The Influence of Quantum Computing on Existing Cryptography

Nandini Bhiva Metkari[1] Ruchi Vinod Shukla[2]
[1,2]Research Student
[1,2]Department of Information Technology
[1,2]B. K. Birla College of Arts, Science, and Commerce (Autonomous), Kalyan, India

Abstract— The aim of this paper is to elucidate the implications of quantum computing in existing cryptography and to introduce the reader to fundamental post-quantum algorithms. In particular, the reader can delve into the following subjects: Existing cryptographic schemes (symmetric and asymmetric), challenges in quantum computing, quantum algorithms (Shor's and Grover's), and publish quantum cryptography. Specifically, the section of Post-Quantum Cryptography.

Keywords: Quantum Computers; Post-Quantum Cryptography; Shor's Algorithm; Grover's Algorithm; Asymmetric Cryptography; Symmetric Cryptography

I. INTRODUCTION

There is no doubt that advancements in science and particularly electronic communications have ended up one of the important technological pillars of the cutting-edge age. The need for confidentiality, integrity, authenticity, and non-repudiation in records transmission and records storage makes the science of cryptography one of the most vital disciplines in information technology. Cryptography, etymologically derived from the Greek phrases hidden and writing, in the manner of securing data in transit or stored by way of 1/3 celebration adversaries. There are two sports of cryptosystems; symmetric and asymmetric.

Quantum computing concept first off added as a concept in 1982 through Richard Feynman, has been researched extensively and is viewed the destructor of the existing contemporary asymmetric cryptography. In addition, it is a fact that symmetric cryptography can additionally be affected by specific quantum algorithms; however, its safety can be accelerated with the use of larger key spaces. Furthermore, algorithms that can break the existing asymmetric cryptoschemes whose security is based on the subject of factorizing massive prime numbers and the discrete logarithm problem have been introduced. It appears that even elliptic curve cryptography which is considered presently the most tightly closed and efficient scheme is weak against quantum computers. Consequently, a need for cryptographic algorithms strong to quantum computations arose.

II. EXISTING CRYPTOGRAPHY

In This Chapter We Give An Explanation For Temporarily The Role Of Symmetric Algorithms, Asymmetric Algorithms And Hash Functions In Modern Cryptography. We Analyze The Problem Of Factorizing Large Numbers, As Properly As The Discrete Logarithm Problem Which Is The Groundwork Of Sturdy Uneven Ciphers

A. *Symmetric Cryptography*

In symmetric cryptography, the sender and the receiver use the identical secret key and the equal cryptographic algorithm to encrypt and decrypt data. For example, Alice can encrypt a plaintext message the use of her shared secret key and Bob can decrypt the message the use of the equal cryptographic algorithm Alice used and the equal shared secret key. The key needs to be saved secret, that means that only Alice and Bob need to know it; therefore, an environment-friendly way for exchanging secret keys over public networks is demanded. Asymmetric cryptography was introduced to solve the problem of key distribution in symmetric cryptography. Popular symmetric algorithms consist of the advanced encryption general (AES) and the information encryption standard (3DES).

B. *Asymmetric Cryptography*

Asymmetric Cryptography Or Public Key Cryptography (Pkc) Is A Form Of Encryption Where The Keys Come In Pairs. Each Birthday Celebration Should Have Its Very Own Personal And Public Key. For Instance, If Bob Needs To Encrypt A Message, Alice Would Send Her Public Key To Bob And Then Bob Can Encrypt The Message With Alice's Public Key. Next, Bob Would Transmit The Encrypted Message To Alice Who Is In A Position To Decrypt The Message With Her Non-Public Key. Thus, We Encrypt The Message With A Public Key And Only The Individual Who Owns The Private Key Can Decrypt The Message. Asymmetric Cryptography Moreover Is Used For Digital Signatures. For Example, Alice Can Signal A Records Digitally With Her Non-Public Key And Bob Can Verify The Signature With Alice's Recognized Public Key.

Fig. 1: Quantum cryptography [16]

C. *Challenges in Quantum Computing*

There are many challenges in quantum computing thatmany researchers are working on.

- Quantum algorithms are by and large probabilistic. This means that in one operation a quantum computers returns many solutions where solely one is the correct. This trial and error for measuring and verifying the correct answer weakens the advantage of quantum computing pace [1].
- Qubits are inclined to errors. They can be affected by heat, noise in the environment, as well as stray electromagnetic couplings. Classical computer systems are susceptible to bit-flips (a zero can turn out to be one and vise versa). Qubits suffer from bit-flips as nicely as phase errors. Direct inspection for blunders ought to be avoided as it will motive the price to collapse, leaving its superposition state.
- Another venture is the situation of coherence. Qubits can continue their quantum nation for a brief length of time. Researchers at the University of New South Wales in Australia have created two distinctive types of qubits (Phosphorous atom and an Artificial atom) and by means of inserting them into a tiny silicon (silicon 28) they have been able to eliminate the magnetic noise that makes them susceptible to errors. Additionally, they stated that the Phosphorous atom has 99.99% accuracy which accounts for 1 error Each 10,000 quantum operations [2]. Their qubits can continue to be in superposition for a total of 35 seconds which is viewed a world records [3]. Moreover, to reap long coherence qubits need not solely to be isolated from the exterior world however to be stored in temperatures attaining the absolute zero. However, this isolation makes it tough to control them except contributing additional noise [1].

IBM in 2017, introduced the definition of Quantum Volume. Quantum extent is a metric to measure how effective a quantum computer is primarily based on how many qubits it has, how good is the error correction on these qubits, and the variety of operations that can be achieved in parallel. Increase in the number of qubit does no longer enhance a quantum computer if the error rate is high. However, improving the error rate would result in a more powerful quantum laptop [4].

III. CRYPTOSYSTEMS VULNERABLE TO QUANTUM ALGORITHMS

This section discusses the have an impact on of quantum algorithms on current cryptography and offers an introduction to Shor's algorithm and Grover's algorithm. Note that Shor's algorithm explained in the following subsection makes the algorithms that depend on the situation of factorizing or computing discrete logarithms vulnerable.

Cryptography plays an essential function in Each and every electronic communications machine today. For instance the security of emails, passwords, monetary transactions, or even electronic voting structures require the same protection targets such as confidentiality and integrity [5]. Cryptography makes sure that solely parties that have exchanged keys can read the encrypted message (also known as authentic parties). Quantum computers threaten the most important aim of every secure and authentic communications due to the fact they are in a position to do computations that Classical (conventional) computer systems cannot. Consequently, quantum computer systems can damage the cryptographic keys quickly by calculating or searching exhaustively all secret keys, allowing an eavesdropper to intercept the verbal exchange channel between true parties (sender/receiver). This venture is considered to be computational infeasible through a traditional computer[6].

According to NIST, quantum computers will bring the end of the current public key encryption schemes [7]. Table I adapted from NIST indicates the have an impact on of quantum computing on present cryptographic schemes.

A. SHOR'S Algorithm In Asymmetric Cryptography

In 1994, the mathematician Peter Shor in his paper "Algorithms for Quantum Computations: Discrete Logarithms and Factoring" [8], proved that factorizing giant integers would Change essentially with a quantum computer

Shor's algorithm can make cutting-edge asymmetric cryptography cave in seeing that is it based on massive prime integer factorizing or the discrete logarithm problem. To understand how Shor's algorithm factorizes giant high numbers we use The following example. We want to discover the high elements of number 15. To do so, we need a 4-qubit register. We can Visualize a 4-qubit register as a normal 4-bit register of a Traditional computer. Number 15 in binary is 1111, so a 4- Qubit register is enough to accommodate (calculate) the prime Factorizing of this number. According to Bone and Castro [8], a calculating carried out on the register can be thought as Computations done in parallel for every possible cost that the Register can take (0-15). This is additionally the solely step wanted to Be performed on a quantum computer.

The algorithm does the following:

- n = 15, is the number we favor to factorize
- x = random variety such as $1 < x < n - 1$
- x is raised to the electricity contained in the register (every possible state) and then divided through n

The rest from this operation is saved in a seconds 4-qubit register. The 2d register now contains The superposition results. Let's count on that x = 2 Which is larger than 1 and smaller than 14.

- If we raise x to the powers of the 4-qubit register which is a most of 15 and divide by way of 15, the reminders are proven in Table II. What we have a look at in the results is a repeating sequence Of four numbers (1,2,4,8). We can confidently say then That f = 4 which is the sequence when x = 2 and n = 15. The cost f can be used to calculate a possible factor with the following equation:

Possible factor: $P = xf/2 - 1$

In case, we get a end result which is no longer a prime wide variety we Repeat the calculation with distinct f values.

Shor's algorithm can be used moreover for computing Discrete logarithm problem. Vazirani [14] explored in detail the methodology of Shor's algorithm and confirmed that by starting from a random superposition kingdom of two integers, and by performing a series of

Fourier transformations, a new superposition can be set-up to supply us with excessive probability Two integers that fulfil an equation. By the use of this equation, we can calculate the cost r which is the unknown "exponent".

B. GROVER'S Algorithm in Symmetric Cryptography

Lov Grover created an algorithm that makes use of quantum computers to search unsorted databases [9]. The algorithm can √N find a particular entry in an unsorted database of N entries in N searches. In comparison, a conventional computer would need N/2 searches to find the equal entry. Bone and Castro [8] remarked the have an effect on of a possible application of Grover's algorithm to crack Data Encryption Standard (DES), which relies on its security on a 56-bit key. The authors remarked that the algorithm wants solely 185 searches to locate the key.

Currently, to forestall passwords cracking we extend the number of key bits (larger key space); as a result, the quantity ofches to locate the key.

Cryptographic Algorithm	Type	Purpose	Impact From Quantum Computer
AES-256	Symmetric key	Encryption	Secure
SHA-256, SHA-3	–	Hash functions	Secure
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Table I: Impact Analysis of Quantum Computing on Encryption Schemes (Adapted From [7])

Register 1:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Register 2:	1	2	4	8	1	2	4	8	1	2	4	8	1	2	4	8

Table II: 4-Qubit Registers with Remainders

searches needed to crack a passwords increases exponentially.Buchmann et al. [11] stated that Grover's algorithm have some application to symmetric cryptosystems but it is not as fact as Shor's algorithm.

IV. POST-QUANTUM CRYPTOGRAPHY

The aim of Post-quantum cryptography (also recognized as quantum-resistant cryptography) is to advance cryptographic systems that are secure in opposition to Each quantum and conventional computers and can interoperate with existing communications protocols and networks [7]. Many Post-quantum public key candidates are actively investigated the last years. In 2016, NIST introduced a name for proposals of algorithms that are believed to be quantum resilient with a cut-off date in November 2017. In January 2018, NIST published the results of the first round. In total eighty two algorithms have been proposed from which 59 are encryption or key change schemes and 23 are signature schemes. After 3 to 5 years of analysis NIST will report the findings and put together a draft of requirements [12]. Furthermore, the National Security Agency (NSA) has already announced plans to migrate their cryptographic requirements to Post-quantum cryptography [13]. The cryptographic algorithms presented in this section do no longer be counted on the hidden subgroup hassle (HSP) such as factorizing integers or computing discrete logarithms, but different complicated mathematical problem.

V. CONCLUSION

In today's world, the place statistics play a particularly important role, the transmission and the storage of information must be maximally secure. Quantum computer systems pose a significant risk to both conventional public key algorithms (such as RSA, ElGamal, ECC and DSA) and symmetric key algorithms (3DES, AES). Year via year it seems that we are getting closer to create a wholly operational familiar quantum pc that can make use of robust quantum algorithms such as Shor's algorithm and Grover's algorithm.

ACKNOWLEDGMENT

A special gratitude is conveyed to our prof. Swapna Augustine Nikale, Department of Information Technology of B.K. Birla College of Arts, Science and Commerce (Autonomous) Kalyan, Thane Mumbai.

REFERENCES

[1] Z. Kirsch, "Quantum Computing: The Risk to Existing Encryption Methods," Ph.D. dissertation, Tufts University, Massachusetts, 2015, http://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf.
[2] J. Muhonen and T. Dehollain, "Storing Quantum Information For 30 Seconds In a Nanoelectronic Device," Nature Nanotechnology, vol. 9, pp. 986–991, 2014.
[3] D-Wave, "Quantum Computing: How D-Wave Systems Work," http: //www.dwavesys.com/our-company/meet-d-wave.
[4] L. S. Bishop, S. Bravyi, A. Cross, J. M. Gambetta, and J. Smolin, "Quantum volume," Technical report, 2017., Tech. Rep., 2017.
[5] M. Campagna and C. Xing, "Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges," ETSI, Tech. Rep. 8, 2015
[6] W. Buchanan and A. Woodward, "Will Quantum Computers be the End of Public Key Encryption?" Journal of Cyber Security Technology, vol. 1, no. 1, pp. 1–22, 2016.
[7] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "NIST: Report on Post-Quantum Cryptography," NIST, Tech. Rep., 2016.
[8] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in Proceedings of the 35th Annual Symposium on Foundations of

Computer Science, ser. SFCS '94. Washington, DC, USA: IEEE Computer Society, 1994, pp. 124–134.
[9] L. Grover, "A Fast Quantum Mechanical Algorithm For Database Search," Bell Labs, New Jersey, Tech. Rep., 1996.
[10] S. Bone and M. Castro, "A Brief History of Quantum Computing," Surveys and Presentations in Information Systems Engineering (SURPRISE), vol. 4, no. 3, pp. 20–45, 1997, http://www.doc.ic.ac.uk/∼nd/ surprise 97/journal/vol4/spb3/.
[11] D. Bernstein, E. Dahmen, and Buch, Introduction to Post-Quantum Cryptography. Springer-Verlag Berlin Heidelberg, 2010.
[12] D. Moody, "The ship has sailed: The nist postquantum crypto competition." [Online]. Available: https: //csrc.nist.gov/CSRC/media//Projects/Post-Quantum-Cryptography/ documents/asiacrypt-2017-moody-pqc.pdf
[13] N. Koblitz and A. Menezes, "A riddle wrapped in an enigma," IEEE Security Privacy, vol. 14, no. 6, pp. 34–42, Nov 2016.
[14] U. Vazirani, "On The Power of Quantum Computation," Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, vol. 356, no. 1743, pp. 1759–1768, 1998.
[15] Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, Audun Jøsang Department of Informatics, University of Oslo, Norway
[16] https://www.google.com/url?sa=i&url=https%3A%2F%2Fquantumxc.com%2Fquantum-cryptography-explained%2F&psig=AOvVaw3e5wYhJhSPfsF-Kh68EWLb&ust=1629617275606000&source=images&cd=vfe&ved=2ahUKEwix6vbHy8HyAhUH_jgGHS-oD8sQjRx6BAgAEAo

