**Mental Poker**

Team Members:

1. Vaibhavi Srivastava (20BCI0239)
2. Nabil Ashraf (20BCI0279)
3. Kaif Ahmad (20BCI0217)
4. Ishaan Lonial (20BCI0240)
5. Jitesh Aggarwal (20BCI0185)
6. Khushi Sharma (20BCI0243)

Branch**:**

Computer Science and Engineering (Specialisation in Information Security)

School**:**

School of Computer Science & Engineering

Submitted To**:**

Madhu Viswanatham Sir



**Abstract:**

Mental Poker is the standard problem of being able to successfully carry out an online game of poker without leaving any scope for collusion or cheating. An efficient and secure mental poker scheme is proposed in this project. It employs commutative encryption and decryption methods. The protocol meets all main security standards and provides a fair way to play Mental Poker that eliminates any possibility of cheating. When compared to other protocols, the protocol is more secure and efficient.

During the game, players have the option of drawing a new card from the "remaining deck" or revealing specific cards in their hand to the other player. They can do so without jeopardising the security of the cards they still have in their hands. With the advent of a Dealer, participants' strategies can be kept private. The protocol is suitable for use in an online card game.

Keywords: commutative encryption and decryption, RSA, SRA, cryptography, plain text, cipher text

**Introduction:**

The idea of playing card games "over the phone," or "Mental Poker," as it is frequently referred to, has played a significant role in the development of cryptography. Mental Poker protocols allow a group of players that are mutually distrustful of each other to play cards electronically instead of using trusted dealers. In mental poker, there are very few assumptions about the conduct of opponents. Adversaries are usually free to form any size coalition and carry out active attacks.

Shamir, Rivest, and Adleman presented a method for playing "Mental Poker" in 1979. Many attempts have been made since then to develop protocols that would allow people to play "Mental Poker." Additional restrictions for a poker protocol must be considered for the purpose of online gambling over the Internet. For card games, the requirement for secure and efficient protocols is growing significantly.

Several protocols based on public key have been developed. Many of these protocols' implementations are insecure, leaking some information about the cards themselves. Players must generate fresh key pairs for each game, which can be computationally costly. Some protocols that use many permutations entail the participation of a trusted Card Salesman in the games. We're looking for a mental poker protocol that's both efficient and secure and can meet all of the major requirements of a genuine poker protocol. Mental Poker is played just like any other regular game of poker; Except that there are no cards. That is, all communications between the players must be accomplished using messages to each other. We therefore aim to use Cryptographical techniques and methods to achieve and create this model successfully. Each player must know which cards are in his hand but must not know which cards are in the hands of the other players. The dealing procedure should ensure that each player has an equal chance of getting all potential hands. The methodology ensures card confidentiality and is simple to use in practice.

**Aim:**

The Aim of this project is to successfully implement a program that enables the users to play a fair game of Poker through any device with an internet connection (for example a mobile phone) without needing the involvement of a trustworthy third-party card dealer and ruling out all possibilities of any unfair practices simultaneously.

**Literature Survey:**

On reading and examining previous research done on the matter, there are some key findings that stand out. The entire point of all research done on Mental Poker is to minimise all ways of collusion and cheating, by preventing players from getting access to the data of other players, and making sure that even if accessed, the information is encrypted efficiently, preventing the cheater to view any partial information.

Firstly, according to Zhao and Varadharajan, using multiple encryptions and decryptions on all individual cards solves the problem of other players not being able to read the cards of another player. For example, a game of two players will have a maximum of just 104 encryptions and decryptions. It’s fairly easy to get rid of the card salesman altogether using this protocol too, with a minimal effect on the prospects of cheating/collusion amongst the players. But this protocol leaves some problems unsolved, for instance, there is no direct way to return a card to the deck.

In continuance, the paper presented by Jordi Castell ‘a-Roca and their team, suggests ways to create a mental poker system that has dropout tolerance, while also making sure there is no need for a trusted third-party dealer. Dropout tolerance means the game can still continue safely even if a player decides to drop out of the session mid game. The idea applied is that in the Kth round of dealing the cards, each individual player computes a new value for d for each card which is then used to raise the card to a random value. This exponent is then encrypted to the card and sent along with the new value. In step 2 of this protocol, when players veto the cards that they have previously gotten, another round of dealing takes place. If a player draws a vetoed card, they cannot use it and therefore are not shown either the value of the card or reveal to them which player it was the initially vetoed the card.

Further research done by Castell ‘a-Roca, Daza and Domingo-Ferrer, showed that using homomorphic encryption protocols to manipulate the cards in an encrypted form, allows the players to manage cards cooperatively. After 52 face up cards are generated, all players have to agree upon which card to choose as Di, post which, the encryption is performed. This facilitates the possibility of there being card manipulation while they are in encrypted form.

Adding to that, Tzer-jen Wei in their paper, recommends that unlike all previous models that use standard L round zero knowledge protocols to check the integrity of the shuffle; A model following the Castell ‘a-Roca protocol (mentioned above) as a foundation, is much faster and reduces the communication cost significantly too. The L-round shuffle verification is replaced by a checksum-like framework. This framework makes sure that each card is re-encrypted with the same random parameter, therefore ruling out all possibilities of there being duplicates or forged cards present in the deck.

The paper written by Coppersmith, suggests that the primes should be of the form 2q+1 where q is prime, which reduces the chances of any player willing to cheat since they would only be able to spot the difference between quadratic and non-quadratic residues, furthermore, to make that information confidential too, the bits of the cards can be appended to ensure that all cards are quadratic residues. It also states that allowing the opponent to pick the random numbers for the procedure of “random padding” is also significantly risky, therefore that leaves us with the only workaround of having to omit that step altogether. This paper makes it abundantly clear that we cannot use the idea of random padding and cannot use a prime number p where the number (p-1) has a small prime divisor, as that enables scope for cheating.

Another paper authored by Goldwasser and Micali suggests a different way to try and keep all partial information hidden from the players. It states that the main idea behind using the RSA scheme, or the Rabin scheme is to select an ideal trapdoor function that is easy to evaluate but hard to trace back from f(x) unless the external key information is known. They therefore suggest replacing the trapdoor functions with probabilistic encryption. That is, the use of a fair coin to encrypt a message along with the plain text itself. This leads to multiple encodings for every individual message, and therefore exponentially harder to crack for any player looking to collude or encroach on partial information.

Subsequently, another method was proposed specifically for the shuffling and dealing of cards that significantly reduced latency and is useful for systems with low resources. The authors believe that having a trusted authority to calculate and allocate a set of public and private keys to each of the players along with their additive shares of the private keys, is the best way to deal cards (Provided that the authority plays a very restricted function). That is, they keys were encrypted with an algorithm that is additively homomorphic and were allocated amongst the challengers.

In a paper by Barnett and Smart, they propose a solution where the foundation of the model is to have a broadcast channel between all the competitors, where the number of bits required to represent any player’s cards after encryption are independent of the number of players, whereas most traditional approaches to this problem have a clear linear relation between the number of players and the number of bits used to represent each card after subsequent padding and encryption. This potentially minimises the avenues for collusion and ensures that even if some parties do decide to collude, they get no more information than they would colluding in a game of poker in real life.

**Survey Table:**

|  |  |
| --- | --- |
| **TITLE** | **VERDICT** |
| **How to play Mental Poker keeping secret all partial information** | Each message's encoding will be determined by the message as well as the outcome of a series of coin flips. Probabilistic Encryption replaces the concept of trapdoor functions |
| **An efficient poker protocol for shuffling and dealing cards** | The proposed approach provides a drastic reduction in latency and general computing cost compared with general systems for shuffling cards. |
| **Mental Poker revisited** | The protocols that follow ensure that the colluding parties receive no more knowledge than they would if they were conspiring in a real game. |
| **A secure Mental poker protocol over the internet** | The protocol entirely eliminates the Card Salesman entity, with only a minor influence owing to player cooperation. |
| **Secure and practical constant round Mental Poker** | This protocol is faster and more secure than the L-round-based protocol. The cost of communication is lowered, both in terms of the number of messages sent and the length of those communications. |
| **Privacy Homomorphisms for E-gambling and mental poker** | Homomorphic encryption may be used to handle cards in encrypted form, allowing players to work together to control cards. |
| **Cryptoprotocols and Subscription to a public key, the secret blocking and the multi-player Mental Poker game** | The divide-and-conquer strategy (using axioms and proving procedures) will almost certainly be implemented in future sophisticated and extensive cryptoprotocols. |
| **Cheating at Mental Poker** | In the sense that seemingly innocuous alterations (option of p, padding with seemingly random bits) might allow for cheating, the card protocol is vulnerable. It is said to not utilise "random padding," and make sure the opponent isn't picking the numbers at random. |
| **Dropout-Tolerant TTP-Free Mental Poker** | This is the first idea to allow both deliberate and unintentional player dropouts using TTP-free approach. The protocol described in this paper might be used to secure multi-party computation. |
| **Using Commutative encryption to share a secret** | The technique is based on the discrete logarithm problem and is expected to be secure. It involves exploiting the operation's commutative property to transfer a secret from one party to another. |

**References:**

|  |
| --- |
| Weblinks:   1. Mordechai Young. Cryptoprotocols: Subscription to a public key, the secret blocking and the multi-player mental poker game. (1985) Available: https://link.springer.com/chapter/10.1007/3-540-39568-7\_35 2. Shaft Goldwasser and Silvio Micali. How To Play Mental Poker Keeping Secret All Partial Information. (Berkeley, 1992) Available: <https://www.researchgate.net/publication/336402406_Probabilistic_encryption_how_to_play_mental_poker_keeping_secret_all_partial_information> 3. Zinah S. Jabbar, Sattar J. Aboud. An Efficient Poker Protocol for Shuffling and Dealing Cards. (2019) Available: <https://www.researchgate.net/publication/336473801_An_Efficient_Poker_Protocol_for_Shuffling_and_Dealing_Cards> 4. Adam Barnett and Nigel P. Smart. Mental Poker revisited. (2003) Available: <https://link.springer.com/chapter/10.1007/978-3-540-40974-8_29> 5. Saied Hosseini Khayat. Using Commutative Encryption to Share a Secret. (August 18, 2008) Availble: https://www.researchgate.net/publication/220334627\_Using\_Commutative\_Encryption\_to\_Share\_a\_Secret 6. Jordi Castella-Roca, Frances Sebe and Josep Domingo-Ferrer. Dropout-Tolerant TTP Free Mental Poker. (2005) Available : https://link.springer.com/chapter/10.1007/11537878\_4 7. Don Coppersmith. Cheating at Mental Poker Don Coppersmith. (1986) Availabe : https://link.springer.com/chapter/10.1007/3-540-39799-X\_10 8. Tzer-jen Wei. Secure and Practical Constant Round Mental Poker. (2014) doi: <https://www.researchgate.net/publication/262382779_Secure_and_practical_constant_round_mental_poker> 9. Jordi Castella-Roca, Vanessa Daza, Josep Domingo-Ferrer, Francesc Sebe. Privacy Homomorphisms for E-Gambling and Mental Poker. (2006) doi: <https://crises-deim.urv.cat/webCrises/publications/bcpi/IEEEhomomorphisms.pdf> 10. Weiliang Zhao, Vijay Varadharajan, Yi Mu. A Secure Mental Poker Protocol Over the Internet. (2003) doi: <https://researchers.mq.edu.au/en/publications/a-secure-mental-poker-protocol-over-the-internet>   Books:   1. Cryptography and Coding 2003, By Institute of Mathematics and Its Applications   (<https://link.springer.com/book/10.1007/978-3-642-10868-6>) |