Extended Elatrash Solution for Game Theoretic Problem

V.V. Lakshmi Prasad, E.Kesavulu Reddy, *Member, IAENG*

Abstract – There are so many applications of cryptography in the field of statistics, particularly in game theory. The area of two party strategic games and the expected equilibrium payoffs can be much higher when a trusted third party assists the players to choose their moves than each player has to choose his move on his own. The role of trusted third party needed to get good payoff. In this paper we propose a beautiful protocol by using extended Elatrash Scheme to remove the mediator (trusted third party) in two player strategic games.

Index Terms— Elatrash scheme, equilibrium, game theory, payoff

I. INTRODUCTION

THE applications of cryptography are essential to solve the problems in the areas of network security, banking, e-commerce, e-business, game theory, internet voting, etc. The research areas of Game theory and cryptography are both extensively studied fields with many problems and solutions. Yet, the cross over between them is surprisingly small: very rarely are tools from one area borrowed to address problems in the other. Some examples of using game theoretic concepts to solve cryptographic problems include the works of Fischer and Wright [8] and Kiliam [9]. The correlated element selection problem consists two cases (i) Special case (ii) General case. In the special case players are "honest but curious" but in the general case players are "malicious". The trusted third party (mediator) [1] handles the total game in both of the cases. To remove the mediator in two player strategic game, here we propose two protocols by using Extended Elatrash Scheme [3, 7] for both the cases.

A. Two player strategic Game

In a two player strategic game [6], there are two players, each with a set of possible moves. The game itself consists of each player choosing a move from the set, and then both players executing their moves simultaneously. The rules of the game specify a payoff function for each player, which is computed on the two moves.

Thus, the payoff of each player depends both on his move and the move of the other player. A strategy for a player is a method for choosing his move. A fundamental assumption of these games is that each player is rational, i.e., its sole objective is to maximize his expected payoff.

A pair of player's strategies achieves equilibrium [6] when these strategies are self-enforcing i.e. each player's strategy is an optimal response to the other player's strategy. In other words, once a player has chosen a move and believes that the other player will follow his strategy. His expected payoff will not increase by changing this move. This notion was introduced in the classical work of Nash [5].

In a Nash equilibrium [5] each player chooses his move independently of the other player. Yet, Aumann showed that in many games, the players can achieve much higher expected payoff, while preserving the "self-enforcement" property, if their strategies are correlated. To actually implement such a correlated equilibrium, a trusted third party called mediator is postulated. This mediator chooses the pair of moves according to the right joint distribution and privately tells each player what his designated move is. Since the strategies are correlated, the move of one player typically carries some information on the move of the other player. In a correlated equilibrium, no player has an incentive to deviate from his designated move, even knowing this extra information about the other player's move. The definitions of Nash equilibrium, correlated equilibrium and some more definitions, theorems are explained in [2].

B. Removing the mediator

The Game theoretic problem is "construction of a two players strategic game with correlated equilibrium, but without actually having a mediator". In the Language of cryptography, we ask if we can design a two party game to eliminate the trusted third party from the original game. It is well known that in the standard cryptographic models the answer is positive, provided that the two players can interact, that they are computationally bounded and assuming same standard hardness assumptions [1, 6]. So that this positive answer can be carried over to the Game theory model as well. Specifically we consider an extended game, in which the players first exchange messages (cheap talk), and then choose their moves and execute them simultaneously as in the original game. The payoffs are still computed as a function of the moves, according to the same payoff function as in the original game.

II. THE CORRELATED ELEMENT SELECTION PROBLEM

In most common games, the joint strategy of the players is described by a short list of pairs [6] {(move1, move2)}, where the strategy is to choose at random pair from this list, and have player1 play move1 and player 2 play move2. The objective of each player is to maximize his expected payoff.

Mr.V.V.Lakshmi Prasad is a senior lecturer in Mathematics, C.A.J .C, Tirupati, Andhra Pradesh-517502, India. (Mobile: + 91 8897596659, Email: lakshmiprasad_v@yahoo.co.in)

Dr. E.Kesavulu Reddy is an assistant professor, Computer Science, S.V.University College of CM & CS, Tirupati, Andhra Pradesh, India-517502. (Mobile: +91 9866430097, Email: ekreddysvu2008@gmail.com)

The result of the game is to get a self-enforcing strategy profile or simply called as equilibrium. Hence to obtain an efficient solution for such games, we need an efficient cryptographic protocol for the following problem:

Two players called preparer (P) and chooser (C), know a list of pairs $\{(a_i, b_i)\}_{i=1}^{m}$ and they need to jointly choose a random index i, and have player P learn only the value a_i and player C learn only the value b_i, we call this problem as the correlated element selection problem.

In this paper we describe our efficient solution for this problem. We explain here a simple protocol for the special case where the two players are "honest but curious" and then modify this protocol to handle the general case where the players can be malicious.

III. EXTENDED ELATRASH SCHEME

Suppose that the user Bob (B) wishes to send the message 'M' to Alice (A). 'A' should do the following:

1. Generate r large random distinct primes p_1, p_2, ….p_r
2. Compute $n = p_1 p_2 \ldots\ldots\ldots p_r$ and
3. $|G| = |GL(k, Z_n)| = (p_1^k - 1)(p_1^k - p)\ldots(p_1^k - p_1^{k-1})(p_2^k - 1)(p_2^k - p_1)\ldots.(p_2^k - p_2^{k-1})\ldots\ldots(p_r^k - 1)(p_r^k - p_r)\ldots..(p_r^k - p_r^{k-1})$
4. Select a random integer 'e' such that gcd (e, |G|) = 1
5. Compute the unique integer d, such that ed ≡ 1 (mod |G|)
6. 'A' publishes his public key (n, k, e)
7. 'A' keeps his private key (n, k, d) secret.

A. Encryption

In order to make 'B' encrypt a message 'M' and send to 'A', 'B' should do the following:

8. Obtain A's public key (n, k, e)
9. Represent the message as a non-singular k x k matrix 'M'
10. Compute the k x k matrix $C \equiv M^e \pmod{n}$
11. Send the cipher text matrix "C" to 'A'

B.Decryption

In order to make 'A' recover the plaintext M from C, he calculates $M \equiv c^d \pmod{n}$ using his private key (n, k, d)

IV. PROTOCOL FOR SPECIAL CASE BASED ON EXTENDED ELATRASH SCHEME OF INDEX 2

1. The preparer selects r suitably large distinct prime numbers p_1, p_2, …..p_r
2. Compute $n = p_1 p_2 \ldots\ldots p_r$ and
$$|G| = |GL(2, Z_n)| = (p_1^2 - 1)(p_1^2 - p_1)(p_2^2 - 1)(p_2^2 - p_2)\ldots\ldots(p_r^2 - 1)(p_r^2 - p_r)$$
3. Select a random integer 'e' such that gcd (e, |G|) = 1
4. Compute the unique integer 'd' such that ed ≡ 1 (mod |G|)

Public key = {n, 2, e} Secret key = {n, 2, d}
Preparer knows both the keys, but chooser knows the public key only.

5. Common input list of pairs $\{(a_i, b_i)\}_{i=1}^{m}$
6. The preparer arranges each ordered pair as 2 x 2 matrices shown below
$$\left\{\begin{bmatrix} a_i & 0 \\ 0 & b_i \end{bmatrix}\right\}_{i=1}^{m}$$
7. The preparer encrypts each matrix by using the encryption formula
$$\begin{bmatrix} c_i & 0 \\ 0 & d_i \end{bmatrix} \equiv \begin{bmatrix} a_i & 0 \\ 0 & b_i \end{bmatrix}^e \pmod{n}$$
Send the list $\{(c_i, d_i)\}_{i=1}^{m}$ to chooser
8. The chooser picks a random pair (c_l, d_l) from the above list and blind the pair with a blinding factor β by computing
$$f \equiv c_l \pmod{n} \text{ and } g \equiv d_l^{\beta} \pmod{n}$$
where gcd (β, ϕ(n)) = 1, now send (f, g) to the preparer
9. After getting the pair (f, g) from the chooser, the preparer decrypts the message with secret key by using the decryption formula
$$\begin{bmatrix} a & 0 \\ 0 & \bar{b} \end{bmatrix} \equiv \begin{bmatrix} f & 0 \\ 0 & g \end{bmatrix}^d \pmod{n}$$

Here 'a' is the preparer's output, now send $\bar{b}$ to chooser.

10. Finally the choosers unblinds $\bar{b}$ by computing $b \equiv \bar{b}^{\beta^{-1}} \pmod{n}$ where $\beta\beta^{-1} \equiv 1 \pmod{\phi(n)}$, here 'b' is the output of chooser.

V. PROTOCOL FOR GENERAL CASE BASED ON EXTENDED ELATRASH SCHEME OF INDEX 2

1. The preparer select r suitably large distinct prime numbers p_1, p_2, …p_r.
2. Compute $n = p_1 p_2 \ldots\ldots\ldots p_r$ and
$$|G| = |GL(2, Z_n)| = (p_1^2 - 1)(p_1^2 - p_1)(p_2^2 - 1)(p_2^2 - p_2)\ldots\ldots(p_r^2 - 1)(p_r^2 - p_r)$$
3. Select a random integer 'e' such that gcd (e, |G|) = 1
4. Compute the unique integer 'd' such that ed ≡ 1 (mod |G|)
Public key = {n, 2, e}Secret key = {n, 2, d}
Preparer knows both the keys whereas chooser knows only public key.
5. Common input list of pairs $\{(a_i, b_i)\}_{i=1}^{m}$
6. The preparer picks a random strings $\{(r_i, s_i)\}_{i=1}^{m}$ and then constructs new string pairs $\{(a_i, r_i), (s_i, b_i)\}_{i=1}^{m}$
7. The preparer arranges each ordered pair as 2 x 2 matrix shown below
$$\left\{\begin{bmatrix} a_i & 0 \\ 0 & r_i \end{bmatrix}, \begin{bmatrix} s_i & 0 \\ 0 & b_i \end{bmatrix}\right\}_{i=1}^{m}$$

8. The preparer encrypts each pair by using encryption formula

$$\begin{bmatrix} c_i & 0 \\ 0 & p_i \end{bmatrix} \equiv \begin{bmatrix} a_i & 0 \\ 0 & r_i \end{bmatrix}^e \pmod{n}$$

$$\begin{bmatrix} q_i & 0 \\ 0 & d_i \end{bmatrix} \equiv \begin{bmatrix} s_i & 0 \\ 0 & b_i \end{bmatrix}^e \pmod{n}$$

now send the list $\left\{(c_i, p_i), (q_i, d_i)\right\}_{i=1}^{m}$ to chooser.

9. The chooser picks a random pairs $\left\{(c_l, p_l), (q_l, d_l)\right\}$ from the above list and blinds the pairs with blinding factors α and β.

$$x \equiv c_l \pmod{n} \ , \ y \equiv p_l^{\alpha} \pmod{n}$$

$$z \equiv q_l \pmod{n} \quad , \ w \equiv d_l^{\beta} \pmod{n}$$

Where gcd (α, $\phi(n)$) = 1, gcd (β, $\phi(n)$) = 1, now send the pairs (x, y), (z, w) to the preparer

10. After getting the two pairs (x, y), (z, w), the preparer decrypts the pairs by using secret key.

$$\begin{bmatrix} a & 0 \\ 0 & \bar{p} \end{bmatrix} \equiv \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix}^d \pmod{n}$$

$$\begin{bmatrix} q & 0 \\ 0 & \bar{b} \end{bmatrix} \equiv \begin{bmatrix} z & 0 \\ 0 & w \end{bmatrix}^d \pmod{n}$$

Here a is the preparer's output, now send $\bar{b}$ to the chooser

11. Finally the chooser unblinds $\bar{b}$ by using the formula $b \equiv \bar{b}^{\beta^{-1}} \pmod{n}$

Where $\beta\beta^{-1} \equiv 1 \pmod{\phi(n)}$, here 'b' is the output of the chooser.

VI. CONCLUSION

The most interesting aspect of our work is the achievement of an energetic solution for a common problem occurring in two party strategic game. Notice that by implementing our cryptographic solution in the game theory setting, we gain on this aspect is eliminating mediator. Generally mediators are not honest, so our protocol helps us to continue the game without mediator. And also we eliminate the problem of early stopping. We can extend our proposed scheme by using Block Ciphers, NTRU cryptosystem, MR-RSA cryptosystem, any cryptosystem based on primality tests.

AUTHOR INFORMATION

I am V.V.Lakshmi Prasad working as a Sr.Lecturer in Mathematics, C.A.J.C Tirupati,(A.P)-India .I presented Five papers in international Conferences. I published four papers in International Journals

I am Dr.E.Kesavulu Reddy working as a Assistant Professor Dept. of. Computer Science, Sri Venkateswara University College of Commerce Management and Computer Science, Tirupati (AP)-India. I received Master of Computer Applications and Doctorate in Computer Science from S.V.University, Tirupati, Andhra Pradesh India. Also I received Master of Philosophy in Computer Science from M.K. University, Madurai, and Tamilnadu, India. I am one paper presented in WCECS2010, U.S.A and two papers published in WCE 2011 & 2012, London, U.K. I published eight papers in International and five in National Journals, also attending in Five International and six National conferences. My research interest in the field of Computer Science in the area of Elliptic Curve Cryptography-Network Security, Data Mining, and Software Engineering.

REFERENCES

[1] V.V. Lakshmi Prasad, "A development of an efficient solution of Game theoretic problem using extended J_2-RSA cryptosystem based on Hill cipher", IJOTMA, 2009, Vol. 1(2), pp: 239-246.

[2] Y. Dodis, S. Halevi and Robin: "A cryptographic solution to a game theoretic problem", IBM J.J. Watson Research Centre, P.O. Box. 704, Yorktown Heights, New York 10598, USA.

[3] Faji Ramadan, EL-Naowk: "A generalization of the RSA Elatrash scheme; JOAS 7(13): 1824-1826, 2007; ISSN 1812-5654 ©2007 Asian Network for Scientific information.

[4] T.M. Apostol: "Introduction to Analytic number theory, Springer International Students Edition. 1980.

[5] J.F. Nash: "Non Cooperative games, Annals of Mathematics, 54, pp: 286-295.

[6] O.Goldreich, S. Micali and A.Wigdeerson: "How to play any mental game", Proceedings of the 19th annual ACM symposium on theory of computing, pages 218-229, 1987.

[7] V.V. Lakshmi Prasad, "Image encryption using J_k-RSA Elatrash scheme" Kuwait ICT Security Forum proceedings" May 5th – 6th, 2009.

[8] M. Fischer, R. Wright. "An application of game-theoretic techniques to cryptography." In advances in computational complexity theory, DIMACS series in discrete mathematics and theoretical computer science Vol. 13, pp: 99-118, 1993.

[9] J. Kilian (More) completeness theorems for secure two party computation. In proceeding of STOC, 2000.