ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.7, No.24, August 2011.

E-mail: info@cccc.net.cn
http://www.dnzs.net.cn
Tel:+86-551-5690963 5690964

代理盲签名研究综述

苏靖枫,李忠

(河南城建学院 计算机科学与工程系,河南 平顶山 467036)

摘要:文章综述了代理盲签名的发展状况,总结出代理盲签名的安全特性及构造方法。概括了几种新型的代理盲签名方案,分析了几种新型的代理盲签名方案的优缺点。最后对代理盲签名的研究前景进行了展望。

关键词:数字签名;代理签名;盲签名;代理盲签名

中图分类号:TP311 **文献标识码**:A **文章编号**:1009-3044(2011)24-5893-03

Survey on Proxy Blind Signature

SU Jing-feng, LI Zhong

(Department of Computer Science and Engineering, Henan University of Urban Construction, Pingdingshan 467036, China)

Abstract: In this paper, the required security properties which a proxy blind signature should have are described, and the universal construction method of a proxy blind signature is generalized, then several new type proxy blind signature schemes are summarized and analyzed, finally several main research directions which are related to proxy blind signature are proposed as well.

Key words: digital signature; proxy signature; blind signature; proxy blind signature

随着电子商务、电子政务等技术的迅速发展,数字签名已经成为保证电子信息真实性的有效手段,应用于特殊领域中的数字签名也应运而生。1996 年,Mambo 等人首次提出了代理签名的概念,代理签名是指当签名人因为某种原因无法亲自对消息或文件进行签名时,将自己的签名权委托给代理签名人并完成签名的过程,验证方能验证这个签名的有效性并区分出这个签名是何人所签;1983 年,Chaum 首次提出了盲签名的概念,盲签名是指消息持有者在不暴露消息内容的前提下能够获得签名者对真实消息的有效签名,并且签名者无法将公布的消息与自己所签的消息联系起来。代理签名和盲签名作为两种特殊的数字签名具有各自的优点,已经得到广泛应用。随着电子现金和匿名性选举技术的不断发展,在实际应用中有时需要将以上所提的两种特殊数字签名相结合。自从 2000 年 Lin 将代理签名和盲签名相结合首次提出代理盲签名[1]概念之后,大量的基于不同体制的代理盲签名方案[2-6]被相继提出,如基于离散对数的代理盲签名方案[2-3]、基于身份的代理盲签名方案[4-5]和基于双线性对的代理盲签名方案[6]等。

1 代理盲签名的安全特性

代理盲签名是代理签名和盲签名的结合,既具有代理签名的特性,又具有盲签名的特性。因而,一个好的代理盲签名方案应具有如下安全特性:

1)不可伪造性:只有指定的代理签名人能够产生有效代理盲签名,任何其他人包括原始签名人在内都不能产生有效的代理盲签名。

2)可验证性:签名接收者能够从代理盲签名中验证代理签名是否有效,并根据有效的代理签名相信原始签名人对所签消息的认同。

3)可鉴别性:任何人都可区分代理盲签名和正常的原始签名人的签名。

4)不可否认性:一旦代理签名人代替原始签名人产生了有效的代理盲签名,他就不能向任何人否认他的行为。

5)防止滥用:代理签名人的责任应当被具体确定,以确保代理密钥对只能用于创建代理盲签名。

6)盲性:所签消息对代理签名者来说是不可见的,并且签名公布后,代理人不能追踪签名。

2 代理盲签名的构造方法

代理盲签名是建立在代理签名理论和盲签名理论的基础上的,因此代理盲签名的构造一般要用到普通数字签名、代理签名或盲签名。代理盲签名的构造主要是以代理签名为基础,对代理签名体制进行盲化,构造出代理盲签名体制,或者以已经存在的盲签名为基础,增加代理授权机制构造出代理盲签名体制。

一个完整的代理盲签名方案,一般包括密钥生成算法、授权代理算法、代理盲签名算法和签名验证算法四个算法,可设为:BPS=(BPKg, BPGr, BPSig, BPVf)。一个普通的数字签名方案一般包括三个算法:密钥生成算法、签名算法和验证算法,可表示为 DS=(Ks, Sig,Vf)。下面以一个普通的数字签名算法为例说明代理盲签名方案构造的一般方法,并指出构造代理盲签名应注意的问题:

假设方案的参与者有原始签名人 A、代理签名人 B 和消息拥有者 R;X_u,Y_u 分别为用户 U 的私钥和公钥;消息的盲化算法为 Bli()。

1)密钥生成过程(由算法 BPKg 实现)

收稿日期:2011-06-11
基金项目:河南省教育厅自然科学研究计划项目(2010B120008)
作者简介:苏靖枫(1978-),男,河南永城人,硕士研究生,讲师,主要研究方向为信息安全、密码学等。

密钥生成算法 BPKg 同普通数字签名的密钥生成算法 Ks 完全一样，方案的各个参与方(原始签名人、代理签名人和消息拥有者)都按照密钥生成算法生成自己的密钥对，私钥秘密保存，公钥在系统内公布。

2)授权代理过程(由算法 BPGr 实现)

(1)原始签名人 A 选择随机数 r，利用其私钥 X_A 和随机数 r 计算出 S_A，并对授权书 M_w 和 S_A 执行签名，即 $S=Sig(M_w, S_A)$，然后把签名结果 S 发送给代理签名人 B。

(2)B 收到签名消息 S 后，利用签名验证算法 Vf 验证签名的正确性，若正确，接受代理，否则，要求原始签名人重新授权或者拒绝代理。授权代理一旦成功，代理人 B 就通过 S 计算出自己的代理密钥 S_P 并秘密保存，计算代理公钥 Y_P 并在系统内公开。

3)代理盲签名过程(由算法 BPSig 实现)

(1) 消息拥有者 R 选择随机数 $r_1, r_2, \cdots r_n$ 作为盲因子，并通过盲化算法对要签名的消息 m 进行盲化，即：$m'=Bli(m, r_1, r_2, \cdots r_n, r)$，然后把 m′ 发送给 B。

(2) B 收到 m′ 后，利用其代理私钥 SP 产生盲消息 m′ 的签名，即 $s=Sig(S_P, m')$，最后把 s 发送给 R。

(3) 消息拥有者 R 收到 s 后，利用 s 计算出盲签名 s′。

(m, m′, s′)就是消息 m 的代理盲签名。

4)签名验证过程(由算法 BPVf 实现)

要证明消息 m 的代理盲签名的有效性，首先要验证代理是通过正确授权的，然后再通过签名验证算法 BPVf 验证签名的正确性。

利用普通的数字签名算法构造代理盲签名方案时要以代理签名和盲签名理论为基础，构造时要保证方案的严谨性，否则构造的代理盲签名就可能存在各种安全问题，没有实际应用的价值。因此，在设计一个代理盲签名方案时要注意以下几个问题：

(1) 算法要力求简洁、高效、易实现。

(2) 算法的设计要能避免各种可能的攻击，如原始签名人的攻击、签名接收者的攻击和一般性伪造攻击等。

(3) 要满足签名的不可追踪性。

3 几种新型的代理盲签名方案及述评

代理盲签名是互联网上不可缺少的数字签名技术，目前很多国内外学者致力于新算法的研究，提出了很多新型的代理盲签名方案，以适应于特定领域内代理盲签名的需求。我们把现有的代理盲签名方案归纳为以下 4 类并分别予以述评。

3.1 具有消息恢复的代理盲签名方案

具有消息恢复的代理盲签名方案是指，原始签名人将原始消息通过加密隐藏在数字签名文件中，从而使代理签名人在不知道所签消息的前提下对消息进行签名，同时，消息接收者在取得签名同时，使用消息恢复密钥自动恢复消息。这种代理盲签名方案具有广阔的应用前景，能够解决实际生活中的很多问题。如某公司董事长想从总经理那要公司未来发展的策划书(知道策划书的人越少越好)，如果此时总经理在外出差，他就委托副经理将策划书交给董事长，但是副经理又不可以知道策划书的具体内容，而董事长既要拿到策划书又要看到策划书的具体内容。为此就需要具有消息恢复的代理盲签名方案。

2008 年，吴晓波等人[7]基于 Schnorr 算法，提出了一个具有消息恢复的代理盲签名方案，使得只有原始签名者和消息接收者能看到原始待签消息，代理签名者看不到消息明文。另外在方案中引入了时间戳和生存期，有效解决了原始签名者和代理签名者相互抵赖的问题。

2010 年，何金妮等人[8]利用椭圆曲线上的双线性对的特性，提出具有消息恢复的代理盲签名方案，该方案不仅有代理签名和盲签名共同的优点，而且可以恢复出消息，并且计算速度较快。

3.2 可收回代理权的代理盲签名方案

代理盲签名体制除了满足基本特性外，能否及时有效地撤销代理签名权也极为重要。如果不能及时地撤销代理签名权，不诚实的代理签名人就可以滥用签名权，从而产生以下问题：不诚实的代理签名者代表原始签名者继续签名，将给原始签名者带来损失；代理签名者在不诚实行为之前所签署的文件如何鉴定。

2008 年，刘文远等人[9]提出来一种可回收代理权的代理盲签名方案，该方案在签名阶段将时间戳嵌入到 Abe-Okamot 部分盲签名中，无需可信的第三方参与，原始签名人就可以根据自己的需要回收代理签名者的代理权，并且代理权的回收不影响以前产生的有效签名的验证，有效地避免了代理权滥用、原始签名人伪造攻击和公钥替换攻击等。

3.3 指定接收人的代理盲签名方案

在实际应用中，为了防止代理签名人滥用代理权而给原始签名人的权益造成危害，除了及时有效地撤销代理签名权外，原始签名人可能希望指定一个签名接收人，代理签名人只能对发给该接收人的信息进行代理签名，只有该接收人才能验证签名，而对除此人以外的其他接收代理签名人则不能代理原始签名人签名。这种代理盲签名方案称为指定签名接收人的代理盲签名方案。本方案除了满足代理盲签名基本的安全特性以外，还应该满足以下三个要求：只有指定的签名接收人才能验证代理签名的有效性；代理签名人不能冒充原始签名人伪造签名的接收人；原始签名人不能否认指定签名接收人的行为。

2008 年，施荣华，汪秋国[10]基于 two-party Schnorr 签名方案，提出一种指定接收人的代理盲签名方案。该方案中，只有指定接收者才可以恢复消息、验证签名的合法性，指定接收人可以向第三方证实签名的有效性。该方案不但满足代理盲签名方案的安全要求，而且还间接地起到了对代理签名人的代理签名的监督作用，防止代理签名人滥用代理签名权。

3.4 无证书的代理盲签名方案

无证书代理盲签名方案的参与方包括：密钥生成中心 KGC、原签名者、代理签名者和用户。在无证书代理盲签名方案中，原始签

名人和代理签名者的密钥生成与基于证书的代理盲签名方案不同，KGC 根据原始签名人的身份 ID 和代理签名者的身份 ID，利用自己的主密钥生成他们对应的部分密钥，并通过安全信道分别发给他们。收到部分密钥后，原始签名人和代理签名者利用已经确定的秘密信息和部分密钥计算出各自的密钥。

无证书的代理盲签名方案不需要利用证书对公钥进行认证，消除了密钥托管，从而解决了证书撤销、存储、分发等诸多问题，并且其安全性能高，认证速度快。因此，它在低带宽和低处理能力的条件下具有广泛的使用环境，例如：移动设备、无线传感器网络等。

2009 年，陈虎等人[11]提出了一个无证书代理盲签名方案，并且声称该方案是安全的。2011 年，吴晨煌等人[12]发现方案[11]存在严重的安全缺陷，即不诚实的用户能够恢复出代理私钥，在此基础上提出一个改进的无证书代理盲签名方案，并证明了改进方案的安全性。

4 展望

1）如何设计一种安全高效的代理盲签名方案。现有代理盲签名方案不但存在各种安全缺陷，例如不能抵抗一般性伪造攻击、具有连接性等，而且计算复杂性高，执行效率低，这也是阻碍代理盲签名方案实际应用的重要原因。因此，设计一个执行效率高，能抵抗各种攻击的代理盲签名方案有待进一步研究。

2）代理盲签名和相关技术的结合及其应用的研究。代理盲签名与相关技术如密码学、门限签名、群签名等之间很容易产生出新的数字签名技术，特别是代理盲签名与相关技术结合的研究还很不够，因此各种签名技术及其相关技术的结合、渗透、交融是数字签名技术一个大有可为的研究方向。例如，代理多重盲签名、多重代理多重盲签名、基于无证书的代理盲签名等都处于起步阶段，但它们都有着良好的应用前景。

3）如何在电子商务等领域更广泛地应用代理盲签名。目前对代理盲签名的研究主要停留在理论上，代理盲签名在电子商务等领域的应用少之甚少。因此，设计出真正切合实际需要的代理盲签名方案，实现代理盲签名在电子商务等领域中的广泛应用是进一步研究需要解决的问题。

5 结论

代理盲签名是一种新的数字签名技术，在电子支付、电子选举、电子支票等要求代理签名且需要保护用户隐私的场合有着广泛的应用前景。因此，对代理盲签名的研究具有重要的意义。本文主要介绍了代理盲签名应具有的基本特性，总结出代理盲签名的构造方法，然后对几种新型的代理盲签名进行了综述，最后提出了几个与代理盲签名相关的值得重视的研究方向。

参考文献：

[1] LINW D, JAN JK.A security personal learning tools using a proxy blind signature scheme [C]// Proceedings of International Conference on Chinese Language Computing. Washington: IEEE Computer Society, 2000: 273-277.

[2] 谭作文,刘卓军,唐春明.基于离散对数的代理盲签名[J].软件学报,2003,14(11):1931-1935.

[3] ZHUOWEN TAN, ZUOJUN LIU, CHUNMING TANG. Digital Proxy Blind Signature Schemes Based on DLP and ECDLP [J]. MM Research Preprints, 2002, 21(7): 212-217.

[4] 农强,吴顺祥.一种基于身份的代理盲签名方案的分析与改进[J].计算机应用,2008,28(8):1940-1942.

[5] 张学军,王育民.高效的基于身份的代理盲签名[J].计算机应用,2006, 26(11):2587-2588.

[6] FANGGUO ZHANG, REIHANNEH SAFAVI-NAINI, LIN CY. New proxy signature, proxy blind signature and proxy ring signature schemes form bilinear pairings [EB/OL]. [2003-5-29]. http: // eprint. iacr. org /2003/104.

[7] 吴晓波,李树栋,陆洪文,等. 一个改进的带消息恢复的代理盲签名方案[J].海军航空工程学院学报,2008,23(6):717-719.

[8] 何金妮,辛小龙.具有消息恢复的代理盲签名[J].计算机工程与应用,2010, 46(35): 112-114.

[9] 刘文远,佟凤, 王宝文等. 一个新的可回收代理权的代理盲签名方案[J]. 电子与信息学报,2008,30(10):2468-22471.

[10] 施荣华, 汪秋国. 一种指定接收人的代理盲签名方案[J].中南大学学报(自然科学版),2008,39(1): 162-165.

[11] 陈虎, 宋如顺. 无证书代理签名和代理盲签名方案[J].计算机工程与应用,2009,45(9): 92-97.

[12] 吴晨煌,梁红梅,陈智雄.一个无证书代理盲签名方案的改进 [J].计算机工程与应用,2011,47(1): 89-91.

(上接第 5888 页)

2 总结

充分利用现有网络的资源来提供更优的业务，提高现有网络资源的利用率，提升现有网络的使用价值，实时关注网络资源利用状态，作到适时对网络进行容量和资源评估，根据网络实际需要进行资源的调整，“拆闲补忙”，利用有限的资源优先保障高价值区域，这是网络优化需要持续关注的内容。通过对 PS 与 CS 的热点区域进行及时的分析，及时观测网络用户行为和动态，作到提前扩容，提前分析，保障网络的问题与用户的感受。

对于文中的拥塞判决标准一定程度上可以反映出各小区的载波的拥塞情况，采用此标准后可以采用网络自动化监控，对于拥塞小区可以作到快速判决，并迅速组织实施扩容，对保障用户的感受提升网络性能与质量将会起到积极作用。由于考虑有限，本文的论述未免有不周之处，需要在后期的优化中继续更新改进，并且随着 HSUPA 的应用，该判决标准也需要进行适时的修正。

代理盲签名研究综述

作者： 苏靖枫， 李忠， SU Jing-feng， LI Zhong
作者单位： 河南城建学院计算机科学与工程系,河南平顶山,467036
刊名： 电脑知识与技术
英文刊名： Computer Knowledge and Technology
年，卷(期)： 2011,07(24)

参考文献(12条)

1. 吴晓波;李树栋;陆洪文 一个改进的带消息恢复的代理盲签名方案[期刊论文]-海军航空工程学院学报 2008(06)

2. FANGGUO ZHANG;REIHANNEH SAFAVI-NAINI;LIN CY New proxy signature,proxy blind signature and proxy ring signature schemes form bilinear pairings 2003

3. 张学军;王育民 高效的基于身份的代理盲签名[期刊论文]-计算机应用 2006(11)

4. 农强;吴顺祥 一种基于身份的代理盲签名方案的分析与改进[期刊论文]-计算机应用 2008(08)

5. ZHUOWEN TAN;ZUOJUN LIU;CHUNMING TANG Digital Proxy Blind Signature Schemes Based on DLP and ECDLP 2002(07)

6. 刘文远;佟凤;王宝文 一个新的可回收代理权的代理盲签名方案[期刊论文]-电子与信息学报 2008(10)

7. 何金妮;辛小龙 具有消息恢复的代理盲签名[期刊论文]-计算机工程与应用 2010(35)

8. 谭作文;刘卓军;唐春明 基于离散对数的代理盲签名[期刊论文]-软件学报 2003(11)

9. 吴晨煌;梁红梅;陈智雄 一个无证书代理盲签名方案的改进[期刊论文]-计算机工程与应用 2011(01)

10. 陈虎;宋如顺 无证书代理签名和代理盲签名方案[期刊论文]-计算机工程与应用 2009(09)

11. 施荣华;汪秋国 一种指定接收人的代理盲签名方案[期刊论文]-中南大学学报（自然科学版） 2008(01)

12. LINW D;JAN JK A security personal learning tools using a proxy blind signature scheme 2000