ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Explicit & Implicit Protocal Based Profile Matching With Privacy Preservation in Mobile Social Networks Anonymously

Nandini
PG Scholar,
Dept of CSE,
B.I.T. Institute of Engineering & Technology,
Hindupur, AP, India.

Parthu Vijay
Associate Professor,
Dept of CSE,
B.I.T. Institute of Engineering & Technology,
Hindupur, AP, India.

Abstract:

This paper matching user profile with privacy preservation in mobile social networks (MSN) is studied and we introduce a family of protocols that match the novel profile. First, we propose an explicit protocol based on a comparison of the profiles matching (eCPM) extending between two parts, an initiator and a responder. The eCPM allows the originator to obtain the matching result based on the comparison of an attribute specified in their profiles, while preventing their attribute values disclosure. We then propose a match based on implicit comparison protocol profile (iCPM) that allows the originator for some messages directly instead of comparing the result of the response. The messages not related to the user profile can be divided into several categories by the responder. The initiator interested implicitly chooses the category that is unknown to the responder.

Two posts in each category are made by the respondent, and only one message can be obtained by the initiator according to the comparison result on a single attribute. ICPM further generalize a protocol based on Predicate Matching Profile implicit (MIPP) that allows comparison of complex criteria involving multiple attributes. The analysis shows the anonymity of these achieve the confidentiality of user profiles protocols. Furthermore, the eCPM reveals the result of the comparison for the initiator and provides only conditionally anonymous; The ICPM and IPPM not reveal the results at all and allow complete anonymity. We analyze the communication overhead and the strength of the anonymity protocols. Here, we present an improved version of eCPM, eCPM called +, eCPM combining strategy with a novel pseudonym based adaptive change predictions. Performance and eCPM + eCPM is comparatively studied through extensive simulations based on traces. Simulation results show that the eCPM + achieves significantly stronger anonymity with a slightly larger number of nicknames that the eCPM.

Keywords:

Mobile Social Network, Profile Matching, Privacy Preservation, Homomorphic Encryption, Oblivious Transfer.

I. INTRODUCTION:

Social networking makes digital communication technology tools to expand the social circle of people sharpening. It has already become an integral and important part of our daily lives, allowing us to contact our family and friends in time. As reported by ComScore [1], the social networking sites like Facebook and Twitter have reached 82 percent of the world's online population, representing 1.2 billion users around the world. Meanwhile, driven by the widespread adoption of advanced hand devices and ubiquitous network connections Bluetooth / WiFi / GSM / LTE, the use of mobile social networking (MSN) has exploded. In MSN, users are able to not only surf the Internet, but also communicate with their peers in the vicinity that use the short-range wireless communications [2] - [6]. Due to its geographical nature, the MSN support many promising and innovative applications[7]-[12]. For example, through the Bluetooth communications, People Net [7] allows searching for effective information between mobile

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

phones neighbors; A message-relay approach is suggested in [8] to facilitate ride sharing and ride sharing in a local region. Realizing the potential benefits presented by MSN, recent research efforts have been made on how to improve the effectiveness and efficiency of communications among users of MSN [9], [11], [12]. They developed specialized routing protocols and data forwarding associated with the social characteristics exhibited by the behavior of users, such as social friendship, [9], social selfishness [11] and social morality [12]. It is encouraging that traditional solutions can be expanded further to troubleshoot MSN, considering the unique social characteristics.

Privacy preservation is an important research topic in social networks. Given that more personal information is shared with the public, violating the privacy of a target user is much easier [13] - [17]. Research efforts [13], [14], [17] have been put into the presentation of identity and privacy issues on social networking sites. Gross and Acquisti [13] argued that users are jeopardizing both offline (eg, stalking) and online (eg, identity theft) based on an analysis of the behavior of more than 4,000 students they have joined a popular social network. Stutzman [14] presented a quantitative analysis of identity information disclosure in social network communities and the subjective opinions of students regarding the identity protection and information disclosure. When social networking platforms extend into the mobile environment, users require more extensive privacy preservation because they are unfamiliar with neighbors nearby that can spy, store and correlate their personal data in different periods and places.

Once personal information is correlated with the location information, the user behavior will be fully disclosed to the public. Chen and Rahman [17] studied various mobile social networking applications (SNAS), such as neighborhood exploring applications for mobile and SNAs specific content sharing applications, which do not provide feedback or control mechanisms for users and can cause localization inappropriate and identity information disclosure.

To overcome the violation of privacy on MSN, many techniques of privacy have been taken in MSN [4] applications, [12], [17] - [23]. For example, when two users are on the MSN, privacy-preserving matching profile acts as a critical first step to help users, especially to strangers, initialize the conversation with others in a manner and privacy preserving distributed. Many research efforts on privacy preserving matching profile [20] - [23] have been carried out. The common objective of these works is to allow the handshake between two users found if users meet the requirement of one another, while eliminating unnecessary disclosure of information if they are not. The original idea of [18], where an agent of the Central Intelligence Agency (CIA) wants to authenticate herself to a server, but does not want to show their CIA credentials unless the server is a shot of the CIA authentic.

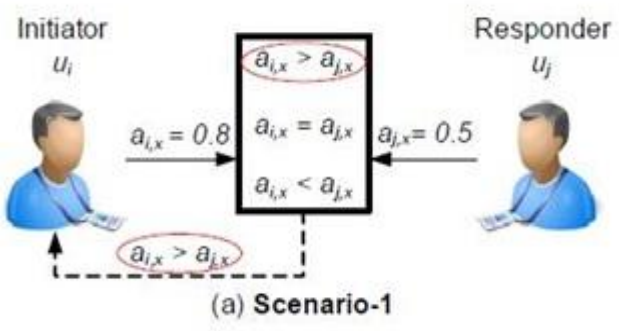
Meanwhile, the server does not want to reveal its CIA credentials to anyone but CIA agents. At MSN, we consider a generalized function to support the exchange of information through the use of a matching profile as a metric. Following the above example, two CIA agents are considered with two different priority levels in the system of the CIA, *A* with a low priority l_A and *B* with a high priority l_B. They are known as an agent of the CIA. However, they do not want to reveal their levels of priority among them. B wants to share some messages to A. The messages are not related to the user profile, and are divided into several categories, for example, messages related to the different regions (New York or Beijing) in different years (2011 or 2012).

B shares a message of a certain category T at once. T category is chosen, but the choice is unknown to B. For each category, B makes two self-defined messages, for example, a low confidential message for the CIA at a lower level and high confidential message for the agent on a higher level. Because $l_A > l_B$, *A* eventually obtains the low-confidential message without knowing that it is a low confidential one. In the meantime, *B* does not know which message *A* receives. The above function offers both A and B the highest anonymity since neither the comparison result

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

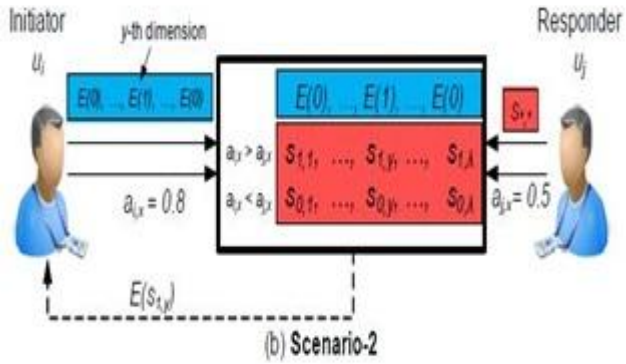
between and is disclosed to *A* or *B* nor the category *T* of *A*'s interest is disclosed to *B*. In the following, we refer to *A* as the initiator *B* as the responder, the attribute used in the comparison (i.e., priority level) as *ax*, and the category *T* of *A*'s interest as T_v. The attribute values of u_i and u_i on the attribute *ax* are denoted by $a_{i,x}$ and $a_{j,x}$, respectively. We first formally describe two scenarios from the above examples.

Scenario-1: The initiator wants to know the result of the comparison, that is, if you have a larger, equal, or less than the responder in a specified attribute value.



(a) Scenario-1

Scenario-2: The initiator expected response actions of a message related to the category of your interest, yet remains unknown to the responder. Meanwhile, the responder wants to share with the originator of a message is determined by the result of the comparison of their attribute values.



(b) Scenario-2

II. RELATED WORK:

Mobile social networking and emerging social media platforms[27]-[29] have attracted much attention recently, and mobile applications have been developed and pervasive practice. In applications of mobile social networks, matching profile acts as a critical first step to help users, especially to strangers, initialize the conversation with others in a distributed manner. Yang et al. [30] introduced a mobile communication system distributed, called E-Small Talker, which facilitates social networking in physical proximity. E-Small Talker automatically discovers and suggests common themes among users to facilitate the conversation. Lu et al. [20] studied the case of e-healthcare by proposing a scheme to compensate for the symptoms of social networks of mobile health. In his opinion, this game system is valuable for patients with the same symptoms to exchange their experiences, mutual support, and inspiration to others.

In general, the matching profile can be categorized based on the formats of the profiles and the types of gambling operations. A well-known coincidence profile FNP scheme [19], where a client and a server to calculate the intersection set so that the client gets the result, while the server learns nothing. Later Kissner et al. [31] applied a matching profile with several operations including set intersection, union, cardinality and excess threshold operations. Moreover, Ye et al. [32] further extended the FNP scheme with a scheme of private correspondence and distributed Dachman-Soled et al. [33] designed to reduce protocol complexity. All the above solutions to the set intersection operation depend homomorphism encryption.

Meanwhile, other studies [34], [35] use an oblivious pseudorandom function to build their profile matching protocols where communication and computational efficiency is improved. Li et al. [21] implemented matching profile according to three increasing levels of privacy: i) developing the common attribute set of the two users; ii) disclose the size of the common attribute set; and iii) revealing the size range of the common attribute is set between a user and their neighbors. In his view, a person honest, but-curious (HBC) adversarial model, which assumes that users try to

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

obtain more information than permitted by the inference results that match the profile, but the truth, follows the protocol. Secure multiparty computation applied the scheme of Shamir secret sharing and homomorphic encryption scheme to achieve the confidentiality of user profiles. In another category matching profile [22], [23], [36], the profiles can be represented as vectors, and the operation can be matching or distance domestic product. Such matching profile is a special case of computing the two parties insurance, which was initially introduced by Yao [37] and later generalized to secure multiparty computation by Goldreich et al. [38]. Specifically, we present two recent works in this category. Dong et al. [23] considered user profile consisting of attribute values and the proximity of two user profiles measured using dot product $f_{\cdot\cdot}(u,v)$.

An existing scalar product protocol [39] has been enhanced to allow secure verifiable computation. The enhanced protocol reveals only if the dot product is above or below a given threshold. The threshold value is selected by the user who starts the matching profile. They noted the potential risk of their anonymity protocols; an adversary can adaptively adjust the threshold value to quickly narrow the range of values of the profile of the victim. Therefore, it is required that the threshold value must be greater than a pre-defined lower limit (a system parameter) to ensure user anonymity. The same problem exists in other studies [21], [22].

Furthermore, Dong et al. [23] Users must make a commitment on their profiles to ensure consistency in profile, but the profile forgery attack can still occur during the commitment phase. Profile protocols proposed matching items are new since the comparison of attribute values are considered as the corresponding operation. The intuitive idea is inspired by the famous millionaire problem Yao '[37] and solution [40]. As in other studies [21] - [23], we propose three different protocols with different levels of anonymity. ECPM for conditional anonymity, anonymity and offer a detailed show the relationship between change and variation analysis pseudonym anonymity.

For the ICPM and IPPM with full anonymity, we show that the use of these protocols does not affect the level of user anonymity, and users are able to fully preserve their privacy.

III. EXPLICIT COMPARISON BASED APPROACH:

ECPM protocol allows two users to compare their attribute values in a given attribute without revealing the values together. However, the protocol reveals the result of the comparison to the initiator, and therefore provides conditional anonymity. The protocol has a fundamental pre-program phase, where the TCA generates all system parameters, user pseudonyms and inlay materials.

A. Bootstrapping:

The protocol has a fundamental bootstrapping phase, where the TCA generates all system parameters, user pseudonyms, and keying materials. Specifically, the TCA runs $\mathcal{G}$ to generate $< p, q, R, R_p, R_q, \mathcal{X} >$ for initiating the homomorphic encryption The TCA generates a pair of public and private keys $(p\mathcal{K}_{TCA}, s\mathcal{K}_{TCA})$ for itself. The public key $p\mathcal{K}_{TCA}$ is open to all users; the private key $s\mathcal{K}_{TCA}$ is a secret which will be used to issue certificates for user pseudonyms and keying materials, as shown below.

The TCA generates disjoint sets of pseudonyms (pid_i) and disjoint sets of homomorphic public keys (pk_i) for users (u_i). For every pid_i and pk_i of u_i, the TCA generates the corresponding secret keys psk_i and sk_i. In correspondence to each pseudonyms pid_i, it assigns a certificate $cert_{pid_i}$ to u_i. Which can be used to conform the validity of pid_i. Generally, the TCA users sk_{TCA} to generate a signature on pid_i and pk_i. The TCA outputs $cert_{pid_i}$ as a tuple $(pk_i, Sign_{sk_{TCA}}(pid_i, pk_i))$. The homomorphic secret key sk_i is delivered to u_i to gather with psk_i; pk_i is tied to pid_i and varies as the change of pseudonyms.

IV. IMPLICIT COMPARISON BASED APPROACH

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Here the profile corresponding implicit base (ICPM), the adoption of the unconscious transfer cryptographic technique is proposed. It is considered that users have different values for any given attribute. The ICPM consists of three main steps. In the first step, a category of interest by setting element to 1 and other elements to 0 length, the vector. Then encode the vector using the homomorphic encryption and sends the encryption vector, but it can still be processed in the ciphertext. In the second step, calculates the input ciphertexts of messages defined for 1≤ message ≤ length.

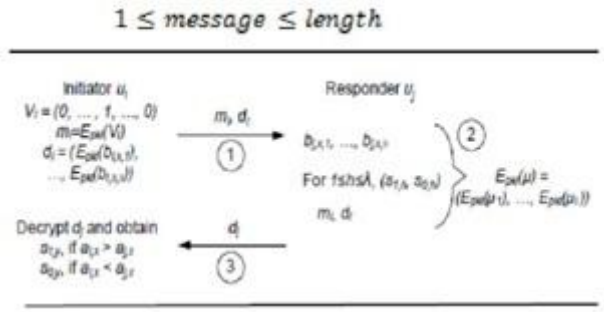


Fig1. ICPM floe.

V. IMPLICIT PREDICTABLE BASED APPROACH

Both eCPM and ICPM perform matching profile on a single attribute. For a game involving multiple attributes, must be performed several times, each time for one attribute. In this section, IPPC extends to cases of multiple attributes, without compromising their anonymity property, and obtain a protocol implicitly Profile Matching based on predicates, i.e. IPPM. This protocol is based on a predicate that is a logical expression made of multiple comparisons covering different attributes and therefore supports sophisticated

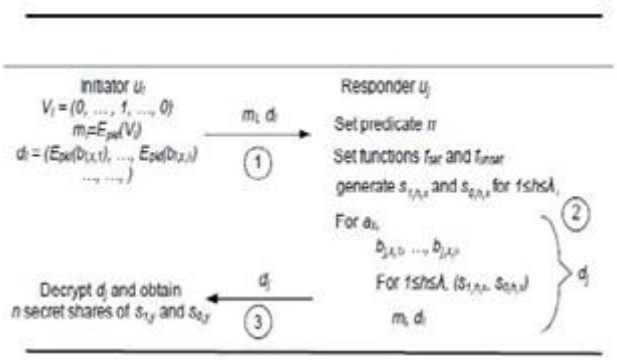


Fig2. IPPM flow.

VI. RESULTS:

The figure shows the behavior of the constant adaptation and post pre-adaptation strategies, respectively, for 5 and 10-anonymity anonymity regarding threshold th . The results are obtained with respect to user 32a. For constant strategy, multiple lines are drawn respectively corresponding to $z = \{1, 2, 4, 10, 20, \text{and } 40\}$. As z goes up, the user consumes a decreasingly number of pseudonyms and has an increasingly break ratio (the ratio of the number of time slots that the k-anonymity of the 32nd user is broken to 10,000). It can be seen that the number of pseudonyms consumed by the post-adaptive and pre-adaptive strategies are much smaller than those of the constant strategy. For example, in the case of 5-anonymity and $th = 0.0763$, the post-adaptive strategy spends 369 pseudonyms and results in a 514 time slot anonymity break period.

The constant strategy consumes 500(>369) pseudonyms and has a 0.0540(>.0514) break ratio. The post-adaptive strategy outperforms the constant strategy in anonymity protection by using fewer pseudonyms to achieve smaller break ratio. Similar phenomena are observed for other th values and 10-anonymity scenario as well. In particular, we find that as expected, the pre-adaptive strategy leads to yet better anonymity performance than the post-adaptive one. It shows that in case of 5-anonymity and th = 0.0763, the pre-adaptive strategy consumes 449(> 369) pseudonyms and results in a 0.0445(< 0.0514) break ratio.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The pre-adaptive strategy consumes slightly more pseudonyms, but achieves significantly shorter anonymity break period.

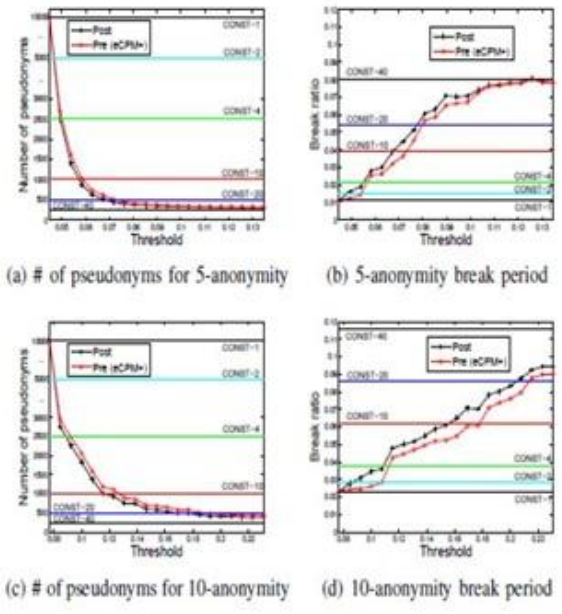


Fig3. Pseudonyms and break ratio

VII. CONCLUSION:

A unique comparison-based profile matching problem in Mobile Social Networks (MSNs) has been investigated, and novel protocols are proposed to solve it. The explicit Comparison based Profile Matching (eCPM) protocol provides conditional anonymity. It reveals the comparison result to the initiator. Considering the *k*-anonymity as a user requirement; the anonymity risk level in relation to the pseudonym change for consecutive eCPM runs is analyzed. Further an enhanced version of the eCPM, i.e., eCPM+ is introduced, by exploiting the prediction-based strategy and adopting the pre-adaptive pseudonym change. The effectiveness of the eCPM+ is validated through extensive simulations using real-trace data. Two protocols with full anonymity, i.e., implicit Comparison-based Profile Matching (iCPM) and implicit Predicate-based Profile Matching (iPPM) has been devised. The iCPM handles profile matching based on a single comparison of an attribute while the iPPM is implemented with a logical expression made of multiple comparisons spanning multiple attributes. The iCPM and the iPPM both enable users to anonymously request for messages and respond to the requests according to the profile matching result, without disclosing any profile information. In current version of the iCPM and the iPPM, $\geqslant$ and $\leqslant$ operations for profile matching is implemented. One future work is to extend them to support more operations, such as $\geqslant$ and $\leqslant$. Currently, the responder needs to transmit the threshold value of the predicate to the initiator, which may reveal partial information of the responder‘s interest. Restricting the disclosure of such parameter will be of significance for advancing comparison-based family of profile matching protocols and warrants deep investigation.

VIII. REFERENCES:

1. “Comscore,” http://www.comscoredatamine.com/.
2. A. G. Miklas, K. K. Gollu, K. K. W. Chan, S. Saroiu, P. K. Gummadi, and E. de Lara, “Exploiting social interactions in mobile systems,” in Ubicomp, 2007, pp. 409–428.
3. S. Ioannidis, A. Chaintreau, and L. Massouli´e, “Optimal and scalable distribution of content updates over a mobile social network,” in Proc. IEEE INFOCOM, 2009, pp. 1422–1430.
4. R. Lu, X. Lin, and X. Shen, “Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks,” in Proc. IEEE INFOCOM, 2010, pp. 632–640.
5. W. He, Y. Huang, K. Nahrstedt, and B. Wu, “Message propagation in adhoc-based proximity mobile social networks,” in PERCOM workshops, 2010, pp. 141–146.
6. D. Niyato, P. Wang, W. Saad, and A. Hjørungnes, “Controlled coalitional games for cooperative mobile social networks,” IEEE Transactions on Vehicular Technology, vol.

60, no. 4, pp. 1812–1824, 2011.

7. M. Motani, V. Srinivasan, and P. Nuggehalli, "Peoplenet: engineering a wireless virtual social network," in MobiCom, 2005, pp. 243–257.

8. M. Brereton, P. Roe, M. Foth, J. M. Bunker, and L. Buys, "Designing participation in agile ridesharing with mobile social software," in OZCHI, 2009, pp. 257–260.

9. E.Bulut and B.Szymanski, "Exploiting friendship relations for efficient routing in delay tolerant mobile social networks," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 12, pp. 2254–2265, 2012.

10. Z. Yang, B. Zhang, J. Dai, A. C. Champion, D. Xuan, and D. Li, "E-smalltalker: A distributed mobile system for social networking in physical proximity," in ICDCS, 2010, pp. 468–477.

11. Q. Li, S. Zhu, and G. Cao, "Routing in socially selfish delay tolerant networks," in Proc. IEEE INFOCOM, 2010, pp. 857–865.

12. X. Liang, X. Li, T. H. Luan, R. Lu, X. Lin, and X. Shen, "Moralitydriven data forwarding with privacy preservation in mobile social networks," IEEE Transactions on Vehicular Technology, vol. 7, no. 61, pp. 3209–3222, 2012.

13. R. Gross, A. Acquisti, and H. J. H. III, "Information revelation and privacy in online social networks," in WPES, 2005, pp. 71–80.

14. F. Stutzman, "An evaluation of identity-sharing behavior in social network communities." iDMAa Journal, vol. 3, no. 1, pp. 10–18, 2006.

15. K. P. N. Puttaswamy, A. Sala, and B. Y. Zhao, "Starclique: guaranteeing user privacy in social networks against intersection attacks," in CoNEXT, 2009, pp. 157– 168.

16. E. Zheleva and L. Getoor, "To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles," in WWW, 2009, pp. 531–540.

17. G. Chen and F. Rahman, "Analyzing privacy designs of mobile social networking applications," IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, vol. 2, pp. 83–88, 2008.

18. D. Balfanz, G. Durfee, N. Shankar, D. K. Smetters, J. Staddon, and H.- C. Wong, "Secret handshakes from pairing-based key agreements," in IEEE Symposium on Security and Privacy, 2003, pp. 180–196.

19. M. J. Freedman, K. Nissim, and B. Pinkas, "Efficient private matching and set intersection," in EUROCRYPT, 2004, pp. 1–19.

20. R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mhealthcare social network," ACM Mobile Networks and Applications (MONET), vol. 16, no. 6, pp. 683–694, 2011.

21. M. Li, N. Cao, S. Yu, and W. Lou, "Findu: Privacy-preserving personal profile matching in mobile social networks," in Proc. IEEE INFOCOM, 2011, pp. 2435– 2443.

22. R. Zhang, Y. Zhang, J. Sun, and G. Yan, "Fine-grained private matching for proximity-based mobile social networking," in Proc. IEEE INFOCOM, 2012, pp. 1969–1977.

23. W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in Proc. IEEE INFOCOM, 2011, pp. 1647– 1655.

24. J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "On noncooperative location

privacy: a game-theoretic analysis," in ACM CCS, 2009, pp. 324–337.

25. R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," IEEE Transactions on Vehicular Technology, vol. 61, no. 1, pp. 86 – 96, 2011.

26. J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in EUROCRYPT, 2008, pp. 146– 162.

27. N. Eagle and A. Pentland, "Social serendipity: mobilizing social software," IEEE Pervasive Computing, vol. 4, no. 2, pp. 28–34, 2005.

28. J. Teng, B. Zhang, X. Li, X. Bai, and D. Xuan, "E-shadow: Lubricating social interaction using mobile phones," in ICDCS, 2011, pp. 909–918.

29. B. Han and A. Srinivasan, "Your friends have more friends than you do: identifying influential mobile users through random walks," in MobiHoc, 2012, pp. 5–14.

30. Z. Yang, B. Zhang, J. Dai, A. C. Champion, D. Xuan, and D. Li, "E-smalltalker: A distributed mobile system for social networking in physical proximity," in ICDCS, 2010, pp. 468–477.

31. L. Kissner and D. X. Song, "Privacy-preserving set operations," in CRYPTO, 2005, pp. 241–257.

32. Q. Ye, H. Wang, and J. Pieprzyk, "Distributed private matching and set operations," in ISPEC, 2008, pp. 347–360.

33. D. Dachman-Soled, T. Malkin, M. Raykova, and M. Yung, "Efficient robust private set intersection," in ACNS, 2009, pp. 125–142.

34. S. Jarecki and X. Liu, "Efficient oblivious pseudorandom function with applications to adaptive ot and secure computation of set intersection," in TCC, 2009, pp. 577–594.

35. C. Hazay and Y. Lindell, "Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries," Journal of Cryptology, vol. 23, no. 3, pp. 422–456, 2010.

36. B. Goethals, S. Laur, H. Lipmaa, and T. Mielik¨ainen, "On private scalar product computation for privacy-preserving data mining," in ICISC, 2004, pp. 104–120.

37. A. C.-C. Yao, "Protocols for secure computations (extended abstract)," in FOCS, 1982, pp. 160–164.

38. O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game or a completeness theorem for protocols with honest majority," in STOC, 1987, pp. 218–229.

39. I. Ioannidis, A. Grama, and M. J. Atallah, "A secure protocol for computing dot-products in clustered and distributed environments," in ICPP, 2002, pp. 379–384.

40. I. F. Blake and V. Kolesnikov, "Strong conditional oblivious transfer and computing on intervals," in

41. ASIACRYPT, 2004, pp. 515–529.
42. P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in EUROCRYPT, 1999, pp. 223–238.
43. M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?" in CCSW, 2011, pp. 113–124.
44. R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications,"IEEE Transactions on

Parallel and Distributed Systems, vol. 23, no. 9, pp. 1621–1631, 2012.

45. H. Ltkepohl, New introduction to multiple time series analysis. Springer, 2005.
46. X. Liang, X. Li, Q. Shen, R. Lu, X. Lin, X. Shen, and W. Zhuang, "Exploiting prediction to enable secure and reliable routing in wireless body area networks," in Proc. IEEE INFOCOM, 2012, pp. 388–396.
47. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.
48. L. Sweeney, "k-anonymity: A model for protecting privacy," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 5, pp. 557– 570, 2002.
49. J. Scott, R. Gass, J. Crowcroft, P. Hui, C. Diot, and A. Chaintreau, "CRAWDAD trace cambridge/ haggle/ imote/infocom (v. 2006-01-31)," Jan. 2006.
50. D. J. Watts, "Small worlds: The dynamics of networks between order and randomness," J. Artificial Societies and Social Simulation, vol. 6, no. 2, 2003.
51. C. Bron and J. Kerbosch, "Finding all cliques of an undirected graph (algorithm 457)," Communications of the ACM, vol. 16, no. 9, pp. 575– 576, 1973.