International Journal of Computer and Internet Security.
ISSN 0974-2247 Volume 6, Number 1 (2014), pp. 1-10

http://www.irphouse.com

Title: The RSA Challenge: Urge for Advent of Neoteric Encryption System

Author: **Amiya Chakraborty**
Address: Department of Computer Science & IT,
College of Engineering Pune, Shivajinagar, M.S., India.
Email - amiya12c@gmail.com Mobile No. : +919970612618

Under the guidance of: **Dr. V. K. Pachghare**
Address: Assistant Professor, Department of Computer Science & IT,
College of Engineering Pune, Shivajinagar, M.S., India.
Email – vkp.comp@coep.ac.in Mobile No. : +9120 25507096 (O)

Abstract

RSA (Rivest Shamir Adleman) public-key encryption has protected privacy and verified authenticity when using computer, gadgets and web browsers around the globe. It is probably the most significant advance in the 3000 year history of cryptography. The reason behind its wide acceptance lies in computational security. However, 1024-bit encryption has been successfully hacked, leaving a single trace or ending human life as we know it. As this is an emerging extensive research oriented field, solution to it remains an open and significant challenge. This paper traces out the utter need for dawn of a modish two-key enciphered procedure. A cryptographic algorithm is proposed based on fully quantum mechanical keys and ciphers. Encryption and decryption are carried out via an appropriate measurement process on entangled states as governed by a quantum mechanical, asymmetrical and dynamical public key distribution. The use of public keys leads to a high availability of our scheme, while their quantum nature is shown to ensure unconditional security of the proposed algorithm.

Keywords – RSA, PKC (Public Key Cryptography), SSL (Secure Sockets Layer), Shor's algorithm, quantum computing, MES (Maximally Entangled State), Unconditional Security

Introduction

Every time you buy something on the internet with your credit card, you use prime numbers to keep your personal information secure. How? Using ***RSA cryptography****;* the first, and still most common (although apparently), PKC implementation. Modular exponentiation ($m^d \bmod n$) is a central operation in PKC [1]. Many cryptographic schemes, including RSA, heavily rely on modular exponentiation for their algorithms.RSA, depends on some marvelous properties of prime numbers. One of these is that it is rather easy to generate large prime numbers, but much harder to factor large numbers into primes. Another is Fermat's little theorem. *The fact that finding primes is "easy," while factoring into primes is "hard" is what makes RSA work* [10]. Although employed with numbers using hundreds of digits, the math behind RSA is relatively straight-forward.

Well, think first about what User A, the person who designs the code, does. First User A generates the random large primes **p** and **q**, then chooses **e** such that it is relatively prime to (p-1)(q-1). Finally User A solves an equation to find **d**:

$$de + (p-1)(q-1)y = 1$$

where all the letters are integers. User A makes **e** and **n** public. This is all anyone needs to send secret messages to User A. Now think about what User B, who wants to decrypt messages sent to User A, needs to know. First User B must factor **n** to find **p** and **q** so as to set up the equation. Then User B solves the equation to find **d**. At this point User B can decrypt User A's messages. Given limited computing resources (e.g. time needed for intractable factoring problem is greater than the age of the universe), the cipher cannot be broken. Nevertheless, the daunting revelation at this juncture is that RSA 1024-bit key has been cracked. This paper exhibits diverse approaches of RSA 1024-bit clampdown; thereafter delineating the necessity of a newfangled public-key cipher.

Modus Operandi of RSA 1024-bit Crackdown

Most of your online traffic is encrypted through a protocol called SSL. Au fond, when you access a website, what's happening is your client (such as a Web browser) is accessing a server, the computer which manages access to the website's centralized data or resource in a network. Through the client-server connection, the server's data comes over the Internet to your screen. An SSL-enabled server and an SSL-enabled client exchange a series of messages; in particular select public key encryption(predominantly RSA 1024-bit cipher) to generate shared secret keys to establish an encrypted SSL connection so that eavesdroppers won't be able to view sensitive information such as credit card info, IP addresses and account details[9].

Regrettably, foremost rationale for RSA 1024-bit crackdown is *Fault Based Attack of RSA authentication.* For any computing system to be secure, both hardware and software have to be trusted. If the hardware layer in a secure system is imperiled, not only it would be feasible to extract covert information about the software, but it would also be extremely toilsome for the software to apprehend that an attack is underway. Three students at University of Michigan were able to successfully hack 1024-bit encryption in OpenSSL on a SPARC-based system in approximately 100

hours [2]. OpenSSL is an open-source SSL implementation of RSA authentication [3], widely deployed in internet and web security applications. The attack requires only limited knowledge of the victim system's hardware. Assailants do not need access to the intramural components of the victim chip, they solely collect distorted signature outputs from the system while subjecting it to ephemeral Achilles heels. Once a sufficient number of corrupted messages have been collected, the private key can be extracted through offline analysis. A theoretical example of a similar attack is presented in [8], where functional errors in the hardware executing the exponentiation algorithm are used to break RSA and other strong cryptographic systems.

Supplementary to aforementioned is *Failure of Random Number Generators.* Main goal of the team of European and American mathematicians and cryptographers was to test the validity of the assumption that different random choices are made each time keys are generated. They found that the vast majority of public keys work as intended. A more disconcerting finding is that two out of every one thousand RSA moduli that they collected offer no security [4]. Conclusion is that the validity of the assumption is questionable and that generating keys in the real world for "multiple-secrets" cryptosystems such as RSA is significantly risky.

On top of everything is the Mathematical attack; that is well-nigh practicable. An international team of mathematicians announced in May, 2007 that they had factored a 307-digit number (approx. 1023.33… binary bits)—a record for the largest factored number and a feat that suggests Internet security may be on its last legs [5].The next target for Arjen Lenstra, a cryptology professor at EPFL in Switzerland is factoring RSA 1024-bit numbers."*It is good advanced warning of the coming dusk of 1024-bit RSA encryption*".

Moreover, of late it was promulgated that Google and the Universities Space Research Association are amalgamating to buy and operate a quantum computer from D-Wave Systems, to be hosted at NASA's Ames Research Center [6]. Using Shor's algorithm, an algorithm that could make unsound code-breaking sound, a sufficiently powerful quantum computer could factor any public RSA key. Did Google, NASA, and the USRA nobbut gleaned access to such a computer? [6]. It's impossible to catastrophize that the very inkling of security depends on integer factorization remaining back-breaking. Eventually, quantum computing will make factorization easy for the people we don't want to have our secrets by 2018 or so as vigorous research on it is underway, and then much of what's based on present-day public key cryptography will be left in shambles [7]. The computational power of the quantum computer is skyrocketing exponentially with the number of entangled qubits. It's like Moore's Law compounded [7]. The general consensus is that RSA 1024-bit will be insecure at any key size and the implication of this attack is that all data encrypted using current standards based security systems such as the ubiquitous SSL used to protect e-commerce and internet banking is at jeopardy.

Algorithm Architecture

We should already be seriously thinking about post-quantum cryptography, in anticipation of the day when a press release announcing the purchase of a powerful-

enough quantum computer hits the wires. Unless, of course, we're acquiescent to breathe in a world with no more enigmas. Is the writing on the wall for 1024-bit encryption? The answer to that question is an unqualified yes. Briefly the standard is still secure, but the clock is definitely ticking. Web sites should be looking toward stronger encryption than RSA 1024-bit. In order to outshine and out class the competitor by entrapping, linking, capitalizing the opportunities through continuous learning, thinking, adoption of change and improvement. We need not to be complacent with customer satisfaction we to go for customer delight and beyond for driving the market. Global source of resources is the key which indicate websites' sensitivity towards emerging trends of market need, taste and preferences. This is possible by updating professionalism, upright value and having full of substance in oneself. In nutshell we need to be proactive rather than reactive. "*Things are becoming less and less secure,*" implying it is about time to change.

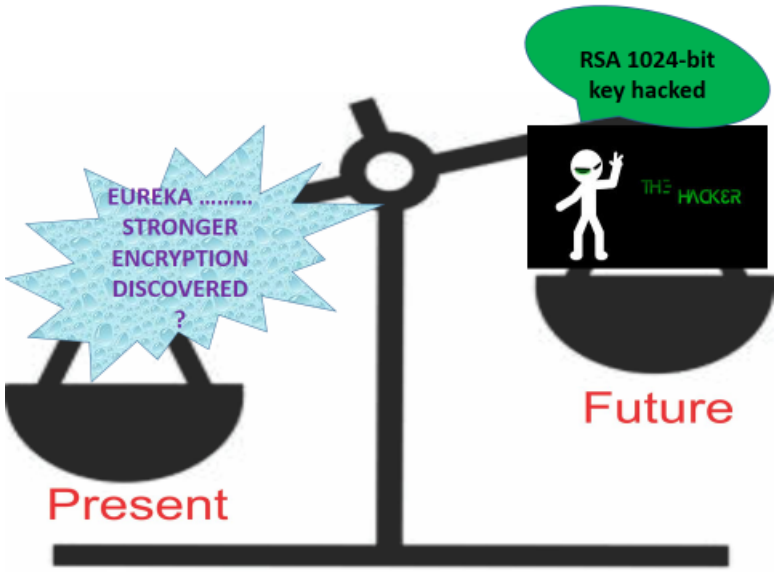

Fig. 1: Envisage: Either unearth efficacious cipher Or bleak future awaits

In this review article we initiate a quantum public key algorithm. The algorithm engages maximally entangled states (MES) of pairs of spin-1/2 particles and their correlation preserving projection on germane orientations. It commences with the causation of public and private keys via the correlation among MES, amalgamated measurement operators and a concatenation of unitary operators. Then the sender, Bob, encrypts his message by recruiting the public key and a quantum logic gate operation which is influenced by the key and furnishes the ciphertext. Finally, the private key is employed by Alice to decrypt this ciphertext. The unconditional security and availability of the proffered algorithm are shown to be guaranteed, respectively, by the no-cloning theorem [11] and by the technology of the public key.

We here unveil a secure key distribution for our quantum PKC via using maximally entangled states of pairs of spin-1/2 particles. The eigenvectors of a single-

particle when measured along an axis z, i.e. σ_z = |0><0| - |1><1| are |0> and |1>, and |+> = (|0> + |1>)/$\sqrt{2}$ as well as |-> = (|0> -|1>) / $\sqrt{2}$ are the eigenstates of the spin operator along the corresponding x axis, i.e. σ_x = |0><1| + |1><0|. We deem the so called Bell states $|\Phi^{\pm}\rangle$ = (|00> ± |11>) / $\sqrt{2}$ and $|\Psi^{\pm}\rangle$ = (|01>±|10>)/$\sqrt{2}$ and the auxiliary MES given by $|\psi^{\pm}\rangle$ (|0-> ±|1+>) / $\sqrt{2}$ and $|\phi^{\pm}\rangle$ = (|0+> ± |1->) / $\sqrt{2}$. We shall allude all these two-particle MES as quantum channels. We comprehend from Fig. 2 that a designated quantum channel and the measurement axis for both particles are correlated, i.e. if two of them (including the channel) are familiar, the third can be determined. Nonetheless, if only one is known, the other parameters remain anonymous. Based on this trait we shall perpetuate in erecting the public key K_p and the commensurate private key K_s.

Key Generation

Alice and Bob are conceptualized to apportion particles of an array of m homogenous MES $|\Phi^{+}\rangle$ with $m \gg n$ at this juncture (where n is the key size). One particle of each MES is kindred with Alice and one with Bob which establishes the one-particle links P_A' and P_B', respectively. The epithets A and B cite Alice's and Bob's particles through the whole of the article. Then Alice and Bob pick respectively a fragment of particles (designated as $\Delta P_A'$ and $\Delta P_B'$, respectively i.e m-n) from the sets P_A' and P_B' to scrutinize eavesdropping by utilizing the procedure presented in Ekert's protocol for quantum key distributions [12]. Whenever eavesdropping transpires, it is mandatory to inaugurate again the succession of quantum channels.

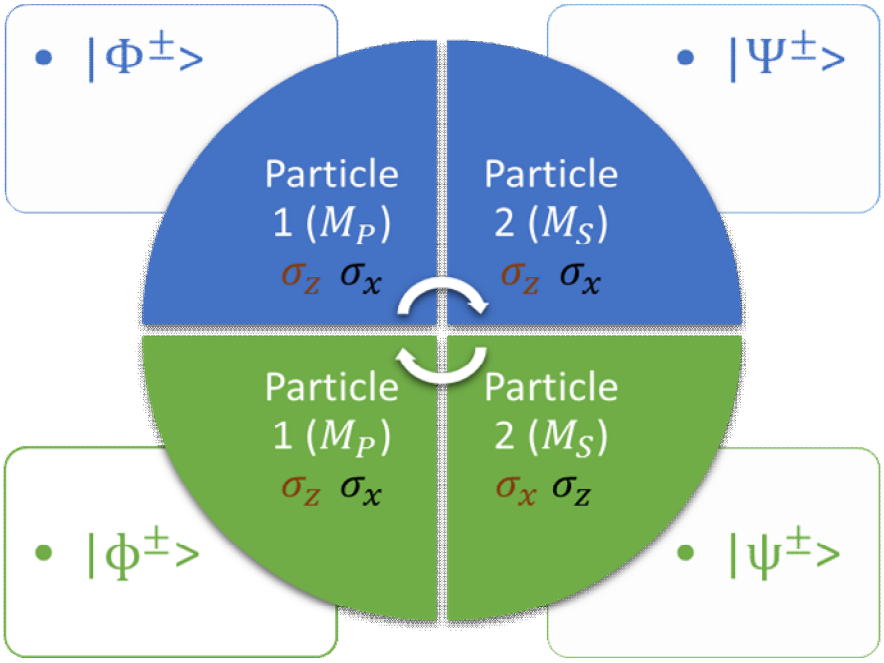

Fig. 2: Measurement axis are indicated for each particle of a MES, along the rows, for obtaining maximum correlation or anti-correlation between the readouts of measurements

Otherwise, the n outstanding entangled states may be methodized to form the set B'. For expediency, we connote the pending n particles as $P_A = P_A' - \Delta P_A' = \{p_A^1, p_A^2, \dots, p_A^n\}$, and $P_B = P_B' - \Delta P_B' = \{p_B^1, p_B^2, \dots, p_B^n\}$. Then Alice forges a set $U_A = \{U_{A1}, U_{A2}, \dots, U_{An}\}$ by arbitrarily choosing $U_{Ai} \in \{I, H, \sigma_x, \sigma_y, \sigma_z, H\sigma_x, H\sigma_y, H\sigma_z\}$ for i ∈ {1, … , n} and thus engenders $B = \{U_{A1}|\Phi^{\pm}\rangle, U_{A2}|\Phi^{\pm}\rangle, \dots, U_{An}|\Phi^{\pm}\rangle\}$. Here I is the identity operator, H is the Hadamard gate i.e. H = $1/\sqrt{2}$(|0><0| + |0><1| + |1><0| - |1><1|), σ_x is Pauli X operator, σ_y is Pauli Y operator, σ_z is Pauli Z operator, and $H\sigma_x$, $H\sigma_y$, $H\sigma_z$ are matix multiplications of Hadamard gate and Pauli operators X, Y, Z respectively. Alice has now attained the set B wherein the complementary operators U_{Ai} need be applicable only on Alice's particle.

Alice actuates the key generation by procuring random strings of quantum channels $B = \{|b_1\rangle, |b_2\rangle, \dots, |b_n\rangle\}$ as stated above and by electing spin operators for one particle $M_p = \{m_p^1, m_p^2, \dots, m_p^n\}$ with $|b_i\rangle \in \{|\Phi^{\pm}\rangle, |\Psi^{\pm}\rangle, |^{\pm}\rangle, |\psi^{\pm}\rangle\}$ and $m_p^i \in \{\sigma_x, \sigma_z\}$. Following Fig. 2Alice is now on a firm footing to decide the spin mensuration axis pertaining to the second particle, producing $M_S = \{m_s^1, m_s^2, \dots, m_s^n\}$. Then, Alice fabricates an auxiliary string of unitary operators $U = \{U_1, U_2, \dots, U_n\}$, where

$$U_i = \begin{pmatrix} \cos\Theta_i & -sin\Theta_i \\ \sin\Theta_i & \cos\Theta_i \end{pmatrix}$$

with Θ_i being a erratic number, which is confidentially chosen by Alice. Coalescing M_p and U, Alice is then capable to build the public key K_p,

$$K_p = \{k_p^1, k_p^2, \dots, k_p^n\}, \quad k_p^i = U_i^{-1} m_p^i U_i. \tag{1}$$

Thus, a spin mensuration operator $k_p^i = \sigma_{n_i}$ along an axis n_i may be universally broadcasted whereas the quantum channel and the mensuration operator on the second particles of the quantum links remain familiar exclusively to Alice. The analogous private key K_S is then erected via

$$K_S = \{k_s^1, k_s^2, \dots, k_s^n\}, \quad k_s^i = U_i^{-1} m_s^i U_i. \tag{2}$$

where $k_s^i = \sigma_{n_i}$ or $n_i^{\perp}$ for Bell states $|b_i\rangle$. The correlation among k_p^i and k_s^i are extracted like Fig. 2 but with x and z substituted by universal orientations n_i and $n_i^{\perp}$ whereupon $n_i^{\perp}$ is an orthogonal direction to n_i.

Encryption

We now theorize that Bob endeavours to send a covert plaintext message φ^M to Alice by virtue of the public key K_p. On methodically gauging the particles P_B by employing the public key K_p, Bob acquires the string $K_B = \{|k_B^1\rangle, |k_B^2\rangle, \dots, |k_B^n\rangle\}$, where $|k_B^i\rangle = k_p^i p_B^i \in \{|0_{n_i}\rangle, |1_{n_i}\rangle\}$ are eigenvectors of σ_{n_i}. The memorandum φ^M is typified by a string of qubits $\varphi^M = \{|\varphi_p^1\rangle, |\varphi_p^2\rangle, \dots, |\varphi_p^n\rangle\}$, where $|\varphi_p^i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$ for i ∈ {1, 2, … , n}. Afterwards Bob shall encrypt the message by implementing a single qubit gate $G_i \in G = \{G_1, G_2, \dots, G_n\}$ via

$$|c_i\rangle = G_i|\varphi_P^i\rangle \quad (3)$$

where G_i = H if $|k_B^i\rangle = |0_{n_i}\rangle$ and G_i = Z (Pauli Z operator) in the other case if $|k_B^i\rangle = |1_{n_i}\rangle$. Thus the qubits $|c_i\rangle$in the ciphertext C are staunchly contingent on the public key.

Decryption

The intent of the decryption algorithm is to decrypt the ciphertext C and to retrieve the plaintext φ^Munder the ascendancy of the private key. Since the private key $K_S$is high-octane for our algorithm, Alice needs to derive the private key $K_S$prior to decrypting the ciphertext. Alice knows the public key $K_P$besides the secret parameters B and U and is thus capacitated to calculate the private key K_S by Eq. (2).Thereafter, Alice is entailed to assess the string of particles $P_A$adopting the private key $K_S$and gains the secret string $K_A = \{|k_A^1\rangle, |k_A^2\rangle, \dots, |k_A^n\rangle\}$, where $|k_A^i\rangle = k_S^i p_A^i$ for i ∈ {1, 2, … , n}.Next Alice is in the position to appraise Bob's mensuration outcomes K_B via K_A because of the interrelationship of the measurement operators and the proficiency of the secret quantum channels B and the set of rotation operators U. Ergo, Alice can obtain Bobs set of qubit gates G and thus decrypt the plaintext via

$$|\varphi_P^i\rangle = G_i^\dagger|c_i\rangle \quad (4)$$

where $G_i^\dagger = \{G_1^\dagger, G_2^\dagger, \dots, G_n^\dagger\}$ are Hermitian Adjoint operators of $G_i$as employed in Eq. (3) for i ∈ {1, 2, … , n}. We observe that the H− and Z− gates may be positively inverted.

The aforementioned algorithm is demonstrated in Fig. 3, which incorporates the encryption and decryption operations. The activities of the encryption and decryption are divided into three phases. In phase I a MES $|\Phi^+\rangle$ is constructed between Alice and Bob, and then, Alice applies a haphazard unitary operation from $U_A$on her particle of the entangled pair, which produces one of the eight quantum channels. In phase II Bob and Alice perform appraisals on their particles using the public and secret keysK_P and K_S, respectively. For encryption and decryption in phase III, the key-hingeing quantum logic gates in G and $G^\dagger$are applied on the plaintext $\varphi^M$and the ciphertext C by Bob and Alice, respectively. We accentuate further that the plaintext φ^M may be blocked for pragmatic applications, when the number of bits of the plaintext overshoots that of the public key K_P. In this state Bob is enjoined to divide the plaintext into L blocks with scope of each same as of the public key n. Then he encrypts each qubit of the ith block for i ∈ {1, 2, … , L}following the encryption stratagem exhibited in Eq. (3). If the unexpurgated plaintext or its ultimate block are shorter than the public key, one should affix some identity symbols, e.g. |0>'s, alike in classic communication, prior to encrypting this segment of the plaintext. Likewise for the decryption, Alice reiterates the decryption operation depicted in Eq. (4) for each chunk until all chunks have been decrypted.

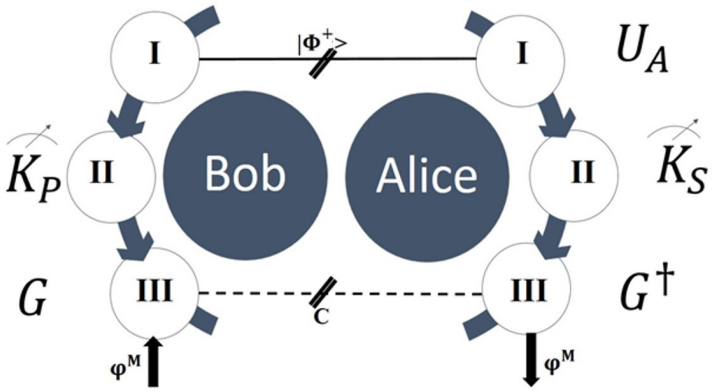

Fig. 3:Diagram of the quantum public key algorithm

Security Analysis

An unconditionally assured algorithm requires it to be intractable for any attacker to grab the private key neither directly nor through the public key, the cipher or any other precarious facet of the algorithm. An attacker Eve may be an eavesdropper or a tamper trying to amend the private key and shall not be presumed here to be restrained in resources in any way. In the first place, the secret key K_S is hingeing on the parameters M_S, $B$and U, so that we shall allude to it as a *dynamical key*. This becomes germane in practical applications because it has been evinced that dynamical keys are more reliable than static keys. There is no way that the secret private key K_S can be determined with the trivial knowledge of the public key K_P, because both the quantum channel and the unitary rotation still remain unfamiliar to the whole world but Alice. The private key K_S is kept undisclosed by the holder while the public key K_P may be propagandized like a telephone number. The use of the public key instigates to a *high availability* for the propounded scheme. At the same time, the high secrecy ofM_S and B precipitates to a high secrecy for the private key.

Besides, the first considered game plan of an attacker shall be to acquire or remould the private key through the public key. Since K_P is public, the attacker is patently able to procure it. The quantum channels, howbeit, inevitable to obtain K_S via K_P are nonorthogonal, e.g. satisfy $|\langle\phi^{\pm}|\Phi^{\pm}\rangle|^2 \neq 0$, which guarantees that any venture to intervene the quantum channel by an intermeddler Eve can be detected because of the noncloning theorem [11]. Thus, the assailant, Eve, cannot be part of the quantum channel without muddling it. Moreover, according to Fig. 2, there is a probability of 1/8 for Eve of getting a single accurate quantum channel. Thus, for an n bit message and the allied quantum channels, the probability for Eve of ambushing without being detected is $(1/8)^n$.This number becomes progressively small for protracted messages but more importantly Eve may not know it even if she has found the precise quantum channels by accident. Those circumstances have been proven unconditionally secure (see first entry in [13] and references therein). In addition, due to the arbitrary variables Θ_i, there is no correspondence between the public key and the private key. Thus without the knowledge of either Bor one of M_P or U, no documentation about

$K_S$is realizable via K_P.

Furthermore we consider the scheme, in which the attacker solicits to procure the plaintext directly through the ciphertext. Since the ciphertext is constructed by the set of gates G which is dictated by K_B, this is necessitated prior to finding the ciphertext. However, except for Bob and Alice, it is inconceivable for anybody to obtain the correct K_B because after Bob's evaluation on P_B using the public key there are two plausible cases for each qubit. It is even unthinkable to procure the accurate ciphertext for any attacker, because the ciphertext encompasses two states $\{Z|\varphi_p^i>, H|\varphi_p^i>\}$, which heed the property $|<\varphi_p^i|Z^\dagger H|\varphi_p^i>|^2 = ½[1+ (\alpha_i^*\beta_i - \beta_i^*\alpha_i)]^2$. If α_i and β_i are specifed to be real numbers, then $|<\varphi_p^i|Z^\dagger H|\varphi_p^i>|^2 = ½$, which means these states are nonorthogonal. Thus the ciphertext may not be discerned like in the B92 protocol [14]. Accordingly, any qubit in the ciphertext is concealed from the attacker, i.e. by the no-cloning theorem, the attacker cannot copy or know it.

Unlike the classic PKC, whose security hinges on the computational complexity presumption, the proposed algorithm does not involve such a presupposition. It is contrived entirely by the natural laws of quantum mechanics, i.e. does not embrace any intrinsic snags. We add ultimately that usually the blocking treatment dwindles the security of the algorithm in the classic cryptography, because this treatment drains some useful data, such as the periodical or pseudo-periodical attributes from the acquired ciphertext (consisting of classic bits), to the attacker. Nevertheless, the blocking treatment in the suggested algorithm does not reveal any efficacious information, because no aggressor is in the position to attain the flawless ciphertext as mentioned above.

Conclusion

In conclusion, an available and sound public key algorithm has been proffered. The proposed algorithm encrypts the clear text memorandum using a public key and decrypts the ciphertext using a private key. The public key may be openly promulgated and the private key is kept undisclosed. Physically, the algorithm is executed by using tie-ups on the mensuration axis of particles of a MES. The use of the public key culminates to a high availability, but it does not subjugates the unconditional security of the postulated algorithm. The availability and the unconditional security have been efficiently integrated in the advocated algorithm.

Acknowledgements

Any accomplishments requires the effort of many people and this work is not different. I thank my Guide Dr. V. K. Pachghare, whose patience and support was instrumental in accomplishing this task. I would like to express the deepest gratitude to my mentor who has the attitude and the substance of a genius: he continually and convincingly conveyed a spirit of adventure in regard to research, and an excitement in regard to experiment and forward thinking. Without his guidance and persistent help this dissertation would not have been possible. I also would like to thank him for showing me some examples that related to the topic of my paper.

I thank the college laboratory staff, whose diligent effort made this paper possible.

I wish to express my gratitude to those who may have contributed to this work, even though anonymously. I owe huge thanks to the departmental library for providing access to numerous international journals, periodicals, university researches, etc.

Every effort has been made to give credit where it is due for the material contained herein. If inadvertently I have omitted giving credit, future work will give due credit to those that are brought to my attention.

References

[1] A. Menezes, P. V. Oorschot, and S. Vanstone. Handbook of Applied Cryptography. CRC Press, Oct. 1996.
[2] Fault-Based Attack of RSA Authentication by Andrea Pellegrini, Valeria Bertacco and Todd Austin http://web.eecs.umich.edu/~valeria/research/publications/DATE10RSA.pdf
[3] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, Feb 1978
[4] Flaw Found in an Online Encryption Methodhttp://www.nytimes.com/2012/02/15/technology/researchers-find-flaw-in-an-online-encryption-method.html?pagewanted=all&_r=1&
[5] A Mighty Number Falls, Press Release – Journalist: Florence Luyhttp://actualites.epfl.ch/presseinfo-com?id=441
[6] The Fall of Contemporary Crypto: Quantum Computing's Challenge to Cyber Security by Derek Soeder http://www.cylance.com/techblog/The-Fall-of-Contemporary-Crypto.shtml
[7] Rose's Law for Quantum computers http://www.abovetopsecret.com/forum/thread936151/pg1
[8] E. Biham, Y. Carmeli, and A. Shamir. Bug Attacks. In Proc. of Advances in Cryptology, Aug 2008.
[9] The Need for Strong SSL Ciphers by Rudolph Araujo http://www.mcafee.com/us/resources/white-papers/foundstone/wp-need-strong-ssldigger.pdf
[10] Patrick J. Flinn and James M. Jordan III. Using the RSA Algorithm for Encryption and Digital Signatures, 1997 Alston & Bird LLP
[11] W. K. Wooters and W. H. Zurek, Nature 299, 802 (1982).
[12] A. K. Ekert, Phys. Rev. Lett. 67, 661, (1991).
[13] C. H. Bennett *et al.*, J. Crypto. 5, 3 (1992); W. T. Buttler *et al.*, Phys. Rev. Lett. 84, 5652 (2000).
[14] C. H. Bennett, and G. Brassard, Advances in Cryptology: Proceedings of Crypto'84, August 1984, Springer-Verlag, 475 (1984); C. H. Bennett, Phys. Rev. Lett., 68, 3121, (1992).