文章编号:1671 - 6833(2012)02 - 0117 - 05

ECC 有序多重签名方案在电力调度系统中的应用

樊爱宛[1], 常 强[2], 鲁书喜[1], 任童童[1]

(1. 平顶山学院 计算机科学与技术学院,河南 平顶山 467002; 2. 贵州电网公司 遵义供电局,贵州 遵义 563002)

摘 要: 针对 RSA 数字签名在电力调度系统应用时执行速度慢和数据存储量大的局限性,设计基于电力调度系统的 ECC 有序多重数字签名方案. 设计方案将调度签名者的身份与调度文件进行哈希函数处理,防止身份替换攻击,保证了消息的完整性;数字签名过程避开逆运算,能够降低时间复杂度;每个调度签名者签名的结果回送给签名中心,防止联合欺骗,保证了合法操作票的可验证性;能够解决电力调度系统的安全性问题. 应用测试表明:该方案签名及验证过程消耗的时间较短,而且具有较小的通信量,能够满足电力调度的实时性要求.

关键词: ECC;有序多重数字签名;电力调度;安全性;实时性

中图分类号: TM711 **文献标志码**: A doi:10.3969/j.issn.1671 - 6833.2012.02.028

0 引言

电力调度审批流程是多个调度员在同一份操作票上进行有序签名,已经涉及到有序多重数字签名技术[1]. 现有的电力调度系统的有序多重数字签名多是以 RSA 数字签名为主[2]. 在相同的安全强度下,椭圆曲线密码(Elliptic Curve Cryptosystem,ECC)[3]的密钥长度或数字签名的长度远小于 RSA,因此在增快执行速度或节省空间方面,ECC 明显要优于 RSA[4-5]. 目前,ECC 有序多重数字签名在电力调度中的应用研究很少. 笔者对电力调度安全性分析后,设计了一个 ECC 有序多重数字签名在电力调度系统中的应用方案,该方案具有抗否认性、抗伪造性、签名整体的可验证性等特点,能够较好的解决电力调度系统的安全性问题,并满足调度系统实时性的要求.

1 电力调度系统安全性研究

电力调度系统安全审批的具体流程见图 1. 利用调度操作平台,由发电调度员提出操作票申请,通过信任中心认证后,获取操作票,在签名后,转发给输电调度员,输电调度员审核签名后,转发给总值调度员,总值调度员审核签名后,交给信任中心审核是否所有人员签名后,方可进入已审综合令库,然后才能出票调度.

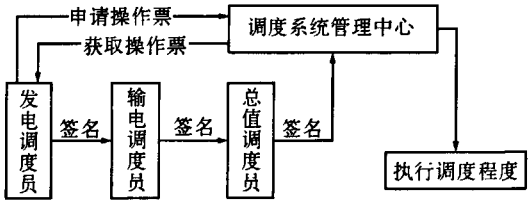

图 1 电力调度系统安全审批流程图

Fig. 1 Flow chart of security approval of electrical dispatching system

在网络化审批过程中,一般需要解决操作票合法性的验证性、操作票内容的抗否认性,操作票发送者身份的可识别性、操作票的完整性和数字签名的抗伪造性等问题.

2 基于电力调度系统的 ECC 有序多重签名

2.1 系统初始化及密钥的生成

2.1.1 签名顺序初始化

假设电力调度系统有 z 个调度员 $u_1, u_2, \cdots, u_z$,按顺序对同一操作票 m 进行签名. 调度系统设置一个签名中心. 为防止冒充签名者伪造签名,由签名中心为每位签名者产生唯一的身份 ID,并将事先安排的签名顺序 $\{ID_1, ID_2, \cdots, ID_Z\}$ 传给每个调度员.

收稿日期:2011 - 10 - 24;修订日期:2011 - 12 - 27

攻关项目:河南省科技计划重点项目(102102210416)

作者简介:樊爱宛(1978 -),男,河南内乡人,平顶山学院讲师,主要从事网络安全研究,E-mail: faw@pdsu.edu.cn.

2.1.2 ECC 初始化

选择有限域 F_q,椭圆曲线参数 $D=\{q, FR, a, b, G, n, h\}$. 其中 q 是所选有限域的阶;FR 是域中元素的表示;$a, b \in F_q$,是定义了椭圆曲线 E 上的两个系数,即 $y^2=x^3+ax+b$;$G \in E(F_q)$ 是椭圆曲线的一个基点;n 是 G 的阶数;h 是辅因子,标识椭圆曲线 E 能够构成子群的个数.

每个调度签名者选择个人私钥 d_i,其中 $i \in [0,z]$;计算 $Q_i = d_i \cdot G$,作为公钥,其中 $i \in [0,z]$.

签名中心选取 d_{CA}作为其私钥,并计算 $Q_{CA} = d_{CA} \cdot G$ 作为其公钥.

所有签名者的公钥由签名中心存储. 每个调度签名者可以从签名中心获取其他调度签名者的公钥.

定义 H 是一个单向安全的 HASH 函数,能够保证数据的完整性和真实性.

2.2 操作票审核的过程

u_1 为了能够得到电力调度的权限,向签名中心提出调度权限申请. 具体步骤如下:

(1) u_1 产生操作票 m. m 含有调度时间、调度内容、调度地点和调度申请人身份 ID 等重要信息;

(2) 为防止非法者冒充 u_1 提交操作票,u_1 对操作票 m 进行签名;

(3) 将 u_1 的签名和操作票 m 通过秘密通道发送给签名中心;

(4) 签名中心得到签名和 m,进行签名验证. 若验证未通过,或者验证通过但是签名中心不允许电力调度操作,则产生警告消息回传给 u_1,然后转入(9),否则转入(5);

(5) 签名中心产生操作票令牌 *Token*. 在每个电力签名者签名前,都需要审核操作令牌 *Token*,以保证操作票的合法性;

(6) 签名中心为操作票产生调度签名时效 *Time*. 要求用户在给定的时间 *Time* 内签名,以防止签名重播;

(7) 签名中心发送 *Token* 和 *Time* 给 u_1;

(8) u_1 验证 *Token* 和 *Time*;

(9) 完成.

在上面步骤中,签名中心产生操作票令牌 *Token*,采用签名中心对操作票 m 和签名时效 *Time* 的签名方式实现. 具体算法如下:

(1) 签名中心随机产生整数 $k(0<k<n)$;

(2) $(x,y)=k \cdot G; r=x \bmod n$;

(3) $hash=\mathrm{H}(m \parallel Time) \bmod n$,其中 $\parallel$ 为连接符号;

(4) $S_{CA}=(k+(r+hash)d_{CA}) \bmod n$;

(5) $Token=(S_{CA}, r)$.

调度签名者在收到 *Token*, m, *Time* 后,对 *Token* 的验证算法如下:

(1) $hash'=\mathrm{H}(m \parallel Time) \bmod n$;

(2) $(x',y')=S_{CA} \cdot G-(r+hash')Q_{CA}$;

(3) 判断 $r=x' \bmod n$ 是否成立. 如果成立,则 *Token* 验证通过,否则失败.

Token 验证产生与验证算法有效性的验证如下:

$$
\begin{aligned}
&(x',y')=S_{CA} \cdot G-(r+hash')Q_{CA}\\
&=((k+(r+hash)d_{CA}) \bmod n)G-(r+hash')Q_{CA}\\
&=((k+(r+\mathrm{H}(m \parallel Time) \bmod n)d_{CA})G-\\
&\quad (r+\mathrm{H}(m \parallel Time) \bmod n)Q_{CA}\\
&=k \cdot G+(r+\mathrm{H}(m \parallel Time) \bmod n)d_{CA} \cdot G-\\
&\quad (r+\mathrm{H}(m \parallel Time) \bmod n)Q_{CA}\\
&=k \cdot G+(r+\mathrm{H}(m \parallel Time) \bmod n)Q_{CA}-\\
&\quad (r+\mathrm{H}(m \parallel Time) \bmod n)Q_{CA}\\
&=k \cdot G=(x,y).
\end{aligned}
$$

2.3 调度签名的过程

调度签名者 $u_i(i \geqslant 1)$ 收到信息后,在经过一系列信息验证后,进行数字签名,具体步骤如下:

(1) 使用 u_i 的私钥 d_i 对 m 和 ID_i 形成签名 S;

(2) 使用秘密随机数产生秘密坐标值 key_i;

(3) 将 $(S, Token, m, Time)$ 发送给下一个签名者 u_{i+1};

(4) 将 (S, key_i, ID_i) 发送给签名中心备案,以便签名中心验证每个签名者真伪.

u_i 的签名算法如下:

(1) u_i 随机产生整数 $k_i(0<k<n)$;

(2) $(x,y)=k \cdot G, r=x \bmod n$;

(3) $hash=\mathrm{H}(m \parallel Time \parallel ID_i) \bmod n$;

(4) $S_i=(k_i+(r_i+hash)d_i \bmod n$;

(5) $S=(S_i, r_i), key_i=(x,y)$.

2.4 调度签名的验证过程

在方案中,要求每位签名者 $u_i(i \geqslant 2)$ 要对 u_{i-1}的签名进行验证. u_1 的签名验证其实就是对 *Token* 的验证. 下面给出电力调度中的 $u_i(i \geqslant 2)$ 签名的验证具体步骤.

(1) 首先判断签名时间 *Time* 的有效性,如果失效,则签名失败,否则,转入(2);

(2) 判断 *Token* 的有效性,保证操作票及操作票令牌的完整性与真实性. 如果失效,则签名失

败,否则转入(3);

(3) 查看 m,如果不同意调度,则转入(5),否则转入(4);

(4) 对 S 进行数字签名验证;

(5) 完成.

u_i 数字签名验证算法如下:

(1) $hash' = \mathrm{H}(m \parallel Time \parallel ID_{i-1}) \bmod n$;

(2) $(x',y') = S_{i-1} \cdot G - (r_{i-1} + hash')Q_{i-1}$;

(3) 判断 $r_{i-1} = x' \bmod n$ 是否成立. 如果成立,则验证通过,否则失败.

2.5 签名中心的验证

签名中心的验证分为对 u_i 的签名验证和对所有签名者的签名验证. 具体步骤如下:

(1) 判断 $Time$ 的有效性. 如果失效,则签名失败,否则,转入(2);

(2) 判断 m 是否被修改. 如果修改,签名失败,否则转入(3);

(3) 对 u_i 的签名验证,可使用 3.5 中的数字签名验证算法. 由于 u_i 提交的 (S, key_i, ID_i) 中还有身份信息和 m,可以通过 u_i 的公钥判断 u_i 身份是否合法,从而得知 m 的完整性;

(4) 对所有签名者的签名验证.

在签名中心已知每个调度签名者发送过来的 $S = (s_i, r_i)$ 和 ID_i 情况下,计算如下:

$$(x,y) = \sum_{i=1}^{z} key_i = \sum_{i=1}^{z} k_i \cdot G; \quad (1)$$

$$R = x \bmod n; \quad (2)$$

$$SA = (\sum_{i=1}^{z} S_i \bmod n)G; \quad (3)$$

$$SB = \sum_{i=1}^{z} (r_i + \mathrm{H}(m \parallel ID_i))Q_i; \quad (4)$$

$$(x,y) = SA - SB. \quad (5)$$

如果 $R = x \bmod n$ 成立,则多重数字签名通过,否则,验证失败.

签名算法的有效性验证如下:

$$(x,y) = SA - SB = (\sum_{i=1}^{z} S_i \bmod n)G - \sum_{i=1}^{z} (r_i + \mathrm{H}(m \parallel ID_i))Q_i$$

$$= S_1 \cdot G + S_2 \cdot G + \cdots + S_z \cdot G - (r_1 + \mathrm{H}(m \parallel ID_1))Q_1 - (r_2 + \mathrm{H}(m \parallel ID_2))Q_2 - \cdots - (r_z + \mathrm{H}(m \parallel ID_z))Q_z$$

$$= [S_1 \cdot G - (r_1 + \mathrm{H}(m \parallel ID_1))Q_1] + [S_2 \cdot G - (r_2 + \mathrm{H}(m \parallel ID_2))Q_2] + \cdots + [S_z \cdot G - (r_z + \mathrm{H}(m \parallel ID_z))Q_z]$$

$$= k_1 \cdot G + k_2 \cdot G + \cdots + k_z \cdot G$$

$$= \sum_{i=1}^{z} k_i \cdot G = (x',y') = (x,y);$$

$$x' \bmod n = x \bmod n = R.$$

2.6 电力调度信息的加密过程

考虑到电力调度信息的机密性,可以使用 ECC 进行加密和解密处理. 加密处理如下:

(1) u_i 的加密算法:u_i 随机选择整数 k,使 $C_1 = k \cdot G$, $C_2 = m + k \cdot Q_{i+1}$,将 (C_1, C_2) 发送给 u_{i+1};

(2) u_{i+1} 的解密算法:$m = C_2 - d_{i+1} \cdot C_1$.

3 方案安全性分析

上述基于电力调度的有序多重签名方案满足以下安全特性:

(1) 不可伪造性. 在抵抗被动攻击时,既使攻击者知道了签名者 u_i 的公用密钥 Q_i,要解出 u_i 的秘密密钥 d_i,或者是知道了公开的 r_i,要解出 k_i,都相当于解椭圆曲线离散对数问题,这比解大整数因式分解和一般有限域离散对数问题更加困难.

(2) 不可否认性. 签名者向签名中心发送的 (S, key_i, ID_i) 中含有了签名者的身份 ID,具有不可否认性.

(3) 不诚实签名者的可识别性. 由于签名中心根据 (S, key_i, ID_i),可以对每个签名者 u_i 的签名进行验证,因此如果签名组成员中有不诚实者,试图伪造签名,则在签名过程中就会被发现.

(4) 可验证性. 每个签名者都可以对前面的签名进行验证.

(5) 签名的完整性. 签名中心通过对 S_i 的验证对所有利用签名者的身份 ID 生成 S_i,保证签名的完整性.

(6) 消息的机密性. 在签名前,使用 ECC 加密算法保证消息的机密性.

(7) 消息的完整性. 当 u_i 向签名中心提交 (S, key_i, ID_i) 后,签名中心会根据对 S 的签名验证,判断消息的完整性,同时可以得出修改 m 的签名者身份.

(8) 操作票的合法性. 如果签名者存疑,可向签名中心提出仲裁,签名中心比较 $Token'$ 和 $Token$ 是否一致,即得操作票的合法性.

笔者方案与其它方案的安全性比较见表 1.

表1 本文方案与其它方案在安全性上的比较

Tab.1 Comparison of security between this paper scheme and other schemes

签名方案	文献[2]	文献[6]	文献[7]	本文方法
不可伪造性	√	√	√	√
不可否认性	√	√	√	√
不诚实签名者的可识别性				√
可验证性	√	√	√	√
签名的完整性			√	√
消息的机密性				√
消息的完整性				√
操作票的合法性				√

4 执行效率分析

4.1 时间复杂度

ECC的各种运算的时间符号定义和时间复杂度换算关系可按文献[8-9]估算. 其中,相对于t_{MUL},t_{ADD}和t_M可以忽略,$t_{EXP}\approx 240t_{MUL}$,$t_{EC\_MUL}\approx 29t_{MUL}$,$t_{EC\_ADD}\approx 0.12t_{MUL}$,$t_H\approx 0.23t_{MUL}$,$t_I\approx 11.6t_{MUL}$.

(1) 操作票审核. 签名中心签名时间为:$t_{EC\_MUL}+t_M+t_H+t_M+t_{ADD}+t_{MUL}+t_{ADD}+t_M\approx 29t_{MUL}+0.23t_{MUL}+t_{MUL}=30.23t_{MUL}$.

操作票申请者验证时间:$t_H+t_{EC\_MUL}+t_{EC\_MUL}+t_{ADD}+t_{EC\_ADD}\approx 58t_{MUL}+0.12t_{MUL}=58.12t_{MUL}$.

(2) 调度签名

$t_{EC\_MUL}+t_M+t_H+t_M+t_{ADD}+t_{MUL}+t_{ADD}+t_M\approx 29t_{MUL}+0.23t_{MUL}+t_{MUL}=30.23t_{MUL}$.

(3) 调度签名的验证

$t_H+t_{EC\_MUL}+t_{EC\_MUL}+t_{ADD}+t_{EC\_ADD}\approx 58t_{MUL}+0.12t_{MUL}=58.12t_{MUL}$.

(4) 签名中心的验证. 假设有z个电力调度签名者,则签名中心验证时间为:$zt_{EC\_ADD}+z(t_H+t_{EC\_ADD}+t_{EC\_MUL})+t_{EC\_ADD}$. 如果调度签名者为3个,则验证时间为:$3t_{EC\_ADD}+3(t_H+t_{EC\_ADD}+t_{EC\_MUL})+t_{EC\_ADD}\approx 88.53t_{MUL}$.

本文方案与其它方案在时间复杂度上的比较见表2. 可以看出,本文方案的计算量明显小于其它方案,具有较高的运行效率.

4.2 通信量

本文方案通信量用调度签名运行中产生的消息数来表示. 在操作票审核过程中,通信双方使用1次交互,2条消息;在调度者审核签名过程使用2条消息,假设有3个调度者参与签名,则整个调度者审核签名使用6条消息. 本文方案使用8条消息,具有较小的通信量.

表2 本文方案与其它方案在时间复杂度上的比较

Tab.2 Comparison of time complexity between this paper scheme and other schemes

数字签名方案	签名	签名的验证	签名中心的验证
文献[2]中的RSA方案	$\geqslant 240t_{MUL}$	$\geqslant 240t_{MUL}$	$\geqslant 240t_{MUL}$
文献[6]方案	$88.23t_{MUL}$	$174t_{MUL}$	$1\,010.592t_{MUL}$
文献[7]方案	$88.23t_{MUL}$	$174t_{MUL}$	-
本文方案	$30.23t_{MUL}$	$58.12t_{MUL}$	$88.53t_{MUL}$

5 应用测试

本文方案在VC6.0环境下进行实现,椭圆曲线q的位数为224位. 针对电力调度命令进行签名和验证,以检验本软件的实用性,整个实验采用Intel酷睿i5-750,4G内存的运行环境,密钥生成过程的平均时间为1 ms,电力调度签名过程消耗的平均时间为9 ms,签名验证过程消耗的平均时间为17 ms,签名中心验证消耗的平均时间为30 ms. 实验表明该系统具有良好的运行效率,能够满足电力调度的实时性要求. 电力调度系统的监测签名的界面如图2示,ECC签名的后台运行过程如图3所示.

图2 电力调度系统的监测签名图

Fig.2 Monitoring and signature of electric power dispatching system

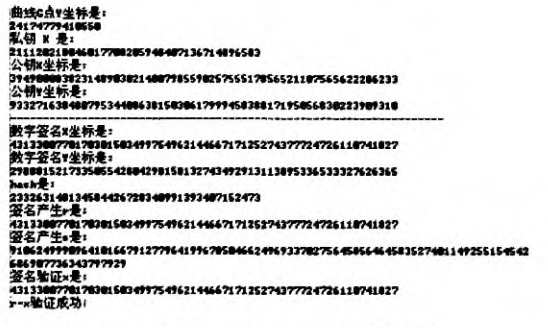

图3 ECC签名后台运行过程图

Fig.3 Chart of ECC signature backstage running process

6 结束语

笔者设计了ECC有序多重数字签名在电力调度中的应用方案,方案满足抗否认性、抗伪造

性、签名整体的可验证性等安全特性.与同类方案相比,克服了消息采用明文传送带来的安全隐患,能够保证消息的完整性,可以对操作票合法性进行验证.方案的计算量优于同类方案,具有较高的运行效率,较小通信量的特点.方案的应用测试表明能够满足电力调度的实时性要求.但是方案是以信任的签名中心为研究前提,没有考虑到签名中心的作弊行为,如何设计基于电力调度系统无认证的有序多重签名是下一步的研究方向.

参考文献:

[1] 徐俊杰,赵京虎.基于 SCADA 系统的地区电网调度操作票系统的设计[J].电力系统保护与控制,2010,38(13):104 - 107.

[2] 陈瑞,叶核亚.B/S 结构的电力调度信息管理系统中的数字签名[J].网络安全技术与应用,2006,5(9):50 - 52.

[3] 耿永军,闫洪亮.一种基于 DSA 变体的盲签名方案[J].郑州大学学报:工学版,2006,27(3):101 - 103.

[4] 李欣妍,芦殿军.基于椭圆曲线密码体制的代理多重盲签名[J].计算机工程与科学,2010,32(11):58 - 59.

[5] 史开泉,陈泽雄,电力系统加密通信与通信认证问题[J].中国电机工程学报,2002,22(10):34 - 38.

[6] 施荣华,胡芳.一种基于椭圆曲线的有序多重数字签名方案[J].计算机工程与应用,2006,27(25):152 - 155.

[7] 刘振,申凯,余昭平.有效的有序多重数字签名方案[J].计算机工程与设计,2008,29(1):28 - 33.

[8] COURTOI N, KLIMOV A, PATARIN J. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations [C]. Berlin, Germany: Springer-Verlag, 2000:392 - 407.

[9] KIPNIS A, SHAMIA A. Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization[C]. Berlin, Germany: Springer-Verlag, 1999:19 - 30.

Research on Application of ECC Sequential Multiple Signature Scheme in Electrical Dispatching System

FAN Ai-wan[1], CHANG Qiang[2], LU Shu-xi[1], REN Tong-tong[1]

(1. Department of Computer Science and Technology, Pingdingshan College, Pingdingshan 467002, China; 2. Zunyi Power Supply Bureau, Guizhou Power Grid Corporation, Zunyi 563002, China)

Abstract: The ECC sequential multiple digital signature scheme is designed based on electrical dispatching system, in view of the limitation of low execution speed and great size of memory of RSA in electrical dispatching system. The scheme will process the identity of signer and the dispatching documents by hash function, avoid the attack of alternative identity and ensure the integrity of information; the digital signature process avoids the inverse operation, and lowers the complication of time; the signing result of each dispatching signer will be sent to the signature center, avoid joint cheating and ensure the verifiability of valid ticket, and the security of electrical dispatching system is then solved. The application test indicates that the duration of signature and verification of the scheme is short, with relatively small communication and the requirement of real-time for power dispatching is satisfied.

Key words: ECC; sequential multiple digital signature; electric dispatching; security; real-time