MM Research Preprints, 212–217
MMRC, AMSS, Academia, Sinica, Beijing
No. 21, December 2002

Digital Proxy Blind Signature Schemes Based on DLP and ECDLP

Zuowen Tan, Zhuojun Liu and Chunming Tang[1)]

Abstract. In a proxy signature scheme, a potential signer delegates his signing power to a proxy, who signs a message on behalf of the original signer. In a blind signature scheme, the signee cannot link the relationship between the blind message and the signature of the chosen message. That is, the signee cannot make a linkage between the blind signature and the identity of the requester. Therefore, it is very suitable for electronic commerce application. In this paper, on the basis of the Schnorr blind signature, we present two digital proxy blind signature schemes, which satisfy the security properties of both the blind signature and the proxy signature.

1. Introduction

In some applications, it is necessary to protect the privacy of participants. In 1982, David Chaum invented a blind signature [1], which satisfies the above requirements. A blind scheme allows the sender to have a given message signed by the signers, without revealing any information about the message or its signature. It does not only achieve the unforgeability property but also achieves the unlinkability property. Blind signature schemes have applications where the requester (the customer) does not want the signee (the bank B) to be capable of associating a postiori a message m and a signature $S_B(m)$ to a specific instance of the scheme. It is very important in electric cash system (see [2],[3],[4]) where a message m might represent a monetary value which the customer can spent. When m and $S_B(m)$ are presented to the bank for payment, the bank is unable to deduce which party was originally given the signed value. In fact, the requester obtains the signature of the message from performing the unblinding function and the signee cannot link the signature and the blind message. This is a typical untraceable scheme which allows a user to withdraw a valid coin from a bank and spend the coin anonymously at a shop.

In 1996, Mambo, Usudu and Okamoto [5] proposed a new concept, proxy signature. In a proxy signature scheme, the original signer delegates his signing capacity to a proxy signer who can sign a message submitted on behalf of the original singer. [5] shows that a proxy scheme has several properties such as non-repudiation, verification, unforgeability, etc. Since the proxy signature plays an important role in some applications, it has received great attention and a lot of research work on it has been done. Mambo, Usudu and Okamoto [6] proposed complete proxy signature, partial proxy signature and signature with an entitlement certificate. Zhang [7], and Kim, Park, and Won [8] proposed threshold proxy signature. L.J. Yi, G.Q. Bai and G.Z. Xiao [9] proposes a proxy multi-signature scheme.

The proxy signature and blind signature have respective advantages. In some real situations, we must apply them both concurrently, for example, in an anonymous proxy electronic

1) Institute of Systems Science, Chinese Academy of Sciences, Beijing(100080)

voting. So far, no papers propose such a scheme in the literature. On the basis of the Schnorr blind signature, We find two proxy blind signature schemes which inherit the security of these two kinds of signatures. We list briefly their security properties in Section 2.

The rest of this paper is organized as follows. Section 3 is dedicated to the construction of a proxy blind signature scheme based on DLP. In Section 4, we discuss the properties of the provided scheme. Section 5 presents a proxy signature scheme based on ECDLP. Section 6, finally, contains the conclusions.

2. Security Property

In the paper, our schemes are a cryptographic primitive involving three entities: a receiver R of the signature, a original signee A and a proxy signer B. In the section, we describe the required features of the schemes we will show in Section 3 and Section 5.

1. **Distinguish-ability** : The proxy signature must be distinguishable from the normal signature.
2. **Non-repudiation**: Neither the origin nor the proxy must be able to sign in place of the other party. In other words, they cannot deny their signatures against anyone.
3. **Verifiability**: The receiver of the signature should be able to verify the proxy signature in a similar way to the verification of the original signature.
4. **Unforgeability**: Only a designated proxy signer can create a valid proxy signature for the original signer (even the original signer cannot do it).
5. **Unlinkability**: When the signature is verified, the signee knows neither the message nor the signature associated with the signature scheme.

3. Presentation of a Proxy Blind Signature Scheme based on DLP

3.1. The system parameters

For the convenience of describing our work, we define the parameters as follows.
-p, q: two large prime numbers, $q \mid p-1$.
-g: an element of Z_p^*, its order is q.
-x_A, x_B: the original signer A's secret key, the proxy signer B's secret key.
-$y_A \equiv g^{x_A} \pmod{p}$: A's public key.
-$y_B \equiv g^{x_B} \pmod{p}$: B's public key.
-$H(\cdot)$: a public cryptographically strong hash function.
-$\|$: which denotes the concatenation of strings.

3.2. The Proxy Phase.

(1) Commission Generation. A randomly chooses $\overline{k} \in Z_q^*$ on the condition there exists the inverse of $\overline{r}y_A^{\overline{r}} \pmod{q}$, where $\overline{r} = g^{\overline{k}} \pmod{p}$. A computes

$$\overline{s} = x_A\overline{r} + \overline{k} \pmod{q} \tag{1}$$

(2) Proxy delivery. A gives the pair $(\overline{r}, \overline{s})$ to the proxy B in a secure manner.

(3) Proxy verification. B checks

$$g^{\overline{s}} = \overline{r} y_A^{\overline{r}} \pmod{p}, \tag{2}$$

which is often called delegation function. If it is correct, B accepts. Then B computes

$$s' = \overline{s} + x_B \pmod{q} \tag{3}$$

as his secret proxy signature key.

3.3. Signing Phase

(1) B chooses randomly a number $k \in Z_q^*$, computes

$$t \equiv g^k \pmod{p} \tag{4}$$

and sends $(\overline{r}, t)$ to R.

(2) R chooses randomly two numbers $a, b \in Z_q^*$, and computes

$$r \equiv t g^b y_B^{-a-b} (\overline{r} y_A^{\overline{r}})^{-a} \pmod{p} \tag{5}$$

$$e \equiv H(r \| m) \pmod{q} \tag{6}$$

$$u \equiv (\overline{r} y_A^{\overline{r}})^{-e+b} y_A^{-e} \pmod{q}, \tag{7}$$

$$e^* \equiv e - a - b \pmod{q} \tag{8}$$

If $r' = 0$, R selects a, b anew. When the r' is determined, R delivers it to B.

(3) After receiving e^*, B computes

$$s'' = e^* s' + k \pmod{q}, \tag{9}$$

using the same k as in (4). Then B sends s'' to R.

3.4. The Extraction Phase

While receiving s'', R computes

$$s = b + s'' \pmod{q} \tag{10}$$

Then, the proxy blind signature is the tuple (m, u, s, e).

3.5. The Verification

The recipient of a proxy blind signature can verify its validity by checking that

$$e \stackrel{?}{=} \mathrm{H}(g^s y_B^{-e} y_A^e u \| m) \pmod{q}. \tag{11}$$

Theorem 1 Suppose all the entities involved in the protocol follow the protocol, then Eqn. 11 holds.

Proof As per Eqn. 6, Eqn. 11 follows from the equation

$$r = g^s y_B^{-e} y_A^e u \pmod{p}. \tag{12}$$

By computing using the equations 1 to 10, we have

$$\begin{aligned} g^s y_B^{-e} y_A^e u &= g^{s''+b} y_B^{-e} y_A^e u = g^{k+b} g^{s'e^*} y_B^{-e} y_A^e u \\ &= t g^b g^{\overline{s}e^*} y_B^{e^*-e} y_A^e u = t g^b g^{\overline{s}(e-a-b)} y_B^{-a-b} y_A^e u \\ &= t g^b (\overline{r} y_A^{\overline{r}})^{e-b} (\overline{r} y_A^{\overline{r}})^{-a} y_B^{-a-b} y_A^e u = r(\mod p). \end{aligned}$$

4. Analysis of the Proposed Scheme

Anyone can verify the validity of the proxy blind signature. Obviously, he can distinguish easily the proxy's signature from normal signature.

Through the valid proxy blind signature, the verifier can confirm that the signature of the message has been entitled by the original. It is because during the verification, the verifier must use the original's public key. Likewise, the proxy cannot repudiate the signature. The scheme offers non-repudiation property.

Theorem 2 The proxy cannot allege his own signature a proxy signature.

Proof Suppose the proxy tries to forge a proxy signature, he must obtain the secret key $x_A$of the original from Eqn. 1 or choose $\overline{s}$ and $\overline{r}$ satisfying Eqn. 2. In Eqn. 1, because $\overline{k}$ is selected randomly, he determines either by guessing or by computing the discrete $log_g\overline{r}$. He succeeds in doing so by the first method with the probability $1/q$. As for the second method, if he first chooses $\overline{r}$ and then tries to find $\overline{s}$, he is again faced with an instance of the discrete logarithm problem. If he first chooses $\overline{s}$ and then tries to find $\overline{r}$, he is trying to solve Eqn. 2 for the unkown $\overline{r}$. This is a problem for which no feasible solution is known.

From the equation 3, we know that only the proxy signee holds his secret proxy signature key s'. Anyone else (even the original) cannot obtain the key and impersonate the proxy. The original signee cannot have the proxy's secret key. Thus we arrive at the following theorem.

Theorem 3 Anyone else (even the original) can impersonate the proxy and forge his proxy signature with a probability $1/q$.

Evidently, B cannot allege his own signature a proxy signature on behalf of A. A can easily find this. Therefore, the scheme is fair for them both.

Theorem 4 When the protocol has been executed, the message sent to the signee is blind for the signee. So the scheme achieves the unlinkability property

Proof In the scheme, the receiver randomly chooses a, $b \in_R Z_q$ and exercises the blinding function(see Eqn. 5, 6 and 7). The signee only obtains the medial values and the blind signature (m, s, u, e). If he tries to find e from e^*, he succeeds with a probability $1/q$. And the use one-way hash function $H(\cdot)$ permits the signee to work out the message m with a negligible probability. Likewise, when he attempts to link y_A or $\overline{r}$ and u, he must solution Eqn. 7 which is an instance of the concrete logarithm. Thus, through the blind signature (m, s, u, v), the signee cannot make a linkage between it and the identity of the requester (the receiver). The scheme achieves the unlinkability property.

5. A Proxy Blind Signature Scheme based on ECDLP

Now, we present an elliptic curve analogue of the proxy blind signature scheme above. For our purposes, an elliptic curve E is a set of points (x, y) with coordinates x and y lying in the field F_q and satisfying a certain cubic equation $y^2 = x^3 + ax + b$ (where $4a^3 + 27b^2 \neq 0$). Let P a point with large prime order n which generates the whole additive group of E. In other words, F_q has a very large character.

The entities involved are still the same three parties as in the first scheme. The original signee A and proxy signee B have their respective key pair (k_A, P_A) and (k_B, P_B), where k_A, k_B are secret keys, P_A, P_B are public keys and $P_A = k_AP$, $P_B = k_BP$. We denote the x coordinate of a point Q on the elliptic curve E by $x(Q)$. The scheme is constructed as

follows. We make conventions that lowercases denote the elements in F_q and capital letters denote the points in the curve E.

5.1. The delegating stage

Original Signee *A* | **Proxy Signee *B***

randomly chooses $\overline{k}$, $1 < \overline{k} < n$.
and computes $\overline{R} = \overline{k}P$,
$\overline{r} = x(\overline{R})$
$\overline{s} = k_A\overline{r} + \overline{k} \pmod n$

$\overline{r},\overline{s},\overline{R}$ →

checks whether $\overline{R} = \overline{s}P - \overline{r}P_A$.
If the equation holds, B computes $s' = \overline{s} + k_B \pmod n$.

5.2. The signature stage

Requester *R* | **Proxy Signee *B***

randomly choose k, where $1 < k < n$,
and computes $T = kP$.

← $\overline{R},\overline{r},T$

randomly choose a, b, where $1 < a,\ b < n$,
$R = T + bP + (-a - b)P_B + (-a)\overline{R} + (-a\overline{r})P_A$,
$r = x(R)$, $e = H(r||m) \pmod n$, $e^* = e - a - b$
$U = (-e + b)R + (-e + b)\overline{r}P_A - eP_A$

e^* →

computes $s'' = e^*s' + k \pmod n$

← s''

computes $s = s'' + b \pmod n$.

The resulting signature is (m, s, e, U). It can be verified by checking that $e \stackrel{?}{=} \mathrm{H}(x(sP - eP_B + eP_A + U)||m)$. The verification equation follows from $R = sP - eP_B + eP_A + U$. The computation is tedious and can be performed in the same way as in Theorem 1.

The security of the scheme is strongly related to the security of the first scheme. Furthermore, because ECDLP is much more difficult than DLP, the scheme has stronger security property. While maintaining the security, the scheme requires less data size and less computations, so it is efficient.

6. Conclusion

In this paper, we propose two secure proxy signature schemes based on DLP and ECDLP. The schemes satisfy the required secure properties of both proxy signature and the blind

signature: distinguish-ability, nonrepudiation, verifiability, unforgeability, and unlinkability. Therefore, the schemes are suitable for many applications where the users' privacy and proxy signature are required. The schemes present are complete blind for the signee. We can improve it by using cut-and-choose technique.

References

[1] D. Chaum, Blind Signature Systems, *Proceedings of Crypto'83*, Plenum, pp.153.

[2] D. Chaum& A. Fiat& M. Naor: Untraceable Electronic Cash, *Proceedings of Crypto'88*,LNCS 403, Springer-Verlag, pp.319-327.

[3] D. Chaum& B.den Boen& E.van Heyst& S. Mjolsnes& A. Steenbeek, Efficient off-line Electronic Check, *Proceedings of Eurocrypt'89*, LNCS 434, Springer-Verlag, pp.294-301.

[4] S. Brands , Untraceable Off-line Cash in Wallets with Observers, *Proceedings of Crypto'93,* LNCS, **773** , Springer Verlag, pp.302-318.

[5] M. Mambo& K. Usuda and E. Okamoto, Proxy Signatures for delegating signing operation, *Proc. 3rd ACM Conference on Computer and communications Security* , ACM Press, 1996. pp.48-57.

[6] M. Mambo, K. Usuda and E. Okamoto, Proxy signatures: Delegation of the power to sign messages. *IEICE Trans. Fundamentals*, 1996, Vol. E79-A, (9), pp.1338-1354.

[7] K. Zhang, Threshold Proxy signature schemes. *1997 Information Security Workshop* , Janpan, 1997, pp.191-197.

[8] S. Kim, S. Park and D. Won, Proxy signature. *Information and Communication Security*, LNCS, Vol. 1334, Springer-Verlag, 1997, pp.223-232.

[9] Lijiang Yi, Guoqiang Bai, Guozhen Xiao, Proxy multi-signature scheme. *Eletron. Lett.*, 2000, 36, pp.527-528.

[10] John D., Memenzes A., The elliptic cure digital signature algorithm. *Canada: Department of Combinations and Optimization*, Technical Report, CORR 31-39.