A Review Paper on the Implications of Quantum Computers to Cryptography

Bavdekar  
*Computer Science Department*   
*BITS Pilani*Pilani, India  
ritikrbavdekar@gmail.com

Chopde  
EEE  
BITS PilaniPilani, India  
chopde@gma

Bhatia  
*Computer Science Department*   
*BITS Pilani*Pilani, India  
ritikrbavdekar@gmail.com

*Abstract*—The development of large quantum computers will have dire consequences for cryptography. Classical cryptographic algorithms are implemented on a large scale in all the major IT applications. Most of the symmetric and asymmetric cryptographic algorithms are vulnerable to quantum algorithms. Grover’s search algorithm gives a square root time boost for the search of the key in the most widely used symmetric schemes, AES and 3DES. The security of asymmetric algorithms like RSA, Diffie Hellman and ECC are based on the mathematical hardness of prime factorization and discrete logarithm. The best solutions available on classical computers take exponential time. Shor’s factoring algorithm can solve the prime factorization problem and the discrete logarithm problem in polynomial time. This problem can be solved using only local quantum computational resources. It is but a matter of a few years before major breakthroughs occur in quantum computing. Soon enough the software and hardware optimization will converge and render all the present asymmetric cryptosystems insecure. This paper analyzes the vulnerability of the classical cryptosystems, introduces all the new post quantum cryptosystem families and summarizes the status of the NIST Post Quantum Cryptography Standardization process.

Keywords— Post Quantum Cryptography, Quantum Computers, Shor’s Algorithm, RSA, Diffie-Hellman, ECC, Lattice-based cryptosystems, Code-based cryptosystems, Isogeny-based cryptosystems, Multivariate Cryptosystems, Hash-based digital signature schemes, Non-Commutative cryptosystems, NIST PQC Standardization Process

# Introduction

Quantum cryptography is the field of cryptography that uses quantum effects to perform cryptographic tasks. These tasks could vary from cryptographic protocols to quantum algorithm cracks. Two of the most well-known applications of quantum information are in cryptography: Quantum Key Distribution and Shor’s Factoring Algorithm. Quantum information opens up a variety of new functionalities in cryptography that are not available in classical information theory. However quantum cryptography does have limitations and challenges.

## Quantum Computing

Quantum mechanics is characterized by its absurdity. It defies intuition. This is due to the concepts like superposition, entanglement and quantum uncertainty. Quantum superposition allows a particle to be at multiple places at the same time. Quantum entanglement describes correlations between particles that are not possible in the classical world. Quantum uncertainty states that if we observe one property of a particle some other property’s information is lost.

The fundamental unit of information in classical computers is a bit. This bit can take only two discrete values 0 and 1. In quantum information the unit is a qubit.[8] This is a unit vector in a two-dimensional complex vector space. A qubit is represented using the ket notation. ∣ψ> = α∣0> + β ∣1> is the notation for a qubit. Here ∣0> and ∣1> are basis vectors in the complex 2d space.α and β are complex numbers whose sum of squares adds up to 1. For representation of 2 or more qubits tensor product is used.

A collection of quantum gates to form a circuit is called a quantum algorithm. Common quantum gates include Controlled NOT Gate, Hadamard gate, negation and phase.

In quantum computing measurement is an operation that takes in a qubit and returns a classical bit( 0 or 1). If a qubit ∣ψ> = α∣0> + β ∣1> is measured the probability of 0 or 1 being returned is |α|2 and |β|2 . Also right after a measurement all information about the qubit is lost and it becomes classical. Post measurement the superposition is lost and depending on the value of the classical bit returned the qubit is transformed into ∣0> state or ∣1> state.

Quantum no-cloning property states that there is no possible way to clone the state of a quantum system. In simple words there is no circuit that can be built which takes in as input a qubit and returns a copy along with the original qubit. Quantum entanglement is a phenomenon in which 2 or more qubits behave in a way that their quantum states can only be defined collectively. They cannot be defined separately.eg (∣00> +∣11>)/√ 2 is state with 2 qubits which cannot be defined individually. This kind of state is called a Bell State.If one of the qubits is measured the other qubits quantum state is also automatically changed.

There are a variety of different physical systems that can be used as quantum devices. These include superconduction qubits , photonic qubits(polarisation of light) and others. Photonic qubits are good for long distance communication while supercomputing qubits are better for quantum interactions.

## Quantum Key Distribution(bb84 protocol)

The protocol is a secure method of sharing a common key between two systems. The algorithm makes the assumptions that there is a classic channel and quantum channel for information transfer. The classic channel is two way while the quantum channel can be one way(from only sender to receiver and no return link). The bit and basis selected for encoding and sending a qubit are both randomly selected.

The protocol considers 2 different orthogonal basis vector sets.[6] (eg-0,90 horizontal-vertical and 45, -45 diagonal polarisation of photons). Alice and Bob decide encodings 0 and 1 in both basis sets. Note- measuring information in one basis set makes us lose information in the other basis set. Alice generates a random key and encodes the bit using a random basis. These qubits are sent to Bob from the quantum channel. Bob uses random basis filters (diagonal or vertical/horizontal) to measure the bits. After that both use a classical method to announce the filters they used for each bit. If they are different filters the bit is discarded. A final key is transmitted which is only known by Alice and Bob. Since Eve can’t clone the qubits and if she measures them information may be lost Bob will know when he announces a few random bits to Alice to ensure no tampering. Also if Eve measured all the qubits using random filters she would have selected a few different filters and lost information of the qubits to measure them again.

## Shor’s Algorithm

Shor designed two different quantum algorithms which can crack the two major hard problems on which the security of present day cryptosystems is based: Prime Factorisation Problem and the Discrete Logarithm Problem. Classical solutions to these problems have exponential solutions. With the help of period finding using Quantum Fourier Transformation Shor designed these probabilistic algorithms in polynomial time. Shor’s algorithm can crack the factoring number problem in polynomial time while before this the best classical solution(General Number Field Sieve) takes exponential time[7].

Both the algorithms consist of 2 major parts. The first part is a classical part that involves converting the problem to a period-finding problem. The second part is the quantum part that takes advantage of quantum parallelism for the period-finding problem.It uses the quantum fourier transformation algorithm to find the period.

Shor’s algorithm is a probabilistic algorithm. It doesn’t always factor the number in the first attempt. With increase in the number of times the algorithm is run the probability of getting a factor increases.

## Grover’s Algorithm

It’s a quantum search algorithm that searches in an unsorted database in O(n1/2).[4] In classical computers, search over an unordered database is an O(n) problem. Grover’s algorithm is also probabilistic and can be repeated several times to ensure the search is complete. To search a Grover iteration is performed. We can repeat iterations the increase the probability of finding the element in a database.

Grover’s algorithm can be used to find the mean and median of data, for finding the inverse value of a function, etc. These tools can be used by quantum cryptanalysts for cracking algorithms. It can also be used to search for keys in symmetric cryptosystems.

## Simon’s Algorithm

Simon’s algorithm is a quantum circuit that finds out if a function is 1 to 1 or 2 to 1. The property of the function states that if two input values map to the same output their XOR results in a constant b. If b is all 0s then it becomes a 1-1 function else it is a 2-1 function.

The classical solution requires O(2n-1+1) to find a collision. The quantum algorithm provides an exponential speedup.[5]

Simon’s algorithm inspired Shor’s algorithm. Simon’s algorithm itself has applications in cryptography provided correct query access model is available.

# Symmetric cryptographic algorithms

.

.

.

Symmetric Cryptography is a branch of cryptography wherein the encryption and decryption algorithms are both executed with a single key. Given key lengths of sufficient size and randomness, it is beyond the scope of current computational resources to perform brute force attacks on such schemes. However due to the heavy reliance on a single key, a major factor towards implementing symmetric cryptography schemes lies in the communication of the secure key from sender to receiver. Such schemes are mostly employed in Data encryption for storage applications.

## Advanced Encryption Standard(AES)

### Basics

AES is a widely used symmetric cryptographic algorithm. It relies on the randomness of ciphertext generated from multiple rounds of a well-defined, standardized symmetric permutation network. The AES schemes in use currently employ 128-bit, 192-bit or 256-bit keys and generally consist of 10, 12 or 14 rounds of 4 stages each. A simple key schedule is used to generate subkeys for each round. Sufficient confusion and diffusion is achieved in the ciphertext through multiple rounds of mixing and substitution.

Each Round of the AES algorithm consists of 4 stages-

1. SubByte : In this stage each byte is substituted with a value given by a relation. These substitutions can be carried out using predetermined S-boxes consisting of 256 values.

2. ShiftRows : In this stage the elements obtained from the S-boxes are then shifted right by guidelines specified in the NIST standard, or chosen independently on a need-by-need basis.

3. MixColumns : Each column is then read as polynomial (a(x)) coefficients which are then multiplied by an encoding polynomial given by –

e(x) = 3x^(3 )+ x^2 + x + 2

The resultant polynomial is then reduced –

a'(x) = a(x)\*e(x)mod(x^4 +1)

The coefficients of a'(x) represent the modified columns of the state array.

4. AddRoundKey : A round key generated by a simple key schedule is added to the state array.

All calculations are done over a Galois Field (256).

The Decryption Algorithm is the same algorithm with the same number of rounds, in a reverse order.

### Classical Exploitations

Vulnerabilities pertaining to repeated sequences of characters in the message, improper key selection have been found and proven to be exploitable. These attacks however do not decrease the computation time required by enough an amount to make it viable for brute force searches. Bounded by current computational resources, AES can be considered ‘secure’.

### Quantum Security

AES has proven to be one of the most robust cryptographic schemes currently in use, proving resilient to the level of exhaustive brute force attacks that are currently computationally viable.

The recent advancements in development of Quantum Computers have however led people to reopen the question of AES’s security against Quantum Computer Brute Force Exhaustive Search attacks, Asymmetric Public-Key schemes such as RSA, ECC, etc have been known to be broken completely by Quantum Exhaustive Searches due to the immense parallel processing possible through superposition of qubits.[9]

Various algorithms that exploit the principle of superposition have been put forward such as Simons Promise, Grover’s Search, and Shor’s Algorithm.

Grover’s Search algorithm reduces the exhaustive key search from O(N) to O((N/M)1/2) trials, where M can be reduced to 1 by choosing functions which give single solutions while implementing AES in a quantum circuit.

One of the major drawbacks of current Quantum Exhaustive Search Algorithms is that for symmetric schemes, they require the scheme to be implemented by a quantum circuit before they can be applied to the cipher. Many implementations of AES as a quantum circuit exist. The crack using Grover’s search algorithm requires the AES algorithm to be on a quantum circuit. This limits the application of the crack only to quantum oracles. Furthermore, as mentioned above, current algorithms are only able to reduce the trials by N1/2, where N is the length of the key. One can simply increase the key length to preserve security, for example, moving from AES-128 to AES-256 can still be considered unbreakable in the face of Brute Force Searches.

# Prepare Your Paper Before Styling

Before you begin to format your paper, first write and save the content as a separate text file. Complete all content and organizational editing before formatting. Please note sections A-D below for more information on proofreading, spelling and grammar.

Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

## Abbreviations and Acronyms

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

## Units

* Use either SI (MKS) or CGS as primary units. (SI units are encouraged.) English units may be used as secondary units (in parentheses). An exception would be the use of English units as identifiers in trade, such as “3.5-inch disk drive”.
* Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.
* Do not mix complete spellings and abbreviations of units: “Wb/m2” or “webers per square meter”, not “webers/m2”. Spell out units when they appear in text: “. . . a few henries”, not “. . . a few H”.
* Use a zero before decimal points: “0.25”, not “.25”. Use “cm3”, not “cc”. (*bullet list*)

## Equations

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled.

Number equations consecutively. Equation numbers, within parentheses, are to position flush right, as in (1), using a right tab stop. To make your equations more compact, you may use the solidus ( / ), the exp function, or appropriate exponents. Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign. Punctuate equations with commas or periods when they are part of a sentence, as in:

*a**b* 

Note that the equation is centered using a center tab stop. Be sure that the symbols in your equation have been defined before or immediately following the equation. Use “(1)”, not “Eq. (1)” or “equation (1)”, except at the beginning of a sentence: “Equation (1) is . . .”

## Some Common Mistakes

* The word “data” is plural, not singular.
* The subscript for the permeability of vacuum **0, and other common scientific constants, is zero with subscript formatting, not a lowercase letter “o”.
* In American English, commas, semicolons, periods, question and exclamation marks are located within quotation marks only when a complete thought or name is cited, such as a title or full quotation. When quotation marks are used, instead of a bold or italic typeface, to highlight a word or phrase, punctuation should appear outside of the quotation marks. A parenthetical phrase or statement at the end of a sentence is punctuated outside of the closing parenthesis (like this). (A parenthetical sentence is punctuated within the parentheses.)
* A graph within a graph is an “inset”, not an “insert”. The word alternatively is preferred to the word “alternately” (unless you really mean something that alternates).
* Do not use the word “essentially” to mean “approximately” or “effectively”.
* In your paper title, if the words “that uses” can accurately replace the word “using”, capitalize the “u”; if not, keep using lower-cased.
* Be aware of the different meanings of the homophones “affect” and “effect”, “complement” and “compliment”, “discreet” and “discrete”, “principal” and “principle”.
* Do not confuse “imply” and “infer”.
* The prefix “non” is not a word; it should be joined to the word it modifies, usually without a hyphen.
* There is no period after the “et” in the Latin abbreviation “et al.”.
* The abbreviation “i.e.” means “that is”, and the abbreviation “e.g.” means “for example”.

An excellent style manual for science writers is [7].

# Using the Template

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

## Authors and Affiliations

**The template is designed for, but not limited to, six authors.** A minimum of one author is required for all conference articles. Author names should be listed starting from left to right and then moving down to the next line. This is the author sequence that will be used in future citations and by indexing services. Names should not be listed in columns nor group by affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization).

### For papers with more than six authors: Add author names horizontally, moving to a third row if needed for more than 8 authors.

### For papers with less than six authors: To change the default, adjust the template as follows.

#### Selection: Highlight all author and affiliation lines.

#### Change number of columns: Select the Columns icon from the MS Word Standard toolbar and then select the correct number of columns from the selection palette.

#### Deletion: Delete the author and affiliation lines for the extra authors.

## Identify the Headings

Headings, or heads, are organizational devices that guide the reader through your paper. There are two types: component heads and text heads.

Component heads identify the different components of your paper and are not topically subordinate to each other. Examples include Acknowledgments and References and, for these, the correct style to use is “Heading 5”. Use “figure caption” for your Figure captions, and “table head” for your table title. Run-in heads, such as “Abstract”, will require you to apply a style (in this case, italic) in addition to the style provided by the drop down menu to differentiate the head from the text.

Text heads organize the topics on a relational, hierarchical basis. For example, the paper title is the primary text head because all subsequent material relates and elaborates on this one topic. If there are two or more sub-topics, the next level head (uppercase Roman numerals) should be used and, conversely, if there are not at least two sub-topics, then no subheads should be introduced. Styles named “Heading 1”, “Heading 2”, “Heading 3”, and “Heading 4” are prescribed.

## Figures and Tables

#### Positioning Figures and Tables: Place figures and tables at the top and bottom of columns. Avoid placing them in the middle of columns. Large figures and tables may span across both columns. Figure captions should be below the figures; table heads should appear above the tables. Insert figures and tables after they are cited in the text. Use the abbreviation “Fig. 1”, even at the beginning of a sentence.

1. Table Type Styles

| Table Head | Table Column Head | | |
| --- | --- | --- | --- |
| Table column subhead | Subhead | Subhead |
| copy | More table copya |  |  |

1. Sample of a Table footnote. (*Table footnote*)
2. Example of a figure caption. (*figure caption*)

Figure Labels: Use 8 point Times New Roman for Figure labels. Use words rather than symbols or abbreviations when writing Figure axis labels to avoid confusing the reader. As an example, write the quantity “Magnetization”, or “Magnetization, M”, not just “M”. If including units in the label, present them within parentheses. Do not label axes only with units. In the example, write “Magnetization (A/m)” or “Magnetization {A[m(1)]}”, not just “A/m”. Do not label axes with a ratio of quantities and units. For example, write “Temperature (K)”, not “Temperature/K”.

##### Acknowledgment *(Heading 5)*

The preferred spelling of the word “acknowledgment” in America is without an “e” after the “g”. Avoid the stilted expression “one of us (R. B. G.) thanks ...”. Instead, try “R. B. G. thanks...”. Put sponsor acknowledgments in the unnumbered footnote on the first page.

##### References

The template will number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in [3]—do not use “Ref. [3]” or “reference [3]” except at the beginning of a sentence: “Reference [3] was the first ...”

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors’ names; do not use “et al.”. Papers that have not been published, even if they have been submitted for publication, should be cited as “unpublished” [4]. Papers that have been accepted for publication should be cited as “in press” [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

1. G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*
2. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
3. I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
4. K. Elissa, “Title of paper if known,” unpublished.
5. R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.
6. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
7. M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

**IEEE conference templates contain guidance text for composing and formatting conference papers. Please ensure that all template text is removed from your conference paper prior to submission to the conference. Failure to remove template text from your paper may result in your paper not being published.**