ID-Based Signature Scheme for Mobile Payment

Maocai Wang[ξ,£] , Guangming Dai[ξ], Hanping Hu[£], Lei Pen[ξ]

[ξ]School of Computer
China University of Geosciences
388 Lumo Road, Hongshan District, Wuhan City,
Hubei Province, China

[£]Institute for Pattern Recognition and Artificial Intelligence
Huazhong University of Science and technology
1037 Luoyu Road, Hongshan District, Wuhan City,
Hubei Province, China

wmc@2001.cug.edu.cn,gmdai@cug.edu.cn,hphu@mail.hust.edu.cn,penglei0114@126.com

ABSTRACT

A main concern in the public key distribution is the authenticity of the public key. Authenticating public keys provides assurance to the entity that the received public key corresponds to the sender's identity. A typical approach to guarantee the authentication of the public key holder relies on a trusted agent named Certificate Authority (CA). The signature based CA binds entity's identity ID to the corresponding public key KU. However, in the mobile payment system, the CA not only adds the system's complexity but also increase the user charge. Therefore, it is the worst security problem in the mobile payment systems that there is no signature so that the non-repudiation service can not effectively be protected. In this paper, an ID-based signature scheme for mobile payment is put forward. In the signature scheme, the public key is the ID of the mobile user or can be obtained by the ID so that the user does not need to access the CA to obtain the public key. This feature is especially desirable for transaction-type mobile applications such as mobile payment. Therefore, the signature scheme can effectively provide the non-repudiation service for mobile payment.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design – *network communication, wireless communication;* E.3 [Data Encryption]: Public key cryptosystems

General Terms

Algorithms, Security

Keywords

ID-Based; Signature Scheme; Mobile Payment; Bilinear Pairing

Mobimedia 2008 July 7-9, 2008, Oulu, Finland.
Copyright 2008 ICST ISBN 978-963-9799-25-7/08/07
DOI 10.4108/ICST.MOBIMEDIA2008. 3924

1. INTRODUCTION

Along with the fast-progressing internet and mobile network in recent years, various kinds of e-commerce emerged, which makes people's life more convenient and colorful. Mobile payment, being incentive to further development of e-commerce, will become the main payment means of e-commerce by and by. The market size of the domestic mobile payment in recent years is shown in the figure 1[1].

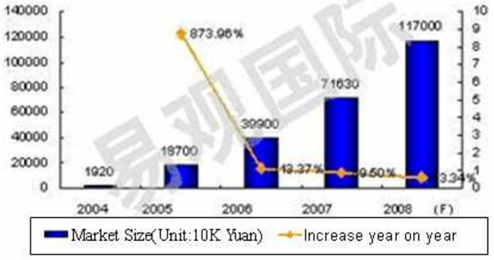

Figure 1. The market size of mobile payment in China in recent years

However, in the mobile payment system, the Certificate Authority (CA) not only adds the system's complexity but also increase the user charge. Therefore, it is the worst security problem in the mobile payment systems that there is no signature so that the non-repudiation service can not effectively be protected[2]. In this paper, an ID-based signature scheme for mobile payment is put forward, in which the public key distribution does not rely on the CA.

2. ID-based Public Key Cryptosystem

Shamir proposed the identity-based (ID-based) public key approach to support public key cryptography without the use of certification[3]. In ID-based public key cryptosystem, user A's public key KU_A is not delivered to user B. User B encrypts a message for user A or verifies a signature from user A using a public key which is derived from user A's identifier IDA (e.g., email address or telephone number; see Fig.2 (3)). The trusted agent has a new role in ID-based public key cryptosystem, and is renamed as the Private Key Generator (PKG)[4]. The PKG issues the private key corresponding to the public key (derived from the identifier ID_A) to user A over a secure channel (Fig.2 (2)). This issuing action takes place after user A is authenticated by the PKG (Fig.2 (1)). To generate private keys, the PKG makes use of a master key which must be kept in secret. The requirement to have an authentic CA's public key for verifying certificates in certificate-based cryptosystem is replaced by the requirement to have authentic PKG's system parameters in ID-based cryptosystem. Notice that both the PKG and the user A know the private key KR$_A$.

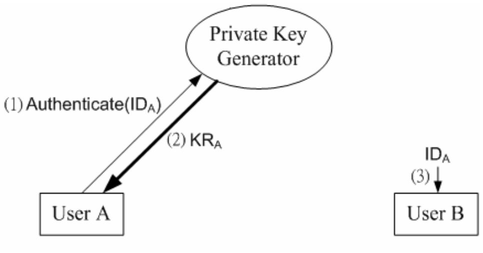

Figure 2. The ID-based public-key distribution

3. ID-based Signature Scheme for Mobile Payment

In the conventional signature scheme, the server needs to communicate with the public key directory for requesting the public key. If the request fails (e.g., the directory server is down), the server can not verify the signature for the user. On the other hand, in an ID-based signature scheme, the server simply uses the user's ID (i.e., the telephone number) as his public key without any request and verification. Thus, the server does not need to access any public key directory before verifying a signature.

The first complete and efficient ID-based encryption scheme was proposed by Boneh and Franklin which uses a bilinear map called Weil pairing over elliptic curves[5]. The bilinear map transforms a pair of elements in group G_1 and sends it to an element in group G_2 in a way that satisfies some properties. The most important property is the bilinearity that it should be linear in each entry of the pair. Assume that P and Q are two elements (e.g., points on elliptic curves) of an additive group G_1. Let $e(P,Q)$ be the element of a multiplicative group G_2, which is the pairing applied to P and Q. Then the pairing must have the following property:

$$e(rP,Q) = e(P,Q)^r = e(P,rQ)$$

Where r is an integer and rP denotes the element generated by r times of additions on P. Weil pairing on elliptic curves is selected as the bilinear map. That is, the elliptic curve group (the set of point collection on elliptic curves) is used as G_1 and the multiplicative group of a finite field is used as G_2.

An identity based signature scheme consists of four algorithms: Setup, Extract, Sign and Verify[6-9]. There are three parties in a signature scheme for mobile payment, the trust authority (or TA), the user and the server. Setup is run by the PKG to generate the master key and the system parameters. This is done on input of a security parameter k_{ID}, which specifies the bit length of the group order and is regarded as the key size of the ID-based scheme. The extraction algorithm is carried out by the PKG to generate a private key corresponding to the identity of a user. As with regular public key cryptography, the signing algorithm takes a message and the user's private key as inputs to produce a signature. Similarly, the verification algorithm is executed by the server to verify the signature with the user's public key, which can be obtained by the user's ID (i.e., the mobile number). The signature scheme described as follows.

Let $t: G \times G -> V$ be a Tate pairing. We assume that $t(a,b)$ can be easily computed for any given random $a,b \in G$ while for any given random $b \in G$ and $c \in V$, it should be infeasible to compute $a \in G$ such that $t(a,b) = c$. We define two hash functions

$$H: \{0,1\}^* -> G \setminus \{0\}$$

$$H^{/}: \{0,1\}^* \times G -> Z_q$$

3.1 Setup

The TA picks a random element $P \in G \setminus \{0\}$ and a secret integer $t \in Z_q$. The TA then computes

$$Q_{TA} = tP$$

and publishes (P, Q_{TA}). The value t is stored only by the TA.

3.2 Extract

This algorithm is performed by the TA when a user requests the secret key corresponding to their identity. Suppose the user's identity is given by the string ID. The public key of the user is then given by

$$Q_{ID} = H(ID)$$

Whilst the private key is computed by the TA as

$$S_{ID} = tQ_{ID}$$

and this value is send to the user.

3.3 Sign

To sign a message m (included Merchant_ID, Merchant_AccountNo, electrCheck_ID, User_AccountNo, User_Payment, etc), the user picks a random integer $k \in Z_q$ and then computes:

1. $r = kP$
2. $v = H^{/}(m,r)$
3. $u = (v/k)S_{ID}$

The pair $(u,r) \in (G \setminus \{0\}, G \setminus \{0\})$ is the signature and then it is send to the server.

3.4 Verify

On receiving a message m and it's signature (u,r), the server computes:

1. $v = H^{/}(m,r)$

2. Accept the signature if and only if $t(u,r) = t(Q_{ID}, Q_{TA})^{v}$.

That this verification equation holds for a valid signature follows from the following algebra:

$$t(u,r) = t((v/k)S_{ID}, kP)$$

$$= t(S_{ID}, P)^{v}$$

$$= t(Q_{ID}, Q_{TA})^{v}$$

The ID-based signature scheme for mobile payment is illustrated in Fig.3. The PKG(Fig.3 (1)) constructs the ID-based cryptosystem. Every mobile user involved in the ID-based cryptosystem is given a subscriber identity module (SIM) card (Fig.3 (2)) at the subscription time. The ID (phone number; e.g., 13123456789 in Fig.3 (3)) and its corresponding private key KR are loaded in the SIM card by the end-to-end security service provider. Note that for standard GSM service, SIM card is always given to a mobile user at the subscription time and the proposed ID-based signature scheme can be pre-loaded into the SIM card without incurring any extra overhead. The mobile phone and server contains two security modules: ID-based signing module (Fig.3 (5)) and ID-based verification module (Fig.3 (10)). When a mobile user wants to sign a payment message (included Merchant_ID, Merchant_AccountNo, electrCheck_ID, User_AccountNo, User_Payment, etc) to server, the user uses his private key KR(Fig.3 (4)) stored in the SIM card to sign the message through the ID-based signing module and obtain the signature. The signature is broadcast by the base station(Fig. 3 (6)) and received by the SMS (Short Message Service) center(Fig. 3 (7)). Then the signature is sent to the server by Internet(Fig. 3 (8)). The server use the user's phone number 13123456789 (Fig.3 (9)) as the public key and verifies the signature through the ID-based verification module and obtain the original payment message.

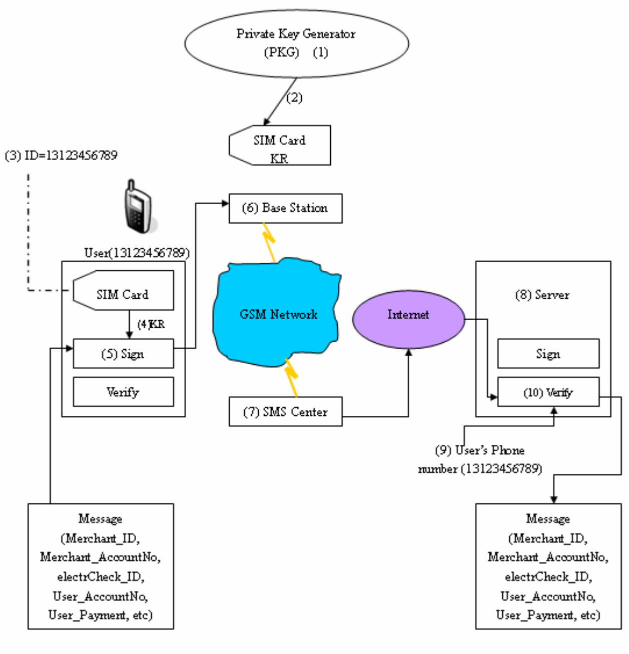

Figure 3. ID-based signature scheme for mobile payment

4. Conclusion

In the mobile payment system, the CA not only adds the system's complexity but also increase the user charge. Therefore, it is the worst security problem in the mobile payment systems that there is no signature so that the non-repudiation service can not effectively be protected. In this paper, an ID-based signature scheme for mobile payment is put forward. In the signature scheme, the public key of a user can be derived from the public information that uniquely identifies the user such as the telephone number, and hence implicitly known to all other users. A major advantage of ID-based signature scheme is that no certificate is needed to bind user names with their public keys. The ID-based signature scheme provides security enhancement to the mobile applications without requiring the users to memorize extra public keys. This feature is especially desirable for transaction-type mobile applications such as mobile payment. Therefore, the signature scheme can effectively provide the non-repudiation service for mobile payment.

5. ACKNOWLEDGMENTS

This research is supported by the National 863 High Tech. Foundation in Information Security under Grant No. 2006AA01Z426 and the Research Foundation for Outstanding Young Teachers, China University of Geosciences (Wuhan) under Grant No. CUGQNL0727.

6. REFERENCES

[1] TRPC. Mobile payments in Asia Pacific.2007.9

[2] Visa International Service Association. 3-D Secure: Mobile Authentication Scenarios,2002

[3] A. Shamir. Identity-based Cryptosystems and Signature Scheme. Proc. CRYPTO'84, 1984: 47-53

[4] J. S. Hwu, S.F. Hsu, Y.B. Lin, etc. End-to-end Security Mechanisms for SMS. International Journal of Security and Networks, 2006(1):177-183

[5] D. Boneh and M. Franklin.Identity-based Encryption from the Weil Pairing. USA, Proc. CRYPTO’01, 2001:213–239

[6] M.C. Wang, H.P. Hu, G.M. Dai. An Efficient Signature Scheme Based on Tate Pairing. Proc. ICICIC’2007, 2007:616-618

[7] K. G. Paterson. ID-based Signatures from Pairings on Elliptic Curves. Electronics Letters 38(18), 2002, 1025-1026

[8] F. Zhang, R.S. Naini and W. Susilo. An efficient signature scheme from bilinear pairings and its applications. Proc. Cryptology-CPKC’04, 2004:277-290

[9] D. Boneh, B. Lynn and H. Shacham. Short signatures from the Weil pairing. Proc. Cryptology- ASIACRYPT’2001, Springer-Verlag, LNCS 2248, 2001, 514-532