A Secure Mental Poker Protocol Over The Internet

Weiliang Zhao [†] **Vijay Varadharajan** [† ‡] **Yi Mu** [‡]

[†] School of Computing and Information Technology
University of Western Sydney,
NSW 2747, Australia
Email: wzhao@cit.uws.edu.au

[‡] Department of Computing
Macquarie University,
NSW 2109, Australia
Email: vijay, ymu@ics.mq.edu.au

Abstract

An efficient and secure mental poker scheme is proposed in this paper. It is based on multiple encryption and decryption of individual cards. The protocol satisfies all major security requirements of a real mental poker. It gets rid of the Card Salesman and guarantees minimal effect due to collusion of players. The protocol is secure and more efficient compared with other known protocols. The strategies of players can be kept confidential with the introduction of a Dealer. The protocol is suitable to be implemented in an on-line card game.

Keywords: Mental Poker, Applied Cryptography, On-line Gambling.

1 Introduction

In 1979, Shamir, Rivest and Adleman (Shamir, Rivest & Adleman 1979) proposed a scheme for playing "Mental Poker". Following this, many attempts have been made to achieve protocols that would allow people to play "Mental Poker" (Fortune & Merrit 1985, Shamir, Rivest & Adleman 1981, Goldwasser & Micali 1982, Barany & Furedi 1983, Yung 1985, Crepeau 1986, Crepeau 1987, Crepeau & Killian 1994). With the growth and popularity of the Internet, on-line gambling is becoming increasingly significant (Hall & Schneier 1997, Zhao, Varadharajan & Mu 2000). Mental poker is one of most popular games of on-line gambling. For the purpose of on-line gambling over the Internet, additional requirements on a poker protocol need to be considered. The need for secure and efficient protocols for card games is becoming increasingly significant.

There have been several protocols based on public-key cryptography described in literature for playing mental poker (Shamir et al. 1981, Lipton 1981, Goldwasser et al. 1982, Yung 1985, Fortune et al 1985, Coppersmith 1986, Kurosawa, Katayama, Ogata & Tsujii 1991). These protocols require that players generate new key pairs for each game they play, which could be computationally intensive. Many of these protocols are not secure in their implementations, and they leak partial information about the cards themselves. There are some protocols based on multiple permutations which require a trusted Card Salesman to be involved in the games. (Hall et al. 1997, Fortune et al 1985, Barany et al 1983). If card games are used for the purpose of on-line gambling, the assumption of a fully trusted Card Salesman is not tolerable. Some protocols (Crepeau 1986, Crepeau 1987, Crepeau et al 1994) have no information leakage and meet many of the important requirements of a real poker game, but they are not practical in their implementation. They use zero-knowledge proof and the protocols are not efficient in shuffling and dealing with cards.

We are interested in efficient and secure mental poker protocol which can satisfy all the major requirements of a real poker protocol. In this paper, we propose a new poker protocol based on multiple encryption and decryption of individual cards. The protocol provides confidentiality of cards and is efficient in real implementation. The protocol is suitable for any number of players to play card games over the Internet. The effect of collusion is minimum and the strategies of players are confidential with the introduction of a Dealer.

Section 2 discusses typical former protocols of mental poker. Individual card cryptosystem and permutation cryptosystem are described in this section. Section 3 describes a multiple encryption and decryption system that will be the principal component of our mental poker protocol. Section 4 describes the details of our mental poker protocol. In this section, initialization of cards, shuffling of a set of cards and the dealing of cards are defined. Section 5 discusses the security properties of our protocol. Section 6 provides the conclusions.

2 Typical Former Protocols of Mental Poker

2.1 Protocol Based on Individual Card Cryptosystem

Adi Shamir, Ronald Rivest and Leonard Adleman (Shamir et al. 1981) utilized commutative cryptosystems to develop their mental poker protocol. Let E_A and D_A be Alice's encryption and decryption functions, E_B and D_B be Bob's encryption and decryption functions respectively. In real implementation, Alice and Bob agree on a large prime number p, and respectively choose secret keys $k = A$ and $k = B$, where $gcd(A, p-1) = gcd(B, p-1) = 1$. Then $E_k(x) \equiv x^k (\mod p)$ and $D_k(x) \equiv x^z (\mod p)$, where $kz \equiv 1 (\mod p-1)$. The above cryptosystem is a commutative cryptosystem. For all messages x, $E_A(D_B(x)) = D_B(E_A(x))$, $E_B(D_A(x)) = D_A(E_B(x))$, $E_A(E_B(x)) = E_B(E_A(x))$, $D_A(D_B(x)) = D_B(D_A(x))$. Alice and Bob will play the game as follows:

1. A deck of cards $\{1, ..., 52\}$ is used in the cryptosystem. Alice encrypts each card in the deck separately. Alice sends the set $\{E_A(1), ..., E_A(52)\}$ in a random order to Bob.

2. Bob chooses five encrypted cards at random, for example $\{E_A(6),\ E_A(8),\ E_A(17),\ E_A(25),\ E_A(33)\}$, and sends them to Alice, Alice could know that they are {6, 8, 17, 25, 33}.

3. Bob chooses five different encrypted cards, for example $\{E_A(3),\ E_A(11),\ E_A(19),\ E_A(23),\ E_A(41)\}$, encrypts them, and sends them back to Alice as a randomly ordered set $\{E_B(E_A(3)),\ E_B(E_A(11)),\ E_B(E_A(19)),\ E_B(E_A(23)),\ E_B(E_A(41))\}$.

4. Alice decrypts cards one by one and sends Bob the resulting set $\{E_B(3),\ E_B(11),\ E_B(19),\ E_B(23),\ E_B(41)\}$. Bob could decrypt and get {3, 11, 19, 23, 41}.

5. At the end of the game, they could exchange their encryption keys and verify that all players have played fairly.

Lipton (Lipton 1981) observed that the above implementation leaks at least one bit of information. For a number x, if $x \equiv y^2 (mod\ n)$ for some y, x is a quadratic residue modulo n; otherwise, x is non-quadratic residue. All keys must be odd numbers, and $x^k \pmod{\text{n}}$ is a quadratic residue if and only if x is. If the players know which cards are quadratic residues and compare them with encrypted cards, players could have one bit of information per card. Lipton provided some suggestions for the one bit information leak, but there is no guarantee that the result is secure (Coppersmith 1986).

2.2 Protocol Based on Permutation Cryptosystem

There is a series of protocols (Hall et al. 1997, Fortune et al 1985, Barany et al 1983) which are based on the multiple permutations. In the following, we will describe a popular protocol. There are three players Alice, Bob and Charles and one Card Salesman. They use the following steps to prepare a deck of cards:

1. Card Salesman chooses a permutation π

2. Alice chooses three permutations A_a, A_b and A_c. Bob chooses three permutations B_a, B_b and B_c. Charles chooses three permutations C_a, C_b and C_c. All the above permutations are sent to Card Salesman confidentially (only the sender and Card Salesman know them).

3. Card Salesman computes and broadcasts the folowing
$$\delta_a = B_a^{-1} C_a^{-1} A_a^{-1} \pi^{-1},$$
$$\delta_b = C_b^{-1} A_b^{-1} B_b^{-1} \pi^{-1},$$
$$\delta_c = A_c^{-1} B_c^{-1} C_c^{-1} \pi^{-1}.$$

If a player, for example Alice, wants to draw a card, the following protocol is used

1. Alice chooses $y = \pi(x)$ which is not in any player's hand and broadcasts y and $\delta_a(y)$.

2. Bob computes and broadcasts $B_a(\delta_a(y))$.

3. Charles computes and broadcasts $C_a(B_a(\delta_a(y)))$.

4. Alice computes $x = A_a(C_a(B_a(\delta_a(y))))$.

5. All players record that $y = \pi(x)$ has been in Alice's hand.

At the end, all permutations are published to check the fairness of the game. The above protocol could guarantee that a player can draw a card which is not in anyone's hand and only he could know what the card is. If the Card Salesman and at least one player plays fairly, there is no way for a player or group of colluding players to get information of cards which are not in their own hands. This protocol requires a Card Salesman to choose a random π and broadcast permutations. If the card game is used for gambling, the assumption that the Card Salesman be fully trusted is not a good one. Another aspect of this permutation based poker scheme is that cheating can only be detected at the end of the game and not during the protocol run.

3 Multi-Party Encryption and Decryption

Based on the ElGamal cryptosystem, we will discuss a multi-party encryption and decryption system. Without losing generality, we assume that there are two parties A and B. The two parties use the same prime number p. They have

$$\mathcal{K}_A = \{(p, \alpha_A, k_A, \beta_A) : \beta_A \equiv {\alpha_A}^{k_A} (\bmod\ p)\}$$
$$\mathcal{K}_B = \{(p, \alpha_B, k_B, \beta_B) : \beta_B \equiv {\alpha_B}^{k_B} (\bmod\ p)\}$$

1. Encryption:

   The original message is x. A chooses random number r_A, and the result of encryption with $\mathcal{K}_A$ has two parts y_{1A} and y_{2A}:

   $$y_{1A} = \alpha_A^{r_A} \bmod\ p$$
   $$y_{2A} = x\beta_A^{r_A} \bmod\ p$$

   B chooses random number r_B and encrypts the ciphertext of A's encryption (actually B encrypts y_{2A}) and gets the following two parts,

   $$y_{1B} = \alpha_B^{r_B} \bmod\ p$$
   $$y_{2AB} = x\beta_A^{r_A}\beta_B^{r_B} \bmod\ p$$

   Actually, there is no difference whether A or B encrypts first; we will get the same ciphertex y_{1A}, y_{1B}, y_{2AB}.

2. Decryption:

   If A uses his private key to decrypt first,

   $$d_{\mathcal{K}_A}(y_{1A},\ y_{2AB}) = \ y_{2AB}\ ({y_{1A}}^{\ k_A})^{-1} = \ y_{2B} \bmod p$$

   and then B uses his private key to decrypt

   $$d_{\mathcal{K}_B}\ y_{2B}) = \ y_{2B}\ ({y_{1B}}^{\ k_B})^{-1} = \ x \bmod\ p$$

   x is the original message.

   Actually, there is no difference whether A or B decrypts first; we could use the following formula to express the whole multi-party decryption

   $$d_{\mathcal{K}_A,\mathcal{K}_B}(\ y_{1A},\ y_{1B},\ y_{2AB}) =$$
   $$y_{2AB}\ ({y_{1A}}^{\ k_A})^{-1}\ ({y_{1B}}^{\ k_B})^{-1} = x \bmod\ p$$

The most important characteristic for the above system is that if a different order is used for encryption, the final ciphertext is the same. If a different order is used for decryption, the original message could be obtained. In next section, we describe the mental poker protocol using the above commutative cryptosystems.

4 Mental Poker Protocols

We assume that many players play a fair on-line "Mental Poker" game. Part of the card game involves shuffling and dealing the cards in a fair manner. All the players must be sure that nobody has stacked the deck. We assume that there is not a trusted third party involved during the game. In this paper, we will only focus on the protocol for shuffling and dealing the cards. We propose a mental poker protocol which can shuffle any set of cards. Unlike protocols based on many permutations (Fortune et al 1985), this protocol always deals with cards one by one. Without losing generality, we assume that there are two players Alice and Bob. There is no real difference, should more players play the game.

4.1 Initialization

1. Alice and Bob agree to choose the same 52 tokens for 52 cards, that are suitable encoding set {1, ... , 52}.
2. Alice and Bob agree to choose the same prime number p.
3. Alice chooses her encryption and decryption key pairs as follows:

$$\mathcal{K}_A = \{(p, \alpha_A, k_A, \beta_A) : \beta_A \equiv {\alpha_A}^{k_A} (\bmod p)\}$$

4. Alice has a public/private key pair pka and ska, ska for signature and pka for verification by others.
5. Bob chooses his encryption and decryption key pairs as follows:

$$\mathcal{K}_B = \{(p, \alpha_B, k_B, \beta_B) : \beta_B \equiv {\alpha_B}^{k_B} (\bmod p)\}$$

6. Bob has public/private key pair pkb and skb, skb for his signature and pkb for verification by others.

4.2 Cards Shuffling

In our protocol, the card shuffling is based on the encryption of individual cards.

1. Alice chooses a secrete random number r_A, and then encrypts original cards one by one. The set of encrypted cards is $\{E_A(1), ..., E_A(52)\}$ in a random order. Alice signs the hash function of r_A to get $< H(r_A) >_{ska}$. Alice sends $\{E_A(1), ..., E_A(52)\}$ and $< H(r_A) >_{ska}$ to Bob.
2. Bob chooses a secret random number r_B, and then encrypts original cards one by one. The set of encrypted cards is $\{E_B(1), ..., E_B(52)\}$ in a random order. Bob signs the hash function of r_B to get $< H(r_B) >_{skb}$. Bob sends $\{E_B(1), ..., E_B(52)\}$ and $< H(r_B) >_{skb}$ to Alice.
3. Alice encrypts the set of cards encrypted by Bob and gets $\{E_{AB}(1), ..., E_{AB}(52)\}$. Alice sends the results to Bob.
4. Bob encrypts the set of cards encrypted by Alice and gets $\{E_{BA}(1), ..., E_{BA}(52)\}$. Bob sends the results to Alice.
5. Alice checks two sets of double encrypted cards with a different encryption order. If the two sets are not equal, then the protocol will be stopped. If they are equal, Alice signs the double encrypted cards one by one. With the notation $C[n] = E_{AB}(n)$ where $(n = \{1, ..., 52\}$ is the order number of cards, Alice gets $\{< H(C[1]) >_{ska}, ..., < H(C[52]) >_{ska}\}$. Alice signs the order of cards and gets $< C[1], ..., C[52] >_{ska}$. Alice sends the double encrypted cards, signatures of cards and signed order of cards to Bob.
6. Bob checks the set of double encrypted cards and their signatures by Alice. Bob checks two sets of double encrypted cards with a different encryption order. If the checks are successful, Bob signs double encrypted cards again and gets $\{< H(C[1]) >_{ska,skb}, ..., < H(C[52]) >_{ska,skb}\}$. Bob signs the order of cards again and gets $< C[1], ..., C[52] >_{ska,skb}$. Bob sends signatures of cards and signed order of cards to Alice.

Now the deck of cards has been prepared. All the cards are encrypted by Alice and Bob with their signatures. Based on our discussion in section 2, encryptions in different order give the same results. We only use a definite order of signatures in the whole protocols. Obviously, if more parties involved, our protocols will work exactly in a similar manner to the above.

4.3 Card Dealing

There are 52 cards encrypted by both Alice and Bob. At the very beginning, the set of available order numbers is $\{1, ..., 52\}$. During the game, if some cards are in players' hands, the corresponding order numbers are deleted from the available set. When a player needs a card, the following protocol is carried out.

1. Alice needs to draw a card m, m is the card order after the double encryptions. She sends m and $< H(m) >_{ska}$ to Bob.
2. Bob checks Alice's signature and then checks that m is in the available set or not. If it is not in the available set, Bob sends Alice a suitable message. If it is in the available set, Bob decrypts the double encrypted card m. The original order of the card is n, the card m is $C[n]$. After Bob's decryption, it becomes $E_A(n)$. Bob sends $E_A(n)$, $< m, H(E_A(n)) >_{skb}$ to Alice. Bob deletes m from his available set.
3. Alice checks Bob's signature and decrypts $E_A(n)$ to open the card and adds the card to her hand. Alice deletes m from her available set.

When the game is over, Alice and Bob reveal their secret random number r_A and r_B. Both Alice and Bob can check whether the other party has been cheating or not. The strategy of each player is completely revealed at the end of the game. In next section, we discuss how to ensure confidentiality of strategy.

If there are many players, the above protocol works in a similar manner. The only difference is that if a player needs a card, all other players will decrypt the card one by one and update their available sets at the same time. A player who needs the card can open the card and add it to his/her hand, and updates his/her available set.

5 Discussion

In the following section, important security properties of our protocol are discussed. We also compare our protocol with previously published protocols.

(I) Complete Confidentiality of Cards
Previous protocols based on individual cards has the shortcoming of leaking of one bit information (Lipton

1981, Coppersmith 1986). Lipton discussed the leakage and gave some suggestions for strengthening the cryptosystem, for example, the cards are encoded originally so that they are all quadratic residues (or all nonresidues). But there is still no guarantee that the result is secure. Indeed, the indication is that bits may still leak. In our protocol, there is no information leakage because the encryption/decryption uses the standard ElGamal cryptosystem.

(II) Without Card Salesman
There is a Card Salesman involved in the previous protocols (Hall et al. 1997, Fortune et al 1985, Barany et al 1983) that are based on multiple permutations. The fairness of this kind of protocols is based on the assumption that the Card Salesman is fully trusted. In real gambling, such an assumption is not appropriate. We can not assume the existence of such a fully trusted party. The protocol presented in this paper gets rid of the Card Salesman completely.

(III) Any Number of Players
Based on the commutativity of multi encryptions and decryptions, it is convenient to expand the protocol to multi-players. With the same prime number p, each player, for example X, has key pair $\mathcal{K}_X = \{(p, \alpha_X, k_X, \beta_X) : \beta_X \equiv {\alpha_X}^{k_X} (\bmod p)\}$. In the card shuffling process, every player X chooses a secret random number r_X. All cards are multi-encrypted by all players. In the card dealing, when player X draws a card, all other players decrypt the card, and only player X can open the card. All players delete the card from the available set.

(IV) Security Against Player Collusions
The protocol can guarantee the minimal effect of collusion. Even if two players collude, they can only obtain each other's cards but not a card of a third player. Because every card is multi-encrypted by all the players, a card is opened only in the case that all players have decrypted it. Any subset of players can not know anything about the cards of other players. No collusion among cheating players can affect the cards drawn by an honest player and untouched cards.

(V) Complete Confidentiality of Strategy
The protocol presented asks players to reveal all information at the end of the game. It makes it impossible for the players to bluff. Real poker players would never accept to play such a game. Fortunately, if the Dealer is involved, it is very easy to modify the above protocol. When shuffling cards, every player X chooses his secret random number r_X and sends $< H(r_X) >$ to the Dealer. During the game, every player sends the information of his actions (for retrieving in the future, except opened cards) to the Dealer. At the end of the game, every player sends his secret random number to the Dealer. The Dealer is able to check the fairness of the whole game. During the game, the card information is confidential to the Dealer. The Dealer is the only person who can know the strategy of each player at the end of the game. Such an assumption is reasonable and acceptable. It is much better than the assumption of a Card Salesman who is fully trusted and knows all card information during the game.

(VI) Efficiency and Clarity
The cryptosystem used in our scheme is based on ElGamal cryptosystem. For a game of two players, there are only 104 times ElGamal encryptions and decryptions(maximum in one whole game). For a game of n players, there are $52 \times n$ ElGamal encryptions and $52 \times n$ ElGamal decryptions (maximum in one whole game). The protocol is efficient. For a group of players, after the system has been setup, they can use their encryption/decryption key pairs and public/private key pairs for multiple games. For a new game, the players only need to choose new secret random numbers (encryption parameters). There are several other successful protocols based on zero-knowledge proofs. Unfortunately they are not practical and are often very complicated and messy. They need a fairly long computation time to shuffle a deck of cards.

6 Conclusions

Our mental poker protocol scheme has achieved the major requirements of a complete poker system. The protocol is secure, efficient and is suitable for any number of players. Our protocol gets rid of the Card Salesman entity completely and there is minimal effect due to collusion of players. With the introduction of a Dealer, the strategies of players can be made confidential to other people (except the Dealer). In this case, the Dealer only becomes aware of the strategies of players at the end of the game. However, there are some open problems which are not solved by our protocol, for example, how to return a card to the deck.

With the growth of popularity of the Internet, the Internet has become an important marketplace for on-line gambling. Card games are widely used in on-line gambling over the Internet. The gambling process requires actions such as placing bets and dealing with payments. Our protocol is based on individual cards. It is easy to combine this protocol with the management protocols of the whole gambling processes. A fair on-line gambling scheme has been proposed by the authors of this paper (Zhao et al. 2000) to guarantee the fairness of on-line gambling. Based on this fair on-line gambling scheme and the card protocol presented here, efficient, fair and secure solution of using card games in on-line gambling can be achieved.

References

Shamir, A, Rivest, R. & Adleman, L. 1979, Mental Poker, MIT/LCS/TM-125, Laboratory for Computer Science, Massachusetts Institute of Technology, 545 Technology Square, Cambridge, MA 02139.

Hall, C. & Schneier, B. 1997, Remote Electronic Gambling, IEEE, pp. 232–238.

Zhao, W. Varadharajan, V. & Mu, Y. 2000, Fair On-line Gambling, 'Proceedings of the 16th Annual Computer Security Applications Conference', ACSAC, pp. 394–400.

Shamir, A. Rivest R. & Adleman, L. 1981, Mental Poker", 'Mathematical Gardner',Wadsworth International, pp. 37–43.

Lipton, R. 1981 , How to Cheat at Mental Poker, 'Proceedings of the AMS Short Course in Cryptography'.

Goldwasser, S. & Micali, S. 1982, Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information, 'Proceedings of the 14th ACM Symposium on the Theory of Computing', pp. 270–299.

Yung, M. 1985, Cryptoprotocols: Subscriptions to a Public Key, the Secret Blocking, and the Multu-Player Mental Poker Game, 'Advances in Cryptology - CRYPTO'84 Proceedings', Springer-Verlag, pp. 439–453.

Fortune, S. & Merrit, M. 1985, Poker Protocols, 'Advances in Crytology - CRYPTO'84 Proceedings', Springer-Verlag, pp. 454–464.

Coppersmith, D. 1985, Cheating at Mental Poker, 'Advances in Cryptology - CRYPTO'85 Proceedings', Springer-Verlag, pp. 104–107.

Kurosawa, K. Katayama, Y. Ogata, W. & and Tsujii, S. 1991, General Public Key Reside Cryptosystems and Mental Poker Protocols, 'Advances in Cryptology - CRYPTO'90 Proceedings', Springer-Verlag, pp. 374–388.

Barany, I. & Furedi, Z. 1983, Mental Poker with Three or More Players, Technical Report, Mathematical Institute of the Hungarian Academy of Science(1983).

Crepeau, C. 1986, A Secure Poker Protocol that Minimizes the Effect of Player Coalitions, 'Advances in Cryptology - CRYPTO'85 Proceedings', Springer-Verlag, pp. 73–86.

Crepeau, C. 1987, A Zero-Knowledge Poker Protocol that Achieves Confidentiality of the Players' Strategy or How to Achieve an Electronic Poker Face, 'Advances in Cryptology - CRYPTO'86 Proceedings', Springer-Verlag, pp. 239–247.

Crepeau, C. & Killian, J. 1994, Discrete Solitary Games, 'Advances in Cryptology - CRYPTO'93 Proceedings', Springer-Verlag, pp. 319–330.