An Efficient Certificateless Blind Signature Scheme in the Random Oracle Model

Hao Xu, Baoyuan Kang, and Yongzheng Niu

School of Computer Science and Software Engineering,
Tianjin Polytechnic University, Tianjin, 300387, China
23880797@qq.com, baoyuankang@aliyun.com, niuer890214@163.com

Abstract. The blind signature schemes are useful in some applications where the anonymity is a thorny issue. The certificateless public key cryptography (CL-PKC) can eliminate the certificate management problem and solve the key escrow problem. In this paper, we put forward a secure and efficient CLBS scheme. We then illustrate that our new scheme is secure in the random oracle model. Also, we theoretically validate that our proposed scheme is more efficient than those existing ones in terms of computational complexity. We hope to transfer our scheme into applications.

Keywords: Certificateless blind signature, Certificateless public key cryptography, Random oracle model, Computational Diffie-Hellman problem.

1 Introduction

The blind signature was first proposed by Chaum [1], which can provide the anonymity of signed message. Informally, blind signature allows the message owner blind the message by the blind factors, and then lets the signer sign the blinded message. At last, the message owner eliminates the blind factors of signature to get the signer's signature of the original message. Blind signature is a special digital signature, it must also meet the property of blindness differing from other signatures. Therefore, blind signature schemes can used in order to eliminate the possible abuse of linkability.

Up to now, even if there have been a lot of researches for blind signature, most of works have been based on a traditional public key infrastructure (PKI) or an identity-based public key cryptography (ID-PKC). In the traditional PKI, the trusted Certificate Authority (CA) needs a large amount of storage and computing time to manage the certificates, which are signatures of CA on the public keys of users. This is called certificate management problem. In the ID-PKC, an inherent problem of ID-PKC is that a Key Generation Center (KGC) generates any user's private key with a master key of KGC. Obviously, a malicious KGC is able to forge the signature of any signer. This is key escrow problem. To tackle the problems above, Al-Riyami and Paterson [2] put forward a new paradigm named certificateless public key cryptography (CL-PKC) in 2003, which avoids the certificate management problem in traditional PKI and eliminates the key escrow problem in ID-PKC.

C.-H. Hsu et al. (Eds.): NPC 2014, LNCS 8707, pp. 563–566, 2014.

Blind signature and CL-PKC have gotten fruitful achievements since they were introduced. However, to our best knowledge, little attention has been paid to the design of provably secure blind signature scheme in CL-PKC [3]. In this paper, we propose an efficient CLBS scheme based on bilinear pairings, then show that our CLBS scheme is existentially unforgeable in the random oracle model under the Computational Diffie-Hellman (CDH) problem.

The remainder of this paper is organized as follows: In Section 2, we present the construction of our new CLBS scheme. We will show that our scheme is security in Section 3. Section 4 shows efficiency comparison with the existing schemes.

2 Certificateless Blind Signature Scheme

In this section, we propose a secure and efficient CLBS scheme. It consists of the following seven algorithms. The details are shown as follows:

- Setup: On the input of a security parameter k, the KGC firstly selects a cyclic additive group G_1 generated by a generator P of prime order q, a cyclic multiplicative group G_2 with the same order q and a bilinear map $e: G_1 \times G_1 \to G_2$, picks the master key master-key $s \in {}_R Z_q^*$ at random and keeps s secret, then sets $P_{pub} = sP$ as the public key. Choose three secure hash functions: $H_1 : \{0,1\}^* \to G_1$, $H_2 : \{0,1\}^* \to G_1$, $H_3 : \{0,1\}^* \to Z_q^*$. The system parameters are params $= \{G_1, G_2, q, e, P, P_{pub}, H_1, H_2, H_3\}$.
- Partial-Private-Key-Extract: For a user with identity $ID_A \in \{0,1\}^*$, KGC computes $Q_{\mathrm{A}} = H_1(ID_A)$ as the public identity of the user, and sends D_A to the user as his partial private key via a secure channel, where $D_A = sQ_A$.
- Set-Secret-Value: Given params, the user with identity ID_A selects a random $x_A \in {}_R Z_q^*$ as his secret value.
- Set-Public-Key: This algorithm accepts params, a user's identity ID_A and secret value x_A, then outputs the public key $P_A = x_A P$ of the user with identity ID_A.
- Set-Private-Key: This algorithm takes as input params, the signer's identity ID_A, partial private key D_A, public key P_A and secret value x_A to produce the signer's private key $SK_A = D_A + x_A T_A$, where $T_A = H_2(ID_A, P_A)$.
- Issue: To sign a message m, the signer with identity ID_A, public key P_A, private key SK_A, executes the following steps with the signature requester:

  (a) Request: The requester requests the signer for a CLBS. After receiving the request, the signer chooses $r \in {}_R Z_q^*$ at random and computes $R' = rP$, then sends R' to the requester.

(b) Blind: Upon receiving R', the requester randomly picks $\alpha, \beta \in {}_R Z_q^*$ as the blind factors, computes $R = \alpha R' + \beta P$, $h' = H_3(m, ID_A, P_A, R)$ and $h = \alpha^{-1} h'$, then sends h back to the signer.

(c) Sign: The signer sends S' to the requester, where $S' = hSK_A + rP_{pub}$.

(d) Unblind: The requester unblinds S' by computing $S = \alpha S' + \beta P_{pub}$, and outputs $\sigma = (R, S)$ as the CLBS on message m.

- Verify: For a message m, and the corresponding signature $\sigma = (R, S)$, the verifier computes the value $h' = H_3(m, ID_A, P_A, R)$, $T_A = H_2(ID_A, P_A)$, then check if the equation:

$$e(S, P) = \left(e(Q_A, P_{pub})e(T_A, P_A)\right)^{h'} e(R, P_{pub})$$

holds. If the equation holds, the signature $\sigma = (R, S)$ is valid.

3 Security

About the security of our CLBS scheme, we have the following two theorems.

Theorem 1. The CLBS scheme is blindness.

Theorem 2. The CLBS scheme is existentially unforgeable under assuming that the CDH problem in a cyclic additive group G_1 is intractable.

4 Efficiency Analysis

We compare our scheme with other three available CLBS schemes [4-6] based on bilinear pairings in terms of secret key size and the required computational cost of signing and verifying. For our scheme, we omit the computation efforts which can be pre-computed by the verifier, for example, the computation of $e(Q_A, P_{pub})$ and $e(T_A, P_A)$. For convenient comparison, we include the following presentation, the notion $|G_1|$ denotes the bit length of an element in G_1, $|q|$ be the binary length of an element in Z_q, P_m be the scalar multiplication on the curve, P_{ex} be the exponentiation operator in G_2 and P_e be the bilinear pairing operation.

Table 1. Performance comparison of different schemes

Scheme	Sign	Verify	Secret key length
[4]	$3P_e+4P_{ex}+7P_m$	$1P_e+1P_{ex}+2P_m$	$\lvert q\rvert+\lvert G_1\rvert$
[5]	$2P_e+1P_{ex}+8P_m$	$3P_e+1P_{ex}+2P_m$	$\lvert q\rvert+\lvert G_1\rvert$
[6]	$3P_e+2P_{ex}+9P_m$	$2P_e+1P_{ex}$	$\lvert q\rvert+\lvert G_1\rvert$
Our scheme	$7P_m$	$2P_e+1P_{ex}$	$\lvert G_1\rvert$

From Table 1, we can clearly see that a prominent merit in our scheme is that no pairing operator is required in the whole signing process. To our best knowledge the computation of the pairing is the most time-consuming in pairing based cryptosystem. Besides, the length of the secret key is also shorter than other schemes. Thus, our scheme is more useful and efficient than the previous schemes.

5 Conclusion

In this paper, we put forward a new CLBS scheme on the bilinear pairings, and give some theorems of the security and efficiency analysis of our scheme, which show that the new proposed CLBS scheme is much more efficient and satisfy both blindness and unforgeability properties. Our CLBS scheme may have applications in areas such as electronic cash systems using CL-PKC.

References

1. Chaum, D.: Blind Signatures for Untraceable Payments. In: Crypto, pp. 199–203 (1982)
2. Al-Riyami, S.S., Paterson, K.G.: Certificateless Public Key Cryptography. In: Laih, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 452–473. Springer, Heidelberg (2003)
3. Zhang, L., Zhang, F.T., Qin, B., Liu, S.B.: Provably-secure Electronic Cash Based on Certificateless Partially-blind Signatures. Electronic Commerce Research and Applications 10(5), 545–552 (2011)
4. Zhang, L., Zhang, F.: Certificateless Signature and Blind Signature. Journal of Electronics (China) 25(5), 629–635 (2008)
5. Zhang, L., Zhang, F., Qin, B., et al.: Provably-secure Electronic Cash Based on Certificateless Partially-blind Signatures. Electronic Commerce Research and Applications 10(5), 545–552 (2011)
6. Liu, J., Zhang, Z., Sun, R., et al.: Certificateless Partially Blind Signature. In: 2012 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 128–133. IEEE (2012)