ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists

Volume 1 Issue 2 September 2011

ERROR FREE E-MESSAGING ON POST QUANTUM CRYPTOSYSTEM

Abhishek Shukla
(Research Scholar Singhania University, Jhunjhunu, Rajsthan).
R.K.G. Institute of Technology,
5th K.M. Stone Delhi-Meerut, Road,
Gzb.U.P. (India)

Meenu Sahni
(Research Scholar Mewar University, Chittorgarh, Rajsthan).
Bhagwati Institute of Technology & Science, Ghaziabad, U.P.

Deo Brat Ojha
R.K.G. Institute of Technology,
5th K.M. Stone Delhi-Meerut, Road, Gzb.U.P. (India)

Abstract

In this paper, we presented an errorless model of communication system for two communicators. It is the model of a real-life secure messaging system for any organization. In this model Alice can send a secret message even to any strange person in an anonymous way. The users of this model are assumed to be may or may not be the members of a closed organization. If any error occurred during the transmission due to teeming channel, it can also be determine & encountered by error correction function.

Keywords: Message, Transmission Error, Stegnography, Error Correction function, Secure Communication.

1. Introduction

Modern steganography has a relatively short history because people did not pay much attention to this skill until Internet security became a social concern. Most people did not know what steganography was because they did not have any means to know the meaning.

Even today ordinary dictionaries do not contain the word “steganography.” Books on steganography are still very few [1], [2].

The most important feature of this steganography is that it has a very large data hiding capacity [3], [4]. Steganography can be applied to variety of information systems. Some

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
Volume 1 Issue 2 September 2011

key is used in these systems when it embeds/extracts secret data. One natural application is a secret mailing system [5], [6] that uses a symmetric key. Another application pays attention to the nature of steganography whereby the external data (e.g., visible image data) and the internal data (any hidden information) cannot be separated by any means. We will term this nature as an "inseparability" of the two forms of data.

In this current paper, we will show an anonymous and covert e-mailing system with some transmission error. Present paper is as follows. In Section 3 describes the scheme of an (Error free E-messaging on Post Quantum Cryptosystem - EEPQC). Section 4 we will show error correction code. How we can make it a safe system with error detection and correction in Section 5. Finally, section 6 is conclusion.

2.BASIC AND PRELIMINARIES:

First select secret key W is a random (k ×k) nonsingular matrix over GF(2) called the scrambling matrix, T is a (k × n) generator matrix of a binary Goppa code T with the capability of correcting n –bit random error vector of weight less than or equal to a, and Q is a random (n × n) permutation matrix.

Public Key: V = WTQ

A tuple $\{P,H,M,f\}$ where $M \subseteq \{0,1\}^k$ is a message set which consider as a code, P is a set of individuals, generally with three elements A as the committing party, B as the party to which commitment is made and TC as the trusted party, f is error correction function and $H = \{t_i, a_i\}$ are called the events occurring at times t_i $i = 0,1,2,$ as per algorithm a_i $i = 0,1,2,$. The scheme always culminates in either acceptance or rejection by A and B.

In the setup phase , the environment is setup initially and public commitment key CK generated, according to the algorithm $setupa\lg(a_0)$ and published to the parties A and B at time t_0 . During the commit phase, Alice commits to a message

$$m \in M \text{ then she finds } g : m \to mV \ .$$

Encryption: E = mV +e, where m is the k -bit message, E is an n -bit cipher text and e is an n -bit random error vector of weight a.
According to the algorithms commitalge1 into string c i.e. her commitment

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
Volume 1 Issue 2 September 2011

$$c = g(m)\ XOR\ E$$

then after Alice sends c to Bob, which Bob will receive as $t(c)$, where t is the transmission function which includes noise.
In the open phase, Alice sends the procedure for revealing the hidden commitment at time t_2 and Bob use this.
So Alice discloses the procedure $g(m)$ and E to Bob to open the commitment. $open\lg(e_2)$:
Bob constructs c' using commitalg, message $t(m)$ and opening key i.e.

$$c' = t(g(m))\ XOR\ \mathrm{t}(E)$$

and checks whether the result is same as the received $t(c)$.

Fuzzy decision making

$$\text{If } (nearness\ (t(c), f(c')) \le Z_0)$$
$$\text{Then A is bound to act as in m}$$
$$\text{Else he is free not to act as m.}$$

Then after acceptance, Bob calculates $f(c')(WTQ)^{-1}$ and finally gets the message.

3. EEPQC:

EEPQC is a steganography application program. In the following description, $M_{EEPQC\,I}$ denotes a member $EEPQC\ I$, and $M_{EEPQC\,II}$ denotes a member $EEPQC\ II$.

An EEPQC consists of the three following components.

1. Envelope Producer (EP).
2. Message Inserter (MI).
3. Envelope Opener (EO).

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
Volume 1 Issue 2 September 2011

We denote $M_{EEPQC\,I}$'s EEPQC as $EEPQC\,I$ (i.e., customized EEPQC by $M_{EEPQC\,I}$). So, it is described as $EEPQC_I=(EP_{EEPQC\,I},MI_{EEPQC\,I},EO_{EEPQC\,I})$.. $EP_{EEPQC\,I}$ is a component that produces $M_{EEPQC\,I}$'s envelope $(E_{EEPQC\,I})$. $(E_{EEPQC\,I})$ is the envelope (actually, an image file) which is used by all other members in the organization when they send a secret message to $(M_{EEPQC\,I})$. $(EO_{EEPQC\,I})$ is produced from an original image (EO). $(M_{EEPQC\,I})$ can select it according to his preference. $(E_{EEPQC\,I})$ has both the name and e-mail address of $(M_{EEPQC\,I})$ on the envelope surface (actually, the name and address are "printed" on image $(E_{EEPQC\,I})$. It will be placed at an open site in the organization so that anyone can get it freely and use it any time. Or someone may ask $(M_{EEPQC\,I})$ to send it directly to him/her. $(MI_{EEPQC\,I})$ is the component to insert (i.e., embed according to the steganographic scheme) $(M_{EEPQC\,I})$'s message into another member's (e.g., $(M_{EEPQC\,II})$)'s envelope $(E_{EEPQC\,II})$ when $(M_{EEPQC\,I})$ is sending a secret message $(Mess._{EEPQC\,I})$ to $(M_{EEPQC\,II})$. One important function of $(M_{EEPQC\,I})$ is that it detects a key $(Key_{EEPQC\,II})$ that has been hidden in the envelope $(Key_{EEPQC\,II})$, and uses it when inserting a message $(Mess._{EEPQC\,I})$ in $(E_{EEPQC\,II})$. $(EO_{EEPQC\,I})$ is a component that opens (extracts) $(E_{EEPQC\,I})$'s "message inserted" envelope $(E_{EEPQC\,I}(Mess._{EEPQC\,II}))$ which $(M_{EEPQC\,I})$ received from someone as an e-mail attachment. The sender $(M_{EEPQC\,II})$ of the secret message $(Mess._{EEPQC\,II})$ is not known until $(M_{EEPQC\,I})$ opens the envelope by using $(EO_{EEPQC\,I})$.

4. Customization of a EEPQC

Customization of an EEPQC for member $(M_{EEPQC\,I})$ takes place in the following way. $(M_{EEPQC\,I})$ first decides a key $(Key_{EEPQC\,I})$ when he installs the EEPQC onto his

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
Volume 1 Issue 2 September 2011

computer. Then he types in his name $(Name_{EEPQC\ I})$ and e-mail address $(\text{Email adr}_{EEPQC\ I})$. $(Key_{EEPQC\ I})$ is secretly hidden (according to a steganographic procedure in his envelope $(E_{EEPQC\ I})$ This $(Key_{EEPQC\ I})$ is eventually transferred to a message sender's $(MI_{EEPQC\ II})$ in an invisible way. $(Name_{EEPQC\ I})$ and $(Name\ adr_{EEPQC\ I})$ are printed out on the envelope surface when $(M_{EEPQC\ I})$ produces $(E_{EEPQC\ I})$ by using $(EP_{EEPQC\ I})$. $(Key_{EEPQC\ I})$ is also set to $(EO_{EEPQC\ I})$ at the time of installation. $(Name_{EEPQC\ I})$ and $(Email\ adr_{EEPQC\ I})$ are also inserted (actually, embedded) automatically by $(MI_{EEPQC\ I})$ any time $(M_{EEPQC\ I})$ inserts his message $(Mess._{EEPQC\ I})$ in another member's envelope $(E_{EEPQC\ I})$. The embedded $(Name_{EEPQC\ I})$ and $(Email\ adr_{EEPQC\ I})$ are extracted by a message receiver $(M_{EEPQC\ II})$ by $(EO_{EEPQC\ II})$.

Error Correction Code:

A metric space is a set C with a distance function

$$dist : C \times C \to R^{+} = [0, \infty),$$

which obeys the usual properties (symmetric, triangle inequalities, zero distance between equal points).

4.1. Definition

Let $C\{0,1\}^n$ be a code set which consists of a set of code words c_i of length n. The distance metric between any two code words $c_i \text{ and } c_j$ in C is defined by

$$dist(c_i, c_j) = \sum_{r=1}^{n} \left| c_{ir} - c_{jr} \right|, \qquad c_i, c_j \in C .$$

This is known as Hamming distance [9].

4.2. Definition

An error correction function f for a code C is defined as

$$f(c_j) = \{c_j \mid dist(c_i, c_j) \text{ is the minimum, over } C \setminus \{c_i\}\}.$$

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
Volume 1 Issue 2 September 2011

Here, $c_j = f(c_i)$ is called the nearest neighbor of c_i.

4.3. Definition

The measurement of nearness between two code words c and c' is defined by

$$\text{nearness}(c,c') = \text{dist}(c,c')/n,$$

it is obvious that $0 \le \text{nearness}(c,c') \le 1.$

4.4. Definition

The fuzzy membership function for a codeword c' to be equal to a given c is defined as [10]

$$FUZZ(c') = \begin{cases} 0 & if\ nearness(c,c') = z \le z_0 < 1 \\ z & otherwise \end{cases}$$

5. How it works

When some member $(M_{EEPQC\ II})$ wants to send a secret message $(Mess._{EEPQC\ II})$ to another member $(M_{EEPQC\ I})$, whether they are acquainted or not, $(M_{EEPQC\ II})$ gets (e.g., downloads) the $(M_{EEPQC\ I})$'s envelope $(E_{EEPQC\ I})$, and uses it to insert his message $(Mess._{EEPQC\ II})$ by using $(MI_{EEPQC\ II})$. When $(M_{EEPQC\ II})$ tries to insert a message, $(M_{EEPQC\ I})$'s key $(Key_{EEPQC\ I})$ is transferred to $(MI_{EEPQC\ II})$ automatically in an invisible manner, and is actually used. $(M_{EEPQC\ I})$ can send $(E_{EEPQCI}(M_{EEPQC\ II}))$directly, or ask someone else to send it to $(M_{EEPQC\ I})$as an e-mail attachment. $(M_{EEPQC\ II})$ can be anonymous because no sender's information is seen on $(E_{EEPQC\ I}(M_{EEPQC\ II}))$. $(Mess._{EEPQC\ I})$ is hidden, and only $(M_{EEPQC\ I})$ can see it by opening the envelope. It is not a problem for $(M_{EEPQC\ II})$ and $(M_{EEPQC\ I})$ to be acquainted or not because $(M_{EEPQC\ II})$ can get anyone's envelope from an open site.

Due to the stymieing channel, there is a chance for the occurrence of error. Let $(M_{EEPQC\ I})$ get message $(t(c)_{EEPQC\ II})$ instead of $(c_{EEPQC\ II})$, where t denote the

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
Volume 1 Issue 2 September 2011

transmission error. Now, $(M_{EEPQC\ I})$ apply error correction function on $(t(c)_{EEPQC\ II})$ and gets $(t(c)_{EEPQC\ II})'$.

$(M_{EEPQC\ I})$ check that $dist\{(t(c)_{EEPQC\ II}),t(c)_{EEPQC\ II})'\}>0$, $(M_{EEPQC\ I})$ will realize that there is an error occur during the transmission. $(M_{EEPQC\ I})$ apply the error correction function f to $(c_{EEPQC\ II})' : f((c_{EEPQC\ II})'$.

Then $(M_{EEPQC\ I})$ will compute nearness

$$(t(c_{EEPQC\ II}),f((c_{EEPQC\ II})')) = \frac{dist\{t(c_{EEPQC\ II}),f((c_{EEPQC\ II})')\}}{n}..$$

$$FUZZ((c_{EEPQC\ II})') = \begin{Bmatrix} 0 & if\ nearness\,(c_{EEPQC\ II}),(c_{EEPQC\ II}\ )') = z \le z_0 < 1 \\ z & otherwise \end{Bmatrix}$$

6. Conclusion

EEPQC is a very easy-to-use system because users are not bothered by any key handling, as the key is always operated automatically. As EEPQC doesn't need any authorization bureau, this system can be very low cost. All these features overcome the drawbacks of an encrypted mailing system. Our approach provides the method to remove the error due to stymieing channel through fuzzy approach.

7. References

[1] Stefan Katzenbeisser and Fabien A.P. Petitcolas (eds), "Information hiding techniques for steganography and digital watermarking", Artech House, 2000.

[2] Neil F. Johnson, Zoran Duric and Sushil Jajodia,"Information Hiding", Kluwer Academic Publishers, 2001.

[3] M. Niimi, H. Noda and E. Kawaguchi,"An image embedding in image by a complexity based region segmentation method", Proceedings of International Conf. on Image Processing'97, Vol.3, pp.74-77, Santa Barbara, Oct., 1997.

[4] E. Kawaguchi and R. O. Eason,"Principle and applications of BPCS-Steganography", Proceedings of SPIE: Multimeda Systems and Applications, Vol.3528, pp.464-463, 1998.

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
Volume 1 Issue 2 September 2011

[5] E. Kawaguchi, et al, "A concept of digital picture envelope for Internet communication" in Information modeling and knowledge bases X, IOS Press, pp.343-349, 1999.

[6]Eiji Kawaguchi, Hideki Noda, Michiharu Niimi and Richard O. Eason, "A Model of Anonymous Covert Mailing System Using Steganographic Scheme, Information modelling and knowledge bases X",IOS Press, pp.81-85,2003.

[7] J.P.Pandey, D.B.Ojha, Ajay Sharma, "Enhance Fuzzy Commitment Scheme: An Approach For Post Quantum Cryptosystem", in Journal of Applied and Theoretical Information Technology, (pp 16-19) Vol. 9, No. 1, Nov. 2009.

[8]V.Pless, " Introduction to theory of Error Correcting Codes", Wiley , New York 1982.

[9].A.A.Al-saggaf,H.S.Acharya,"A Fuzzy Commitment Scheme"IEEE International Conference on Advances in Computer Vision and Information Technology 28-30November 2007 – India