An Efficient Poker Protocol for Shuffling and Dealing Cards

Zinah S. Jabbar, Sattar J. Aboud

Abstract: ***This paper proposes a new card game and dealing system, designed specifically for poker games. The proposed method benefits from two poker characteristics games that are ignored by public card systems. First, cards are dealt in poker games in the form of rounds, betting with them, instead of all at once. Second, the total number of cards dealt in poker game cards is depending on the number of players but is usually less than half the total. With these remarks in mind, the proposed method distributes the computing cost of dealing cards evenly across the rounds. Compared to systems that provide a full introduction to the deck, the proposed approach provides a significant reduction in the total cost of computing. Also, it's fair and strong. It perfectly fits hardware such as smartphones. The presented system is fast and secure mental poker protocol. It is twice as fast as similar protocols.***

Keywords**: public key encryption, system distribution, poker games, cryptanalysis.***

I. INTRODUCTION

The poker game is complicated but it is convenient and secure for multiparty cryptography protocols. Actually, poker systems are applicable until outside the domain of e-games, since many of the cryptography structures of poker are utilized in other multiparty computing implementations, such as e-voting systems, private multi-party trust computation, privacy-preserving clustering, and some other systems. It must differentiate between the poker systems, such as those based on trusted authority, and other systems that are free of a trusted authority. For example, Chou-Yeh in 2002 [1] stated that the trusted authority-based systems headed are more effective and the existence of trusted authority often provides the impression of justice of the players. But, in 1986 Crepeau [2] claimed that the useful poker systems must be devoid of any trusted authority. The aim as claimed is that anyone could be bribed, especially with no devices secure and without creating complete resistant programs yet to prevent tampering. Therefore, in the past ten years, there have been many types of research on poker systems without the adoption of trusted authority [3].

However, in this paper, the authors believe that in applied practice, the system should adopt trusted authority to calculate the public and private keys of the players, and distribute additive shares of private keys to the participants. However, this trusted authority must play a quite restricted function. It only participates in key generation and is then not ignored. This restricted assistance is for creating sets of users only.

Revised Manuscript Received on October 05, 2019.

Sattar J. Aboud, Information Technology College, Imam Ja'afar Al-Sadiq University, Baghdad-Iraq, sattar_aboud@yahoo.com

Zinah S. Jabbar, Information Technology College, Imam Ja'afar Al-Sadiq University, Baghdad-Iraq, sattarzeina@gmail.com

The proposed method of dealing with cards is easy in theory. Different to common systems, it does not shuffle the entire set of cards in the first step, since it is a time- consuming step. Instead, it creates the cards one after another once wanted. Allow range [1,...,52] to denote 52 cards in the deck. To create the card, users together calculate the encryption $e(c)$ for a random integer $c \in [1,...,52]$. At this time, the users compare an encoded message $e(c)$ to the entire encrypted cards $e(c_1),..., e(c_t)$ which previously dealt with a present game. When the match is obtained, the recently created card $e(c)$ is abandoned then the users attempt to create the card again. When a match is not found, the new card $e(c)$ is valid. To handle this, users decrypt the card and eject c. To deal face down, users assistance a card receiver decrypt them, so that the receiver realizes only c. This system is effective if the card numbers that have been dealt with in the game are small compared with the group of cards; almost all poker systems have this feature. It is inappropriate to deal with a full range of cards. Moreover, the computing cost of trading cards is not each gained in advance, but is distributed over multiple rounds of gaming, providing users with much less time than initial hiding. It will also be evident in the remainder of such article, that the system is special. No user or combination of users, lower than the threshold, can affect the card creation system, nor get something related to cards that have been distributed to other users. The proposed system is preferably suitable for resource-limited tools, for example next-generation of mobile phones.

II. RELATED WORKS

RSA introduced in 1979 [4] the first poker game that allows for two users to play the game only. Later, Goldwasser and Micali indicated that there is a security error in the RSA game [5]. However, Crepeau presented in 1987 [6] the first secure poker system. Subsequently, many other systems were offered. For example, in 2003 Zhao *et al* [7] proposed a free poker system that accommodates more than two users. But, in 2004, Roca and Ferrer [8] explained how they could attack this protocol and proposed a new system in 2004 [9]. Then, Zhao and Vadaharajan introduced in 2005 [10] a revised version of the system. But, Castella and Roca in 2006 [11] indicated that the revised version was insecure and resembled the RSA system.

In 2008, Chun and Chao [12] introduced a poker protocol to accomplish the distribution of encryption, detection and verification in an entirely distributed manner.

In 2012, Bayer and Groth [13] proposed a zero-knowledge proof of correctness for shuffle. But, their system needs a certificate that covers a public key utilized to create specific encryption messages and the generalized Pedersen commitment. In 2014, Wei and Wang [14] proposed another system. Inappropriately, the security examples utilized in this protocol have not been officially identified and appear to be somewhat weak according to the unofficial explanations provided via the creators. However, in 2017, Bentov *et al.* [15] introduced the result of the general probability that an unfair multiparty computation system using improved trapdoor permutations gives a security proof.

This paper is organized as follows. Section 2 reviews the relevant works. The full description of the proposed methodology is described in Section 3. Section 4 the result analysis of the protocol game that use a set of fifty-two cards. Finally, Section 5 is the conclusion.

III. THE PROPOSED METHODOLOGY

This section provides an outline of the proposed poker methodology. To handle with the card, users together create an encryption key e of a random number $c \in \{1,...,52\}$ without disclosing c. To avert dealing with the same card two times, users should make sure that the recently created card $e(c)$ does not resemble every one of cards now distributed. The problem is that such comparison concerning encoded cards should be completed in the manner that is not disclosed unless $e(c)$ is previously dealt with. When $e(c)$ is dealt with, users replicate the algorithm and attempt to obtain a fresh card $e(c')$ until one is discovered that is not yet dealt with. The full depiction of the system is as below. The system needs a public-key e beside the following characteristics:

- The public key and the private key of the protocols might be allocated amongst w challengers.
- The key encryption e is additively homomorphic, that is $e(m_1)e(m_2) = e(m_1 + m_2)$.
- Assumed two messages $e(c)$ and $e(c')$. Suppose that there is a system that permits to joint owners of the private key to see if $c = c' \bmod 52$ without disclosing any key.

The description of encryption systems with the above characteristics are in Sections 3. However, the trading card system is as follows**.**

Users together will share and create public and private keys. Each user obtains public keys and a share of the private keys. As soon as forming the group, the same public and private keys are reused to handle multiple cards. The poker system must be set up again only when the user exits, goes in as a new user or creates another group. Users retain the table $T = \{e(c_1),..., e(c_t)\}$ that comprises encrypting each card which has been traded of the existing group. Table T contains both face up cards and face down cards. If the new deck is formed, it will initialize to $T = 0$. Poker system handling card, if face-up or face-down is as follows:

1. Each user U_i selects $b_i \in \{1,...,52\}$, then calculates the encrypted message $e(b_i)$ and produces an inflexible commitment to $e(b_i)$.
2. Every user U_i then discloses $e(b_i)$, and each user must check that all the commitments are true. But, when any one of the commitments is wrong, the poker system terminates and the honest users set up a new group which eliminates the corrupt users.
3. By an additive homomorphism of e, the users calculate $e(c)$, such that $c = \Sigma_i b_i$
4. When $T \neq 0$ the users should check if the card $e(c)$ actually goes to T. For each encrypted message $e(c') \in T$, the users execute the multiparty protocol to check if $c = c' \bmod 52$. When there exists $e(c') \in T$ where $c = c' \bmod 52$, the users throw the card $e(c)$ and re-run the poker that deals with the card in step 1. Observe that the card $e(c')$ previously dealt with has not changed due to the collision.
5. The users add $e(c)$ to the table T. To handle the card at the top, the users decrypt $e(c)$ and give $c \bmod 52$. To deal face-to-face with user U_j, all users other than U_j partly recover $e(c)$ using the share secret key. A resultant encrypted message can be recovered by U_j only.

In the remainder of this paper, authors offer an encryption system with the needed features, testing the cost of computing to create a set, establishing a deck and dealing with the card. The collision numbers that deal with the f cards is around $\frac{1}{52}\left(\frac{f(f-1)}{2}\right)$ if f is much less than 52.

Also, the authors propose the applications of the poker game system to deal with cards based on the probabilistic public key encryption system published in 1994 [16]. The Benaloh system is more effective than the Elgamal encryption system published in 1985[17] since it provides a great benefit for producing an effective distribution key creation when using a reliable trusted authority. Assume that w indicates the user numbers. First, see the meaning and practical characteristics of the Benaloh system. The Benaloh is probabilistic cryptography, a semantically secure public key. This encryption system applies two of the three characteristics it needs. It is an additively homomorphic and permits for modular message comparison. Benaloh's probabilistic coding contains an added similarity coefficient; such that b is an odd number specifying the cryptographic function. For implementations, initialize $b = 53$ then, get the encryption system using mod 53 instead of 52. It is easy to handle this contradiction. The users insert a distinct card number 53 added to the table T in the deck preparation to ensure that they are not dealt with.

IV. THE ALGORITHM PROPOSED

The algorithms proposed are as follows:

Algorithm for Key Generation

The steps of the algorithm are as follows:

1. Selects a block size b ; // in this use $b = 53$
2. Selects two prime integers p, q ; // b divides $p-1$
3. Computes the $\gcd(b,(p-1)/b) = 1$; // is co-prime
4. Computes the $\gcd(b, q-1) = b$; // is co-prime
5. Computes the modulus $n = pq$;
6. Computes the phi $\theta = (p-1)(q-1)$;
7. Selects an integer $g \in Z_n^*$;
8. Checks that $g^{\theta/b} \neq 1 \bmod n$
9. Determines the public key by (n, g, b) ;
10. Determines the private key by $x = (p-1)(q-1)/b$;

Remark

There are many current protocols that deal with the RSA-key creation distribution. However, in this paper, none of these protocols will not adapt on the distributed key creation for probabilistic encryption because most of these protocols are not useful for practical usage. But, in practice should a trusted authority calculate (n, g) , and distribute additive shares of $x = (p-1)(q-1)/b$ for the users. Also, observe in this paper that the duty of the trusted authority is very restricted. It only engages in key creation and helps in creating groups of users and will never be used again.

Algorithm for Encryption

The steps of the algorithms are as follows:

1. Selects an integer message $m \in Z_b$;
2. Selects an integer number $s \in Z_n^*$;
3. Computes the randomized encryption of m by $c(m) = g^m s^b \bmod n$;
4. Now, it is easy to check: $c(m_1) \times c(m_2) = c(m_1 + m_2)$;

Algorithm for Decryption

The steps of the algorithms are as follows:

1. Considers encrypted message $c(m) = g^m s^b \bmod n$;
2. Recovers that $x = (p-1)(q-1)/b$;
3. Considers that $c(m)^x = g^{mx}$;
4. Creates table of items $g^x \bmod n$ for $m \in \{1,...,b-1\}$;
5. Decrypts a message $c(m)$ via searching for the item $c(m)^x \bmod n$ on a table;

Notes

1. Suppose that $m_1, m_2 \in Z_b$, assume that $a_1 = c(m_1)$ with $a_2 = c(m_2)$. Then, it is straightforward to check that $a_1 a_2 = c(m_1 + m_2)$.
2. Assume that $c(m_1)$ and $c(m_2)$ are two encrypted messages. The objective is to see if $m_1 = m_2 \bmod b$ apart from disclosing any data. Users initially calculate $c(m_1)/c(m_2) = c(m)$, where $m = m_1 - m_2 \bmod b$. The challenge is to see if $m = 0 \bmod b$. Adequate, every user U_i selects $d_i \in \{1,...,52\}$ then computes $c(m)^{d_i} \bmod n$.
3. Assume that $d = \Sigma_i d_i$. User $\prod_i c(m)^{d_i} = c(m)^d$. Observe that $c(m)^d = g^{md} s^{bd} \bmod n$ and so $c(m)^d$ is the encoding of $md \bmod b$. Also, because $b = 53$ is prime in this implementation, $md = 0 \bmod b$ when $m = 0 \bmod b$. But, for $m \neq 0 \bmod b$, the result md is regularly spread to $\{1,...,52\}$.
4. Users will decode $c(m)^d$ and produce $m_1 = m_2 \bmod b$ when $md = 0 \bmod b$. The computing cost of dealing with the card of this protocol is $4k|T|/(1-|T|/52)$.

V. THE RESULT ANALYSIS

Finds a private key $n = pq = 241 \cdot 179 = 43139$, assume that $b = 15$. Algorithm 1 can be utilized to calculate the best appropriate value of b when begin selecting randomly two prime numbers p and q , nonetheless a smoother and minor number can be employed as an alternative, for the uncomplicated decryption.

Algorithm 1 to calculate b

```
b := p − 1 ;
while gcd(q − 1, b) ≠ 1 do
        b := b / gcd(b, q − 1) ;
end ; // while
```

Check that $b = 15$ divides $p-1 = 240 = 16 \cdot 15$, b then $(p-1)/b = 16$ are co-prime, $b = 15 = 3 \cdot 5$ and $q - 1 = 178 = 2 \cdot 89$ are relatively prime. Suppose that $g = 27$, with $\gcd(g, n) = 1$ then $g^{\theta/b} 40097 \neq 1 \bmod n$ thus as stated by Benaloh key creation method that the new requirements are accepted.

Therefore, $g^1 12^b = 24187 \bmod n$ is a true encoding of $m_1 = 1$, whereas $g^6 4^b = 24187 \bmod n$ is also a true encoding of $m_2 = 6$. Actually, check that with this selection of g , the real message space is now Z_5 rather than Z_{15} therefore the vagueness in decoding. Observe that in Z_p $g^5 = 27^5 = 8 = 41^{15} = 41^b$. This requires that a true encoding of 5 is also a true encoding of 0 . For clear-text m , the group of encoding of m is equal the group of encoding of $m+5$, therefore a failure in clear-text space. The clear-text space that is not failure can be verified by brute force with this slight set of keys.

In this select of p and q, there are $\frac{b-1}{b}\theta(n) = 39872$ probable values of g as said by the first paper, but 17088 of them will cause the vagueness in decoding, that a percentage of $3/7$, reducing the message space to both Z_3 or Z_5.

The authors, in this paper look at games that play with a collection of fifty two cards. Observe that this paper just focuses on distributing cards and casino rounds that can have effect on round communication numbers. For instance, the total cost of computing for shuffling and dealing cards in one Texas Holdem game is amongst the 5 users, 59% lesser with the proposed system compared to the most effective systems. The first standby time prior to the initial round of games is 76% lesser. The proposed system provides similar developments for 7 card stud and other poker systems [18].

At first, two cards are allocated face-to-face every user and a round of games follows. Then, in the middle of the desk, 3 cards remain handled together. There will be an additional round of gaming. After that extra gambling round, one more card is allocated in the middle. On the other side, in the center, the last card remains handled face up, after last round of game. Every user handles seven cards, start by two face-down cards and one face-up card. At that point, every face-up user is handled by 3 additional cards, then betting rounds among them. At that point, the last card remains handled face-down, trailed via the last gaming round.

The table below indicates the total cost of w user game, estimated to the extent that every user is required to achieve the amount of exponentiations. The first segment displays a mix-net solution expense. The subsequent segment indicates the cost of the proposed system being executed in dense probabilistic encryption. The expenses of a Texas Holdem coordinate with three and five users individually. Fundamentally the same as outcomes are gotten with 7 card stud. The dense probabilistic encryption application of the proposed system is the best useful via a broad margin, but it depends on a trusted authority for original key creation.

Table- I: Shows the total cost of w user game

System	Encryption Scheme	
	Mix-network	***Dense Probabilistic Encryption***
Texas Holdem with 3 users		
Deck preparing and first round	3912	193
Extra round	25	204
Texas Holdem with 5 users		
Deck preparing and first round	5457	975
Extra round	35	654

VI. CONCLUSION

The authors in this paper proposed a fresh system intended specifically of poker games 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. The proposed system is ideal for systems that are resource-limited.

ACKNOWLEDGMENT

The Authors wish to extend their thanks to the University of Imam Ja'afar Al-Sadiq, at Baghdad-Iraq, Faculty of Information Technology for their help suggestions and their financial support.

REFERENCES

1. Chou J., and Yeh Y., "Mental poker game based on a bit commitment scheme through network", Computer Networks, vol. 38, pp. 247-255, 2002.
2. Crepeau C., "A secure poker protocol that minimizes the effect of player coalitions", in Advances in Cryptology CRYPTO'85, LNCS 218, pp. 73-86, 1986.
3. Bernado David, Rafael Dowsley, Mario Larangeira, "Kaleidoscope: An Efficient Poker Protocol with Payment Distribution and Penalty Enforcement", Financial Cryptography and Data Security 2018.
4. Shamir A., Rives R., Adelman L., "Mental Poker", this report was prepared with the support of MaUona1 Science Foundation grants No.'s MCS78—05849 and MCS78—04343; and by the Office of Naval Research under contract No. 1979.
5. Goldwasser S., Micali S., "Probabilistic encryption & how to play mental poker keeping secret all partial information", Proceedings of the fourteenth annual ACM symposium on Theory of computing, pages 365377, 1982.
6. Crepeau C., "A zero-knowledge Poker protocol that achieves confidentiality of the players' strategy or How to achieve an electronic Poker face, Proceedings on Advances in cryptologyCRYPTO'86.
7. Zhao W., Vadaharajan V., Mu, Y., "A secure mental poker protocol over the Internet", Australasian Information Security Workshop, vol. 21 of Conferences in Research and Practice in Information Technology, pp. 105-109, Adelaide, Australia: Australian Computing Society, 2003.
8. Castella Roca, Domingo Ferrer, "On the security of an efficient TTP-free mental poker protocol", International Conference on Information Technology: Coding and Computing, 2004, Proceeding, ITCC 2004, IEEE.
9. Castella-Roca, "Contributions to Mental Poker", Thesis, 2004.
10. Zhao W., Varadharajan V., "Efficient TTP-free mental poker protocols", in Proceedings of ITCC'2005, Los Alamitos CA: IEEE Computing Society, vol. 1, pp. 745-750, April 2005.
11. Castella-Roca, Domingo-Ferrer, Sebe F., "On the Security of a Repaired Mental Poker Protocol", Proceedings of the Third International Conference on Information Technology: New Generations (ITNG'06)-Volume 00, pages 664668, 2006.
12. Chun-Chao, "Secure and verifiable P2P Cards Games", IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2008.
13. Stephanie Bayer, Jens Groth, "Efficient zero-knowledge argument for correctness of a shuffle", Advances in Cryptology – EUROCRYPT 2012, volume 7237 of Lecture Notes in Computer Science, pp. 263–280, Cambridge, UK, April 15–19, 2012, Springer, Heidelberg, Germany.
14. Tzer-jen Wei, "Secure and practical constant round mental poker", Information Sciences, 273:352–386, 2014.
15. Iddo Bentov, Ranjit Kumaresan, Andrew Miller, "Instantaneous decentralized poker", eprint.iacr.org/2017/875
16. Benaloh J., "Dense probabilistic encryption", In Proceedings of the Workshop on Selected Areas in Cryptography 1994, pages 120–128.
17. ElGamal T., "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, 31(4):469–472, Jul 1985.
18. Sattar J. Aboud, Mohammad A. AL-Fayoumi, "An Efficient Internet Bingo Scheme", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014.

AUTHORS PROFILE

Zinah S. Jabbar is a lecturer in Information Technology College, University of Imam Ja'afar Al-Sadiq, Baghdad-Iraq. **Zinah** specializes in Databases, Information Security and Cryptography and she holds a first-class BSc in Computer Science, and MSc in Databases. **Zinah** currently is a Lecturer and conduct her research at the Information Technology College, University of Imam Ja'afar Al-Sadiq. **Zinah** has delivered a range of hand-on technical training on topics such as Database Security as part of a proactive approach to protect computer systems. She has many years of experience with the University of Imam Ja'afar Al-Sadiq.

Also, she has leading IT training courses in Lab. Earlier in her career; she was a lecturer at the School of Computer Science and Technology, Al Rafidain University College. She has published numerous professional and peer-reviewed articles. Her research interests include Databases Security, Applied Cryptography Schemes and Security for Cyber-Physical Systems. Additionally, **Zinah** is interested in multidisciplinary projects to mitigate cyber-related challenges such as online anti-social behavior. By the end of 2019, **Zinah** has supervised 20 BSc final year projects to successful completion

Sattar J. Aboud is a full professor in Information Technology College, University of Imam Ja'afar Al-Sadiq, at Baghdad-Iraq. Sattar specializes in Information Security and Applied Cryptography and holds a first-class Postgraduate Diploma in Computing Science, and PhD in Computing Systems, both degrees from Glasgow University, UK. Sattar is a full professor and conduct his research at the Faculty of Information Technology; University of Imam Ja'afar Al-Sadiq, Baghdad-Iraq. Sattar has delivered a range of hand-on technical training on topics such as Encryption Schemes, Digital Signature Schemes, Authentication and Identification Protocols, Algorithms Analysis and Design, Information Security Management, Network Security, Cyber security including Ethical Hacking as part of a proactive approach to protect computer systems. He has more than 30 years of experience with Transnational Education as a Link-coordinator of franchised courses and a flying faculty team, supported MSc and PhD programs at many Universities, as well as delivering Executive Master's degrees in Cyber security through leading IT training providers in the UK such as QA Ltd. He has published more than 150 professional and peer-reviewed articles. His research interests include Asymmetric Encryption, Digital Signatures, User Authentication Methods, Cyber Security and Security for Cyber-Physical Systems. Additionally, Sattar is interested in multidisciplinary PhD and MSc projects to mitigate security-related challenges such as Authentication Protocols. By the end of 2018, Sattar has supervised and exam more than 150 PhD and MSc dissertations to successful completion. His interest in a broad range of collaborative activities has led to work with national and international researchers to publish in leading journals and to write proposals addressing funding calls, in total he has assisted in the generation of over $3m. Within his area of expertise, he has also worked with new businesses, to launch new products, and authored 6 chapters in books by the end of 2017. His quality work has attracted various awards, recent recognitions include a Best Conference Paper Award in 2016, nomination by University of Bedfordshire, and to a Student Led Teaching Award in 2003 by the University of Philadelphia. When Sattar has free time, he enjoys reading, walking, and travelling.