第16卷 第11期
2006年11月

计算机技术与发展
COMPUTER TECHNOLOGY AND DEVELOPMENT

Vol. 16 No. 11
Nov. 2006

基于双线性对的代理盲签名

蔡庆华
(安庆师范学院 计算机与信息学院,安徽 安庆 246011)

摘 要:代理签名让原始签名者可以将其数字签名权力委托给代理签名者,使其能够代理原始签名者签发指定的数字消息;盲签名使用户能将给定的消息让别人签发,而又不泄漏任何有关的信息给签名者。文中结合两者的优点,利用基于椭圆曲线上的Weil配对的双线性映射,构造了一个基于双线性对的代理盲签名方案,并对其安全性进行了分析。

关键词:双线性映射;Weil配对;代理签名;盲签名
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2006)11-0166-02

A Proxy Blind Signature Scheme Based on Bilinear Pairing

CAI Qing-hua
(College of Computer Science and Information, Anqing Teachers' College, Anqing 246011, China)

Abstract: Proxy signature allows an original signer to delegate his/her signing capability to a proxy signer such that the proxy signer can sign messages on behalf of the original signer. Blind signature allows a user to have a given message signed by the signer without revealing any information about the message. Based on bilinear projection of weil pairing, a proxy blind signature scheme is presented, which satisfies the security properties of both proxy signature scheme and blind signature scheme. A simple security analysis of the newly proposed scheme is also given.

Key words: bilinear paring; weil pairing; proxy signature; blind signature

0 引 言

代理签名[1]适应于经理因事不能亲自签名而将签名权利交由秘书签名的场合。盲签名[2]在电子选举、电子投票中有着广泛应用,它们分别适用于不同场合,都有其各自的优点。在有些情况下,还需要两者同时应用,比如:在匿名电子投票中,A 由于不可避免的原因不能参加选举,他可以将自己的投票权委托给他信任的 B,让 B 实行盲签名。文中利用基于椭圆曲线上的Weil配对(Weil Pairing)的双线性映射,构造了一个代理盲数字签名方案。这个方案继承了代理签名和盲签名的安全性优点。

Bilinear pairings 是代数曲线的 Weil pairing 和 Tate pairing,是构造基于身份的加密方案的重要工具[3]。

假设 G_1 是一个由 P 产生的循环加法群,它的阶是 q,G_2 是一个阶为 q 的循环乘法群,则 Bilinear pairings 是映射 $e: G_1 \times G_1 \to G_2$。假定离散对数问题(DLP问题)在两个群上都是困难的,则 Bilinear pairings 有以下性质:

(1) 双线性:对任意的 P, Q, RG,有 $e(P, Q+R) = e(P,Q)e(P,R)$;$e(P+Q,R) = e(P,R)e(Q,R)$;对任何 $a \in Zq*$,aP 表示 P 自加 a 次,因而对任意的 $a, b \in Zq*$,有 $e(aP, bQ) = e(P,Q)^{ab}$。

(2) 非退化性:存在 $P, Q \in G$,使得 $e(P,Q)$ 不等于1。

(3) 可计算性:对于 $P, Q \in G$,存在一个高效的算法计算 $e(P,Q)$。

设 G 是一个由 P 生成的阶为素数 l 的加法循环群($G = < P >$),假定在 G 上乘法和逆在单位时间内可计算出,且 $a, b, c \in Zq*$。那么有以下4个数学问题:

a. DLP(离散对数问题):给定两个成员 P 和 Q,很难找到一个存在的整数 n,使得 $P = nQ$。

b. CDHP(计算上的 Diffie-Hellman 问题):给出(P, aP, bP),计算 abP 是困难的,不存在多项式时间算法。

c. DDHP(决定性的 Diffie-Hellman 问题):给出(P, aP, bP, cP),能够判断在 $Zq*$ 上 $c = ab$ 是否成立。

d. GDHP:在素数阶循环群 G 上,DDHP 在多项式时间内能被解决,但没有任何可能的算法可以解决 CDHP。

在素数阶循环群 G 上,DDHP 在多项式时间内能被解决,但没有任何可能的算法可以解决 CDHP,称 G 为 GDH 群。这样的群在有限域上的椭圆曲线上能够获得,下面的签名方案就是基于此类 GDH 群。

1 基于双线性对的数字签名

1.1 基本方案

1)系统初始化。

收稿日期:2006-02-22
基金项目:安徽省教育厅自然科学研究项目(2005KJ365zc)
作者简介:蔡庆华(1974-),男,安徽太湖人,讲师,硕士,研究方向为计算机网络与信息安全。

设 G_1,G_2 分别是阶为 q 的加法群和乘法群,其中 q 是素数,在 G_1,G_2 中离散对数问题都是难解的。设 e 是由椭圆曲线上的Weil配对派生得到的一 $G_1 * G_1$ 到 G_2 的双线性映射,$H:\{0,1\}^* \rightarrow G_1$,是一公开的单向加密Hash函数。

2) 密钥生成。

用户 A 随机选取一个整数 x 作为密钥,$x \in Zq*$,计算公开点 $Y = xP$,并将其作为公钥。

3) 签名生成。

对于消息 m,签名者计算:$S = xH(m)$,S 即为消息 m 的签名。

4) 签名验证。

消息接收方接收到明文签名文对(m,S)后,验证下式是否成立:

$e(S,P) = e(H(m),Y)$,若成立,则签名正确,否则签名不正确。

1.2 方案分析

正确性分析:$e(S,P) = e(xH(m),P) = e(H(m),xP) = e(H(m),Y)$

安全性分析:若假设 CDHP 是困难的,该体制已在随机预言模式下被证明对抗任意选择明文攻击是安全的[4]。

2 基于双线性对的代理盲签名方案

设 G_1 为有限域 Fq 上的椭圆曲线有理点群的一个加法子群,P 是 G_1 的生成员;G_2 取这个有限域上的一个乘法子群,双线性映射 e 是由椭圆曲线上 Weil 配对派生得到,H_1,H_2 是单向 Hash 函数,其中 $H_1:\{0,1\}^* \rightarrow G_1$,$H_2:\{0,1\}^* \times G_2 \rightarrow Fq$,原始签名人和代理签名人私钥分别为 x_a 和 x_b,其公钥分别为 $Y_a = x_aP$ 和 $Y_b = x_bP$。

2.1 代理密钥生成

第一步:原始签名人确定授权证书 m_w,在 m_w 中确定代理的诸多事宜,随机选择 $t \in Zq*$,计算 $T = tP$,$h = H_2(m_w,T)$,$Q = H_1(m_w)$ 并计算 $V = (t + hx_a)Q$,$s = (ht + x_a)$,则原始签名人对 m_w 的签名为 $\delta = (T,V)$,然后原始签名人将(δ,s)和 m_w 秘密地发送给代理签名人。

第二步:代理签名人验证证书 m_w 的合法性,即检验下列方程是否成立。

$e(P,V) = e(T + hY_a, H_1(m_w))$

$sP = hT + Y_a$

当且仅当上面等式成立时接受(δ,s),若(δ,s)有效,代理签名人计算出 $x = s + x_b$,作为自己的代理秘密。

2.2 代理盲签名生成

代理签名人 B 给 R 的消息 m 用代理密钥 x 生成代理数字签名,其过程如下:

代理签名人 B 选择 $P_2 \in G_1$,计算:$r_B = e(P_2,P)$,并传给 R;

R 选取 $P_3 \in G_1$,$k \in Zq*$,收到 r_B 后计算:$r = r_B^k e(P_3,P)$,$V = H_2(m,r)$,$V' = V/k$,将 V' 传给 B;

B 计算 $U_B = V'x + P_2$,并将 U_B 送给 R;

R 计算:$U = kU_B + P_3$,则得到对消息 m 的 B 代理 A 的盲数字签名为(U,r,V)。

2.3 代理盲签名验证

签名接收人 R 可用下列等式验证:$e(U,P) = e(H_2(m,r),H_2(m_w,T)T + Y_a + Y_b)r$,如果成立,接收人就可接收签名,否则拒绝此签名。

3 方案分析

3.1 正确性分析

如果方案中的每一方都遵循此协议,则验证等式成立。证明:$e(U,P) = e(kU_B + P_3,P) = e(kV'x + kP_2 + P_3,P) = e(kV/kx + kP_2 + P_3,P) = e(Vx + kP_2 + P_3,P) = e(H_2(m,r)x + kP_2 + P_3,P) = e(H_2(m,r)x,P)e(kP_2 + P_3,P) = e(H_2(m,r),xP)e(kP_2 + P_3,P) = e(H_2(m,r),xP)r = e(H_2(m,r),(s + x_b)P)r = e(H_2(m,r),sP + x_bP)r = e(H_2(m,r),H_2(m_w,T)T + Y_a + Y_b)r$

3.2 安全性分析

一个代理盲签名应满足以下几个安全性要求[5]:可区分性、不可伪造性、可识别性、不可否认性和盲性。下面说明文中方案同样满足以上要求。

(1)可区分性:这一点很显然,因为有效的代理签名中包含有授权证书 m_w,而且证书 m_w、原始签名人和代理签名人的公钥都要在代理签名的验证过程中出现。

(2) 不可伪造性:若第三方想冒充代理签名人和原始代理人对消息 m 伪造代理签名,但他没有原始签名人对授权证书 m_w 的签名(δ,s),则不可能伪造;另一方面,原始签名人也不能伪造代理签名,因为代理签名人用原始签名人所不知的代理私钥产生代理盲签名。

(3) 可识别性:完整有效的代理签名有原始签名人授权证书 m_w 和公钥及代理签名人公钥,于是任何人都能从验证等式上确定相应代理签名人和原始签名人的身份。

(4) 不可否认性:代理签名人一旦产生了代理盲签名,他将不能否认所产生的代理签名。在验证过程中验证者必须用到代理签名人和原始签名人的公钥,因而他们不能否认自己产生的签名。

(5) 盲性:在签名过程中,B 和 R 之间实行的是交互协议,在交互时,消息并没有发给签名者,所以签名者不知道所签消息是什么。

4 小　结

构造了一个基于双线性对的代理盲签名方案,该方案具有代理签名与盲签名各自独特的优点。当用户的隐私权和代理签名都需要的时候,代理盲签名是很好的选择。因此,本方案特别适用于在要求代理签名并要保证用户消息的私有性场合,如电子支付和电子投票系统。

(下转第 190 页)

库中。以 MS SQL Servers 的数据转换服务从源数据库中抽取和转换数据，送到数据仓库中。在分析系统中采用 Microsoft SQL Server Analysis Services。Analysis Services 用于联机分析处理(OLAP) 和数据挖掘的中间层服务器。在分析服务器中，连接数据仓库作为分析系统的数据源，然后利用维度表和事实表创建共享维度或专用维度，并定义维度的层次关系。在 Analysis Services 中可以在同一个维度表创建多个不同的维度，并且可以在日期型单个字段中根据需要创建不同层次的多个维度。维度定义好后，把维度和事实表结合起来，建立用于决策分析的多维数据模型[10]。

4 结 论

商品房销售数据仓库模型的设计提出了一个基于数据仓库技术的决策分析系统。利用数据仓库进行商品房销售带来的好处是多向的：

第一，地产商可以通过网上直接进行有针对性的市场调研，了解消费者的需求和心态，便于进行分析和定位，把握营销策划的方向。通过各种手段收集的数据库本身也是最好的准客户档案。

第二，有利于为客户提供个性化的售前售后服务。数据库营销利用网络的交互式运作，为供需之间开展双向交流提供了便利。

第三，可以实现远程售楼管理，有利于总部与分部的即时沟通。在促销展示数字化方面，部分房地产企业开始通过先进的数字技术展示楼盘，丰富楼盘广告的表现形式。

总之，在今后的研究中要进一步实现数据挖掘的功能，从数据仓库中寻找出隐含的、潜在的有用信息，进行商品房销售预测、商品房购买分析以及顾客价值分析，从而支持更深层次的分析和决策。

参考文献：

[1] 胡 峰. 运用 CRM 系统提升房地产营销管理绩效[J]. 北京房地产，2005(3)：81－83.

[2] 王 丹. 房地产营销进入网络时代[N/OL]. 2005－04－19. http://www.loushi.com/.

[3] Han Jiawei, Kamber M. 数据挖掘：概念与技术[M]. 北京：机械工业出版社，2001.

[4] 陈京民. 数据仓库原理设计与应用[M]. 北京：中国水利水电出版社，2004.

[5] 林杰斌. 数据挖掘与 OLAP 理论与务实[M]. 北京：清华大学出版社，2004.

[6] 贺广生，蔡 勇. 基于数据仓库的销售分析系统的设计和实现[J]. 江南大学学报，2002(2)：143－146.

[7] 张 格，张子刚. 给予系统观念的房地产营销策略研究[J]. 房地产营销，2005(1)：143－146.

[8] 卜一德. 房地产开发经营管理实用手册[M]. 北京：中国建筑工业出版社，2002.

[9] 戴 彬，余建桥. 数据仓库技术在农产品销售中的应用及分析[J]. 农业网络信息，2005(7)：37－39.

[10] 任锦鸾. 数据仓库中数据结构设计方法的研究[J]. 计算机工程与应用，2001(22)：116－118.

(上接第 167 页)

参考文献：

[1] Mambo M, Usuda K, Okamoto E. Proxy Signature for Delegating Signing[C]// In Proc 3rd ACM Conference on Computer and Communications Security. New Delhi, India, New York: ACM Press, 1996.

[2] Chaum D. Blind signature systems[C]// Proceedings of the Crypto 83. New York: Springer－Verlag, 1998：153－156.

[3] Bonch D, Lynn B, Shacham H. Short signatures from the Weil pairing[C]// In: Advances in Cryptology－ Asiacrypt' 2001, Lecture Notes in Computer Science 2248. Heidelberg: Springer, 2002：514－532.

[4] 马春波，何大可. 基于双线性映射的卡梅隆门限签名方案[J]. 计算机研究与发展，2005，42(8)：1427－1430.

[5] 李素娟. 一种基于身份的代理盲签名[J]. 南京工业大学学报，2005，27(3)：107－110.

(上接第 187 页)

参考文献：

[1] 张延松，薛永生，张 宇，等. 数据网格的动态读/写复制策略的研究[J]. 计算机科学，2004(10)：104－107.

[2] Ranganathan K, Iamnitchi A, Foster I. Improving Data Availability through Dynamic Model－Driven Replication in Large Peer－to－Peer Communities[C]//In: Proc of the Workshop on Global and Peer－to－Peer Computing on Large Scale Distributed Systems. Berlin: IEEE Computer Society, 2002.

[3] 何炎祥，范清风，张力飞. 网格计算中动态复制策略的设计[J]. 计算机工程，2004(3)：94－98.

[4] 周 旭，卢显良，侯孟书，等. 频率自适应的动态副本管理机制[J]. 计算机科学，2005(2)：133－136.

[5] 庞丽萍，陈 勇. 网格环境下数据副本创建策略[J]. 计算机工程与科学，2005(2)：1－3.

[6] Lee Byoung－Dai, Weissman J B. An Adaptive Service Grid Architecture Using Dynamic Replica Management[C]//Proc of the 2nd Int'l Workshop on Grid Computing. Denver, Colorado: [s.n.], 2001：63－74.

[7] Lamehamedi H. Data Replication Strategies in Grid Environments[EB/OL]. 2002－07. http://www.cs.rpi.edu/~szymansk/papers/ica3pp.02.pdf.