New randomized partially blind signature scheme

Xinghua Zhang

Dept. of Mathematics and Information Science, Langfang Teachers University

Langfang, Hebei, China

biyesheji2006@163.com

Keywords: Bilinear mapping；Partial blind signature; Blindness; Public information can not be replaced

Abstract: The existing partially blind signature schemes rarely consider the random,and had less strict proof on random. Based on bilinear pairings and elliptic curve discrete logarithm problem,this article proposes a new randomized partially blind signature scheme. The random parameters jointly generated by the signer and the signature receiver who selectes random number in this scheme. It is proved that the scheme satisfies unforgeability, partial blindness, effective against other people in the public information substitution attack.

1 Introduction

In order to realize the payment system which is not tracked, the concept of blind signature was first proposed by Chuam[1] in 1982 based on blind signature technology.The signer completed signature, he did not know the specific content of the messages. The signer can't relate the signature process with the intermediate results and the final published signature. The characteristics of blind signature is called blindness, it effectively protect the privacy of the user, thus the blind signature is widely used need to protect user privacy in electronic voting, electronic cash and other occasions.However, this is completely blind, thus the signer doesn’t know any information of the signed message.it is very easy to cause the signature is used illegally. In order to solve the contradiction between the blind signature is anonymous and controllability, in 1996, Abe [2] proposed the concept of partial blind signature. Partially blind signatures will put the signed message is divided into two parts: one is public information which is agreemented by the signer and the user.For example, the scope of the signed message. The other part is the message which is waiting for signature keeps blind. This scheme not only to protect the privacy of the user and make the signer can control the part of the contents of the signature.

In recent years, various partial blind signature schemes was proposed, in 2014, Zhang Yanhong [3] proposed a partial blind signature based on identity. In 2014, Huang Rufen [4] proposed a partially blind signature scheme based on certificate. In 2014, He Junjie [5] proposed the improvement scheme on the partially blind signature scheme without the certificate.

At present, few scholars to study the randomized characteristics. Fan[6] proposed a randomized blind signature scheme based on RSA. Chien [7] proposed a new randomized partially blind signature scheme, but Kwon [8] pointed out that the attacker can successfully remove the randomization factor signer introduced from the message in the above two schemes, thus the security is not high. Fan [9] proposed a randomized blind signature scheme based on bilinear pairings, it can be proved secure. According to the design idea of this scheme, this paper proposes a new randomized partially blind signature scheme based on bilinear pairings. The new scheme completed random strict proof.It satisfies unforgeability, blindness, can resist the other attacker on public information substitution attack.

2. Preliminary Knowledge

In this section, we briefly review the concepts of bilinear pairings and some related mathematical problems.

2.1 Bilinear pairings

Let G_1 be a cyclic additive group generated by q,whose order is a prime q,and G_2 be a cyclic multiplicative group of the same order q.A map $e: G_1 \times G_1 \rightarrow G_2$ is called a bilinear map if it has the following properties:

(1)Bilinearity: There exists $P,Q,R \in G_1; a,b \in Z; e(aP,bQ) = e(P,Q)^{ab}$

(2)Non-degeneracy: There exists $P,Q \in G_1, P \neq 0; e(P,Q) \neq 1$

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

2.2 Computational problems

Here we present some computational hard problems, which form the basis security of our schemes.

(1) Discrete Logarithm Problem (DLP): Given two group elements P and Q, $P,Q \in G_1$, $Q = xP \in G_1$, It is difficult to compute $x \in Z_q^*$.

(2)Decision Diffie-Hellman Problem (DDHP): For $a,b,c \in Z_q^*$ and $P \in G_1^*$, given P,aP,bP,cP, decide whether $c = ab \bmod q$.

(3)Computational Diffie-Hellman Problem (CDHP): For $P \in G_1^*$ and $a,b \in Z_q^*$, given P,aP,bP,cP, compute abP.

(4)Bilinear Diffie-Hellman problem (BDH): For $P \in G_1^*$ and $a,b,c \in Z_q^*$, given P,aP,bP,cP, compute $e(P,P)^{abc}$.

3 new scheme

(1)Parameter settings

Given the security parameter k.Let G_1 be a cyclic additive group generated by q,whose order is a prime q,and G_2 be a cyclic multiplicative group of the same order q. $P \in G_1$. A bilinear pairing is a map: $e: G_1 \times G_1 \rightarrow G_2$,.it chooses two cryptographic hash functions H_0, H_1. $H_0: \{0,1\}^* \times G_1 \rightarrow G_1$, $H_1: \{0,1\}^* \rightarrow G_1$.

The signer chooses two random numbers $x_1, x_2 \in Z_q^*$, then computes the corresponding public key $y_1 = x_1 P$, $y_2 = x_2 P$. The system parameters $\{G_1, G_2, e, q, P, y_1, y_2, H_0, H_1\}$ are published and x_1, x_2 are kept secret.

A is the signer, B is the signature receiver, C is the signature verifier. m is the message, M is embedded into the behind of the message, it is public information that the signer and the signature receiver prior consultation.

(2)Blind stage

B sends M to A, A verifies the correctness of M. If M is in accordance with the provisions of negotiation, the signer chooses a random number $t \in Z_q^*$, computes $W = tP$. A sneds W to B,after receiving W, B chooses three random numbers $r_1, r_2, v \in Z_q^*$,computes random parameters $u = Wv$, $m_1 = r_1 H_0(m \| u) + r_2 P$, $m_2 = r_1 v (\bmod q)$.

Then B sends the blind message (m_1, m_2) to A.

(3)Signature stage

After receiving (m_1, m_2) from B, A computes $S' = x_1 m_1 + t m_2 W + x_2 m_2 H_1(M)$,then A sneds S' to B.

(4)Literacy stage.

B computes $S = r_1^{-1}(S' - r_2 y_1)$,then (S, m, u, M) is the signature of message m and the public information M.

(5) verification stage

C examines whether this equation is established or not: $e(S,P)=e(H_0(m\|u),y_1)e(u,u)e(H_1(M),y_2)$. If the equation holds, the signature is valid, otherwise invalid.

4 Scheme Analysis

4.1 Correctness analysis

The correctness of the verification equation:

$$e(S,P)=e(r_1^{-1}(S^{'}-r_2y_1),P)$$
$$=e(r_1^{-1}(x_1m_1+tm_2W+x_2m_2H_1(M)-r_2y_1),P)$$
$$=e(r_1^{-1}(x_1r_1H_0(m\|u)+x_1r_2P+tr_1vW+x_2r_1vH_1(M)-r_2y_1),P)$$
$$=e(r_1^{-1}(x_1r_1H_0(m\|u)+x_1r_2P+tr_1vW+x_2r_1vH_1(M)-r_2x_1P),P)$$
$$=e(r_1^{-1}(x_1r_1H_0(m\|u)+tr_1vW+x_2r_1vH_1(M)),P)=e(x_1H_0(m\|u)+tu+x_2vH_1(M),P)$$
$$=e(H_0(m\|u),x_1P)e(tu,P)e(H_1(M),x_2vP)=e(H_0(m\|u),x_1P)e(u,tP)e(H_1(M),y_2v)$$
$$=e(H_0(m\|u),y_1)e(u,tP)e(H_1(M),y_2v)=e(H_0(m\|u),y_1)e(u,W)e(H_1(M),y_2v)$$
$$=e(H_0(m\|u),y_1)e(u,Wv)e(H_1(M),y_2)=e(H_0(m\|u),y_1)e(u,u)e(H_1(M),y_2)$$

4.2 Unforgeability Analysis

(1)The signature receiver forged partially blind signature is not feasible.

The signer joined the random number and its own private key x_1,x_2 in the signature process. It is not feasible that the signature receiver forges partially blind signature, and solving x_1,x_2 will face the discrete logarithm problem solving on the elliptic curve.

(2)The signer forges partial blind signature is not feasible.

The signer forge a signature will face two major difficulties:

1)The signer put the message into blindness by posing as the signature receiver.Because of $m_1=r_1H_0(m\|u)+r_2P$ and r_1,r_2 are unknown, the signer cannot be completed on message m with blind;

2) The signer put the signature literacy processing by posing as the signature receiver. Because of $S=r_1^{-1}(S^{'}-r_2y_1)$ and r_1,r_2 are unknown, the signer cannot be completed on the signature $S^{'}$ with literacy.

4.3Partial blindness

On the one hand, the signature receiver can not compute tm_2W when he doesn't know t.On the other hand, because of the signer to complete the signature (m_2,M),then (m_2,M) is the data the dual role of the signature receiver join blind factors in the original message and Hashi function. If the signer doesn't know the blind factors r_1,r_2,v, he can't get any message of the original message.

4.4 Resistance to replace consultation information attack

The new partial blind signature scheme will bind up public information M and the signer's private key x_2,in addition to the signer, anyone solves out the signature private key x_2 from the public key y_2 will face the problem of elliptic curve discrete logarithm, thus it is not feasible. When the public information M is embedded into the partially blind signature, the other people want to the consultation public information M is replaced by a new public information $M^{'}$, it is not feasible. Because other people do not know the partial private key x_2 and random number t, $H_1(M)$ will be replaced by $H_1(M^{'})$ will face hash collision problem, thus the scheme effectively overcomes the replacement of public information M to other people.

5. Conclusion

Because partial blind signature has a wide application prospect in the field of e-business and e-government , thus many scholars have conducted in-depth discussion and Research on the partially blind signature.This paper presents a new efficient randomization partially blind signature scheme based on bilinear pairing.Currently there are few scholars to study the randomized characteristics. The security analysis shows that the scheme is effective against other people in the public information substitution attack, unforgeability, partial blindness, wider application scope.

6. Acknowledgement

This work is financial supported by the Natural Science Foundation of Hebei Province(Project :”Theory and Application Research on certificate proxy blind signature scheme”). The author also would like to thank the Science and Technology Research Youth Fund Project of the Colleges and Universities of Hebei Province (No.QN20131047).

References

[1]CHAUM D.Blind signatures for untraceable payments[J].Advances in Cryptology Proceedings of Crypto, 1983,82(3):199-203.

[2]ABE M,FUJISAKI E.How to date blind signatures[C]//Advances in Cryptology-ASIACRYPTO'96,LNCS 1163.Berlin: Springer-Verlag,1996:244-251.

[3] Zhang Yanhong,Chen Ming.the standard model enhanced ID based partially blind signature[J].Journal of Sichuan University(Engineering Science Edition),2014,(01) :95-101.

[4]Huang Rufen,Qiang Nong,Huang Zhenjie.provable security partially blind signature scheme based certificate[J].Computer Engineering,2014,(06):109－114.

[5]He Junjie,Zhang Fan,Shao Hui.analysis and improvement of a certificateless partially blind signature scheme[J].Journal of Xinyang Normal University(Natural Science Edition),2014,(02) :170-175.

[6]Fan C I,Chen W K,Yeh Y S.Randomization Enhanced Chaum’s Blind Signature Scheme[J].Computer Communications,2000,23(17):1677-1680.

[7]Chien H Y, Jan J K, Tseng Y M. RSA-based Partially Blind Signature with Low Computation[C]//Proc. of the 8th Int’l Conf. on Parallel and Distributed Systems. [S. l.]: IEEE Press, 2001.

[8]Kwon M S, Cho Y K. Randomization Enhanced Blind Signature Schemes Based on RSA [J]. IEICE Trans. on Fundam Electron Commun. Comput . Sci., 2003, E86-A(3): 730-733.

[9]Fan C I, Sun Weizhe. Provably Secure Randomized Blind Signature Scheme Based on Bilinear Pairing [J]. Computers and Mathematics with Applications, 2010, 60(2): 285-293.