Journal of Zhejiang University SCIENCE A
ISSN 1009-3095 (Print); ISSN 1862-1775 (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

Protection of mobile location privacy by using blind signature*

LIAO Jian†, QI Ying-hao, HUANG Pei-wei, RONG Meng-tian, LI Sheng-hong
(*Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China*)
†E-mail: liaojian@sjtu.edu.cn

Received Sept. 21, 2005; revision accepted Jan. 9, 2006

Abstract: Location privacy means a user keeps his/her geographical location secret. If location information falls into the wrong hands, an adversary can physically locate a person. To address this privacy issue, Qi *et al*.(2004a; 2004b) proposed a special and feasible architecture, using blind signature to generate an authorized anonymous ID replacing the real ID of a legitimate mobile user. The original purpose of his architecture was to eliminate the relationship of authorized anonymous ID and real ID. We present an algorithm to break out Qi's registration and re-confusion protocol, and then propose a new mechanism based on bilinear pairings to protect location privacy. Moreover we show that the administrator or third parity cannot obtain information on the legitimate user's authorized anonymous ID and real ID in our proposed protocols.

Key words: Mobile computing, Location privacy, Security techniques and system, Blind signature, Location-based services
doi:10.1631/jzus.2006.A0984 **Document code:** A **CLC number:** TN918; TP301

INTRODUCTION

Improvements in sensor and wireless communication technology enable accurate, automated determination and dissemination of a user or object's position. There is great interest in exploiting this positional data through location-based services (LBS). Because of the widespread use of relatively cheap cellular phones or other mobile devices, many location services will be based on tracking technology to reveal the mobile user's "personal" location at any given time (Einar, 2001). This kind of threat also exists in multi-hop network, because the user's data packets must be sent to some base station, whose administrator can get the location of the mobile user.

Several studies showed that many individuals were concerned about personal privacy (Fox, 2000). To address the location privacy issue, architecture for location privacy control was presented and experimented (Gruteser *et al*., 2003; Beresford and Stajano, 2004; Gedik and Ling, 2005). Gruteser and Grunwald (2003) pointed out that anonymity could provide a high degree of privacy, save service users from dealing with service providers' privacy policies, and reduce the service providers' requirements for safeguarding private information. Moreover we think this anonymity must be authenticated. Qi *et al*.(2004a; 2004b) proposed a special architecture to protect location privacy. In Qi's architecture, a special method—blind signature—was employed to generate an authorized anonymous ID that replaces the real ID of an authorized mobile device. With authorized anonymous ID, the mobile user achieves complete personal control over location privacy while maintaining the authentication function required by the administration.

We mainly focus on analyzing the registration protocols of Qi's scheme. Qi's registration protocol was originally aimed at eliminating the relationship of real ID and authorized anonymous ID of a legitimate user. After implementation of the registration protocol, a legitimate mobile device obtains an authorized anonymous ID and is granted permission to access the wireless infrastructure. A third party, even the administrator of the wireless infrastructure, gets no

* Project (No. 60402019/F0102) supported by the National Natural Science Foundation of China

information on the relationship between authorized anonymous ID and real ID. Unfortunately we think Qi's registration protocol may not delete the linkability of the real ID and authorized anonymous ID. The same flaws exist in the re-confusion protocol. We present an algorithm to help the user understand how to break Qi's registration protocol. A full analysis of the linkability in Qi's registration protocol and re-confusion protocol is presented below. We also propose an improved registration and re-confusion protocol using the same cryptographic technique, blind signature based on bilinear pairings. We also show that the administrator cannot obtain information on the legitimate user's authorized anonymous ID and real ID. By employing technology similar to Zhang *et al*.(2003)'s, we can prove that the third party or the administrator cannot forge the valid authorized anonymous ID of any legitimate mobile user.

BLIND SIGNATURE

The concept of blind signatures introduced in (Chaum, 1982) provides anonymity of users in applications such as electronic voting, electronic payment systems, etc. In contrast to regular signature schemes, a blind signature scheme is an interactive two-party protocol between a user and a signer. It allows the user to obtain a signature on a message in a way that the signer cannot have any hint of the message or the signature of the sender. In this section we recall the formal definition and the standard security notion for blind signature schemes introduced in (Chaum, 1982; Zhang *et al*., 2003; Bellare *et al*., 2001; Boldyreva, 2003).

Syntax A blind signature scheme BS=(Kg, *Signer*, *User*, Vf) is given below:

(1) The probabilistic key generation algorithm Kg takes as input security parameters *params* and outputs a pair (pk,sk) of public-secret keys for signer.

(2) "Signer" and "User" are two interactive probabilistic Turing machines that run in polynomial time. Each machine has a read-only input tape, a write-only output tape, a read/write work tape, and a read-only random tape. The machines communicate using a read-only and a write-only tape. Both machines have a common input consisting of a public key pk produced by the key generation algorithm. As private inputs, the "Signer" machine has the secret key sk corresponding to pk, and the "User" machine has a message m to be signed. The two parties interact, and at the end of the interaction the expected local output is as follows: the "Signer" outputs one of the two messages *completed*, *not-completed*, and the "User" outputs either *fail* or a signature δ on m.

(3) The deterministic Vf verification algorithm takes as input the public key pk, a message m and a candidate signature δ and outputs 0/1, i.e., it either rejects or accepts.

It is required that for all (pk,sk) which have non-zero probability of being output by Kg, and all messages m, if $\delta \in_R$(*Signer*(sk), *User*(m)) then Vf(pk, (m,δ))=1.

Security of a blind signature scheme is in terms of three requirements: completeness, blindness and non-forgeability. Blindness must satisfy that the administrator cannot link a signature to the instance of the signing protocol that produces the corresponding blind signature. The most powerful attack on a blind signature is one-more signature forgery introduced by Bellare *et al*.(2001).

ANALYSIS ON QI'S PROTOCOL

Qi's authorized anonymous ID-based scheme

There are two phases in Qi's scheme: (1) the registration phase specified by a registration protocol, and (2) the controlled connection phase specified by a controlled connection protocol. In the first phase, a mobile user obtains an authorized anonymous ID from the Administrator of the wireless infrastructure. In the second phase the authenticated mobile device uses authorized anonymous ID to request for connection and authenticate the packets by access points. The protocol in this phase is similar to other architecture engaged in authorized ID, so discussion focuses on the registration protocols. The definition of some notations used in Qi's protocols is listed in Table 1.

Table 1 Notations used in Qi's protocols

Symbol	Definition
$E_x(m)$	Encrypt m by using key x
$H(m)$	One-way hash function with input m
$D_x(c)$	Decrypt a cipher c by using key x
r_0,r_1	Random numbers

Qi's registration protocol is presented below:

Step 1: The user generates random values r_0,r_1, encrypts $E_A(r_0)$, computes $c_0=E_A(r_0)\cdot H(r_1)$, and then sends c_0 to administrator.

Step 2: The administrator authenticates the user. If the user is permitted to access the wireless infrastructure, the registration protocol continues.

Step 3: The administrator signs c_0 by computing $c_1=D_A(c_0)=r_0D_A(H(r_1))$ and then sends c_1 to the user.

Step 4: The user removes the blind factor $id=c_1/r_0$.

Step 5: Verification: If $E_A(id)\neq H(r_1)$ then abort. If the former equation holds, the user keeps *id* as authorized anonymous ID.

Analysis of Qi's registration protocol

The purpose of Qi's registration protocol is eliminating the relationship of real ID and authorized anonymous ID of a legitimate user. After implementing the registration protocol, a legitimate mobile user obtains an authorized anonymous ID and is granted permission to access the wireless infrastructure. The user hides the authorized anonymous ID only by multiplying a blind factor r_0, so the security of the blind signature scheme adopted in Qi's protocol is based on factorization. It means if we get any one of the two big primes, this kind of blind signature scheme will be defeated.

Now we start to break Qi's registration protocols. Assume that n users U_i (i=1, …, n) want to access to the wireless infrastructure, we present an algorithm B below that the administrator of wireless infrastructure breaks Qi's registration protocols:

Step 1: Acting just as Step 1 and Step 2 of Qi's registration protocols. The user U_i (i=1, …, n) randomly chooses values r_{0i}, r_{1i}, computes $c_{0i}=E_A(r_{0i})\cdot H(r_{1i})$, and then sends c_{0i} to the administrator. The administrator authenticates the user U_i. The administrator monitors the communication with the user U_i (i=1, …, n) and records the tuple $\{(U_i, c_{0i})\}$.

Step 2: The administrator signs c_{0i} by computing $c_{1i}=D_A(c_{0i})=r_{0i}D_A(H(r_{1i}))$, sends c_{1i} to the user U_i and records the tuple $\{(U_i, c_{0i}, c_{1i})\}$. Just as Step 4 and Step 5 of Qi's registration protocols describe, the user U_i obtains its corresponding authorized-anonymous identity id_i. Although maintaining the list L_1:$\{(U_1, c_{01}, c_{11}), (U_2, c_{02}, c_{12}), \ldots, (U_n, c_{0n}, c_{1n})\}$ and L_2:$\{id_1, id_2, \ldots, id_n\}$, the administrator does not know at all the relationship of L_1 and L_2, namely, the relationship of $\{U_1, U_2, \ldots, U_n\}$ and $\{id_1, id_2, \ldots, id_n\}$.

Step 3: Assume that an authorized-anonymous identity $id'\in L_2$ was chosen, the administrator wants to find out the corresponding real user's identity from L_1. The administrator encrypts id' by computing $E_A(id')$. For j=1, the administrator gets r_{0j} by computing $c_{1j}(id')^{-1}$ and then verifies whether equation below holds:

$$c_{0j} = E_A(r'_{0j})\cdot E_A(id'). \tag{1}$$

If Eq.(1) holds, the administrator finds out that c_{0j} comes from id'. Furthermore the linkability between the user's real ID U_j and id' will also be compromised. Otherwise the administrator increases so that $j=j+1$, $j\in(1, 2, \ldots, n)$ and repeats Step 3 mentioned above, if $j>n$, the administrator fails to break Qi's registration protocols.

Now we demonstrate the validity of Eq.(1). For some $j\in(1, 2, \ldots, n)$, we assume the administrator finds out the relationship between the real identity of the user U_j and his/her authorized anonymous identity id'. Namely, the administrator gets a tuple $\{(U_j, c_{0j}, c_{1j}, id')\}$ in which four elements must satisfy Eq.(1). We deduce Eq.(1) as follows:

$$\begin{aligned} &E_A(r'_0)\cdot E_A(id') \\ &\quad=E_A(c_1\cdot(id')^{-1})\cdot E_A(D_A(H(r_1))) \\ &\quad=E_A(r_0\cdot D_A(H(r_1))\cdot(D_A(H(r_1)))^{-1})\cdot H(r_1) \\ &\quad= E_A(r_0)\cdot H(r_1)=c_0. \end{aligned} \tag{2}$$

Obviously, when id' does not correspond to view c_{0j}, c_{1j}, Eq.(2) is not true due to different random values r_{0j}, r_{1j} included in id' and c_{0j}. Otherwise, the administrator can find out the linkability between id' and c_{0j}, which reveal the relationship between real ID U_j ($j\in$1, 2, …, n) and anonymous ID id'.

It is good that Qi introduced Chaum's RSA blind signature to protect the location privacy. But the reason why their analysis of the unlinkability is wrong is that they did not consider that the randomness r_0 introduced during the blinding phase can be removed easily. From the analysis above, we easily know that the re-confusion protocol also has the same fault.

OUR IMPROVED PROTOCOL

Bilinear pairing and gap Diffie-Hellman groups

Our protocol is based on bilinear pairings. We introduce some definitions and notations below. Let G_1 be a cyclic group generated by P, whose order is a prime p, and G_2 be a cyclic multiplicative group of the same order p. The discrete logarithm problems in both G_1 and G_2 are difficult. Let e: $G_1\times G_1\to G_2$ be a pairing which satisfies the following properties:

(1) Bilinearity: $e(P_1+P_2,Q)=e(P_1,Q)e(P_2,Q)$ and $e(aP, bQ)=(e(P,Q))^{ab}$;

(2) Non-degeneration: There exists P, $Q\in G_1$ such that $e(P,Q)\neq 1$;

(3) Computability: There is an efficient algorithm to compute $e(P,Q)$, $\forall P$, $Q\in G_1$.

Definition 1 Given an element P of a group G and a 2-tuple (P,aP), the discrete logarithm problem (DLP) is to compute a. It is a difficult math problem.

Definition 2 Given a generator P of a group G and a 3-tuple (aP,bP,cP), the decisional Diffie-Hellman problem (DDH problem) is to decide whether $c=ab$.

Definition 3 Given a generator P of a group G and a 2-tuple (aP,bP), the computational Diffie-Hellman problem (CDH problem) is to compute abP.

Definition 4 If G is a group such that the DDH problem can be solved in polynomial time but no probabilistic algorithm can solve CDH problem with non-negligible advantage within polynomial time, then we call G a gap Diffie-Hellman (GDH) group.

We assume the existence of a bilinear map e: $G_1\times G_1\to G_2$ that one can solve DDH problem in polynomial time.

Improved registration protocol

The proposed registration protocol is aimed at eliminating the relationship between the real ID and the authorized anonymous ID. Our scheme is presented below:

Step 1: The user generates random values r_0, $r_1\in {}_RZ_P^*$, computes $c_0=H(r_1)+r_0P_{\text{pub}}$, and then sends c_0 to the administrator.

Step 2: The administrator authenticates the user. If the user is permitted to access the wireless infrastructure, the registration protocol continues.

Step 3: The administrator signs c_0 by computing $c_1=x^{-1}c_0$ and then sends c_1 to the user.

Step 4: The user removes the blind factor $id=c_1-r_0P$. The user verifies whether the equation $e(P_{\text{pub}},id)=e(P,H(r_1))$ holds. If it holds, the anonymous ID id is a valid ID. Or the user aborts and goes to Step 1.

Step 5: Verification: If $e(P,H(r_1))\neq e(P_{\text{pub}},id)$ then abort. If the former equation holds, the user keeps id as authorized anonymous ID.

Due to limitation of the paper's length, modified re-confusion protocol is omitted here.

ANALYSIS OF OUR PROTOCOL'S SECURITY

From the perspective of the cryptanalysis, we present our security proof. We must guarantee that (1) the mobile user obtains complete authorized anonymous ID, (2) the administrator cannot obtain any information on the legitimate user's authorized anonymous ID and real ID, and (3) the third party or the administrator cannot forge any authorized anonymous ID. For simplicity we only analyze the registration protocol, which is the prototype of the re-confusion protocol.

Completeness

The completeness can be verified by the follow equations:

$$\begin{aligned} e(P_{\text{pub}},id)&=e(xP,c_1-r_0P)=e(xP,x^{-1}c_0-r_0P)\\ &=e(xP,x^{-1}(H(r_1)+r_0P_{\text{pub}})-r_0P)\\ &=e(xP,x^{-1}H(r_1)+r_0P-r_0P)=e(P,H(r_1)). \end{aligned} \quad (3)$$

The demonstration presented above ensures that the legitimate mobile user obtains the correct authorized anonymous ID.

Blindness

Considering our registration protocol, we can prove that the administrator cannot obtain any information on the legitimate user's authorized anonymous ID and real ID, which is similar to the proof of blindness property in (Zhang *et al*., 2003).

To prove the blindness of our scheme, we show that given a valid authorized anonymous ID id and any view (c_0,c_1), there always exists a unique blinding factor $r_0\in {}_RZ_P^*$. Since the blinding factor r_0 is chosen randomly, the blindness of the signature scheme is naturally satisfied.

Given a valid *id* and any view (c_0,c_1), then the two equations below must hold for r_0.

$$c_0=H(r_1)+r_0P_{\text{pub}}, \quad (4)$$

$$id=c_1-r_0P. \quad (5)$$

From Eq.(5), we can deduce that r_0' exists uniquely. Next, we must verify such r_0' satisfies Eq.(4) too.

Since *id* is a valid authorized anonymous ID, we get

$$e(P,H(r_1))=e(P_{\text{pub}},id). \quad (6)$$

Now we consider whether Eq.(4) holds for such r_0':

$$\begin{aligned} &e(H(r_1)+r_0'P_{\text{pub}},P)\\ &=e(H(r_1),P)e(r_0'P_{\text{pub}},P)\\ &=e(id,P_{\text{pub}})e(r_0'P_{\text{pub}},P)\\ &=e(c_1-r_0'P,P_{\text{pub}})e(r_0'P,P_{\text{pub}})\\ &=e(c_1,P_{\text{pub}})=e(x^{-1}c_0,P_{\text{pub}})=e(c_0,P), \end{aligned} \quad (7)$$

where Eqs.(5) and (6) and equation $c_1=x^{-1}c_0$ are used.

From the property of non-degeneration of the bilinear pairing, we have

$$c_0=H(r_1)+r_0P_{\text{pub}}\leftrightarrow e(H(r_1)+r_0P_{\text{pub}},P)=e(c_0,P). \quad (8)$$

Hence the blind factors r_0 always exist which lead to the same relation defined in our registration protocol, so any view of our blind signature is unlinkable to any valid authorized anonymous ID.

Unforgeability

In our registration protocol forgeability means that a third party or the administrator of wireless infrastructure can forge a valid authorized anonymous ID related to real ID of any legitimate mobile user. Actually, the forgeability cannot bring bad effect on personal control over location privacy, but we still give the method to prove the un-forgeability of our scheme. The accepted formalization of security for blind signature is security against one-more forgery. Bellare *et al*.(2001) promoted Chosen Target RSA Inversion assumption and suggested that an analogue of this assumption can be formulated for any family of one-way functions. Similar to the proof of security in (Bellare *et al*., 2001), Boldyreva (2003) reduced the security in the sense of unforgeability of their blind signature scheme to the Chosen-Target CDH assumption. Security of the RSA blind signature was proven to be secure assuming difficulty of the chosen target RSA inversion problem. Based on the contribution of (Bellare *et al*., 2001; Boldyreva, 2003), Zhang *et al*.(2003) defined Chosen-Target Inversion CDH assumption and proved the security of their blind signature scheme on this assumption. Assuming that Chosen-Target Inversion CDH problem is difficult, we can also use technique similar to that above to prove that our scheme prevents from one-more forgery under chosen message attacks. We present the following theorem:

Theorem 1 If the chosen-target inverse CDH assumption is difficult in the group G_1, then our blind scheme is secure against one-more forgery under chosen message attacks.

Due to this paper's limitation in length, the security proof is omitted here.

CONCLUSION

Qi He adapted a special and feasible method, blind signature, to generate an authorized anonymous ID that replaces the real ID of an authorized mobile device. They presented two-phase protocol to address location privacy, but did not consider that the randomness r_0 introduced during the blinding phase can be removed easily. We prove that the administrator can link real ID with authorized anonymous ID. Furthermore we propose an improved registration and re-confusion protocol using the same cryptographic technique, blind signature based on bilinear pairings. Analyzing the security of our proposed protocols we conclude that the administrator cannot obtain any information on the legitimate user's authorized anonymous ID and real ID.

References

Bellare, M., Namprempre, C., Pointcheval, D., Semanko, M., 2001. The One-More-RSA-Inversion Problems and the Security of Chaum's Blind Signature Scheme. Financial Cryptography'01. Springer LNCS, **2339**:319-338.

Beresford, A.R., Stajano, F., 2004. Mix Zones: User Privacy in Location-Aware Services. Proceedings of the Second IEEE Annual Conference, Pervasive Computing and Communications Workshops'04, p.127-131. [doi:10.1109/PERCOMW.2004.1276918]

Boldyreva, A., 2003. Efficient Threshold Signature, Multisignature and Blind Signature Schemes Based on the Gap-Diffie-Hellman Group Signature Scheme. Public Key Cryptography-PKC'03. Springer LNCS, **2139**: 31-46.

Chaum, D., 1982. Blind Signatures for Untraceable Payments. Proceedings of Crypto'82.

Einar, S., 2001. Concepts for Personal Location Privacy Policies. Proceedings of the ACM Conference on Electronic Commerce (EC'01), p.48-57.

Fox, S., 2000. The Internet Life Report. Trust and Privacy Online: Why Americans Want to Rewrite the Rules. The Pew Internet & American Life Project, available at: http://www.pewinternet.org/reports/pdfs/PIP_Trust_Privacy_Report.pdf.

Gedik, B., Ling, L., 2005. Location Privacy in Mobile Systems: A Personalized Anonymization Model. Proceedings of 25th IEEE International Conference on Distributed Computing Systems (ICDCS 2005), p.620-629. [doi:10.1109/ICDCS.2005.48]

Gruteser, M., Grunwald, D., 2003. Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking. Proceedings of ACM/USENIX International Conference on Mobile Systems, Applications, and Services.

Gruteser, M., Schelle, G., Jain, A., Han, R., Grunwald, D., 2003. Privacy-Aware Location Sensor Networks. Proceedings of HotOS'03, 9th Workshop on Hot Topics in Operating Systems, USENIX, p.163-168.

Hills, A., 1999. Wireless andrew. *IEEE Spectrum*, **36**(6):49-53. [doi:10.1109/6.769269]

Qi, H., Wu, D., Khosla, P., 2004a. The quest for personal control over mobile location privacy. *IEEE Communications Magazine*, **42**(5):130-136. [doi:10.1109/MCOM.2004.1299356]

Qi, H., Wu, D., Khosla, P., 2004b. A Mechanism for Personal Control over Mobile Location Privacy. Proceedings of IEEE/ACM First International Workshop on Broadband Wireless Services and Applications, BroadWISE 2004.

Zhang, F., Safavi-Naini, R., Susilo, W., 2003. Efficient Verifiably Encrypted Signature and Partially Blind Signature from Bilinear Pairings. Progress in Cryptology-INDOCRYPT'03. Springer LNCS, **2904**:191-204.