盲签名及其在电子商务中的应用

沈 瑛[1],郑河荣[1],范俊波[2]
(1.浙江工业大学 信息工程学院,浙江 杭州 310032;
2.西南交通大学 计算机与通信工程学院,四川 成都 610031)

摘要: 电子商务正在成为一种重要的商务发展模式,它的安全性是通过以密码学为基础的技术和协议来保障的。盲签名技术由于其所具有的匿名性、不可伪造性等特性而应用于电子商务的诸多领域,起着越来越重要的作用。本文围绕盲签名的概念展开,首先给出了盲签名的一般模式,然后在此基础上分别阐述强盲签名、弱盲签名、代理盲签名和部分盲签名等主要的盲签名方案,并讨论它们在电子商务中的应用领域,最后给出了它在电子商务中的两个较成熟的应用——电子现金和电子投票。

关键词: 盲签名;电子现金;电子投票
中图分类号: TP309.7 文献标识码: A 文章编号: 1006-4303(2004)04-0397-06

Blind signature scheme in electronic business

SHEN Ying[1], ZHENG He-rong[1], FAN Jun-bo[2]
(1. College of Information Engineering, Zhejiang University of Technology, Hangzhou 310032, China;
2. College of Computer & Communication Enginering, Southwest Jiaotong University, Chengdu 610031, China)

Abstract Electronic business is turning to an important business pattern. Its security is based on the cryptology technology and protocols. Blind signature can provide anonymity, unforgery within the security. With the developing of electronic business, blind signature technology is playing a more and more important role in this field. This paper focuses on the blind signature scheme. First, a general protocol is described. Then, the main schemas of blind signature are illuminated, such as strong blind signature, week blind signature, partial blind signature and proxy blind signature. We also analyze their application field in electronic business. Finally, we explain its application in e-cash and e-voting, the most mature fields by now.

Key words blind signature; E-cash; E-voting

0 引 言

随着网络经济时代的到来,电子商务已逐步从理念转变为一种重要的商务发展模式。电子商务

收稿日期: 2003-11-16;修订日期: 2004-04-30
作者简介: 沈 瑛(1976-),女,浙江绍兴人,硕士,主要研究方向: 信息安全。
?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki

与传统模式的根本不同在于用户和商家通过网络交易,双方不必见面。这种方式可以降低双方的交易成本,拓宽了选择的余地,交易便捷可行,是一种互惠互利的方式。目前电子商务在各地已陆续开展,逐步崭露头角。但与传统经济相比,它占的比重还很小。相当多的商家和用户持谨慎观望态度,他们的主要顾虑是交易的安全性。由于交易时双方不见面,因而对认证双方的身份合法性,保护交易数据安全传输等的安全性措施,对于电子商务能否受广大用户认可是相当关键的。

电子商务的安全性是通过以密码学为基础的技术和协议来保障的。盲签名技术是其中实现电子现金等的关键技术,本文着重介绍盲签名技术在当前的发展方向和主要的方案,阐述它在电子商务诸多领域的应用。

1 盲签名协议

盲签名由 Chaum(1982)[1]首次提出。盲签名区别于普通签名方案的是,在提供签名服务的同时,签名者在签署文件时并不了解文件的真实内容。Chaum用一个形象的示例说明了盲签名:签名前先把文件放入一个带有复写纸的信封(盲化),签名人直接在信封上签名,透过复写纸写到文件上。这个过程中信封没有打开,所以无法了解文件的真实内容。事后当文件持有人打开信封(去盲),签名者可以验证签名,但他不能在签名和文件间建立联系。盲签名的这种特性能适应许多商务活动的保密需求:在认证的同时不泄露内容,如合同、遗嘱的公证,保付支票的使用,电子货币,电子投票等。

为防止签名者在不知内容的情况下误签不利于他的内容,盲签名实施时还要采用分割选择(cut and choose)技术[2],以概率方式审查文件的内容。一般的盲签名协议如下,其中 U为用户,S为签名人:

(1) U准备 N 份内容相同的文件,分别乘以不同的随机数(盲因子)实现盲化。

(2) U将盲化后的 N 份文件提交给 S。

(3) S随机选择一部分(如: $N-1$个)文件,向 U索要盲因子,恢复出文件(去盲),审查内容是否符合要求。

(4) 如果审查通过,S从未审查的文件中任取一份盲签名,并发给 U;否则协议终止。

(5) U对收到的签名文件去盲,得到原文件和签名。

其中(3)可以有多种方案,来减少 U欺骗的可能性。如不考虑(3),可以用标记(下文同)表示盲签名:文件 m,签名函数 S,盲化函数 R,去盲化函数 R^{-1},签名认证函数 C,则盲签名算法一般过程为:

(a) 盲化 U→S: $R(m)$;

(b) 签名 S→U: $S(R(m))$;

(c) 去盲 U: $R^{-1}(S(R(m)))=S(m)$;

(d) 验证: $C(S(m))$。

2 常用的盲签名方案

由盲签名的匿名性和不可关联性,结合实际应用的需要,盲签名的研究逐步深入。目前较常用的盲签名方案主要有强盲签名、弱盲签名、部分盲签名、代理盲签名等。其中强盲签名方案应用最广,大部分场合都趋向于强盲签名的实现。其它几种主要立足于特殊应用需求,是强盲签名的重要补充。

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki

2.1 强盲签名

强盲签名[3,4]又称为完全盲签名,它遵循 Chaum原始定义,是指签名者无法建立 S(R(*m*))到 S(*m*)的联系 (S(R(*m*))为盲消息 R(*m*)的签名, S(*m*)为去盲后得到的真实消息 *m*的签名)。正是这点实现了不可追踪性 (untraceable)和匿名性,是盲签名的重要特色。它主要应用于电子商务中,诸如电子现金的使用和电子投票等有匿名性要求的领域。完全盲签名的研究已经比较成熟,如盲 RSA签名和盲 Schnorr签名方案是主要的实现方案。以最早的 RSA盲签名实现方案[5]为例:

设签名人 S有公钥 (*e*,*n*),私钥 *d*,要对用户 U的文件 *m*进行完全盲签名。

(1) U选取随机整数 $k \in [1, n-1]$,盲化 *m*为: $t = mk^e \bmod n$,并将 *t*发给 S。

(2) S签名 *t*: $t^d = (mk^e)^d \bmod n$。

(3) U对 *t*去盲: $s = t^d / k \bmod n$。

*s*是最终的签名,易证: $t^d = (mk^e)^d = m^d k \bmod n$,故 $s = t^d / k \bmod n = m^d \bmod n$。S的效果相当于签名人 S直接对 *m*签名,但 S不知道 *m*的内容。这个协议中,由于 S不知道 *k*,不能从 t^d 得到 *s*。

2.2 弱盲签名

所谓弱盲签名[3]方案是指签名者 S仅知道 S(R(*m*))不知道 S(*m*);但一旦公开 S(*m*), S可以建立两者间的联系,即可以获知 *m*是 U的文件。如果把 *m*看作是一个电子现金,则 U在该用电子现金支付给商家,再由商家到银行兑付时,银行就可以从签名 S(*m*)中了解是 U消费的,从而可以追踪 U的行为,这显然不满足匿名性。但是从另一角度看,这种方案可以用于遗嘱、合同等的电子公证,在一段时间内保护信息秘密,在合适的场合公布有关内容及 U的身份,提高可靠性。

2.3 部分盲签名

部分盲签名[6]的特殊性在于被签名的文件是由 U和 S共同产生的,包括 U的原始文件和 S的有关信息 (如,身份信息)。设 S的有关信息 I,则部分盲签名的主要思路是: U将 *m*盲化后提交给 S, S用私钥对 I和 R(*m*)的合成信息签名并发给 U, U去盲后得到最终的签名。任何人可以根据 S的公钥验证签名。

(1) 盲化 U→ S: R(*m*)。

(2) 签名 S→ U: S(R(*m*), I)。

(3) 去盲 U: R-1(S(R(*m*), I)= S(*m*, I)。

(4) 验证: C(S(*m*, I))。

部分盲签名允许签名人在签名中添加信息,可以防止用户滥用签名。它如用于电子现金协议中可避免使用分割选择方法,在保证 *m*的有效性的同时,比引言中的一般盲签名方案,可以大大降低双方交互的通信量。

2.4 代理盲签名

代理盲签名是代理签名和盲签名两种方案的结合。作为代理签名,一般满足不可伪造性、可验证性、可鉴别性、不可否认性,即经授权的代理签名者可以产生合法的代理签名,包括授权人在内的其他人都不能伪造它;他人可验证代理签名是否合法,鉴别出代理签名人;代理签名一旦生成,签名者不能否认自己的签名。代理盲签名除了上述特性以外,还满足盲签名的基本条件: 被签名消息对签名者不可见,签名者事后不能追踪签名。

一个代理盲签名方案可分为三个阶段: 代理授权、签名和验证,比普通的盲签名多了授权的内容,验证的复杂度也增加了,要区分代理签名和普通签名。

代理盲签名是近年来出现的一种新的签名技术,它可用于电子商务中 CA证书、电子现金、电子选票的签发等,对于构建电子商务的服务平台也是很重要的一环。

关于代理盲签名的有关内容,详见文献 [7,8]。

除此以外,还有一些特别的盲签名,如多重盲签名、盲参数签名、群盲签名和阈值盲签名等,都

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki

是盲签名方案和其它签名结合衍生出来的,用于特定的应用领域.

3 盲签名在电子商务中的应用

3.1 电子现金

电子现金又称数字现金,最早由 Chaum等(1990)在文献[9]首次提出,是目前新型的电子商务支付方式. 随着电子商务的发展,用户对消费的匿名性需求日益突出. 电子现金正是由于这一需求而产生的,人们归纳出典型的电子现金相对于传统的网上支付方式,具有以下特点[4, 10]:

(1) 匿名性: 用户可以象现金一样匿名消费,银行等不能跟踪电子现金的使用;而通常支票和信用卡都具有审计线索.

(2) 不可伪造: 用户不能伪造出有效的电子现金.

(3) 不可重用: 电子现金的持有人不能重复使用同一份电子现金.

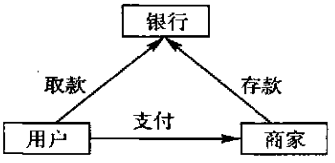

图 1 电子现金的基本模型

(4) 离线性: 用户可以离线保存数字现金,离线支付.

(5) 可分性: 大额的电子现金可以分成若干小面额的进行支付.

(6) 可转移性: 电子现金可转借他人.

在上述前三项是电子现金系统一般要满足的,目前很少有各项全满足的实用高效的方案[10].

电子现金的基本模型如图 1,一般包括银行、用户和商家三方,由取款、支付和存款三个子协议组成. 用户与银行执行取款协议从银行提取电子现金;用户与商家执行支付协议支付电子现金;商家与银行执行存款协议,将交易所得的电子现金存入银行.

盲签名是保证电子现金系统匿名性的关键技术. 文献[11]分别用 B, U, C表示银行、用户和商家,基于盲签名的电子现金基本方案如下:

(1) 取款

· U用身份认证协议向 B证明身份

· U将 N 份电子现金文件 m(内含金额、用户 ID及唯一的随机数等信息)用不同的盲因子盲化后交给 B

· B随机选择一部分(如: $N-1$ 个)文件,向 U索要盲因子,恢复出文件(去盲),审查内容是否符合要求

· 如果审查通过, B从未审查的文件中任取一份盲签名,并发给 U,从 U的帐户中减去相应金额;否则协议终止

· U对收到的签名文件去盲,得到电子现金

(2) 支付

· U与 C交易时,把电子现金交给 C

· C验证 B的签名,如是伪造的,则拒收;否则进一步检测用户(可选),通过后接受电子现金,提供等价的服务

(3) 存款

· C向 B递交电子现金和帐户信息

· B验证签名,若是伪造的,则拒收;否则查询数据库是否有相同的签名(防止重复使用电子现金),若找到则 C或 U重用电子现金,拒收;否则接受,在 C的帐户中加上相应金额,在数据库中添加签名

这里盲签名在取款协议中完成,在交易中多次验证. 为保证匿名性,一般使用强盲签名,可满足匿名性、不可伪造和不可重用的特性. 如进一步考虑支持离线性、可分性、可转移性,则可以变换为

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki

其它盲签名方案。其中如何采用高效的方案降低交互通信量及发现非法行为(如伪造,重用等)如何追究责任人等是研究的热点。由于匿名性可能被不法分子用于犯罪,如洗钱、匿名绑架或敲诈等,在电子现金系统中倾向于采用公正的盲签名方案[12]。即一方面保证合法用户的匿名性,银行和商家无法跟踪,另一方面当非法的行为发生时,有撤消匿名性的机制(一般由可信的第三方授权),可以判定谁是非法者。

3.2 电子投票

电子投票[4, 13, 14]是另一种盲签名的重要应用。与传统方式相比电子投票在网上开展,投票人不必赶到固定的投票点,可以节约成本,扩大投票的范围,方便快捷。因此,近年来它备受关注。

电子选举理想的协议[2]至少要有这样六项要求:

(1) 只有经授权的投票者才能投票。

(2) 每个人只能投票一次。

(3) 任何人都不能确定别人投谁的票。

(4) 没有人能复制其它人的选票。

(5) 没有人能修改其他人的选票而不被发现。

(6) 每个投票者都可以保证他的选票在最后的表中被计算在内。

此外,有些投票方案可能有如下要求:

(7) 每个人都知道谁投了票及谁没有投。

从上可知,电子投票要求在保持鉴别的同时,能以某种办法切断投票者与选票的关系。盲签名协议恰好胜任这一点。

电子投票有很多种模型,比较常用的是由一个注册机构审核投票人资格,一个投票机构接受投票的模式。投票过程可分为三阶段: 注册、投票和计票。设投票人为 U,注册机构 R,投票机构 V,以 yes和 no方式投票,则协议可以简单描述为:

(a) 注册

· U→ R　U证明自己的身份,并提交两张内容分别为 yes, no选票(每张选票各选一随机数为唯一序列号加入),选票分别盲化

· R→ U:　R确认 U的身份合法,并尚未参加投票;若符合条件,则将两张选票签名后返回给 U,否则拒绝 U的请求

(b) 投票

· U:　去盲后得到两张合法选票

· U→ V:　U按自己的意愿向 V提交一张选票,并用 V的公钥加密后发送给 V

· V→ U:　V用私钥解密后,验证签名。如签名有效,再查看数据库,选票中的序列号是否有记录。若有,则为重复选票,此票作废,终止协议;否则计票,并记录该序列号

(c) 计票

· V统计选票,并公布结果,以及选票对应的序列号

协议中采用盲签名使投票内容保密,在注册和投票时,R和 V分别检查各自的数据库,能确保只有经授权的投票人才能投票,每人投票不会超过一次。统计汇总时列出每个序列号所对应的选票内容,投票人若没找到自己的序列号,或发现选票内容改变了,可以发现舞弊现象,因此该方案满足电子投票的基本要求。但协议本身过于简单,如对 R和 V联手作弊增加莫须有的选票,当不同选票序列号冲突的处理等。如果考虑实际中的特殊情况,投票人委托他人代投,V授权下级子注册机构签名等等,可以采用特殊的盲签名方案,如代理盲签名和群盲签名。

电子现金和电子投票仅仅是盲签名在电子商务中应用的两个比较成熟的领域,盲签名在电子商务的其它领域也发挥着日益重要的作用,如进行口令认证、密钥分配和推动匿名评审制度等。

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki

4 结 论

盲签名是当前密码学研究领域中的一个热点,在电子商务中有着广阔的应用。本文通过对若干盲签名方案及其应用领域的讨论,概要总结了盲签名在电子现金和电子投票两大应用领域的技术问题。但由于应用问题的多样性和复杂性,目前在算法实现方面还存在诸多缺陷,有待突破。

参考文献:

[1] chaum D. Blind Signatures for Untraceable Payments[A]. Proc Cryto 82[C]. Santa Barbara, California: Springer-Verlag, 1983. 199-203.
[2] Bruce Schneier(美). 应用密码学—— 协议、算法与 C源程序[M]. 吴世忠,祝世雄,张文政,等译. 北京: 机械工业出版社, 2000.
[3] 祁 明,张 凌. 基于口令的盲签名方案[J]. 计算机工程与设计, 1998, 19(2): 16-20.
[4] 祁 明,史国庆. 强盲签名技术的研究与应用[J]. 计算机应用研究, 2001, (3): 34-37.
[5] Chaum D. Security Without Identification: Transaction Systems to Make Big Brother Obsolete[J]. Communications of the ACM, 1985, 28(10): 1030-1044.
[6] 钟 鸣,杨义先. 一种基于比特承诺的部分盲签名方案[J]. 通信学报, 2001, 22(9): 1-6.
[7] 王泽成,苏晓萍,汪精明. 一个基于椭圆曲线的代理签名和代理盲签名方案[J]. 青海大学学报, 2002, 20(3): 36-39.
[8] 祁明,许柏桐. 代理签名技术的研究与发展[J]. 计算机应用研究, 2001(9): 29-32.
[9] Chaum D, Fiat A, Naor M. Untraceable electronic cash[A]. Advances in cryptology crypto 88[C]. Berlin: Springer-Verlag, 1989. 319-327.
[10] 陈 恺,魏仕民,肖国镇. 电子现金系统的研究与发展[J]. 西安电子科技大学学报 (自然科学版), 2000, 27(4): 510-514.
[11] 钟 鸣,杨义先. 一种基于 RSA盲签名和二次剩余的电子现金方案[J]. 北京邮电大学学报, 2000, 23(3): 87-90.
[12] 陈 恺,杨 波,王育民,等. 利用电子钱包的有效的公正支付系统[J]. 计算机学报, 2001, 24(11): 1-5.
[13] 陈晓峰,王育民. 基于匿名通讯信道的安全电子投票方案[J]. 电子学报, 2003, 31(3): 390-393.
[14] 汪保友,杨 凤,胡运发. 基于盲签名的在线选举方案[J]. 小型微型计算机系统, 2002(3): 588-591.

(责任编辑: 陈石平)

(上接第 396页)

参考文献:

[1] Sami Zahran. 软件过程改进[M]. 陈新 罗劲枫译. 北京: 中信出版社, 2002.
[2] Carnegie Mellon University/software Engineering Institute. The Capability maturity model: guidelines for the software process[M]. Reading, MA: Addison-Wesley Publishing Company, 1995.
[3] 曹会明, 金茂忠, 刘超. 一种有效的软件过程改善模型[J]. 计算机工程与应用, 2001, 12: 89-92.
[4] Mark C, Paulk. A comparison of ISO9001 and the Capability maturity model for software[R]. Technical Report: CMU/SEI-94-TR-2, 1994.
[5] Humphrey W S. Managing the Software Process[M]. Reading, MA: Addison-Wesley, 1989.
[6] 郜宪林. 软件企业提高 CMM成熟度等级的一种途径[J]. 计算机工程与应用, 2002. 1: 111-113.
[7] 刘春颂, 扬寿保. CMM导入小型企业 /小型项目的研究[J]. 计算机工程与应用, 2002. 9: 88-91.
[8] 李 健, 金茂忠. 中小型企业软件过程改善方法研究[J]. 计算机工程与应用, 2001. 19: 107-111.

(责任编辑: 翁爱湘)

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki