DOI:10.16707/j.cnki.fjpc.2015.02.041

一种基于组合公钥密码的盲签名

刘 涤
(武汉商学院 湖北 武汉 430058)

【摘 要】组合公钥密码技术是我国自主研发的一种新的认证技术,其核心算法是基于椭圆曲线离散对数求解难题构建而成,实现了将标识作为公钥的标识认证,解决了密钥管理规模化的问题。本文将探讨一种基于组合公钥密码技术的盲签名。

【关键词】数字签名 组合公钥密码 盲签名

1、引言

数字签名是对传统文件中的手写签名的一种数字模拟,在某些场合中能够代替手写签名,具有保证数据的完整性、机密性、安全性和不可否认性的功用。盲签名是一种特殊的数字签名,这种签名要求签名人能够在不知道签名文件内容的情况下对文件进行签名,就像是个里面装有复写纸的信封交给签名人签名,签名人只用在信封上签字就可以把签名通过复写纸签在信封中的文件上。另外,即使签名人以后看到被他签名的文件,也不能判断出这个签名是他何时为何人所签生成的[1]。盲签名在电子投票领域、电子现金系统、电子政务领域中有着广泛的应用。盲签名是 1982 年由 D.chaum 首次提出,随后,人们根据数字签名的发展,基于大素数因子分解问题,离散对数问题,二次剩余问题等先后提出了各种盲签名方案,推动了盲签名技术向前发展。1999 年,南湘浩教授提出了组合公钥技术,2005 年公布,2006 年获得国家专利[2]。组合公钥技术是我国自主研发的一种新的认证技术,与目前正在使用的 PKI、IBE 等认证技术并称为三大认证技术。组合公钥技术不需要可信第三方的在线认证,在椭圆曲线的基础上实现了将标识作为公钥的标识认证,解决了密钥管理规模化的问题。本文将探讨一种基于组合公钥密码技术的盲签名。

2、组合公钥算法原理

组合公钥(Combined Public Key)算法是基于椭圆曲线的离散对数难题构建公钥矩阵和私钥矩阵,将实体标识映射为矩阵的行坐标与列坐标序列,用以对矩阵元素进行选取与组合,生成公钥和私钥对。本文采用椭圆曲线离散对数问题构建组合公钥体制,并以有限域 $E_P(a、b)$(p 不等于 2 和 3 的素数)上椭圆曲线群说明该密钥管理算法的构建方法和原理[3]。

⑴ 初始化:选定椭圆曲线密码参数 $T=(a,b,G,n,p)$,设私钥矩阵和公钥矩阵为 $m\times h$ 阶矩阵。私钥矩阵 SKK 中的元素 r_{ij} 与对应椭圆曲线上的点 $r_{ij}G$ 即为公钥矩阵 PSK 中的对应元素。

$$SSK=\begin{bmatrix} r_{11} & r_{12} & r_{13}\cdots r_{1h} \\ r_{21} & r_{22} & r_{23}\cdots r_{2h} \\ \vdots & \vdots & \vdots \quad \vdots \\ r_{m1} & r_{m2} & r_{m3}\cdots r_{mh} \end{bmatrix}$$

$$PSK=\begin{bmatrix} R_{11} & R_{12} & R_{13}\cdots R_{1h} \\ R_{21} & R_{22} & R_{23}\cdots R_{2h} \\ \vdots & \vdots & \vdots \quad \vdots \\ R_{m1} & R_{m2} & R_{m3}\cdots R_{mh} \end{bmatrix}=\begin{bmatrix} r_{11}G & r_{12}G & r_{13}G\cdots r_{1h}G \\ r_{21}G & r_{22}G & r_{23}G\cdots r_{2h}G \\ \vdots & \vdots & \vdots \quad \vdots \\ r_{m1}G & r_{m2}G & r_{m3}G\cdots r_{mh}G \end{bmatrix}$$

⑵ 基于标识的组合密钥的生成

CPK 基于标识的密钥生成与分发采用了包括对标识的 Hash 运算,行映射算法和列置换算法[4]。

设行映射算法生成的行坐标序列为 $(i_0,i_1,i_2,\cdots,i_{h-1})$,它是一个模 m 的随机数列;设列置换算法生成的列为 $(j_0,j_1,\cdots,j_{h-1})$,它是一个 h 元置换。据此,可得到私钥

$$SK=(r_{i_0j_0}+r_{i_1j_1}+\cdots+r_{i_{h-1}j_{h-1}})\bmod n$$

公钥 PK=

$$\begin{aligned} &r_{i_0j_0}G+r_{i_1j_1}G+\cdots+r_{i_{h-1}j_{h-1}}G \\ &=(r_{i_0j_0}+r_{i_1j_1}+\cdots+r_{i_{h-1}j_{h-1}})G \\ &=SK\cdot G \end{aligned}$$

3、盲签名的安全性要求

盲签名先由消息拥有者将消息盲化,再将盲化后的消息发给签名者,签名者签名后将消息发给消息拥有者。消息拥有者将签了名的盲消息去除盲因子从而得到签名者原消息签名。

设 Alice 为消息拥有者,Bob 为签名者。

① Alice 将原消息 m 用一个随机因子盲化得到盲消息 m′,然后将盲消息 m′传给 Bob。

② Bob 对盲消息 m′用自己的私钥签名,然后将签名 sig(m′)传给 Alice。

③ Alice 将盲签名 sig(m′)去除盲化因子,得到关于原消息 m 的签名 sig(m)。

4、一种基于组合公钥密码的盲签名

根据已经公布的椭圆曲线的数字签名和前面所述的组合公钥算法原理,本文提出一种基于 CPK 的盲签名方案。

⑴ 初始化:设消息拥有者 Alice 的身份标识为 ID_A,签名者 Bob 的身份标识为 ID_B,由注册中心为两个用户分别生成组合密钥对 (d_A,P_A),(d_B,P_B) 通过存储介质发给 Alice 和 Bob。

⑵ 盲化:用户 Alice 先将消息 m 取 Hash 值得到 Hash(m)。Alice 选择一个随机数或伪随机数 δ,使得 $0<\delta<n$,并计算 $\delta G=(x',y')$,$\xi=x'\bmod n$。如果 $\xi=0$ 则重新计算。盲化后消息为 $m'=H(m)+\xi\cdot G$,Alice 将盲签名 m′发给用户 B。

⑶ 签名:用户 Bob 作如下步骤:

①选择一个随机或伪随机数 k,使得 $0<k<n$;

②计算 $kG=(x_1,y_1)$;

③计算 $r=x_1\bmod n$,如果 $r=0$ 则回到第①步;

④计算签名 $sig(m')=r(k+d_B(H(m)+\xi\cdot G))\bmod n$;

⑤发送 $(r,Sig(m'))$ 给 Alice。

基金项目:武汉商学院校级青年项目基金,课题编号:2013Q012

⑷ 去盲：Alice 收到 (r,Sig (m′)) 后，计算

$$\begin{aligned}Sig(m) &= Sig(m') - rP_B \cdot \xi \\ &= r\big(k + d_B(H(m) + \xi G)\big) - rP_B\xi \\ &= r\big(k + d_B H(m)\big) + rd_B\xi G - rP_B\xi \\ &= r\big(k + d_B H(m)\big) + rd_B G\xi - rP_B\xi \\ &= r\big(k + d_B H(m)\big) + rP_B\xi - rP_B\xi \\ &= r\big(k + d_B H(m)\big)\mathrm{mod}n\end{aligned}$$

⑸ 验证：Alice 计算 r^{-1} Sig (m) G−H (m) $P_B=(x_2,y_2)$，计算 $v=x_2 \mathrm{mod}n$，如果 v=r 则接受签名，如果 $v\neq r$ 则拒绝接受签名。

验证过程：

$$\begin{aligned}&r^{-1}Sig(m)G - H(m)P_B \\ &= r^{-1}r(k + d_B H(m))G - H(m)P_B \\ &= kG + d_B H(m)G - H(m)P_B \\ &= kG + P_B H(m) - H(m)P_B \\ &= kG \\ &= (x_2,\ y_2)\end{aligned}$$

5、安全性分析

该方案是基于组合公钥密码技术和椭圆曲线离散对数问题[5]构成的，具有椭圆曲线密码和组合公钥密码的安全性。

⑴ 机密性：攻击者截获盲签名 sig (m′)，因为不知道签名者私钥，所以不能恢复消息 m。

⑵ 签名私钥的安全性：攻击者截获数据 (r,sig (m′)) 后，试图获取签名者私钥是非常困难的。因为签名方程中含有攻击者未知的消息密钥 ξ,k，如果想从 $kG=(x_1,y_1)$，$\delta G=(x',y')$，$\xi=x' \mathrm{mod}n$ 中求出 ξ,k，则会遇到求解椭圆曲线离散对数的难题，是十分困难的。

⑶ 盲性：因为消息拥有者用盲化因子 ξ 将消息盲化，所以签名者不知道消息的具体内容。

⑷ 不可否认性：由于在盲签名过程中使用了签名者的私钥 d_B，而私钥 d_B 只有 Bob 签名者拥有，所以签名人不能否认自己产生的签名。

⑸ 不可伪造性：盲签名是否由签名者产生，Alice 只用计算 r^{-1} Sig (m) G−H (m) $P_B=kG=(x_2,y_2)$，并计算 $v=x_2 \mathrm{mod}n$，判断 v 是否等于 r，若相等则可证明是由 Bob 产生；若不相等，则说明签名被伪造或篡改，不可接受。

6、结束语

本文将组合公钥密码技术应用到盲签名中，采用了组合公钥密码技术是基于椭圆曲线离散对数难题的优势，提出了一种新的盲签名方案。该方案具有机密性，盲性，不可否认性，不可伪造性，保障了盲签名的安全性。该方案计算过程不复杂，可提高签名的效率。

参考文献：

[1] 杨义先，钮心忻.应用密码学 [M] .北京邮电大学出版社，2006.
[2] 李雪. 标识认证打开信息安全新天地——走进南相浩教授的 CPK 世界 [J] .信息安全与通信保密，2006(9) :9 - 11.
[3] 邓文，邓辉舫，田文春，郑东曦.组合公钥标识认证系统的设计及密钥生成的实现 [J] .计算机应用，2007(8):1939 - 1941.
[4] 陈华平，关志.关于 CPK 若干问题的说明 [J] .信息安全与通信保密，2007(9) :47 - 49.
[5] 攸安.椭圆曲线密码体系研究 [M] .华中科技大学出版社，2006 (10) : 22 - 55.

作者简介：

刘涤：1980 年 10 月出生，女、湖北黄石人，研究生学历，研究方向为信息与编码。现为武汉商学院信息工程系讲师。

(上接第 125 页)

校外实训的一个重要功能就是检验教学成果，找出教学过程中存在的问题与不足，为教学改革提供重要依据。中职本科是四年制，而且大部分在中职的时候有了一定的专业基础，大一大二的时候是巩固基础知识，提高专业技能。大三或大四则是应偏重校外的顶岗实习。让学生对自己的能力和素质有一个全面的认识，并且有充分的时间去完善和提升自己。

实习的过程，就是一次了解自己的过程，也是人格完善的过程。了解自己的思想，自己的学习，自己的人际交往的能力，从开始的浮燥到心态的稳定，学会服从，学会收敛，学会遵守规则。

三、提高教师能力素质，改进教学方法

教师是对学生进行培养教育的主体，教师能力和素质的提高直接影响到人才培养的效果。鼓励教师进行教学改革，中职本科学生自主学习能力差，学习兴趣不足，如果按照常规的四年制本科教学方式学生及易产生厌学情绪，教师在教学过程中，应多采用项目教学法。要求教师即要有雄厚的文化知识，又要掌握专业技术，还要讲究教学方法，不但能做学生的老师、还要做学生的朋友、师傅。

四、总结

计算机专业是一个实用、实践性很强的专业，而就业是人才培养的最终目标，是学以致用的根本所在。所以中职本科学校需要改变原有的专业教学模式，以市场用人机制为导向，以就业为最终目的，深化教学改革，建立学生实践学习基地，从而更有效的提高学生技能水平，适应就业的需要。

参考文献：

[1] 顾荣．基于校企合作的计算机应用专业人才培养模式研究 [J] ．福建电脑，2010 (4)
[2] 孟学英，石忠，吴树罡．高职学院产学研结合的内涵与实质探析 [J] .滨洲职业学院学报，2006，(2).
[3] 李学勇，王鑫，谭义红．《应用型本科院校信息与计算科学专业人才培养模式》[J] 长沙大学学报，2009
[4] 顾可民．《计算机专业实用型人才培养模式的研究与实践》[J] ．辽宁教育研究，2007