Quantum Computing: Attack on Symmetric and Asymmetric Cryptography

Harold Alejandro Villanueva Borda
Computer Science
Universidad Católica San Pablo
harold.villanueva@ucsp.edu.pe

***Abstract*—Currently, classical cryptography protects the exchange of information, however, the advances in quantum computing endanger such protection, since, with the new quantum algorithms it has been demonstrated that it is possible to breach and break many classical cryptosystems, either asymmetric or symmetric. This survey will show different techniques that are used to solve problems such as factorization of large numbers, discrete logarithms, and polynomial time, in order to break symmetric and asymmetric cryptosystems such as DES (Data Encryption Standard) and RSA (Rivest, Shamir and Adleman).**

***Index Terms*—Cryptography, Security Privacy, QFT, Shor's Algorithm, Grover Algorithm, RSA, DES, AES**

I. Introducción

In the 1980s the renowned theoretical physicist Richard Phillips Feynman noticed that the simulation of certain effects of quantum mechanics on a classical computer is not very efficient, so he came up with the idea of building quantum computers, but this was slow to develop due to its complexity. In 1994 MIT mathematician Peter Shor Williston designed a polynomial-time quantum algorithm for integer factorization. [18].

In the world of computing the bit is known, in turn there is the quantum bit or also called qbit, where it can be put in a superposition state that encodes 0 and 1. In classical computing parallel processes are used to reduce the processing time of some calculations, on the other hand in a quantum system parallelism is used massively. Unlike classical computing where you can read the result of a parallel thread, in quantum computing because the measurement is probabilistic can not choose which result to read so access to the results is totally restricted and to access a measurement is performed, this solution is being improved over the years involving algorithms known as Shor factorization, Grover's algorithm, however all recent proposals have scalability problems and requires a breakthrough to overcome the tens of qbit. [18].

Today many assume that implementing an ”unbreakable” cryptographic algorithm is impossible, so nowadays they focus more on resisting the attack. The most widely used encryption algorithms are RSA, DES, AES (Advanced Encryption Standard); although it is true that these algorithms are designed to resist attacks from current computers, but it is a matter of time before these systems become less and less resistant. This problem led to the development of quantum cryptography, which is based on the laws of quantum mechanics in order to protect the secrecy of messages. [14]. Currently, with the constant research on quantum computing, we are about to enter a new era of cryptography in which a new quantum key distribution protocol BB84, developed by Charles Bennet and Gilles Brassard in 1984, is being proposed. [3].

Quantum algorithms represent a danger to classical cryptography; the most famous and threatening is Shor's algorithm since it solves the integer factorization problem, as well as the difficulty of discrete logarithms in polynomial time. [22]. The Quantum Fourier transform plays an important role and is at the core of the algorithms.

There are currently 3 major directions of research into quantum computing public-key attacks [23]:

1) Improve, modify, simplify Shor's algorithm and if possible invent one that outperforms Shor.
2) Quantum attack algorithms based on adiabatic quantum computation.
3) Quantum attack algorithms based on the quantum walk principle.

Nowadays, the use of classical computing in everyday life is normal and for the exchange of information, public key cryptography such as RSA (Rivest, Shamir and Adleman) is used, where the encryption of data sent from a sender to a receiver is reliable. The protection provided by various classical cryptographic algorithms are to some extent highly secure and efficient, but at some point they will cease to be so and even more so with the development of quantum computing.

This survey will show fundamental concepts of quantum computing, as well as quantum algorithms and their functionalities. On the other hand, the research in this survey will focus on breaking the security of symmetric and asymmetric encryption, making use of ideas such as Grover's algorithm and Shor's algorithm to deal with the solution of discrete logarithms and the factorization of large integers, as well as the important use and the great role played by the Quantum Fourier Transform.

II. Computación cuántica

- *Circuitos*

Circuits are networks composed of wires that carry bit values to gates that perform elementary operations on the bits. All circuits we consider will be acyclic, meaning that the bits move through the circuit linearly and the wires never feed back to a previous location in the circuit. A circuit is an array or network of gates, which is terminology often used in the quantum environment. The gates come from a finite family, and take information from the input wires and deliver information along some output wires. [9].

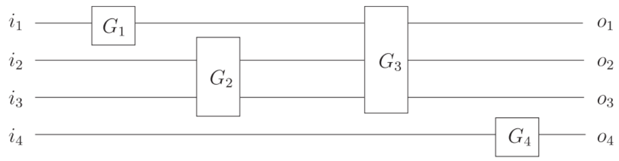
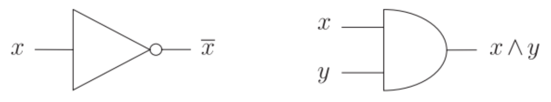


Fig. 1. Circuit diagram [9]

Definicion: A set of gates is universal for classical calculus if, for any positive integer n, m and function $f : \{0,1\}^n \to \{0,1\}^m$, a circuit can be built to calculate f using only gates from that set up [9].

- *Reversible computing*

The theory of quantum computation is related to a theory of reversible computation. A computation is reversible if it is always possible to uniquely recover the input, given the output. For example, the operation NOT is reversible, because if the output bit is 0, you know that the input bit must have been 1, and vice versa. On the other hand, the operation AND is not reversible [9].



x	$\overline{x}$
0	1
1	0

x	y	$x \wedge y$
0	0	0
0	1	0
1	0	0
1	1	1

Fig. 2. NOT and AND gates [9]

Each door in a finite family of doors can be made reversible by adding some additional input and output wires if needed [9].

- *Dirac notation and Hilbert spaces*

Dirac notation was invented by Paul Dirac and is often used in quantum mechanics. This notation identifies a vector that is written inside a 'ket' and resembles $|a\rangle$ [9]. The canonical basis of a two-dimensional vector space has two vectors, denoted by $\{|0\rangle, |1\rangle\}$ in Dirac notation, where $|0\rangle$ y $|1\rangle$ have the following representation [16]:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \; y \; |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1}$$

These vectors have two entries, unit length and are orthogonal. Then, this basis is orthonormal. It is called canonical basis in linear algebra and computational basis in quantum computation. Note that $|0\rangle$ is not the null vector, but the first vector of the canonical basis. All entries of the null vector are equal to 0 [16].

Vector spaces are over complex numbers and are of finite dimension, which significantly simplifies the mathematics involved, in turn, vector spaces are members of a class of vector spaces called Hilbert spaces and is given by this notation $\mathcal{H}$ [9].

- *Qubit and overlay*

The basic memory unit of a classical computer is the bit, which assumes 0 or 1. Typically, the bit is implemented using two different voltages, following the convention that the low or zero voltage represents the 0 bit and the high voltage represents the 1 bit. The basic memory unit of a quantum computer is the qubit, which also assumes, at the end of the computation, 0 or 1 [16].

The difference with the classical device occurs during the computation since the qubit supports the simultaneous coexistence of 0 and 1, i.e., before the measurement, the state of a qubit is represented by a two-dimensional vector $norma-1$ and the states of a qubit corresponding to 0 and 1 are $|0\rangle$ and $|1\rangle$. Quantum coexistence is represented mathematically by a linear combination of orthonormal vectors as follows. [16]:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2}$$

where α and β are complex numbers obeying the constraint.

$$|\alpha|^2 + |\beta|^2 = 1 \tag{3}$$

The state of the qubit is the vector $|\psi\rangle$ standard 1 with tickets α y β. Complex numbers α y β are the amplitudes of the state $|\psi\rangle$.

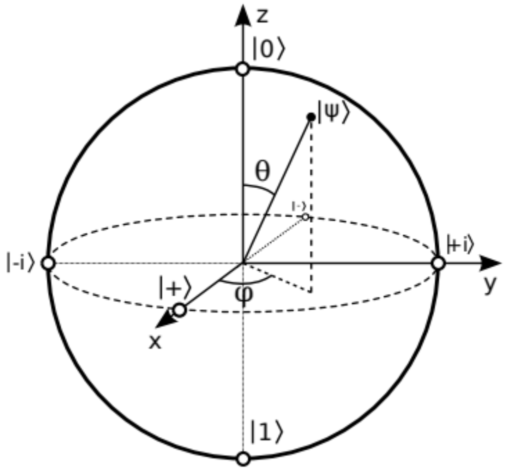


Fig. 3. Bloch sphere and location of the states $|0\rangle$, $|1\rangle$, $|\pm\rangle$ y $|\pm\rangle$. An arbitrary status is displayed $|\psi\rangle$ with spherical angles θ y φ [16].

- *Circuit of a Boolean function*

Now it will be shown, how to obtain the quantum circuit from a truth table; this will be achieved by means of multiqubit Toffoli gates. To show that multi-qubit Toffoli gates can implement any Boolean function in a quantum computer, let us take as an example the 3 bit Boolean function $f(a, b, c)$ defined by the following truth table [16]:

a	b	c	$f(a,b,c)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

Fig. 4. Circuit that implements f [16]

Since f has three input bits, we use multi-qubit Toffoli gates with three controls. The fourth qubit is the target. The output of f is the output of a measurement of the target qubit. Since f has two clauses in disjunctive normal form, we use two multiqubit Toffoli gates. The first gate must be triggered by the input $|001\rangle$ and the second by $|110\rangle$, corresponding to the rows of the truth table whose output is [16]:

The following circuit implements f:

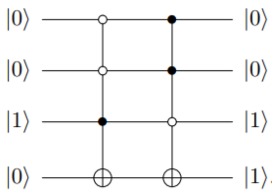


Fig. 5. Circuit that implements f [16]

Note that if the input is $|a, b, c\rangle|0\rangle$, then the output is $|a, b, c\rangle|f(a, b, c)\rangle$. This shows that the quantum computer can compute any n-bit Boolean function using a multiqubit Toffoli gate with $(n + 1)$ qubits for each 1 output of the truth table. Unfortunately, this technique of constructing quantum circuits to compute truth tables is not efficient, since the number of multiqubit Toffoli gates increases exponentially as a function of the number of qubits in the worst-case scenario [16].

III. Quantum Algorithms

- *The Deutsch Algorithm*

This algorithm is based on the Quantum Fourier Transform and illustrates the key ideas of parallelism and quantum interference that are used in all useful algorithms. [10]. On the other hand, this is the first algorithm that exploits quantum parallelism using only 2 qbits, which has inspired the construction of several quantum algorithms that are much more efficient. [15].

Deutsch's problem was posed in 1985, even without using the quantum circuit model. A generalization of Deutsch's algorithm is the Deutsch-Jozsa algorithm. [15] has exactly the same structure as its previous version and as with Deutsch's algorithm, we have a reversible circuit that implements an unknown function f, but this time f is a function of n bit strings to a single bit [10].

Deutsch's problem

Input: a black box for calculating an unknown function function $f : \{0, 1\} \to \{0, 1\}$.

Problem: Determine the value of $f(0) \oplus f(1)$ by making inquiries to f.

Suppose you have a reversible circuit to calculate an unknown function of 1 bit $f : \{0, 1\} \to \{0, 1\}$: We treat the reversible circuit as a black box, this means that by applying the circuit to obtain values of $f(x)$ for x inputs, no information from the inner workings of the circuit will be obtained to learn about the function.

f. Classically, the number of queries you perform to determine $f(0) \oplus f(1)$ is 2 [10].

- *Quantum Transform Fourier*

  The Fourier transform converts a function in the time domain into its component frequencies in the frequency domain by transforming a list of uniformly spaced function samples into a list of coefficients for a finite sequence of complex sinusoids, ordered by frequency. In quantum computing, the QFT (Quantum Fourier Transform) is the quantum analog of the DFT (Discret Fourier Transform). The QFT can be performed efficiently on a quantum computer using exponentially fewer gates than are required to compute classically. In QIP (quantum information processing), the QFT is a generalization of the Hadamard transform and both are quite similar, except that the QFT introduces a phase [19].

  In quantum information processing (QIP), the quantum Fourier transform (QFT) has a wealth of applications: Shor's algorithm and phase estimation are just a few well-known examples. Shor's quantum factorization algorithm, one of the most cited quantum algorithms, relies heavily on the QFT and efficiently finds integer prime factors of large numbers in quantum computers. [19].

- *Grover Algorithm*

  This quantum algorithm provides a polynomial speedup over the best known classical algorithms to solve many important problems. This quantum search algorithm performs a generic search, e.g., given a large integer N, one can efficiently recognize whether an integer p is a non-trivial factor of N. Quantum search is a tool to speed up such generic searches. [8].

  The search problem

  Input: A black box U_f to compute an unknown function $f : \{0,1\}^n \rightarrow \{0,1\}$.

  Problem: Find an entry $x \in \{0,1\}^n$ such that $f(x) = 1$..

  If the function f is only provided as a black box, then the following are necessary $\Omega(\sqrt{2}^n)$ black-box applications to solve the search problem with high probability for any input. Therefore, quantum algorithms can provide, at most, a quadratic speedup over classical exhaustive search. Grover's algorithm performs the search quadratically faster than can be done classically. If there is exactly one solution, a classical deterministic brute-force search takes $2^n - 1$ queries in the worst case. In fact, any classical algorithm, which for any function finds a solution with probability at least $\frac{2}{3}$, should make inquiries $\Omega(2^n)$ in the worst case. Grover's quantum search algorithm only takes $O(\sqrt{2}^n)$ = $O(\sqrt{2}^{\frac{n}{2}})$ queries [8].

  In particular, Grover's algorithm provides a quadratic speedup in the solution of NP-complete problems, which explain many of the important hard problems in computer science. [8]. On the other hand, the power of quantum algorithms, as discovered by Lov Grover, is that $\frac{N}{2}$ can be improved to $O(N^{1/2})$. Compared to a classical randomized search algorithm, the factor of $O(N^{1/2})$ is $O(N^{1/2})$. $\frac{1}{2}$ enters the exponent, which is a great improvement. We will now explain how and why the algorithm works. [12].

- *Shor's Algorithm*

  Shor's algorithm, presented at a 1994 conference, describes two quantum algorithms for factoring discrete integers and logarithms that run in polynomial time. Shor exploits not only quantum parallelism but also entanglement. [17].

  1) General idea

     In Shor's factoring algorithm (SFA), the objective is to find a non-trivial factor of a composite integer N. Briefly stated, SFA works as follows. It randomly picks an integer $y < N$ and checks whether y and N are coprime. If y is coprime with N, then SFA runs a special quantum subroutine to obtain the order $2r$ of N with certain probability ($2r$ is here an integer). In the original SFA and all previous SFAs, if $2r$ was an even integer y $y^r \not\equiv -1(\text{mod } N)$, then SFA uses y and $2r$ to obtain a nontrivial factor of N. However, if the result r obtained by the quantum-order search subroutine was not $2r$, or $2r$ was not an even integer, or $y^r \equiv -1(\text{mod } N)$, then the quantum subroutine would have to be executed again. [13].

  2) Detailed explanation of the Shor algorithm [27]
     - Choose a number d with small prime factors such that $2n^2 \leq d \leq 3n^2$.
     - Choose a random integer x that is a coprime of n.
     - Repeat the following steps, record d times using the same x each time:
       - ∗ Create a quantum memory register of $2d$ non-negative integers modulo n and divide it into two halves called reg1 and reg2. For the state of the entire register we write the vector ket $|reg1, reg2\rangle$.

- Load reg1 with the integers $0, 1, ..., d--1$ and reg2 with zeros everywhere, then normalize the register so that we can write the state of the entire register as a ket vector (Dirac notation).

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} |a, 0\rangle \tag{4}$$

- Perform the transformation $x \to x^a (\text{mod } .n)$ (using quantum parallelism) at each (unnormalized) number in reg1 and place the results in the corresponding places in reg2. Denote by r the period of the above transformation. Then the state of the complete (normalized) register becomes

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} |a, x^a (\text{mod } .n)\rangle \tag{5}$$

- Measure the content of reg2 by the hermitian operator A. This then collapses to some k and has the effect of projecting the state of reg1 to be a superposition of exactly those values of a for which $x^a = k(\text{mod } .n)$. Therefore, the status of the complete registry is

$$|\psi\rangle = \frac{1}{\#M} \sum_{a' \in M} |a', k\rangle \tag{6}$$

where $M := \left\{ a' : x^{a'} = k(\text{mod}.n) \right\}$

- Compute the discrete (fast) Fourier transform of the projected state in reg1 and return this result to reg1. This maps the projected state in reg1 into a superposition

$$|\psi\rangle = \frac{1}{\#M} \sum_{a' \in M} |a', k\rangle \tag{7}$$

- Now, the Fourier transform in reg1 is a periodic function with a peak at multiples of the inverse period $\frac{1}{r}$. The states corresponding to integer multiples of $\frac{1}{r}$ and those close to them appear with larger probability amplitudes than those that do not correspond to integer multiples of the inverse period. Then, at each step, we obtain a number h' such that $\frac{h'}{d}$ is close to multiple $\frac{\lambda}{r}$ of the inverse period of the exponential map for some $\lambda \in \mathbb{N}$. To estimate λ, the continued fraction expansion can be calculated from $\frac{h'}{d}$ as long as the denominator is less than n and then retain the nearest fraction as $\frac{\lambda}{r}$. If this is done frequently enough, we have sufficient samples of λ_i that lead to a conjecture of the actual λ and, therefore, of r.
    - Now that we know r, we can determine the factors of n with high probability. [27].

We note that, of course (with a rather low probability), Shor's algorithm may fail. Such counterexamples are easily constructed. But they represent rather atypical cases. Moreover, instead of using the classical (fast) Fourier transform, there are also quantum algorithms for the Fourier transform, which make Shor's algorithm work even faster in practice, but not to the point of improving the linear order of complexity [27].

IV. Graphical representation of the taxonomy

Figure 6 below shows how the classification is organized according to this survey. 6 shows how the classification is organized according to this survey. On the one hand, there is the attack on the classical symmetric cryptography and on the other hand the asymmetric part, as well as the subclassification of the Grover algorithm and the Shor algorithm respectively.

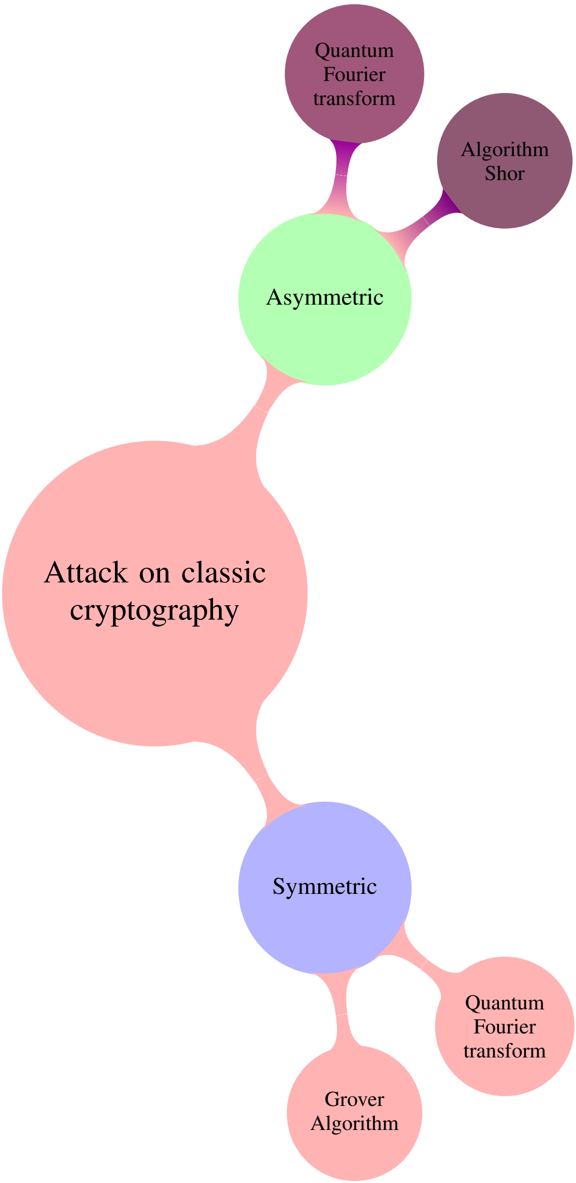

Quantum Fourier transform
Algorithm Shor
Asymmetric
Attack on classic cryptography
Symmetric
Quantum Fourier transform
Grover Algorithm

Fig. 6 Graphical representation of the taxonomy

V. Trabajos Relacionados

- Cryptographic attack possibilities on the RSA algorithm by means of classical and quantum computation

  The RSA cryptographic system is used for the design of encryption, its security protocol works according to the principle of large integer factorization that decomposes the composite number into a product of prime numbers. This survey describes a brute-force attack, which aims to find the secret key by successively querying the encryption function with all possible keys. On the other hand, to breach the RSA algorithm it is necessary to factor large integers, currently there is no algorithm in polynomial time that can perform it on a classical computer, however in this survey the Shor Algorithm is proposed, which manages to factor large integers in polynomial time, but this algorithm can only be executed on a quantum computer. [21].

- Quantum Algorithm for Attacking RSA Based on Fourier Transform and Fixed-Point

  Shor designs a quantum polynomial time algorithm to find the order r of an element a in the multiplicative group Z_n^* , which is used to factorize the positive integer n to break the famous RSA cryptographic system, but is subject to a condition, where r is required to be even, however this survey proposes a fixed point attack based on the inverse quantum Fourier transform and phase estimation, this algorithm runs in quantum polynomial time and does not need to explicitly factorize the modulus n and also does not require r to be even, this proposal ensures that the probability of success is higher against the Shor algorithm, but the time complexity is the same for both [23], [26].

- Experimental Analysis of Attacks on RSA Rabin Cryptosystems using Quantum Shor's Algorithm

  This survey proposes how Shor's algorithm can break cryptographic algorithms based on factorization such as RSA and Rabin's algorithms using IBM Quantum Experience, but this experiment will be done with no more than 7 bits, since IBM offers only 32 qubits. The focus of the survey is to demonstrate that the Quantum Shor algorithm poses a danger to asymmetric cryptosystems that use large prime number products for key generation. [7].

- Quantum Grover Attack on the Simplified-AES

  This survey presents how to attack the Simplified Advanced Encryption Standard Encryption (S-AES) algorithm using Grover's algorithm, where quantum circuits are built for the main components of S-AES and then put together to form a quantum version of the algorithm; in this way the S-AES is integrated into a black box that will pass through Grover's algorithm to recover the secret key in quadratic acceleration. [1].

- Variational quantum attacks threaten advanced encryption standard based symmetric cryptography

  This survey proposes a Variational Quantum Attack Algorithm (VQAA) for AES (Advanced Encryption Standard) symmetric cryptography and shows how VQAA is sometimes much faster than Grover's algorithm using the same order of search space queries, as well as showing the relationship between entanglement entropy, concurrency and cost function. [22].

- A Variational Quantum Attack for AES-like Symmetric

Cryptography

In this paper, the authors used asymmetric cryptography, such as RSA, to transmit the secret key and symmetric cryptography, such as Advanced Encryption Standard (AES), to encrypt data. With the development of quantum computers, more attention has been given to the security analysis of classical cryptography under quantum attacks. Shor's algorithm is capable of decrypting RSA cryptography in polynomial time, which seriously threatens the security of asymmetric cryptography. For symmetric cryptography, Grover's algorithm can find the key in a set having N entries by evaluating only the order of $\sqrt{N}$ entries. In that paper the authors show efficient quantum implementations of AES and Data Encryption Standard (DES) are proposed based on fewer quantum resources, such as qubits, quantum gates and circuit depths. At the writing of this paper, it is still in the noisy intermediate scale quantum (NISQ) era, i.e., when quantum computing systems are characterized by low number of qubits, low fidelity and shallow quantum circuits. Under these constraints, several classical quantum hybrid algorithms have been proposed, including the variational quantum algorithm (VQA) and the quantum approximate optimization algorithm (QAOA). These hybrid algorithms have significant advantages for solving combinatorial and fundamental state Hamiltonian optimization problems. In the design employed by the authors, the parameterized quantum circuit (PQC) operates in the key space and the cost function is designed according to the known ciphertext, as well as showing through simulations that the VQAA, on average, uses the same order of search space queries as Grover's algorithm. However, in some cases, it is even faster than Grover's algorithm. We also investigate the relationship between entanglement entropy, concurrency and cost function, and find that the speedup achieved is related to entropy, which is not unexpected, because entropy by definition represents the specific degree of surprise in revealing a given problem solution/result. [25].

- Algebraic attacks on block ciphers using quantum annealing

This paper presents a method for the transformation of symmetric encryption algebraic equations into the QUBO (Quadratic Unconstrained Binary Optimization) problem. After such transformation, the obtained QUBO problem can be solved using the quantum annealing approach, especially on the DWave computer. First, algebraic encryption equations must be obtained. The idea here is the same as in the case of algebraic attacks. After obtaining the Boolean equations of the given cipher in normal algebraic form, each equation f must be transformed into an equation of Boolean variables with integer coefficients. After the transformation of the given equations, each equation must be linearized, finally, one can obtain the problem in the QUBO form. The authors present the results of transforming the full AES-128 cipher to the QUBO problem, where the number of variables of the equivalent QUBO problem is equal to 237,915, which means, at least theoretically, that the problem can be solved using the D-Wave Advantage computer. Unfortunately, it is difficult to estimate the time this process would require. [4].

- Quantum Attack-Resistent Certificateless Multi-Receiver Signcryption Scheme

Signcryption is a cryptographic primitive that provides both signing and encryption simultaneously to confidential information with lower computational and communication overhead than the traditional approach of signing and then encrypting, there are two types of sign encryption schemes. One is based on traditional public key infrastructure, which causes the costly certificate management problem; the other is based on identity-based public key cryptography, which avoids certificate management, but causes the key escrow problem. To date, implementations of almost all certificate-less signature encryption schemes are based on traditional public-key cryptosystems, where security is mainly based on hard problems such as factor decomposition and discrete logarithm. However, quantum computing has provided a potential challenge to these difficult mathematical problems. Multivariate public key cryptography (MPKC), which can withstand quantum attacks, is one of the alternative solutions to secure communications in the post-quantum era. The security of MPKC is based on the Multivariate Quadratic (MQ) problem and the Polynomial Isomorphism (PI) problem. Compared to identity-based cryptography, MPKC has lower computational complexity and higher efficiency, which makes MPKC well suited for implementing highly secure communications for low-end devices. MPKC-based schemes have been studied extensively and several excellent schemes have been proposed. For example, SFLASH, a signature scheme based on MPKC, has been recommended by the European NESSIE Consortium since 2003 as the best known solution for implementation in low-cost smart cards. The authors employed MPKC to construct an efficient quantum attack-resistant certificateless multi-receiver signature encryption scheme, which combines the certificateless cryptosystem and MPKC. The new scheme not only has the advantage of the certificate-less cryptosystem, which avoids the key management problem, but also resists quantum attack only with lightweight computation such as multivariate quadratic polynomial operations. In the scheme, multivariate quadratic polynomial operations, which have lower computational complexity than bilinear matching operations, are used to encrypt a message for a certain number of receivers. Therefore, the scheme presented in the paper is more efficient than existing CLMSC schemes and is suitable for mobile terminals with low computational power. The security analysis shows that our scheme is a secure multi-recipient signature encryption scheme based on MPKC, and it also has important security properties, such as message confidentiality, unforgeability, non-repudiation, perfect forward secrecy, perfect backward secrecy, and public verifiability. [11].

- Quantum Attacks on 1K-AES and PRINCE

  Clearly, quantum cryptanalysis research is important in both theory and applications, as it stimulates the development of post-quantum cryptography. In this paper, the authors studied quantum sliding attack in 1K-AES (1K-Advanced Encryption Standard) and quantum related key attack in PRINCE. The main contributions of this paper include the following two aspects. 1. They propose the quantum sliding attack in 1K-AES by introducing the BHT (Brassard-Høyer-Tapp) algorithm. They imply that the quantum sliding attack could also be applied in the construction of the substitution permutation network (SPN), in addition to the iterated Even-Mansour cipher and Feistel constructions. In the proposed quantum attack, they generalize the BHT algorithm to the situation where the number of marked elements is not known in advance. In addition, they provide an implementation scheme of the classifier oracle based on the quantum phase estimation algorithm. The quantum attack presented by the authors in this paper can achieve sub-quadratic speedup with the same probability of success regardless of query complexity, time complexity, or memory complexity. In addition, the proposed quantum sliding attack on 1K-AES reduces the query complexity by a factor of $2^{\frac{n}{6}}$ compared to Grover's search in 1K-AES. 2. The authors of the paper claim that the generalized BHT algorithm could also be introduced in the related key attack in PRINCE. Therefore, this attack is also proposed, since, it can recover the first subkey; the query complexity, time complexity and memory complexity are $O(2^f racn3)$ when the probability of success is about $O(2^f racn3)$ when the probability of success is about $O(2^f racn3)$. 63%. After retrieving the first subkey, the other subkey can be retrieved by Grover's search. Therefore, the complexity of the query increases to $O(2^{\frac{n}{2}})$ when we consider the whole quantum attack on PRINCE. Compared to Grover's search in PRINCE, the query complexity of the entire quantum attack is reduced from $O(2^n)$ to $O(2^n)$. $O(2^{\frac{n}{2}})$. When compared to the combination of Grover's and Simon's algorithms in PRINCE, the query complexity of this attack is reduced from $O(n.2^{\frac{n}{2}})$ to $O(2^{\frac{n}{2}})$ [5].

- Quantum Polynomial-Time Fixed-Point Attack for RSA

  It is well known that the security of RSA depends essentially only on the computational intractability of the integer factorization problem (IFP) and, in particular, is only assured if the IFP does not have an efficient algorithm. That is, anyone who can solve the IFP in polynomial time can break the RSA cryptographic system in polynomial time. There are many methods to attack RSA, such as integer factorization attacks, discrete logarithm attacks, public exponent attacks, private exponent attacks, and side-channel attacks. The most powerful method to crack RSA on a classical computer is to use the NFS (Number Field Sieve) to factor n, which runs in subexponential time. $\mathcal{O}(exp(c(n)^{\frac{1}{3}})(\log\log n)^{\frac{2}{3}})$, where my $C \approx 1.92$. However, a quantum factorization algorithm in polynomial time, proposed by Shor in 1994, can solve the IFP in a time proportional to $\mathcal{O}((\log n)^{2+\varepsilon})$. Recent research has sought to reduce the number of quantum bits and make it easier to run on a quantum computer with fewer quantum bits. However, it has long been known that there is no need to factor n if the only goal is to attack RSA. In fact, to recover M from C, it suffices to calculate the order, r, of the fixed point C. Once the order r has been found, the plaintext M is simply the element M. $C^{e^{r-1}}$ mod n. In classical computing, this computation is equivalent to factoring n, which is believed to be difficult. In this paper, the authors presented a new polynomial-time quantum algorithm that can be used to attack RSA without factoring the modulus n [24].

- Quantum attacks on pseudorandom generators

  A random generator is a system whose output consists of totally unpredictable numerical sequences. Such generators are composed of two elements:

  - A non-deterministic phenomenon
  - A post-processor that compresses the previously produced sequence to minimize statistical defects.

  Pseudorandom generators are deterministic and recursive algorithms and play an important role in cryptography. Session keys, initialization vectors, salts that are encrypted with passwords, and unique parameters in digital signatures are examples of the cryptographic application of pseudorandom generators. Several efficient quantum computing algorithms have been proposed for problems where no polynomial-time classical computing algorithm is known. In this paper, the authors present a quantum attack on the Blum-Micali generator, which is a cryptographically secure pseudorandom generator that has been widely adopted in cryptosystems. The proposed attack is composed of three stages: the second stage is a Grover-inspired procedure and the third stage uses Shor's discrete logarithm algorithm. As a result of this attack, the previous and future output of the generator becomes predictable, thus completely compromising the security of the generator. [6].

VI. Strengths and weaknesses analysis

While quantum computing has advanced dramatically over the past decade, its potential applications have yet to be demonstrated on a large scale. Such demonstrations are likely to require advances in physics, computer science and engineering, as quantum computers are prone to errors due to quantum coherence and environmental conditions. [20].

On the other hand, it is said that in the future, a quantum computer (QC) will be able to solve some problems much faster than a classical computer (CC), which is called quantum advantage, this is because the computing power of QC is growing faster than that of CC. One of the measures of Quantum Computer performance introduced by IBM is Quantum Volume. To achieve a quantum advantage in the next decade, IBM stated that they ”need to at least double the quantum volume of our quantum computing systems every year.” In January 2020, Chow and Gambetta confirmed that IBM is on track to achieve this goal with a new 28-qubit quantum computer that demonstrates quantum volume of 32 [28].

- *Attack on asymmetric cryptography*

  All current asymmetric algorithms (RSA, ECC, DH, DSA) can be decrypted by quantum computers. They are based on the prime factorization problem or the discrete logarithm problem, which are easy to solve on quantum computers using Shor’s algorithm. Mathematicians and cryptographers used these number theory problems to found the security of asymmetric algorithms. Now they have to look for new mathematical problems that quantum computers cannot easily solve. [2].

  Currently all asymmetric algorithms are based on mathematical problems for which people have been searching for solutions for centuries. However, the weakness they have is that quantum computers are good at parallel tasks that require one result at the end. Since the algorithms require only one result at the end, a superposition of qubits can be used to parallelize all the computations and then the result can be measured. To avoid taking advantage of the parallelism of quantum computers, algorithms that require multiple outcomes can be used. Thus, the parallelism of quantum computers cannot be used to its full extent. [2].

- *Attack on Symmetric Cryptography*

  Symmetric algorithms and hash functions are relatively secure in a post-quantum world. Grover’s algorithm can accelerate attacks by square root complexity, however, most algorithms can be re-secured by doubling the key size [2]. When considering applications of Grover’s algorithm, it should be emphasized that the database is not explicitly represented. Instead, an oracle is invoked to evaluate an element by its index. Reading an entire database element by element and converting it to such a representation can take much longer than Grover’s search. To account for such effects, Grover’s algorithm can be thought of as a solution to an equation or constraint. In such applications, the oracle is a way to verify the constraint and is not related to the search algorithm. This separation generally avoids algorithmic optimizations, while conventional search algorithms often rely on such optimizations and avoid exhaustive search [20].

Some important limitations of IBM’s quantum computer [20]:

- Coherence problems:

  The device must constantly fight against the environment that acts to degrade the coherence of the system. And, therefore, the delicate quantum information stored in a quantum computer is extremely susceptible to noise. The qubits must be kept cool or else they will easily collapse. The error due to qubit entanglement is high. Multiqubit gate errors were much higher than single-qubit gate errors..

- Limited connectivity between qubits:

  This is another major limitation, therefore, there is a need to employ a large number of swap gates which increases the gate count (which adds to the gate errors) especially the cnots which have quite high errors and therefore greatly reduce the expected state fidelity and also the circuits become complex and difficult to understand and debug.

IBM’s simulators already have limited code length (comparatively, LIQ$Ui|\rangle$ and Quirk Quantum Simulator have relaxed code lengths), so it becomes difficult to implement large circuits or extend circuits to add error correction gates or solve the problem of limited connectivity by adding more swapping. gates. Implementing the tofolli gate for 16 qubits required many additional qubits or a large number of stages, which are not possible in current IBM devices and, therefore, implementing 16-qubit Grover search in IBM simulators and real devices was unrealistic [20].

VII. Conclusions

As reviewed, it is concluded that quantum cryptography is a newly and rapidly emerging field and therefore many companies around the world are investing resources to increase the knowledge and practices currently in place with respect to post-quantum security. Further advances in technology based on quantum mechanics could lead to an expansion of these capabilities, resulting in better and more efficient ways to implement symmetric cryptosystems, and as long as symmetric cryptography is not implemented with quantum oracles, they are safe from quantum attacks.

Today our current classical data is secure, however, using classical computing we can break this security, and to achieve this there are algorithms with an exponential execution time, which decreases the probability that they can be breached. However, with the advances in quantum computing it was possible to design and implement algorithms that can achieve the same goal in polynomial time, the only limitation would be that there is not yet the amount of qubits needed to break a symmetric or asymmetric encryption method of 2048 bits; it should be noted that advances in quantum computing are fast and that to counter possible quantum attacks use is made of post-quantum cryptography.

VIII. Future work

In quantum computing, the size of a number is measured in terms of its length in bits. A large number can be represented using several qubits. However, due to the limitations of current technology, it is difficult to work with very large numbers using a limited number of qubits. Therefore, to improve this problem, I will investigate data compression techniques to reduce the amount of information needed to represent a large number, which allows working with it using a reduced number of qubits, as well as error correction techniques to reduce the impact of noise in large number computations.

On the other hand, mentioning the term ”noise”; it is known that this is one of the main challenges in the implementation of quantum computing. Noise can be any external interference that affects the quantum state of a system, which can cause errors in computations. One of the main problems is that it can cause qubits to lose their coherence, which makes it difficult to perform accurate quantum operations, for this reason I am also interested in investigating different approaches such as error correction and the use of noise reduction techniques in quantum circuits.

References

[1] Mishal Almazrooie et al. “Quantum Grover Attack on the Simplified-AES”. In: *Proceedings of the 2018 7th International Conference on Software and Computer Applications*. ICSCA 2018. Kuantan, Malaysia: Association for Computing Machinery, 2018, pp. 204–211.

[2] Ritik Bavdekar et al. “Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research”. In: *CoRR* abs/2202.02826 (2022). arXiv: 2202.02826.

[3] Dagmar Bruss et al. “Quantum Cryptography: A Survey”. In: *ACM Comput. Surv.* 39.2 (2007), 6–es.

[4] Elżbieta Burek et al. “Algebraic Attacks on Block Ciphers Using Quantum Annealing”. In: *IEEE Transactions on Emerging Topics in Computing* 10.2 (2022), pp. 678–689.

[5] Binbin Cai et al. “Quantum Attacks on 1K-AES and PRINCE”. In: *The Computer Journal* (Feb. 2022).

[6] Elloá Guedes, Francisco de Assis, and BERNARDO LULA. “Quantum attacks on pseudorandom generators”. In: *Mathematical Structures in Computer Science* 23 (June 2013).

[7] Babita Jajodia and Ritu Thombre. “Experimental Analysis of Attacks on RSA Rabin Cryptosystems using Quantum Shor’s Algorithm”. In: Apr. 2021.

[8] Phillip Kaye, Raymond Laflamme, and Michele Mosca. “ALGORITHMS BASED ON AMPLITUDE AMPLIFICATION”. In: (Nov. 2006), pp. 152–163.

[9] Phillip Kaye, Raymond Laflamme, and Michele Mosca. “INTRODUCTION AND BACKGROUND and LINEAR ALGEBRA AND THE DIRAC NOTATION”. In: (Nov. 2006), pp. 01–37.

[10] Phillip Kaye, Raymond Laflamme, and Michele Mosca. “Introductory Quantum Algorithms”. In: (Nov. 2006), pp. 94–99.

[11] Huixian Li et al. “Quantum Attack-Resistent Certificateless Multi-Receiver Signcryption Scheme”. In: *PloS one* 8 (June 2013), e49141.

[12] Richard J. Lipton and Kenneth W. Regan. “Grover’s Algorithm”. In: *Quantum Algorithms via Linear Algebra: A Primer*. 2014, pp. 115–128.

[13] Daniel Neuenschwander. “3 Factorization with Quantum Computers: Shor’s Algorithm”. In: *Probabilistic and Statistical Methods in Cryptology: An Introduction by Selected Topics*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 37–45.

[14] Nick Papanikolaou. “An Introduction to Quantum Cryptography”. In: *XRDS* 11.3 (2005), p. 3.

[15] Renato Portugal. “Deutsch’s Algorithm”. In: (Sept. 2022), pp. 26–31.

[16] Renato Portugal. “Quantum Circuits ”. In: (Sept. 2022), pp. 03–24.

[17] Renato Portugal. “Shor’s Algorithm for Factoring Integers ”. In: (Sept. 2022), pp. 56–74.

[18] Eleanor Rieffel and Wolfgang Polak. “An Introduction to Quantum Computing for Non-Physicists”. In: *ACM Comput. Surv.* 32.3 (2000), pp. 300–335.

[19] Jacob Hammond Shlomo Kashani Maryam Alqasemi. “A quantum Fourier transform (QFT) based note detection algorithm”. In: (Apr. 2022), pp. 4–8.

[20] Akanksha Singhal and Arko Chatterjee. *Grover’s Algorithm*. July 2018. DOI: 10.13140/RG.2.2.30860.95366.

[21] Kapil Kumar Soni and Akhtar Rasool. “Cryptographic Attack Possibilities over RSA Algorithm through Classical and Quantum Computation”. In: *2018 International Conference on Smart Systems and Inventive Technology (ICSSIT)*. 2018, pp. 11–15.

[22] Y. Wang, H. Zhang, and H. Wang. “Quantum Algorithm for Attacking RSA Based on the eth Root”. In: *Gongcheng Kexue Yu Jishu/Advanced Engineering Science* 50 (2018), pp. 163–169.

[23] Yahui Wang, Huanguo Zhang, and Houzhen Wang. “Quantum polynomial-time fixed-point attack for RSA”. In: *China Communications* 15.2 (2018), pp. 25–32.

[24] Yahui Wang, Huanguo Zhang, and Houzhen Wang. “Quantum polynomial-time fixed-point attack for RSA”. In: *China Communications* 15.2 (2018), pp. 25–32.

[25] ZeGuo Wang et al. “A Variational Quantum Attack for AES-like Symmetric Cryptography”. In: (May 2022).

[26] WANG, Yahui and ZHANG, Huanguo. “Quantum Algorithm for Attacking RSA Based on Fourier Transform and Fixed-Point”. In: *Wuhan Univ. J. Nat. Sci.* 26.6 (2021), pp. 489–494.

[27] Guoliang Xu et al. “Improving the Success Probability for Shor’s Factorization Algorithm”. In: *Reversibility and Universality: Essays Presented to Kenichi Morita on the Occasion of his 70th Birthday*. Ed. by Andrew Adamatzky. Cham: Springer International Publishing, 2018, pp. 447–462.

[28] Lei Zhang, Andriy Miranskyy, and Walid Rjaibi. *Quantum Advantage and Y2K Bug: Comparison*. July 2019.