Intelligent Information Management, **2010, 2, 559-562**
doi:10.4236/iim.2010.29064 Published Online September 2010 (http://www.SciRP.org/journal/iim)

Improvement of Chen-Zhang-Liu's IRPB Signature Scheme

Dezhi Gao
College of Information Science and Engineering, Shandong University of Science and Technology, Qingdao, Shandong, China
E-mail: *dezhi_gao@yahoo.com.cn*
Received June 8, 2010; *revised July* 18, 2010; *accepted August* 21, 2010

Abstract

Restrictive partially blind signatures incorporate the advantages of restrictive blind signatures and partially blind signatures, which play an important role in electronic commerce. Recently, Chen-Zhang-Liu first proposed an ID-based restrictive partially blind (IRPB) signature from bilinear pairings. Later, Hu-Huang showed that the Chen-Zhang-Liu's scheme has a security weakness, and pointed out that their scheme does not satisfy the property of restrictiveness as they claimed. In this paper, we improve Chen-Zhang-Liu's scheme and propose a new signature scheme from bilinear pairings. The improved scheme can resist the Hu-Huang's attack.

Keywords: Cryptography, Bilinear Pairings, Restrictiveness, Partially Blind Signature, ID-Based Restrictive Partially Blind Signature

1. Introduction

Blind signature scheme were first introduced by Chaum [1] to protect the right of an individual privacy. A blind signature allows a user to acquire a signature without giving the signer any information about the actual message or the resulting signature. And blind signature techniques have been widely used in anonymous electronic cash(e-cash) and anonymous voting systems.

Restrictive blind signatures firstly introduced by Brands [2], which allows a user to receive a blind signature on a message not known to the signer but the choice of message is restricted and must conform to certain rules. Furthermore, he proposed a highly efficient electronic cash system, where the bank ensures that the user is restricted to embed his identity in the resulting blind signature.

A partially blind signature scheme allows a signer to produce a blind signature on a message for a user, where the signature explicitly includes common agreed information which remains clearly visible despite the blinding process. The concept was first introduced by Abe and Fujisaki[3].

In an electronic cash system, embedding user identity information in the blind signature enables the bank to learn the identity of double spenders. Maitland and Boyd [4] first proposed a provably secure restrictive partially blind signature scheme, which satisfies the partial blindness and restrictive blindness.

Recently, Chen-Zhang-Liu[5] proposed the first ID-based restrictive partially blind signature scheme(IRPB) by combining an ID-based partially blind signature scheme proposed by Chow *et al*.[6] with an ID-based restrictive blind signature scheme proposed by Chen-Zhang-Liu[7]. However, X. M. Hu. and S. T. Huang.[8] found that Chen-Zhang-Liu's scheme had an important weakness. Their scheme does not achieve the restrictiveness property as they claimed. They showed, in an electronic cash system constructed by Chen-Zhang-Liu, an account-holder cannot be caught when he performs double-spending. In this paper, we propose an improvement of Chen-Zhang-Liu's scheme, and the new scheme can resist the Hu-Huang *et al*.'s attack.

The rest of the paper is organized as follows: In Section 2, we briefly review Chen-Zhang-Liu's scheme. We propose an improvement of Chen-Zhang-Liu's scheme in Section 3. The completeness and security of improved scheme are discussed in Section 4. Finally, conclusions will be made in Section 5.

2. Review of Chen-Zhang-Liu's Scheme

2.1. Basic Concepts on Bilinear Pairings

Let G_1 be an additive cyclic group with prime order q, G_2 be a multiplicative cyclic group of same order and P be a generator of G_1. Let $e: G_1 \times G_1 \to G_2$ be a bilinear mapping with the following properties:

1) bilinear: $e(aP,bQ) = e(P,Q)^{ab}$ for all $P,Q \in G_1$ and $a,b \in Z_q^*$;

2) non-degenerate: there exists P and $Q \in G_1$ such that $e(P,Q) \neq 1$;

3) computable: there exists an efficient algorithm to compute $e(P,Q)$ for $P,Q \in G_1$.

The bilinear pairings can be derived from the Weil or Tate pairings.

2.2. Complexity Assumptions

Let G be a cyclic multiplicative group generated by g, whose order is a prime q, assume that the inversion and multiplication in G can be computed efficiently.

Discrete Logarithm Problem (DLP): Given two elements g and h, to find an integer $n \in Z_q^*$, such that $h = g^n$ whenever such an integer exists.

We assume that the discrete logarithm problem (DLP) in both G_1 and G_2 are hard.

2.3. Chen-Zhang-Liu's ID-based Restrictive Partially Blind Signature Scheme

Chen-Zhang-Liu's ID-based restrictive partially blind signature scheme (Chen *et al*.,2007) consists of four phases: *system parameters generation, key generation, signature generation and signature verification*. For simplicity, we will use the same notation as Chen-Zhang-Liu's scheme.

Define two cryptographic secure hash functions

$$H: \{0,1\}^* \to G_1 \quad \text{and} \quad H_1: G_1^3 \times G_2^4 \to Z_q.$$

-*System parameters generation:* On input security parameter k, output the master key $s \in_R Z_q^*$ and the system parameter

$$\text{params} = \{G_1, G_2, e, q, P, P_{pub}, k, H, H_1\}.$$

-*Key generation:* Given *params* and the signer's identity information ID, output the signer's private key

$$S_{ID} = sQ_{ID} = sH(ID).$$

-*Signature generation*: Let Δ be the shared information and a message M be from the receiver.

Publish $g = e(P,Q_{ID})$ and $y = e(P_{pub},Q_{ID})$.

- The signer randomly chooses $Q \in_R G_1, r \in_R Z_q^*$ and computes $z = e(M,S_{ID}), a = e(P,Q), \quad b = e(M,Q)$, $U = rP$ and $Y = rQ_{ID}$. He then sends (z,a,b,U,Y) to the receiver.
- The receiver randomly generates $\alpha,\beta,u,v,\lambda,\mu,\gamma \in_R Z_q^*$, and computes $M' = \alpha M + \beta P$, $z' = z^\alpha y^\beta A = e(M',Q_{ID})$, $a' = a^u g^v$, $b' = a^{u\beta} b^{u\alpha} A^v$, $Y' = \lambda Y + \lambda\mu Q_{ID} - \gamma H(\Delta)$, $U' = \lambda U + \gamma P_{pub}$, $h = \lambda^{-1} H_1(M',Y',U',A,z',a',b') + \mu$ and $c' = hu$. He then sends h to the signer.
- The signer computes $S_1 = Q + hS_{ID}$, $S_2 = (r+h) S_{ID} + rH(\Delta)$ and sends (S_1,S_2) to the receiver.
- If the equations $e(P,S_1) = ay^h$ and $e(M,S_1) = bz^h$ hold, the receiver computes $s_1' = uS_1 + vQ_{ID}$ and $s_2' = \lambda S_2$. Thus, the tuple (Y',U',z',c',s_1',s_2') is the signature for Δ and M'.

-*Signature verification*: Given a tuple (Y',U',z',c',s_1',s_2') for Δ and M', the verifier computes $A = e(M', Q_{ID})$, $a' = e(P,s_1')y^{-c'}$ and $b' = e(M',s_1')z^{1-c'}$. The verifier accepts the signature if the following equation holds:

$$e(s_2',P) = e(Y' + H_1(M',Y',U',A,z',a'b')Q_{ID}, P_{pub}) \times e(H(\Delta),U').$$

Unfortunately, Hu-Huang [8] pointed out that above scheme is insecure and can not achieve the property of restrictiveness as they claimed. Any adversary receiver can obtain a valid signature for a message.

3. Improvement of Chen-Zhang-Liu's Scheme

In [8], X.M. Hu *et al*. found that above scheme had an important weakness. Any adversary receiver can obtain a valid signature for a message M' with any form. The main reason is that the Chen-Zhang-Liu's scheme had more variable parameters. In this section, we present an improvement of Chen-Zhang-Liu's scheme. The system initialization phase is the same as the one presented in Section 2. In the following, we only describe the *Signature generation* and *Signature verification*.

-*System parameters generation*: The parameters generation is just as before.

-*Key generation*: The key generation is just as before.

-*Signature generation*: Let Δ be the shared information and a message M be from the receiver.

Publish $g = e(P,Q_{ID})$ and $y = e(P_{pub},Q_{ID})$.

- The signer randomly chooses $Q \in_R G_1, r \in_R Z_q^*$ and computes $z = e(M,S_{ID}), a = e(P,Q)$, $b = e(M,Q)$, $U = rP$ and $Y = rQ_{ID}$. He then sends (z,a,b,U,Y) to the receiver.
- The receiver randomly generates $\alpha,\beta,u,v \in_R Z_q^*$, and computes $M' = \alpha M + \beta P$, $A = e(M',Q_{ID})$, $z' = z^\alpha y^\beta$, $a' = a^u g^v$, $b' = a^{u\beta} b^{u\alpha} A^v$, $Y' = (\alpha+\beta)Y + (\alpha+\beta)(\beta+u)Q_{ID} - (u+v)H(\Delta)$, $U' = (\alpha+\beta)U + (u+v)P_{pub}$, $h = (\alpha+\beta)^{-1} H_1(M',Y',U',A,z',a',b')$

$+(\beta+u)$ and $c'=hu$. He then sends h to the signer.

- The signer computes $S_1=Q+hS_{ID}$, $S_2=(r+h)S_{ID}+rH(\Delta)$, and sends (S_1,S_2) to the receiver.
- If the equations $e(P,S_1)=ay^h$ and $e(M,S_1)=bz^h$ hold, the receiver computes $s_1'=uS_1+vQ_{ID}$ and $s_2'=\lambda S_2$. Thus, the tuple (Y',U',z',c',s_1',s_2') is the signature for Δ and M'.

-*Signature verification*: Given a tuple (Y',U',z',c',s_1',s_2') for Δ and M', the verifier computes $A=e(M',Q_{ID})$, $a'=e(P,s_1')y^{-c'}$ and $b'=e(M',s_1')z^{1-c'}$. The verifier accepts the signature if the following equation holds:

$$e(s_2',P)=e(Y'+H_1(M',Y',U',A,z',a',b')Q_{ID},P_{pub})\times e(H(\Delta),U')$$

4. Discussion

In this section, we first discuss the completeness of our improved scheme, and then show the new scheme can resist against the proposed attack by X.M. Hu. *et al*.

Theorem 1. The improved scheme achieves the property of completeness.

Proof. Note that

$$e(P,s_1')=e(P,S_1)^u\cdot e(P,Q_{ID})^v=(ay^h)^u g^v=a'y^{c'}$$

$$e(M',s_1')=e(M',S_1)^u\cdot e(M',Q_{ID})^v=e(\alpha M+\beta P,S_1)^u\cdot A^v=b'z^{c'}$$

and

$$\begin{aligned}
&e(s_2',P)=e((\alpha+\beta)S_2,P)\\
&=e((\alpha+\beta)(r+h)S_{ID}+(\alpha+\beta)H(\Delta),P)\\
&=e((\alpha+\beta)r+H_1(M',Y',U',A,z',a',b')\\
&\quad+(\alpha+\beta)(\beta+u)Q_{ID},P_{pub})\cdot e(H(\Delta),(\alpha+\beta)rP)\\
&=e((\alpha+\beta)r+H_1(M',Y',U',A,z',a',b')\\
&\quad+(\alpha+\beta)(\beta+u)Q_{ID},P_{pub})\cdot e(H(\Delta),U'-\gamma P_{pub})\\
&=e((\alpha+\beta)r+H_1(M',Y',U',A,z',a',b')\\
&\quad+(\alpha+\beta)(\beta+u)Q_{ID}-\gamma H(\Delta),P_{pub})\cdot e(H(\Delta),U')\\
&=e((Y'+H_1(M',Y',U',A,z',a',b')Q_{ID},P_{pub})\\
&\quad\cdot e(H(\Delta),U')
\end{aligned}$$

Thus, the improved scheme achieves the property of completeness.

Theorem 2. The improved scheme is secure and can resist the attack proposed by Hu-Huang.

Proof. Hu-Huang pointed out that the Chen-Zhang-Liu's scheme is insecure, the key reason is that their scheme was constructed by simply assembling Chow *et al*.'s scheme (2005) and Chen *et al*.'s scheme (2005). In their scheme, the receiver randomly generated seven numbers, and these numbers have redundancy. Any adversary can constructs (z',a',b') without using the values of (z,a,b) in step in the Chen-Zhang-Liu's scheme. Comparison with the Chen-Zhang-Liu's scheme, our improved scheme only choose $\alpha+\beta$, $\beta+u$ and $u+v$, instead of choosing the parameters λ, μ and γ, respectively, and the verification equation is same as that of Chen-Zhang-Liu. Thus, we reduce the variable parameters and only need four parameters instead of seven parameters in Chen-Zhang-Liu's scheme. Since the parameters $\alpha+\beta$, $\beta+u$ and $u+v$ are depend on the parameters α, β, u and v in the improved scheme, the recipient obtains a signature on a message that can only be the form $M'=\alpha M+\beta P$ with α and β randomly chosen by the recipient. Similar to Chen-Zhang-Liu's analysis, our scheme achieves the property of restrictiveness and can resist the Hu-Huang's attack.

The other properties of the improved scheme are same as the Chen-Zhang-Liu's scheme, we omit them.

5. Conclusions

Chen-Zhang-Liu proposed the first ID-based restrictive partially blind signature scheme (IRPB) by combing the ID-based partially blind signature scheme with the ID-based restrictive blind signature scheme. Recently, X.M Hu *et al*. showed the Chen-Zhang-Liu's scheme did not satisfy the property of restrictiveness as they claimed. In this paper, we give an improved version of Chen-Zhang-Liu's scheme, and the improved scheme can resist the attack proposed by X. M. Hu *et al*.

6. Acknowledgements

The author wishes to thank the anonymous referees for their valuable comments and suggestions.

7. References

[1] D. Chaum, "Blind Signatures for Untraceable Payments," *Advances in Cryptology Crypto'*82，Springer-Verlag, Germany, 1982, pp. 199-203.

[2] S. Brands, "Untraceable off-Line Cash in Wallets with Observers," *Advances in Cryptology Crypto'*93, *LNCS 773*, Springer-Verlag, Germany, 1993, pp. 302-318.

[3] M. Abe and E. Fujisaki, "How to Date Blind Signatures," *Advances in Cryptology-Asiacrypt* 1996, *LNCS* 1163, Springer-Verlag, Germany, 1996, pp. 244-251.

[4] G. Maitland and C. Boyd, "A Provably Secure Restrictive Blind Signature Scheme," *PKC'02, LNCS* 2274, Springer-Verlag, Germany, 2002, pp. 99-114.

[5] X. F. Chen, F. G. Zhang and S. L. Liu, "ID-Based Restrictive Partially Blind Signatures and Applications," *The Journal of Systems and Software*, Vol. 80, No. 2,

2007, pp. 64-71.

[6] S. M. Chow, C. K. Hui and S. M. Yin, "Two Improved Partially Blind Signature Schemes from Bilinear Pairings," *ACISP'*05, *LNCS* 3574, Springer-Verlag, Germany, 2005, pp. 316-328.

[7] X. F. Chen, F. G. Zhang and S. L. Liu, "ID-Based Restrictive Partially Blind Signatures and Applications," 2007. http://eprint. iacr.org/2005/3/319/.

[8] X. M. Hu and S. T. Huang, "Analysis of ID-Based Restrictive Partially Blind Signatures and Applications," *The Journal of Systems and Software*, Vol. 81, No. 11, 2008, pp. 1951-1954.

