LIP3: A Lightweighted Fine-Grained Privacy-Preserving Profile Matching Mechanism for Mobile Social Networks in Proximity

Yufeng Wang[1(✉)], Xiaohong Chen[1], Qun Jin[2], and Jianhua Ma[3]

[1] Nanjing University of Posts and Telecommunications, Nanjing 210003, China
wfwang@njupt.edu.cn
[2] Waseda University, Saitama 359-1192, Japan
jin@waseda.jp
[3] Hosei University, Tokyo 184-8584, Japan
jianhua@hosei.ac.jp

Abstract. Recently, Device to Device (D2D) based mobile social networking in proximity (MSNP) has witnessed great development on smartphones, which enable actively/passively and continuously seek for relevant value in one's physical proximity, through direct communicating with other individuals within the communication range, without the support of centralized networking infrastructure. Specially, a user would like to find out and interact with some strangers with similar interest in vicinity through profile matching. However, in matching process, individuals always have to reveal their personal and private profiles to strangers, which conflicts with users' growing privacy concerns. To achieve privacy preserving profile matching (i.e., friend discovery), many schemes are proposed based on homomorphic and commutative encryption, which bring tremendous computation and communication overheads, and are not practical for the resource limited mobile devices in MSNP. In this paper we adapt Confusion Matrix Transformation (CMT) method to design a Lightweighted fIne-grained Privacy-Preserving Profile matching mechanism, LIP3, which can not only efficiently realize privacy-preserving profile matching, but obtain the strict measurement of cosine similarity between individuals, while other existing CMT-based schemes can only roughly estimate the matching value.

Keywords: Mobile social networking in proximity (MSNP) · Privacy-Preserving · Profile matching · Confusion matrix transformation

1 Introduction

Today, modern mobile phones have the capability to detect proximity of other users and offer means to communicate and share data in ad-hoc way, with the people in the proximity, which naturally integrates those two trends: wireless opportunistic networking and decentralized online social networks, and leads to the great development

G. Wang et al. (Eds.): ICA3PP 2015 Workshops, LNCS 9532, pp. 166–176, 2015.
DOI: 10.1007/978-3-319-27161-3_15

and deployment of D2D based MSNP (Mobile social network in proximity), which is explicitly defined as: A wireless peer-to-peer (P2P) networking of spontaneously and opportunistically connected users (e.g., through the Bluetooth/WiFi interfaces on their mobile devices), exploits both geo-proximity and social interests as the primary filters in determining who is discoverable on the social network [1]. In contrast to traditional web-based online social networking, D2D based MSNP can enable more tangible face-to-face social interactions in public places such as parks, stadiums, and train stations, etc.

In MSNPs, individuals can maintain and store their sensitive data by themselves, which can alleviate the problem of big brother (privacy concern) in traditional MSN. This implies that the omniscient OSN provider that has become "a big brother", collects and stores all user's data (messages, profiles, location, relations, etc.), which may cause serious privacy concern, e.g., selling users' personal information, and targeted advertising, However, MSNP users still face growing privacy concerns.

Basically, the first step toward effective D2D based MSNP is for mobile users to choose whom to interact with. As an example, Alice wants to conduct a proximal talk with nearby passengers at the airport. Since she can simultaneously interact with only one or a few persons, it is crucial for her to select those who can lead to the most meaningful social interactions: The natural way is to select those whose social profiles most match hers. Widely known as profile matching, this method is rooted in the social fact that people normally prefer to socialize with others having similar interests or background over complete strangers.

A major challenge for profile matching is to ensure the privacy of personal profiles which often contain highly sensitive information related to gender, interests, political tendency, health conditions, and so on. This challenge necessitates private matching, in which two users compare personal profiles without disclosing them to each other. Generally, there are two mainstreams of approaches to solving the privacy-preserving profile-based friend matching problem. The first category is converted into Private Set Intersection or Private Set Intersection Cardinality, whereby two mutually mistrusting parties, each holding a private data set, jointly compute the intersection, or the intersection cardinality of the two sets without leaking any additional information to either party. These schemes could enable only coarse-grained private matching and are unable to further differentiate users with the same attribute(s). To solve this problem and thus further enhance the usability of MSNP, the second category includes fine-grained private matching mechanisms, which consider a user's profile as a vector with fine-grained attribute values, and measures the social similarity by private vector dot product [2].

Although, both kinds of approaches could effectively enforce privacy-preserving profile-matching among nearby users without the support of the trusted third party, they have the following disadvantage: Always rely on public-key cryptosystem and homomorphic encryption [3–6]. Usually, multiple rounds of interactions are required to perform the public key exchange and private matching between each pair of parties, which incurs high communication and computation costs to resource-limited mobile terminals in MSNP.

Based on non-homomorphic encryption-based privacy-preserving scalar product computation [7], an EWPM (Efficient Weight-based Private Matching) protocol was

proposed to employ Confusion Matrix Transformation algorithm instead of computation-consuming homomorphic cryptographic system, to achieve the privacy preserving goal with a higher efficiency [8]. The main weakpoint in EWPM is that the inferred matching value doesn't have strict semantic meaning, and can only roughly represents the profile similarity among users. For example, in the following Subsect. 3.3, we give a special case, in which the obtained matching values by EWPM for two pairs of users are identical, but according to strict similarity metric (e.g., cosine similarity), those two matching values are not same.

Based on the above observation, this paper designs a Lightweighted fIne-grained Privacy-Preserving Profile matching mechanism for D2D based MSNP, LIP3, which, in comparison with the existing CMT schemes (e.g., EWPM), can provide strict and accurate profile matching value-cosine similarity result among individuals. The numerical results show that LIP3 can provide more accurate similarity measurement than EWPM, and bring no more computation and communication overheads.

The rest of this paper is organized as follows. Section 2 gives the system model of LIP3, and the adversary models dealt with in this paper. In Sect. 3, we describe the details of the proposed system, LIP3, and give an example to illustrate the advantage of LIP3 over EWPM. In Sect. 4, the security and complexity analysis are schematically provided. Finally, we briefly conclude this paper.

2 LIP3 System Model

2.1 System Architecture of LIP3

When people join MSNPs, they usually begin by creating a profile, and then interact with other users. The content of profile could be very broad, such as personal background, hobbies, contacts, places they have been to, etc. Privacy-preserving profile matching is a common and helpful way to make new friends with common interest or experience, find lost connections, or search for expert, without revealing participants' personal and private profiles.

Specifically, each user's interest profile is defined from a public attribute set consisting of n attributes. The number of n may range from several tens to several hundreds. Each attribute is associated with a user-specific integer value $i \in [1, l]$ (called as the weight of an attribute) indicating the corresponding user's association with this attribute. The higher the value of this attribute is, the more interest the user has in the attribute. Usually, letting l equal 10 may be sufficient to differentiate user's interest level. Suppose two users Alice and Bob's interest sets are characterized as the following profile vectors $\vec{u}_A = (u_{A_1}, u_{A_2}, \ldots, u_{A_n})$ and $\vec{u}_B = (u_{B_1}, u_{B_2}, \cdots, u_{B_n})$, respectively. Each individual can modify her/his profile later on when needed. The most widely applied similarity metric to infer the matching value between individuals, say Alice and Bob, is cosine similarity:

$$similarity\,(A, B) = \frac{\vec{u}_A \cdot \vec{u}_B}{\|\vec{u}_A\| \cdot \|\vec{u}_B\|} = \frac{\sum_{i=1}^{l} u_{A_i} \cdot u_{B_i}}{\sqrt{\sum_{i=1}^{l} (u_{A_i})^2} \cdot \sqrt{\sum_{i=1}^{l} (u_{B_i})^2}} \tag{1}$$

Assume that Alice wants to find someone to chat, e.g., when waiting for the flight to depart. As the first step (Peer discovery), she broadcasts a chatting request via the MSNP application on her smartphone to discover proximate users of the same MSNP application. Suppose that she receives multiple responses including one from Bob who may also simultaneously respond to other persons. Due to time constraints or other reasons, both Alice and Bob can only interact with one stranger whose profile best matches hers or his. The next step (Profile Matching) is thus for Alice (or Bob) to compare her (or his) profile with those of others who responded to her (or whom he responded to). LIP3 will enable two users to measure the accurate similarity value between the above fine-grained privacy-preserving personal profiles using cosine similarity metrics.

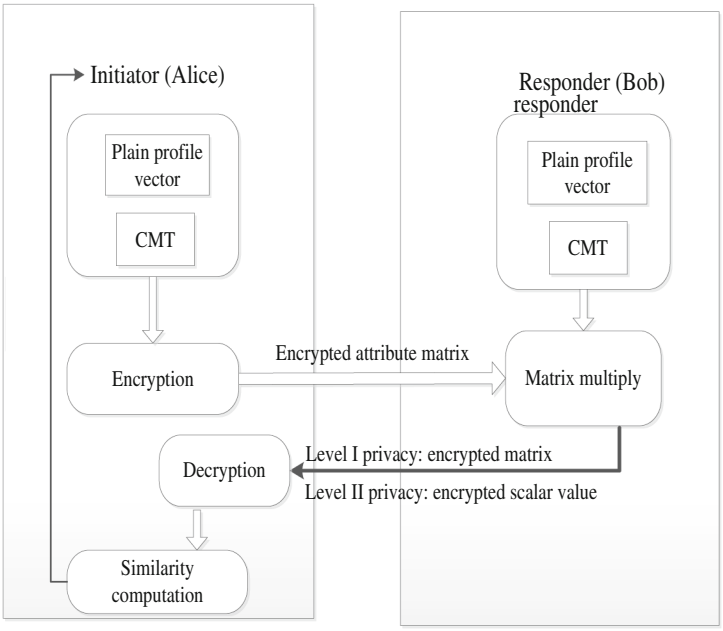

Fig. 1. System architecture of LIP3 scheme

Figure 1 illustrates the system architecture of the proposed privacy-preserving profile matching scheme LIP3, which is composed of two mobile users with specific interest profiles, and several component which facilitate the similarity calculation in LIP3 scheme.

The plain profile vectors in the initiator (say Alice) and responder (say Bob) are firstly transformed into corresponding attribute matrices through CMT, which can completely describe users' profiles. Then the initiator encrypts her attribute matrix and sends it to responder. The responder Bob will calculate the multiplication between the received encrypted matrix and the attribute matrix of herself. The obtained matrix (in Level I privacy) or the scalar value (in Level II privacy) will be sent to initiator who, then decrypts and obtains the cosine similarity between initiator and responder. Note that, in our proposal, the module of responder's profile vector should be explicitly sent to initiators.

2.2 Adversary Models

There exists attacks from outside adversaries, such as eavesdropping the wireless communication channel or modifying, replying and injecting the captured messages. We assume the users in our protocol are honest-but-curious (HBC), which means they will comply with the algorithmic procedure, but they are curious about other users and try to learn more information than allowed. Furthermore, some users may be inside attackers who monitor the matching process and obtain the intermediate results without complying the agreements. They try to infer users' profiles through these observations. Based on the adversary models, similar as [8], the following two privacy levels are defined.

- Level-I privacy: when LIP3 ends, both the initiator and responder learn nothing about each other's attribute, when they are HBC.
- Level-II privacy: when the LIP3 ends, both the initiator and responder learn nothing about each other's attribute, even when they are inside attackers.

3 The Detailed Procedure of LIP3

In our scheme, each individual, say Alice's profile vector is explicitly encoded into a profile matrix $\boldsymbol{A}_{l\times n}$ whose elements depend on the individual's personal attributes and weights. This matrix can completely describe an user's profile, in which the row vectors indicate the weight of interest and column vectors mean the public attribute. Specifically, if the value of the jth attribute of Alice is set as i ($i \in [1, l]$), then she sets $a_{ij} = 1$ and $a_{mj} = 0$ where $a_{mj} \in \boldsymbol{A}_{l\times n}$, $m \neq i$.

A MSNP session involves two users and usually consists of three phases. First, two users need discover each other in the neighbor-discovery phase. Second, they need compare their personal profiles in the matching phase. Last, two matching users enter the interaction phase for real information exchange.

3.1 Preliminary LIP3 that Satisfy the Level-I Privacy

The main contribution of our paper is that LIP3 explicitly defines a weight matrix $\boldsymbol{W}_{l\times l} = (w_{ij})_{l\times l}$ through which the accurate cosine similarity can be inferred, without revealing individuals' private profiles. Specifically, the element w_{ij} is given as the Eq. (2).

$$\left(w_{ij}\right)_{l\times l} = i \cdot j \tag{2}$$

In LIP3, the initiator (Alice) and responder (Bob) respectively hold the attribute matrices $\boldsymbol{A}_{l\times n}$ and $\boldsymbol{B}_{l\times n}$, which are transformed from the both users' plain profile vectors. p and q are two large primes. $\boldsymbol{C}_{l\times n}$ and $\boldsymbol{R}_{l\times n}$ are two matrixes used for hiding personal information. The vector $\overrightarrow{\boldsymbol{k}}$ is the secret key kept by initiator to decrypt the original results. The detailed procedure of LIP3 is given as follows.

- The initiator initializes her personal profile according to Algorithm 1, which can be run offline, and broadcasts her friend discovery request to others. When Algorithm 1 ends, the initiator keeps $\overrightarrow{\boldsymbol{k}} = [k_1, k_2, \cdots, k_l]$, and q secretly and sends $\boldsymbol{A}^*_{\boldsymbol{l\times n}}$ to the responder;
- After receiving $\boldsymbol{A}^*_{\boldsymbol{l\times n}}$, the responder computes $\boldsymbol{D_{l\times l}} = (d_{ij})_{l\times l}$ according to Algorithm 2 and sends $\boldsymbol{D_{l\times l}}$ to the initiator;
- The initiator operates the following steps: $\boldsymbol{T_{l\times l}} = \left(t_{ij}\right)_{l\times l} = \left(d_{ij} + k_i\right) mod\ q$. It is shown that the above constructed equation $\boldsymbol{T_{l\times l}} = \boldsymbol{A_{l\times n}} \times \boldsymbol{B^T_{l\times n}}$. Moreover, let $\boldsymbol{T^*_{l\times l}} = \left(t^*_{ij}\right)_{l\times l}$, and $t^*_{ij} = \frac{t_{ij} - (t_{ij} mod\ p^2)}{p^2}$;
- The initiator considers the corresponding weights and computes:

$$H_{l\times l} = W_{l\times l} \cdot * T^*_{l\times l} = \begin{pmatrix} w_{11} \cdot t^*_{11} & \cdots & w_{1l} \cdot t^*_{1l} \\ \vdots & \cdots & \vdots \\ w_{l1} \cdot t^*_{l1} & \cdots & w_{ll} \cdot t^*_{ll} \end{pmatrix} \tag{3}$$

- in which the operator $\cdot *$ denote multiplying the corresponding elements of two matrices $\boldsymbol{W_{l\times l}}$ and $\boldsymbol{T^*_{l\times l}}$ to obtain the matrix $\boldsymbol{H_{l\times l}}$.
- The initiator calculates the matching value $\tau = \sum_{i=1}^{l}\sum_{j=1}^{l} h_{ij}$, which equals the value $\overrightarrow{\boldsymbol{u}}_A \cdot \overrightarrow{\boldsymbol{u}}_B$, then the cosine similarity between two interacting individuals can be obtained.

The Algorithms 1 and 2 used in the LIP3 operation procedures are given as follows.

Algorithm 1. Initialization algorithm for private configuration

---

Input: Initiator's attribute matrix $\boldsymbol{A_{l\times n}}$;
Output: Encrypted matrix $\boldsymbol{A^*_{l\times n}}$;
Choose two large primes p **and** q, **where** $|p| = 256$ **and** $q > (n+1)\cdot l^2 \cdot p^2$;
Randomly generate two matrixes $\boldsymbol{C_{l\times n}}$ **and** $\boldsymbol{R_{l\times n}}$, $\forall c_{ij} \in \boldsymbol{C_{l\times n}}$, $\forall r_{ij} \in \boldsymbol{R_{l\times n}}$, $\sum_{i=1}^{l}\left(\sum_{j=1}^{n} c_{ij}\right) < (p - l\cdot n)$, $\left|r_{ij}\cdot q\right| \approx 1024$;
$\forall a_{ij} \in \boldsymbol{A_{l\times n}}, \forall a^*_{ij} \in \boldsymbol{A^*_{l\times n}}, k_i \in \overrightarrow{\boldsymbol{k}}$, **the following procedure is done:**
FOR (i=1; i ≤ l; i++) **DO**
    $k_i = 0$;
FOR (j=1; j ≤ n; j++) **DO**
IF $a_{ij} = 1$ **THEN** $a^*_{ij} = p + c_{ij} + r_{ij}\cdot q$;
ELSE $a^*_{ij} = c_{ij} + r_{ij}\cdot q$;
ENDIF
$k_i = k_i + r_{ij}\cdot q - c_{ij}$;
ENDFOR
ENDFOR

Algorithm 2. LIP3 for achieving the Level-I privacy

Input: $A^*_{l\times n}$, $B_{l\times n}$;
Output: The cosine similarity between two individuals;
Compute $\boldsymbol{D_{l\times l}} = (t_{ij})_{l\times l}$ through the following operations:
FOR (i =1; i ≤ l; i++) **DO**
  FOR (j=1; j ≤ l; j++) **DO**
    $d_{ij} = 0$;
    FOR (m=1; m ≤ n; m++) **DO**
      IF ($b_{im} = 1$) **THEN** $d_{ij} = d_{ij} + p \cdot a^*_{im}$;
      ELSE $d_{ij} = d_{ij} + a^*_{im}$;
      ENDIF
    ENDFOR
  ENDFOR
ENDFOR
The responder sends computed $\boldsymbol{D}_{l\times l}$and $\|\vec{v}\|$ to the initiator, according to the above equations (1), (2) and (3), the initiator computes τ, then
$similarity(A,B) = \frac{\tau}{\|\vec{u}_A\|\cdot\|\vec{u}_B\|}$

3.2 Enhanced LIP3 Satisfying Level-II Privacy

Note that the above procedures can only satisfies the privacy level I. In order to resist the malicious users to achieve the Level-II privacy, instead of directly sending the matrix $\boldsymbol{D}_{l\times l}$ to initiator, the responder can send the scalar value $\sigma = \sum_{i=1}^{l}\sum_{j=1}^{l} t_{ij}$ to initiator, in which $(t_{ij})_{l\times l} = D_{l\times l} \cdot *W_{l\times l}$ is calculated based on Eq. (2). And then, on receiving the message σ, the initiator decrypts the matching value τ via the following operators:

$$\tau_1 = \left(\sigma + l\left(\sum_{i=1}^{l} k_i\right)\right) mod\ q;\ \tau = \vec{\boldsymbol{u}}_A \cdot \vec{\boldsymbol{u}}_B = \frac{\tau_1 - (\tau_1 mod\ p^2)}{p^2}$$

Then the cosine similarity between Alice and Bob is following:

$$similarity(A,B) = \frac{\tau}{\left\|\vec{\boldsymbol{u}}_A\right\| \cdot \left\|\vec{\boldsymbol{u}}_B\right\|}$$

3.3 The Advantage of LIP3 over EWPM

We use a simple example to verify the correctness of our scheme. We assume three users Alice, Bob and Charles are within the communication range. The number of attributes n, is 3, and the maximal attribute value l, is 2. Suppose Alice is the initiator,

with profile $\overrightarrow{\boldsymbol{u}}_A = (1,1,2)$, translate to matrix is $\boldsymbol{A}_{2\times 3} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, Bob and Charles are the responders and the profiles of Bob and Charles are $\overrightarrow{\boldsymbol{u}}_B = (1,1,1)$, matrix $\boldsymbol{B}_{2\times 3} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$, $\overrightarrow{\boldsymbol{u}}_c = (1,2,1)$ matrix $\boldsymbol{C}_{2\times 3} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, respectively. Since the calculation process between Alice and Bob is similar to that of Alice and Charles, we just describe the process between Alice and Bob in detail, and give the matching value between Alice and Charles directly. Similarly as [8], we can get: $\boldsymbol{T}^*_{2\times 2} = \begin{pmatrix} 2 & 0 \\ 1 & 0 \end{pmatrix}$ which numerically equals the result as $\boldsymbol{A}_{2\times 3} \times \boldsymbol{B}^T_{2\times 3}$.

Then, according to Eq. (2), we obtain $\boldsymbol{W}_{2\times 2} = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$, then $\boldsymbol{H}_{l\times l} = \boldsymbol{W}_{2\times 2} \cdot *\boldsymbol{T}^*_{2\times 2} = \begin{pmatrix} 2 & 0 \\ 2 & 0 \end{pmatrix}$; $\tau_{AB} = \sum_{i=1}^{l}\sum_{j=1}^{l} h_{ij} = 4$.

Note that, interestingly, the term τ equals the value of $\overrightarrow{\boldsymbol{u}}_A \cdot \overrightarrow{\boldsymbol{u}}_B$. Therefore, the similarity value between Alice and Bob is: $similarity(A,B) = \frac{\tau_{AB}}{\left\|\overrightarrow{\boldsymbol{u}}_A\right\| \cdot \left\|\overrightarrow{\boldsymbol{u}}_B\right\|} = \frac{4}{\sqrt{3}\times\sqrt{6}} = 0.943$.

Similarly, we can get the value $\tau_{AC} = 5$, and the similarity value between Alice and Charles is: $similarity(A,C) = \frac{\tau_{AC}}{\left\|\overrightarrow{\boldsymbol{u}}_A\right\| \cdot \left\|\overrightarrow{\boldsymbol{u}}_C\right\|} == \frac{5}{\sqrt{6}\times\sqrt{6}} = 0.833$.

Obviously, For initiator Alice, Bob is the better matching person than Charles.

However, using the protocol EWPM proposed in [8], We can only obtain $S_{AB} = 3$ (the matching value between Alice and Bob), and $S_{AC} = 3$ (the matching value between Alice and Charles). Those values neither have strict semantic meaning, nor distinguish whether Alice is more matching with Bob or Charles. Thus, LIP3 is obviously advantage over EWPM in terms of matching accuracy (measured with profile similarity).

4 Preliminary Performance Analysis

4.1 Security Analysis

① **Schematic Proof of Privacy Level I.** Depending on secure property of the confused matrix transformation, the correctness of the LIP3 is straightforward. However, in level I privacy, through $\boldsymbol{D}_{l\times l}$, the initiator can obtain the $\boldsymbol{T}_{l\times l}$ that numerically equals $\boldsymbol{A}_{l\times n} \times \boldsymbol{B}^T_{l\times n}$, and then it is possible for initiator to infer the responder's profile matrix $\boldsymbol{B}$. However, as they are both HBC users, the initiator will not monitor the matching process and decrypt the intermediate results get the original results of $\boldsymbol{A}_{l\times n} \times \boldsymbol{B}^T_{l\times n}$, so she learns nothing about the responder other than the matching value. The privacy of the responder can be protected too.

Table 1. Complexity comparison among LIP3, EWPM and fine-grained privacy-preserving profile matching schemes

Protocol	Offline Comp.		Online Comp		Comm. (in bits)	
	Initiator	Responder	Initiator	Responder	Initiator	Responder
Fine-grained	$2l \cdot n \cdot exp_1 + l \cdot n \cdot mul_2$	–	$1 \cdot exp_2$	$1 \cdot exp_1 + 1 \cdot exp_2 + n \cdot mul_2$	$l \cdot n \cdot 2048$	$1 \cdot 2048$
EWPM Level-I	$2l \cdot n \cdot add + l \cdot n \cdot mul_1$	–	$3l \cdot l \cdot add + 2l \cdot l \cdot mul_1$	$l \cdot n \cdot add + l \cdot n \cdot mul_1$	$(l \cdot n + 2) \cdot 1024$	$l \cdot l \cdot 1024$
EWPM Level-II	$2l \cdot n \cdot add + l \cdot n \cdot mul_1$	–	$(l + 2) \cdot add$	$l \cdot n \cdot add + l \cdot n \cdot mul_1$	$(l \cdot n + 2) \cdot 1024$	$1 \cdot 1024$
LIP3 Level-I	$2l \cdot n \cdot add + (l \cdot n + l \cdot l) \cdot mul_1$	–	$3l \cdot l \cdot add + 2l \cdot l \cdot mul_1$	$l \cdot n \cdot add + l \cdot n \cdot mul_1$	$(l \cdot n + 2) \cdot 1024$	$l \cdot l \cdot 1024$
LIP3 Level-II	$2l \cdot n \cdot add + (l \cdot n + l \cdot l) \cdot mul_1$	–	$(l + 2) \cdot add$	$l \cdot n \cdot add + l \cdot n \cdot mul_1$	$(l \cdot n + 2) \cdot 1024$	$1 \cdot 1024$

② **Schematic Proof of Privacy Level II.** The key point of proving the privacy level II of LIP3 lies in that: In level II, the responder only sends σ instead of $\boldsymbol{D}_{l\times l}$ to the initiator. Even the initiator Alice has $\overrightarrow{\boldsymbol{k}}$ to get the original data, she has no way to learn the computation process. While the responder Bob knows the process, but he cannot obtain the $\overrightarrow{\boldsymbol{k}}$. In this way, the users' privacy is protected from the internal attackers.

4.2 Complexity Analysis

Similar as EWPM [8], we can also use the offline, online computation cost as well as the communication overhead to measure the complexity of the proposed scheme LIP3. The computation cost is evaluated using the number of the multiplication and exponentiation operations, since these operations are always resource-consuming in mobile devices. The communication overhead is evaluated by counting the transmitting and receiving bits.

In our paper, h represents the hash function SHA-256, exp_1 means 1024-bit exponentiation operation, exp_2 means 2048-bit exponentiation operation, *add* indicates modular addition, and mul_1 and mul_2 mean 1024-bit and 2048-bit multiplication operation, respectively.

Assume that each user's interest profile has n attributes, and the highest attribute value is l. Table 1 gives the corresponding complexities in the existing Fine-grained [4] scheme, EWPM [8], and our proposal LIP3. Note that LIP3 uses similar matching method as EWPM, so we compare the complexities of both Level-I and Level-II in those two schemes.

From Table 1, we can observe that, similar as EWPM, compared with Fine-grained scheme, LIP3 reduces computation and communication costs significantly. Specifically, in comparison EWPM, our scheme LIP3 only brings additional computation of the modules of the initiator's and responder's profile vectors, and additional transmission of a scalar value, which are all constant operations, independent of the parameters used in LIP3, e.g., the number of attributes n, and the maximal attribute value l. Those trivial additional overhead can be totally negligible.

5 Conclusion

In this paper, we propose an effective and secure CMT based privacy-preserving profile matching scheme for D2D based MSNP, LIP3, which can infer the accurate cosine similarity between two users by considering both the number of the common interests and the corresponding weights. In comparison with the existing CMT schemes (e.g., EWPM), LIP 3 can provide strict and accurate profile matching value, i.e., cosine similarity result, among individuals, without incurring extra computation and communication overhead. Therefore, LIP3 is suitable to be implemented by resource-constrained mobile devices, especially for various MSNP applications.

Acknowledgments. This work was supported by the NSFC 61171092, the JiangSu Educational Bureau Project under Grant 14KJA510004, and Prospective Research Project on Future Networks (JiangSu Future Networks Innovation Institute).

References

1. Wang, Y.F., Vasilakos, A.V., Jin, Q., Ma, J.H.: Survey on mobile social networking in proximity (MSNP): approaches, challenges and architecture. ACM/Springer, Wirel. Netw. (WINET) **20**(6), 1295–1311 (2014)
2. Wang, Y.F., Xu J.: Overview on privacy-preserving profile-matching mechanisms in mobile social networks in proximity (MSNP). In: Proceedings of the 9th Asia Joint Conference on Information Security (AsiaJCIS) (2014)
3. Niu, B., Zhang, T., Zhu, X., et al.: Priority-Aware Private Matching Schemes for Proximity-based Mobile Social Networks, arXiv preprint arXiv: 1401.8064 (2014)
4. Zhang, R., Zhang, Y., Sun, J., et al.: Fine-grained private matching for proximity-based mobile social networking. In: Proceedings of the IEEE INFOCOM (2012)
5. Zhang, R., Zhang, J., Zhang, Y., et al.: Privacy-preserving profile matching for proximity-based mobile social networking. IEEE J. Selected Areas Commun. **31**(9), 656–668 (2013)
6. Zhu, H.J., Du, S.G., Li, M.Y., Gao, Z.Y.: Fairness-aware and privacy-preserving friend matching protocol in mobile social networks. IEEE Trans. Emerg. Topics Comput. **1**(1), 192–200 (2013)
7. Lu, R., Lin, X., Shen, X.: SPOC: a secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency. IEEE Trans. Parallel Distrib. Syst. **24**(3), 614–624 (2013)
8. Zhu, X.Y., Liu, J., Jiang, S.R., Chen, Z.B, Li, H., Efficient weight-based private matching for proximity-based mobile social networks. In: Proceedings of the IEEE ICC (2014)