International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Quantum Hacking: Challenges and Countermeasures

Mohammad Suhail[1], Mohd Kaif[2]

[1,2]Computer Engineering Department, Zakir Husain College of Engineering and Technology, Aligarh Muslim University

Abstract

The advent of quantum computing technology presents both unprecedented opportunities and profound threats to the field of cryptography. While quantum computers promise exponential speedup for certain computational tasks, they also pose a formidable challenge to the security of classical cryptographic systems. Quantum hacking, encompassing a spectrum of attacks leveraging the unique properties of quantum mechanics, has emerged as a pivotal area of research in the context of quantum information security.

This review paper provides a comprehensive examination of quantum hacking, its underlying principles, and the vulnerabilities it exploits. We delve into the quantum algorithms and techniques that threaten classical cryptographic primitives, such as factoring large integers and solving discrete logarithm problems. Special attention is given to Shor's algorithm, heralded for its potential to break widely-used encryption schemes.

In response to these threats, we explore the promising field of post-quantum cryptography, which aims to develop encryption and signature schemes resilient against quantum attacks. We survey quantum-resistant cryptographic protocol, the quantum key distribution (QKD), which leverage the principles of quantum mechanics to ensure secure key exchange in the era of quantum computing.

As quantum hacking continually evolves, so too must our countermeasures. This review paper presents a balanced assessment of the current state of quantum hacking and the strategies for defending against it. It concludes by highlighting the importance of collaborative efforts among researchers, industry, and policymakers to ensure the integrity of our digital communications in a post-quantum world.

Keywords: Quantum Hacking, Quantum Information Security, Post-Quantum Cryptography, Quantum algorithms, Quantum-resistant cryptographic protocol

1. Introduction

In recent years, advancements in quantum computing technology have opened up new avenues for innovation and research. However, along with the promises of faster processing and enhanced computational capabilities comes the rising concern of quantum hacking. Quantum hacking refers to the exploitation of vulnerabilities inherent in quantum systems to compromise the security of data transmission, encryption protocols, and other related applications.

The field of quantum hacking is gaining substantial attention due to its potential to disrupt the security of various sectors, including finance, communication, and defense. Traditional cryptographic methods, which have been reliable for decades, are at risk of being rendered obsolete in the face of quantum

computing capabilities. As quantum computers continue to evolve, the concern for protecting sensitive information from quantum attacks becomes more urgent.

The purpose of this research review paper is to provide a brief review of the current state of quantum hacking, highlighting the various techniques employed by malicious actors to exploit quantum systems. By understanding the vulnerabilities and potential risks associated with quantum computing, researchers can develop effective countermeasures and strategies to mitigate the threat of quantum hacking.

This paper aims to delve into the fundamental principles of quantum computing and cryptography, explore the vulnerabilities that quantum systems expose, and analyze the existing quantum hacking techniques. Moreover, it will examine the potential impact of quantum hacking on various sectors and discuss the ongoing efforts in developing quantum-safe cryptographic solutions.

Through this research review, it is expected to contribute to the understanding of the current landscape of quantum hacking and provide insights into the future implications of this emerging field. By identifying the challenges and opportunities presented by quantum computing, policymakers, researchers, and industry professionals can work together to develop robust security measures that can withstand the threat of quantum hacking.

2. CURRENT SECURITY SYSTEM

The idea of information, which is currently measured in bits, and the formalization of probabilities are relatively new, although having a significant impact on our daily lives. It is fascinating to realize that QC is at the nexus of quantum mechanics and information theory and that the security of quantum cryptography is closely related to the conflict between quantum mechanics and relativity, or the famous Einstein-Rosen-Podolsky (EPR) paradox (Einstein et al., 1935).

The art of concealing information from unauthorized parties is known as cryptography. One utilizes encryption to accomplish this; a message is coupled with some additional secret information, called the key, using an algorithm to create a cipher. Say, for example, that Alice is encrypting and sending the message, Bob is receiving it, and Eve is the malicious listener. Unlocking the cryptogram without Bob's key should be difficult for a cryptosystem to be deemed secure. In reality, this requirement is frequently relaxed, and all that is needed is for the system to be sufficiently hard to break. It is proposed that the message should continue to be secure as long as the data it contains is valuable.

The two main classes of crypto-systems namely, the public key and the secret key (private key) crypto-systems:

2.1 THE SECRET KEY CRYPTOSYSTEM

It is also called Symmetric key cryptography. This system is based on a secret key which is used for various cryptographic operations. It is necessary for sender and receiver to have this key. Traditionally say, Alice (the sender) and Bob (the receiver) both have a private secret key. Alice sending a message encrypt using that key and sends the message and Bob receives the encrypted code and decrypt it using the private key. Since the Eavesdropper Eve don’t has the key he can’t read real message. But in this case there is no public key, so the private key should be shared by a secure method (some trusted means or personal meeting) to every pair of message sender and receiver. This out to be expensive and complicated. A one-time pad (OTP) is one of such technique invented in 1917 by Gilbert Vernam and Major Joseph Mauborgne. It is considered mathematically unbreakable if certain conditions are met –

1. The key must remain a secret.

2. The key must be cryptographically random.
3. The key should never be used again.

Hence, it provides perfect security. Even if hacker has infinite computational power, he can never break the OTP cipher. To encrypt a plaintext, we use its corresponding ASCII message m, than using secret key k, for each position I between 1 and |m|, it is computed by us as –

- $(m[i] + k[i])\%128$, where $m[i]$ and $k[i]$ are converted to their representation to do arithmetic.

An example is given here. The plaintext $'HELLO'$ is encrypted with the secret key $'david'$. Then, each character is converted to its corresponding ASCII representation. Now, the first one is $'H'+'d'$ [where $'H'$ is 72 and $'d'$is 100 in ASCII]. On addition, a result of 172 is obtained. After taking the modulo operation, $172\%128$ yields 44, which is $','$ in ASCII. This process is performed for all characters, resulting in a cipher of the same length as the original code (Refer to FIG. 1).

Similarly, for decryption (Refer to FIG. 2), the cipher-text 'c' is taken, and the plaintext is recovered by subtracting each letters ASCII value in secret key from corresponding letters ASCII value in cipher as –

- $(c[i] - k[i])\%128$, where $c[i]$ and $k[i]$ are converted to their representation to do arithmetic.

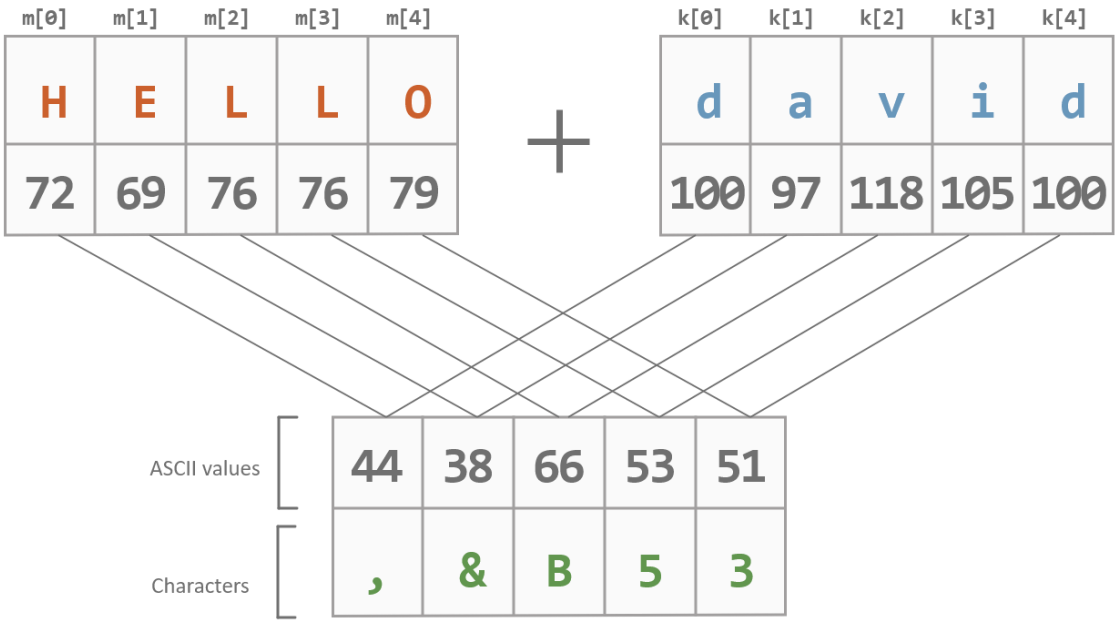

Figure 1: The figure shows the Encryption Process of a message using a Private Key to create a Cipher-text.

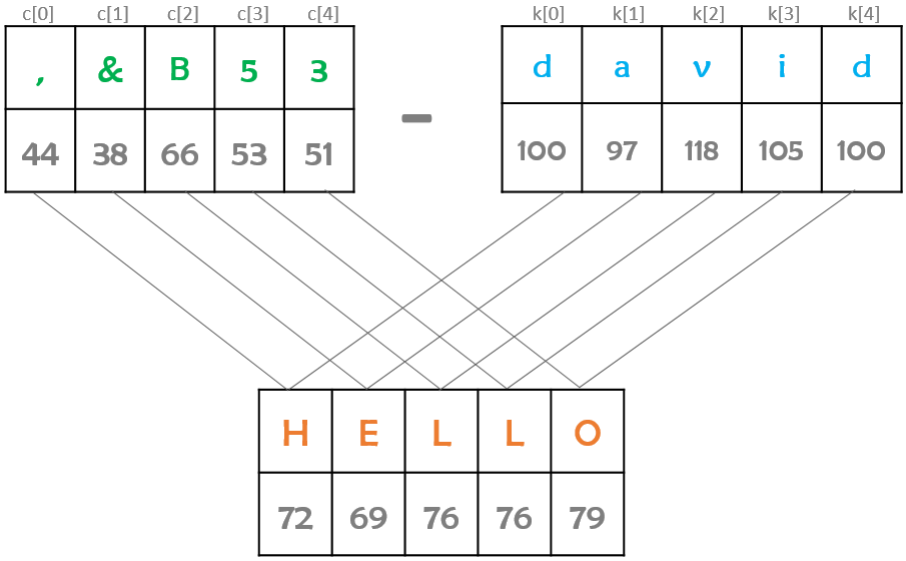

Figure 2: The figure shows the Decryption Process of a Cypher-text using a Private Key to regain the Original Message.

dec	hex	oct	char	dec	hex	oct	char	dec	hex	oct	char	dec	hex	oct	char
0	0	000	NULL	32	20	040	space	64	40	100	@	96	60	140	`
1	1	001	SOH	33	21	041	!	65	41	101	A	97	61	141	a
2	2	002	STX	34	22	042	"	66	42	102	B	98	62	142	b
3	3	003	ETX	35	23	043	#	67	43	103	C	99	63	143	c
4	4	004	EOT	36	24	044	$	68	44	104	D	100	64	144	d
5	5	005	ENQ	37	25	045	%	69	45	105	E	101	65	145	e
6	6	006	ACK	38	26	046	&	70	46	106	F	102	66	146	f
7	7	007	BEL	39	27	047	'	71	47	107	G	103	67	147	g
8	8	010	BS	40	28	050	(	72	48	110	H	104	68	150	h
9	9	011	TAB	41	29	051	)	73	49	111	I	105	69	151	i
10	a	012	LF	42	2a	052	*	74	4a	112	J	106	6a	152	j
11	b	013	VT	43	2b	053	+	75	4b	113	K	107	6b	153	k
12	c	014	FF	44	2c	054	,	76	4c	114	L	108	6c	154	l
13	d	015	CR	45	2d	055	-	77	4d	115	M	109	6d	155	m
14	e	016	SO	46	2e	056	.	78	4e	116	N	110	6e	156	n
15	f	017	SI	47	2f	057	/	79	4f	117	O	111	6f	157	o
16	10	020	DLE	48	30	060	0	80	50	120	P	112	70	160	p
17	11	021	DC1	49	31	061	1	81	51	121	Q	113	71	161	q
18	12	022	DC2	50	32	062	2	82	52	122	R	114	72	162	r
19	13	023	DC3	51	33	063	3	83	53	123	S	115	73	163	s
20	14	024	DC4	52	34	064	4	84	54	124	T	116	74	164	t
21	15	025	NAK	53	35	065	5	85	55	125	U	117	75	165	u
22	16	026	SYN	54	36	066	6	86	56	126	V	118	76	166	v
23	17	027	ETB	55	37	067	7	87	57	127	W	119	77	167	w
24	18	030	CAN	56	38	070	8	88	58	130	X	120	78	170	x
25	19	031	EM	57	39	071	9	89	59	131	Y	121	79	171	y
26	1a	032	SUB	58	3a	072	:	90	5a	132	Z	122	7a	172	z
27	1b	033	ESC	59	3b	073	;	91	5b	133	[	123	7b	173	{
28	1c	034	FS	60	3c	074	<	92	5c	134	\	124	7c	174	|
29	1d	035	GS	61	3d	075	=	93	5d	135	]	125	7d	175	}
30	1e	036	RS	62	3e	076	>	94	5e	136	^	126	7e	176	~
31	1f	037	US	63	3f	077	?	95	5f	137	_	127	7f	177	DEL

Figure 3: The figure shows the list of all 128 ASCII characters from 0 to 127 with their corresponding decimal, hexadecimal and octal equivalents.

The one-time pad cryptosystem is well-known in cryptography for being characterized by a property referred to as perfect secrecy, which informally indicates that no information about the corresponding plaintext, apart from its length, is revealed by the ciphertext. Let the previous example be considered, in which the cipher is $',\&B53'$.

This cipher could have been generated by any five-letter plaintext message because for any such message, there exists a secret key that could have been used to encrypt that message, resulting in the ciphertext $',\&B53'$. The plaintext message could have been $'HELLO'$, encrypted with the secret key $'david'$, but it is equally likely that the message $'FUNNY'$ could have been sent using the secret

key $'fQtgZ'$. Due to perfect secrecy, no information about the original plaintext message can be obtained by an eavesdropper, even if they possess the entire ciphertext.

The One-Time Pad is not commonly employed in modern encryption systems due to its drawbacks. The essential requirement of never reusing the key implies that the size of the key must be equivalent to the size of the plaintext. This imposes a constraint on storage space, rendering OTP encryption impractical for encrypting large amounts of data. Generating substantial quantities of cryptographically random data is challenging, particularly in systems with low entropy.

2.2 THE PUBLIC KEY CRYPTOSYSTEM

This is also called Asymmetric key cryptography. Let K be the set of all "keys" and M be the set of all possible messages. For each key $k \in K$ there exists both an encryption function $E_k(m)$: $M \to M$ and a decryption function $D_k(m)$: $M \to M$. The following requirements must be met for these functions to qualify as public key cryptosystems –

1. For every message-character $m \in M$ and every key-character $k \in K$, the values of function $E_k(m)$ and $D_k(m)$ are not difficult to compute.
2. For every message-character $m \in M$ and every key-character $k \in K, E_k\big(D_k(m)\big) = m$ and $D_k\big(E_k(m)\big) = m$.
3. For almost every message-character $k \in K$ if somebody knows only the function E_k, it is computationally infeasible to compute D_k.
4. For a given message-character $k \in K$, it is easy to find the functions E_k and D_k.

If a function E_k satisfies all 4 points (1 to 4 given above) than the function is called a trap-door one-way permutation. The function is called so because it is simple to compute in one direction but not in other. The inverse functions become easy to compute once specific information is provided, which is referred to as the trap-door.

This system is based on so-called one-way functions, which make it simple to calculate f(x) for a given x but challenging to calculate x from f(x). "Difficult" signifies that the task will require a time that increases exponentially with the quantity of input bits. The RSA (Named on Ron Rivest, Adi Shamir, and Leonard Adleman who developed algorithm in 1977) crypto-system very popular from last 20 years is based on the factorizing of large integers. For example computing 211×197 is very easy and can be completed in few seconds, however finding prime factor of 41567 can take some time.

To encrypt a message, two large prime numbers p and q, each about 50 digits, are chosen by Bob. After p and q are selected, n is obtained as $n = p * q$. The encryption key or public key (which is made publicly available), is represented by the pair of integers (e, n) and the decryption key or private key is represented by the pair (d, n). The message can now be encrypted by Alice using this public key and transmitted to Bob, who then decrypts it with the private key. To encrypt a given message m, it is first represented as an integer within the range of 0 to n − 1. If the message is too large, it is divided into blocks until each block falls within the range of 0 to n − 1. Then m is encrypted by raising its power to e than taking modulo n. The resulting ciphertext is denoted as c.

$$c = m^e (mod\ n)$$

The cipher-text is decrypted by raising it to the power d than taking modulo n.

$$m = c^d (mod\ n)$$

The integer's e and d are closely related to p and q. Choose d to be any large random integer that is relatively prime to $(p-1)(q-1)$. Then e is the multiplicative inverse of d modulo $(p-1)(q-1)$.

Example –

1. Let prime number be $p = 7\ and\ q = 17$
2. $n = p \times q = 119$
3. $\psi(n) = (p-1) \times (q-1) = 16 \times 6 = 96$
4. Public/encrypting key $e = 5$
5. Calculate private/decrypting key $d = ((\psi(n) \times i) + 1)/e$
   a. $d = (96 \times 1 + 1)/5 = 19.4$
   b. $d = (96 \times 2 + 1)/5 = 38.6$
   c. $d = (96 \times 1 + 1)/5 = 57.8$
   d. $d = (96 \times 1 + 1)/5 = 77$ [Integer, stop here $d = 77$]
6. Public key pair $\{ e, n \} = \{ 5, 119 \}$
7. Private key pair $\{ d, n \} = \{ 77, 119 \}$
8. Plain text $PT = 6$, Cipher-text $CT = PT^e\ mod\ n = 6^5\ mod\ 119 = 41$. [Cipher-text = 41]
9. Cipher-text $CT = 41, PT = CT^d\ mod\ n = 41^{77}\ mod\ 119 = 6$ [Plain-text = 6]

For known algorithms of factorization of integer n, the time for calculating Prime factors increases exponentially with the number of bits of n, and one can easily improve the safety of RSA by choosing a longer key. In 2016, a simple recalculation estimated that breaking a 64-bit key would take approximately 545 years. To put this into perspective, consider that AES (Advanced Encryption Standard), which typically uses keys that are either 128 or 256 bits long, has never been broken. The most powerful method for breaking RSA is to use the NFS (Number Field Sieve) which runs in sub-exponential-time complexity $O\left(\exp\left(a(\log n)^{\frac{1}{3}}\right)(\log\log n)^{\frac{2}{3}}\right)$, where $a \approx 1.92$. In fact, all factoring algorithms that have been developed up to this date, including the NFS, are unable to execute in polynomial time. It is important to creating unbreakable cryptography because of ineffectiveness of factorization.

Nevertheless, two significant faults might compromise the effectiveness of RSA. Firstly, it remains uncertain whether factorizing is genuinely challenging, and if a rapid algorithm for factorization emerges, it would compromise the security of the RSA framework. Moreover, although the emergence of such an algorithm is yet to be revealed, there is no guarantee it does not exist. This situation is even more concerning given recent advancements in quantum computation theory, which suggests that the creation of such machines will eventually be possible. Should either of these eventualities materialize, RSA would no longer be significant, and the only option remaining would be to shift to Secret-Key/Private Key cryptosystems.

3. QUANTUM HACKING CHALLENGES

Security is the sole purpose for cryptographic algorithms, so that your personal information either from bank or from any other places may not get into malicious hands. Who can use this information get into your personal space or use this info to transfer money from your bank without your will. The most commonly used algorithm as talked earlier is RSA (Rivest-Shamir-Adleman) ensures that the malicious decryption is not possible in a given time under certain circumstances. Nevertheless, most of these cryptographic schemes could be broken suddenly with unanticipated advances in algorithms and hardware, such as quantum computers. This is because these Quantum computers can efficiently prime

factorize very large integers in polynomial-time. There are many methods for attacking RSA, such as the integer factorization attack, the discrete logarithm attacks, the public exponent attacks, the private exponent attacks and side channel attacks. There are some quantum computer approaches with are successfully implemented {First implementation of Shor's algorithm (factorization of 15 = 3x5) was realized using nuclear magnetic resonance (Vandersypen et al., 2001)}. IBM has 20 qubits superconductivity based quantum computers. Google, IonQ, Rigetti also has supercomputers in laboratories. Still there are many technical challenges for building hardware for gate based quantum computers with large number of qubits.

3.1 Shor's Algorithm for Factorization

It is a polynomial time quantum factoring algorithm, proposed by Shor in 1994. One can solve the Integer Factorization Problem in a time proportional to $O((\log n)^{2+\varepsilon})$. Instead of giving a quantum computer algorithm to find the factor of integer n, it finds the order of an element x in the, which is the least integer r such that $x^r \equiv 1\ (mod\ n)$, where gcd(x, n) $= 1$. So, there is randomized reduction from factoring to the order of an element. To factor an odd number n, for a given method to calculate the order of an element, we choose a random x and find the order of r_x of x and hence compute gcd $(x^{\frac{r_x}{2}} - 1,\ n)$. This only fails if $x^{\frac{r_x}{2}} \equiv -1\ (mod\ n)$. Using this it can be shown that this to find the factor of an integer by this algorithm has probability at least $1 - {}^{1}/_{2^k}$ where k is the number of distinct prime factors of n. This algorithm fails if the number n is a power of prime number, which can be efficiently done with already present factorizing algorithms.

To find value of r for given x and n, such that $x^r \equiv 1\ (mod\ n)$, we proceed as. Firstly, find the smooth q with $2n^2 \leq q < 4n^2$. Next, we put our machine in uniform superposition of states, leaving machine in state

Algorithm for attacking RSA	Success probability	Time complexity	Qubits	Theoretical basis	Type of attack
[12, 13]	P_{Shor}	$O\left((\log n)^3\right)$	$3\lceil \log n \rceil$	Factorization	Integer factorization attack
[14]	$\varphi(r)/3r$	$O\left((\log n)^3\right)$	$4\lceil \log n \rceil$	Factorization	Integer factorization attack
[14]	P_{Shor}	$O\left((\log n)^3\right)$	$3\lceil \log n \rceil$	Factorization	Integer factorization attack
Shor's	$\approx \frac{\varphi(r)}{r}$	$O\left((\log n)^3\right)$	$3\lceil \log n \rceil$	Non-factorization	RSA fixed-point attack

where $3\varphi(r)/\pi^2 r \leq P_{Shor} < 4\varphi(r)/\pi^2 r$.

Table 1: Resource Comparison of Algorithms

$$\frac{1}{q^{1/2}}\sum_{a=0}^{q-1}|a\rangle$$

Next, we compute $x^a \ (mod\ n)$, this leaves our machine in the state

$$\frac{1}{q^{1/2}}\sum_{a=0}^{q-1}|a, x^a \ (mod\ n)\rangle$$

Next, we perform quantum Fourier transformation A_q mapping $a \rightarrow c$ with amplitude $\frac{1}{q^{1/2}}\exp\left(\frac{2\pi iac}{q}\right)$, this leaves our machine in state

$$\frac{1}{q}\sum_{a=0}^{q-1}\exp\left(\frac{2\pi iac}{q}\right)|c, x^a \ (mod\ n)\rangle$$

Finally, we observe the machine and observe the value of c, now we compute the probability that our machine should end in the state $|c, x^a \ (mod\ n)\rangle$, where we may assume $0 \leq k < r$. Summing over all possibility, we get the probability,

$$\left|\frac{1}{q}\sum_{a:x^a\equiv x^k}\exp\left(\frac{2\pi iac}{q}\right)\right|^2$$

Where sum is over all a, $0 \leq a < q$, such that $x^a \equiv x^k (mod\ n)$. Because the order of x is r this sum is equivalent over all a satisfying $a \equiv k \ (mod\ r)$. Writing $a = br + k$, we find that the above probability is

$$\left|\frac{1}{q}\sum_{b=0}^{\lfloor(q-k-1)/r\rfloor}\exp\left(\frac{2\pi i(br+k)c}{q}\right)\right|^2$$

We can ignore the term of $\exp\left(\frac{2\pi ikc}{q}\right)$, as it can be factored out of sum and has magnitude 1. We can replace rc with $\{\text{rc}\}_q$, where $\{\text{rc}\}_q$ is the residue which is congruent to rc (mod q) and is in the range $-\frac{q}{2} < \{rc\}_q \leq \frac{q}{2}$. This leaves us with expression

$$\left|\frac{1}{q}\sum_{b=0}^{\lfloor(q-k-1)/r\rfloor}\exp\left(\frac{2\pi ib\{rc\}_q}{q}\right)\right|^2$$

We can show that $\{rc\}_q$ is small enough, hence we can use the change of variable $t = \frac{b}{q}$ and approximate sum with integral as

$$\left|\int_0^{\frac{1}{q}\lfloor(q-k-1)/r\rfloor}\exp\left(2\pi ib\{rc\}_q t\right)dt\right|^2$$

If $|\{rc\}_q| \leq r/2$, this quantity can be shown to be shown to be asymptotically bounded below by $4/(\pi^2 r^2)$, and thus at least $1/3r^2$. The probability of seeing a given state $|c, x^k \ (mod\ n)\rangle$ will thus be at least $1/3r^2$ if

$$\frac{-r}{2} \leq \{rc\}_q < \frac{r}{2}$$

I.e. if there is a d such that

$$\frac{-r}{2} \leq rc - dq < \frac{r}{2}$$

Dividing by rq and rearranging the terms gives

$$\left|\frac{c}{q} - \frac{d}{r}\right| \leq \frac{1}{2q}$$

We know c and q, because $q \leq 2n^2$, there is at most one fraction d/r with $r < n$ that satisfies the above inequality. Thus we can obtain the fraction d/r in the lowest terms by rounding c/q to the nearest fraction having denominator smaller than n. This fraction can be obtained in Polynomial time by using a continued fraction expansion of c/q.If we have fraction d/r in the lowest terms and if d is prime to r, we will get r. Thus, ones we have the factors of the RSA public key, it means we have the private key also. So anyone with the public key can decrypt the data and has the access to the secret information. The whole world will be under threat.

3.2 Shor's Algorithm for Discrete Logarithm

On the similar ground Shor's algorithm can also be used for calculating discrete logarithm problem efficiently in polynomial-time. The discrete log problem is stated as: given a prime p, a generator g of the multiplicative group (mod p) and an x (mod p), find r such that $g^r \equiv x \ (mod\ p)$.

4. Countermeasures and Solutions to these Challenges

With emergence of quantum computers the threat to privacy is increasing. One can think of going back to Secret key cryptographic scheme in which each pair of sender and receiver has a secret key which is used to both encrypt and decrypt the data. But this may or may not work as we are still advancing in quantum algorithms as like the Grover's algorithm which can search the unsorted database in a time proportional to $O(\sqrt{n})$ which requires $O(n)$ operations for classical algorithms (Grover, 1996), so there may be development of new algorithm that can guess the key efficiently. Than the secret key scheme will also fail. So, the question arises what should be done?

The answer is Quantum cryptographic which is in fact quantum key distribution (QKD) protocol (Bennett & Brassard, 1984), which has been implemented and commercially available for more than a decade. Quantum mechanics can be used to design a completely secure quantum channel by the use of photons which tiny packet of energy and the concept of polarization is related to the orientation of the electric field component of these waves. Ordinary light consist of light having different polarizations. If we pass this light to a polarizer the unnecessary polarization trims out and it has a particular polarization. These polarized photons is referred as a qubit in quantum cryptography (similar to a bit in in Classical Computing).

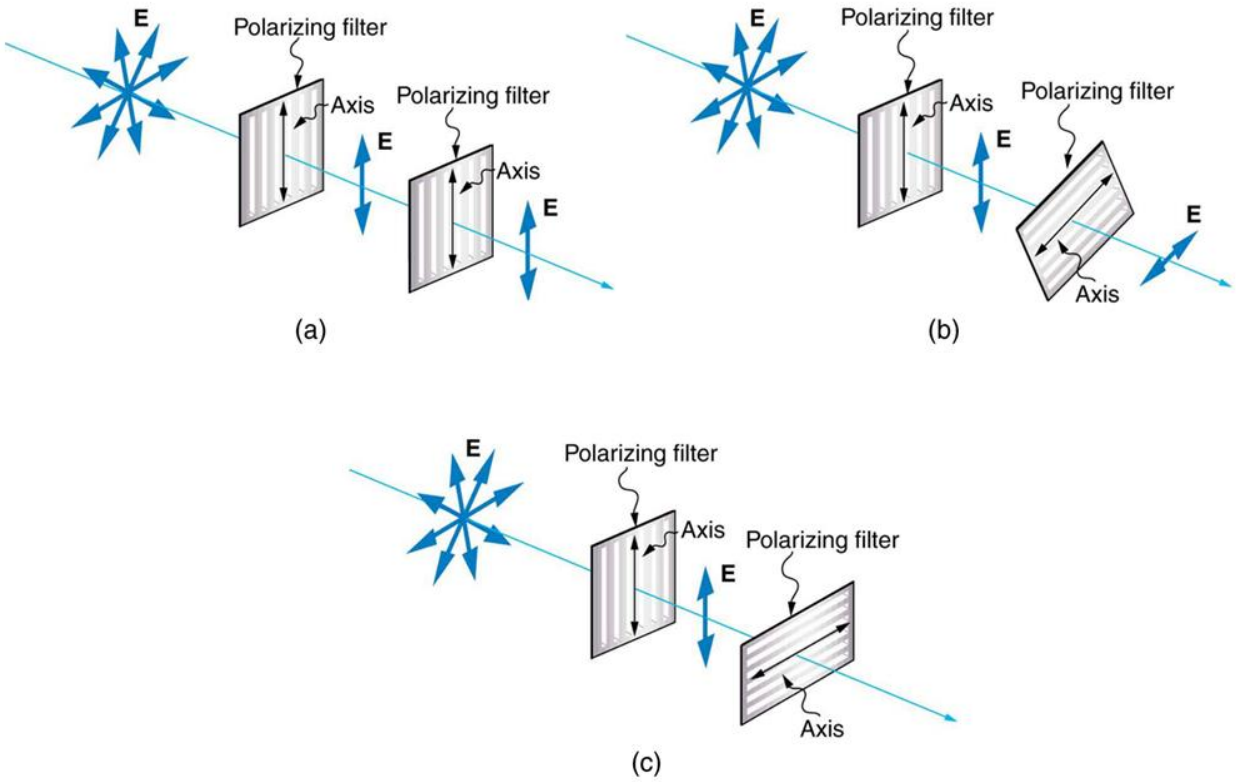

Figure 2: Unpolarized light enters the first filter which only allows light in specific direction. Second Polarizer is used to again polarize the photon to different orientation.

a) Second polarizer allows the whole photon, no trimming occurs.
b) Second polarizer is diagonal, it emits the component of initial polarization.
c) Second polarizer is at 90^{o} which allows to photon through it.

We send a polarized photon and receiver measures the polarization which is accomplished by using another polarizer filter. But this detection can be done conveniently by birefringent crystal (like calcite) which sends incident photon depending on their polarization, on one of the two paths.

1. It passed the horizontally polarized light as it is.
2. Vertically polarized light is deflected by some angle.
3. Diagonally polarized light are repolarized at random in either the vertical or horizontal direction and are shifted accordingly.

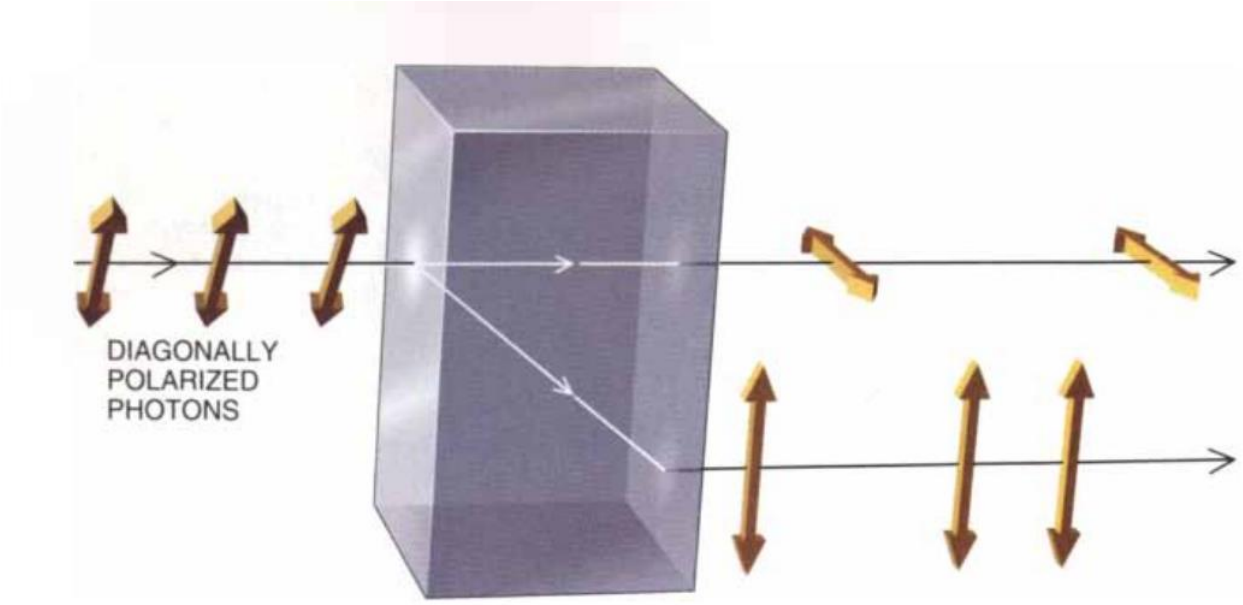

Figure 3: Diagonally polarized light entering into calcite crystal.

We use two detectors at upper and lower. If upper detects it is horizontal is lower detects it is vertical. But it fails for diagonally polarized light. So we rotate apparatus by 45^{o}. Now either we can share a secret key and use it to subsequently encrypt or decrypt data or we can use a public channel as described below.
Describing a similar scheme, let Alice and Bob use the public channel. First Alice generated and send a polarized photon to Bob. He decides randomly to choose any one method (either Rectilinear or Diagonal orientation of apparatus) to measure photon. Bob only announces this method publicly but not the results. Alice tells him publicly that he has choose right kind or not. They both discards wrong measurements.
As stated by fundamental concept of Quantum Mechanics, one cannot make an exact copy of a qubit (No Cloning Theorem). So, if Eve interprets some photon, there will be change in photon if she further transmit it to Bob. So to detect Eve, on comparison if there is evidence of eavesdropping they disregards their data and start with fresh batch. These type of scheme can be further extended to more number of qubits. Greater the number of qubits, greater is security against Brute-Force attack. These methods can be further refined to get better quantum channel and ensure a secured data transfer even after advent of Quantum Computers.

5. Conclusion

Concluding the notions now we can say that quantum computing has the potential to break the current security system in near future. So, we need to optimize the post quantum cryptographic schemes and replace the old cryptosystem with quantum cryptosystem as soon as possible. Still, there is big challenges in front of Quantum computer so that these shall be able to replace the existing computers. Real quantum crypto analysis is most likely to be finalized in 10 years.

6. References

1. Bennett, C. H., Brassard, G., & Ekert, A. K. (1992). Quantum cryptography. *Scientific American*, *267*(4), 50–57. https://doi.org/10.1038/scientificamerican1092-50

2. Kanamori, Yoshito and Yoo, Seong-Moo (2020) "Quantum Computing: Principles and Applications," Journal of International Technology and Information Management: Vol. 29: Iss. 2, Article 3.D. https://doi.org/10.58729/1941-6679.1410
3. Gisin, N. *et al.* (2002) *Quantum cryptography*, *Reviews of Modern Physics*. Available at: https://doi.org/10.1103/RevModPhys.74.145
4. Zahabiun, N. (2020) *One time pad encrypted messaging system*, *UDSpace*. Available at: https://udspace.udel.edu/handle/19716/27786
5. Zbinden, H., Bechmann-Pasquinucci, H., Gisin, N. *et al.* Quantum cryptography . *Appl Phys B* **67**, 743–748 (1998). https://doi.org/10.1007/s003400050574
6. Robles, S. (2006). The RSA Cryptosystem. Massachusetts Institute of Technology. Retrieved September 22, 2023, from https://dspace.mit.edu/bitstream/handle/1721.1/100853/18-304-spring-2006/contents/projects/rsa_robles.pdf
7. Rivest, R. L., Shamir, A., & Adleman, L. M. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126. https://doi.org/10.1145/359340.359342
8. Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 124-134. https://doi.org/10.1109/SFCS.1994.365700
9. Wang, Y., Zhang, Y., & Li, Y. (2018). Quantum polynomial-time fixed-point attack for RSA. China Communications, 15(2), 25-34. https://doi.org/10.1109/CC.2018.8300269
10. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 212-219. https://doi.org/10.1145/237814.237866
11. Liu, D. (n.d.). The one-time pad. University of Toronto. Retrieved October 6, 2023, from https://www.cs.toronto.edu/~david/course-notes/csc110-111/08-cryptography/02-one-time-pad.html
12. Shor, P. W. (1997). Polynomial-Time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484–1509. https://doi.org/10.1137/s0097539795293172
13. Wu, W., Zhang, H., Wang, H., Mao, S., Jia, J., & Liu, J. (2015b). A public key cryptosystem based on data complexity under quantum environment. Science China Information Sciences, 58(11), 1–11. https://doi.org/10.1007/s11432-015-5408-5
14. Cao, Z., & Cao, Z. (2014). On Shor's Factoring Algorithm with More Registers and the Problem to Certify Quantum Computers. IACR Cryptology ePrint Archive, 2014, 721. https://eprint.iacr.org/2014/721.pdf
15. L.H Liu and Z.J Cao, "On computing $ord_n(n)$ and its application", Information and Computation, vol. 204, no. 7, 2006, pp. 1173-1178.