

一种新的基于离散对数的弱盲签名方案

于 丹, 缪祥华

(昆明理工大学 信息工程与自动化学院, 云南 昆明 650500)

摘 要:盲签名是接收者在签署消息的时候, 不让签名者知道消息的具体内容, 从而采取的一种特殊的数字签名技术。文中简介了盲签名方案的分类, 由于弱签名具有可追踪性, 可以对消息拥有者进行追踪, 可以应用于很多需要对签名建立联系的电子领域中。由于盲参数签名方案具有不安全性, 所以文中在对 J. Camenisch 提出的盲参数签名方案基础上, 结合盲参数签名方案与已有的弱盲签名方案的构造方法, 构造出了一种新的基于 ElGamal 的离散对数的弱盲签名方案, 并对提出的弱盲签名方案进行了安全性的分析和效率的比较。

关键词:盲签名; 弱盲签名; 离散对数

中图分类号: TP309

文献标识码: A

文章编号: 1673-629X(2013)10-0123-04

doi: 10.3969/j.issn.1673-629X.2013.10.031

A New Weak Blind Signature Scheme Based on Discrete Logarithms

YU Dan, MIAO Xiang-hua

(College of Information Engineering and Automation, Kunming University of Science and Technology,
Kunming 650500, China)

Abstract: Blind signature is a special digital signature technology, which is the content of news that the signer don't know and get signed by receiver. In this paper, briefly introduce the classification of blind signature, due to the weak signature has traceability, it can track the news owner, which can be applied many electronic field contact to signature. Because blind parameter digital signature is unsafe, on the basis of J. Camenisch's blind parameter digital signature scheme, by integrating present blind parameter digital signature scheme and the signature, it constructs a new weak blind digital signature based on ElGamal discrete logarithms. It analyzes security of the new weak blind digital signature and conducts the efficiency comparison.

Key words: blind signature; weak blind signature; discrete logarithms

0 引 言

数字签名是现代密码学最重要的组成部分之一, 是设计密码协议的一个基本模块。如果数字签名被授权可以发送数据时, 那么它必须具有可靠性、真实性和不可否认性^[1]。然而, 普通的数字签名在电子贸易和电子政务方面并不能满足它所需要的要求。比如, 数字签名不能保护信息拥有者的匿名性, 而在电子支付和电子投票系统必须保证信息拥有者的隐私, 所以有了盲签名的概念。

盲签名^[2]是 Chaum 首次在 1982 年提出的, 盲签名是接收者允许签名者对消息 m 进行签名, 但是签名者并不知道任何关于 m 的信息。盲签名是一种特殊的数字签名^[3], 它能保证信息拥有者的匿名性从而保护用户的隐私。正因为如此, 盲签名被广泛应用在电

子投票和电子现金中。在电子投票系统中, 选票需要管理者进行签名才能有效, 但是选票的内容包括管理者在内的任何人都不知道。在电子支付系统中, 银行在每一次交易中, 签名电子现金时必须保证用户的匿名性。

Chaum 第一次提出基于大整数分解的盲签名方案是在 1983 年, 方案中使用者在某种程度上获得签名的信息, 而签名者既不知道原消息, 也不知道签名的结果, 这种方案保证了不可追踪性和不可连接性。1995 年, Harn 第一次介绍了基于离散对数的盲签名方案。在随后的几年里, 盲签名得到了很大的发展, 通过对签名方案的不断改进, 已经提出了很多有效且安全的盲签名方案, 将一般的数字签名盲化后不仅增加了安全性, 而且使得应用的领域更加广泛。像短签名减少了

收稿日期: 2012-12-22

修回日期: 2013-03-26

网络出版时间: 2013-07-24

基金项目: 昆明理工大学科学研究基金 (2007-29)

作者简介: 于 丹 (1987-), 女, 吉林长春人, 在读硕士, 研究方向为信息安全、盲签名、密码学; 缪祥华, 副教授, 博士, 研究方向为信息安全。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20130724.1003.027.html>

计算的复杂度,代理签名^[4]可以将签名授权给其他签名者。

下面按照对不同参数的盲化以及盲化的强度进行分类:

(1)强盲签名:因为管理者不能跟踪授权的选票,所以强盲签名方案被用在电子投票系统。所以强盲签名就是签约人无法从签名过程获得的信息中跟踪消息所有者。

(2)弱盲签名:在电子支付系统中,银行就可以用弱盲签名方案来追踪违法的客户,比如盗取账号的人、洗钱者。所以弱盲签名就可以通过跟踪消息的拥有者来达到追踪的目的。

(3)部分盲签名顾名思义,就是在于被签名的消息文件是由接收者和签名者共同产生的,包括接收者的原消息 m 和签名者的相关信息(如身份信息 ID)。假设签名者的有关信息为 m ,则部分盲签名的过程是:签名者将原消息 m 盲化为 m' 后发送给签名者,然后签名者用其私钥将 m_w 和 m' 合并后进行签名并发送给接收者,接收者通过去盲后得到最终的签名。任何人可以根据签名者的公钥来对签名进行验证。

也可以根据不同数学问题而建立起来的盲签名来进行分类:

(1)基于大数分解问题的盲签名:RSA 签名方案就是两个著名签名方案之一,其安全性就是基于大数分解的困难性。自首次提出将盲签名应用在 RSA 签名方案后,Chaum 第一次应用在电子现金系统的取款协议上。在 RSA 盲签名方案中,选取一个大复合数 n , a ,私钥为 d ,公钥为 e ,为了使得消息 m 在签名的过程中是保密的,用户将产生一个随机数 $r \in \mathbb{Z}_n^*$ 来达到盲化的效果,发送 $m' = mr^e \pmod n$ 给签名者,然后签名者对 m' 进行签名 $s' = m'^d \pmod n$ 并发送给接收者,接收者就很简单地计算出 $s = s' r^{-1} \pmod n$ 即是 m 的有效签名。

(2)基于离散对数问题的盲签名^[5-6]:基于 ELGamal 也是常常被用来作为安全有效的盲签名。这个转化过程被一次应用在没有“cut-and-choose”的电子现金系统中。

Schnorr 方案是非常有名的零知识算法^[7-9],将 Schnorr 加入盲化因子就可以变成 Schnorr 的盲签名,从而达到期望的效果。ELGamal 在加密和解密的时候,速度比较快,这个优点可以用在快速签名的领域中。

由于弱盲参数签名需要把消息发送给签名者,如果签名者泄露信息给其他人,这样就会使得签名变得不安全,所以文中将消息进行盲化处理变成弱盲签名,使得签名变得更加安全。

1 ELGamal 签名方案

在 ELGamal 签名方案中,选取 p 是 Z_p 中的一个素数,集合 $Z_p = \{0, 1, 2, \dots, p\}$,令 a 是 $\text{GF}(p)$ 中的本原元,消息集 $p = Z_p^*$,签名集 $A = Z_p^* * Z_{p-1}^*$ 。

私钥:用户随机选取 $x, x \in Z_p$ 为私钥。

公钥:计算 $y = a^x \pmod p$,选取 y 为公钥。

签名过程:

(1) Alice 将给定要签名的消息为 $m \in Z_p$ 发送给 Bob。

(2) Bob 接收到 Alice 发送的消息 m 后,生成一个随机数 $k, k \in Z_p$;计算 $r = a^k \pmod p, s = k^{-1}(m - xr) \pmod (p-1)$ 。则签名结果为 (r, s) 。把签名结果发送给接收者 Alice。

验证过程:

取得发送方的公钥 y ;计算 $a^m = r^s * y^r \pmod p$ 是否成立;若成立,则签名有效,若不成立,则签名无效。

签名的验证:

$$\begin{aligned} a^m &= r^s * y^r \pmod p \\ &= a^{ks} * a^{xr} \pmod p \\ &= a^{kx+mr} \pmod p \\ &= a^m \pmod p \end{aligned}$$

所以 (r, s) 是 Alice 对消息的有效签名。

2 J. Camenisch 的盲参数签名方案

在该方案中, p 是一个大素数, a 是 $\text{GF}(p)$ 中的本原元,签名者 Bob 的秘密钥为 $x, x \in [1, p-1]$,公钥为 $y = a^x \pmod p$ 。J. Camenisch 的盲参数签名方案如下:

签名过程:

(1) 接收者 Alice 选择 $m \in [1, p-1]$,随机选取 $h \in Z_{p-1}^*$,计算 $\beta = a^h \pmod p$,将 (m, β) 发送给 Bob。

(2) Bob 选择一个随机数 $k \in Z_{p-1}^*$,计算 $r' = \beta^k \pmod p, s' = [k^{-1}(m + xr')] \pmod (p-1)$,将 (r', s') 发送给 Alice。

(3) Alice 计算 $r = r', s = (s' h^{-1}) \pmod (p-1)$ 。 m 的签名为 $\text{sig}(m) = (r, s)$ 。

验证过程:

验证 $r^s = a^m * y^r \pmod p$ 是否成立,若成立,则签名有效;若不成立,则签名无效。基本过程如图 1 所示。

签名的验证:

$$\begin{aligned} r^s &= a^m * a^{xr} \pmod p \\ \beta^{ks} &= a^{m+xr} \pmod p \\ a^{hks} &= a^{m+xr} \pmod p \text{ 可以得到} \\ hks &= (m + xr) \pmod p \\ hk s' h^{-1} &= (m + xr) \pmod p \end{aligned}$$

$ks' = (m + xr) \bmod p$
 $s' = [k^{-1}(m + xr')] \bmod (p - 1)$
所以 (r, s) 是 Alice 对消息的有效签名。

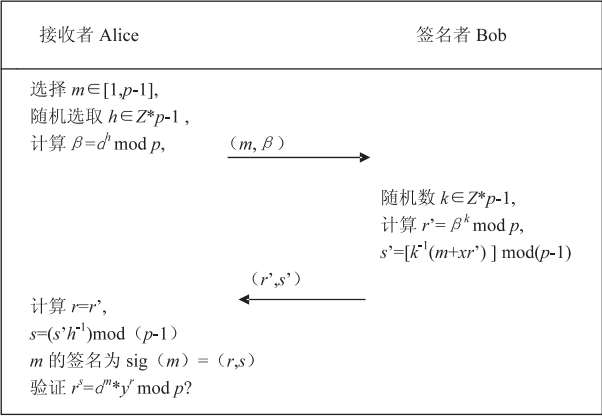


图 1 J. Camenisch 的盲参数签名方案

可以看到在这个签名方案中, Alice 必须要将消息 m 传给 Bob 才能进行对其签名, Bob 就可能泄露消息或者发给其他人, 从而造成信息的流失和不必要的麻烦。下面结合盲参数签名方案与已有的弱盲签名方案^[9]的构造方法, 基于离散对数构造出一个新的弱盲签名方案^[10]。在这个方案中既实现了对消息盲化处理后进行签名, 又具有可跟踪性。

3 新的弱盲签名方案

在该方案中, p 是一个大素数, a 是 $\text{GF}(p)$ 中的本原元, 签名者 Bob 的密钥为 $x, x \in [1, p - 1]$, 公钥为 $y = a^x \bmod p$ 。新的弱盲签名方案如下:

签名过程:

- (1) 接收者 Alice 选择 $m \in [1, p - 1]$, 随机选取 $h \in Z_{p-1}$, 计算 $\beta = a^h \bmod p$, 将 β 发送给 Bob。
- (2) Bob 选择一个随机数 $k \in Z_{p-1}^*$, 计算 $r' = \beta^k \bmod p$, 将 r' 发送给 Alice。
- (3) Alice 随机选取 $a, b \in Z_{p-1}^*$, 计算 $r = (r'^a a^b) \bmod p, m' = [r'^{-1}(mr + b)] \bmod (p - 1)$, 将 m' 发送给 Bob。
- (4) Bob 计算 $s' = [k(m'r' - x)] \bmod (p - 1)$ 。将 s' 发送给 Alice。
- (5) Alice 计算 $s = (a^{-1} h^{-1} s') \bmod (p - 1)$, m 的签名为 $\text{sig}(m) = (r, s)$ 。

验证过程:

验证 $y = (r^s * a^{mr}) \bmod p$ 是否成立, 若成立, 则签名有效; 若不成立, 则签名无效。基本过程如图 2 所示。

签名的验证

由 $s' = [k(m'r' - x)] \bmod (p - 1)$ 得
 $x = s' + k(m'r' + r') \bmod (p - 1)$ (1)

若 $y = (r^s * a^{mr}) \bmod p$ 成立, 则 $y = r^s a^{mr} \bmod p = (a^{ahks} * a^b) * a^{mr} \bmod p$, 由此可得
 $x = (ahks + mr + b) \bmod (p - 1)$ (2)
将(1) 带入(2) 得
 $s' + k(m' + r') = (ahks + mr + b) \bmod (p - 1)$

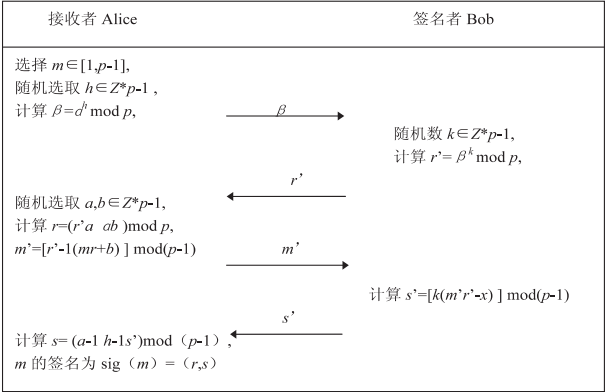


图 2 新的弱盲签名方案

比较 k 前面的系数和常数项, 可得:

$s = (a^{-1} h^{-1} s') \bmod (p - 1)$
 $m' = [r'^{-1}(mr + b)] \bmod (p - 1)$
上述过程逆推, 即得 $y = (r^s * a^{mr}) \bmod p$ 。

4 安全性的分析和证明

(1) 定理 1 (可跟踪性): 签名者 Bob 得到的是盲化后的消息 m' 和自己签名后的 $\text{sig}(m')$, 而无法得知最终的签名 $\text{sig}(m)$ 。如果签名者 Bob 存储 $\text{sig}(m')$ 或其他中间产生的相关数据, 如果 $\text{sig}(m)$ 被公开后, Bob 就可以找到 $\text{sig}(m')$ 和 $\text{sig}(m)$ 之间的关系, 从而达到对消息拥有者 Alice 的跟踪^[11]。即该方案具有可跟踪性。

证明: 如果签名者保留 (m', r', s', β, k) , 则当 Alice 公开 $\text{sig}(m) = (r, s)$ 后, Bob 由 $s = (a^{-1} h^{-1} s') \bmod (p - 1), m' = [r'^{-1}(mr + b)] \bmod (p - 1)$ 可确定出 $b', (ah)'$ 。为了证实 $\text{sig}(m) = (r, s)$ 是从 $\text{sig}(m') = (m', r', s')$ 所求得, Bob 只需验证等式 $r = (a^k)^{(ah)'} * a^{b'} \bmod p$ 和 $m' = [r'^{-1}(mr + b)] \bmod (p - 1)$ 是否成立, 若成立, 则可确认 $\text{sig}(m)$ 和 $\text{sig}(m')$ 相对应。

(2) 定理 2 (不可伪造性): 如果接收者 Alice 或者签名者 Bob 想要伪造签名并合法化, 就必须从中解决离散对数问题, 而由上面可知离散对数是属于数学上的难解问题, 所以该方案具有不可伪造性^[12]。下面通过两个方面来证明此方案的不可伪造性。

①接收者 Alice 伪造盲签名并将其合法化的可能性。

签名者 Bob 在盲签名的过程中加入了随机数, 使接收者 Alice 和其他攻击者都不能推测出签名者 Bob

签名的具体内容,该随机性可以有效地抵御选择明文攻击,防止接收者 Alice 的伪造签名。在该安全的签名方案中,用户无法知道签名者 Bob 的随机数。

证明:签名者 Bob 随机选取 $k \in Z_{p-1}^*$, 计算 $r' = \beta^k \bmod p$, 将 r' 发送给 Alice, Alice 发送 $m' = [r'^{-1}(mr + b)] \bmod (p - 1)$ 给 Bob, Bob 发送 $s' = [k(m'r' - x)] \bmod (p - 1)$ 给 Alice。如果攻击者 Alice 试图知道随机数 k , 则接收者或者攻击者必须从 $\beta = a^h \bmod p, r' = \beta^k \bmod p$ 计算得到 h 和 k , 而解决此类问题就需要面对有限域上的求解离散对数的难题。

② 签名者伪造合法盲签名的可能性。
证明:如果签名者 Bob 想要伪造一个合法的签名, 那么他会有两个问题需要解决: 第一, 如果签名者想要冒充 Alice 将原消息 m 进行盲化, 由 $m' = [r'^{-1}(mr + b)] \bmod (p - 1)$ 可知, 在不知道 b 的情况下, Bob 根本无法完成对消息 m 的盲化过程。第二, 如果签名者想要冒充 Alice 进行脱盲处理, 则由 $s = (a^{-1}h^{-1}s') \bmod (p - 1)$ 可知, 在 a, h 都不知道的情况下, 签名者 Bob 也无法实现对签名 s' 的脱盲。解决上述问题同样需要面临有限域上求解离散对数的难题。

(3) 定理 3 (弱盲性): 该方案具有弱盲性。
证明: 由 $m' = [r'^{-1}(mr + b)] \bmod (p - 1)$ 可知 Alice 发送给 Bob 的是经过盲化之后的消息 m' 。而如果要找出 $\text{sig}(m)$ 和 $\text{sig}(m')$ 之间的关系, 这就需要知道消息 m , 才能计算出 $b, (ah)$, 从而成为一个弱签名方案。

5 实验结果及效率的分析

下面的实验数据是通过实验 CAP 软件计算出的结果, 可以证明出该方案在理论上是可行的, 具有正确性和可操作性。

在实验中, p 是一个大素数, 可以选择 $p = 129\,841$, $a = 26$ 是 $\text{GF}(p)$ 中的本原元, 签名者 Bob 的密钥为 x , $x \in [1, 129\,840]$, 可以选择 $x = 423$, 公钥为 $y = a^x \bmod p = 115\,917$ 。新的弱盲签名方案如下:

- 签名过程:
- (1) 接收者 Alice 选择 $m \in [1, 129\,840]$, 可以取 $m = 541$, 随机选取 $h = 48\,827 \in Z_{129\,840}$, 计算 $\beta = a^h \bmod p = 29\,422$, 将 β 发送给 Bob。
- (2) Bob 选择一个随机数 $k = 879 \in Z_{129\,840}^*$, 计算 $r' = \beta^k \bmod p = 126\,521$, 将 r' 发送给 Alice。
- (3) Alice 随机选取 $a, b \in Z_{129\,840}^*$, 我们不妨取 $a = 122\,951, b = 325$, 计算 $r = (r'^a a^b) \bmod p = 93\,158, m' = [r'^{-1}(mr + b)] \bmod (p - 1) = 74\,283$, 将 m' 发送给 Bob。
- (4) Bob 计算 $s' = [k(m'r' - x)] \bmod (p - 1) =$

66 420。将 s' 发送给 Alice。
(5) Alice 计算 $s = (a^{-1}h^{-1}s') \bmod (p - 1) = 54\,300, m$ 签名为 $\text{sig}(m) = (r, s) = (93\,158, 54\,300)$ 。
这时候只需要验证 $y = 115\,917 = (r^s * a^{mr}) \bmod p$ 是否成立, 如果成立, 则接受该签名。

由上述实验数据可知, 文中所提出的新的弱盲签名方案是正确、有效的。在实际的应用中, 很容易在奔腾四微型机上实现方案中的签名过程和验证过程, 从而说明所提出的新的弱盲签名方案具有实际可操作性。试验中可以采用 309 左右素数 p , 集合为 Z_p 。其中所采用的是有效的 Montgomery 算法和扩展 Euclid 算法。

将文献[4]中的弱盲签名方案和文中的方案进行计算效率的对比, 主要是在盲化函数的运算过程中有所不同, 所以, 只要比较出文献中的签名方案和文中方案在盲化过程的计算效率就能得出文中方案具有很高的效率, 具体数据如表 1 所示。其中, T_{mul}, T_h 分别代表乘法运算、求逆运算在模 p 的情况下所花的时间。

表 1 计算效率比较

盲签名方案	盲化过程中的运算时间
方案 1	$4T_{mul} + 3T_h$
方案 2	$7T_{mul} + 2T_h$
方案 3	$2T_{mul} + 2T_h$
方案 4	$2T_{mul}$
方案 5	$2T_{mul} + 2T_h$
方案 6	$4T_{mul} + 1T_h$
文中方案	$2T_{mul} + 1T_h$

可以看到文中的方案要比方案 4 多了一次求逆运算。但是当 k 值取得很大的时候, 方案 4 中的 s 会变得很小, 这样很容易被攻破, 从而降低了签名的安全性。

6 结束语

文中结合盲参数签名方案与已有的弱盲签名方案的构造方案, 提出了一种新的弱盲签名方案。同时, 还证明了该方案是安全的, 且计算性能有明显优势。此外, 能否将该思想应用于其他电子签名系统(如授权签名系统)中, 还有待研究。

参考文献:

[1] 范 函, 张少武. 对两个基于离散对数的数学签名方案的攻击分析与改进[J]. 计算机应用, 2011, 31(7): 1859-1861.

[2] Chaum D. Blind signature for untraceable payments[C]//Proc of Crypto 82. New York: Plenum Press, 1983: 199-203.

[3] Song F, Cui Z. Electronic voting scheme about ElGamal blind-signatures based on XML[C]//Proc of 2012 International

在观察中的视点方向来计算出目标点在虚拟空间的三个分量值,在准备好了视点、目标点、视点方向这三个值后调用 gluLookAt() 即可实现主板任意角度的浏览。可以通过左右键实现左转右转,上下键实现前移后移, PgUp、PgDown 键实现仰俯角,这样可以满足用户多方面浏览主板的各个部件。

4 结束语

该系统利用 3DS MAX 软件对华硕 AT3N7A-I 主板上大部分部件进行了精细的模拟,并导出它们的. 3ds 文件,利用 Deep Exploration. exe 软件对. 3ds 文件优化和更改,使模型显示出来的效果更好。然后调用 OpenGL 的大量函数实现三维主板模型的显示,并最终实现主板的浏览功能。该系统的不足之处在于只实现了键盘控制漫游的功能,无法利用鼠标实现漫游,对主板部件不能实现放大、缩小的功能。该系统功能较为单一,没有很好地实现人机交互功能,在今后的学习与研究中会在这些不足中继续改进。

参考文献:

[1] 汪成为,高文,王行仁. 灵境(虚拟现实)技术的理论、实现及应用[M]. 北京:清华大学出版社,1998.

+++++

(上接第 126 页)

Workshop on Information and Electronics Engineering. [s. l.]:[s. n.],2012:2721-2725.

[4] 蔡庆华,陈文莉. 基于双线性对的代理签名[J]. 计算机技术与发展,2006,16(9):230-232.

[5] 杜伟章,陈克非. 基于离散对数问题构造弱盲签名方案[J]. 计算机工程与应用,2003,39(16):11-12.

[6] 袁丁,范平志. 基于离散对数问题的盲数字签名改进方案[J]. 四川大学学报(自然科学版),2006,43(4):787-789.

[7] 李波,邱小平. 复合离散对数与安全认证研究[J]. 计算机科学,2004,31(6):146-148.

+++++

(上接第 153 页)

[9] Gersho A,Gray R M. Vector quantization and signal compression[M]. New York:Kluwer,1992.

[10] 韩静宇,陈善学,刘丹蕾,等. 矢量量化快速码字搜索算法研究综述[J]. 黑龙江科技信息,2009(3):45-45.

[11] 郝东来,葛建华. 一种多小区 MIMO 系统的分层预编码方案[J]. 西安电子科技大学学报(自然科学版),2010,37(4):624-629.

[12] 王伟达,何旭,武刚. 基于最小均方误差的多用户 MIMO 下行预编码[J]. 电子技术应用,2009(2):108-110.

[2] Addison A C. Emerging Trend in Virtual Heritage[J]. IEEE MultiMedia,2000,7(2):22-25.

[3] 柯育龙. 基于 VRML 的校园系统建模的研究[D]. 成都:西南交通大学,2006.

[4] Kahaner D. Japanese activities in virtual reality[J]. IEEE Computer Graphics and Applications,1994,14(1):75-78.

[5] 杨键,耿卫东,潘云鹤,等. 基于图像的虚拟景观漫游[J]. 计算机辅助设计与图形学学报,2001,13(3):229-235.

[6] Wright R,Sweet M. OpenGL 超级宝典[M]. 第 2 版. 北京:人民邮电出版社,2001.

[7] 万剑华,李桂荃,张纪松. 基于 OpenGL 的三维城市景观模型的建立[J]. 石油大学学报(自然科学版),2003,27(1):102-104.

[8] 李彦娜. 虚拟现实与图形建模技术在仿真中的应用研究[D]. 北京:北京工商大学,2004.

[9] 汤晓安,陈敏,孙茂印. 复杂几何模型的混合绘制算法研究[J]. 计算机辅助设计与图形学学报,2002,14(6):509-512.

[10] 曾强,张凯,郑世力,等. 3DSMax7 建筑表现图设计精彩实例[M]. 北京:清华大学出版社,2005.

[11] Kanaya I,Chen Qian,Kanemoto Y,et al. Three-Dimensional Modeling for Virtual Relic Restoration[J]. IEEE MultiMedia,2000,7(2):42-44.

+++++

[8] 陈华,蔡光兴. Schnorr 盲签名的一般化及其安全性分析[J]. 信息安全与通信保密,2007(6):231-233.

[9] 李方伟,万丽,闫少军. 基于椭圆曲线的盲代理盲签名方案[J]. 计算机工程,2012,38(3):139-140.

[10] 马冬兰,张建中. 对 Wu-Wang 盲签名方案的攻击与改进[J]. 计算机工程与应用,2012,48(4):77-78.

[11] 万丽,李方伟,闫少军. 一个代理盲签名方案的分析与改进[J]. 计算机应用,2011(4):989-991.

[12] 敖青云,陈克非,白英彩. 基于离散对数问题的一般盲签名方案[J]. 计算机工程与应用,2001(1):12-13.

+++++

[13] Yuan F,Yang C. Phase ambiguity quantization for per-cell codebook based limited feedback coordinated multi-point transmission systems[C]//Proc of Int Conf on Vehi Tech. Yokohama:IEEE,2011.

[14] Love D J,Robert W H,Strohme T. Grassmannian beamforming for multiple-input multiple-output wireless systems[J]. IEEE Transactions on Information Theory,2003,49(10):2735-2746.

一种新的基于离散对数的弱盲签名方案

作者：[于丹](#)，[缪祥华](#)，[YU Dan](#)，[MIAO Xiang-hua](#)
作者单位：[昆明理工大学 信息工程与自动化学院, 云南 昆明, 650500](#)
刊名：[计算机技术与发展](#)

英文刊名：[Computer Technology and Development](#)

年，卷(期)：2013(10)

本文链接：http://d.wanfangdata.com.cn/Periodical_wjfz201310031.aspx