A HYBRID QUANTUM ENCRYPTION ALGORITHM THAT UTILIZES PHOTON ROTATION TO INSURE SECURE TRANSMISSION OF DATA

Karthik Paidi, Anthony Kunkel, Dennis Guster, Renat Sultanov and Erich Rice

Master of Science in Information Assurance Program
Saint Cloud State University
Saint Cloud Minnesota, USA

Abstract

The development of quantum mechanics has led to the possibility of quantum information systems. While there are some quantum devices used in quantum information systems, they are not yet in wide spread use. Therefore, a stop gap solution is to devise hybrid algorithms that use quantum concepts to strengthen classical approaches. This paper offers such as solution that uses the spin rotation of photons to add the power of quantum systems to a classical encryption algorithm.

Keywords: Quantum encryption; information leak; *adaptive algorithm*; security improvement.

1.Introduction

The development of quantum mechanics can be traced back to the work of pioneers such as [23]. However, limitations within the current computing architecture have led to renewed interest in regard to the possibilities of quantum systems. Beginning in the 80s the application of quantum algorithms to information systems problems became practical resulting in useful protocols such as quantum key distribution (QKD) [2], [1], [28] quantum secret sharing (QSS) [8], [6], [27] quantum direct communication (QDC) [7], [17], [18], [19] quantum teleportation (QT) [25], [5] just to name a few.

This new quantum world has also led to the development of quantum computers as well which will revolutionize computing through the use of Qbits leading to amazing processing speed up. In fact, while this speed up is welcomed on many fronts it will render obsolete the current classical encryption algorithms Bernstein, et al, 2009[3]. So therefore, to ensure secret data transmission in the future it is imperative that quantum-based algorithms be devised, tested and implemented to fill the gap. While this is a daunting task there has been some successes in QKD [26].

While it would be difficult to implement a full secure quantum based transmission system on a complex world-wide system such as the internet there are hybrid systems that are now available which support transmission distances of 100s of kilometers[15]. Therefore one of the most effective means of securing data during this transition period would be to focus on a hybrid method that would use quantum seeding and obscure the key in an entirely unpredictable manner. This would begin by using qbits as a means to accomplish the seeding phase.

Qbits can be implemented through a variety of physical systems. Some common examples are ion traps, cavity quantum electrodynamics (QED), nuclear magnetic resonance (NMR), and with the use of quantum dots [22]. For the purposes of this paper it will be viewed as the polarization state of a photon. In the qbit world it is not a single angle but rather, a polarization state consists of all planes in which the electromagnetic wave of a photon propagates. Further, this polarization of a randomly polarized photon is a superposition of any pair of orthogonal states. For example an orthogonal polarization state pairs might be based on horizontal and vertical polarization such as +45° and -45° diagonal polarization.

Specifically in this paper our algorithm will split 0-360 degrees into 2 partitions 0-180 and 181-360. So therefore two possibilities result, either the bits can be in the range of 0-180 or 181-360 degree. This results in four possible ways of associating the data. While this is a relative simplistic way of using qbits the purpose of this paper is a proof of concept. Certainly subsequent work would employ a much more sophisticated use of qbits. Besides using qbits to generate the seed numbers in a truly random fashion there is still a need when using a hybrid algorithm to further complicate the encryption of the key. This can often be accomplished by creating a decoy key or a portion thereof (Lo et al, 2005). In the algorithm devised here in this will be done by constructing the key from embedding arrays and inserting padding randomly.

2.Review of Literature

The work of Bennett and Brassard, 1984 [2] provided a practical means of deploying data transmission using quantum keys. This protocol which has become known as BB84 in its original form it used photon polarization states as the transmission logic. From a quantum perspective, any two pairs of conjugate states can be used to support the protocol. Because several optical fiber based implementations have been devised to use phase based encoding the practicality of this method has increased. Further refinements in the form of a two-step process of this basic BB84 logic have followed. These two steps described as information reconciliation and privacy amplification were first presented by Bennett et al., 1992 [1]. Briefly, information reconciliation can be viewed as a form of error correction carried out during the key exchange, which is designed to ensure that both keys are identical. For more information about a sample protocol using this technique see Brassard and Salvail , 1993 [4].

The second step has been deemed privacy amplification which is a method for almost removing any partial information that might be obtained about the key by an eavesdropper. Specifically, privacy amplification takes the actual key and modifies it to confuse a hacker. Often the resulting key is shorter which provides a potential eavesdropper with only minimal information about the new key. This process is often accomplished by using a universal hash function. For more information concerning this process please refer to, Kaser and Lemire, 2013 [12]. It is a variant in the privacy application process which is the main focus of this paper.

While the development of a full scale internet style quantum encrypted network is still some time off there have been commercial successes. Of particular note would be the work of DARPA (Quantum, 2005), Id Quantique [11] and Los Alamos National Laboratory[9]. While it is generally accepted that the quantum based systems offer enhance security beyond classical solution in part because hacking attacks can be detected. In part the hesitation to adopt them comes from a high equipment cost perceived lack of need. However, it is undeniable that quantum computers continue to progress an exhibit computing speeds that are significantly faster that classical computers[16]. Kirsch, 2015 [13] puts the danger quantum computing poses to classical encryption methods such as RSA into perspective: “a quantum computer can factor a 300 digit number in the same amount of time that an ordinary computer could multiply the factor together, rendering our current encryption methods obsolete”.

Therefore, in the meantime hybrid algorithms are need as a stop gap measure to protect against quantum brute force attacks designed to compromise the encryption key. This of course is the main focus of this paper. In production systems there is often an option of combining a QKE unconditionally secure key exchange sub-system with traditional encryption algorithms such as 3DES or AES [10], [20]While this type of hybrid system cannot be considered unconditionally secure it still offer some security advantages over traditional purely classical strategies. Specifically, the public key authentication mechanism would have to be broken before or during the execution of the QKE protocol [24].

Work with hybrid quantum keys continues to appear in the literature and in many cases the goal is to use a quantum generator and then use mathematical function to obscure the key further. A recent example of this approach is presented by Lai, Xue, Orgun, Xiao and Pieprzyk, Feb. 2015 [14]. They devised a protocol that applies extended unitary operations derived from four basic unitary operations and distributed fountain codes. When testing this protocol they found it to be highly efficient /secure and as planned it provides authentication of parties and detection of eavesdropping.

Because of the effectiveness of hybrid QKD protocols in preventing attacks in the quantum channel a recent work describes the value of applying it to wireless communication. Nail and Reddy, 2015 [21] devised new scheme with the combination of quantum cryptography and classical cryptography for 802.11i wireless LANs. This ground breaking work demonstrated the value and transferability of quantum cryptography and can be viewed as a significant step forward toward securing communications in wireless networks. When tested the hybrid quantum key distribution protocol they devised added robustness in securing wireless networks.

In sum it is clear that quantum encryption can offer distinct advantages over purely classical solutions. While the development of large numbers of large-scale quantum computers is still some time away the problem of current classical algorithms becoming obsolete cannot be ignored. Therefore, stopgap solutions such as hybrid algorithms are still important and it is hoped that the hybrid algorithm offered herein will contribute to the understanding of such concepts both operationally and educationally.

3.Methodology and Sample Problem

To illustrate the methodology and the characteristics of the quantum random number generator based algorithm a sample test of 168 bits was undertaken and is described below.

QRNG ALGORITHM SAMPLE TESTING WITH 168 BITS:

The 168 bits below are the basis for the sample test:

1,1,1,0,0,0,0,1,1,0,0,0,0,0,1,1,1,0,1,1,0,1,0,0

0,0,0,1,1,0,0,0,0,1,1,1,1,0,0,1,1,1,0,0,0,0,0,0

1,1,1,0,0,0,0,1,1,0,0,0,0,0,1,1,1,0,0,0,0,1,1,0

0,0,0,1,1,0,0,1,0,1,1,1,1,0,0,1,1,1,0,1,0,0,0,1

0,1,1,0,0,0,0,1,1,0,0,0,0,0,1,1,1,0,1,1,1,0,0,0

1,0,0,1,1,0,0,1,0,1,1,1,1,0,0,1,1,1,0,0,1,0,0,1

1,1,0,1,0,0,0,0,1,1,0,0,1,1,0,0,1,0,0,0,1,0,1,1

After the algorithm reads the sample bits then it goes into the spin generation phase. In this proof of concept test we will use only a single spin. The angle associated with this spin will be associated with the sample bits. In this simple example the potential 0-360 degree angles are placed into 2 partitions 0-180 and 181-360. So therefore, only two angle possibilities are possible, either the bits can be the range of 0-180 or 181-360. This results in four ways of association, which will be delineated below.

3.1Conversion of bits to angles

In sum, the first spin will generate an angle in the range of 0-360 degrees. It can be any number (angle) such as 0 or 360 degrees or any other angle in between these numbers which when associated with the first bit in the sample results in four possible cases.

These four cases are described below:

Case1: first spin is in range of 0-180 and first bit is 0
Case2: first spin is in range of 0-180 and first bit is 1
Case3: first spin is in range of 181-360 and first bit is 0
Case4: first spin is in range of 181-360 and first bit is 1

- If the case 1 is true then we check for the I th bit of the random generated bits then if the I th bit is 0 then we generate random angle in the range of 0-180 else we will generate angles in the range of 181-360 i.e for 1
- If case 2 is true then we check for the I th bit of the random generated bits then if the I th bit is 0 we generate random angles in the range of 181-360 else we will generate angles in the range of 0-180 i.e for 1
- If the case 3 is true then we check for the I th bit of the random generated bits then if the I th bit is 0 then we generate random angle in the range of 181-360 else we will generate angles in the range of 0-180 i.e for 1
- If case 4 is true then we check for the I th bit of the random generated bits then if the I th bit is 0 we generate random angles in the rage of 0-180 else we will generate angles in the range of 181-360 i.e for 1

The 168 bits were placed in a java class entitled RNG and the spin angles were calculated for the first bit and each respective bit up to the 168^{th} bit in the sample. In the screen below one can see that in our test case the first angle generated is 41 degrees, which is in the range of 0-180. So a quick review of the case defined earlier reveals that it belongs to case 2 because the angle is in range of 0-180 and first bit is 1. The subsequent logic will then follow the sequence specified for the case 2.

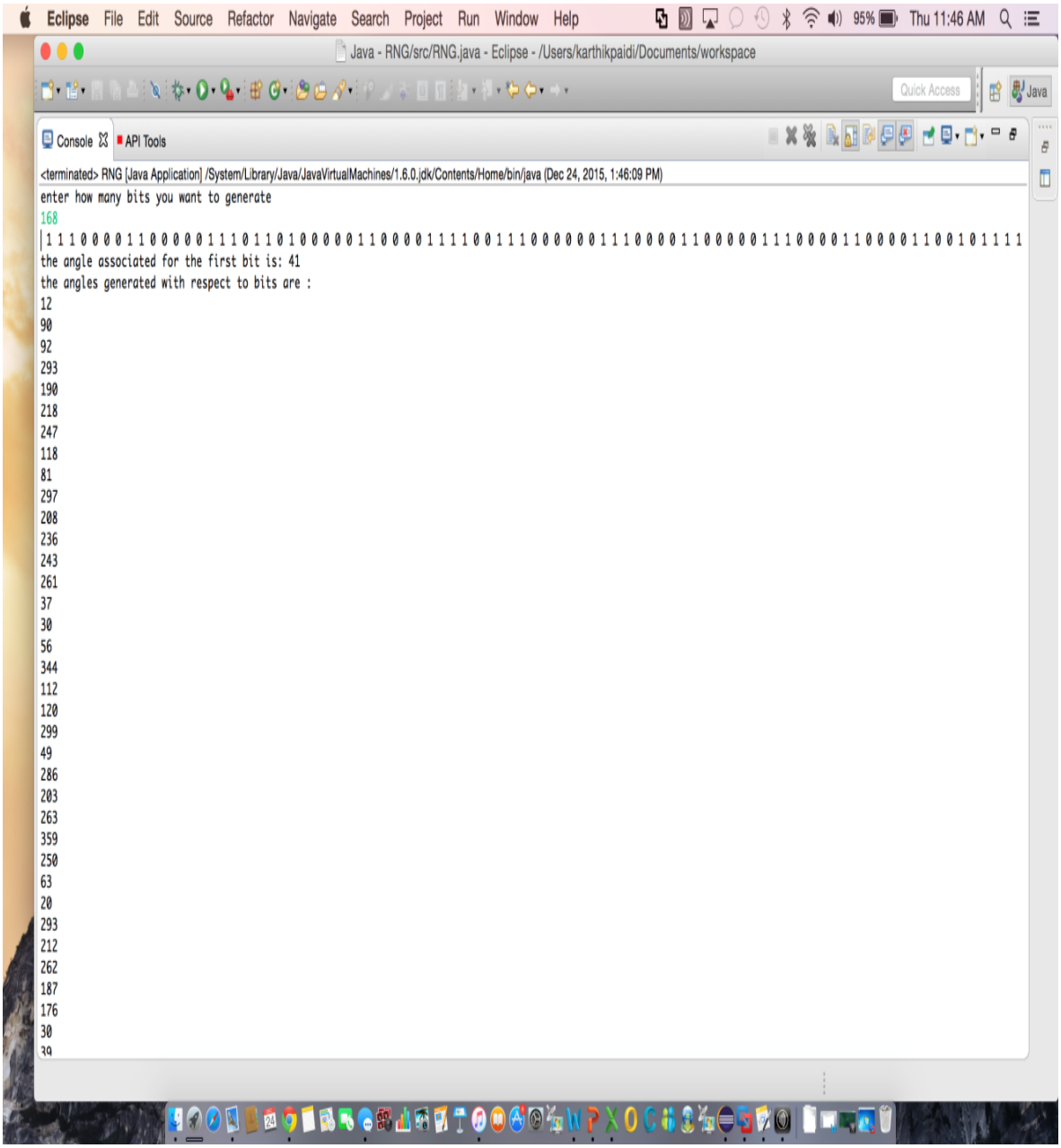

Figure 1:shows the 168 bits, first spin angle and corresponding angles

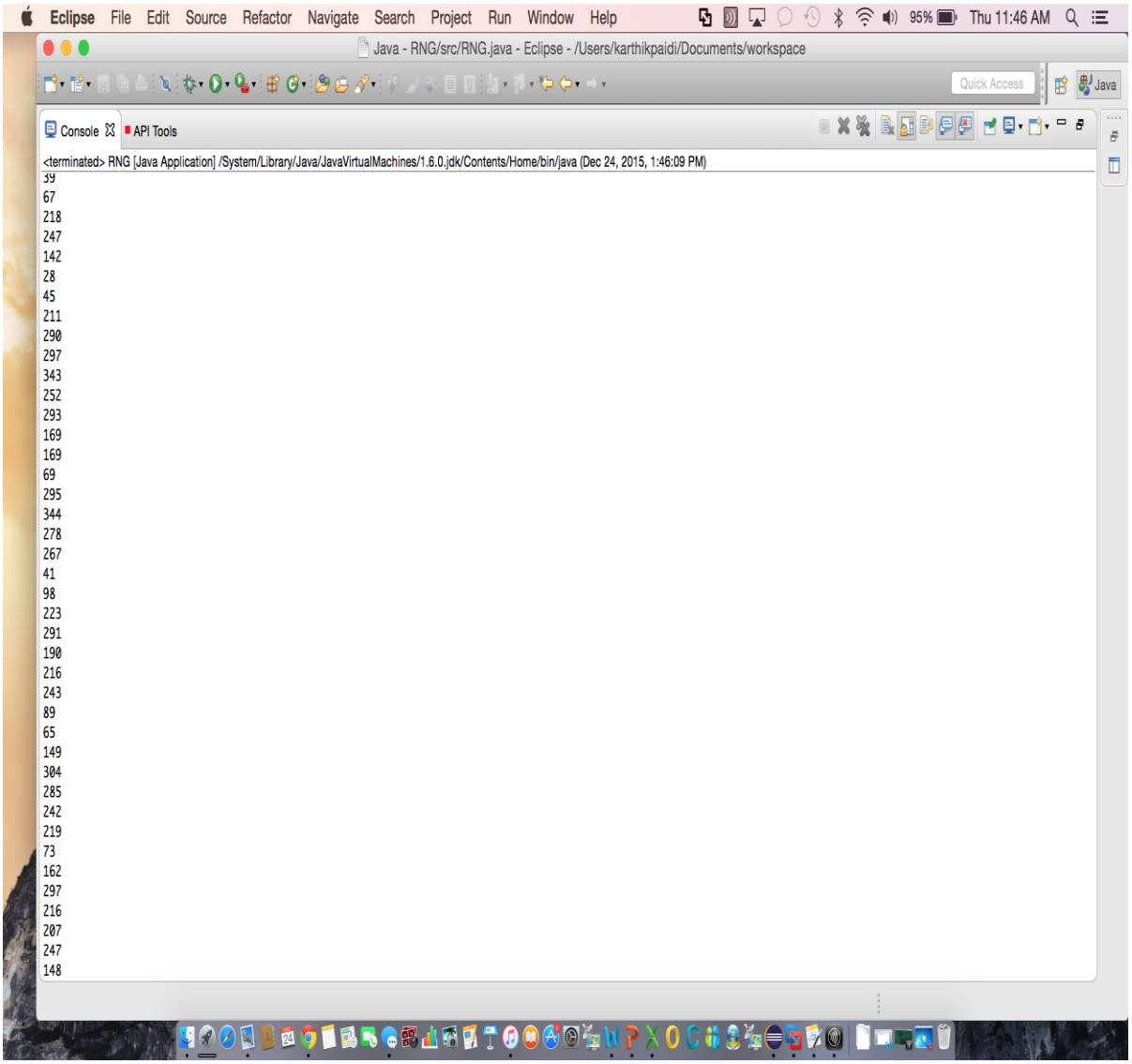

Figure 2: shows the corresponding angles generated for the bits

3.2Conversion of angles to bits

This process include several steps but the key step to be noticed is to remembering the first bit and the corresponding first angle that we have generated, further steps include the four different cases like the above conversion process those are as followed

The four cases are:

Case1: first spin is in range of 0-180 and first bit is 0
Case2: first spin is in range of 0-180 and first bit is 1
Case3: first spin is in range of 181-360 and first bit is 0
Case4: first spin is in range of 181-360 and first bit is 1

- If the case 1 is true then we check for the condition angle we got is in which range weather in 0-180 or 181-360 then if the angle is in range of 0-180 and the case 1 is true then the bit will be 0 else the bit we generate will be 1
- If the case 2 is true then we check for the condition angle we got is in which range weather in 0-180 or 181-360 then if the angle is in the range of 0-180 and the case 2 is true then the bits will be 1 else the bit we generate will be 0
- If the case 3 is true then we check for the condition angle we got is in which range weather in 0-180 or 181-360 then if the angle is in range of 181-360 and the case 3 is true then the bit will be 0 else the bit we generate will be 1
- If the case 4 is true then we check for the condition angle we got is in which range weather in 0-180 or 181-360 then if the angle is in the range of 181-360 and the case 4 is true then the bits will be 1 else the bit we generate will be 0

Given the conditions above if we look at the first spin and the first bit angle, 41 and 1 then it is classified as case 2 and after following the sequence of execution the bits will be returned as first given as input.

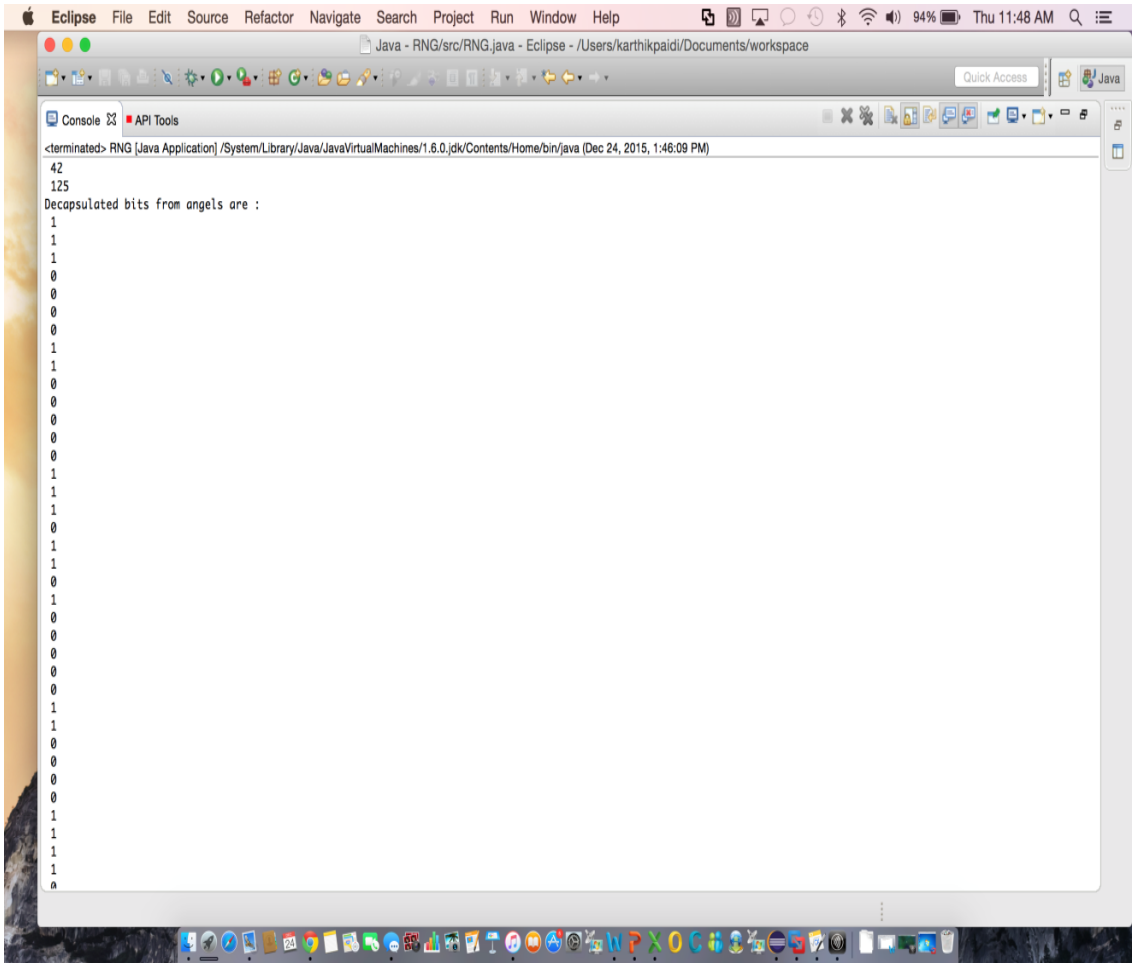

Figure 3: shows the bits conversion process from angles

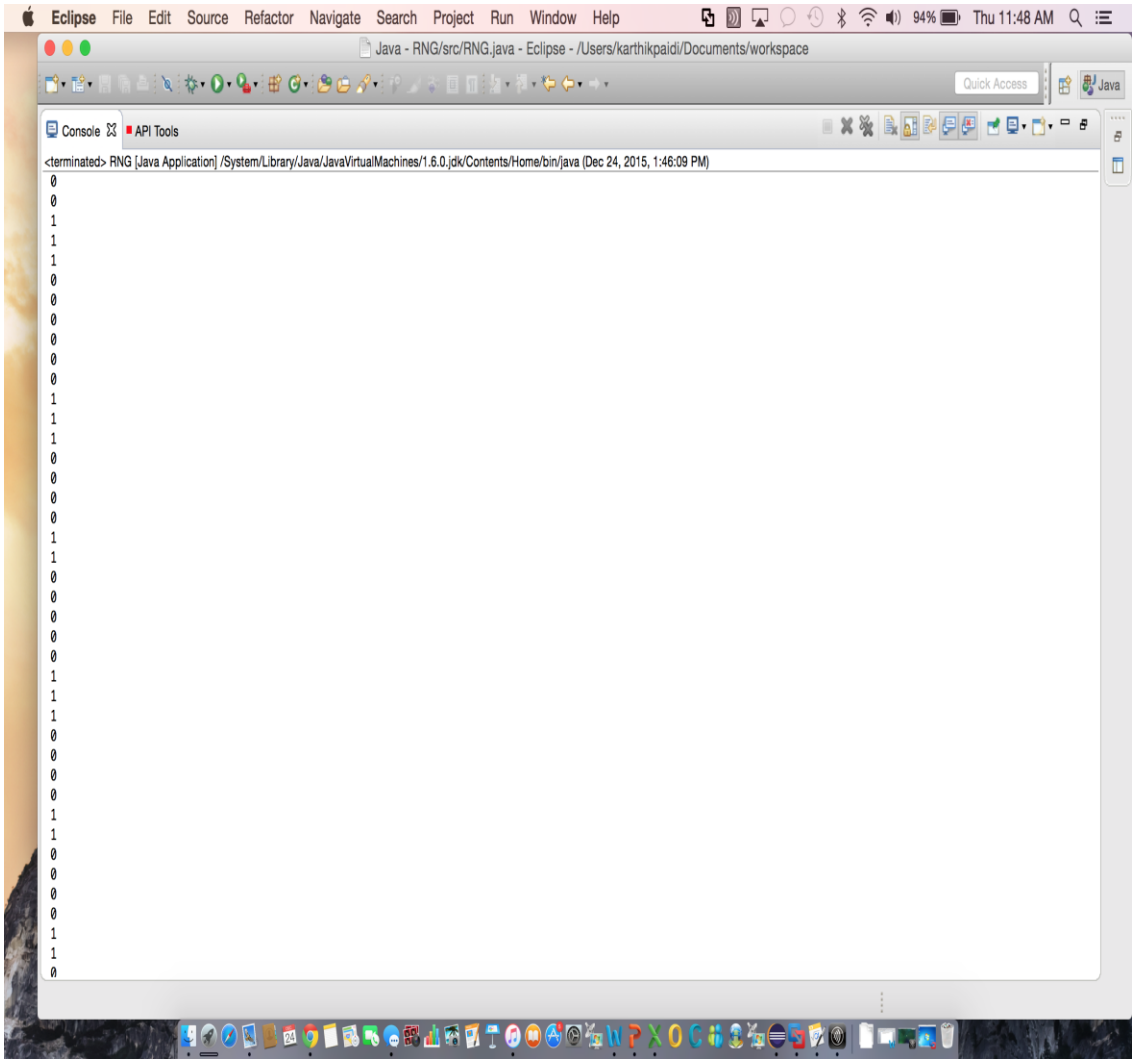

Figure 4:shows the converted bits with respect to the angles

The figures 3 and 4 above depict the conversion process and returns the actual bits entered as input. It is important to note that if this encapsulation process was repeated even with the same number of bits or with the same bits the first spin angle would change so depending on that sequence and the case used the encapsulation scheme would be totally different. So in other words, each encryption session is unique. If one looks at how classical commonly used data stream encryption services work and algorithm is employed and some sort of binary value is linked into that algorithm so that each session is unique. So in the case of secure shell each user would have a different key value. However, how long a given user would use the same key value may vary. Often the keys are downloaded and used over and over again. A quick examination of a VM within the authors' cloud is depicted below and it was determined that the key in question had been in use for about three years.

```
buster@bros:/etc/ssh$ stat ssh_host_rsa_key
  File: `ssh_host_rsa_key'
  Size: 1679            Blocks: 8          IO Block:
4096   regular file
Device: 801h/2049d      Inode: 138536      Links: 1
Access: (0600/-rw-------)  Uid: (    0/    root)
Gid: (    0/    root)
Access: 2016-02-04 17:48:18.115417908 -0600
Modify: 2013-02-09 13:40:16.464628528 -0600
Change: 2013-02-09 13:40:16.464628528 -0600
 Birth: -
```

Employing a more sophisticated system such as Kerberos does reduce the vulnerability scenario because Kerberos uses tickets, which have set expiration times. Once again a quick examination of a VM within the authors' cloud is depicted below and it was determined that the ticket is good for about one day. This certainly lessens the vulnerability window when compared to secure shell.

```
02/05/16 12:49:32  02/05/16 22:49:32
host/bros.cnrl.local@CNRL.LOCAL
        renew until 02/06/16 00:49:26
```

4.Discussion/Conclusions

While this paper was designed to provide a proof of concept scenario a number of positive things emerged. First, this hybrid algorithm was not based on being able to factor large numbers so it would not be vulnerable to a quantum computer being able to factor such number very quickly. Second, creation of a quantum device that would report random spin angle of protons would be very effective in randomizing some encapsulation method which in this case would be the spin angles. Third, this method utilizes an encryption technique that when applied is unique each time because it relies entirely on quantum randomly generated spin angles not a fixed key.

As previously stated this paper was designed as a proof of concept and there are certainly ways of improving the sophistication of the algorithm presented. For example, expanding the number of cases would add significant variance and make it much more difficult to guess angle interrelationships. In its current form with binary number its complexity can be described as 2 to the 2^{nd} power, which gives us four cases. By raising the exponent in the model to the 3^{rd} power eight cases could be easily devised. This would involve a 90-degree of separation and create four angle zones. Instead of just encapsulating the resulting angles in hexadecimal a more sophisticated encryption algorithm could be applied. For example because the code used herein was written in java it would be really

easy to call the AES-128 algorithm as a class from a library. At the very least using an odd number system such as base 17 would be better than just using the old standby: hexadecimal. Also simple things like distributing padding within the key sequence could be used to further obscure the actual data or bit angles.

Like it or not quantum concepts will continue to permeate computing over the next decades. While it is difficult to work entirely in that world at this point the need is coming. It is hoped that hybrid attempts such as the one presented herein will raise awareness and introduce people to the complexities, advantages and challenges of quantum computing.

References

[1] C. H. Bennett, *Phys. Rev. Lett.* 68 (1992) 3121.

[2] C. H. Bennett and G. Brassard, *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing*, Bangalore, India, December 1984, pp. 175–179.

[3] *Bernstein, Daniel J.; Buchmann, Johannes; Dahmen, Erik, eds. (2009). Post-quantum cryptography. Springer.*

[4] G. Brassard and L. Salvail "Secret key reconciliation by public discussion" Advances in Cryptology: Eurocrypt 93 Proc. pp 410-23 (1993).

[5] D. Bouwmeester *et al.*, *Nature* 390 (1997) 575.

[6] R. Cleve, D. Gottesman and H. K. Lo, *Phys. Rev. Lett.* 83 (1999) 648.

[7] F. G. Deng, G. L. Long and X. S. Liu, *Phys. Rev. A* 68 (2003) 042317.

[8] M. Hillery, V. Buzek and A. Berthiaume, *Phys. Rev. A* 59 (1999) 1829.

[9] *Hughes, Richard J.; Nordholt, Jane E.; McCabe, Kevin P.; Newell, Raymond T.; Peterson, Charles G.; Somma, Rolando D. (2013). "Network-Centric Quantum Communications with Application to Critical Infrastructure Protection". arXiv:1305.0305.*

[10] idQuantique SA, Geneva, Switzerland, http://www.idquantique.com.

[11] *Jordans, Frank (12 October 2007). "Swiss Call New Vote Encryption System 'Unbreakable'". technewsworld.com. Archived from the original on 2007-12-09. Retrieved 8 March 2013.*

[12] *Kaser, Owen; Lemire, Daniel (2013). "Strongly universal string hashing is fast". Computer Journal (Oxford University Press).*

[13] *Kirsch, Z. (2015). Quantum Computing: The Risk to Existing Encryption Methods.* http://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf.

[14] Lai, H., Xue, L., Orgun, M., Xiao, J. and Pieprzyk, J. (Feb. 2015). A hybrid quantum key distribution protocol based on extended unitary operations and fountain codes. Journal of Quantum Information Processing, 14(22), pp 697-713.

[15] LaMonica, M. (2013). Long-Distance Quantum Cryptography. http://spectrum.ieee.org/computing/networks/longdistance-quantum-cryptography.

[16] Lee, C. (2015). http://arstechnica.com/science/2015/09/d-wave-unveils-new-quantum-computing-benchmark-and-its-fast/.

[17] W. J. Liu *et al.*, *Chin. Phys. Lett.* 25 (2008) 2354.

[18] W. J. Liu *et al.*, *Chin. Phys. B* 18 (2009) 4105.

[19] Z. H. Liu *et al.*, *Sci. Chin. Inf. Sci.* 55 (2012) 360.

[20] MagiQ Technologies, New York, USA, http://www.magiqtech.com.

[21] Nail, R. L. and Reddy, P. C. (Dec. 2015). Towards Secure Quantum Key Distribution Protocol for Wireless LANS: a Hybrid Approach. Journal of Quantum Information Processing. 14(12). Pp 4557-4574.

[22] Nielsen, N. and I. Chung. (2000). Quantum Computation and Quantum Information. Cambridge Press.

[23] *Planck, M. (1914). The Theory of Heat Radiation. Masius, M. (transl.) (2nd ed.). P. Blakiston's Son & Co. OL 7154661M.*

[24] Paterson, K., Piper, F. and Schack,R. (2007). Why quantum cryptography? Quantum Communication and Security, Proceedings, NATO Advanced Research Workshop, edited by M. ˙Zukowski, S.Kilin and J. Kowalik, p. 175–180 (IOS Press, Amsterdam).Quantum cryptography network gets wireless link - info-tech - 7 June 2005 - New Scientist.

[25] L. Vaidman, *Phys. Rev. A* 49 (1994) 1473.

[26] *Vazirani, Umesh; Vidick, Thomas (2014). "Fully Device-Independent Quantum Key Distribution". Physical Review Letters **113**: 140501.*

[27] L.Xiao, G. L.Long,F. G. Deng and J. W. Pan, *Phys. Rev.A* 69(2004) 052307.

[28] J. Yang, B. J. Xu and H. Guo, *Phys. Rev. A* 86 (2012) 042314.