Towards Privacy Preserving Commutative Encryption-Based Matchmaking in Mobile Social Network

Fizza Abbas[1], Ubaidullah Rajput[1], Adnan Manzoor[2], Imtiaz Ali Halepoto[1], Ayaz Hussain[3]
[1]Department of Computer Systems Engineering, Quaid e Awam UEST, Nawabshah, Pakistan
[2]Department of Information Technology, Quaid e Awam UEST Nawabshah, Pakistan
[3]Department of Electrical Engineering, Balochistan University of Engineering and Technology, Khuzdar, Pakistan

***Abstract*—The last decade or so has witnessed a sharp rise in the growth of mobile devices. These mobile devices and wireless communication technologies enable people around the globe to instantaneously communicate with each other. This leads to the emergence of a new type of social networking known as Mobile Social Network (MSN). MSN offers a wide range of useful applications, such as group text services, social gaming, location-based services (to name a few). One of the popular applications of MSN is matchmaking where people match their interests/hobbies to find the like-minded people for a possible friendship. However, revealing personal hobbies can pose significant threats on a user's privacy. Therefore, a privacy preserving evaluation method is needed to find the similarity between users' interests. There are various techniques to achieve privacy preserving matchmaking, such as commutative encryption, oblivious transfer and homomorphic encryption. This paper discusses the feasibility of commutative encryption by evaluating recently proposed schemes. The paper attempts to identify various shortcomings in the present work and discusses future directions.**

***Keywords*—Privacy; security; matchmaking; interests; mobile social network**

I. Introduction

A Mobile Social Network (MSN) enables its users to make social ties between them using mobile devices and communication technologies [1]. MSN offers many useful applications such as locations-based services where nearby people share their experiences about restaurants, shopping malls, and social gaming that allows friends to play online games with each other (to name a few). One of the most popular applications of MSN is matchmaking where people find the similarity between their profiles to establish a possible friendship. Peoples' profiles consist of personal information such as political affiliations, sexual orientation and health status etc. Disclosure of such information to a stalker may seriously jeopardize the privacy of a user. In recent past, many researchers have proposed privacy preserving matchmaking schemes to privately evaluate the interest-wise similarity between their profiles. We can classify these techniques as a private set intersection (PSI) or private cardinality set intersection (PCSI) problem [2], [9], [10]. These techniques take their notion from the set theory where intersection operation is used to find the common elements in the sets. Here, private set intersection refers to the oblivious evaluation of intersection operation. There are other techniques to blindly calculate the similarity such as cosine similarity can be used with the help of homomorphic encryption which incurs significant communication and computation costs. Moreover, it does not find interest to interest matching rather it calculates a similarity score [3], [4].

The remaining paper is organized as follows. The succeeding section discusses commutative encryption-based matchmaking protocols and their limitations. Section 3 provides the discussion. Section 4 concludes the paper along with future work.

II. Matchmaking Protocols

In this section, we discuss various commutative encryption-based protocols. Notations used in this paper are shown in Table I.

A. Agrawal et al. Protocol

Agrawal et al. presented the pioneer work regarding the commutative encryption. Originally, their work was intended to information sharing in between private databases [5]. They formulated their matching problem as a PSI problem. In case, the evaluation only finds the number of matches, the problem becomes PCSI. PSI and PCSI find the similar objects blindly [9], [10].

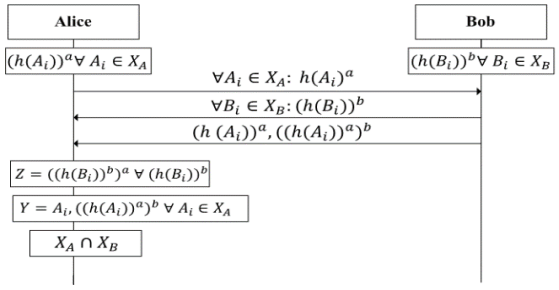

Fig. 1. Working of Agrawal et al. protocol [5].

The protocol proposed by Agrawal et al. uses the power function $f_e(x) = x^e mod\ p$ that has commutative properties i.e. the order of encryption is independent. Therefore, its security is based on Decisional Diffie-Hellman hypothesis (DDH). Suppose that a is the secret key of Alice, b is the secret key of Bob and m is the message then $((msg1)^a)^b = ((msg2)^b)^a, iff\ msg1 == msg2$.

TABLE I. NOTATIONS

Notations	Explanation
Alice	The protocol initiator
Bob	Responder
i	Index
X_A	Set containing Alice interests
X_B	Set containing Bob interests
A_i	i_{th} interest Alice
B_i	i_{th} interest Bob
a, b	Secret key of Alice and Bob respectively
h	Hash
PK_A, PK_B	Public key of Alice and Bob respectively
SK_A, SK_B	Secret key of Alice and Bob respectively
SK_{PIS} SK_{VS}, SK_{IdV}	Private key of third party server

A user's profile, consists of i number of interests require i number of modular exponentiations. The working of Agrawal's protocol is shown in Fig. 1. In this figure, we have two users Alice and Bob, each having i number of interests, who want to securely compute the intersection of their interests. First, Alice and Bob exponentiate (encrypt) their interests with their respective keys and exchange the exponentiated interests. After that, Bob commutatively exponentiates Alice's interests with his key and then makes pairs of each of these commutatively exponentiated interests and corresponding Alice's exponentiated value. Bob sends all these pairs to Alice. Similarly, Alice commutatively exponentiates Bob's exponentiated values with her key. If her commutative encryption matches with those sent by Bob, then Alice identifies it with the first element of the pair. However, there are many possible attacks on this scheme. Firstly, an attacker can freely choose his/her interests during various runs of the protocol against the same user and eventually finds all the interests of the victim. Secondly, there is no limit on the number of interests. Therefore, an attacker can form a very large set of interests that include nearly every possible interest.

There is a strong chance that victims set will become a subset of attacker set and the attacker will know all elements of victim's interests.

Another drawback is that the initiator only learns the result of the evaluation. This allows an adversary to learn the results and then run away without running the protocol as a responder. Finally, Bob can reorder the pairs $(h(Ai))^a, ((h(Ai))^a)b$. Therefore, Alice incorrectly identifies the matched interests.

B. Xie et al. Protocol

Xie et al. [6] identify the attacks on Agrawal's protocol and propose their protocol to overcome the shortcomings of [5]. In their protocol, they utilize two trusted servers. One is used to certify a user and the other is used to certify the interests of a user. The protocol in [6] uses commitments to ensure that any of the user should not be able to malicious reorder the encrypted interests' pairs in step # 5. Once the intersection has been computed and mutual interests are identified, both Alice and Bob exchange the matched interests though a shared secret computed with the help of Diffie-Hellman exchange to ensure each other that both have computed the same result. Fig. 2 shows the complete working of [6]. Although this protocol offers improvements over Agrawal's protocol, but it introduces new attacks and fails to prevent some attacks that were also present in [5]. First, the protocol of Xie et al. uses two servers and therefore, assumes that both the servers are fully trusted. These servers contain critical user identity and interests' information and in case of a compromise, the privacy of the participants may severely jeopardized. Another major drawback of [6] is that it does not prevent the attack where any of Alice and Bob reorders the pair $(h(Ai))^a, ((h(Ai))^a)^b$. The protocol assumes that such attack can be detected in the end where Alice and Bob exchange the interests. However, once Alice receives maliciously reordered interests from dishonest Bob, then she will send those same presumed interests to Bob in the shared key. Bob will decrypt the message and will simply send those interests back to Alice and trick her to believe that the matching was successful.

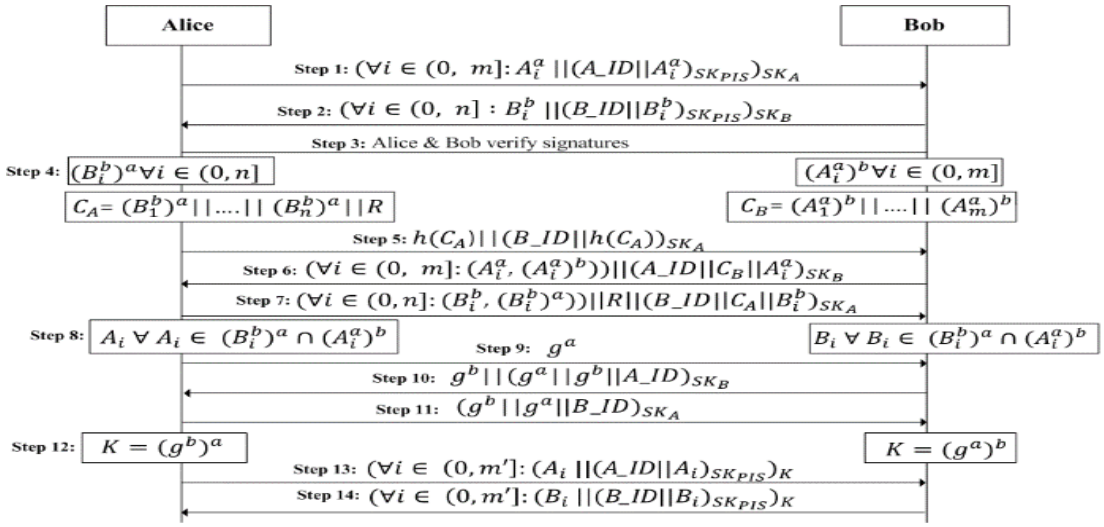

Fig. 2. Working of Xie et al. protocol [6].

Moreover, the protocol does not prevent from the attack where a malicious Alice will send gibberish values to Bob in step # 5 and then actual gibberish values in step # 7. Due to exponentiation, Bob will be unable to know the values are gibberish and will take it as an unsuccessful match. Therefore, Alice will learn the number of matched interests and Bob will know nothing.

C. Wang et al. Protocol

Wang et al. [7] proposed another protocol that attempt to overcome the shortcomings of both [5] and [6]. First, the protocol in [7] combines the two trusted servers into a single server. Second, their protocol allows an initiator to run the protocol with several candidates in the first stage and finds the one candidate, described as the best match, with the most number of matches. Once the best candidate is found, the protocol proceeds almost in the same way as of [6]. However, in the end, instead of exchanging matched interests in a shared key, both Alice and Bob send the result to the trusted server that verifies the result and sends one's result to other. The Wang's protocol is given in detail in Fig. 3.

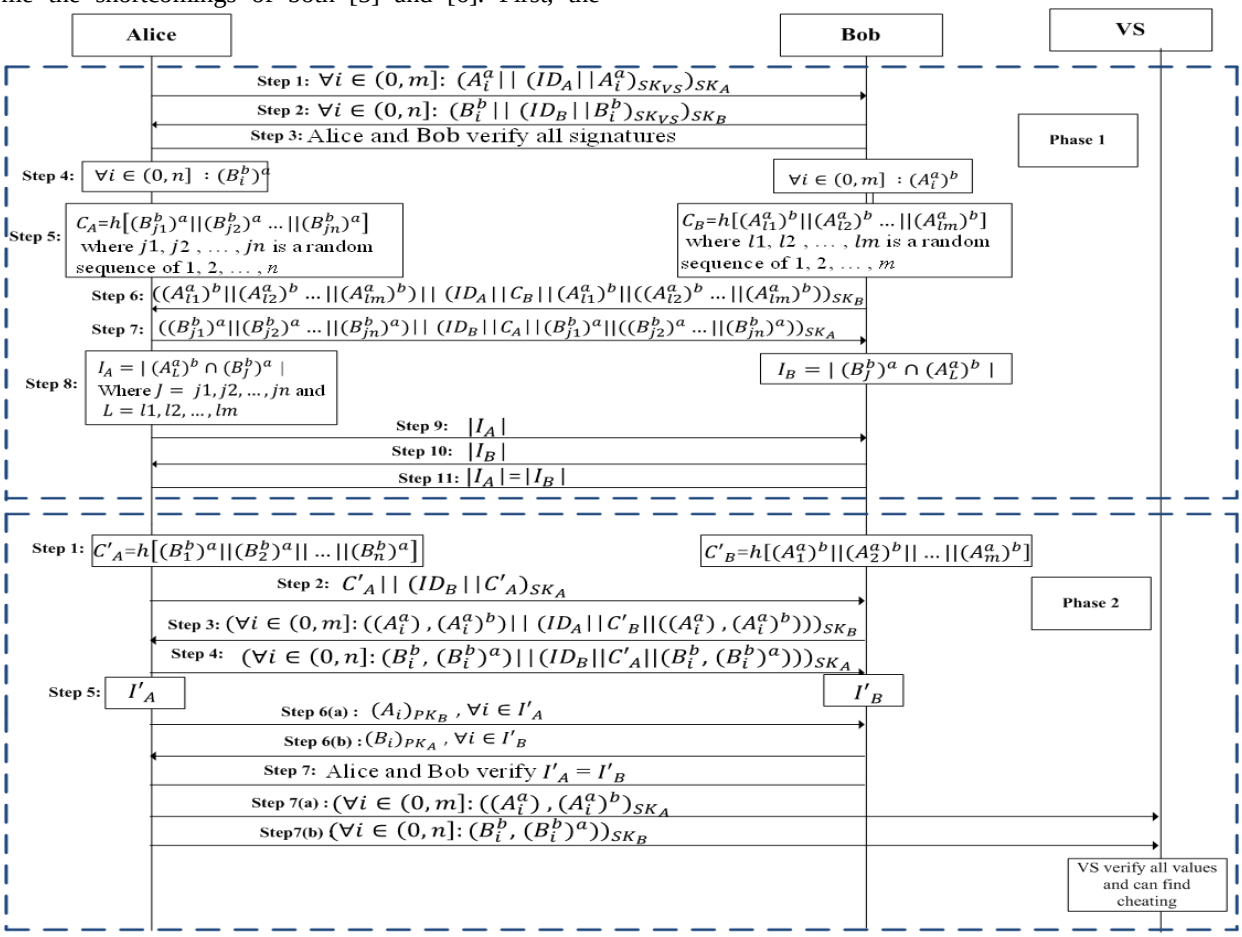

Fig. 3. Working of Wang et al. [7].

The protocol attempts to provide improvements over Xie's protocol. However, the main contribution seems to be the idea of finding the best match among a number of candidates. Many of the attacks on [6] are also possible in [7]. The unified servers till requires full trust of users, indeed, in the end of the protocol, the trusted server knows the result as well. Alice still can send the gibberish values to Bob and remains undetected. In the result, Alice knows the number of matched results. Similarly, the detection of cheating is not possible when both users exchange the actual interests in each other's public key. The malicious user will simply receive the actual values and send them back to other.

D. Fizza et al. Protocol

The authors of [8] propose a protocol to improve the work of [6] and [7] as shown in Fig. 4. They reduce the trust on server by restricting the role of server in only verifying the number of interests of user. The server does not know the actual interests' values. Author in [8] uses the idea of introduces dummy interests in the interest set of both users. These dummy interests are known to both Alice and Bob but their relevant position in the set is only known to the set holder. Therefore, the gibberish values attack is nullified as the malicious user must correctly guess the position of dummy interests in the set which is very hard to guess. Moreover, author in [8] introduces a hash-based advantage less mechanism for interests exchange that ensures to find any mismatch in the exchanged results. However, one the drawback of [8] is the extra cost of exponentiating the dummy interests and the extra exchanges of commitments during the exchange of actual interests.

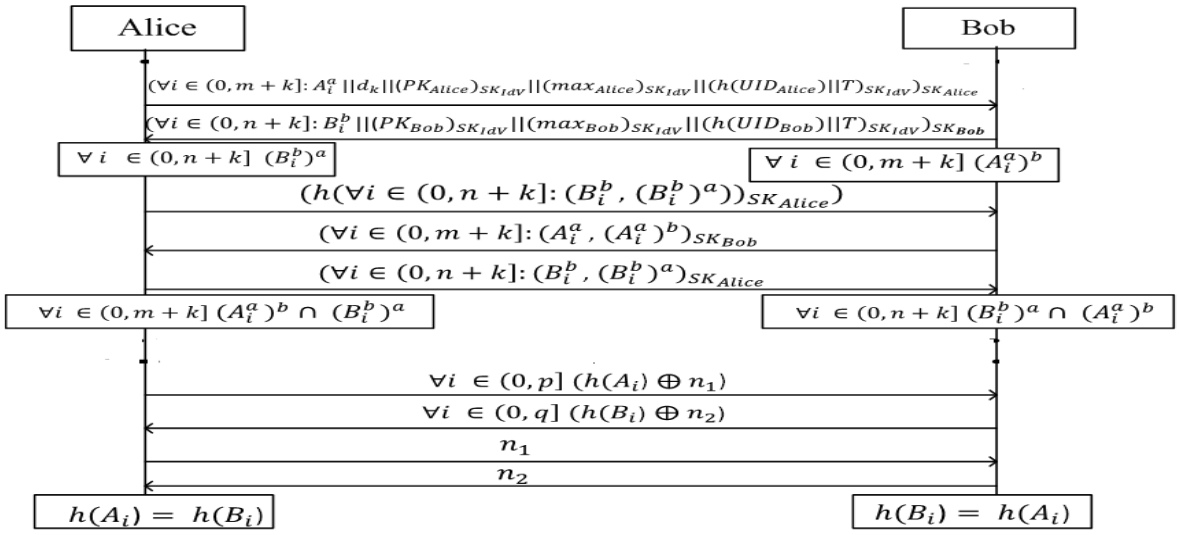

Fig. 4. Working of Fizza et al. protocol [8].

III. Discussion

By looking at the literature survey it is evident that the commutative based encryption can provide significantly fast and reasonably secure PSI and PCSI based intersections. The protocols proposed for privacy preserving matchmaking based on commutative encryption have been increasingly secure. However, we a tradeoff where increased security and privacy requires increased computational and communication cost. The protocols in [5] paved the way for secure commutative based matchmaking. The protocols [6] and [7] improved the functionality and shortcomings of [5]; however, they introduced trust related issues as well as allowed malicious users to go unnoticed after cheating. The authors of [8] successfully eliminated above mentioned flaws but their protocol is slightly costlier in terms of communications and computation. Nonetheless, by keeping in mind the ever-increasing computing and communication capabilities of devices and telecommunication networks, these costs can be neglected by comparing the benefits being offered.

In future, there is need to improve the state of the art protocols by keeping the cost as low as possible. This becomes more significant because mostly matchmaking applications are designed for the people on the move carrying handheld devices and therefore, it required the matchmaking protocols to be light weighted both in terms of computation and communication.

IV. Conclusion

Matchmaking is one the famous application of mobile social network. Users share their private information with each other. To preserve users' privacy during matchmaking is not a trivial task. Therefore, many matchmaking protocols are proposed. This paper provides working of Agrawal et al., Xie et al., Wang et al. and Fizza et al. along with their limitations. In the end, a comparison is presented that compares the state of the art along with the benefit they offer over each other. Finally, the paper signifies the need of light weight matchmaking protocols as possible future research directions.

References

[1] Y. Najaflou, B. Jedari, F. Xia, L. T. Yang, and M. S. Obaidat :safety challenges and solutions in mobile social networks," IEEE System Journal, vol. 9, no.3, pp. 834-854, 2015.

[2] N. Kayastha, D. Niyato, P. Wang, and E. Hossain, " Applications, architecture, and protocol design issues for mobile social networks: A survey," Proceessings of the IEEE, vol. 99, no. 12, pp. 2130-2158, 2011.

[3] L. P. Cox, A. Dalton, and V. Marupadi, "Smokescreen: flexible privacy controls for presence-sharing," in Proceedings of the 5th international conference on Mobile systems, applications and services. ACM, pp. 233–245, 2007.

[4] X. Hu, T. H. Chu, V. C. Leung, E. C. H. Ngai, P. Kruchten, and H. C. Chan, "A survey on mobile social networks: Applications, platforms, system architectures, and future research directions," IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1557–1581, 2015.

[5] R. Agrawal, A. Evfimievski, and R. Srikant, "Information sharing across private databases," in Proceedings of the 2003 ACM SIGMOD international conference on Management of data. ACM, pp. 86–97, 2003.

[6] Q. Xie and U. Hengartner, "Privacy-preserving matchmaking for mobile social networking secure against malicious users," in Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference. IEEE, pp. 252–259, 2011.

[7] Y. Wang, J. Hou, Y. Xia, and H. Li, "Efficient privacy preserving matchmaking for mobile social networking," Concurrency and Computation: Practice and Experience, vol. 27, no. 12, pp. 2924–2937, 2015.

[8] F. Abbas, U. Rajput, and H. Oh, "Prism: Privacy-aware interest sharing and matching in mobile social networks," vol. 4, pp. 2594–2603, 2016.

[9] M. J. Freedman, K. Nissim, and B. Pinkas, "Efficient private matching and set intersection," in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, pp. 1–19, 2004.

[10] C. Hazay and Y. Lindell, ``Efcient protocols for set intersection and pattern matching with security against malicious and covert adversaries," in Proc. 5th Conf. Theory Cryptogr. (TCC), pp. 155-175, 2008.