International Journal of Combinatorial Graph Theory and Applications
Vol. 4, No. 2, (July- December, 2019)

ON THE CONSTRUCTION OF POLLY CRACKER PUBLIC KEY CRYPTOSYSTEMS BASED ON MARKED GRAPHS

K. Thirusangu, R. Rajeswari & K. Balasangu

RECEIVED: December 04,2017. Revised March 08, 2018

Abstract: In this note, we construct certain special cases of Polly Cracker Public Key Cryptosystems on the domain of marked graphs.

2000 Mathematics Subject Classification: 68Q85,94A60.

Keywords: Public Key Cryptosystems, Marked Graphs, Siphon, Trap

1. INTRODUCTION

From ancient times, people have used Cryptography, especialy to send secret messages in coded form during war communications. Since the seventies, there has been a lot of interest in the construction of Public Key Cryptosystems (PKC) ever since the idea was introduced by Diffie and Hellman [1]. In 1995, Koblitz proposed a general Public Key Cryptosystems called Polly Cracker, which is combinatorial and algebraic in nature [3].

Petri nets are one of the most popular models for the representation and analysis of parallel processes. It has a wide range of applications including information systems, operation systems, databases, communication protocols, computer hardware architectures, security systems, manufacturing systems, defence command and control, business processes, banking systems, chemical processes, nuclear waste systems and telecommunications [4].

This can be represented as a particular kind of bipartite graph consisting of two kinds of nodes called places and transitions. Directed arcs are used to connect places to transitions (output of places) and to connect transitions to places (input of places) [5]. One of the subclass of Petri nets namely marked graphs has been defined as an ordinary Petri net in which each place has exactly one input transition and one output transition. The study of structural properties and behavioral properties for marked graphs has been made utilizing siphons and traps [6]. A nonempty subset of places J is called a siphon if every transition having an output place in J has an input place in J. A nonempty subset of places Q is called a trap if every transition having an input place in Q has an output place in Q [7].

In this paper, we construct certain special cases of Polly Cracker Public Key Cryptosystems on the domain of marked graphs namely, (i). The subset of places of a marked graph which is both siphon and trap whose input transitions equal to output transitions and both of them equal the set of all transitions of a marked graph (ii) The subset of places of a marked graph whose removal makes the resulting marked graph not to have subsets which are both siphon and trap [2].

2. PRELIMINARIES

In this section, we present some basic definitions relevant to this paper:

Definition 2.1: A Petri net is a triple $N = (P, T, F)$ where P is a finite set of places, T is a finite set of transitions, such that

(i) $P \cup T \neq \phi$

(ii) $P \cap T = \phi$

(iii) $F \subseteq (P \times T) \cup (T \times P)$ is a set of directed arcs.

Definition 2.2: For all $p \in P$,

$$^{\bullet}p = \{t \in T \mid (t, p) \in F\}, \quad p^{\bullet} = \{t \in T \mid (p, t) \in F\}$$

are the pre and post sets of p respectively. Similarly, For all $t \in T$,

$$^{\bullet}t = \{p \in P \mid (p, t) \in F\}, \quad t^{\bullet} = \{p \in P \mid (t, p) \in F\}$$

are the pre and post sets of t respectively.

Definition 2.3: A Petri net is said to be a marked graph if $|^{\bullet}p| = |p^{\bullet}| = 1$ for all $p \in P$.

Definition 2.4: A non empty subset of places J in a marked graph is called a siphon if $^{\bullet}J \subseteq J^{\bullet}$. That is every transition having an output place in J has an input place in J.

Definition 2.5: A nonempty subset of places Q in a marked graph is called a trap if $Q^{\bullet} \subseteq {}^{\bullet}Q$. That is every transition having an input place in Q has an output place in Q.

Definition 2.6: A non empty subset Z of places in a marked graph is said to be both siphon and trap if $^{\bullet}Z = Z^{\bullet}$. That is, every transition having an input place in Z has an output place in Z and vice versa.

Definition 2.7: A Polly Cracker Public Key Cryptosystem is described as follows:

- K is a finite field.
- $X = \{x_i\}$ is a set of variables.
- Alice wants to be able to receive a message $\alpha \in K$ from Bob.

- Her Private Key is a random vector $Y \in K^n$.
- Her Public Key is a set of polynomials $F = \{q_j\}$ which vanish on Y.
- To send a message α, Bob generates an element $\beta = g_i q_j$ of the ideal $I(F)$ and sends her the Ciphertext polynomial $C = \alpha + \beta$.
- Alice finds α by evaluating the Ciphertext polynomial C on Y as $C(Y) = \beta(Y) + \alpha = \alpha$.

In this note, for convenience, we take the field K as K_2 and messages as single bits either 0 or 1.

3. MAIN RESULT

In this section, we construct certain special cases of Polly Cracker Public Key Cryptosystems on the subsets of places of marked graphs.

Theorem 3.1: There exists a *PKC* on a marked graph $N = (P, T, I, O)$, where the place set P of N has a subset W, which is both siphon and trap whose input transitions equal to output transitions and both of them equal the set of all transitions T of N.

Proof: Suppose K be a finite field and let the given marked graph has m places and n transitions, namely, $P = \{p_1, p_2, ..., p_m\}$ and $T = \{t_1, t_2, ..., t_n\}$. Let $X = \{x_i \mid 1 \leq i \leq m\}$ be a set of variables corresponding to the places in the place set P of N. Assume that the set W has r elements. Then $r \leq m$. Let us construct a private key Y as a random vector over K^m such that the i^{th} component of Y, $y_i = 1$ if the place $p_i \in W$ and $y_i = 0$ if the place $p_i \notin W$. Let $F(N)$ denote a basis of polynomials in the variables $\{x_i\}$. To construct a Public Key let us define

$$F_1 = \sum_{i}^{m} x_i \ \text{if } m \text{ is even} \quad \text{and} \quad F_1 = \left(\sum_{i}^{m} x_i\right) - 1 \ \text{if } m \text{ is odd}$$

Denote the polynomial in F_1 as $f_1'(x)$.

For all $t_s \in T$ define,

$$F_2 = \left\{ f_s(x) \mid f_s(x) = \prod_{x_i \in {}^{\bullet}t_s} (1 - x_i) \prod_{x_j \in t_s^{\bullet}} (1 - x_j) \right\}$$

Let $F(N) = F_1 \cup F_2$. This $F(N)$ will be served as a Public Key of the required *PKC* system. To encript the message define a set of polynomials $G = \{g_j(x_i)\}$, for $j \geq 1$. The Ciphertext polynomial is obtained by

$$C = \sum_{i,\, j=1}^{n} f_i(x)\, g_j(x) + \alpha + f_1'(x)\, g_j(x)$$

Since $f_1'(x)$ and $f_i(x)$ for $i = 1, 2, ..., n$, vanish on Y, we will get α at decription. Hence the theorem. □

Note 1: In [6], the problem of obtaining the set W satisfing the requirement of the above theorem was transformed as the problem of obtaining a directed Hamiltonion circuit in a digraph, which is a NP-COMPLETE problem. So, breaking the private key is difficult even though the Public Key is known to the public and hence the constructed *PKC* is a secured one.

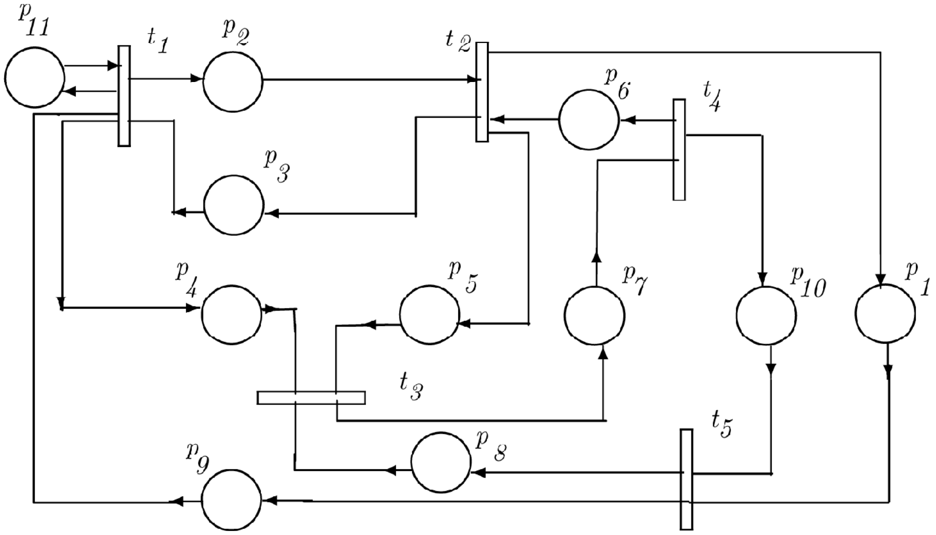

Figure 1: Marked Fraph

Example 3.1: Consider the marked graph shown in Fig. 1.

This marked graph has 11 places and 5 transitions. Clearly the set $W = \{p_1, p_4, p_6, p_7, p_9\}$ satisfies the requirement of the theorem. For convenience let us take the field K as K_2 and messages as single bits either 0 or 1.

Private Key: Define $Y = (y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11}) \in K_2^{(11)}$. Define $y_i = 1$ if $p_i \in W$ and 0 otherwise. Hence, $Y = (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$ and $r = 5$ which is an odd number.

Public Key: The marked graph N and the basis $F = F_1 \cup F_2$, where

$$F_1 = x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_{10} + x_{11} - 1.$$

$$F_2 = \{f_1(x), f_2(x), f_3(x), f_4(x), f_5(x)\} \text{ where}$$

$$f_1(\mathrm{x}) = (1 + x_{11})(1 + x_2)(1 + x_4)(1 - x_3)(1 - x_9)(1 - x_{11})$$

$$f_2(x) = (1 + x_3)(1 + x_5)(1 + x_1)(1 - x_2)(1 - x_6)$$

$$f_3(x) = (1 + x_7)(1 - x_4)(1 - x_5)(1 - x_8)$$

$$f_4(x) = (1 + x_{10})(1 + x_6)(1 - x_7)$$

$$f_5(x) = (1 + x_8)(1 + x_9)(1 - x_1)(1 - x_{10})$$

Encryption: Let $\alpha = 1$.

$$G = \{g_1(x), g_2(x), g_3(x), g_4(x), g_5(x)\} \text{ where}$$

$$g_1(x) = x_1^5 + x_1^4 - x_2^3 + x_3^2 - x^4$$

$$g_2(x) = x_1^5 x_2^3 - x_1^4 x_5^3 x_4^3 - x_3^2 x_2^3 x_1^2 + x_3^2 + x^4$$

$$g_3(x) = x_1^5 + x_1^4 x_2^5 - x_1^4 x_4^2 x_2^3 + x_3^6 x_1^2 - x_5^4 x_4^3 x_5^2$$

$$g_4(x) = x_1^2 x_3^5 + x_2^3 x_3^4 + x_4^2 x_5^3 x_3^5 - x_2^6 x_5^2 + x_2^3 x_5^2$$

$$g_5(x) = x_4^5 x_2^3 - x_1^4 x_3^3 x_4^3 - x_1^2 x_2^3 x_5^2 + x_5^2 x_2^3 + x_4^3 x_2^2$$

The Ciphertext polynomial is:

$$\begin{aligned} C(x) = 1 &+ [x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_{10} + x_{11} - 1] \\ &[x_1^5 + x_1^4 x_2^5 - x_1^4 x_4^2 x_2^3 + x_3^6 x_1^2 - x_5^4 x_4^3 x_5^2] + [(1 + x_{11})(1 + x_2)(1 + x_4) \\ &(1 - x_3)(1 - x_9)(1 - x_{11})] [x_1^5 + x_1^4 - x_2^3 + x_3^2 - x_4] + [x_1^5 x_2^3 - x_1^4 x_5^3 x_4^3 \\ &- x_3^2 x_2^3 x_1^2 + x_3^2 + x_4] [(1 + x_3)(1 + x_5)(1 + x_1)(1 - x_2)(1 - x_6)] \\ &- [(1 + x_7)(1 - x_4)(1 - x_5)(1 - x_8)] [x_1^5 + x_1^4 x_2^5 - x_1^4 x_4^2 x_2^3 + x_3^6 x_1^2 \\ &- x_5^4 x_4^3 x_5^2] + [x_1^2 x_3^5 + x_2^3 x_3^4 + x_4^2 x_5^3 x_3^5 - x^6{}_2 x^2{}_5 + x^3{}_2 x^2{}_5] [(1 + x_{10})(1 + x_6) \\ &(1 - x_7)] - [(1 + x_8)(1 + x_9)(1 - x_1)(1 - x_{10})] [x_4^5 x_2^3 - x_1^4 x_3^3 x_4^3 - x_1^2 x_2^3 x_5^2 \\ &+ x_5^2 x_2^3 + x_4^3 x_2^2]. \end{aligned}$$

Decryption: α will be found by evaluating the polynomial $C(x)$ at $Y = (1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$. This yields $\alpha = 1$.

Theorem 3.2: There exist a *PKC* on a marked graph $N = (P, T, I, O)$, where the place set P of N has a subset W, whose removal makes the resulting marked graph N' not to have subsets which are both siphon and trap.

Proof: Let us take the sets K, P, T and X as in the previous theorem. Take $r = |P| - |W|$. Then $r \leq m$. Let us construct a private key Y as a random vector over K^m such that the i^{th} component of Y, $y_i = 1$ if the place $p_i \notin W$ and $y_i = 0$ if the place $p_i \in W$. Let $F(N)$ denote a basis of polynomials in the variables $\{x_i \mid 1 \leq i \leq m\}$. To construct a Public Key let us define,

$$F_1 = \left(\sum_i^m x_i\right) - 1 \text{ if } m \text{ is odd} \quad \text{and} \quad F_1 = \sum_i^m x_i \text{ if } m \text{ is even,}$$

Denote the polynomial in F_1 as $f_1'(x)$.

For all $t_s \in T$ define ,

$$f_s(x) = \left\{\sum_{i,j} (1 - x_i)(1 - x_j) + \sum_i x_i^2\right\}$$

where the first part of the above $f_s(x)$ is $\forall (p_i, p_j)_{(i \neq j)} \in {}^\bullet t_s \times t_s^\bullet$ and the second part of the above $f_s(x)$ is $\forall p_i \in {}^\bullet t_s \cap t_s^\bullet$

Let $F_2 = \{f_s(x)\}, \forall t_s \in T$

Let $F(N) = F_1 \cup F_2$. This $F(N)$ will act as a Public Key of the required *PKC* system. To encript the message define a set of polynomials $G = \{g_j(x_i)\}$, for $j \geq 1$. The Ciphertext polynomial is obtained by

$$C = \sum_{i,j=1}^{n} f_i(x)\, g_j(x) + \alpha + f_1'(x)\, g_j(x)$$

Since $f_1'(x)$ and $f_i(x)$ for $i = 1, 2, ..., n$, vanish on Y, we will get α at decription. Hence the theorem.

Proof: *Note 2:* In [5], the problem of obtaining the set W satisfing the requirement of the above theorem was transformed as the problem of obtaining a minimal feed back set in a digraph, which is a NP-COMPLETE problem.

So, breaking the private key is difficult even though the Public Key is known to the public and hence this *PKC* is also a secured one.

Example 3.2: Consider the marked graph shown in Fig. 1.

Here $m = 11$ and $n = 5$. Clearly the set $W = \{p_2, p_7, p_{11}\}$ satisfies the requirement of this theorem. Here also, for convenience let us take the field K as K_2 and messages as single bits either 0 or 1.

Private Key: Let $Y = (y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11}) \in K_2^{(11)}$. Define $y_i = 1$ if $p_i \notin W$ and 0 otherwise. Hence, $Y = (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$ and $r = 8$ which is an even number.

Public Key: The marked graph N and the basis $F = F_1 \cup F_2$, where

$$F_1 = x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_{10} + x_{11}.$$

$$F_2 = \{f_1(x), f_2(x), f_3(x), f_4(x), f_5(x)\} \text{ where}$$

$$\begin{aligned}
f_1(x) &= (1-x_{11})(1-x_4) + (1-x_3)(1-x_4) + (1-x_9)(1-x_4) \\
&\quad + (1-x_{11})(1-x_3) + (1-x_{11})(1-x_9) + (1-x_{11})(1-x_2) \\
&\quad + (1-x_3)(1-x_2) + (1-x_9)(1-x_2) + x_{11}^2 \\
f_2(x) &= (1-x_2)(1-x_3) + (1-x_1)(1-x_2) + (1-x_6)(1-x_3) \\
&\quad + (1-x_1)(1-x_6) + (1-x_2)(1-x_5) + (1-x_6)(1-x_5) \\
f_3(x) &= (1-x_5)(1-x_7) + (1-x_4)(1-x_7) + (1-x_8)(1-x_7) \\
f_4(x) &= (1-x_7)(1-x_6) + (1-x_{10})(1-x_7) \\
f_5(x) &= (1-x_1)(1-x_8)+(1-x_{10})(1-x_8)+(1-x_1)(1-x_9)+(1-x_{10})(1-x_9)
\end{aligned}$$

Encryption: Let $\alpha = 1$.

$$G = \{g_1(x), g_2(x), g_3(x), g_4(x), g_5(x)\} \text{ where}$$

$$\begin{aligned}
g_1(x) &= x_{10}^5 x_4^8 + x_{11}^4 x_3^6 - x_9^3 + x_5^2 x_2^7 - x_4^9 - x_9^8 x_6^3 x_7^5 \\
g_2(x) &= x_9^5 x_3^6 - x_1^7 x_2^7 x_9^4 - x_8^4 x_6^5 x_1^3 + x_3^8 + x_2^6 \\
g_3(x) &= x_{11}^8 + x_{10}^{14} x_4^5 - x_1^5 x_4^7 x_5^3 + x_7^6 x_1^6 - x_6^4 x_4^7 x_7^4 \\
g_4(x) &= x_1^8 x_7^8 + x_2^9 x_1^4 + x_4^6 x_5^3 x_{10}^5 - x_2^{16} x_5^9 + x_1^3 x_5^6 \\
g_5(x) &= x_4^{15} x_{10}^3 - x_1^9 x_7^8 x_3^7 - x_1^6 x_{11}^3 x_5^7 + x_{10}^8 x_2^9 + x_4^3 x_1^7
\end{aligned}$$

The Ciphertext polynomial is:

$$\begin{aligned}
C(x) &= 1 + [x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_{10} + x_{11}] \\
&\quad [x_4^{15} x_{10}^3 - x_1^9 x_7^8 x_3^7 - x_1^6 x_{11}^3 x_5^7 + x_{10}^8 x_2^9 + x_4^3 x_1^7] + [(1-x_{11})(1-x_4) \\
&\quad +(1-x_3)(1-x_4)+(1-x_9)(1-x_4)+(1-x_{11})(1-x_3)+(1-x_{11})(1-x_9) \\
&\quad +(1-x_{11})(1-x_2)+(1-x_3)(1-x_2)+(1-x_9)(1-x_2)+x_{11}^2][x_{10}^5 x_4^8 \\
&\quad + x_{11}^4 x_3^6 - x_9^3 + x_5^2 x_2^7 - x_4^9 - x_9^8 x_6^3 x_7^5] + [x_9^5 x_3^6 - x_1^7 x_2^7 x_9^4 - x_8^4 x_6^5 x_1^3 + x_3^8 \\
&\quad +x^6{}_2][(1-x_2)(1-x_3)+(1-x_1)(1-x_2)+(1-x_6)(1-x_3)+(1-x_1)(1-x_6) \\
&\quad +(1-x_2)(1-x_5)+(1-x_6)(1-x_5)]+[(1-x_5)(1-x_7)+(1-x_4)(1-x_7) \\
&\quad + (1-x_8)(1-x_7)][x_{11}^8 + x_{10}^{14} x_4^5 - x_1^5 x_4^7 x_5^3 + x_7^6 x_1^6 - x_6^4 x_4^7 x_7^4] + [x_1^8 x_7^8 \\
&\quad + x_2^9 x_1^4 + x_4^6 x_5^3 x_{10}^5 - x_2^{16} x_5^9 + x_1^3 x_5^6][(1-x_7)(1-x_6) + (1-x_{10})(1-x_7)] \\
&\quad + [(1-x_1)(1-x_8) + (1-x_{10})(1-x_8) + (1-x_1)(1-x_9) \\
&\quad + (1-x_{10})(1-x_9)][x_4^{15} x_{10}^3 - x_1^9 x_7^8 x_3^7 - x_1^6 x_{11}^3 x_5^7 + x_{10}^8 x_2^9 + x_4^3 x_1^7]
\end{aligned}$$

Decryption: α will be found by evaluating the polynomial $C(x)$ at

$Y = (1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0)$. This yields $\alpha = 1$.

4. CONCLUSION

We have constructed certain special cases of Polly Cracker Public Key Cryp- to systems on the domain of marked graphs namely, (i). The subset of places of a marked graph which is both siphon and trap whose input transitions equal to output transitions and both of them equal the set of all transitions of a marked graph (ii) The subset of places of a marked graph whose removal makes the resulting marked graph not to have subsets which are both siphon and trap. It is shown that this system is a secured one.

REFERENCES

[1] Die and Hellman, New Directions in Cryptography, *IEE Transactions on Information Theory*, *IT*, **22**, (1976), 644 -652.

[2] M. R. Gary, and D. S. Johnson, Computers and Interactability, *A Guide to the Theory of NP-Completeness*, Freeman, San Francisco, (1979).

[3] N. Koblitz, Computational Algebra Problems Arising from Combinatorial Cryptography, Discussion Meeting on Cryptography and Computation, Indian Institute of Science, Bangalore, India, (1995).

[4] T. Murata, Petri Nets: Properties, *Analysis and Applications, Proceedings of IEEE*, **77(4)**, (1989), 541-580.

[5] J. L. Peterson, *Petri Net Theory and Modelling of the Systems*, Prentice Hall, Englewood, Cliffs, (1981).

[6] K. Thirusangu, and K. Rangarajan, Marked Graphs and Hamiltonion Graphs, *Microelectronics and Reliability*, **37(8)**, (1997), 1243-1250.

[7] K. Thirusangu, and K. Rangarajan, Polly Cracker Public Key Cryptosystems on Marked Graphs, *Proceedigs of the National Seminar on Modeling and Computer Simulation of Real Life Situations*, St. Xavier's College, Tamilnadu, India, (1996), 195-203.

K. Thirusangu
Department of Mathematics,
Anna University Chennai, Chennai, Tamilnadu, India
E-mail: ktsangu@yahoo.com
on lien from SIVET College, Gowrivakkam, Chennai-73

R. Rajeswari
Department of Mathematics,
Sathyabama University, Chennai, Tamilnadu, India

K. Balasangu
Department of Mathematics,
A.A.G. Arts College, Villupuram, Tamilnadu, India