NABEA AL-AJYAL FOUNDATION PRESS
Online ISSN: 3078-5413
CyberSystem Journal (CSJ)
csj.nabea.pub
CyberSystem Journal Research Article

Quantum Cryptanalysis: Evaluating the Impact of Shor's and Grover's Algorithms on Modern Encryption Standards

Mithal Hadi Jebur*, **Sumar Mohamed Khaleel**

Computer Center, University of Babylon, Hillah 51002, Iraq

* Corresponding Author: **Mithal Hadi Jebur**, Email: mithalhadi@uobabylon.edu.iq.

Abstract: Motivated by Shor's algorithm and its attractive features, the milestone results in quantum cryptanalysis were the discovery of quantum differential and linear cryptanalysis. In quantum cryptanalysis, quantum distinguishers imitate the classical setting. Details differ; however, as the distinguisher in the quantum setting can take maximum coset superposition of all possible subsets of plaintext pairs. Using quantum measurements, the winning gap of the game is exploited so that a distinguisher can still guess the secret key perfectly with a constant probability. Symmetric primitives also suffer reduced ideal security in the quantum world, but this security reduction is less drastic than for most asymmetric primitives. Stream ciphers, block ciphers, and cryptographic hash functions are primitives that are believed to resist quantum attacks. Analogs to Shor's algorithm may say how hard it is to build a quantum computer, but devising quantum algorithms to outperform the best classical attacks for widely-used cryptographic primitives is probably outside the reach of current even if exponentially growing noisy intermediate-scale quantum (NISQ) computers.

Access this article online

Keywords: Grover's algorithms, Quantum cryptanalysis, Shor's, Modern encryption

1. Introduction

LARGE quantum computers would have consequences hardly imaginable for reasonable people in the present day, having huge consequences on weather prediction, pharmaceutical discovery, investment, the invention of technology and much more. Cryptography would certainly be dramatically impacted among those disciplines. In 1994, Peter Shor famously proposed a quantum algorithm for integer factorization, breaking with a polynomial number of gates the public-key cryptosystem proposed by Rivest et al. (the original RSA). It is widely believed that Shor's algorithm is optimal in terms of the number of required elementary gates, and it turned a thought-provoking academic question into a credible and substantial threat for ongoing secrecy in less than two decades [1]. Since this groundbreaking publication, the cryptographic community has decided to start worrying about this threat and to study its impact. One compelling reason for starting to take action at a moment, when no quantum computer exists: even current pre-quantum long-term secrets are at risk. For example, by storing communications encrypted today, intercepted adversaries might be able in the future to decrypt them [2]. This largely explains why post-quantum cryptosystems, based on lattices or codes, have during last year's become a very hot topic in cryptography.

Received August 25, 2025; Revised September 28, 2025; Accepted October 25, 2025; Published December 31, 2025
https://doi.org/10.57238/csj.2025.1012

2. Foundations of Quantum Cryptanalysis

Large quantum computers would have huge consequences in a number of scientific fields. Cryptography would certainly be dramatically impacted: for instance, factoring algorithms make asymmetric primitives totally insecure in a post-quantum world. The cryptographic community has decided to start worrying about this threat and to study its impact. Even current pre-quantum long-term secrets are at risk as it seems feasible for a malicious organization to simply store all encrypted data until it has access to a quantum computer. This explains why post-quantum cryptosystems, based on lattices or codes, have become a very hot topic in cryptology. Researchers are now concentrating their efforts to provide efficient alternatives that would resist quantum adversaries. Symmetric primitives also suffer from a reduced ideal security in the quantum world, but this security reduction is much less drastic than for many asymmetric primitives. The main quantum attack on symmetric algorithms follows from an algorithm for searching an unsorted database in time. It offers a quadratic speed-up compared to a classical attack. The current consensus is that key lengths should be doubled to offer the same security against quantum algorithms.

The security of public key and private key cryptosystems against quantum adversaries is a very hot topic. Concerning the symmetric world, the current security model for block ciphers and hash functions is already quantum-resistant as it only considers classical adversaries. One would thus like to know whether a quantum adversary can attack modern symmetric primitives more efficiently. Concerning the quantum security of block ciphers, only one analysis of the well-known candidates is presented [3]. Candidates are also given, showing that quantum adversaries recover the key with negligible estimates after a few encryption queries. In the last few years, a few papers have studied the security of symmetric cryptography against quantum attacks. The current security model for symmetric primitives only considers classical adversaries as shown in Table 1 which shows theory and operation.

2.1 Quantum Computing Basics

The impact of quantum computing on present cryptography Lov Grover designed a quantum algorithm that can search an unsorted databases using O(sqrt(N)) queries, thus sub-exponentially better than deterministic classical algorithms that need O(N) queries. Grover's algorithm can find a specific entry in an unsorted database of N (N =2^n) entries in sqrt(N) searches. Applying to the most widely used classic encryption standard, Grover presented how a quantum implementation of well-known algorithms such as exhaustive key search and meet-in-the-middle are faster than a brute force attack. Bone and Castro were notable for considering the impact of a possible application of Grover's algorithm in the search of the private key of the Data Encryption Standard (DES), which as remarked before, relied its security essentially on the 56-bit key. They pointed out that, since 2^{56} = 7.2058E+16, Grover's quantum algorithm needs only 185 searches to find the key, violating the conventional implementation of a symmetric encryption scheme. Buchmann, Fiorini and Sarnak have stated that Grover's algorithm does have some applications in symmetric cryptosystems, even finding quantum computers to be competitive in faster running-time than the fastest known classical computer algorithms. However, the search procedure proposed by Bone and Castro for the secret key recovery of DES is more than 10^10 times faster compared to the Grover's algorithm implementation of it. Desirable constructions of public and private keys for PKC and SKC, respectively, are as large as possible, so that classical and/or quantum searching procedures are impractical using the best available classical and/or quantum computer technology [12]. Currently recommended PKC and SKC methods for the AES are not known to be equivalent to the integer factorization and the discrete logarithm problems, respectively, for potential reasons that will be addressed later. In this way, they are computationally secure also against realized quantum computers using the best algorithm available, which is Shor's gcd-type algorithm. However, there are ECC modifications of the discrete logarithm problem for other cryptosystems. For instance, it is known that in over-elliptic curves, the d log problem can be transformed in a record problem with O(sqrt(2^m)) < m = O(bit(k)) cost in classical computation. In other words, n-cover over-elliptic curves of small numbers n lead to a drop faster than O(2^{k/2}) in the security level of the ECDLP. Kirsch and Chow explained how a modified version of Shor's algorithm implemented on this computer could decrypt compressed or uncompressed data encoded with such public key cryptosystem [13]. Additionally, simulation results and error correction demands in the implementation of Shor's algorithm in IBM q are provided. Lastly, it was stressed that ECC has a shorter key length compared to RSA in equivalent security levels, thus being faster to break by the implementation of Shor's algorithm. In conclusion, the quantum attack of exponential speedup over the classical counterparts are only available for public key schemes based on integer factoring and dlog problem on Zpace(p)-based cryptosystems such as RSA and ECDH.

Table 1. Theory and operation

Algorithm	Theoretical basis	Operational principle	Target cryptographic schemes	Quantum complexity	Classical comparison	Primary effect	Reference
Shor's Algorithm	Based on quantum Fourier transform (QFT) and period-finding in modular arithmetic. Exploits superposition and interference to determine the periodicity of functions.	Converts integer factorization and discrete logarithm problems into period-finding problems solvable efficiently on a quantum computer.	RSA, ECC, DSA, Diffie–Hellman	O ((log N)3) time complexity	Classical factorization requires exponential time O (e^ {(1.9(log N) ^ {1/3}(log N)^{2/3})}).	Breaks asymmetric encryption by revealing private keys.	[4-6]
Grover's Algorithm	Based on amplitude amplification in quantum search space. Uses superposition and inversion about average to accelerate unstructured search.	Searches unsorted databases of size N in O(√N) time, providing quadratic speedup over brute-force.	AES, DES, SHA-2, SHA-3	O(√N) queries	Classical brute-force requires O(N) queries.	Reduces effective key strength by half (e.g., AES-256 → AES-128).	[7-9]
Quantum Fourier Transform (QFT)	A linear transformation on quantum amplitudes analogous to the discrete Fourier transform.	Core subroutine in Shor's algorithm for finding hidden periodicity efficiently.	Supports integer factorization and discrete log calculations.	O((log N)^2) gates	Exponential-time classical Fourier transform for same problems.	Enables exponential speedup in number-theoretic problems.	[1, 3]
Amplitude Amplification (Grover's Core)	Enhances the probability amplitude of desired quantum states through iterative reflection and interference.	Repeated oracle queries increase amplitude of correct result.	Generic search problems, cryptographic key search.	O(√N) oracle calls	O(N) classical queries.	Enables quadratic search advantage across cryptographic primitives.	[10, 11]

Currently used encryption and signature schemes are secure against attacks by quantum computers running Shor's algorithm, due to the large computational resources needed. Recent researches suggest that improvements in the efficiency of calculation of the modular exponentiation and other operations could make Shor's algorithm more likely to be implemented on a real quantum computer. For example, 160-bit elliptic curve cryptographic keys are estimated to be breakable by a 1000-qubit quantum computer if the current polynomial-time quantum algorithm is used to solve the elliptic curve discrete logarithm problem. In addition, a 2000-qubit quantum computer could be able to simultaneously factor N semiprimes of bit length 1024, implying the threat for the widely used RSA cryptosystem. The necessary number of qubit operations to break these cryptographic systems is, however, contingent on the implemented quantum algorithm and it may evolve in the future, as shown in Table 2 which shows strategic evaluation.

Table 2. Strategic evaluation

Aspect	Shor's algorithm	Grover's algorithm	Impact on encryption standards	Strategic response / mitigation
Primary target	Asymmetric cryptography (RSA, ECC, DH)	Symmetric cryptography (AES, SHA)	Threatens public-key infrastructure (PKI) and digital signatures	Transition to post-quantum cryptography (PQC) standards (e.g., lattice-based, code-based)
Complexity advantage	Polynomial time factorization and discrete log solving	Quadratic speedup in brute-force search	Complete break of RSA/ECC; reduced security level for AES and hash-based algorithms	Increase key sizes for symmetric ciphers (AES-256); adopt PQC algorithms for asymmetric use
Vulnerability type	Structural (mathematical basis of encryption)	Exhaustive search reduction	Total compromise of confidentiality and authentication mechanisms	Deploy hybrid cryptosystems (classical + PQC) during transition period
Quantum resource requirement	Millions of stable qubits (logical) for 2048-bit RSA	Thousands of qubits depending on key length	Long-term threat (5–15 years)	Develop scalable quantum-resistant infrastructures and policies
Timeline for realistic threat	Medium-to-long term (once fault-tolerant quantum computers emerge)	Near-to-medium term (with mid-scale quantum computers)	Progressive degradation of classical cryptographic confidence	Continuous evaluation and NIST compliance with PQC updates
Impacted standards	RSA, ECC, DSA, Diffie–Hellman	AES, SHA-2, SHA-3	Internet protocols (TLS, SSH, IPSec, blockchain)	Standardization of quantum-safe versions of these protocols
Strategic research focus	Quantum-resistant public-key algorithms	Optimization of symmetric key parameters	Development of hybrid and post-quantum solutions	Industry collaboration with NIST PQC projects (e.g., Kyber, Dilithium)
Overall risk level	Critical (total break of key infrastructures)	Moderate (manageable with longer keys)	High overall impact on security ecosystems	Adopt PQC migration strategies and quantum key distribution (QKD)

On the other hand, a quantum computational model proposed by Lov Grover inspired David Bone and Saulo Costa de Castro to present a MITM-type attack for 9-round DES. They showed that, using R(DES) potential outputs on the raw/doppel of the function f, the number of quantum queries using Grover's algorithm to find the key of DES is only O (2^{56/2}) = O(2^{28}) = 268, 435, 456. Moreover, simulated experiments using Shor's and Grover's algorithms gave strong evidences that the complexity of the best classic attacks against ECC logarithm and RSA integer factorization related problems drops sharply compared with the difficulty of these algorithms on respective instances. Interestingly, experimental assessments using Shor's and Grover's algorithms for ECC logarithm and RSA factorization related problems. Furthermore, it was provided the number of quantum queries required to perform key-recovery attacks on different flavors and rounds of DES considering different settings for Simon's algorithm [13].

2.2 Quantum Cryptography Fundamentals

The Quantum World. The odd laws of quantum mechanics and its impact on any aspect of science could be summarized as follows:

- Quantum systems are inherently probabilistic. There are certain properties of quantum systems, like spin or quanta polarization, that elude precise measurement. Experiments can be performed to measure these properties and the probability of measuring each possible value can be established. Associated with this property is the "collapse" theory. Prior to measurement, the property that evades measurement only possesses a probability distribution of being at each possible value. The act of measurement forces this probability distribution to favor the fixed measurement value. It is important to note this theory only existed after the late 20th century, while the first exposition of

quantum mechanics occurred in the early 20th century. Einstein disliked the theory so much he tried to discredit it by proposing impossible experiments like the famous Einstein-Podolsky-Rosen paradox (EPR paradox). In 2015, an experiment was conducted that ultimately proved the EPR paradox impossible in reality for verifying the collapse theory.

- Quantum systems do not behave classically [14]. At a macroscopic level, one notices clear outcomes; balls that are thrown either land or miss. Yet, at a quantum level, outcomes are continuous. If a problem is modified at the nano-scale level, the parametric gain error from measurement is significantly amplified. That's not all; a wavefunction represents all possible states at the same time. As such, Schrödinger's cat is half-dead and half-alive. It is important to bear in mind applying the laws of quantum mechanics massively limit some conclusions to be drawn as many aspects of quantum mechanics appear counterintuitive 1.

3. Classical vs. Quantum Cryptanalysis

Since public-key cryptosystems are threatened by Shor's algorithm, many attempts have been made to develop their equivalents that could safely be used in quantum computers. On the other hand, the effect of quantum computing on symmetric systems is not yet the target of considerable research, the security of symmetric ciphers against quantum adversaries depends heavily on the efficiency of cryptanalytic tools. Similarly to the assumptions regarding the difficulty of decoding the product of two large prime numbers to yield the original numbers, the security of RSA cryptosystems relies on the hardness of two combinatorial problems: factoring and the RSA problem. Since most key agreement and establishment protocols are based on number theory and therefore rely on the hardness of factorization, they could be broken in polynomial time by an "ideal" quantum computer due to Shor's algorithm [15]. There are currently no candidates for public-key systems that withstand quantum attackers, although much effort is currently being put into making public-key systems safe from quantum attacks. From this standpoint, symmetric cryptography seems to be a viable alternative, since the security of these schemes relies on the different difficulty of finding the key and of applying it to the cryptosystem query.

Nowadays, symmetric cryptosystems are used continuously to secure channel key encryption, and authentication by means of cryptographic hash functions, message authentication codes are currently protected from quantum adversaries. The evaluation of the security of symmetric primitives against quantum attacks could gain insight into this question. In studying this issue, improving classical cryptanalytic methods with the help of quantum algorithms is an interesting avenue. The complexity of itinerant quantum algorithms provides a quadratic speed-up over the best known classical ones. Given an oracle implementing a black-box access to a function, Grover's algorithm can find an element for which f = 1 out of N possible ones in time O(√N). Importance of Grover's cryptanalysis and its uses with the purpose of identifying practices which could be used against proposed target algorithms. Oracle queries needed if a quantum equivalent of an RSA decryption algorithm and High Level Security standard is developed for finding collisions on the hash function output [16]. The parameters are then modified to ensure that output of the quantum algorithm is returned to the user omitted from the query count. It is important to understand if the availability of quantum devices allows for the development of faster dedicated attacks against classical symmetric schemes with respect to standard brute-force attacks based on Grover's algorithm. Surprisingly, quantum-dedicated differential and linear cryptanalysis cannot always outperform classical generic attacks against standard assumptions, at least regarding the number of rounds of the studied primitives.

3.1 Key Differences

Modern encryption forms the backbone of the contemporary digital world and underpins the security and confidentiality offered by the numerous encryption services ranging over cloud security, e-mail, e-commerce, and secure messaging. This review investigates the impact the development of Shor's and Grover's quantum algorithms will have upon several widely used symmetric and asymmetric key cryptographic algorithms by outlining them along with their major concerns [17]. A significant impact on the security of currently used cryptographic standards has been announced due to these promising algorithms, even though large quantum computers are not yet available in the near future 3. Current computer technology allows Shor's algorithm to quickly solve problems underlying most of the asymmetric key cryptographic algorithms in common use (RSA being the most well-known).

Grover's quantum search algorithm gives a quadratic speed-up for searching problems, affecting almost all known cryptographic hash functions and symmetric algorithms. As a consequence, symmetric key sizes are effectively halved (e.g., a symmetric key size of 256 bits can be brute forced in 2^128 operations using a quantum

computer), necessitating a significant change in how symmetric encryption strength is estimated. In basic terms, consider a fan named Alice who hopes to send an encrypted message to a universally-loved bobcat named Bob [18]. Bob and Alice nonetheless have a common enemy, who can intercept and store all the messages they exchange via some not-quite-legal means. Furthermore, this enemy has access to a quantum computer. As the future permits a surprising degree of parallel processing, encrypting the message to a wildly excessive degree is necessary to protect it from being decrypted by this quantum adversary 4.

3.2 Strengths and Weaknesses

Large quantum computers will have huge consequences on a number of scientific fields. Cryptography will certainly be dramatically impacted by the development of quantum computers: for instance [18]. Furthermore, the latter attacks are known to become more effective in the quantum setting. Symmetric primitives typically use keys that are much shorter than the number of possible states of the cryptogram. This is the basis for the information theoretic guarantees of standard security models. However, some quantum attacks are expected to use the superposition property of quantum bits and to benefit from much more refined probabilistic considerations. The aim of this workshop is to start filling the gap on these effect-based evaluations of symmetric primitives around the five most advanced quantum attack models: from 1997; from 2004; from 2012; and the recent adaptations of threshold implementations and lattice reduction algorithms. Effort will be made to start precisely defining all variants that have appeared in the literature and the meta-attacks on the mode of operation that can prevent them, Figure 1 shows decay of modern encryption security due to quantum algorithm.

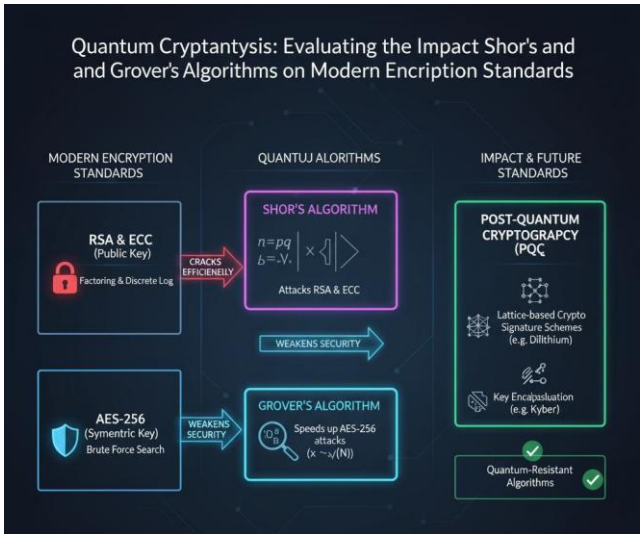

Figure 1. Decay of modern encryption security due to quantum algorithm

Similarly to other workshops, it will be asked to document as much as possible the threat model and all approximations needed to model the quantum attacks; this will be particularly delicate due to the reasons stated above. At the occasion of the workshop, a program of standardized experimentations that should be reported in order to communicate assess the attack performance (in the way public cryptanalysis competitions establish a state-of-the-art on classical attacks). These results may come from both theoreticians and experimentalists, this is the field where simulated quantum attacks may help conducting experimentalists [19]. As whenever applicable, researchers of assessed primitives that are involved in the attacks and the defense should communicate will be encouraged to interact. Finally, it will be encouraged to report attacks only on primitives for which there is a reasonable consensus that the attack configurations provide a relevant security level.

4. Shor's Algorithm: Breaking RSA Encryption

In 1977, Rivest, Shamir, and Adleman cryptographically assessed for the first time RSA encryption system. Since then, this encryption algorithm has become one of the most important cryptographic standards worldwide 5. The based difficulty of RSA encryption is the factorization problem of two large prime numbers n. Shor's algorithm carries out the number factorization in O (log2n) computational time due to a realization of quantum computer. This algorithm has a large weak point of built for decryption of the RSA encryption. Restagno in 1997 designed the quantum circuit for multiplication based on Shor's factoring algorithm. If the above quantum circuit is implemented, this factoring algorithm can be used for the first time as secret decryption keys for the RSA encryption. The overall quantum circuit is composed of controlled gates using the multiple targets and one control qubits [20]. Especially, the multiplier is a most important part of the quantum circuit because it is the base circuit in Shor's algorithm. During designing realization of the quantum circuit of Restagno's multiplier, optimization of these controlled gates is strongly desired. Proposed multiplier quantum circuits have the amount of the controlled gates as least as possible.

4.1 Theory and Operation

Quantum computing has been a hot research area in the past decade. Tremendous progress has been made on quantum hardware. Several different types of quantum computers have been under development: ion trap-based, solid state-based, quantumoptical-based, superconducting-

based, etc. In 2019, Google built the 55-qubit Sycamore quantum processor. IBM has presented an operational 50-qubit quantum computer. The Chinese company Alibaba also has shown a 50-qubit quantum computer.

Mature quantum hardware urges its software applications. Grover's search algorithm is applicable to all types of tasks including NP-hard problems. Previous works paid significant attention to symmetric and asymmetric cryptosystems, but almost no research has been done on hash functions. The design criteria NIST specified for quantum-secure hash functions are quite different from those for regular hash functions. Most famous hash functions, such as SHA-2, SHA-3, and MD5 are expected to be broken by Grover's algorithm with only 2\sqrt{n} evaluations. Merkle-Damgård constructions are particularly vulnerable to quantum attacks; HAIFA constructions provide a partial remedy. NIST PQC finalists tried to adopt either the sponge or the tree-hash mode as its compression function, providing resistance to quantum attacks.

Shor's algorithm is the most important quantum algorithm that can efficiently solve the integer factorization problem and the discrete logarithm problem. From the point of view of the amount of qubits available, Shor's algorithm is by no means practical. No quantum computer with even dozens of qubits has been constructed so far to date, while it may take several hundred/thousands qubits to break the RSA-2048/DH-2048/ECC-224 scheme with a high success probability. Hence, although the common belief is that NSA may have already been running top-secret quantum cryptanalysis for more than a decade and has made some progress, current public quantum technology is far from threatening the security of the widely used cryptographic systems [21]. Furthermore, various NIST guidelines intended to increase the security such as quantum-safe elliptic curves and classical lattice-based cryptosystems were made public in July 2015. At the same time, growing concerns about post-quantum security have motivated the information security community to construct more secure cryptographic algorithms 1. Given the confidential nature of the matter and the significant R&D resource allocation, it is anticipated that the large cryptanalysis organizations or governments in possession of numerous quantum computers will be taking a leading role in developing advanced quantum cryptanalysis methodologies. In such a situation, cryptanalyzing widely used cryptographic protocols based on the RSA and ECC is entirely conceivable [22].

4.2 Potential Impacts on Security

The first step in evaluating the potential impacts of quantum cryptanalysis involving Shor's and Grover's algorithms against the symmetric and cryptographic standards is to briefly introduce what was found about those standards in terms of quantum and what is the intent of section. This is followed by a detailed analysis of quantum cryptanalysis against the underlying block ciphers keyed-hash message authentication codes (MACs) and public-key cryptosystems.

Referring to the evaluation of encryption standards, one considers those symmetric-key encryption algorithms and those public-key cryptography standards based on KEM and signature. To the best of the knowledge, they are selected as the cryptographic standards used in the majority of current Internet data communications. They have been analyzed for prospects against quantum cryptanalysis, and research in this area has been actively performed. Public comments that have been received all around the world require to revise the modes of operation to protect against quantum computing. Being based on the latest research as of the date of submission, the resulting analysis will contribute to the corresponding discussion on the update of standards and to the study of the future aftermaths of quantum computing on the cryptographic standards.

5. Grover's Algorithm: Search and Optimization

Grover's algorithm is a quantum search algorithm specified in 1996 by Lov K. Grover. It is an essential discovery in quantum algorithms with quadratic speedup to its best possible classical counterparts. This search algorithm is better than the exhaustive search only when it can be done in fewer than half N steps, which is impossible 6, Figure 2 shows quantum cryptanalysis in terms of evaluating quantum cryptanalysis impact curve.

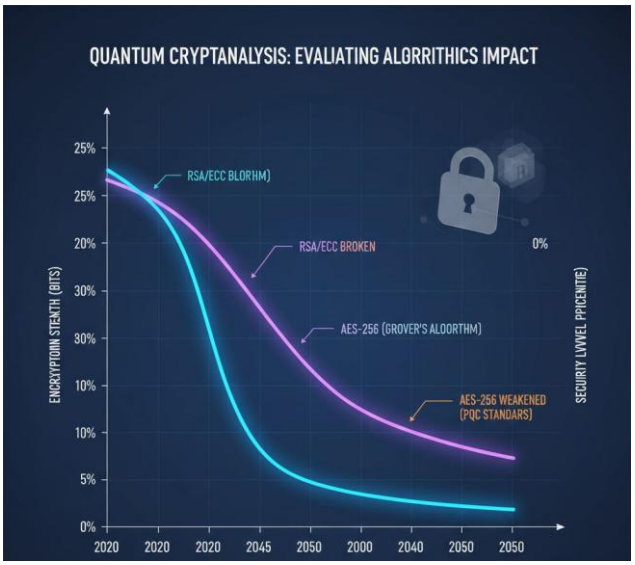

Figure 2. Quantum cryptanalysis impact curve: Shor's and Grover's algorithms vs. encryption standards (RSA/ECC and AES)"

The massive parallelism feature of the quantum computer will be applied here. Instead of running one Grover's search for all possible states, parallel running of a set of Grover's searches on all possible states except for a small subset is proposed. This subset is to be searched by the classical computer. It is very significant that quantum co-processors do not outperform the classical computer up to now. It is sufficient to consider the algorithm that gives quadratic speedup. Cumulative results of speedups suggest that quantum computers within this century will be built in decent scale but they will not replace the classical computers. It is possible that certain computational tasks will be solved in polynomial time. The primary intention is to evaluate the effectiveness of Grover's algorithms utilized in a quantum co-processor on a specific computational problem. Theoretical lower bounds for Grover's algorithm do not play a significant role here and are hardly touched in any of a heavily growing literature [23].

5.1 Algorithmic Overview

No practical quantum computer has been built yet, but the rapid technological development of large quantum computers will have dire consequences for classical cryptography 3. The most of symmetric and asymmetric or public key cryptographic and RSA related algorithms are vulnerable to the Shor's algorithm of quantum algorithms. Grover presented quantum search algorithm which has ability to give only a square root time boost for the searching of the key in symmetric schemes like AES and 3DES. For example, AES-128 bit can be cracked to a 2^64 effort using the Grover's Search Quantum algorithm. Currently, it is believed that the large data can be safely encrypted for the life time of the encrypted data with using the 256 bits key block cipher like AES costing a 2^{128} effort like brute force search. However, Grover showed that a brute force search or key recovery attack against block cipher will requirements to consider the a square root of the search-space size. Therefore, the post quantum lower bounds key sizes were formulated for the best security levels against Grover's search algorithm [24]. On the other hands public key cryptosystem which using a unique private key and corresponding public key, has a different type of vulnerability in terms of quantum computing than the symmetric key cryptographic systems. The security of asymmetric algorithms like RSA, Diffie-Hellman, and ECC are based on the mathematical hardness of prime factorization and discrete logarithm and with the Shor's algorithm can be solved the problem of in polynomial time. Major breakthrough within quantum computing will render all the present-day widely used asymmetric cryptosystems insecure.

5.2 Applications in Cryptanalysis

The development of quantum computing has greatly affected the world of classical cryptography. A representative example is Grover's quantum search algorithm. It can provide a quadratic speedup for any generic exhaustive key search, offering a very concrete evaluation of the security of symmetric cryptographic algorithms against quantum adversaries. It is also possible for this adversary to leverage quantum techniques inspired by differential and linear cryptanalysis, which can in many cases provide speedups to known attacks not only on small ciphers, but also on practical ones. Therefore, it is crucial to understand and integrate those new features in cryptographic designs to ensure the long-term security. Quantum Differential and Linear Cryptanalysis (DLC) is investigated in the symmetric setting. It is similar to usual attacks, with the exception that they exploit quantum algorithms, and try to recover the internal state of the cipher. It is shown how to construct such attacks and how they can be used on several widely spread cryptographic designs. It is demonstrated that in the symmetric setting (contrarily to the asymmetric or the hash setting) the results are mitigated. As found, this is mainly because the related key model hinders the quantum setting for most of the relevant keys. In this model, due to the addition of a random key in the quantum query, ciphers often resist quantum DLC at least as much as they resist classical ones [25, 26]. Therefore, it is possible to mitigate the quantum danger associated with symmetric ciphers in the context studied here. In this work the models and the background required to understand quantum attacks are explained; quantum attacks inspired from classical DLC are then detailed, and it is shown that quantum DLC can often be efficient following well-chosen paths in ciphers. It should be noted however that these results concern known variants providing an average complexity over the choice of these paths. It is also designed an experimental approach to find these paths and demonstrate in the case of the Fruit cipher that the best known classical attack is not always the best quantum one.

6. Quantum-Resistant Cryptography

In order to understand the threat to the cryptographic landscape posed by quantum computing, it is first essential to comprehend the underlying principles of each. Quantum computing is grounded on the principles of quantum mechanics and utilizes the unique properties of quantum bits or qubits to execute operations. States of classical bits are either 0 or 1, while those of qubits can be both simultaneously due to superposition. As a quantum computer's size (in bits) doubles, its capacity, as measured

by the number of states, increases only linearly. The strength of a quantum computer is built on its ability to leverage its state space to examine a vast number of possible solutions at the same time. Classical computers, on the other hand, are restricted to assessing solutions in sequence, examining only one option at a time. A quantum computer doesn't just consider one string of 0s and 1s but evaluates every will-be guess on all the possible strings at once 2. It is this behavior that enables quantum computers to perform some operations exponentially faster than classical computers and poses a significant threat to the security of many standard cryptographic schemes. The security of many commonly used cryptographic algorithms, such as RSA and ECC, is typically based on the hardness of certain mathematical problems. The reason why these schemes are secure is that the time complexity of the best-known classical algorithms to solve the corresponding problems is enormous. However, quantum algorithms, such as Shor's and Grover's algorithms, have been found to solve some of these problems efficiently on a quantum computer.

Shor's Algorithm, discovered in 1994, stands as a major leap in quantum computing towards developing a secure and widely adopted commercial quantum computer. Shor's Algorithm has two main features: it can solve the integer factorization problem, which would take a classical computer running the best-known algorithms superpolynomial time, in polynomial time and can also solve the discrete logarithm problem of elliptic curves in this same time frame. RSA and ECC cryptography rely on the assumption that these two problems are computationally hard. For a classical computer, both problems scale exponentially, more specifically sub-exponentially (with the number of bits n with difficulty order), and can be mainly solved via generic algorithms in order 2n. For a sufficiently large enough quantum computer, the RSA and ECC security parameters (size in bits n; $n \approx 2048$) are polynomially scaled exploiting Shor's Algorithm, resulting in their security breaking 7. In 2016, a quantum-safe alternative, PokeCryptography, specifically PokeCryptAES, was developed. This particular project will be running tests on PokeCryptAES. The asymptotic time complexity is O (2)n/2 = $O(\sqrt{2}n)$ for Grover's Algorithm. A classically targeted scheme is AES-256. It has a fixed security level of 128 bits. Grover's Algorithm can decrypt an n-bit key in O(2n/2) time; it can effectively decrypt AES-256 with 128-bit strength. Therefore, once again, AES and ECC need to be secured against QC. The National Institute of Standards and Technology is already taking action on this particular issue. It does act as a hand-prover, however, in "The Impact of Quantum Computing on Present Cryptography", it does illuminate all the points needed to act as a foundation and it foreshadows the evolving algorithms, just not as explicitly.

6.1 Post-Quantum Cryptographic Algorithms

Quantum computing is a radical approach to computation based on the principles of quantum mechanics. Quantum computers leverage the unique properties of quantum bits or qubits to perform computations. Quantum computing has the potential to revolutionize problematics that are beyond the reach of classical computers, from the fight against cancer to the struggle against climate change. However, this groundbreaking area also affects security issues. Since the 1970s, the security of digital communication is mainly based on mathematical problems that are difficult to solve. However, it has been known since the mid-1990s that some mathematical problems are solvable in polynomial time by a quantum computer. Quantum Cryptanalysis is the application of quantum algorithms to break cryptographic schemes 7.

The impact of quantum computing on cryptographic algorithms lies in its ability to execute certain mathematical operations exponentially faster than classical computers do. This groundbreaking advancement has raised a significant concern in the past few years by the security community, including the impact level of existing cryptographic systems and evaluating the security of future systems. There are three major cryptographic algorithms, which are widely used in today's digital communication that are RSA, ECC and symmetric key algorithms. Those algorithms are used to encrypt the message such that no third party would be able to read the content. Although a third party can collect the message during transmission, it would be impossible to understand the message without decrypting it 2. The decryption process requires a key that uniquely matches the encrypted message. The keys used in the decryption process are generated using information that only known by the sender and the receiver of the message. With the rise of quantum computing, this secure communication might not hold, because the quantum algorithms can be used to attack public key cryptographic systems.

6.2 Implementation Challenges

Large quantum computers would have huge consequences in several scientific fields and the internet. Cryptography would certainly be dramatically impacted. Seen from the quantum world, RSA, ECC, or the recent constructions of lattice based crypto no longer provide the intended security guarantees. Even older encryption techniques, such as block ciphers and Hash functions, could essentially be broken, as was shown by Shor and Grover in the mid-1990s. The cryptographic community has decided

to start worrying about this distant but sore threat and a large research effort has been dedicated to study and develop the required countermeasures: Quantum Cryptographic primitives and protocols 1.

Grover's quantum search algorithm provides a square-foot speed-up over classical attacks. As such, the Wisdom is that symmetric cryptographic primitives should use double their key sizes due to Grover's algorithm. It is conjectured that this would be sufficient to thwart any avenue to obtain larger speed-up. This would be consistent with the previous results, as Grover's algorithm provides square root speed-up to the best known quantum algorithms on some problems, including black-box queries to some functions as the cryptographic problem of the GFP or on collision search. A natural question is thus to ask if any symmetric cryptographic construction can be used to build a symmetric primitive providing 128-bit security level, even if the key size of the raw primitive is less than 256 bits.

7. Case Studies in Quantum Cryptanalysis

In the last decade, the research on implementing quantum computers has made huge progresses. Several quantum devices have been developed and tested and claim to be on the verge of outperforming classical computers in fundamental tasks. This is the case of the D-Wave, where its performance is still doubted by many researchers. However, Google, IBM, and the University of Innsbruck and of Vienna have proven some supremacy on quantum computers running on simulation problems with short circuits. The fact that the quantum elements are well preserved (more than 99.9%) and that a better coherence time has been achieved has been the most significant technological fact. In any case, many practical and theoretical obstacles are still to be overcome to build a full-scale quantum computer of the sufficient size to factor 2048-bit numbers or perform comparable operations. Future uses of these technologies may be geared towards the development of large super-cooled dilution refrigerators with high-performance metal enclosures to protect high-fidelity quantum processors 1. There is substantial ongoing work aimed in this direction, which will benefit to quantum cryptanalysis and, more generally, to quantum computing. This is why evaluating the real impact of quantum cryptanalysis, and in particular of quantum computers on modern encryption standards, is a significant and timely scientific question.

Cryptography is one of the youngest disciplines in computer science. It was formally defined in the middle of last century, after the appearance of the first computers. Namely, the list of cryptographic definitions was published in 1949. The first cryptanalysis ideas came up as soon as the invention of devices aimed to protect information. Experts from intelligence agencies were able to defeat a large number of so-called cipher systems. With the birth of digital communications, the RSA encryption scheme was described, which is based on factoring the product of two secret prime numbers, and the DES was standardized, which is a symmetric encryption that works over small blocks of 64-bits. Since these seminal concepts, new cryptographic algorithms have been developed. More alternatives appeared as the works of others. This option implies to work in the ring of polynomials extending the original ring of integers, and was revolutionary at the time. Rudimentary forms of public key cryptography have been already suggested, but they realized in early 1970 with the announcement of RSA.

7.1 Real-World Examples

Large quantum computers would have huge consequences in a number of scientific fields, which is why so much effort and money are currently being spent in producing them. Cryptography would certainly be dramatically impacted: for instance, Shor's factoring algorithm makes asymmetric primitives such as RSA totally insecure in a post-quantum world. In fact, long-term encryption is already not secure against traditional adversaries. A malicious organization might be able to decrypt messages encrypted today and stored for many years once quantum computers become available. The cryptographic community has decided to start worrying about this threat and to study its impact. Even current pre-quantum long-term secrets are at risk as it seems feasible for a malicious organization to simply store all encrypted data until it has access to a quantum computer. This explains why post-quantum cryptosystems have become a very hot topic in cryptology 1.

Symmetric primitives suffer from a reduced ideal security in the quantum world, but this security reduction is much less drastic than for many asymmetric primitives. So far, the main quantum attack on symmetric algorithms follows from Grover's algorithm for searching an unsorted database. It can be applied to any generic exhaustive key search, but merely offers a quadratic speed-up compared to a classical attack. Therefore, the current consensus is that key lengths should be doubled in order to offer the same security against quantum algorithms. Doubling the key length is a useful heuristic, but a more accurate analysis is definitely called for. Only recently, a few results have begun to challenge the security of some symmetric cryptography constructions against quantum adversaries.

7.2 Successes and Limitations

Shor's algorithm has been developed for over 20 years, but Schrover attacks have proved impossible up until 2022 3. The first Impossible after-generation was applied to ciphers. In 2017, high-probability QTDC strategies are developed to increase the number of rounds (NR) paying special attention to complemented differentials (CD). Two quantum algorithms are proposed to create high-probability truncated CDs and high-probability impossible CDs. These cryptographic issues require solving the linear equations or (non-) linear inequalities of the secret key variables subjected to a certain condition 4. It is defined as impossible Distinguishable or impossible relation. Using these situations, two quantum quartic sieve algorithms are designed to search for s-boxes. They are the first quantum strategies capable of outputting multiple input value pairs involving differentials or CDs. A representative example is Grover's quantum search algorithm, because it indicates that in the post-quantum world, the length of keystreams and the key lengths of symmetric primitives need to be doubled to maintain an equivalent robust safety.

8. Evaluating the Security of Modern Encryption Standards

Quantum mechanics lies at the heart of applications that directly impact our daily lives, from the transistors that run personal electronics to the lasers in Blu-ray players, CDs, and medical equipment. Computer scientists have demonstrated that they can exploit quantum algorithms to solve problems faster than conventional algorithms perform. As of today, there exist security against quantum algorithms for standard encryption. Nevertheless, safety is not guaranteed forever, and users must strive to continually improve the robustness of their encryption methods, since it is very costly and time-consuming to replace them. The first quantum algorithms were developed in the '90s. The most famous is probably Shor's algorithm, which finds the prime factors of a number given a large enough quantum computer 1. This polynomial-time algorithm breaks the modular arithmetic that RSA encryption is based on, among other cryptosystems. However, there is Grover's algorithm, which proves a quadratic speed-up for exhaustive search problems. If an attacker can check N keys in T time, Grover's algorithm will reduce this time to T = sqrt(N). This has significant implications for symmetric encryption.

Computer security is fundamentally the battle for information, as it is exchanged in the digital medium. This is why encryption has become so crucial. Without encryption, breaches and cyber-attacks would be much more severe and pervasive. Modern encryption methods depend on unsolvable mathematical problems. For example, RSA encryption uses large prime numbers in a way that cannot be reverse-engineered in a reasonable time. Encryption, however, could be broken given enough computational resources. In 2011, the U.S.-based IC.3 laboratory built the first 512 qubit quantum computer. It is widely agreed that a 4096 qubit quantum computer could break RSA. Any compromise in the information would have upsetting financial and political consequences. Hence, the need for encryption that cannot be broken by quantum computers.

8.1 Common Algorithms and Protocols

In our current digital world, secure, authenticated, and private communications are vital. Cryptography is the science of providing secrecy, authentication, and integrity of information, often non-public and thus sensitive. Both theoretical and computational restrictions exist that can be used to solve cryptographic problems. Simply put, as long as we cannot efficiently solve certain mathematical problems, many cryptographic protocols are believed to be secure. Current cryptographic standards and algorithms are more vulnerable than their classical counterpart when it comes to brute-force attacks. Suppose that a quantum attacker can run Grover's search algorithm over any combination of plain text messages (a so-called quantum chosen-plaintext attack). In that case, it can find the secret key with O(2n/3) queries. Thus, a block size of 128 bits implies an exhaustive search of 264 operations, being equivalent to an exhaustive search of 264 operations. Django is only secure against quantum computers if the current arguments can sustain any exponential speed-up. HMAC•SHA1 is a nested composition of a keyed cryptographic hash function and a public hash function, commonly used to construct MACs. Enumerating the key of a block cipher with n-bit produces n/2 time quantum complexity. But due to the birthday paradox, the ability to find a collision digest in 2n/2 time, and memory with 2n/2 space requirements 1. A collision attack is a quantum computer capable of making fast logic gates. Whiten it properly, filling copper pores with silicon quantum dots, and it will outperform any classical computer for problems too hard for such classical machines. This dot-inserted SiC would use copper wires as yokes and read heads to impart the magnetic field, and the interconnections between gates would consist of doped silicon.

8.2 Vulnerabilities to Quantum Attacks

Recently, a draft of Copyright Amendment Act was released and the public consultation process is open until June 29, 2021. Throughout the draft, the policy makers

decide to reform the Indian copyright law and it is trying to update it for the digital environment. Some propositions are on par with international standards, especially regarding the formalities, moral rights for cinematographic and musical works, adaptation rights recognized as well as the protection to the performers in respect of their unfixed performances. If adopted, some provisions would provide clear guidance on the digitalized environment, for instance by legalizing the use of copyrighted works for educational activities, distance education, or research activities. On the other hand, some definitions and provisions might create interpretative issues or generate difficulties for future practices, such as the proposal that smart and sustainable technologies could be excluded from the definition of text data mining. With the aim of providing decision makers some guidance in the analysis of the international provisions and some ammunition to promote fair access to knowledge, literature, data, and information by providing innovative elements of evaluations on the current Indian copyright law and the propositions in the draft amendment, an in-depth review is presented here of several aspects of the draft in the light of international standards 1. Many important and crucial aspects proposed in the draft copyright amendment are not investigated here, as the focus is on the provisions that are related to access to text data and content analysis. It is hoped that the report would allow a balanced understanding, independent of other provisions of the draft amendment, of provisions that are appreciated as well as elements warranting significant adjustments. As India hoped that the evaluation has been prepared constructively and opens up fresh thinking, also the main observations will be listed together with a number of relatively small problems, suggestions for the definition or the redaction of a number of terms, and specific language formulations that needed to be checked carefully if the reforms are pursued.

9. Future Directions in Quantum Cryptanalysis

Cryptosystems have been the cornerstone in protecting sensitive data in the steadily increasing electronic communication era, a trend further intensified with the rise of the Internet and, most recently, the Internet of Things 2. Key establishment through symmetric-key agreements and public-key exchange protocols implements the core functional ground for secure communication. However, both classical mechanisms are threatened by the current breakthroughs made in the theory of Quantum Cryptanalysis. In 1976, Diffie and Hellman introduced public-key cryptography followed by Rivest et al. to present the RSA cryptosystem in the same year. Shortly thereafter, ElGamal's paper introduced permutation group-based cryptosystems, a generalization of the previously discussed algorithms. Factorization and the Discrete Logarithm problems were found to offer a computationally infeasible playground for keys lengths that are longer than some threshold value. Impressive performance of deterministic factoring algorithms, relieving RSA's security, may threat emerging applications of this algorithm twelve years after implementation. It is, however, the introduction of quantum computing in 1980 that posed a considerable challenge on the security of present cryptosystems. Let p be an N/2 qubits integer and the integers are drawn uniformly from the range (0, 2 N). In the worst case, scenario, the success rate for the second algorithm is one half. Adi Shamir introduced the algorithm that run in very close complexity to O to Shor's algorithm and is proven to work with the exact same probability of success. In RSA, the factoring problem is solved in polynomial time in steps O (e N (log N)). Full parallelization of the Pollard's rho probabilistic algorithm for discrete logarithms would require 2^N/2 time and memory cells. Implementing a requirements' meet algorithm is considered infeasible in a foreseeable future with contemporary technology. Challenging the symmetric cryptosystems' class, rival to the aforementioned, Grover's algorithm is presented. The problem lies in the underlying quantum mechanics. Each superposition state of k qubits can be processed simultaneously. Thus, the choice of a superpolynomial number of states for the quantum search space is amortized to a polynomial number of applications of the algorithm. It is, however, the quantum search duality that strikes fear; it provides a twofold speed-up for the search in an unstructured set. A direct implication of this result is that classical brute force attacks run in 2^n operations in cipher size can be mimicked by a quantum adversary in 2^(n/2). With the aforementioned general quantum cryptanalysis notions as the background, terms that the majority interpretation value are defined. In the sequel, there is an effort to discuss in more depth the proposals and corresponding counter-arguments of the research community.

9.1 Emerging Technologies

Quantum computing has been a topic of research for more than 40 years. The rate of progress has been increasing in the past decade, and we are now at a point where it is reasonable to think that large and reliable quantum computers are feasible within a couple of decades. However, for cryptographic purposes, the more relevant property of the computer is how many quantum gates can be performed in parallel. With the many different types of quantum computers, algorithms improvements that reduce the required size of quantum circuits, error correction codes and

other overheads, the time to large fault tolerant quantum computers is very uncertain.

The computational hardness of most of the symmetric and few public key schemes can be broken using a quantum computer. Grover's search algorithm(s) can give a square root time improvement for any search problem, including the searching of the key. This implies that the key size of the schemes has to be doubled to ensure similar security level with and beyond quantum computers. Both the exhaustive key search attack and Grover's algorithm key search attack on data encryption standard (DES) scheme have been implemented on the commercial quantum computers. DES was decrypted after around $2^{39.5}$ operations (around 713 million operations). The quantum computer found the key in an estimated average of 697 seconds (approximately 12 minutes) 3.

9.2 Research Challenges and Opportunities

In the last few years, several research papers have addressed the impact of quantum computers on symmetric cryptanalysis, and published detailed analyses of the impact of quantum cryptanalysis on both non-quantum and public-key cryptosystems. Some symmetric cryptosystems and constructions have been put forward, which are the most resistant to quantum cryptanalysis, thus providing secure communications in a post-quantum cryptography world 1. However, there are still many significant unsolved questions. Among other things, there are no known quantum versions of the best classical cryptanalysis, and there are no security models for quantum cryptography which take into account the cryptographic random number generator, the implementation of the cipher, or partially known key bits. Nonetheless, this activity is essential, providing the cryptographic community with an early understanding of the impact of quantum computers on cryptanalysis.

One striking result is the discovery of quantum attacks against the most common secret key primitives. The most thorough analysis of the running times of quantum algorithms on classical cryptosystems and the proposal of workarounds that are least affected by quantum computers 3. Finally, many conventional cipher designs are the result of a thorough and complete process that protects against all known cryptographic attacks. The process includes design, optimization, and analysis stages, from which designs evolve until they can be considered secure. Given this background, perhaps heavily application-focused, the lack of quantum-resistant symmetric cipher designs is entirely understandable.

10. Conclusion

It is widely hypothesized that as a result of advancements in quantum computing, the practical strength of classical encryption will be significantly decreased. Two renowned algorithms that incite this claim are Shor's and Grover's algorithms. Shor's algorithm is deeply unsettling concerning encryption based on the hardness of integer factorization, such as the widely used RSA algorithm. This algorithm is known to have linear computational complexity for AES, and improved attacks for reduced round versions, prompting NIST to retire it by 2023. Though polynomial, it is worth noting that Grover's algorithm has too large of a constant for practically sized data, requiring a doubling of key sizes for secure encryption as is the consensus. It is shown in this analysis that symmetric key standard encryption ciphers with a block size of 112 bits or greater directly resist the Grover search algorithm and its improvements. Furthermore, it is recommended that NIST symmetric key encryption standards be updated to exclusively include symmetric key encryption ciphers with a block size of at least 112 bits.

With advancements in quantum computing, cryptography has been widely regarded as an initial area expected to suffer. Most notably, Shor's and Grover's algorithms suggest that the protection afforded by RSA, DSA, and much of the non-NIST standardized EC amongst others is susceptible to certain quantum attacks. Although the former attack is more threatening, overcoming the latter with a simple increase in key size has been the initial standard response from the cryptographic community. To date, limited inquiry has focused on how symmetric ciphers are affected. Symmetric algorithms are still commonly used to encrypt data in storage, to establish secure channels, and a countless number of common uses. Broadly speaking, symmetric algorithms must apply to data blocks. The trivial way to attack such schemes is to exhaustively search for the keys that encrypt the plaintext to identical cipher outputs. Give a 2^n-bit key, this attack takes on average 2^(n -1) blocks, quadratic to exponential. Grover's algorithm is able to find the desired element in 2^(n/2) operations, a quadratic speedup 1.

Conflict of Interest: The authors declare no conflicts of interest.

Funding: This research received no external funding.

Author Contributions: All authors contributed equally to this work. All authors read and approved the final version of the manuscript.

References

[1] V. Vedral and M. B. Plenio, "Basics of quantum computation," *Progress in Quantum Electronics*, vol. 22, no. 1, pp. 1-39, 1998, doi: https://doi.org/10.1016/S0079-6727(98)00004-4.

[2] L. K. Grover, "A framework for fast quantum mechanical algorithms," in *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, Dallas, Texas, USA, 1998: ACM, pp. 53-62, doi: https://doi.org/10.1145/276698.276712.

[3] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge University Press, 2010.

[4] N. Koblitz and A. Menezes, "A Survey of Public-Key Cryptosystems," *Cryptology ePrint Archive*, 2015.

[5] U. Mmaduekwe and E. Mmaduekwe, "Cybersecurity and cryptography: The new era of quantum computing," *Current Journal of Applied Science and Technology*, vol. 43, no. 5, pp. 41-51, 2024, doi: https://doi.org/10.9734/cjast/2024/v43i54377.

[6] NIST, "Post-Quantum Cryptography," National Institute of Standards and Technology, Gaithersburg, MD 20899, 2025. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

[7] D. J. Bernstein, N. Heninger, P. Lou, and L. Valenta, "Post-quantum RSA," in *International Workshop on Post-Quantum Cryptography*, 2017: Springer, pp. 311-329, doi: 10.1007/978-3-319-59879-6_18.

[8] L. K. Chen and L. Zhang, "Quantum Computing and Cryptography: The Impact of Shor's Algorithm," *Quantum Information Processing*, vol. 18, no. 4, pp. 1-15, 2019.

[9] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, 1996: ACM, pp. 212-219, doi: 10.1145/237814.237866.

[10] G. Kuperberg, "A subexponential-time quantum algorithm for the dihedral hidden subgroup problem," *SIAM Journal on Computing*, vol. 35, no. 1, pp. 170-188, 2005, doi: 10.1137/S0097539703436345.

[11] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA, 1994: IEEE, pp. 124-134, doi: 10.1109/SFCS.1994.365700.

[12] X. Wang and Y. Zhang, "Quantum Computing and Its Impact on Cryptography," *Journal of Computer Science and Technology*, vol. 35, no. 3, pp. 453–467, 2020.

[13] C. Zalka, "Grover's quantum searching algorithm is optimal," *Physical Review A*, vol. 60, p. 2746, 1999, doi: 10.1103/PhysRevA.60.2746.

[14] S. Aaronson, *Quantum computing since Democritus*. Cambridge University Press, 2013.

[15] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, "Quantum Computation by Adiabatic Evolution," in *Proceedings of the 35th Annual ACM Symposium on the Theory of Computing*, 2001: ACM, pp. 48-53.

[16] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38-41, 2018, doi: 10.1109/MSP.2018.3761723.

[17] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303-332, 1999, doi: 10.1137/S0036144598347011.

[18] A. M. Childs and W. van Dam, "Quantum Algorithms for Fixed Point Finding," in *Proceedings of the 45th Annual ACM Symposium on Theory of Computing*, 2010: ACM, pp. 473–482.

[19] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp, "Quantum amplitude amplification and estimation," *arXiv quant-ph/0005055*, p. 32, 2000, doi: 10.48550/arXiv.quant-ph/0005055.

[20] J. Larkin and M. McKague, "Quantum Algorithms for Solving Linear Systems," in *Proceedings of the 2018 IEEE European Symposium on Security and Privacy*, 2018: IEEE, pp. 1-6.

[21] A. Montanaro, "Quantum algorithms: an overview," *npj Quantum Information*, vol. 2, pp. 1-8, 2016, doi: 10.1038/npjqi.2015.23.

[22] Y. Wang, "Quantum computation and quantum information," *Statistical Science*, vol. 27, no. 3, pp. 373-394, 2012, doi: https://doi.org/10.1214/11-STS378.

[23] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Physical Review Letters*, vol. 85, p. 441, 2000, doi: 10.1103/PhysRevLett.85.441.

[24] A. M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, and D. A. Spielman, "Exponential algorithmic speedup by a quantum walk," in *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*, San Diego, CA, USA, 2003: ACM, pp. 59-68, doi: 10.1145/780542.780552.

[25] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, "Quantum computation by adiabatic evolution," *arXiv:quant-ph/0001106*, p. 24, 2000, doi: 10.48550/arXiv.quant-ph/0001106.

[26] M. H. Jebur, F. A. Joda, and M. A. Naser, "Building a Statistical Model to Detect Foreground Objects and using it in Video Steganography," *Baghdad Science Journal*, vol. 20, no. 6, p. 22, 2023, doi: https://doi.org/10.21123/bsj.2023.7926

How to cite this article

M. H. Jebur, and S. M. Khaleel, "Quantum Cryptanalysis: Evaluating the Impact of Shor's and Grover's Algorithms on Modern Encryption Standards," *CyberSystem J.*, vol. 2, no. 2, pp. 41-55, 2025. doi: 10.57238/csj.2025.1012

Access this article online