International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 8, Issue 1, January - February 2019 ISSN 2278-6856

Hybrid Approach for Providing Security by Using Quantum and Elliptic Curve Cryptography

N.Srilatha[1], N.Srikanth[2], B.MANIKANTA[3]

[1]Assistant Professor, Head of the Department, Dept. of CSE, IIIT Srikakulam, RGUKT-AP, Andhra Pradesh, India

[2]Assistant Professor, Dept. of CSE, Nalandha Institute of Engineering & Technology, Andhra Pradesh, India

[3]1st Year B.Tech, Dept. of CSE, IIIT Srikakulam, RGUKT-AP, Andhra Pradesh, India

ABSTRACT
Cryptography is the best way to provide security to unprotected storage of data. In this paper providing more security by using two techniques 1. Elliptic Curve Cryptography 2.Quantum key. Elliptic curve cryptography (ECC) is a modern type of public-key cryptography wherein the encryption key is made public, whereas the decryption key is kept private. Quantum key generation (BB84 Protocol) is used to generate a strong key for encryption of the data. In existing system key of the ECC is generated randomly within the range of prime number N. In proposed Quantum Elliptic Curve QECC algorithm the Key for the Elliptic curve cryptography is generated by the Quantum key distribution algorithm. If the key is not within the range of prime number N then it can regenerate the key value by using BB84 protocol until it accepts by the ECC. By combining this two algorithms security of the data is more increased by the Quantum Elliptic Curve Encryption algorithm.
Keywords: Quantum Key, Elliptic Cryptography

I. INTRODUCTION

Cryptography is the strongest tool for controlling against many kinds of security threats that changes the message from structured data to unstructured data [1][2].
Cryptography is the best way to provide security to unprotected storage of data. There are two fields in Cryptography named as Symmetric Cryptography and Asymmetric Cryptography [3]. ECC (Elliptic Curve Cryptography) is the best Asymmetric Cryptography standard [4]the structure data is easily understood by the every one, so we can convert this format into unstructured data. Now a day we have so many methods for providing the security. The classical cryptography is based on symmetric key or asymmetric key techniques. Symmetric cryptography, also known as secret key cryptography, uses one secret key for both encryption and decryption [5][6]. Symmetric key is provide the security for the possible attacks but it does not work for the brute force attack secret key, by using the DES algorithm we can solve this problem [6][7]. Asymmetric cryptography, also known as public key cryptography, has both a public and a private key, either of which can be used for encryption/decryption. Classical Cryptography suffers from Key Distribution problem, how to communicate the key securely between two pair of users. Security is a problem of key distribution. Quantum Key Distribution is used for providing secure transmission. It enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages. A unique property of Quantum Cryptography is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. This quantum cryptography enables the transfer of data through quits which have the special property that they change their states if they are copied. In simulation of quantum key exchange and authentication followed by an implementation of DNA based algorithm for secure message exchange was implemented. Various protocols that implement quantum key distribution are BB84, B92, Ekert protocols. Generally, the BB84 protocol coding scheme uses four non-orthogonal polarization states where as B92 protocol uses only two orthogonal states that will polarize each of the photon that will be transmitted. In this protocol, sender and receiver have to communicate within two channels, Quantum channel and public channel to share a secret key. In [8] Ekert protocol is a 3-state protocol that uses three non-orthogonal polarization states that will polarize each of the photon.The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e. non-quantum) communication Various security problems exist in designed key distribution protocols; for example, a malicious attacker may derive the session key from the key distribution process. A legitimate participant cannot ensure that the received session key is correct or fresh and a legitimate participant cannot confirm the identity of the other participant. Designing secure key distribution protocols in communication security is a top priority.ECC (Elliptic Curve Cryptography) provides Security much more better way as compared to many Symmetric as well as asymmetric standards [9]. For example, a 160-bit ECC encryption key provides the same security as a 1024-bit RSA encryption key and can be up to 15 times faster, depending on the platform on which it is implemented [10]. Using ECC we get process in less time, less memory, less computations and less power consumption as compare to other Asymmetric type but its performance in terms of speed and area requirements was poor as compared to Symmetric type of Cryptography [11]-[12]. So as we know about Security and performance trade-off; we have to provide a solution in the way like it can improve performance without compromising security; in fact it has to improve performance with improvement in security

[13].Referrence [14] uses Elliptical curve cryptography which is one of the finest mathematical technique invented by Kobitz and Miller. It is complex in nature as compared to other algorithms. It is a trap door function where calculation proceeds in the single direction and the backtracking with reverse engineering methods is quite difficult such this quality make the ECC unique. The security of the ECC lies in discrete logarithm and it is an exponential algorithm which is difficult to break. There are many options other than ECC to encrypt or decrypt the images, like RSA, AES etc, but ECC gives the same security level with RSA at a smaller key size. ECC with multiple threads is used to implement end to end security against man in middle attacks. Reference [15] uses a dynamics approach to the elliptic curve selection, but it has a problem with space complexity. Reference [16] involves the DNA scrambling sequence with ECC for stockpiling the cloud information. Reference [17] uses the Elliptic Curve Diffie–Hellman Encryption with DNA for RGB images with better key sensitivity. Reference [18] uses ECC with Magic matrix notations which is capable to encrypt multimedia data. Reference [19] combines two different cryptographies to convert symmetric encryption to asymmetric. Here Elliptical Curve Cryptography (ECC) keys are used with Hill Cipher algorithm. The first work to introduce a fully balanced ECC implementation was by Batina et al. [20]. The authors modified the non-complete addition formulas over binary extension fields in order to make them balanced. For point multiplication, the Montgomery ladder algorithm was used. The implementation was implemented on an FPGA and the resistance against an SPA attack was evaluated.Twisted Edwards curves and twisted Hessian curves [21]. They all operate over binary extension fields. The work of Renes et al. [22] was the first to propose complete addition formulas on Weierstrass curves over prime fields. In [23], Massolino et al. present the first FPGA implementation of the formulas in [24]. The result is a competitive design emphasizing parallelization possibilities.

II. Relatedwork:

1. Quantum key Distribution Technique

In Quantum Cryptography (using BB84 protocol) a Quantum Key Distribution is used for providing secure transmission. In 1984 Charles Bennett and Gilles Brassard published the first QKD protocol. It was based on Heisenberg's Uncertainty Principle and is simply known as the BB84 protocol after the author's names and the year in which it was published. The basic model for QKD protocols involves two parties, referred to as Alice and Bob, wishing to exchange a key both with access to a classical public communication channel and a quantum communication channel. **Table1** shows how a bit can be encoded in the polarization state of photon in BB84.

TABLE I. BB84 LOOKUP TABLE

Direction	→	↑	↖	↗
Symbols	H	V	L	R
Bits	0	1	0	1

In BB84 protocol, only four directions are used for generating the key. Hacker easily guesses the key from these four directions.

2. Elliptic Curve Cryptography

For the past two decades, Elliptic Curve Cryptography (ECC) has been an attractive alternative to instantiate publickey schemes, multimedia encryption [25], bit coin services [26] [27], etc. for good reasons such as shorter key size, high speed, and lower memory usage. These founded reputations of ECC lie fundamentally on its gorithmically hard discrete logarithm problem (DLP). The elliptic curve in prime finite field *FP* is about cloud of points described by the curve equation of the form [18] $y^2 = x^3 + ax + b \bmod p$ (2) where *x*, *y*, *a*, and *b* are all elements within the *FP*. The coefficients *a*and *b* determine what points will be on the curve. The below fig shows the algorithm of the Elliptic.

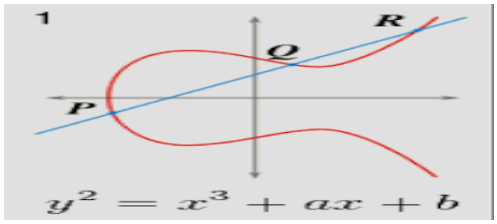

Fig: Elliptic curve Cryptography

EC Three Point Operations

Since each curve has a designated point, finding meaning with each point requires calculations using the EC point

a. Point Addition: Adding the x and y components of an EC are not as easy as adding two numbers. The idea can be associated with connecting two points using a line and then intersecting that line with the curve. In Point Addition, the two points P and Q are added together to obtain another point R on the same EC using the equation.

$R = P + Q, P \neq Q$

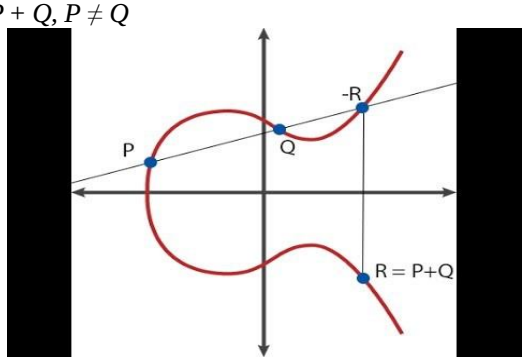

Fig 2: Point Addition of Elliptic Curve algorithm

However, this operation only works when the two components are not the same.

b. Point Doubling: This operation is performed when two points added are identical. Point Doubling is the

addition of a point (P) to itself to obtain another point (Q) on the same EC. The equation for this calculation is:$Q = P+ P$

c. *Point Multiplication:* This is one compound operation of the two operations discussed above. In thisoperation, point addition and point doubling are repeatedly used to find the result. Let point *P* be a pointin EC multiplied with a scalar k (integer) to obtain another point Q on the same EC, giving the equation:$Q = kP$

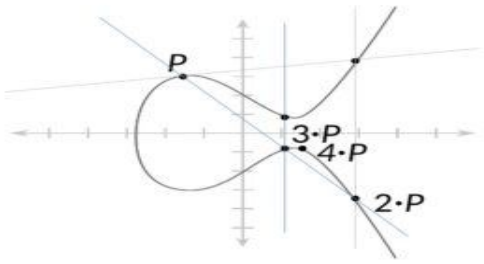

Fig 3: Pont Multiplication of Elliptic Curve algorithm

III. Proposed WORK

This paper proposes a new technique by combining the Quantum Cryptography (BB84 protocol) and Elliptic Curve Cryptography is called QECC Technique. To overcome the drawbacks of Existing systems here two level QECC technique is proposed for providing more security. In existing system key of the ECC is generated randomly within the range of prime number N.in QECC algorithm the Key for the Elliptic curve cryptography is generated by the Quantum key distribution algorithm. If the key is not within the range of prime number N then it can regenerate the key value by using BB84 protocol until it accepts by the ECC.

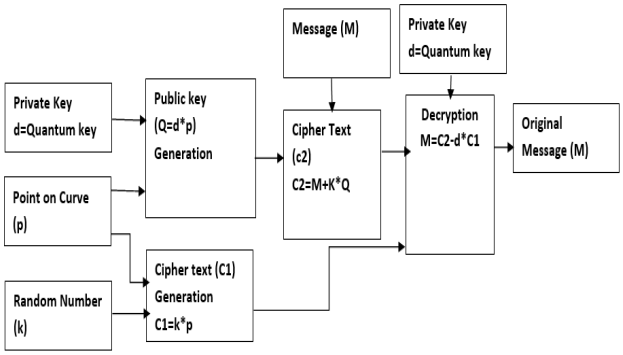

Fig 4: QECC Algorithm

Quantum Key generation (BB84 protocol)

1. Take the Alice and Bob patterns as s1 and s2 strings. Alice string
2. Generate the actual key of Alice and Bob patterns by using BB84 protocol.
3. Compare the key1 and key2 bits for generating key3. If key1 bit equal to key2 bit then key3 value is 1 otherwise 0.
4. Convert key3 from binary to decimal.

QECC Encryption

1. Plain text
2. Take the Equation
   $Y^2 = X^3+aX+b$
   Take a and b any random numbers
3. Take Point P, integer d,N values
   Here
   P is a one of the point of the curve
   N is a Prime value
   Take the key3 value as'd' within the range of **'N'**
4. Generate Q using the equation
   Q=d * P
   Here Q is a Public key and d is a private key
5. Mapping output is M here M is a point which is mapped from message to point
6. Randomly select k which is range with in the 1 to n-1
7. Generate Cipher Text one by using the below equation
   C1=k*P
8. Generate Cipher Text C2 by using the below equation
   C2=M+k*Q
   The two Cipher Text which are send from Sender to Receiver C1, C2.

QECC Decryption

1. We have to get back the message 'm' that was send to us,

   M = C2 – d * C1
   M is the original message that we have send.

2. Output of the ECC Decryption is M

Example:

1. Let the message is "ab"

   Ascii code of a– 97b – 98
   Binary number of ab in 8 bits each is 0110000101100010
   Adding 8-bits of 0's at the end 011000010110001000000000
   Corresponding decimal number is X=6382080
2. Elliptic curve equation is $y^2 = X^3 +ax+b$

Let a=2, b=3, P (prime numbers>x) = 7000003, d=5, k=6
Value of Y when X=6382080, a=2, b=3, $y^2 =(6382080)^3 +2(6382080) + 3 \% 7000003$
Here y^2 is not a perfect square, then X=X+1, X= 6382081
Y becomes 126212
Message point m(x,y) = (6382081, 126212)

3. Another point on the curve is P(x,y) = (3,6)
4. Generate Q using the equation.
   Q = d*p
   Q = 5*(3, 6)
   Q = (3433820, 6372745)
5. C_1 = 6*(3, 6)

= (6696657, 1829975)

6. C2 = M + K*Q

= M + 6*(3433820, 6372745)
= M + (2526824, 2648990)
= (6382081, 126212) + (2526824, 2648990)
= (5829652, 5807224)

7. M = C_2 –d*C_1

=C_2 -5*(6696657, 1829975)
= (5829652, 5807224) – (2526824, 2648990)
= (5829652, 5807224) + (2526824, -2648990)
= (6382081, 126212)

8. Then take 6382081 i.e M(x)
   Binary value of decimal is 01100001011000100000000001
   Discarding the last 8-bits, then 01100001011000100
   The final message “ab”

IV Conclusion

The proposed method of encryption and decryption is far better than existing methods like Elliptic and Quantum Key Distribution (BB84 protocol). The strength of the proposed method is the complex cipher generation from two strong keys. As Quantum computing is a very promising field that keeps the ability to overcome many limitations of silicon computers.Quantum cryptography indicates that it is uncompromisingly secure key distribution, faster key refresh rate than traditional approaches, truly random key generation. In this paper, the proposed method is combining the both two strong techniques. Future enhancement of this paper is performs the mapping techniques from message to Curve points.

References:

[1] B.Jyoshna”Mechanisms for secure data transmission A Survey”, Published in International of Computer Science and Engineering(IJCSE), Vol.-2(8), PP(82-83) August 2014.

[2] R.Shah and Y. S. Chouhan, "Encoding of Hindi Text Using Steganography Technique", International Journal of Scientific Research in Computer Science and Engineering, Vol.2(1),pp. 22-28, Feb 2014.

[3] Anupama T, Dr. M. B. Manjunath, "Fpga implementation of elliptic curve crypto processor over gf(2'63) : A Review," International Journal of Science, Engineering and Technology Research (USETR) , Volume 3, Issue 5, May 2014.

[4] Amir Moradi, Alessandro Barenghi, Christof Paar and Timo Kasper, "On the Vulnerability of FPGA Bit stream Encryption against Power Analysis Attacks," Proceedings of the 18th ACM conference on Computer and communications, pp: 111-124, October 20 II.

[5] Alia, M.A., Yahya,A., “Public–Key Steganography Based on Matching Method”, European Journal of Scientific Research, Vol(2), PP223-231 Aug (2010).

[6] G. Cui, L. Qin, Y. Wang and X. Zhang, “An encryption scheme using DNA technology”, Bio Inspired Computing:

Theories and Applications, pp. 37-42, 2008.

[7] Z. Chen and J. Xu, "One-time-pads encryption in the tile assembly model," Bio-Inspired Computing: Theories and Applications,Vol-46 pp.23- 30,may 2008.

[8] Azarderakhsh, mehran mozaffar kermani, David jao,”post quantum cryptography on FPGA based on isolegines on elliptic curves” IEEE journal,VOL(64),pp86-99,2017

[9] A.Kaleel Rahuman and G.Athisha, "Reconfigurable Architecture for Elliptic Curve Cryptography Using FPGA", Hindawi Publishing Corporation Mathematical Problems in Engineering, 2013.

[10] Bobade, Sunil Devidas, and Vijay R. Mankar. "VLSI architecture for an area efficient Elliptic Curve Cryptographic processor for embedded systems." Industrial Instrumentation and Control (ICIC), 2015 International Conference on. IEEE, 2015.

[11] Anupama T, Dr. M. B. Manjunath, "Fpga implementation of elliptic curve crypto processor over gf(2'63) : A Review," International Journal of Science, Engineering and Technology Research (USETR) , Volume 3, Issue 5, May 2014.

[12] Hossein Mahdizadeh and Massoud Masoumi, ""Novel architecture for efficient FPGA implementation of elliptic curve cryptographic processor over GF(2'63)", IEEE Transactions on very large scale integration (vIsi) systems, Vol. 21, No. 12, pp: 2330- 2333, Dec.2013.

[13]Prashant Ahuja, Prof. Hiren Soni. “Comparative Study of Secure and Efficient Cryptography on FPGA” Journal of Emerging Technologies

and Innovative Research (JETIR), February 2018, Volume 5, Issue

[14] Shaikh, A. A., & Vani, N. S. (2015). An extended approach for securing the Short Messaging Services of GSM using multi-threading elliptical curve cryptography. *2015 International Conference on Communication, Information & Computing Technology (ICCICT).* doi:10.1109/iccict.2015.7045733

[15] Som, S., Majumder, R., & Dutta, S. (2017). Elliptic curve cryptography: A dynamic paradigm. *2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS).* doi:10.1109/ictus.2017.8286045

[16] Selvi, S., Gobi, M., Kanchana, M., & Mary, S. F. (2017). Hyper elliptic curve cryptography in multi cloud-security using DNA (genetic) techniques. *2017 International Conference on Computing Methodologies and Communication (ICCMC).* doi:10.1109/iccmc.2017.8282604.

[17] Kumar, M., Iqbal, A., & Kumar, P. (2016). A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography. *Signal Processing, 125*, 187-202. doi:10.1016/j.sigpro.2016.01.017

[18] Nagaraj, S., Raju, G., & Rao, K. K. (2015). Image Encryption Using Elliptic Curve Cryptography and Matrix. *Procedia Computer Science, 48*, 276-281. doi:10.1016/j.procs.2015.04.182

[19] Dawahdeh, Z. E., Yaakob, S. N., & Razif bin Othman, R. (2017). A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher. *Journal of King Saud University - Computer and Information Sciences.*

[20] L. Batina, N. Mentens, B. Preneel, and I. Verbauwhede, "Balanced point operations for side-channel protection of elliptic curve cryptography,"*IEE Proceedings-Information Security*, vol. 152, no. 1, pp. 57–65, 2005.

[21] D. J. Bernstein, C. Chuengsatiansup, D. Kohel, and T. Lange, "Twisted hessian curves," in International Conference on Cryptology and Information Security in Latin America (LATINCRYPT), ser. LNCS, K. Lauter and F. Rodr´ıguez-Henr´ıquez, Eds., no. 9230. Springer, 2015, pp. 269– 294.

[22] J. Renes, C. Costello, and L. Batina, "Complete addition formulas for prime order elliptic curves," in 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), ser. LNCS, M. Fischlin and J.-S. Coron, Eds., no. 9665. Springer, 2016, pp. 403–428.

[23] P. M. C. Massolino, J. Renes, and L. Batina, "Implementing complete formulas on Weierstrass curves in hardware," in International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE), ser. LNCS, C. Carlet, M. A. Hasan, and V. Saraswat, Eds., no. 10076. Springer, 2016, pp. 89–108.

[24] Ł. Chmielewski, P. M. C. Massolino, J. Vliegen, L. Batina, and N. Mentens, "Completing the complete ECC formulae with countermeasures," Journal of Low Power Electronics and Applications, vol. 7, no. 1, 2017.

[25] L. D. Singh and K. M. Singh, "Image Encryption using Elliptic Curve Cryptography," in Procedia Computer Science, 2015, vol. 54, pp. 472–481.

[26] Q. ShenTu and J. Yu, "A Blind-Mixing Scheme for Bitcoin based on an Elliptic Curve Cryptography Blind Digital Signature Algorithm," Arxiv, no. 1, pp. 1–17, 2015.

[27] N. Courtois, G. Song, and R. Castellucci, "Speed Optimizations in Bitcoin Key Recovery Attacks," Tatra Mt. Math. Publ., vol. 67, no. 1, pp. 55–68, 2016.

[28] K. Lauter, "The advantages of elliptic curve cryptography for wireless security," IEEE Wirel. Commun., vol. 11, no. 1, pp. 62–67, 2004.

[29] C. Paar and J. Pelzl, Understanding Cryptography. Springer-Verlag, 2010.