An Efficient ID based Proxy Signature, Proxy Blind Signature and Proxy Partial Blind Signature

Dr. Banshidhar Majhi
Professor, CSE Department,
NIT Rourkela

Deepak Kumar Sahu
Student, CSE Department,
NIT Rourkela

RamNarayan Subudhi
Student, CSE Department,
NIT Rourkela

Abstract

Identity-based (ID based) public key cryptosystem gives an efficient alternative for key management as compared to certificate based public key settings. A proxy signature is a method for an entity to delegate signing capabilities to other participants so that they can sign on behalf of the entity with in a given context. In this paper, we have proposed a new ID-based proxy signature which is more efficient than [2]. Then we have extended our study in developing a blind -signature and partial blind signature using the above proxy signing key. We also have analyzed security of our new scheme briefly.

Keywords

ID base signatures, proxy signatures, bilinear pairing, blind signature, partial blind signature, Elliptic curves

1. Introduction

Shamir [6] proposed the concept of ID-based cryptosystems. In an ID-based cryptosystem, a user's public key can be derived directly from his identity information instead of being extracted from a certificate issued by certification authority. Proxy signature is a method for an entity to delegate signing capabilities to other participants so that they can sign on behalf of the entity with in a given context. Practically, proxy signature is gaining importance and momentum particularly when it comes to distributed computing where delegation of rights is quite common. Other applications are grid computing, mobile applications, distributed shared object systems and global distribution networks. Mambo, Usuda and Okamoto [5] gave the first efficient solution to proxy signature. Jing Xu, Zhenfeng zhang and Dengguo Feng [2] gave a successful model for ID based proxy signature however their scheme is very costly, we have tried to come up with an efficient scheme.

Chaum [9] came up with a concept of blind signature scheme which allows a user to obtain signatures from a signer on any documents without revealing any information about the message or its signature.

A partially blind signature [10] using proxy key allows a proxy signer to explicitly embed an agreed common information into a blind signature. chow et al [11] first proposed an ID-based partially blind signature scheme based on bilinear pairings. We will show that our partially blind signature by proxy signer also satisfies the following three properties.
(i)Verifiability (ii)PartialBlindness (iii)Unforgeability

The fact of paper is organized as follows. In section-2, preliminaries relating to bilinear pairing are given. In section-3, we give some definitions used in this paper. In section-4, the proposed ID-based proxy signature is present and efficiency is compared to [2] in section 5, the proposed blind signature using the above proxy key is present. In section-6, the proposed partial blind signature using the above proxy key is present. In section-7, we have discussed briefly the security of our signature schemes Section- 8 conclude this paper.

2. Bilinear Pairing

Let us consider **G** and **G'** two additive groups and **H** a multiplicative one. A pairing of on *G, G', H* is simple is a special function ***e*** which takes an element of *G XG'* and produces and element of **H** as on output.

e : G x G' → H (1)

The most important property that is required there, is bilinearity, meaning that

For all S_1, S_2 € G and T_1, T_2€ G',

$e\ (S_1 + S_2, T_1) = e(S_1, T_1)\ {*}e\ (S_2, T_1)$ (2)

$e\ (S_{1,}\ T_1 + T_2) = e\ (S_1, T_1)\ {*}e\ (S_1, T_2)$ (3)

Properties:

Bilinearity: $e(aP,bP)= e(P,P)^{ab}$ for all P,Q€G_1 and a,b€z_q

Non-degeneracy: There exists P, Q €G_1**,** such that e (P,Q)≠ 1, in other words, the map does not send all pairs in G_1 x G_2 to the identity in G_2.

978-0-7695-3513-5/08 $25.00 © 2008 IEEE
DOI 10.1109/ICIT.2008.38

Computability: There is an efficient algorithm to compute e (P,Q) for all P, Q €$G_{1.}$

Weil pairing and Tate paring is used for the construction of pairings.

3. Definitions

3.1 Definition of ID based Proxy Signature

Scheme we give a formal definition of ID based Proxy Signature Scheme similar to [2]. Following algorithms should be considered

G:

KCG (Key generation center) chooses a random number s€ Z_q^* and sets $P_{pub} = sP$.

He publishers system parameters.

$\{G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H_3\}$

$e: G_1 \text{ x } G_1 \rightarrow G_2$

$H_1 : \{0,1\}^* \rightarrow Z_q^*$

$H_2 : \{0,1\}^* \rightarrow G_1$

$H_3 : \{0,1\}^* \text{ x } G_1 \rightarrow Z_q^*$

K:

A user submits his/her identity information (ID) and authenticates him to KCG. KCG computes the user's private key $S_{ID} = s\ Q_{ID} = s\ H_2$ (ID) and sends to user. Keeps s as mater key secrete.

S:

The signing algorithm, which takes a signing key S_{ID0} of original designator and warrant (w) as input and output a signature S_{w0}. S_{w0} must contain some common shared information secrete to both delegator and proxy signer.

V:

A verification algorithm that accepts the delegated signature runs by proxy signer to accept **($S_{w0,}$ w).**

D:

A development of proxy's ID using the delegated warrant signature and warrant w.Thus develops a proxy signing key S_{w1}

PS:

The proxy signing algorithm, which takes a proxy signing key S_{w1}, message m and a warrant w and outputs proxy signature (U,V,w)

PV:

Takes identity X of original designator and verifies the (U,V,w)

3.2 Definition of (Partial) Blind signature using proxy key

We give a formal definition of (partial) blind signature. This definition inherits definition 3.1 with additional features of blind (partial) signature. This can be defined through following algorithms:

Initiator (I)

The requester requests for the start of the session by logging in to server and proxy server responds to it.

Blind (B)

the requester blinds the message to be signed by the proxy signer

Sign (S)

The proxy signer signs (if partial blind signature embeds some common information to signature) the blinded message and returns it along with its warrant w that he got from original signer.

Un blinding (UB)

The requester un blinds the signature and gives the tuple (m,U',V') as signature.

Verification (V1)

The requester or any third party can verify the sign by using the information of signature and original signer (X)

3.3 Definition of Problems that form the basis of our security

Let us define formally the problems, we are dealing with.

a)Let G be a finite cyclic group and let g be a generator of G. the discrete logarithm problem **(DLP)** in G is as follows: Given (g, a. g) with uniformly random choice of a $Z^*_{|G|}$, find a

b)Let G be a finite cyclic group and let g be a generator of G. The computational Diffie – Hellman Problem **(CDHP)** in G is as follows : Given (g,a.g, b.g) with uniformly random choices of a, b $Z^*_{|G|}$, compute (ab).g

c)Let G be a finite cyclic group and let g be a generator of G. The decisional diffie Hellman problem **(DDHP)** in G is a follows: Given (g,a.g, b.g) with uniformly random choices of a, b $Z^*_{|G|}$, decide whether (ab). g = c.g

d)The Bilinear Diffie- Hellman problem **(BDHP)** in (G_1,G_2,e) is defined as follows: given (P,aP,bP,cP) for some a,b,c € Z_q^* compute v€G_2 such that $v=e(P,P)^{abc}$

There are two variations of CDHP:

Inverse CDHP

For a Z_p^*, given P, aP to compute $a^{-1}P$

Square CDHP

For a Z_p^*, given P, aP to compute a^2 P

It is clear that the CDHP can easily the solved, if the DLP can be solved. If the DLP can be solved, we can indeed. Find a from a.g and compute (ab). g we then say **DLP => CDHP** but reciprocity is not true. Yet as far as we know, solving DLP is the only known method to solve CDHP, and for this reason the CDHP is believed to be as hard as DLP, which is usually exponentially difficult.

Concerning DDHP is another story, suppose indeed that we can compute a bilinear map $e: G \times G \rightarrow G_2$ we want to confirm that $cP = ab\ P$ for the tuple (P, ap, bp, cp) where $a, b, c\ Z_q^*$

$e(aP, bP) = e(P, cP)$

$LHS = e(p,p)^{ab} = e(P, ab\ P)$

If relation holds then,

$cP = ab\ P$

Groups for which DDHP is easy and CDHP is hard are called **gap groups** and we will concentrate our schemes on these groups only.

4. The Proposed ID-based Proxy Signature

4.1 The Scheme

G :

KCG (Key generation center) chooses a random number $s€\ Z_q^*$ and sets $P_{pub} = sP$. He publishers system parameters.

$Params=\{G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H_3\}$

K:

The original signer submits his/her identity information ID_0 and authenticates him to KCG. KCG computes the user's private key $S_{ID0} = s\ Q_{ID0} = s\ H_2\ (ID_0)$ and sends to user. Keeps s as mater key secrete. Similarly proxy signer obtains Q_{ID1} and S_{ID1} using its ID_1.

S:

Input: $\mathbf{S_{ID0}}$, w (warrant), c (common information between original signer and proxy signer)

Output:(S_{w0},w,Y') and public key $X= H_3(w,Y')Q_{ID0}+H_1(c)Y'+Q_{ID1}$

Algorithm:

1. Choose randomly $a € Z_q^*$
2. $Y'=aQ_{ID0}$ (4)
3. $w'=H_3(w,Y')+a\ H_1(c) \bmod q$ (5)
4. $S_{W0}=w'S_{ID0}$ (6)
5. $X= H_3(w,Y')Q_{ID0}+H_1(c)Y'+Q_{ID1}$

Then sends the output along any insecure channel (security discussed later)

V:

The proxy signer verifies the signature

Ver1: $e(S_{w0},P)=e(H_3(w,Y')Q_{ID0}+H_1(c)Y', P_{pub})$

D:

A development of proxy's ID using the delegated warrant signature S_{W0} and warrant w $S_{W1}=S_{W0}+S_{ID1}$

PS:

The proxy signing algorithm

Input:- (X,w,m) //m is the message to be signed

Output:- (U,V,w)

Algorithm

1. Choose randomly $r € Z_q^*$
2. $U=r.H_3(w,X)P$ (7)
3. $h=H_3(m,U)$ (8)
4. $V=(h+r)^{-1}S_{w1}$ (9)

The proxy signer sends (U,V,w) as its signature

PV:

The requester takes identity X of original signer is public and verifies (U,V,w) as

Ver2: $e(U+H_3(m,U)H_3(w,X)P,V)=e(H_3(w,X)P_{pub} ,X)$

4.2 Correctness

Ver1:

$e(S_{W0},P)$

Using equation 5 and 6, we get

$e((H_3(w,Y')+a\ H_1(c))sQ_{ID0} ,P)$

$e(H_3(w,Y')\ Q_{ID0}+a\ H_1(c)\ Q_{ID0} ,sP)$

using equation 4, we get

$e(H_3(w,Y')\ Q_{ID0} + H_1(c)Y', P_{pub})$ (proved)

Ver2:

$e(U+H_3(m,U)H_3(w,X)P,V)$

using equation 7, we get

$e(r.H_3(w,X)P+ H_3(m,U)H_3(w,X)P,V)$

using equation 8 and 9, we get

$e((r+h)\ H_3(m,U)P, (h+r)^{-1}S_{w1})$

using bilinearity property

$e(H_3(m,U)P, S_{w1})$

$e(H_3(m,U)P,sX)$

using bilinearity property

$e(sH_3(m,U)P,X)$

since, $P_{pub}=sP$, we get

$e(H_3(m,U)P_{pub} ,X)$ (proved)

4.3 Efficiency

Here, we compare our ID based proxy signature with the scheme [2] in terms of computational power and show summary in table 1.

We denote G_1A the point addition on G_1, G_1M the point scalar multiplication on G_1, z_qM as multiplication on Z_q^* , z_qD as division on Z_q^* , z_qA as addition on Z_q^* ,MTP (map to point) the hashing operation and P_a the pairing operation.

We note that the computation of the pairing operation is the most time consuming though a set of work has been done to reduce the complexity. The scheme in [2] needs a special hash function: MTP (map to point) which needs at least one quadratic or cubic equation over finite field to be solved. Our scheme limits this function to KGC where only once this function is invoked. However in our scheme neither the original signer nor the proxy signer compute MTP operation they only ask for a general cryptographic hash function.

Table-1: The efficiency comparison table

Phases	Existing scheme [2]	The proposed scheme
Original signer	$2G_1M+MTP+G_1A$	$2G_1M+ z_qA + z_qM$
Verification	$2MTP+3Pa$	$2G_1 M+2Pa$
Proxy key Generation	$G_1 M+G_1A$	G_1A
Proxy Signature	$2G_1 M+MTP+G_1A$	$4G_1 M+2G_1A+ z_qM$
Verification	$4MTP+ G_1 M+5Pa$	$3G_1 M+ G_1 A+2Pa+z_QM$

The total cost of our scheme is $11G_1M+4G_1A+4Pa+4z_QM+z_QA+MTP$ which is much less than $6G_1M+3G_1A+8Pa+8MTP$.

5. A proxy Blind Signature

5.1 The scheme

Instructor (I)
He requests for the start of a session by logging in. The proxy signer does the following

$U=r.H_3(w,X)P$ (10)

And sends (U,w) to requester

Blind (B)
The requester does the following

1. choose randomly a € Z_q^*
2. $U'=aU$ (11)
3. $h'=a^{-1}H_3(m,U')\text{mod } q$ (12)

Sends h' to proxy signer

Sign (S)
The proxy signer uses its proxy key S_{w1} and signs the message $V=(h'+r)S_{w1}$ (13)
and returns V to requester

Un blind (UB)
The requester unblinds the signature

$V'=a^{-1}V$ (14)

Verification
The requester gives (m,U',V',w) as his certificate. The requester or any third party takes w and finds X i.e original signers ID.
Then verifies as

$e(U'+H_3(m,U')H_3(w,X)P,V')=e(H_3(w,X)P_{pub},X)$

5.2 Correctness

$V'=(h+ar)^{-1}$ S_{w1}using equation 12, 13 and 14, where $h=H_3(m,U')$

$e(U'+H_3(m,U')H_3(w,X)P,V')$
using equation 10 and 11, we get
$e(ar.H_3(w,X)P+ H_3(m,U)H_3(w,X)P,V)$
$e((ar+h)\ H_3(m,U')P, (h+ar)^{-1}S_{w1})$
using bilinearity property
$e(H_3(m,U')P, S_{w1})$
$e(H_3(m,U')P,sX)$
using bilinearity property
$e(sH_3(m,U')P,X)$
since, $P_{pub}=sP$, we get
$e(H_3(m,U')P_{pub} ,X)$ (proved)

6. A proxy partial blind signature:

A proxy partial blind signature allows a proxy signer to explicitly embed a presaged common information c_1 into into the blind signature without loss of blindness property.

6.1 The scheme

Instructor (I)
The request for the start of a session by logging in. The proxy signer do the following
$U=r.H_3(w,X)P$
And sends (U,w) to requester

Blind (B)
The requester do the following
1.choose randomly a € Z_q^*
2.$U'=aU$
3.$h'=a^{-1}H_3(m,U')\text{mod } q$
Sends h' to proxy signer

Sign (S)
The proxy signer uses its proxy key S_{w1} and signs the message

1. Proxy Signer chooses randomly $r€Z_q^*$
2. Computes $R=rP$
3. $Y=X+H_1(c_1)R$ c_1 -->secret common message
4. $V=(h'+r)^{-1}$ $(S_{w1} +rH_1(c_1)P_{pub})$ and returns (V,Y) to requester.

Un blind (UB)
The requester un blinds the signature
$V'=a^{-1}V$
And shows (U',V',Y,w) as his proof

Verification
The requester gives (m,U',V',w) as his certificate. The requester or any third party takes w and finds X i.e original signers ID.
Then verifies as

$e(U'+H_3(m,U')H_3(w,X)P,V')=e(H_3(w,X)P_{pub},Y)$

6.2 Correctness

$V'=(h+ar)^{-1} S_{w1}$ where $h=H_3(m,U')$

$e(U'+H_3(m,U')H_3(w,X)P,V')$
$e(ar.H_3(w,X)P+ H_3(m,U)H_3(w,X)P,V)$
$e((ar+h) H_3(m,U')P, (h+ar)^{-1} (S_{w1}+rH_1(c)P_{pub}))$
$e(H_3(m,U')P, S_{w1} + rH_1(c)P_{pub})$
$e(H_3(m,U')P,s(X+ rH_1(c)P))$
$e(sH_3(m,U')P,X+ rH_1(c)P)$
$e(H_3(m,U')P_{pub} ,Y)$

7. Security analysis

Anyone cannot forge on S_w' of a warrant w', since there are two signatures on the warrant. First the original signer signs the warrant
$w'=H_3(w,Y')+a\ H_1(c) \bmod q$
$S_{W0}=w'S_{ID0}$
Then the proxy signer also signs
$S_{w1}=S_{w0}+S_{ID1}$
Above all, both share a common information c. These all make above delegation not requiring any secure channel for delivery of signed warrant.
Even this adversary cannot get S_{w1} of proxy signer because S_{w1} must satisfy
$e(S_{w1},P)=e(H_3(w,Y')Q_{ID0}+H_1(c)Y'+Q_{ID1}, P_{pub})$
To compute S_{w1} from P,S_{w0},w is CDHP.
The above delegation is partial with a warrant. It can be regarded as generation of proxy key in proxy signature. The proxy secret is S_{w1} and the proxy public is $X= H_3(w,Y')Q_{ID0}+H_1(c)Y'+Q_{ID1}$
Then the proxy signer can use this pair for use proxy signature and proxy blind signatures.

8. Conclusion

In this paper we have tried to develop and work on a new ID based delegation that scores over [2] in its computational power. Our schemes on proxy blind signature and proxy partial blind signatures are based on our above delegation scheme. The security of our scheme is tightly related to Computational Diffe-Hellman problem(CDHP) in random oracle model.

References

[1] H.-U. Park and L.-Y. Lee. A digital nominative proxy signature scheme for mobile communications. In ICICS 2001, volume 2229 of LNCS, 451C455. Springer-Verlag, 2001

[2] ID-Based Proxy Signature Using Bilinear Pairings ,Jing Xu, Zhenfeng Zhang, and Dengguo Feng

[3] An Efficient ID-Based Partially Blind Signature Scheme by Xiaoming Hu, Shangteng Huang. In Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing

[4] An efficient Signature Scheme from Bilinear Pairings and Its Applications by Fangguo Zhang, Reihaneh Safavi-Naini and Willy Susilo

[5] M. Mambo, K. Usuda, and E. Okamoto. Proxy signatures for delegating signing operation. In Proceedings of the 3rd ACM Conference on Computer and Communications Security (CCS), 48C57. ACM, 1996.

[6] A.Shamir, "Identity-based cryptosystems and signature schemes", *Advances in Cryptology-Crypto 84*, LNCS 196,1984, pp. 47-53.

[7]Q.H.Wu,W.Susilo, and Y.Mu, "Efficient Partially Blind Signature with Provable Security", *ICCSA 2006*, 2006, pp. 345-354.

[8]S. Lal and A. K. Awasthi. Proxy blind signature scheme. Cryptology ePrint Archive, Report 2003/072. Available at http://eprint.iacr.org/, 2003.

[9]D.Chaum, "Blind signature systems", *Proceedings of the Crypto'83*, 1998, pp. 153-156.

[10] M.Abe and E.Fujisaki, "How to date blind signatures", *Advances in Cryptology-AisaCrypt'96*, LNCS 1163, 1996, pp.244-251.

[11] S.S.MChow, L.C.K.Hui, and S.M.Yiu, "Two Improved Partially Blind Signature Schemes from Bilinear Pairings", *Information Security and Privacy: 10th Australasian Conference, ACISP 2005*, LNCS 3574, 2005, pp. 316-328.