International Journal of Mathematical Sciences
Vol. 17, Nos. 3-4, July-December 2018, pp. 347-362

ISSN: 0972-754X

POLLY CRACKER PUBLIC KEY CRYPTOSYSTEM USING GRAPH PARAMETERS

Anooja. I, Vinod. S and Biju. G. S

Abstract: Cryptography is the art of protect information by transforming it to unreadable format called Cipher text. The process of converting plain text to cipher text called encryption, and the process of converting cipher text on its original plain text called decryption. In this paper, we extend a generalization of the original Polly Cracker public key cryptosystem using some graph elements which will be used for data encryption and decryption with higher security.

Keywords: Cryptosystem, clique, edge covering, independent set, private key, public key

2010 AMS subject classifications: 06C20, 94C15

1. INTRODUCTION

Public-key cryptography was pioneered by Diffie and Hellman [1]. Rivest et al. [2] proposed RSA cryptosystem, ElGamal [3] build cryptosystem using the discrete logarithm problem and Koblitz Koblitz [4] constructed public-key cryptosystem using elliptic curves. There has been a lot of on-going research work to find more secure and efficient public key cryptosystems based on algebraic structures such as non-abelian groups, linear groups, semigroups and power series rings (see Anshel et al. [5], Baumslag et al. [6], Maze et al. [7], Shpilrain and Zapata [8]), and where the security is based on hard algorithmic problems from combinatorial group theory.

Fellows and Koblitz [9, 10] describe a conceptual public key cryptosystem called Polly Cracker. In this system, the publickey consists of a finite set of multivariate polynomials with coefficients in some finite field, and the secret key consists of a common zero of these polynomials.

Graphs may be used for the design of stream ciphers, block ciphers or public key ciphers. Graph theory is widely used as a tool of encryption, due to its various properties and its easy representation in computers as a matrix. Yamuna et al. [11] presented an encryption mechanism using Hamilton path properties, they encrypt data twice, once using the Hamilton path, and the second using the complete graph to impose more secure method. Paszkiewicz et al. [12] proposed a method of using paths between a pair of graph vertices and spanning trees for designing effective poly alphabetic substitution ciphers. The period of alphabet changeovers is equal to

the number of paths between a pair of selected vertices on the graph, the number of spanning trees or is a multiple of these values. Various papers based on graph theory applications have been studied and we explore the usage of Graph theory in cryptography has been proposed here.

2. POLLY CRACKER PUBLIC KEY CRYPTOSYSTEM

For a detailed description of Polly Cracker we refer to Fellows and Koblitz [9, 10. Subsequently, we give only a short description of this system which is sufficient for describing our attack.

Consider the rings of polynomials $\mathbb{F}[t_1, t_2, ..., t_n]$ where $\mathbb{F}$ is a finite field. Alice wants to receive messages $m \in \mathbb{F}$ from Bob. Alice's secret key is a random vector $y \in \mathbb{F}^n$ and public key is a set $B = \{q_i\}$ of polynomials which vanish on *y*. To send a message, Bob choose polynomials $\{g_i\} \in \mathbb{F}[t_1, t_2, ..., t_n]$ randomly and generates an element $p = \sum g_j q_j$ of the ideal $J(B)$ and sends the polynomial $c = p + m$ to Alice. The message *m* is found by evaluating $c(y) = p(y) + m = m$.

An edge covering of a graph $G = (V, E)$ is a subset *L* of *E* such that each vertex of *G* is an end of some edges in *L*. A clique of a simple graph *G* is a subset *S* of *V* such that $G[S]$ is complete. Spanning subgraph of *G* is a subgraph *H* with *V*(*H*) = *V*(*G*). A subset *S* of *V* is called a Vertex independent set of *G* if no two vertices of *S* are adjacent in *G*. A subset *L* of *E* is called an Edge independent set of *G* if no two of which are adjacent.

3. POLLY CRACKER PUBLIC KEY CRYPTOSYSTEM BASED ON EDGE COVERING OF A GRAPH

Public Key : Graph *G* and cardinality of edge cover *l*

Private Key : Edge cover E' and a vector y

Working Procedure

Let us consider a non-trivial, finite, connected graph $G = (V, E)$ and $|E| = m$.

Take the edge cover E' of G such that $|E'| = l$.

Now consider the rings of polynomials $\mathbb{F}[X] = \mathbb{F}[x_{e_i} : e_i \in E]$, where $\mathbb{F}$ is a finite field so that the variable set is $\{x_{e_i} : e_i \in E\}$. Here we take the field $\mathbb{F}$ as $\mathbb{F}_2$ and messages as single bits 0 or 1.

Let B be a set of polynomials in the variables $\{x_{e_i} : e_i \in E\} = B(G)$.

Let $X_1 = \begin{cases} \left\{\sum\left(x_{e_i}\right) - 1 : e_i \in E\right\} & \text{if } l \text{ is odd} \\ \left\{\sum\left(x_{e_i}\right) : e_i \in E\right\} & \text{if } l \text{ is even} \end{cases}$

& $X_2 = \left\{\left(1 - x_{e_i}\right)\left(1 - x_{e_j}\right)x_{e_i} : e_i \text{ and } e_j \text{ are adjacent}\right\}$.

Then $B = X_1 \cup X_2 = \left\{P_k\left(x_{e_i}\right)\right\}$.

Define $f : E \to \{0,1\}$ by $f\left(e_i\right) = \begin{cases} 1 & \text{if } e_i \in E' \\ 0 & \text{otherwise} \end{cases}$.

Then $y = \left(f\left(e_1\right), f\left(e_2\right), ..., f\left(e_m\right)\right) \in \mathbb{F}^{m=|E|}$.

Suppose the commander wants to send a message to a soldier.

Soldier's public key: Graph G and l.

Soldier's private key: E' and y.

Encryption

For encrypting the message *m*, the commander chooses polynomials $Q_k \in \mathbb{F}[X]$ randomly. Then the ciphertext polynomial is obtained as

$$C = \sum P_k\, Q_k + m$$

The commander sends this *C* to a soldier.

Decryption

After receiving the ciphertext *C*, Soldier evaluate this *C* at his secret key *y* to obtain the original message, i.e., $C(y) = \left(\sum P_k\, Q_k + m\right)(y) = m$.

Illustration

Suppose the commander wants to send the message *m* to a soldier.

Consider $G = (V, E)$ given in figure 1.

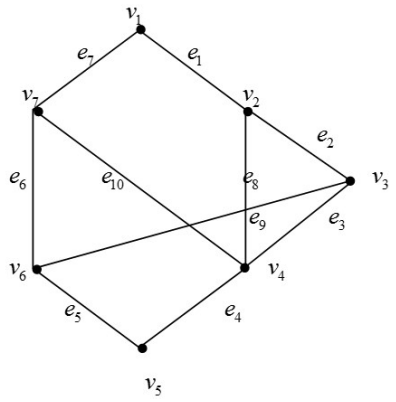

Figure 1: G

Here $E=\{e_1,e_2,e_3,e_4,e_5,e_6,e_7,e_8,e_9,e_{10}\}$ and $|E|=10$.

Take the edge cover $E'=\{e_1,e_3,e_5,e_7\}$ and $|E'|=4$.

Then $f(e_1)=f(e_3)=f(e_5)=f(e_7)=1$,

$f(e_2)=f(e_4)=f(e_6)=f(e_8)=f(e_9)=f(e_{10})=0$

and $y=(1,0,1,0,1,0,1,0,0,0)\in\mathbb{F}^{10}$.

Soldier's public key: Graph G and $|E'|=4$.

Soldier's private key: E' and y.

Let $X_1=\{x_{e_1}+x_{e_2}+x_{e_3}+x_{e_4}+x_{e_5}+x_{e_6}+x_{e_7}+x_{e_8}+x_{e_9}+x_{e_{10}}\}$ since $|E'|$ is even

and

$$X_2=\{(1-x_{e_1})(1-x_{e_2})x_{e_1},(1-x_{e_1})(1-x_{e_7})x_{e_1},(1-x_{e_1})(1-x_{e_8})x_{e_1},(1-x_{e_2})(1-x_{e_3})x_{e_2},$$

$$(1-x_{e_2})(1-x_{e_8})x_{e_2},(1-x_{e_2})(1-x_{e_9})x_{e_2},(1-x_{e_3})(1-x_{e_4})x_{e_3},(1-x_{e_3})(1-x_{e_8})x_{e_3},$$

$$(1-x_{e_3})(1-x_{e_9})x_{e_3},(1-x_{e_3})(1-x_{e_{10}})x_{e_3},(1-x_{e_4})(1-x_{e_5})x_{e_4},(1-x_{e_4})(1-x_{e_8})x_{e_4},$$

$$(1-x_{e_4})(1-x_{e_{10}})x_{e_4},(1-x_{e_5})(1-x_{e_6})x_{e_5},(1-x_{e_5})(1-x_{e_9})x_{e_5},(1-x_{e_6})(1-x_{e_7})x_{e_6},$$

$\left(1-x_{e_6}\right)\left(1-x_{e_9}\right)x_{e_6},\left(1-x_{e_6}\right)\left(1-x_{e_{10}}\right)x_{e_6},\left(1-x_{e_7}\right)\left(1-x_{e_{10}}\right)x_{e_7},\left(1-x_{e_8}\right)\left(1-x_{e_{10}}\right)x_{e_8}\Big\}$

$B=X_1\cup X_2=\left\{P_k\left(x_{e_i}\right)\right\}$.

Let $m=1$ be the message. Then the commander randomly choose $Q_1=x_{e_3}+x_{e_5}+x_{e_7}$, $Q_2=x_{e_1}^2x_{e_2}$ and $Q_3=1-x_{e_8}x_{e_9}$.

Encryption

$$C=\sum P_k\ Q_k+m$$

$$=\left(1-x_{e_3}\right)\left(1-x_{e_8}\right)x_{e_3}\left(x_{e_3}+x_{e_5}+x_{e_7}\right)+\left(1-x_{e_4}\right)\left(1-x_{e_5}\right)x_{v_4}x_{e_1}^2x_{e_2}+$$

$$\left(1-x_{e_1}\right)\left(1-x_{e_8}\right)x_{e_1}\left(1-x_{e_8}x_{e_9}\right)+1$$

$$=x_{e_3}^2-x_{e_3}^3+x_{e_3}^3x_{e_8}+x_{e_3}x_{e_5}-x_{e_3}^2x_{e_5}-x_{e_3}x_{e_5}x_{e_8}+x_{e_3}^2x_{e_5}x_{e_8}+x_{e_3}x_{e_7}-$$

$$x_{e_3}^2x_{e_7}-x_{e_3}x_{e_7}x_{e_8}+x_{e_1}^2x_{e_2}x_{e_4}-x_{e_1}^2x_{e_2}x_{e_4}^2-x_{e_1}^2x_{e_2}x_{e_4}x_{e_5}+x_{e_1}^2x_{e_2}x_{e_4}^2x_{e_5}+x_{e_1}-x_{e_1}^2-$$

$$x_{e_1}x_{e_8}+x_{e_1}^2x_{e_8}-x_{e_1}x_{e_8}x_{e_9}+x_{e_1}^2x_{e_8}x_{e_9}+x_{e_1}x_{e_8}^2x_{e_9}-x_{e_1}^2x_{e_8}^2x_{e_9}+1.$$

Decryption

$C\left(y\right)=C\left(1,0,1,0,1,0,1,0,0,0\right)\ =1=m$.

4. POLLY CRACKER PUBLIC KEY CRYPTOSYSTEM BASED ON CLIQUE OF A GRAPH

Public Key : Graph *G* and cardinality of the clique *k*

Private Key : Clique V' and a vector y

Working Procedure

Let us consider a non-trivial, finite, connected graph $G=\left(V,E\right)$ and $\left|V\right|=n$. Take the clique V' of G such that $\left|V'\right|=k$. Now consider the rings of polynomials $\mathbb{F}\left[X\right]=\mathbb{F}\left[x_{v_i}:v_i\in V\right]$, where $\mathbb{F}$ is a finite field so that the variable set is $\left\{x_{v_i}:v_i\in V\right\}$. Here we take the field $\mathbb{F}$ as $\mathbb{F}_2$ and messages as single bits 0 or 1.

Let B be a set of polynomials in the variables $\left\{x_{v_i} : v_i \in V\right\} = B(G)$.

Let $X_1 = \begin{cases} \left\{\sum\left(x_{v_i}\right) - 1 : v_i \in V\right\} & \text{if} \quad k \quad \text{is} \quad \text{odd} \\ \left\{\sum\left(x_{v_i}\right) : v_i \in V\right\} & \text{if} \quad k \quad \text{is} \quad \text{even} \end{cases}$

and $X_2 = \left\{\left(1 - x_{v_i}\right)\left(1 - x_{v_j}\right)x_{v_i} : \left(v_i, v_j\right) \in E\right\}$.

Then $B = X_1 \cup X_2 = \left\{P_l\left(x_{v_i}\right)\right\}$.

Define $f : V \to \{0,1\}$ by $f\left(v_i\right) = \begin{cases} 1 & \text{if} \quad v_i \in V' \\ 0 & \text{otherwise} \end{cases}$.

Then $y = \left(f\left(v_1\right), f\left(v_2\right), ..., f\left(v_n\right)\right) \in \mathbb{F}^{n=|V|}$.

Suppose the commander wants to send a message to a soldier.

Soldier's public key: Graph G and k.

Soldier's private key: V' and y.

Encryption

For encrypting the message m, the commander chooses polynomials $Q_l \in \mathbb{F}[X]$ randomly. Then the ciphertext polynomial is obtained as

$$C = \sum P_l \; Q_l + m$$

The commander sends this C to a soldier.

Decryption

After receiving the ciphertext C, Soldier evaluate this C at his secret key y to obtain the original message, i.e., $C(y) = \left(\sum P_l \; Q_l + m\right)(y) = m$.

Illustration

Suppose the commander wants to send the message m to a soldier.

Consider $G = (V, E)$ as in figure 2.

Here $V = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$ and $|V| = 7$.

Take the clique $V' = \{v_2, v_3, v_4\}$ and $|V'| = 3$.

Then $f(v_2) = f(v_3) = f(v_4) = 1$, $f(v_1) = f(v_5) = f(v_6) = f(v_7) = 0$

and $y = (0,1,1,1,0,0,0) \in \mathbb{F}^7$.

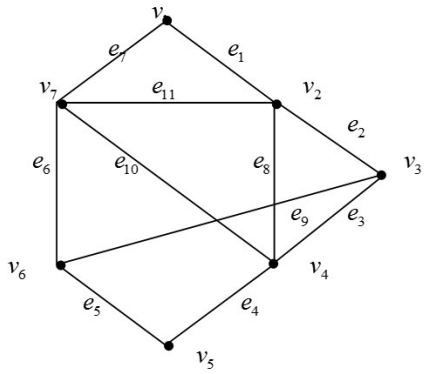

Figure 2 : G

Soldier's public key**:** Graph *G* and $|V'| = 3$.

Soldier's private key**:** V' and y.

Let $X_1 = \{x_{v_1} + x_{v_2} + x_{v_3} + x_{v_4} + x_{v_5} + x_{v_6} + x_{v_7} - 1\}$ since $|V'|$ is odd.

and

$$X_2 = \{(1-x_{v_1})(1-x_{v_2})x_{v_1}, (1-x_{v_2})(1-x_{v_3})x_{v_2}, (1-x_{v_3})(1-x_{v_4})x_{v_3}, (1-x_{v_4})(1-x_{v_5})x_{v_4},$$

$$(1-x_{v_5})(1-x_{v_6})x_{v_5}, (1-x_{v_6})(1-x_{v_7})x_{v_6}, (1-x_{v_7})(1-x_{v_1})x_{v_7}, (1-x_{v_2})(1-x_{v_4})x_{v_2},$$

$$(1-x_{v_3})(1-x_{v_6})x_{v_3}, (1-x_{v_4})(1-x_{v_7})x_{v_4}, (1-x_{v_2})(1-x_{v_7})x_{v_2}\}$$

$B = X_1 \cup X_2 = \{P_l(x_{v_i})\}$.

Let $m = 1$ be the message. Then the commander randomly choose $Q_1 = x_{v_4} + x_{v_6} + x_{v_7}$ and $Q_2 = x_{v_3}^2 + x_{v_5}^3$.

Encryption

$$C = \sum P_l \; Q_l + m$$

$$= \left(1-x_{v_4}\right)\left(1-x_{v_5}\right)x_{v_4}\left(x_{v_4}+x_{v_6}+x_{v_7}\right)+\left(1-x_{v_3}\right)\left(1-x_{v_6}\right)x_{v_3}\left(x_{v_3}^2+x_{v_5}^3\right)+1$$

$$= x_{v_4}^2 - x_{v_4}^3 - x_{v_4}^2 x_{v_5} + x_{v_4}^3 x_{v_5} + x_{v_4} x_{v_6} - x_{v_4}^2 x_{v_6} - x_{v_4} x_{v_5} x_{v_6} + x_{v_4}^2 x_{v_5} x_{v_6} +$$

$$x_{v_4} x_{v_7} - x_{v_4}^2 x_{v_7} - x_{v_4} x_{v_5} x_{v_7} + x_{v_4}^2 x_{v_5} x_{v_7} + x_{v_3}^3 - x_{v_3}^4 - x_{v_3}^3 x_{v_6} + x_{v_3}^4 x_{v_6} +$$

$$x_{v_3} x_{v_5}^3 - x_{v_3}^2 x_{v_5}^3 - x_{v_3} x_{v_5}^3 x_{v_6} + x_{v_3}^2 x_{v_5}^3 x_{v_6} + 1.$$

Decryption

$C(y) = C(0,1,1,1,0,0,0) \quad = 1 = m$.

5. POLLY CRACKER PUBLIC KEY CRYPTOSYSTEM BASED VERTEX INDEPENDENT SET OF A GRAPH

Let us consider a non-trivial, finite, connected graph $G = (V, E)$ and $|V| = n$.

Take the vertex independent set V' of G such that $|V'| = k$.

Now consider the rings of polynomials $\mathbb{F}[X] = \mathbb{F}[x_v : v \in V]$, where $\mathbb{F}$ is a finite field so that the variable set is $\{x_v : v \in V\}$. Here we take $\mathbb{F}$ as $\mathbb{F}_2$ and messages as single bits 0 or 1.

Let B be a set of polynomials in the variables $\{x_v : v \in V\} = B(G)$.

Let $B_1 = \begin{cases} \{\sum(x_v) - 1 : v \in V\} & \textit{if} \quad k \quad \textit{is} \quad \textit{odd} \\ \{\sum(x_v) : v \in V\} & \textit{if} \quad k \quad \textit{is} \quad \textit{even} \end{cases}$

and $B_2 = \{x_u x_v : (u,v) \in E\}$.

Then $B = B_1 \cup B_2 = \{f_i\}$.

Define $y_v : V \to \{0,1\}$ by $y_v = \begin{cases} 1 & \textit{if} \quad v \in V' \\ 0 & \textit{otherwise} \end{cases}$.

Then $y = (y_{v_1}, y_{v_2}, ..., y_{v_n}) \in \mathbb{F}^{n=|V|}$.

Suppose Bob wants to send a message to Alice.

Alice's public key: Graph G and k.

Alice's private key: V' and y.

Encryption

For encrypting the message *m*, Bob choose polynomials $g_i \in \mathbb{F}[X]$ randomly. Then the ciphertext polynomial is obtained as

$$c = \sum f_i g_i + m$$

Bob sends this *c* to Alice.

Decryption

After receiving the ciphertext *c*, Alice evaluate this *c* at her secret key *y* to obtain the original message, i.e., $c(y) = \left(\sum f_i g_i + m\right)(y) = m$.

Illustration

Suppose Bob wants to send the message m to Alice.

Consider $G = (V, E)$ given in figure 1.

Here $V = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$ and $|V| = 7$.

Take the vertex independent set $V' = \{v_1, v_4, v_6\}$ and $|V'| = 3$.

Then $y_{v_1} = y_{v_4} = y_{v_6} = 1$, $y_{v_2} = y_{v_3} = y_{v_5} = y_{v_7} = 0$ and $y = (1,0,0,1,0,1,0) \in \mathbb{F}^7$.

Alice's public key: Graph G and $|V'| = 3$.

Alice's private key: V' *and* y.

Let $B_1 = \left\{x_{v_1} + x_{v_2} + x_{v_3} + x_{v_4} + x_{v_5} + x_{v_6} + x_{v_7} - 1\right\}$ since $|V'|$ is odd.

and $B_2 = \left\{x_{v_1}x_{v_2}, x_{v_2}x_{v_3}, x_{v_3}x_{v_4}, x_{v_4}x_{v_5}, x_{v_5}x_{v_6}, x_{v_6}x_{v_7}, x_{v_7}x_{v_1}, x_{v_2}x_{v_4}, x_{v_3}x_{v_6}, x_{v_4}x_{v_7}\right\}$.

$B = B_1 \cup B_2 = \{f_i\}$.

Let $m = 1$ be the message. Then Bob randomly choose $g_1 = x_{v_3}x_{v_5}$, $g_2 = x_{v_3}^3$ and $g_3 = x_{v_4} + x_{v_7}$.

Encryption

$$c = \sum f_i g_i + m$$

$$= x_{v_2} x_{v_3} x_{v_3} x_{v_5} + x_{v_6} x_{v_7} x_{v_3}^3 + \left(x_{v_1} + x_{v_2} + x_{v_3} + x_{v_4} + x_{v_5} + x_{v_6} + x_{v_7} - 1 \right)\left(x_{v_4} + x_{v_7} \right) + 1$$

$$= x_{v_2} x_{v_3}^2 x_{v_5} + x_{v_3}^3 x_{v_6} x_{v_7} + x_{v_1} x_{v_4} + x_{v_2} x_{v_4} + x_{v_3} x_{v_4} + x_{v_4}^2 + x_{v_4} x_{v_5} + x_{v_4} x_{v_6} + x_{v_4} x_{v_7} - x_{v_4} +$$

$$x_{v_1} x_{v_7} + x_{v_2} x_{v_7} + x_{v_3} x_{v_7} + x_{v_4} x_{v_7} + x_{v_5} x_{v_7} + x_{v_6} x_{v_7} + x_{v_7}^2 - x_{v_7} + 1 .$$

Decryption

$c(y) = c(1,0,0,1,0,1,0) = 1 = m$.

6. POLLY CRACKER PUBLIC KEY CRYPTOSYSTEM BASED ON EDGE INDEPENDENT SET OF A GRAPH

Let us consider a non-trivial, finite, connected graph $G = (V, E)$ and $|E| = m$.

Take the edge independent set E' of G such that $|E'| = l$.

Now consider the rings of polynomials $\mathbb{F}[X] = \mathbb{F}[x_e : e \in E]$, where $\mathbb{F}$ is a finite field so that the variable set is $\{x_e : e \in E\}$. Here we take the field $\mathbb{F}$ as $\mathbb{F}_2$ and messages as single bits 0 or 1.

Let B be a set of polynomials in the variables $\{x_e : e \in E\} = B(G)$.

Let $B_1 = \begin{cases} \left\{ \sum (x_e) - 1 : e \in E \right\} & \text{if } l \text{ is odd} \\ \left\{ \sum (x_e) : e \in E \right\} & \text{if } l \text{ is even} \end{cases}$

and $B_2 = \left\{ x_{e_1} x_{e_2} : e_1 \text{ and } e_2 \text{ are adjacent} \right\}$.

Then $B = B_1 \cup B_2 = \{ f_i \}$.

Define $y_e : E \to \{0,1\}$ by $y_e = \begin{cases} 1 & \text{if } e \in E' \\ 0 & \text{otherwise} \end{cases}$.

Then $y = \left(y_{e_1}, y_{e_2}, ..., y_{e_m} \right) \in \mathbb{F}^{m=|E|}$.

Suppose Bob wants to send a message to Alice.

Alice's public key: Graph G and l.

Alice's private key: E' and y.

Encryption

For encrypting the message *m*, Bob choose polynomials $g_i \in \mathbb{F}[X]$ randomly. Then the ciphertext polynomial is obtained as

$$c = \sum f_i g_i + m$$

Bob sends this *c* to Alice.

Decryption

After receiving the ciphertext *c*, Alice evaluate this *c* at her secret key *y* to obtain the original message, i.e., $c(y) = \left(\sum f_i g_i + m\right)(y) = m$.

Illustration

Suppose Bob wants to send the message *m* to Alice.

Consider $G = (V, E)$ given in figure 1.

Here $E = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9, e_{10}\}$ and $|E| = 10$.

Take the edge independent set $E' = \{e_1, e_3, e_5\}$ and $|E'| = 3$.

Then $y_{e_1} = y_{e_3} = y_{e_5} = 1$, $y_{e_2} = y_{e_4} = y_{e_6} = y_{e_7} = y_{e_8} = y_{e_9} = y_{e_{10}} = 0$

and $y = (1,0,1,0,1,0,0,0,0,0) \in \mathbb{F}^{10}$.

Alice's public key**:** Graph G and $|E'| = 3$.

Alice's private key**:** E' *and* y.

Let $B_1 = \left\{x_{e_1} + x_{e_2} + x_{e_3} + x_{e_4} + x_{e_5} + x_{e_6} + x_{e_7} + x_{e_8} + x_{e_9} + x_{e_{10}} - 1\right\}$ since $|E'|$ is odd.

and $B_2 = \{x_{e_1}x_{e_2}, x_{e_1}x_{e_7}, x_{e_1}x_{e_8}, x_{e_2}x_{e_3}, x_{e_2}x_{e_8}, x_{e_2}x_{e_9}, x_{e_3}x_{e_4}, x_{e_3}x_{e_8}, x_{e_3}x_{e_9}, x_{e_3}x_{e_{10}},$

$$x_{e_4}x_{e_5}, x_{e_4}x_{e_8}, x_{e_4}x_{e_{10}}, x_{e_5}x_{e_6}, x_{e_5}x_{e_9}, x_{e_6}x_{e_7}, x_{e_6}x_{e_9}, x_{e_6}x_{e_{10}}, x_{e_7}x_{e_{10}}, x_{e_8}x_{e_{10}}\}$$

$$B = B_1 \cup B_2 = \{f_i\}.$$

Let $m = 1$ be the message. Then Bob randomly choose $g_1 = x_{e_2}x_{e_3}^2$, $g_2 = x_{e_1} - x_{e_5}$ and $g_3 = 1 - x_{e_{10}}$.

Encryption

$$c = \sum f_i g_i + m$$

$$= \left(x_{e_1} + x_{e_2} + x_{e_3} + x_{e_4} + x_{e_5} + x_{e_6} + x_{e_7} + x_{e_8} + x_{e_9} + x_{e_{10}} - 1 \right) x_{e_2} x_{e_3}^2 +$$

$$x_{e_5} x_{e_6} \left(x_{e_1} - x_{e_5} \right) + x_{v_6} x_{e_9} \left(1 - x_{e_{10}} \right) + 1$$

$$= x_{e_1} x_{e_2} x_{e_3}^2 + x_{e_2}^2 x_{e_3}^2 + x_{e_2} x_{e_3}^3 + x_{e_2} x_{e_3}^2 x_{e_4} + x_{e_2} x_{e_3}^2 x_{e_5} + x_{e_2} x_{e_3}^2 x_{e_6} + x_{e_2} x_{e_3}^2 x_{e_7} + x_{e_2} x_{e_3}^2 x_{e_8} +$$

$$x_{e_2} x_{e_3}^2 x_{e_9} + x_{e_2} x_{e_3}^2 x_{e_{10}} - x_{e_2} x_{e_3}^2 + x_{e_1} x_{e_5} x_{e_6} - x_{e_3}^2 x_{e_6} + x_{e_6} x_{e_9} - x_{e_6} x_{e_9} x_{e_{10}} + 1.$$

Decryption

$c(y) = c(1,0,1,0,1,0,0,0,0,0) = 1 = m$.

7. POLLY CRACKER PUBLIC KEY CRYPTOSYSTEM BASED ON SPANNING SUBGRAPH OF A GRAPH

Let us consider a non-trivial, finite, connected graph $G = (V, E)$ and $|V| = n$. Take the spanning subgraph $H = (V, E_1)$ of G and $U = \{v : v$ is an end vertices of $e \in E_1\}$ such that $|U| = k$.

Now consider the rings of polynomials $\mathbb{F}[X] = \mathbb{F}[x_v : v \in V]$, where $\mathbb{F}$ is a finite field so that the variable set is $\{x_v : v \in V\}$. Here we take the field $\mathbb{F}$ as $\mathbb{F}_2$ and messages as single bits 0 or 1.

Let B be a set of polynomials in the variables $\{x_v : v \in V\} = B(G)$.

Let $B_1 = \begin{cases} \left\{ \sum (x_v) - 1 : v \in V \right\} & \text{if } k \text{ is odd} \\ \left\{ \sum (x_v) : v \in V \right\} & \text{if } k \text{ is even} \end{cases}$

and $B_2 = \left\{ (1 - x_u)(1 - x_v) x_u : (u, v) \in E \right\}$.

Then $B = B_1 \cup B_2 = \{ f_i \}$.

Define $y_v : V \to \{0,1\}$ by $y_v = \begin{cases} 1 & \text{if } v \in U \\ 0 & \text{otherwise} \end{cases}$.

Then $y = \left(y_{v_1}, y_{v_2}, ..., y_{v_n} \right) \in \mathbb{F}^{n=|V|}$.

Suppose Bob wants to send a message to Alice.

Alice's public key: Graph G and k.

Alice's private key: H and y.

Encryption

For encrypting the message m, Bob choose polynomials $g_i \in \mathbb{F}[X]$ randomly. Then the ciphertext polynomial is obtained as

$$c = \sum f_i g_i + m$$

Bob sends this c to Alice.

Decryption

After receiving the ciphertext c, Alice evaluate this c at her secret key y to obtain the original message, i.e., $c(y) = \left(\sum f_i g_i + m\right)(y) = m$.

Illustration

Suppose Bob wants to send the message m to Alice.

Consider $G = (V, E)$ as in figure 1.

Here $V = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$ and $|V| = 7$.

Consider the spanning subgraph $H = (V, E_1)$ of the graph G given in figure 3.

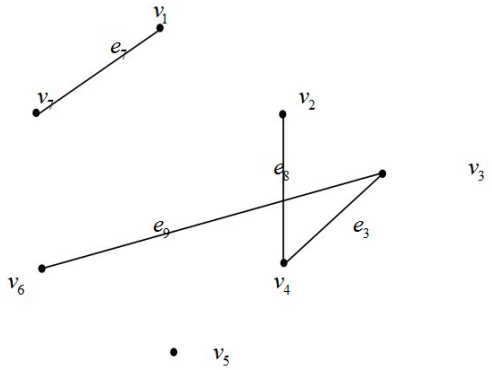

Figure 3: *H*

$U = \{v_1, v_2, v_3, v_4, v_6, v_7\}$ and $|U| = 6$.

Then $y_{v_1} = y_{v_2} = y_{v_3} = y_{v_4} = y_{v_6} = y_{v_7} = 1$, $y_{v_5} = 0$ and $y = (1,1,1,1,0,1,1) \in \mathbb{F}^7$.

Alice's public key: Graph G and $|U| = 6$.

Alice's private key: H *and* y.

Let $B_1 = \{x_{v_1} + x_{v_2} + x_{v_3} + x_{v_4} + x_{v_5} + x_{v_6} + x_{v_7}\}$ since $|U|$ is even.

a n d

$$B_2 = \{(1-x_{v_1})(1-x_{v_2})x_{v_1}, (1-x_{v_2})(1-x_{v_3})x_{v_2}, (1-x_{v_3})(1-x_{v_4})x_{v_3}, (1-x_{v_4})(1-x_{v_5})x_{v_4},$$
$$(1-x_{v_5})(1-x_{v_6})x_{v_5}, (1-x_{v_6})(1-x_{v_7})x_{v_6}, (1-x_{v_7})(1-x_{v_1})x_{v_7}, (1-x_{v_2})(1-x_{v_4})x_{v_2},$$

$$(1-x_{v_3})(1-x_{v_6})x_{v_3}, (1-x_{v_4})(1-x_{v_7})x_{v_4}\}.$$

$B = B_1 \cup B_2 = \{f_i\}$.

Let $m = 1$ be the message. Then Bob randomly choose $g_1 = x_{v_2} + x_{v_7}$ and $g_2 = x_{v_1} x_{v_3} x_{v_5}$.

Encryption

$$c = \sum f_i g_i + m$$
$$= (1-x_{v_3})(1-x_{v_4})x_{v_3}(x_{v_2} + x_{v_7}) + (1-x_{v_7})(1-x_{v_1})x_{v_7}x_{v_1}x_{v_3}x_{v_5} + 1$$
$$= x_{v_2}x_{v_3} - x_{v_2}x_{v_3}^2 - x_{v_2}x_{v_3}x_{v_4} + x_{v_2}x_{v_3}^2x_{v_4} + x_{v_3}x_{v_7} - x_{v_3}^2x_{v_7} - x_{v_3}x_{v_4}x_{v_7}$$
$$- x_{v_3}^2x_{v_4}x_{v_7} + x_{v_1}x_{v_3}x_{v_5}x_{v_7} - x_{v_1}^2x_{v_3}x_{v_5}x_{v_7} - x_{v_1}x_{v_3}x_{v_5}x_{v_7}^2 + x_{v_1}^2x_{v_3}x_{v_5}x_{v_7}^2 + 1.$$

Decryption

$c(y) = c(1,1,1,1,0,1,1) = 1 = m$.

8. CONCLUSION

The cryptosystsem presented for data security system furnishes very promising results. We have generalized an existing cryptosystem using certain graph elements which will be used for data encryption and decryption with higher security.

REFERENCES

[1] Whitfield Diffie and Martin Hellman, *New directions in cryptography*, IEEE transactions on Information Theory, 22(6):644–654, 1976.

[2] Ronald L Rivest, Adi Shamir, and Leonard Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, 21(2):120–126, 1978.

[3] Taher ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE transactions on information theory, 31(4):469–472, 1985.

[4] Neal Koblit, *Elliptic curve cryptosystems*, Mathematics of computation, 48(177): 203–209, 1987.

[5] Iris Anshel, Michael Anshel, and Dorian Goldfeld, *An algebraic method for public key cryptograph*, Mathematical Research Letters, 6(3–4):287–291, 1999.

[6] Gilbert Baumslag, Benjamin Fine, and Xiaowei Xu, *Cryptosystems using linear groups*, Applicable Algebra in Engineering, Communication and Computing, 17(3):205–217, 2006.

[7] Gerard Maze, Chris Monico, and Joachim Rosenthal, *Public key cryptography based on semigroup actions*, Advances of Mathematics of Communications, 1(4):489–507, 2007

[8] Vladimir Shpilrain and Gabriel Zapata, *Combinatorial group theory and public key cryptography*, Applicable Algebra in Engineering, Communication and Computing, 17(3):291–302, 2006.

[9] Michael Fellows and Neal Koblit, *Combinatorial cryptosystems galore*! Finite Fields: Theory, Applications, and Algorithms, G. L. Mullen and P. J.-S. Shiue, Eds. Providence, RI: Amer. Math. Soc., Comtemporary Mathematics,168:51- 61, 1994.

[10] Neal Koblitz. Algebraic aspects of cryptography, *Algorithms and Computation in Mathematics*, With an appendix on hyper elliptic curves by A. J. Menezes, Y.-H.Wu, and R. J. Zuccherato. Berlin, Heidelberg, Germany: Springer-Verlag, 3: 51–61, 1998.

[11] M Yamuna, Meenal Gogia, Ashish Sikka, and Md Jazib Hayat Khan, *Encryption using graph theory and linear algebra,*. International Journal of Computer Application, 5(2):102–107, 2012.

[12] Andrzej Paszkiewicz, Anna G´orska, Karol G´orski, Zbigniew Kotulski, Kamil Kulesza, and Janusz Szczepa´nski, *Proposals of graph based ciphers, theory and implementations.*, In Proceedings of the Regional Conference on Military Communication and Information Systems. CIS Solutions for an Enlarged NATO, RCMIS, 2001.

Anooja. I
Department of Mathematics,
CMS College Kottayam (Autonomous),
Kottayam, Kerala, India

Vinod. S
Department of Mathematics,
Government College for Women,
Thiruvananthapuram, Kerala, India

Biju. G. S
Department of Mathematics,
College of Engineering,
Thiruvananthapuram, Kerala, India