Confidentiality of communication/computation as well as Authentication and Authorization.

Although various security approaches have been proposed from the academic research community, none of them have been able to guarantee a hundred percent level of security for cloud computing. Crystography can be a suitable solution to security problems of cloud computing.

The term "Crystography" refers to the combination of Cryptography and Steganography for the purpose of enhancing the security of communications, usually involving; images, text or even voice over public networks.

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication [1]. It protects information by transforming it into an unreadable format. It is useful to achieve confidential transmission over a public network. The original text, or *plaintext*, is converted into a coded equivalent called *ciphertext* via an encryption algorithm. Only those who possess a secret key can decipher (*decrypt*) the ciphertext into plaintext [4].

5. The Cryptographic Technique

According to [2], a message in readable form is referred to in cryptographic terms as plaintext. The process of disguising a message in such a way as to hide its substance is called encryption and the resulting message is referred to as ciphertext. The reverse process (decryption) takes ciphertext, C as input and restores the original plaintext. P. The encryption function E operates on P to produce C:

$$E(P) = C \quad (1)$$

In the reverse process, the decryption function D operates on C to produce P:

$$D(C) = P \quad (2)$$

A cryptographic algorithm called a cipher, is a mathematical function that is used for encryption and decryption requires the cryptosystem kept secret. This method is called security by obscurity and is used only in very specific cases. All modern encryption algorithms use a key, denoted by K. The value of this key affects the encryption and decryption functions. The functions become:

$$E(K,P) = C \quad (3)$$

$$D(K,C) = P \quad (4)$$

Cryptography systems can be broadly classified into symmetric-key systems, that use a single key (i.e., a *password*) that both the sender and the receiver have, as well as public-key systems that use two keys, a *public key* known to everyone and a *private key* that only the recipient of messages uses. In the rest of this paper, we will focus more on public key cryptography.

6. Motivation

Public key cryptography is used in e-commerce for authentication (electronic signatures) and secure communication (encryption). The most widely used cryptosystems RSA and ECC (elliptic curve cryptosystems) are based on the problem of integer factorization and discrete logarithm respectively. Improvements in factorization algorithm and computation power demands larger bit size in RSA key. At present the recommended key size is of 1024 bits which may have to be increased to 4096 bits by 2015 [18]. Larger key size makes RSA less efficient for practical applications. ECC are more efficient as compared to RSA, but its shortest signature is of 320 bits which is still long for many applications [1]. Although RSA and ECC have these drawbacks, they are still not broken. But in 1999, Peter Shor discovered a polynomial time algorithm for integer factorization and computation of discrete logarithm on quantum computers [8]. The resultant explosive increase in processing power of computers, will greatly produce reductions in the work factor required to solve IFP and DLP problems [1].

To the best of our knowledge, most existing Crystosytems are built around Public key Cryptographic schemes like RSA and Elliptic Curve Cryptography (ECC), whose security stems from the difficulty in solving Integer Factorisation Problem (IFP) and Discrete Logarithm problem (DLP) respectively. Thus, once we have quantum computers in commercial quantity, such systems can no longer be considered secure.

So there is a strong motivation to develop public key crystographic systems based on problems which are secure on both conventional and quantum computers.

7. Post-Quantum Cryptography

Attention of many cryptography researchers have now shifted to building systems equipped with resistance to both classical and quantum attacks. To this end, there are basically four main classes of public-key cryptography that are believed to fall into this category:

- Code-based cryptography
- Hash-based cryptography
- Lattice-based cryptography
- Multivariate public-key cryptography.

8. Multivariate Public Key Cryptography

Multivariate Quadratic Polynomials gives a new direction to the field of cryptography. Cryptography based on them can be a possible option applicable to both conventional and quantum computers [8]. In multivariate cryptography, security is based on the problem of solving system of nonlinear

equations which is proven to be Non deterministic Polynomial Complete or hard (NP-complete/NP-Hard), over a finite field.

Figure 2 shows such a system of *m* quadratic equations in *n* variables.

$$
\begin{aligned}
p^{(1)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)}\cdot x_i x_j + \sum_{i=1}^{n} p_i^{(1)}\cdot x_i + p_0^{(1)} \\
p^{(2)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)}\cdot x_i x_j + \sum_{i=1}^{n} p_i^{(2)}\cdot x_i + p_0^{(2)} \\
&\vdots \\
p^{(m)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)}\cdot x_i x_j + \sum_{i=1}^{n} p_i^{(m)}\cdot x_i + p_0^{(m)}.
\end{aligned}
$$

Figure 2. A System of Quadratic Polynomials

This means, we wish to solve the system of equations in figure 2, for a given $P = (p^1, \ldots p^m) \in F_q^m$ and the unknown $x = (x_1,x_2....,x_n) \in F_q^m$.

True to the term quadratic, in the above system of equations, the polynomials p_i have the form;

$p_i (x_1, x_2...., x_n) = \Sigma(1\leq j\leq k\leq n) \gamma_{i,j,k} x_j x_k + \Sigma_{(j=1 \text{ to } n)} \beta_{i,j} x_j + \alpha_i$ for $1\leq i\leq m$; $1\leq j\leq k\leq n$ and $\alpha_i, \beta_{i,j}, \gamma_{i,j,k} \in F_q$ (the constant, linear and quadratic coefficients respectively). It has been shown that over a finite field, this problem is NP hard.

Petzoldt Albrecht in [15] pointed out that, beyond the supposed resistance against quantum computer attacks, multivariate schemes enjoy a number of advantages that includes:

- **Speed:** Multivariate schemes are very fast, especially for signatures. In fact, there are many hints that multivariate schemes can be faster than classical public key schemes like RSA and ECC.

- **Modest Computational Requirements:** The mathematical operations performed by multivariate schemes are usually very simple: Most schemes need only addition and multiplication over small finite fields. Therefore multivariate schemes require only modest computational resources, and this makes them attractive for the use on low cost devices such as RFID chips and smart cards, without the need of a cryptographic coprocessor.

- **Hardness of the MQ-Problem: T**he best known attacks against this problem are still exponential. This is in contrast to schemes based on the problem of integer factorization, which can be solved in sub-exponential time by algorithms like the number field sieve. From this point of view, the trust in the hardness of the MQ-Problem might be stronger than for integer factorization and the parameters of multivariate schemes have not to be adapted as drastically as those of RSA.

- **Variety of Cryptographic Schemes: I**t is always better to have cryptographic schemes based on a large variety of problems. As mentioned above, nearly all cryptographic schemes used today are based either on the integer factorization or the discrete logarithm problem. Therefore, a major cryptanalytic success against one of these two problems would lead to a severe security problem. With having a greater range of cryptographic schemes, the impacts of such a cryptanalytic break through would be much less grave.

9. Steganography

One of the principal weaknesses of all encryption systems is that the form of the output data (the ciphertext), if intercepted, alerts the intruder to the fact that the information being transmitted may be of some importance and that it is thereby worth attacking. It is therefore of significant value if a method can be found that allows data to be transmitted by embedding it in non-sensitive information after (or otherwise) it has been encrypted [3].

This is known as Steganography which is concerned with developing methods of writing hidden messages in such a way that no one, apart from the intended recipient, knows of the existence of the message in contrast to cryptography in which the existence of the message itself is not disguised but the content is scrambled [10].

A steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion [16]. As an example, it is possible to embed a text inside an image or an audio file.

Although Cryptography and Steganography are both excellent means of protecting information from unwanted parties, neither of these two technologies alone is perfect as both can be broken. It is for this reason that most experts would suggest using both to add multiple layers of security [14].

Other researchers also opined that although Steganography technologies are very important part of the future of Internet security and privacy on open systems such as the Internet, it is a better idea to use the properties of Cryptography and Steganography together to provide a very acceptable amount of privacy for anyone connecting to and communicating over these systems.

There is therefore a serious motivation, for a Crystographic (cryptographic + steganographic) system, that will not only make messages/information unintelligible, but also hide the mere existence of such gibberish away from suspicion of any eavesdropper or attacker.

This paper specifically proposes a framework that will integrate Multivariate Quadratic Polynomial based Cryptography with Steganography. This chemistry is expected to add multiple layer of security and satisfy requirements such

as capacity, security and robustness for secure data transmission over an open channel.

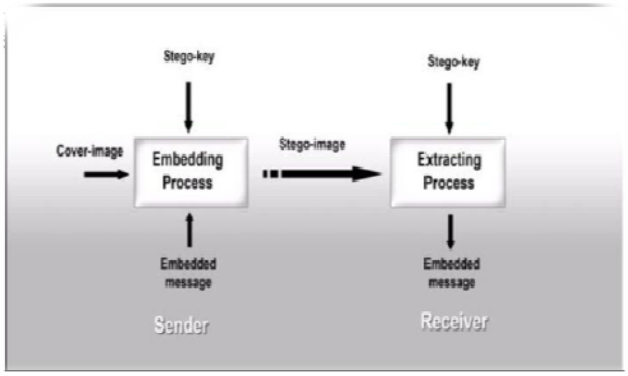

Figure 3. A general Steganographic framework

10. The Proposed System

The modern formulation of steganography is often given in terms of the *prisoners' problem* [12] where Alice and Bob are two inmates who wish to communicate in order to hatch an escape plan. However, all communication between them is examined by the warden, Wendy, who will put them in solitary confinement at the slightest suspicion of covert communication.

In the proposed system, we have Bob (the *sender*) wishing to send a secret message *P* to Alice (the *receiver*): in order to do this, Bob first encrypts the message using a Multivariate Quadratic Polynomial encryption algorithm to produce a ciphertext, *M*. He then chooses a cover image *C*. The steganographic algorithm identifies *C*'s redundant bits (i.e., those that can be modified without arising Wendy's suspicion), then the embedding process creates a *stego image S* by replacing these redundant bits with data from *M*.

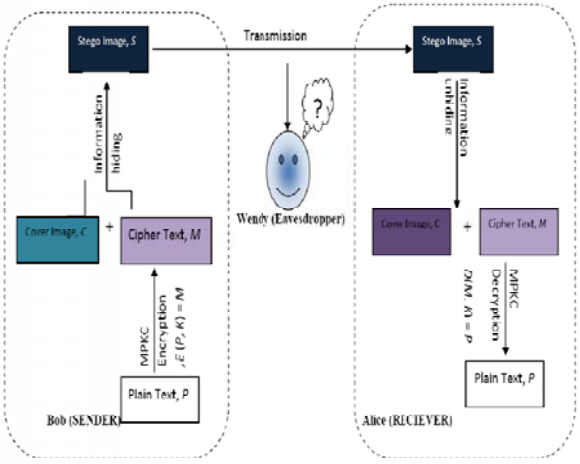

Figure 4. A Conceptual model of the proposed crystographic system

S is transmitted over a public channel (monitored by Wendy) and is received by Alice only if Wendy has no suspicion on it. Once Alice receives *S*, she can get *M* through the extracting process.

The embedding process represents the critical task for a steganographic system since *S* must be as similar as possible to *C* for avoiding Wendy's intervention (Wendy acts for the *eavesdropper*).

Least significant bit (LSB) insertion is a common and simple approach to embed information in a cover file: it overwrites the LSB of a pixel with an *M*'s bit. If we choose a 24-bit image as cover, we can store 3 bits in each pixel. To the human eye, the resulting stego image will look identical to the cover image [12].

Unfortunately, modifying the cover image changes its statistical properties, so eavesdroppers can detect the distortions in the resulting stego image's statistical properties. In fact, the embedding of high-entropy data (often due to encryption) changes the histogram of colour frequencies in a predictable way. Since standard steganographic systems do not provide strong message encryption, this work proposes a scenario where *M* is encrypted before embedding. Because of this, we're proposing a two-step protocol: first we must cipher *P* using a Multivariate Quadratic Polynomial based Encryption Algorithm (that is, a Post Quantum Encryption Algorithm) to obtain a ciphertext, *M* and then we can embed *M* in *C* using the Least Significant Bit (LSB) technique in order to produce a stego image, *S,* which is then transmitted over the network to the receiver..

The Simplified diagram in figure 4 shows the flow of data across the proposed system, from a sender to a receiver.

10.1. PHASE 1: Encryption

Before sending a piece of message, a sender first encrypts the message, using a Multivariate Quadratic Polynomial based encryption algorithm. This algorithm is necessary for enhancing the robustness of the security of the proposed system. This should make the system useful or relevant in both classical computing as well as in the post quantum era.

10.2. PHASE 2: Hiding the cipher text in a cover image

Once the encryption is done, the resultant ciphertext is then hidden in a cover image. Hiding information inside images is a popular technique nowadays. An image with a secret message inside can easily be spread over the World Wide Web or in newsgroups. The most common methods for making these alterations involve the usage of the least significant bit (LSB), masking, filtering and transformations on the cover image. These techniques can be used with varying degrees of success on different types of image files [5].

10.1.1. The Least Significant Bits (LSB) Approach. A simple approach for embedding information in cover image is using Least Significant Bits (LSB). The simplest steganography techniques embed the bits of the message

directly into least significant bit plane of the cover image in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small. To hide a secret message inside an image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24-bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel. For example, the following grid can be considered as 3 pixels of a 24-bit color image, using 9 bytes of memory:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

When the character A, which binary value equals 10000001, is inserted, the following grid results:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

In this case, only three bits needed to be changed to insert the character successfully. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximal cover size. The result changes that are made to the least significant bits are too small to be recognized by the human visual system (HVS), so the message is effectively hidden [14]. As shown, the least significant bit of third color remains without any changes. It can be used for checking the correctness.

10.3. PHASE 3: Receiver splits Stego Image into Cover Image and CipherText

On receiving the Stego Image, *S,* the receiver performs a reverse of the Message hiding process, to reveal the cover image, *C* and the ciphertext, *M*.

10.4. PHASE 4: Decryption

The receiver then, applies the decryption algorithm and key corresponding to the one used for encryption by the sender, on the ciphertext *M* in order to get back the original plaintext message, *P*.

11. Conclusion

Various techniques have been developed for enhancing the security confidentiality of cloud communication/computation. None of these however have been able to guarantee one hundred percent security [9].

Crystography is a very new and interesting topic for researchers and the combination of Cryptography and Steganography is used in it so all security purpose are solved.

This paper has proposed a public key multi-level security system (crystosystem) that will guarantee security of cloud computing in both Classical and Post Quantum Computing era.

12. References

[1] Alese, B. K., Philemon E. D., Falaki, S. O., (2012). “Comparative Analysis of Public-Key Encryption Schemes”. International Journal of Engineering and Technology Volume 2 No. 9, September, 2012.

[2] Alowolodu O.D, Alese B.K, Adetunmbi, A.O., Adewale O.S., Ogundele, O.S. (2013). “Elliptic Curve Cryptography for Securing Cloud Computing Applications”. International Journal of Computer Applications (0975 – 8887) Volume 66– No.23, March 2013.

[3] Blackledge, J., (2010). “Information Hiding using Stochastic Diffusion for the Covert Transmission of Encrypted Images”. ISSC 2010, UCC, Cork, June 23-24

[4] Bloisi, D.D. , Locchi, L: “Image based Steganography and cryptography”, Computer Vision theory and applications volume 1 , pp. 127-134 .

[5] Cachin C. (2005). Digital Steganography, Encyclopedia of Cryptography and Security.

[6] Daniele, C (2009). "Cloud Computing: benefits, risks and recommendations for information security." Available online at www.google.com

[7] Dahal S. (2012). “Security Architecture for Cloud Computing Platform”. Master of Science Thesis Stockholm, Sweden 2012. TRITA-ICT-EX-2012:291 available online at www.google.com

[8] Ding, J. Gower, J. and Schmidt, D. (2006), “Multivariate Public Key Cryptosystems.” Springer Publishers.

[9] Gabriel A.J., Alese B.K., Adetunmbi A.O. and Adewale O.S. (2010). “Design and Implementation of Internet Protocol Security Filtering Rules in a Network Environment”. International Journal of Computer Science and Information Security (IJCSIS), U.S.A. Vol. 9, No. 7. Pages 134-143.

[10] Johnson, N.F. and Katzenbeisser, S. (2000), “A survey of steganographic techniques,” in Proc. Information Hiding, Norwood, MA, 2000, pp. 43–78.

[11] Kaufman, L. M. (2010) "Can public-cloud security meet its unique challenges?" Security & Privacy, IEEE 8.4(2010): 55-57.

[12] Kharrazi, M., Sencar, H. T., and Memon, N. (2004). “Image steganography: Concepts and practice”. In WSPC Lecture Notes Series.

[13] Kui, R., Wang, C. and Wang, Q. (2012) "Security challenges for the public cloud." Internet Computing, IEEE 16.1 (2012): 69-73.

[14] Luthra L., Dawra, M., (2013); "VCS: A New Security Framework" Journal of Engineering, Computers & Applied Sciences (JEC&AS) ISSN No: 23195606 Volume 2, No.7, July 2013

[15] Petzoldt A. (2013). "Selecting and Reducing Key sizes for Multivariate Cryptography". PhD. Thesis. Technical University Darmstadt.

[16] Provos, N. and Honeyman, P. (2003). "Hide and seek: An introduction to steganography". IEEE SECURITY & PRIVACY.

[17] Rajyaguru, M.H. (2012) "CRYSTOGRAPHY- Combination of Cryptography and Steganography With Rapidly Changing Keys". International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 10, October 2012)

[18] Schneier, B. (1996). "Applied Cryptography - protocols, algorithms, and source code in C". John Wiley & Sons, Inc., 2nd edition, 1996. ISBN 0-471-12845-7 or 0-471-11709-9.

[19] Shor, P. (1997) "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM Journal on Computing. 26 no. 5, 1484-1509

[20] Sosinsky B. (2011). "Cloud Computing Bible". 1st ed. Wiley; 2011.

[21] Subashini S. and Kavitha, V. (2011) "A Survey on Security Minimal issues in service delivery models of cloud computing" Journal of Network and Computer Applications, 34(1), 2011, pp 1-11

[22] Sultan N (2010). Cloud computing for education: A new-dawn? International Journal of Information Management 30 (2010) 109–116

