基于离散对数的代理盲签名*

谭作文+, 刘卓军, 唐春明

(中国科学院 数学与系统科学研究院 系统科学研究所 数学机械化重点实验室,北京 100080)

A Proxy Blind Signature Scheme Based on DLP

TAN Zuo-Wen+, LIU Zhuo-Jun, TANG Chun-Ming

(Key Laboratory of Mathematics Mechanization Research, Institute of Systems Science, Academy of Mathematics and Systems Science, The Chinese Academy of Sciences, Beijing 100080, China)

+ Corresponding author: Phn: 86-10-62682054, E-mail: Tanzywl@163.net

http://www.amss.ac.cn

Received 2003-04-07; Accepted 2003-07-14

Tan ZW, Liu ZJ, Tang CM. A proxy blind signature scheme based on DLP. *Journal of Software*, 2003,14(11): 1931~1935.

http://www.jos.org.cn/1000-9825/14/1931.htm

Abstract: Proxy signatures are very useful tools with which a potential signer can delegate his signing power to a proxy signer who signs a message on behalf of the original signer. A blind signature is the concept with a salient feature that the signer cannot make a linkage between the blind signature and the identity of the requester. Therefore, it is very suitable for electronic commerce. On the basis of the blind Schnorr signature, this paper presents a digital proxy blind signature scheme, which satisfies the security properties of both the blind signature scheme and the proxy signature scheme.

Key words: DLP; proxy signature; blind signature; electronic business

摘 要: 代理签名是一种非常有用的密码学工具.使用它,原始签名人能将其数字签名权力委托给代理签名人.在盲签名方案中,消息的内容对签名者是不可见的.签名被接收者泄露后,签名者不能追踪签名.代理签名和盲签名在实际中分别有着广泛的应用.结合两者的优点,在 Schnorr 签名的基础上,提出了一个代理盲签名方案.

关键词: 离散对数;代理签名;盲签名;电子商务

中图法分类号: TP309 **文献标识码**: A

In some applications, it is necessary to protect the privacy of participants. David Chaum invented the blind

* Supported by the National Grand Fundamental Research 973 Program of China under Grant No.1998030600 (国家重点基础研究发展规划(973))

TAN Zuo-Wen was born in 1967. He is a Ph.D. candidate at the Institute of Systems Science, the Chinese Academy of Sciences. His current research interests include information security, network security and cryptography. **LIU Zhuo-Jun** was born in 1958. He is a professor and doctoral supervisor at the Institute of Systems Science, the Chinese Academy of Sciences. His research areas are symbolic computation and information security. **TANG Chun-Ming** was born in 1972. He is a Ph. D. candidate at the Institute of Systems Science, the Chinese Academy of Sciences. His current research interests include information security and cryptography.

signature[1], which satisfies the above requirement. 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 achieve not only the unforgeability property but also the unlinkability property. Blind signature schemes have applications where the requester (say, the customer) does not want the signer (say, the bank B) to be capable of associating a message m and a signature $SB(m)$ to a specific instance of the scheme. It is very important in an electric cash system[2~4] where a message m may represent a monetary value which the customer can spend. When m and SB(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 signer 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.

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. These are two scenarios. Traveling executives can delegate to their secretaries to sign documents during their absence. A company with many departments can have a department called the proxy department, whose only job would be to sign documents on behalf of the other departments of the company when those departments have too many things to do and they cannot sign the documents that will have to be signed by those departments. As shown in Ref.[5], a proxy scheme has several properties such as non-repudiation, verification, unforgeability, etc. The proxy signature is different from ordinary signatures. When a receiver verifies a proxy signature, he verifies the signature itself and original signer's delegation together. Furthermore, once the proxy signer creates a valid proxy signature for the original signer, the proxy signer cannot repudiate his signature creation against anyone, and the original signer cannot deny that he delegates his signing power to the proxy signer. Since the proxy signature has these salient features, it plays an important role in some applications. It has received great attention and a lot of research work has been done. Lee, Kim and Kim[6] provided new classifications of proxy signatures: strong vs. weak proxy signatures, designated vs. non-designated proxy signatures, and self-proxy signatures. Zhang[7] proposed threshold proxy signature schemes. Hsu, Wu and Wu[8] analyzed and improved a threshold proxy scheme. Wang and Fu [9] proposed an anonymity-revoking blind proxy signature scheme.

The proxy signature and blind signature have their respective advantages. In some real situations, we must apply both of them concurrently, for example, in an anonymous proxy electronic voting. On the basis of the Schnorr blind signature, we propose a proxy blind signature scheme which inherits the security of these two kinds of signatures.

The rest of this paper is organized as follows. In Section 1, we recall the Schnorr blind signature. We list briefly some of its security properties in Section 2. Section 3 is dedicated to the construction of the proxy blind signature scheme based on DLP (the discrete logarithm problem). In Section 4, we discuss the properties of the provided scheme. Finally Section 5 contains the conclusions.

1 The Blind Schnorr Signature

In this section, we briefly recall the blind Schnorr signature. Let p and q be two large primes such that $q|p-1$. Let g be a generator of a multiplicative subgroup of Z_p^* with order q. $H(\cdot)$ denotes a strong hash function. These parameters are public. The signer A has a private key x_A and a corresponding public key $y_A \equiv g^{x_A} \pmod p$. To sign the message m, the signer A chooses a random $k \in Z_q^*$, computes and sends the "commitment" $r = g^k \pmod p$. The receiver R blinds the r into $r' = rg^{-a}y^{-b} \mod p$ with $a, b \in_R Z_q^*$ and computes $e' = H(r||m) \bmod q$. R sends the 'challenge' $e=e'+b \bmod q$ to the signer. Once A obtains the value e, the signer A responds with a value s which

satisfies the equation $g^s y^e = r \pmod p$. One can easily verify that, with $s' = s - a$, (e', s') is a valid Schnorr signature of the message m by the verification equation $e' \stackrel{?}{=} H(g^{s'} y^{e'} \| m \bmod p)$.

2 Security Properties

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

(1) Distinguishability: The proxy signature must be distinguishable from the normal signature.

(2) Nonrepudiation: Neither the original signer nor the proxy signer 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 signer 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 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.

— $x_A, x_B \in Z_q^*$: 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 Proxy phase

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

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

(b) *Proxy delivery*. A gives the pair $(\bar{r}, \bar{s})$ to the proxy B via a secure channel.

(c) *Proxy verification*. B checks

$$g^{\bar{s}} = \bar{r}\bar{y}_A^{\bar{r}} \pmod p \tag{2}$$

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

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

as his secret proxy signature key.

3.3 Signing phase

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

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

and then sends $(\bar{r}, t)$ to the receiver R.

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

$$r = tg^b y_B^{-a-b} (\bar{r} y_A^{\bar{r}})^{-a} \pmod{p} \quad (5)$$

$$e = H(r \| m) \pmod{q} \quad (6)$$

$$u = (\bar{r} y_A^{\bar{r}})^{-e+b} y_A^{-e} \pmod{p} \quad (7)$$

$$e^* = e\text{-}a\text{-}b \pmod{q} \quad (8)$$

If r=0, R selects a, b anew. Once r, a and b are determined, the receiver R delivers e^* to the proxy B.

(c) After receiving e^*, B computes

$$s'' = e^* s' + k \pmod{q} \quad (9)$$

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

3.4 Extraction phase

While receiving s'', R computes

$$s = b + s'' \pmod{q} \quad (10)$$

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

3.5 Verification

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

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

Theorem 1. (Correctness) Suppose all the entities involved in the scheme follow the protocol, then Eq.(11) holds.

Proof. Eq.(11) follows from the equation

$$r = g^s y_B^{-e} y_A^e u \pmod{p} \quad (12)$$

By using Eqs.(1) to (10), we have

$$\begin{aligned} g^s y_B^{-e} y_A^e u &= g^{s''+b} y_B^{-e} y_A^e u = g^{k+b} g^{s'e^*} y_B^{-e} y_A^e u \\ &= tg^b g^{\bar{s}e^*} y_B^{e^*-e} y_A^e u = tg^b g^{\bar{s}(e-a-b)} y_B^{-a-b} y_A^e u \\ &= tg^b (\bar{r} y_A^{\bar{r}})^{e-b} (\bar{r} y_A^{\bar{r}})^{-a} y_B^{-a-b} y_A^e u = r \pmod{p}. \end{aligned}$$

□

4 Analysis of the Proposed Scheme

Anyone can verify the validity of the proxy blind signature. Obviously, he can easily distinguish 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, because the verifier must use the original's public key during the verification. Likewise, the proxy cannot repudiate the signature. The scheme offers non-repudiation property.

Theorem 2. The proxy can allege his own signature a proxy signature with a success probability 1/q.

Proof. Suppose the proxy tries to forge a proxy signature, he must obtain the secret key x_A of the original from Eq.(1) or choose $\bar{s}$ and $\bar{r}$ which satisfy Eq.(2). Because $\bar{k}$ is selected randomly in Eq.(1), he determines either by guessing or by computing the discrete $\log_g \bar{r}$. He succeeds in doing so by the first method with the probability 1/q.

As for the second method, if he first chooses $\bar{r}$ and then tries to find $\bar{s}$, he is again faced with an instance of the discrete logarithm problem. If he first chooses $\bar{s}$ and then tries to find $\bar{r}$, he is trying to solve Eq.(2) for the unkown $\bar{r}$. This is a problem that does not seem to be related to any well-studied problem such as the discrete logarithm problem and no feasible solution to the problem is known[10]. □

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

Proof. An adversary (including the original signer) wants to impersonate the proxy signer to sign the message m. He can intercept the delegation pair ($\bar{s}$, $\bar{r}$), but he cannot obtain the secret proxy signature key s' from Eq.(3), since there is still an unknown x_B to the adversary in Eq.(3). Because of $x_B \in Z_q^*$, the adversary can obtain the proper secret proxy signature key by guessing it with at most a probability 1/q. That is, anyone else (even the original) can impersonate the proxy successfully with a probability 1/q. □

Through the above two theorems, we know that the proxy signer B cannot allege easily his own signature a proxy signature on behalf of the original singer A and the original signer A can not impersonate easily the proxy signer or allege his normal signature B's proxy signature. Therefore, the proxy blind scheme is fair for both of them.

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

Proof. In the scheme, the receiver randomly chooses a, $b \in Z_q$ and exercises the blinding function (see Eqs.(5), (6) and (7)). The signer 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. Using one-way hash function H (·) permits the signer to work out the message m with a negligible probability. Likewise, when he attempts to link y_A or $\bar{r}$ to u, he must find a solution to Eq.(7) which is an instance of the discrete logarithm problems. Thus, through the blind signature (m, s, u, v), the signer cannot make a linkage between the signature and the identity of the requester (the receiver). The scheme achieves the unlinkability property. □

5 Conclusions

In this paper, we propose a secure proxy signature scheme based on DLP. The scheme satisfies the required secure properties of both the proxy signature and the blind signature: distinguishability, nonrepudiation, verifiability, unforgeability, and unlinkability. Therefore, the scheme is suitable for many applications where the users' privacy and proxy signature are required. From the scheme, we can easily obtain an analog based on ECDLP[11].

References:

[1] Chaum D. Blind signature systems. In: Chaum D, ed. Proceedings of the Crypto'83. New York: Springer-Verlag, 1998. 153~156.
[2] Chaum D, Fiat A, Naor M. Untraceable electronic cash. In: Goldwasser S, ed. Proceedings of the Crypto'88. LNCS 403, New York: Springer-Verlag, 1990. 319~327.
[3] Chaum D, Boen B, Heyst E, Mjolsnes S, Steenbeek A. Efficient off-line electronic check. In: Quisquater J, Vandewalle J, eds. Proceedings of the Eurocrypt'89. LNCS 434, Berlin: Springer-Verlag, 1990. 294~301.
[4] Brands S. Untraceable off-line cash in wallets with observers. In: Douglas RS, ed. Proceedings of the Crypto'93. LNCS 773, New York: Springer-Verlag, 1994. 302~318.
[5] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation. In: Proceedings of the 3rd ACM Conference on Computer and communications Security. New Delhi: ACM Press, 1996. 48~57.
[6] Lee B, Kim H, Kim K. Strong proxy signature and its applications. In: Proceedings of the 2001 Symposium on Cryptography and Information Security (SCIS 2001). 2001.
[7] Zhang K. Threshold proxy signature schemes. In: Okamoto E, Davida G, Mambo M, eds. Proceedings of the Information Security Workshop 1997. LNCS 1396, Berlin: Springer-Verlag, 1998. 191~197.
[8] Hsu CL, Wu TS, Wu TC. Improvement of threshold proxy signature scheme. Applied Mathematics and Computation, 2003,136: 315~321.
[9] Wang XM, Fu FW. An anonymity-revoking blind proxy signature scheme. Chinese Journal of Computers, 2003,26(1):51~54 (in Chinese with English abstract).
[10] Stinson DR. Cryptography Theory and Practice. 2nd ed., New York: CRC Press, 2002. 282~285.
[11] Tan ZW, Liu ZJ, Tang CM. Digital proxy blind signature schemes based on DLP and ECDLP. Vol.21, Beijing: Key Laboratory of Mathematics Mechanization Research, Academy of Mathematics and Systems Science, the Chinese of Academy of Sciences, 2002. 212~217.

附中文参考文献:

[9] 王晓明,符方伟.可撤消匿名性的盲代理签名方案.计算机学报,2003,26(1):51~54.