EPiC Series in Computing

Volume 45, 2017, Pages 63–67

SCSS 2017. The 8th International Symposium on
Symbolic Computation in Software Science 2017

# Private Profile Matching for Mobile Social Networks Based on Fuzzy Extractors

Jaweher Zouari[1], Mohamed Hamdi[1], and Tai-Hoon Kim[2]

[1] Higher Scool of Communications SupCom, Carthage University, Tunis, Tunisia
jaweher.zouari,mmh@supcom.tn
[2] Sungshin Women University, Korea
taihoon@sungshin.ac.kr

**Abstract**

Interacting with geographically proximate users who present similar interests and preferences is a key service offered by mobile social networks which leads to the creation of new connections that combine physical and social closeness. Usually these interactions are based on social profile matching where users publish their preferences and attributes to enable the search for a similar profile. Such public search would result in the leakage of sensitive or identifiable information to strangers who are not always potential friends. As a consequence this promising feature of mobile social networking may cause serious privacy breaches if not addressed properly. Most existent work relies on homomorphic encryption for privacy preservation during profile matching, while we propose in this paper a novel approach based on the fuzzy extractor which performs private matching of two sets and reveals them only if they overlap considerably. Our scheme achieves a desirable trade off between security and complexity.

## 1 Introduction

In the last decade, mobile equipements became augmented with promising technologies such as positioning utilities, UMTS and LTE connectivity, near field and Wi-Fi interfaces, and different monitors. These advances gave mobile devices incredible capabilities such as high speed internet access, localization, short range communications and semantic awareness. These technologies allowed for the migration of social networking from legacy desktops to mobile devices leading to mobile social networking and a myriad of new applications that offer immediacy, ubiquity and pervasiveness[1][2]. The attractiveness of mobile social applications has made them an integral part of the everyday life of billions of users. For instance Facebook Messenger and What-sApp mobile messaging applications reached in 2016 one billion of monthly active users around the globe. Several mobile social applications are providing people with viable opportunities such as socializing with their near peers that are proximate both in location and in interests. Lovegety, PeopleNet and Proxidating are examples. This opportunistic social networking is enabled by profile matching of users who happen to be in the proximity of each other. Although offering exiting opportunities to mobile users, mobile social network applications are bringing critical privacy issues with regard to users personal information such as exposing their personal contact details or disclosing their private profiles. Several privacy related attacks that are targeting mobile social network users are reported in the literature[3] , making the privacy preservation an urgent need in this field. To this end, several proposals proliferated to address these threats most of which are based on encryption and homomorphic cryptosystems[4][5].

We propose in this paper a new approach to address privacy challenges in mobile social networks that is not based on encryption but rather on chaffing, which can be viewed as concealing private data into a lot of random noise. To this end we use a key binding cryptosystem known as the fuzzy extractor [6], which is a modified version of the cryptographic construct proposed by Juels and Sudan in 2002[7] allowing to lock a secret key under an unordered genuine set in order to obtain a vault that both protects the genuine set and the secret key. During unlocking, only a set that overlaps considerably with the genuine set can be used to open the vault and recover the secret key. Offering promising privacy preservation abilities, the fuzzy vault was most widely deployed in the field of biometrics to protect biometric templates and especially fingerprints. In this paper we show how the fuzzy vault can best fit the privacy requirements of mobile social applications by providing high security levels.

## 1.1 Motivation

We describe here a motivation scenario. Assume Alice is a mobile social network user having a social profile at some social network provider. Suppose Alice is at a conference or in some public place and wants to socialize with people who share her preferences and interest, all or some of them, among the nearby persons. An easy approach would be to make social profiles public so that similar proximate users can discover each other. However Alice is reluctant about exposing her private attributes to foreigners. She is looking for a solution allowing her to afford her profile only to similar persons so that she can interact with, or perhaps meet them face-to-face, while concealing this same profile from strangers who are not like her to some extent. Note that this scenario implies an asynchronous communication pattern where Alice would afford a private version of her profile, and Bob, another MSN (Mobile Social Network) user desiring to contact Alice, can make the profile matching at a deferred time. Note also that Alice is just looking for similar profiles not identical ones and she would be glad to define herself the amount of similarity she is satisfied with. Our proposed protocol meets Alices expectations in terms of privacy preserving profile matching.

## 1.2 Contribution

We propose in this paper a privacy preserving profile matching protocol which, to our best knowledge is the first of its kind to be based on the fuzzy extractor for mobile social networks. We show how privacy preservation can be performed by means other than the long established tool which is homomorphic encryption. Our second contribution is to provide a new formalization to the information theoretic security of the cryptosystem based on an alternative decoding algorithm. Third, we provide a countermeasure to a known vulnerability of the fuzzy vault which appears in the presence of multiple records of the same user.

# 2 Profile Model

## 2.1 Mobile Social Network Scenario

The aim of the private matching protocol is to protect the privacy of user profiles during mobile social interactions. To this end we assume users are equipped with mobile devices where the profile matching protocol is a functionality offered by mobile social application providers. As MSN users are frequently surrounded by familiar strangers who are not their friends but probably should be, a typical MSN scenario can be divided into three steps. The first consists in a discovery phase where the user scans the neighbourhood through a i-Fi or a Blue-tooth interface. Then a matching operation is performed against neighbouring users to select the closest profile in some distance metric. Finally a connection is established between the matched users under their mutual consent. In such scenario, personal profiles should be made public in order to be matched by proximate peers, which is conflicting with privacy requirements of users who wish to reveal their profiles and contact details only to people with very similar interests and attributes. Most proposals for privacy preservation are based on encryption where the profile is published on a concealed way and a key derived from the attributes is created. Only persons with same attributes order can decrypt the concealed profile. Moreover a threshold is set on the similarity degree between the two attribute vectors and only results surpassing the threshold allow interaction. The problem with this solution is the lack of flexibility. If someone has approximately the same attributes as the concealed profile, with one or two differences in the attribute vector due to altered order or additional items he will not be able to access the profile and interact with the related user, while the latter still wishes to be contacted by the former. In other words only profiles with identical items number at identical order can interact, which is not practical in mobile social networks where profiles are not necessarily generated in the same order or even by the same social network provider. Thus an amount of order invariance and dissimilarity tolerance, which is rather inevitable in our case, is required. We need a sort of a private profile that can be published by the user and unlocked only by persons with highly similar interests, regardless of their attribute orders or number of items, provided they overlap sufficiently.

## 2.2 Coordinate-based Profile Model

profile is a set of attributes defined in a particular context. It consists of preferences and interests in the case of a social network, health records and diseases for a health healthcare network or it can be diplomas and affiliations in an academic context. We stick to the social field as a reference context for its familiarity. Thus a user profile is a set of interests and preferences such as favorite movies, books, TV series, music, and sports. Each category contains a number of public items from which the user chooses his favorite ones. In order to prevent fake profiles or forged attributes, we may infer profile items from ones account at a trusted social network provider instead of being entered by the user himself. This would ensure verifiability and authenticity of attributes. We represent the universe of items in the different categories by an x-coordinate system with a one to one correspondence between items and x-coordinates. A user profile corresponds then to an unordered set of items represented by their x-coordinates.We obtain this way a set A of unordered elements that should be published in a privacy preserving manner so that only users with close attributes can see it.

# 3 Proposed Scheme

Assume we have a secret s (e.g. contact details) and a set A of attributes represented as x-coordinates. We map these x-coordinates to finite field elements by associating the element of index i to the finite field element encoding the integer i. We work on the galois field GF(16). For locking, we generate a polynomial P of degree k over the finite field GF(16) from the secret s. An agreed on way for doing so is by making the elements of s the coefficients of P. Then we project the encoded set of attributes into the polynomial P by evaluating P on each element. We obtain the genuine set of (x,P(x)) pairs which are points laying on P. After binding attributes to the secret s by projecting them on P, we need to conceal the obtained genuine set. To this end we generate a polynomial M which is the sum of P and the product of (x - t) with t in A. For every genuine point we have M(x) = P(x), while M(x) is different from P(x) for any point not belonging to A. This polynomial M is the private profile of Alice which she can publish with an hash of P and expect to be securely contacted by socially close users only. For Matching, a user Bob will form his query attributes in the same way Alice does, map them to finite field elements and project them on the published polynomial M to obtain the query set pairs (x,M(x)). If Bob shares enough preferences and interests with Alice then he will obtain a high number of points laying on P, since M(x) = P(x) for x in A. If Bob has at least k+1 shared attributes with Alice he can obtain K+1 points laying on P, which he can interpolate using Lagrange polynomial to recover P and thus s. Otherwise he can't recover P and more importantly he won't learn nothing about Alice's attributes. In order to find the suitable the (k+1) pairs among all the query set, Bob iterates through all possible combinations of (k+1) points until he recovers P (by comparing the interpolated polynomial with the published hash of P). If Bob is sufficiently close to Alice, he will soon hit enough genuine pairs and recover P, which makes the scheme viable for potential friends. The security of the scheme stems from the fact that without knowledge of (k+1) genuine pairs the secret polynomial can' t be reconstructed, even with k points. Thus the security is information theoretic and doesn't rely on any cryptographic assumption.The computation complexity and the storage overhead of the scheme are optimal for a potential friend.

# 4 Conclusion

Mobile social networking offers viable opportunities for making connections provided it is conceived with enough privacy awareness. We proposed in this paper a privacy preserving profile matching mechanism based on the fuzzy extractor which is a modified version of the fuzzy vault. The scheme offers high security with lightweight computation for a potential friend.

# References

[1] Xiping, H., Terry H. S. C., Victor C. M. L., Edith C.-H. N., Philippe K., Henry C. B. C.: A Survey on Mobile Social Networks: Applications, Platforms, System Architectures, and Future Research Directions. J. IEEE Communication Surveys and Tutorials. vol 17, no. 3, 1857-1881 ,2015.

[2] Nafa J., Sherali Z., Biju S.: Mobile Social Networking Applications. J. Communications of the ACM. vol 56. no 3, 71-79 , 2013.

[3] Chen G., Rahman F.: Analyzing privacy designs of mobile social networking applications. IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, vol. 2, 8388 ,2008.

[4] Li M., Cao N., Yu S.,Lou W.: FindU: Privacy-preserving personal profile matching in mobile social networks. In Proc. INFOCOM11. 2435 2443,2011.

[5] Dong W., Dave V., Qiu I., Zhong Y.: Secure Friend Discovery in Mobile Social Network. In Proc. INFOCOM11. 1647-1655 ,2011.

[6] Dodis Y., Reyzin L., Smith A.: Fuzzy extractors How to generate strong keys from biometrics and other noisy data. In EUROCRYPT. 523540 ,2004.

[7] Juels A., Sudan M.: A fuzzy vault scheme. In Proc. IEEE Int. Symp. Information theory, Lausanne,Switzerland. p. 408 ,2002.