researchers and field experts to work on new post-quantum cryptography algorithms to counter quantum computers' ability.

I. Introduction

The first freely programmable computer was created by German Konrad Zuse between 1936 and 1938 [1]. Later, ENIAC—or Electronic Numerical Integrator and Computer—was designed. ENIAC is the first programmable general-purpose digital computer ever created. It normally handled signed 10-digit numbers in the decimal system, but it was so well-constructed that it could handle operations with as many as 20 digits [2]. Less than 30 years later, in 1970, Intel introduced the first single-chip microprocessor, which had 2,600 manually placed transistors at 100 kHz [3]. Ever since, computers have evolved exponentially, getting smaller and more powerful rapidly. The number of atoms needed to represent a bit—short for binary digit—kept decreasing. Gordon Moore first observed this in 1965 and became known as Moore's Law: the power of computers doubles every year or two [4]. However, it has slowed down since then, and some industry and field experts say it does not apply anymore [5]. Now, Intel announced its Intel® Core™ i9-10900K Processor in 2020, which has 10 cores, 20 threads, and a max frequency of 5.3GHz [6]. However, computer parts are approaching sizes so small that our computers might reach their maximum potential [7].

II. How Modern Processors Work

1. CPU

A central processing unit (CPU) gives instructions that make up programs. It performs logic, arithmetic operations, input, and output. CPUs are generally composed of a memory unit consisting of ROM, RAM, Cache—, a Control Unit (CU), and an Arithmetic Logic Unit (ALU). These contain logic gates: electronic circuits that change one or more input to an output.

2. Logic Gates

There are 7 logic gates, and each has a different function: AND, OR, NOT, NAND, NOR, XOR, and XNOR.

i. AND gate:
The output of this logic gate is only true if both inputs are true. (fig. 1)

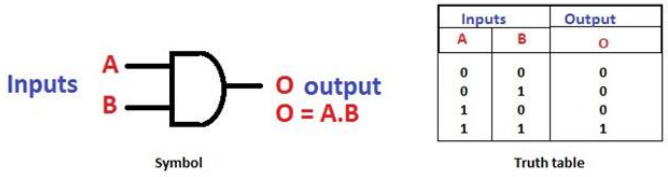
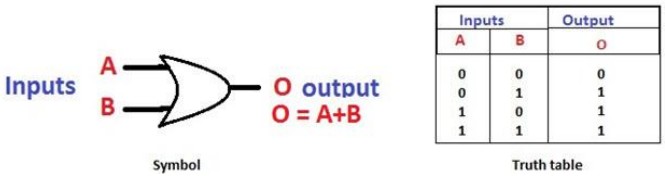


Figure 1: AND gate [8]

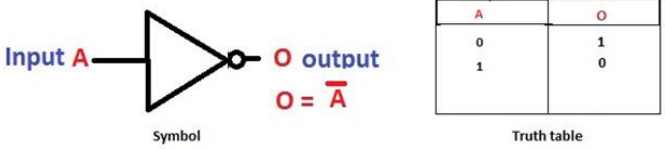
ii. OR gate:
The output of this logic gate is true if one or more inputs are true. (fig. 2)



Inputs		Output
A	B	O
0	0	0
0	1	1
1	0	1
1	1	1

Figure 2: OR gate [8]

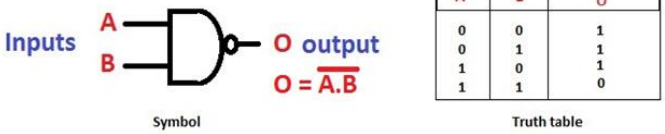
iii. NOT gate:
The output of this logic gate is the opposite of the input (for example, if the input is true, the output will be false). (fig. 3)



Inputs	Output
A	O
0	1
1	0

Figure 3: NOT gate [8]

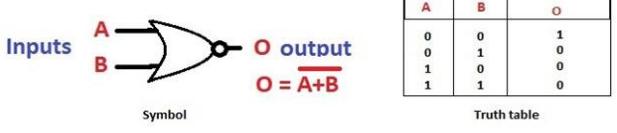
iv. NAND (NOT + AND) gate:
The output of this logic gate is the opposite of the output of the AND gate (for example, if one input is false and one is true and we use the AND gate, it will be false, but since we use NAND, it will be the opposite of false which is true). (fig. 4)



Inputs		Output
A	B	O
0	0	1
0	1	1
1	0	1
1	1	0

Figure 4: NAND gate [8]

v. NOR (NOT + OR) gate:
The output of this logic gate is the opposite of the output of the OR gate (for example, if one input is false and one is true and we use the OR gate, it will be true, but since we use NOR, it will be the opposite of true which is false). (fig. 5)



Inputs		Output
A	B	O
0	0	1
0	1	0
1	0	0
1	1	0

Figure 5: NOR gate [8]

vi. XOR (Exclusive + OR) gate:
The output of this logic gate is similar to the OR gate's output, except that if all of the inputs are true, it will be false. (fig. 6)

Inputs		Output
A	B	O
0	0	0
0	1	1
1	0	1
1	1	0

Figure 6: XOR gate [8]

vii. XNOR (Exclusive + NOR) gate:
The output of this logic gate is similar to the NOR gate's output, except that if all of the inputs are true, it will be true. (fig. 7) [8]

Inputs		Output
A	B	O
0	0	1
0	1	0
1	0	0
1	1	1

Figure 7: XNOR gate [8]

These logic gates are made by combining diodes, resistors, and transistors: semiconductor devices are considered one of the basic building blocks of modern electronics.

3. Transistors

CPUs can contain up to billions of transistors. A transistor can work either as an amplifier or as a switch:

i. As an amplifier, it transforms a weak electric current into a stronger current. This is not commonly used in computers.

ii. It can be switched on or off as a switch, storing two different numbers: zero and one—which stand for off and on respectively—to either block or allow information coming through. These numbers are called bits, which stands for binary digits, the smallest unit of information used in electronics.

Today, transistors are typically 14nm. For reference: Eukaryotic cells normally range between 10-100µm in diameter [9], or 714 to 7143 times larger than a transistor. This gives electrons the ability to penetrate the transistors' barriers, a phenomenon known as quantum tunneling. The smaller the size of transistors get, the easier it is for electrons to quantum tunnel (fig. 8) [10] [11].

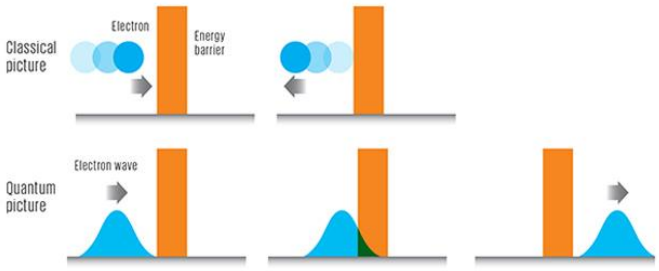


Figure 9: Quantum Tunneling [10]

III. Quantum Computing

In 1985, David Deutsch attempted to define a device that can efficiently simulate an arbitrary physical system. Because physics laws are ultimately quantum mechanical, he considered computing devices based upon quantum mechanics, which lead to our modern conception of a quantum computer [7]. A traditional digital computer uses bits in one of two states, on or off, 1 or 0, true or false. So, a 4-bit computer can hold any one of 16 (2^4) possible numbers (0000, 0001, 0010…1111).

However, quantum computers do not use bits. They use qubits or quantum bits (quantum binary digits). Qubits do not work the same as bits, they can be 0 or 1, but they can also be in proportions of each (between 0 and 1). This is what we call "superposition": a qubit cannot be defined as a specific value unless we measure it at a very specific point, that is, when it is either 0 or 1. A qubit can be any two-level quantum system: spin, magnetic field, or a single photon. A qubit, unlike bits, can be all these 16 possible numbers at once. This number grows exponentially with each qubit, where a 30-qubit computer would be comparable to a digital computer performing 10 trillion floating-point operations per second, or TFLOPS—comparable to our current supercomputers [12]. In 2020, IBM announced that they are working on a 1,121-qubit quantum computer and expect to finish in 2023 [13]. Quantum computers need only the square root of time required by standard computers to find something in a database. This is known as Grover's law ($O(\sqrt{n})$) [14]. In February 2021, China launched its first quantum computer operating system.

IV. Cryptography

Cryptography, which means "secret/hidden writing" in Greek, is a technique used nowadays to provide privacy for individuals and organizations at a high level. Billions of people use cryptography to protect data and information. It has evolved throughout the age, from Julius Caesar's Caesar cipher—where plaintext letters are replaced by other letters with a fixed shift number (fig. 9)—to today's block ciphers and hash functions [15].

V. How quantum computers might affect cryptography

Many IT security aspects rely on encryption and public-key cryptography, which are essential for business, e-commerce, protecting secret and confidential information. These are based on algorithms that are difficult to trick with modern computers and cannot be attacked by brute force like elliptic curve cryptosystems (ECCs) [16]. However, quantum computer algorithms like Shor's algorithm—a polynomial-time algorithm that can factor an integer—can heavily reduce the time required for computers to break these algorithms [17].

However, scientists are working on algorithms that can resist quantum computers, known as quantum-resistant algorithms, which post-quantum cryptography will depend on. In August 2015, the U.S. National Security Agency (NSA) declared its plan to turn to quantum-resistant algorithms. Later at PQCrypto 2016, a conference for post-quantum cryptography, NIST called for quantum-resistant schemes, leading the way to new public key standards. These efforts were later followed by SAFEcrypto, supported by the European Union Horizon 2020 project, and CryptoMathCREST,

supported by Japan Science and Technology Agency [16].

A	B	C	D	E	F	G	H	I	J	K	L	M
D	**I**	**Q**	**M**	**T**	**B**	**Z**	**S**	**Y**	**K**	**V**	**O**	**F**

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	**R**	**J**	**A**	**U**	**W**	**P**	**X**	**H**	**L**	**C**	**N**	**G**

Figure 10: Caesar Cipher [15]

VI. Conclusion

Quantum computers are the next technological step for humanity. Digital computers are reaching their maximum potential because of their very small size and Moore's law became almost obsolete. Although digital computers are enough for our daily life, quantum computers will be used for accurate and fast simulations important in many fields, drug development, space exploration, artificial intelligence, solving difficult problems, and many more. However, quantum computers can also be used in breaking algorithms and ruining IT security, but scientists and field experts are working on creating quantum-resistant algorithms.

VII. References

[1] K. Zuse, "Chapter 3," in The Computer - My Life, Springer, 1993, pp. 33–53.

[2] H. H. Goldstine and A. Goldstine, "The Electronic Numerical Integrator and Computer (ENIAC)," Mathematical Tables and Other Aids to Computation, vol. 2, no. 15, p. 97, 1946.

[3] F. Koushanfar, V. Prabhu, M. Potkonjak and J. M. Rabaey, "Processors for mobile applications," Proceedings 2000 International Conference on Computer Design, Austin, TX, USA, 2000, pp. 603-608, doi: 10.1109/ICCD.2000.878354.

[4] E. Mollick, "Establishing Moore's Law," IEEE Annals of the History of Computing, vol. 28, no. 3, pp. 62–75, 2006.

[5] E. Shein, "Moore's Law turns 55: Is it still relevant?," TechRepublic, 17-Apr-2020. [Online]. Available: https://www.techrepublic.com/article/moores-law-turns-55-is-it-still-relevant/. [Accessed: 10-Feb-2021].

[6] "Intel® Core™ i9-10900K Processor," Intel, 2020. [Online]. Available: https://www.intel.com/content/www/us/en/products/processors/core/i9-processors/i9-10900k.html. [Accessed: 06-Feb-2021].

[7] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, 10th Anniversary. Cambridge: Cambridge University Press, 2010.

[8] "Basic Logic Gates with Truth Tables - Digital Logic Circuits," ElProCus, 07-Dec-2020. [Online]. Available: https://www.elprocus.com/basic-logic-gates-with-truth-tables/. [Accessed: 05-Feb-2021].

[9] L. Bartee, W. Shriner, and C. Creech, "Comparing Prokaryotic and Eukaryotic Cells," Principles of Biology. [Online]. Available: https://openoregon.pressbooks.pub/mhccmajorsbio/chapter/comparing-prokaryotic-and-eukaryotic-cells/. [Accessed: 05-Feb-2021].

[10] A. Seabaugh, "The Tunneling Transistor," IEEE Spectrum: Technology, Engineering, and Science News, 30-Sep-2013. [Online]. Available: https://spectrum.ieee.org/semiconductors/devices/the-tunneling-transistor. [Accessed: 05-Feb-2021].

[11] R. G. Lerner and G. L. Trigg, "Tunneling," in Encyclopedia of physics, Weinheim: Wiley-VCH, 2005, p. 1308.

[12] W. C. Holton, "Quantum computer," Encyclopædia Britannica. [Online]. Available: https://www.britannica.com/technology/quantum-computer. [Accessed: 10-Feb-2021].

[13] J. Gambetta, "IBM's Roadmap For Scaling Quantum Technology," IBM Research Blog, 15-Sep-2020. [Online]. Available: https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/. [Accessed: 10-Feb-2021].

[14] L. K. Grover, "A fast quantum mechanical algorithm for database search," Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96, p. 212, Jul. 1996.

[15] A. M. Qadir and N. Varol, "A Review Paper on Cryptography," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 2019.

[16] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a Quantum World," IEEE Communications Magazine, vol. 55, no. 2, pp. 116–120, 2017.

[17] R. Stubbs, "Quantum Computing and its Impact on Cryptography," Cryptomathic, 29-Apr-2018. [Online]. Available: https://www.cryptomathic.com/news-events/blog/quantum-computing-and-its-impact-on-cryptography. [Accessed: 10-Feb-2021].