International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 03, March 2017
www.ijates.com
ijates
ISSN 2348 - 7550

QUANTUM SECURE AUTHENTICATION (QSA) FOR SMART CARDS

P.Gayathri Pavani[1], Meghna Daftary[2]

[1,2] Department of Physics, H&S, Sphoorthy Engineering College, (INDIA).

ABSTRACT

Credit card fraud and identity theft are deliberate threats addressed by consumers and industries. It is the challenging issue that is being encountered to safeguard and protect financial data and personal information from criminal activity.Quantum-Secure Authentication is an innovative method that is helping in resolving this problem. It utilizes the unique quantum property of a light to create a secure question and answer exchange that cannot be spoofed. The article outlines the review of how one can restrict the unauthorized access utilizing the Quantum cryptography security model.

Keywords: quantum cryptography, quantum security authentication, Magstripes, Smart Cards

I.1NTRODUCTION

1.1 Why To Study Quantum Properties?

In classical mechanics at any instant identifying the position of particle and momentum is simple. As well known, in wave mechanics, moving particle is a wave group and the identification ofparticle in the wave group is indefinite that could be stated as narrower the wave group higher is the accuracy inlocating the particle but determining the wavelength of the wave is not accurate. In a wide wave group, wavelength can be well defined and hence momentum also becomes accurate but due to more width of the wave group locating the position of the particle becomes less accurate. Thus we have Heisenberg uncertainty principle stating that it is impossible for us to measure two things simultaneously at a time.

For example, it is impossible to determine both the position and momentum of an object at the same time. In practice, these principles have been extended to photons. Photons behave like waves and can be polarized. Quantum properties of photons allow them to be in multiple locations at the same time, thus allowing us to create a complex verification method. It has been decades since the discovery of the quantum properties of matter but scientists still have a hard time in understanding them. With the interest in up growing research in QSA authors have taken up the work to have a review on how QSA is working and its necessity for the further development in the technology.

1.2 Present Day Encoding and Authorization

Example: Magstripe based credit/debit cards, RFI cards and more.

The strip on the back of a credit card is called a magnetic stripe, or a magstripe. The magnetic stripe has many iron-based magnetic particles on it. Essentially the stripe acts as a bar magnet. One end is the northpole and the other end is a south pole. As noted before strip is made from very small magnetic particles (20 millionths of an inch). So on a small scale each particle acts as a tiny bar magnet, and since they are aligned in the North-South direction, the entire stripe is a bar magnet. Thus when a magnetic strip is placed in a very strong external magnetic field(of the opposite polarity – so if the magnetic stripe was N-S, the external field is aligned in S-N) then the polarity of the particles on the stripe are flipped. This action of flipping the magnetic field on the stripe is what “encoding” information is discussed elsewhere[1]. Different types of magnetic materials used on cards have different coercivity. Coercivity is the measure of the resistance of the magnetic material in becoming demagnetised. Magstripes that contain three tracks that can typically be read by most point-of –sale hardware, which are general purpose computers programmed to perform certain things. The computer is also called a card reader. When you swipe or insert a magnetized card, the card reader picks up data from the tiny iron particles in the magnetic strip. A credit/debit card can be demagnetized because the information in the magnetic stripe is magnetic; it is attracted to anything else that is magnetic, so being in contact with the magnetic field will erase the information by realigning the iron particles in the magnetic stripe.Common things that demagnetize credit/debit cards are security screening devices,cell phones, speakers, fridge magnets, magnetic clasps on purses and a lot more. Newer RFID credit cards that are no contact cards are vulnerable to a new technology can steal one’s credit/debit card information without even touching one. The technology can be installed anywhere and is very cheap and thus the encoded data could be easily lost and can make even the most highly secure card vulnerable[3].

1.3 Drawback’s of Today’s Security

The question that now arises is that why are the researchers so interested in quantum properties? We need security everywhere, mainly when we are dealing with money and transactions. But hackers are constantly working to crack security innovations. In the hacking process, one is the sender and the other is the eavesdropper. Sender tries to create complex objects and structures that are according to him difficult to copy; the eavesdropper then tries to copy them and often succeeds. We know that it would take millions of years to break the strongest encryption keys used in defence and government however there is no saying that these keys will be secure forever as they are based on factorizing large numbers. To our knowledge, very long keys such as 2048-bit keys are very safe, as it would take millions and millions of years using the most advanced computers to break them. Recently, however, a key using RSA Security’s RC5-64 algorithm was broken [2, 3]. A student at Notre Dame University, using 10,000 computers working around the clock for 549 days, broke a 109-bit key. This demonstrates both the difficulty of breaking keys and the fact that they can be broken given enough computer power. Someone may eventually discover a mathematical shortcut that allows rapid factoring of large numbers. [2]

II LITERATURE SURVEY

The detailed account of review of related literature pertaining to variables under study, Quantum Computing and Quantum Algorithms was presented by David L. Mills et al. (1993), describing the Network Time Protocol (NTP), specifies its formal structure and summarizes information useful for its implementation[4].

RotheJ. (2002) gave a brief overview of the history and the foundations of classical cryptography, and modern public-key cryptography. A function is one-way if it is easy to compute, but hard to invert. [5]Christopher B. McCubbin (2009) analyzed the security of IPsec against a class of attacks known as the IV attacks, which are based on modifying the initialization vector (IV) of a CBC encrypted packet during transmission[6]. Caliskan, D (2011) showed that in transferring data secretly between two people who are far away from each other Public Key Cryptosystem can be used and RSA is one of the fames Public Key Cryptosystem[7]. Weiqiang Liu (2012) refers that Quantum dot cellular automata (QCA) technology is expected to offer fast computation performance, high density and low power consumption.A power analysis attack can reveal the secret key from measurements of the power consumption during the encryption and decryption process. As there is no electric current flow in QCA technology, the power consumption of QCA circuits is extremely low when compared to their CMOS counterparts. Therefore, in this paper an investigation into both the best and worst case scenarios for attackers is carried out to ascertain if QCA circuits are immune to power analysis attack. A QCA design of a sub module of the Serpent cipher is 57 proposed. It is believed that QCA could be a nice technology in the future for the implementation of security architectures resistant to power analysis attack [8].Quantum Computing and Quantum Algorithms Bennett, C. H. (1992) proves that the security of quantum key distribution relies on the inviolable laws of quantum mechanics, and the impossibility of perfect cloning of non-orthogonal states implies the security of this protocol[9]. Elliot, C (2002) show how quantum key distribution (QKD) techniques can be employed within realistic, highly secure communications systems, using the internet architecture for a specific example[10]. Schartner, P et al. (2009) illustrates that among the various proposals for quantum network design, the trusted node model is still the most flexible one for delivery of messages over arbitrary long distances[11]. Sharbaf, M.S. et al. (2009) refers that Quantum cryptography is an emerging technology in which two parties can secure network communications by applying the phenomena of quantum physics. The security of these transmissions is based on the inviolability of the laws of quantum mechanics. Quantum cryptography was born in the early seventies when Steven Wiesner wrote "Conjugate Coding" [12]. The principle of photon polarization states that, an eavesdropper cannot copy unknown qubits i.e. 59 unknown quantum states, due to no-cloning theorem which was first presented by Wootters and Zurek in 1982. The research paper concentrates on the theory of quantum authentication technique [13].

III HOW TOSOLVE THE PROBLEM?

Literature shows the solution in three words Quantum Secure Authentication (QSA). This innovative security can confirm the identity of any person, objects or structures including credit or debit cards even if a fraction of information has been stolen. The keys could not be reproduced in any of the digital form. Hence it is of no use to the hacker due to the properties of quantum physics. In addition, authentication would require numerous useless tries and having access to both the sender as well as the link which would tamper the channel thus destroying the properties of quantum theory and finding no access to the key. In quantum properties of light, characteristics of Absorption, Emission and Stimulated Emission takes place. It uses odd properties of quantum theory of light to create a secure question and answer exchange that cannot be copied.

IV CONSTRUCTION

A credit or a debit card would contain a paper-thin section of white paint containing millions of nanoparticles. With the help of lasers, individual photons of light are projected onto the tiny paint strip where they bounce around the nanoparticles. They keep on bouncing until they go back to the surface, creating a pattern used to authenticate the card in the first place and it results in a unique authentication pattern that is forever changing, as photons can be in multiple places at the same time.[14]This method, according to the researchers, would make authentication impossible for hackers to hack. It becomes difficult to intersect with the verification process- even if they tried to intersect the question and answer exchange- it would result in the collapse of the quantum properties of the light and the destruction of information being transmitted.This is where there is a difference to ‘normal light'. If a normal light is projected onto the area which allows an attacker could use to measure the entering and returning patterns. But with quantum physics, single ‘photon' dots appear to have more information than projected, making it difficult for a fraudster.

$$|\uparrow\rangle = |0\rangle , \quad |\downarrow\rangle = |1\rangle .$$

Quantum Information - Qubit (quantum bit): superposition of 0 and 1.

where$A$ and B are complex numbers.

Qubit = any two-level quantum system

e.g. an electron with spin

e.g. a photon with polarization

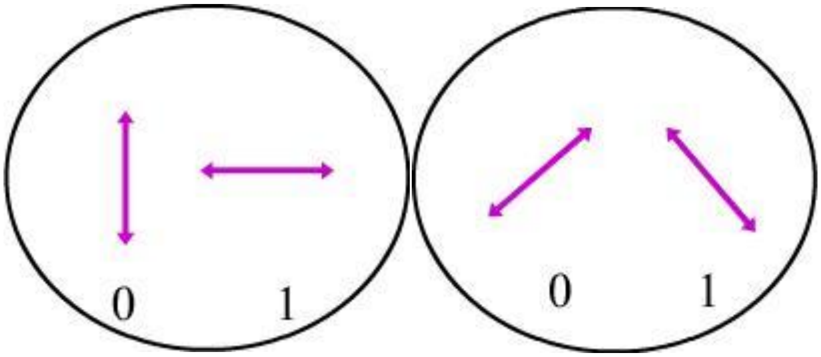
$$|\updownarrow\rangle = |0\rangle , |\leftrightarrow\rangle$$

Note: This is a general statein a superposition of0 and 1

V WORKING

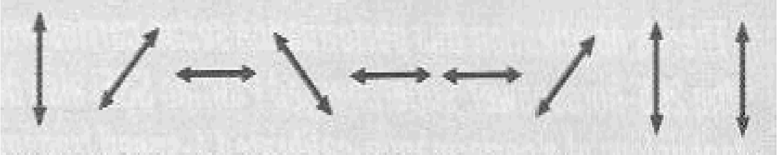
We can exploit the quantum properties of light to sendsecret messages. Light has particle as well as wave like properties, and the waves can be aligned, or polarized, in any direction. Varying wavelengths of light which are present in the ordinary sunlight(which produce the colours in a rainbow) arepolarized in a random fashion. Laser lightis polarized in one direction because it has a light of single wavelength. Lasers can be used to produce photons with a given polarization. Tilting of the light wave can be thought of as polarization. The following examplepolarized photons will be used verticallyorhorizontally, at45degreesand135degrees, denoted|,—,/and\. A calcite crystal can be used as a quantum filter.[5] Vertically or horizontally polarized photons(|or—) will pass through the filter unchangedif the crystal is held in a vertical position. If a photon that is diagonally polarized (/or \) passes through the vertical filter, but the unique part is thatthe polarization will be changed to vertical or horizontal (|or—)in a totally random fashion. Thus, information is lost if the crystal is not aligned correctly, depending on the polarization of the incoming photon. This is what makes it difficult to steal a quantum message without detection. Even though there is a 75probability of decoding a given bit (or photon),after only10 bits of message there is only a 5 percent probability that the eavesdropper measured all of the photons correctly.[5]If the clevereavesdropper then tries topasson the message to the intended recipient, we can easilydetect that someone hasread the message because the originalinformation and the received information will no longer be in good agreement.

CONJUGATE OBSERVABLES



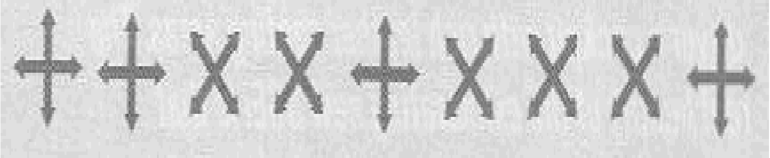
It is fundamentallyIMPOSSIBLE to determine the
Polarization of a single photon in the two bases simultaneously.
(The two self- adjoinoperators representing the two observables do not
Commute. Therefore, they cannot be simultaneously diagonalized.
And, it makes no sense to talk about their simultaneous eigenvectors.)

Followingisan exampleof howpolarizedphotonscan beused to make securekeys.Alicefirstencodesthedataintoa stringof 1 and 0. It is importanttonote that Alicewillusethe“—“and“/”polarizationsrandomlytocodethe0and likewisethe|and\polarizations randomlyfor1.IfAlice sends a one as a vertically polarized photon,and Eve measures it with atilted crystal(because Eve is guessing that it has a“/”or“\” polarization), the result will be of no use to Evebecauseshemeasured it incorrectly. The diagram below show Alice mights end a message using the four different polarizations. The binary strings entis‘100100011’.



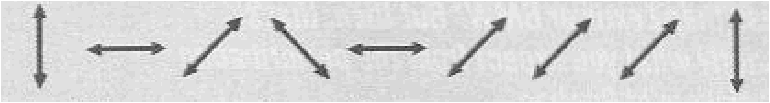
[15]

Bob chooses a measurement type randomly: which is either with the crystal vertical or slantedfor each photon that Alice had sent. The polarised photonswill correctly pass through it, because of the vertical crystal,which is also called as rectilinear measurement, and is designated as“+”. This orientation at which Bobtilts the crystal at a 45 or135 degree angle, which passes correctlyis also called a diagonal measurement, designated “X”. Bob’s random measurements are shown in the diagram below



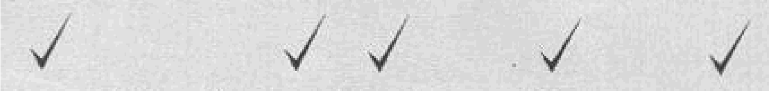
[15]

IfBob uses rectilinear measurement for a photon, his measurement will be “correct”, the measurement would never change the polarization in case of a rectilinear measurement. In diagonal measurement, Bob makes the wrong measurement, and the45-degree photon will come through the crystal randomly as either a horizontal or vertical photon. The following diagram shows the results of Bob’s measurements.



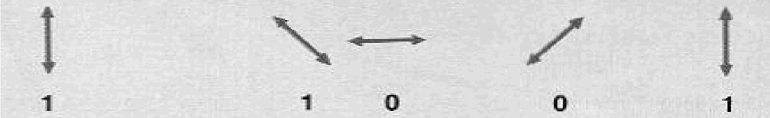
[15]

Then ext step is for Bob to publicly announce which measurements he made (not the results of the measurements). Alice publicly tells Bob for which photons he made the correct type of measurement. The correct measurements made by Bob are checked below.



[15]

Bob keeps all of the results for which he has made the correct measurement and discards the rest. There is loss of some photons because the detectors are not100%efficient.The remaining 1’s and 0’swill make up the key, as seen in the next diagram. The one and zeroes that are left will contain secret information.[15]



Similarly it can be used in the credit/debit cards. The key is authenticated by illuminating it with a light pulse containing fewer photons than spatial degrees of freedom and verifying the spatial shape of the reflected light. As we have mentioned earlier that photons and nanoparticles can be thought of as metallic balls bouncing in the pinball machine.It would be like dropping 10 bowling balls onto the ground and creating 200 separate impacts. It’s impossible to know precisely what information was sent (what pattern was created on the floor) just by collecting the 10 bowling balls. If you tried to observe them falling, it would disrupt the entire system. (Quantum Secure Authentication)QSA does not depend on secrecy of stored data, does not depend on unproven mathematical assumptions, and is straightforward to implement with current technology.

VI CONCLUSION

Using a dual core procedure that involves error correction at one stage and privacy amplification at later, well identifiable portion of secured information can be derived from a quanum transmission. This piece of information is denoted as gain factor. There are four major constituents involve dingain factor – the observed errorrate,the probability that sender’s source indicated that a valid signal was created,theprobabilitythatsendersentamulti-photonpulseandtheprobability that a pulse sent by sender leads to a successful detection by receiver. These factors are combined into an equation to calculate the gain factor for a given quantum implementation. Theequationisbeyondthescopeofthispaper. What is important about the equation s that is possible to derive are - liable secure amount of information from a given transmission and that useful improvements can be made by manipulating & modifying physical equipment to improve gain factor. As an example, itis possible to determine if a signal contains multiple photons. There are detectors that will restrict the sender from sending any information containingmultiple photons. Thus the gainorpercentageofsecureinformationtransmission is quite high in making system more reliable and secure.

REFERENCES

[1]Rankl, Wolfgang. Effing, Wolfgang.(*Smart Card Handbook, John Wiley & Sons Ltd.UK, 2010*) .

[2]Gottesman, Daniel & Lo, Hoi-Kwong, *Quantum Cheating to Quantum Security. Physics Today, Nov 2000*. URL: http://www.aip.org/web2/aiphome/pt/vol-53/iss-11/p22.html (29 Oct. 2002).

[3]http://money.howstuffworks.com/atm-skimming2.htm

[4]David L. Mills,*Quantum Computing and Quantum Algorithms, 1993*

[5]*Quantum Cryptography, BBN Technologies, 21 Oct. 2002,*
URL:http://www.bbn.com/networking/quantumcryptography.html

[6]Christopher B. McCubbin, *Centre for Telecommunications Research, (2009) 89- 97*

[7]Caliskan D,*An application of RSA in data transfer,2011*

[8]W. Liu, L. Lu, M. O'Neill, E. E. Swartzlander, Jr., and R. Woods, *Design of quantum-dot cellular automata circuits using cut-set retiming, IEEE Trans. Nanotechnol, vol. 10, 2011,1150-1160.*

[9]Charles H. Bennet, *Quantum Cryptography, T.J Watson Research Centre,1992.*

[10] Chip Elliott, *Building the quantum network, New Journal of Physics, Volume 4,2002*

[11]Schartner P, *Quantum network design, Nano and Micro Technologies, 2009*

[12],Sharbaf, M.S, *Quantum Cryptography: A New Generation of Information Technology Security System, Information Technologies: New Generation,2009*

[13]W. K. WOOTTERS& W. H. ZUREK, *Letters to nature, 299,1982, 802-803.*

[14]Masters, Gerry. Turner, Phillip. *Forensic Data Recovery and Examination of Magnetic Swipe Card Cloning Devices. Digital Investigation. Volume 4, Supplement 1, September 2007, Pages 16-22.*

[15]Dwyer, Jeffrey, *Quantum Cryptography, URL:*
http://www.cyberbeach.net/~jdwyer/quantum_crypto/quantum1.htm, 2002.