CN43-1258/TP
ISSN 1007-130X
计算机工程与科学
COMPUTER ENGINEERING & SCIENCE
2005 年第 27 卷第 7 期
Vol 27, No 7, 2005

文章编号: 1007-130X(2005)07-0083-03

盲签名研究综述*
A Survey of Blind Signature Studies

史有辉, 李伟生
SHI You-hui, LI Wei-sheng
(北京交通大学计算机与信息技术学院, 北京 100044)
(Department of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China)

摘 要: 文章评述了目前盲签名及其应用已经取得的研究成果, 划分了研究发展的三个阶段, 并指出了现有的盲签名方案中存在的一些缺陷。最后, 本文提出了在这一领域中几个值得重视的研究方向。

Abstract: This paper surveys the studies in the field of blind signature first. Then several problems in the existing schemes are presented. Finally, three main research directions are pointed out as well.

关键词: 盲签名; 群盲签名; 部分盲签名; 比特承认; 离散对数

Key words: blind signature; group blind signature; partial blind signature; bit commitment; discrete logarithm

中图分类号: TP309 文献标识码: A

1 引言

数字签名是一项重要的计算机安全技术, 它的基本作用是保证传送的信息不被篡改和伪造, 并确认签名者的身份。盲签名是一种特殊的数字签名。1983 年, Chuam 首先提出了盲签名的概念[1]。之后, 对盲签名的研究不断深入, 强盲签名、部分盲签名的概念陆续被提出[2,3]。

盲签名是指签名者并不知道所签文件或消息的具体内容, 而文件或消息的拥有者又可以签名得到签名人关于真实文件或消息的签名。D. Chaum 曾给出了关于盲签名更直观的说明: 所谓盲签名, 就是先将要隐蔽的文件放入信封, 再将一张复写纸也放入信封, 签名的过程就是签名者将名字签在信封上, 他的签名便透过复写纸签到了文件上。基于盲签名的特点, 盲签名技术在电子货币、电子投票、电子支付等应用中的匿名性方面起着重要作用, 国内外学者就此进行了许多相关研究并取得了一定成果[4-6]。

2 盲签名

盲数字签名方案具有的特性: 消息的内容对签名者是盲的。

盲签名的实现: 由 Alice 发送盲消息 m' 给 Bob, 由 Bob 对盲消息 m' 进行签名, 并发送$(m', sign(m'))$给 Alice, Alice 利用$(m', sign(m'))$推得对消息 m 的签名 $sign(m)$, 得到$(m, sign(m))$。当 Bob 看到$(m, sign(m))$时可以验证它是自己对盲消息 m' 的有效签名。

强盲数字签名方案具有如下特性[2]:

(1) 消息的内容对签名者是盲的;

(2) 在签名被接收者泄漏后, 签名者不能追踪签名。

假设 u、v 是定义在两个不同概率空间的随机变量, 其概率分布分别为 $P(u)$、$P(v)$, 联合分布为 $P(u,v)$, 如果在多项式时间内无法区分概率分布 $P(u, v)$ 与 $P(u) * P(v)$, 则称 u、v 是不可联系的。

在盲签名方案中, 即使签名者存储盲消息 m' 及其签名 $sign(m')$ 或其他有关数据, 待$(m, sign(m))$公开后签名者也无法找出$(m', sign(m'))$和$(m, sign(m))$之间的联系, 即$(m', sign(m'))$和$(m, sign(m))$是不可联系的, 进而也就无法追踪到消息 m, 则称为强盲签名方案。若签名者可以将二者联系, 则称为弱盲签名方案。

3 盲签名的发展阶段及应用

经仔细研究, 我们认为盲签名的发展大致可以划分为以下三个阶段:

(1)1983~1994: 盲签名的提出与初步探索阶段。1983 年, Chaum 提出了首个盲签名方案, 方案建立在分解大整

* 收稿日期: 2003-11-13; 修订日期: 2004-02-12
作者简介: 史有辉(1978-), 男, 新疆塔城人, 硕士生, 研究方向为网络安全和网络数据库; 李伟生, 教授, 研究方向为算法设计与分析、网络数据库。
通讯地址: 100010 北京市东城区东四西大街 155 号西楼旅游分销业务部; Tel: (010) 84099781; E-mail: ccsyh@163.net
Address: Tourism Section, West Building, 155 Dongsi Avenue West, Dongcheng District, Beijing 100010, P.R. China

数困难性基础上,随后又给出了一个无法追踪支付系统中的盲签名方案[4]。1993 年,Okamoto 提出了第一个基于离散对数的盲签名方案[5]。1994 年,Carmenisch 等又提出一个基于离散对数的盲签名方案[6],同年 Hoster 推广了这个方案,提出一个基于离散对数的元盲签名方案[7]。

(2) 1995~ 1996:盲签名的进一步研究阶段。1995 年,L. Harn 给出了盲签名应该具备的另外两个特性[2],指出 Carmenisch 和 Hoster 等提出的基于离散对数的盲签名方案均不符合第二个特性,不是真正意义上的盲签名。很快,P. Horster、M. Michels 和 H. Petersen 作出回应,论证自己的方案作为盲签名方案的正确性。这次争论直接导致了强盲签名概念的提出,后来称 L. Harn 提出的盲签名[2]为强盲签名。1996 年,FAN 和 LEI 提出了一个基于二次剩余的有效盲签名方案[8]。之后,他们又提出了对于二次计算复杂度几乎最小的、更有效的盲签名方案[9]。这个阶段是一个活跃的讨论阶段。

(3) 1997~ 现今:盲签名深入、交叉研究阶段。2000 年,Elsayed Mohammeid 等提出了一种新的基于 ELGamal 的盲签名方案,该方案保证了在多次签名后相应的签名不同,因而使盲签名具有了匿名性[10]。同年,姚亦峰等提出了利用二元仿射变换,由 Harn 和 Xu 提出的 18 种安全广义 ELGamal 型数字签名方案[11]出发,构造其盲签名方案的方法[12]。2001 年,Hung-Yu Chien 等将部分盲签名应用于 RSA 上,提出一种低计算复杂度的部分盲签名方案[13]。这在移动客户端、智能卡等方面很有应用价值。1998 年,A. Lysyanskaya 和 Z. Ramzan 提出了群盲签名概念[14]。2001 年,钟鸣等先提出了一种基于比特承诺的盲签名方案[15]。2003 年,史有辉等提出了一种基于 XML 的 RSA 盲签名方案[16]。

盲签名是当前广泛应用的数字签名技术的重要组成部分之一,有着重要的应用价值和长远的应用前景。现今,已经提出的应用主要集中在电子支付[4]和电子现金[14,17]两方面。同时,在金融合同的签署、遗嘱签署、CA 证书的颁发等方面也有重要的应用。相信在未来社会中,盲签名技术的应用必将为社会经济发展做出更大的贡献。

4 盲签名的近期主要研究

4.1 群盲签名

A. Lysyanskaya 和 Z. Ramzan 将盲签名和群签名概念[18]结合起来提出了群盲签名[14],是对 J. Camenish 和 M. Stadler 的群签名方案[19]的推广。一个群盲签名方案应满足以下六条性质:

(1) 签名的盲性。签名人不知道对文件签过名,但他的签名却是可以验证的。

(2) 不可伪造性。只有群成员才能产生有效的签名。

(3) 不可否认性。签名人不可否认他自己的身份,群管理人总是可以确定发布合法签名的签名人的身份。

(4) 匿名性。除了群管理员外,任何人不能确定签名人的身份。

(5) 不关联性。在不打开签名的情况下任何人不能确定两个不同的签名是否是同一个群成员产生的。

(6) 安全性。群管理员和任何群成员都不能以其他群成员的名义签名。

文献[14]不仅给出了群盲签名的概念和一个具体方案,而且还指出了如何利用群签名构造多银行电子现金系统;文献[17]对群盲签名作了进一步的研究。

4.2 基于比特承诺的盲签名

4.2.1 部分盲签名方案的基本思想

部分盲签名方案可以看作一个集合$\{x, f(x), c, S(), V(), B(), U()\}$。其中,$x$ 和 $f(x)$ 分别是签名者的私钥和公钥。c 是签名者将在不泄露给发送者的前提下加入签名中的信息;$S(x, c, m)$ 是签名者用私钥 x 对信息 m 的签名;$V()$ 是签名验证函数,它使得$\{f(x), m, S(x, c, m)\}$满足 $V(f(x), m, S(x, c, m))$;$B()$ 是致盲函数,它使得 $B(m, r)$ 与消息 m 及致盲因子 r 统计无关;$U()$ 是脱盲函数,它使得 $U(S, r')$ 是脱盲后用户取得的最终签名,而且在脱盲因子 r' 不泄露的前提下 $U(S, r')$ 与 S 统计无关。

部分盲签名协议如下:

(1) 发送方将致盲后的信息 $B(m, r)$ 发送给签名方。

(2) 签名方用其私钥对信息进行签名,然后将签名 $S(x, c, B(m, r))$ 发送给发送方。

(3) 发送方检查签名是否满足验证函数 $V()$,接着对签名进行脱盲,即计算 $U(S(x, c, B(m, r)), r')$,从而计算得 $S(x, c, m)$。然后可以将签名和被签名信息 m 发送给签名方。

(4) 签名方可以检查 $S(x, c, m)$ 和 m 是否满足验证函数 $V()$,但无法获取任何有关用户的身份 c 的信息。

4.2.2 比特承诺

我们使用与文献[2]相同的比特承诺方案。

要建立比特承诺方案,B 首先生成素数 p(满足 $p = 2q+1$,这里 q 也是素数)、元素 G 和 g,使得它们在群 Zp 中的阶为 q。B 将 p、G 和 q 送给 U,然后 U 检查 $q = (p-1)/2$ 是不是一个素数(通过概率测试),以及 G 和 g 的阶是否为 q(通过检查等式 $G^q = 1 \bmod p$ 和 $g^q = 1 \bmod p$ 是否成立)。

U 能够提交任何整数 $s \in Zq$,这是通过随机选择 $R \in Zq$,然后计算比特承诺,即通过 $BCg(R, S) = G^R g^S \bmod p$ 实现的。比特承诺的公布是通过揭示 R 和 s 的值来实现的。为了简化表达,我们也可以把 $BCg(R, s)$ 写成 $BC(R, s)$ 或 $BC(s)$。

以下是一些基于比特承诺的协议,通过这些协议,U 能以一种零知识的方式向 B 证明被提交的整数位于某一区间内,或两个被提交的整数相等。限于篇幅的关系,这里我们不给出协议的具体流程。协议的详细流程请参见文献[2]。

令 $I = [a, b] (= \{x \mid a \leqslant x \leqslant b\})$,$e = b - a$,$I \pm e = [a - e, b + e]$。

协议一:比特承诺的检查。

共同输入:x 和 (P, G, g, I)。

U 向 B 证明:U 知道 (R, s),使得 $x = BCg(R, s)$ 和 $s \in I \pm e$。

协议二:两个比特承诺的比较。

共同输入:x, x' 和 (P, G, g, I)。

U 向 B 证明:U 知道 (R, R', s),使得 $x = BCg(R, s)$,$x' = BCg(R', s)$,且 $s \in I \pm e$。

协议三:模乘协议。

共同输入: x, y, z, n' 和 $(P, G, g, I = [n, 2n])(|(P-1)/2| \geqslant 2|n| + 6)$。

U 向 B 证明: U 知道 $(R, R', R^n, s, t, \alpha)$, 使得 $x = BCg(R, s)$, $y = BCg(R', t)$, $z = BCg(R'', \alpha)$, $\alpha = st(\mathrm{mod}\ t)$, 且 $s, t, \alpha \in [0, 3n](= I \pm e)$。

4.2.3 基于比特承诺的部分盲签名方案

下面介绍一种比特承诺的部分盲签名方案[15]。

令 $x \in_R S$ 代表在集合 S 中随机选择元素 x, Z_N^* 代表去掉 0 元素后的模 N 剩余类群, $H: \{0,1\}^* \rightarrow \{0,1\}^{2|N|}$ 代表一个多项式时间内可计算的单向 hash 函数。

签名者 S 随机选择私钥 $e \in_R Z_q^*$ 并将公钥 $BCg(e)$ 公开。p 和 q 的定义请参见 4.2.2 节。用户 p 获得关于信息 m 的部分盲签名的协议如下:

(1) S 选择 $u \in_R Z_q^*$, 然后计算并发送 $\alpha = BCg(u)$ 给 P。

(2) P 选择 $k, r \in_R Z_q^*$ 并计算 $\alpha = BCg(u)^* (BCg(e))^k BCg(r) \mathrm{mod}\ p$。根据比特承诺方案的性质有: $\alpha = BCg(u + ke + r)$。

(3) P 计算 $\varepsilon = H(m, \alpha) + k \mathrm{mod}\ q$, 然后将它发送给 S。

(4) S 计算 $R = u + \varepsilon^* e \mathrm{mod}\ p$, 并将 R 发送给 P。这里 S 可以把 ε 存储于数据库中作为用户 P 的身份标志信息, 以备将来用户 P 滥用签名时辨别其身份。

(5) P 验证是否 $BCg(R) = \alpha \cdot (BCg(e))^{\varepsilon} \mathrm{mod}\ p$, 然后 P 计算 $\rho = R + r \mathrm{mod}\ q$ 及 $T = BCg(\rho)$, 从而获得信息 m 的签名 $\{m, \alpha, T\}$。

另一用户 V 验证一个部分盲签名的有效性协议如下:

(1) P 将 $\{m, \alpha, T\}$ 发送给 V;

(2) V 计算 $H(m, \alpha)$ 然后验证是否 $T = \alpha \cdot (BCg(e))^{H(m, \alpha)} \mathrm{mod}\ p$;

(3) P 随后使用 5.2.2 节的 Check Commitment 协议向 V 证明他知道 ρ 使得 $T = BCg(\rho)$, 同时不泄露任何有关 ρ 的信息。

基于比特承诺的部分盲签名方案允许签名者在签名中加入用户的身份信息。这一新特征在提供了防止用户滥用签名方法的同时, 还能保证签名者不能侵犯用户的身份隐私。容易证明, 在这种部分盲签名方案中, 通过选择明文攻击来伪造签名的难度相当于攻破离散对数问题的难度。但是, 方案的效率还有待进一步提高, 并应将方案的安全性建立在更一般性的密码学假设的基础上。

5 展望

(1) 如何设计高效的盲签名方案。现有盲签名方案的效率并不太令人满意, 而且存在提高的空间[8, 9, 19], 所以设计高效的方案值得关注。

(2) 与盲签名相关的数字签名及其应用的研究。在各种签名技术及其相关技术(RSA、密码学、代理签名、盲签名、门限签名等)之间很容易产生出新的数字签名技术, 特别是与盲签名相关的数字签名及其应用的研究还很不够, 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, 群盲签名[14]、基于比特流信息的盲签名[15]、利用广义 ELGamal 型签名或 DSS 构造强盲签名[11, 12]等都处于起步阶段, 但它们却有着实际和良好的应用前景。

(3) 如何在电子商务等领域更广泛地应用盲签名。在现有的文献中已经出现一些关于盲签名在电子商务等领域的应用研究[4, 14, 17], 但距离被广泛使用还有一段距离, 主要是因为现有盲签名方案的复杂性、安全性、适用性等方面存在一些不足。因而, 提出高效、安全、实用的盲签名的电子商务应用是一个重要的研究方向。

6 结束语

本文总结并评述了目前盲签名及其应用已经取得的研究成果, 划分了研究发展的三个阶段, 并指出了现有的盲签名方案中存在的一些缺陷。最后提出了这一领域中几个值得重视的研究方向。

参考文献:

[1] D Chaum. Blind Signature Systems[A]. Proc CRYPTO' 83[C]. 1984. 153-156.

[2] L Harn. Cryptanalysis of the Blind Signature Based on the Discrete Logarithm Problem[J]. Electronic Letters, 1995, 31(14): 1136-1137.

[3] M Abe, E Fujisaki. How to Date Blind Signature[A]. Proc of Advances in Cryptology-Asiacrypt[C]. 1996. 244-251.

[4] D Chaum. Blind Signature for Untraceable Payments[A]. Proc CRYPTO' 82[C]. 1983. 199-203.

[5] T Okamoto. Provable Secure and Practical Identification Schemes and Corresponding Signature Schemes[A]. Proc Crypto' 92[C]. 1993. 31-53.

[6] J Chamenisch, J M Piveteau, M A Stadler. Blind Signatures Based on the Discrete Logarithm Problem[A]. Eurocrypt' 94[C]. 1995. 428-432.

[7] P Horster, M Michels, H Petersen. Meta Message Recovery and Meta Blind Signature Based on the Discrete Logarithm Problem and Their Applications[A]. Pre-Proc Asiacryp' 94[C]. 1994. 185-196.

[8] G-I FAN, G-L LEI. Efficient Blind Signature Scheme Based on Quadratic Residues[J]. Electronic Letters, 1996, 32(9): 811-813.

[9] G-I FAN, G-L LEI. User Efficient Blind Signatures[J]. Electronic Letters, 1996, 34(6): 544-546.

[10] Elsayed Mohammed, A E Emarah, K El-Shennawy. A Blind Signature Scheme Based on ELGamal Signature[A]. 17th National Radio Science Conf[C]. 2000. 51-53.

[11] L Harn, Y Xu. Design of Generalized ELGamal Type Digital Signature Schemes Based on Discrete Logarithm[J]. Electronic Letters, 1993, 29(12): 2025-2026.

[12] 姚亦峰, 朱华飞, 陈抗生. 基于二元仿射变换的广义 ELGamal 型盲签名方案[J]. 电子学报, 2000, 28(7): 128-129.

[13] Hung-Yu Chien, Jinn-Ke Jan, Yuh-Min Tseag. Rsa-Based Partially Blind Signature with Low Computation[J]. Proc of Asiacrpt' 2000[C]. 2001. 385-389.

[14] A Lysyanskaya, Z Ramzan. Group Blind Digital Signature: A Scalable Solution to Eletronic Cash[A]. Proc of the 2nd Financial Cryptography Conf[C]. 1998. 184-197.

[15] 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.

[16] 史有辉, 李伟生. 一种基于RSA的XML盲签名方案[J]. 计算机工程, 2004, 30(19): 101-103.

[17] T Okamoto. An Efficient Divisible Electronic Cash Scheme

(下转第 94 页)

1993. 207-216.
[2] 李绪成, 王保保. 挖掘关联规则中 Apriori 算法的一种改进[J]. 软件技术与数据库, 2002, 28(7): 104-106
[3] 陆丽娜, 陈亚萍, 魏恒义, 等. 挖掘关联规则 Apriori 算法的研究[J]. 小型微型计算机系统, 2000, 21(9): 940-943.
[4] 朱玉全, 孙志挥. 一种有效的关联规则增量式更新算法[J]. 计算机工程与应用, 2001, 23(9): 28-29.
[5] 高峰, 谢剑英. 一种无冗余的关联规则发现算法[J]. 上海交通大学学报, 2001, 35(2): 256-258.
[6] 罗可, 吴杰. 怎样获得有效的关联规则[J]. 小型微型计算机系统, 2002, 23(6): 711-713.
[7] 倪志伟, 蔡庆生, 方瑾. 用神经网络来挖掘数据库中的关联规则[J]. 系统仿真学报, 2000, 12(6): 685-687.
[8] 周欣, 沙朝锋, 朱扬勇, 等. 兴趣度-关联规则的又一个阈值[J]. 计算机研究与发展, 2000, 37(5): 627-633.
[9] 周皓锋, 朱扬勇, 施伯乐. 一个基于兴趣度的关联规则采掘算法[J]. 计算机研究与发展, 2002, 39(4): 450-457.
[10] http://www.ics.uci.edu/~mlearn/MLSummary.html, 2003-05.

(上接第 85 页)

[A]. Proc of Advances in Cryptology-Crypo'95[C]. 1995. 438-435.
[18] D Chaum, V E Hheyst. Group Signature[A]. Proc of Eurocrypt'91[C]. 1991. 257-265.
[19] J Camenish, M Stadler. Efficient Group Signature for Large Groups[A]. Proc of Eurocrypt'97[C]. 1997. 410-424.
[20] J Camenish, M Michels. A Group Signature Scheme with Improved Efficiency[A]. Proc of Asiacrpt'98[J]. 1998. 160-174.
[21] Z Ramzan. Group Blind Signature a Lacarte[EB/OL]. http://theory.lcs.mit.edu/~zulfikar/homepage.html, 1999-03.

(上接第 87 页)

7000, 调节 R-7000 的解调模式为 AM, 接收频点为 320MHz。这时, 我们从 R-7000 的扬声器里清晰地听到了收音机的声音, 即交叉调制造成了用户音频信息的泄露。

5 结束语

我们通过以上实验对移动电话交叉调制可能产生信息泄露的可能性做了定性研究。从实验中可以得出以下结论:

移动台交叉调制辐射信号产生信息泄露的可能性确实存在, 可以被接收并经过处理后还原。在我们的实验中, CDMA 和 GSM 的射频信号在足够强的时候, 都和测试电路中的用户信息产生了交叉调制现象, FAM 对 CDMA 和 GSM 射频信号解调后都在示波器上看到了原始信息。我们的实验中, 信号源 2 就相当于固定频点发射信号的移动台, 在某些情况下也可能是基站。只要有固定频点的 GSM 或 CDMA 信号发射, 就有可能造成周围的用户电路系统产生交叉调制信息泄漏发射。CDMA 是固定频点发射, GSM 是跳频发射, 但广播信道也是固定频点发射。这种交叉调制造成泄密的可能性应该引起我们的高度重视。

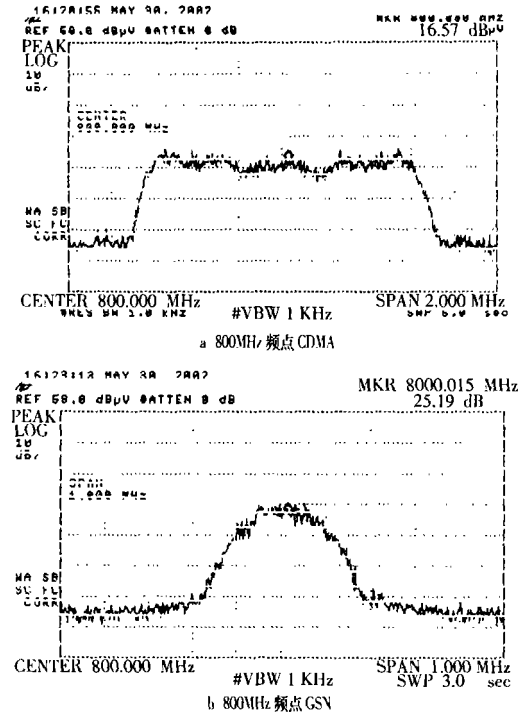

图 5 交叉调制频谱

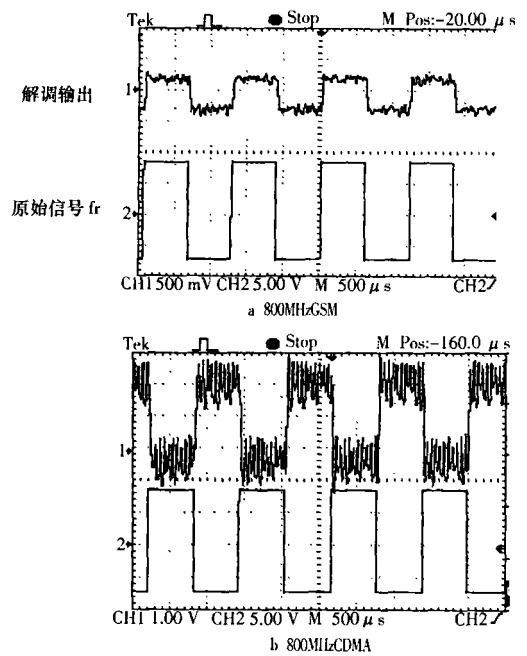

图 6 交叉调制解调波形

参考文献:

[1] 石长生, 李国定. 红信号电磁辐射泄漏发射分类[A]. 中国计算机学会信息保密专业委员会论文集[C]. 2001.