

湖南电网发电竞价信息加密系统的开发

姚建刚¹, 罗滇生¹, 陈 亮¹, 银车来², 付维生², 陈庆祺²

(1. 湖南大学电气与信息工程学院, 长沙 410082; 2. 湖南电力调度通信中心, 长沙 410007)

摘要: 实行发电竞价上网是实现电力市场化的重要举措和必经步骤。文中根据电力市场条件下发电竞价的特点和信息发布对加密技术的要求, 将电子商务信息技术应用于发电竞价系统。采用 1024 bit 公开密钥算法 RSA, 形成了完整的加密、解密、身份验证和证据保全等技术手段, 为保证发电竞价上网的“公正、公平、公开”提供了有力的技术支持。

关键词: 发电竞价; 加密技术; 身份验证

中图分类号: TM 73; TP 309.7

0 引言

促进资源的优化配置、提高效率、降低成本、降低用户电价是发展电力市场的目的^[1]。当今世界的电力工业正朝着打破垄断、鼓励竞争的方向蓬勃发展。从目前来看, 我国的电力工业正处于厂网分开、建立发电侧电力市场的关键时期, 实行发电竞价上网是实现电力市场化的重要举措和必经步骤。

本文作者在承担湖南省发电竞价系统的开发过程中, 将电子商务信息加密技术运用于竞价系统, 从而确保了发电竞价的“公正、公平、公开”。

1 系统功能

发电竞价上网数据申报及信息发布系统(以下简称竞价系统)包含 3 个既可以独立运行、又相互关联的系统: 在各个发电厂(企业)运行的客户端、在省电力调度中心运行的服务端以及为各个发电厂(企业)提供身份认证与密钥生成的认证中心。客户端运行在各个发电厂(企业), 负责将各个电厂的竞价信息经过处理发送到服务端, 接收服务端发布的任何合法信息; 服务端运行在省电力调度中心, 负责接收各个电厂的竞价信息, 自动或人工开标、竞标, 将竞标的结果以及各种运行参数信息在 Internet 上发布; 认证中心负责生成密钥对, 给每个发电厂(企业)提供身份证明, 以及用户数字证书的维护等。各子系统的组成与功能介绍如下。

1.1 客户端

a. 标书处理: 对标书的处理过程要求严格、规范, 包括标书的拟订、审核、批准以及标书上报时进行标书的加密、签署数字签名等。

b. 信息查询: 从 Internet 上查询标书的参数, 如最高电价、最低电价和最高电量等, 以及每次的竞标结果和省电力调度中心公布的各种月报、季报、年报。

c. 系统维护: 设置和维护系统的运行环境, 包括时间与省电力调度中心同步; 形成操作日志, 对可能引起灾难的原因进行分析, 对灾难后果进行恢复等。

d. 用户管理: 包括用户的增加、减少, 以及用户权限的分配等。

1.2 服务端

a. 标书处理: 包括标书的接收、识别和保存。

b. 公开竞标: 将各个电厂的标书解密, 公开进行竞标, 形成竞标结果。

c. 数据处理与信息发布: 数据(各种月报、季报、年报)经过拟订、审核和批准, 可以在 Internet 上发布。

d. 系统维护: 设置和维护系统的运行环境, 协调省电力调度中心与各电厂同步; 形成操作日志, 对可能引起灾难的原因进行分析, 对灾难后果进行恢复; 同步更换各个发电厂的数字证书等。

e. 用户管理: 包括用户的增加、减少以及用户权限的分配等。

1.3 认证中心

认证中心最基本和最核心的作用是审核用户的合法身份, 发放用户的有效数字证书, 其基本功能如下。

a. 认证中心政策制订: 包括对申请证书用户的审核要求及认证中心自身运作的要求等。

b. 认证中心密钥管理: 用于签名用户证书的密钥和其他密钥的产生、更新、备份、恢复等。

c. 用户证书管理: 包括接收用户的证书请求,

审核用户的合法身份,发放用户的有效数字证书,管理用户的证书等。

d. 黑名单管理:包括注销用户的数字证书,定期产生黑名单,发布黑名单。注销证书就是将证书从证书库中移到黑名单申请库中,生成黑名单。

e. 系统维护管理:包括系统运行日志、审计、备份和灾难恢复等。

2 加密过程与加密算法

2.1 公开密钥算法 RSA

竞标系统所得到的结果将直接影响各发电厂(企业)的经济利益。只有规范各个发电厂(企业)的竞价行为,保证电力市场的运作稳定、有序,才能最大限度地体现“公正、公平、公开”的原则。本文采用 RSA 公开密钥算法。

竞标系统采用公开密钥算法。该加密算法 E 和解密算法 D 必须满足 3 点要求^[2]: $D(E(P)) = P$; E 导出 D 极其困难;由一段明文不可能破译出 E 。

此方法的工作过程如下:加密算法 E 和解密算法 D 以及密钥都是公开的,如其名称公开密钥算法,但需将解密密钥保密。如果电厂要传输标书到省电力调度中心,首先用省电力调度中心的加密密钥将标书加密,标书到省电力调度中心后用省电力调度中心的解密密钥解密。由于加密系统非常可靠,其他任何人都无法阅读加密后的标书,且从公开密钥推导出解密密钥非常困难。因此省电力调度中心可以安全地与各发电厂(企业)通信。

公开密钥加密法要求每个使用者都有 2 个密钥:一个公开密钥,供所有人使用,用来加密传送给该用户的信息;另一个秘密密钥,该用户用它来解密信息。我们把这两个密钥分别称为公开密钥和私有密钥。方法运用如下^[3]:①选择 2 个质数 p 和 q (典型地应大于 10^{100});②计算 $n = p \times q$ 和 $z = (p - 1) \times (q - 1)$;③选择一个与 z 互为质数的数 d ;④找出 e ,使得 $e \times d = 1 \bmod z$ 。

有了这些预先计算出的参数,即可准备开始加密。把明文(看做一个 bit 串)划分成块,使各段明文信息 p 满足 $0 \leq p \leq n$ 。把明文分成 k bit 的块即可满足这一要求,其中, k 为满足 $2^k < n$ 的最大整数。

对信息 p 加密,计算 $C = p^e \pmod n$ 。解密 C 要计算 $P = C^d \pmod n$ 。可以证明,对于在指定范围内的所有 P ,加密函数和解密函数互为反函数。实行加密需要 e 和 n ,实施解密需要 d 和 n 。因此,公开密钥由 (e, n) 构成,私有密钥由 (d, n) 构成^[4]。

此算法的安全性建立在难以对大数提取因子的基础上。根据研究,200 位的数分解因子需要 40 亿

年的时间,对 500 位的数分解因子需要 10^{25} 年。我们在竞标系统中使用的是 1 024 bit,具有足够的保密强度。所有使用的密钥对由认证中心生成。

2.2 公开密钥的数字签名

要保证标书的真实性和可靠性,必须由是否存在授权的亲笔签名来确定。发生法律纠纷时,可以此为证据。因此需要设计出一个代替亲笔签名的方案,即需要这样一个系统,各个发电厂(企业)可以通过该系统能以如下方式向省电力调度中心发送自己的签名报文(即所谓的数字签名系统):省电力调度中心能够验证发送方宣称的身份;发电厂(企业)以后不能否认报文是他发送的;省电力调度中心自己不能伪造该报文。

数字签名的方法有很多,在竞标系统中采用公开密钥的数字签名。各个发电厂(企业)传送给省电力调度中心的标书都必须经过加密处理,标书传到省电力调度中心后再解密。整个过程采用公开密钥的数字签名,这种算法既有数字签名的作用,又可实现标书的加密、解密。

首先,由认证中心给每个发电厂(企业)发放数字证书(以下用 D_C 代替),也就是所谓的每个发电厂(企业)的私有密钥,同时每个发电厂(企业)还拥有省电力调度中心的公开密钥(以下用 E_T 代替);而省电力调度中心拥有每个发电厂(企业)的公开密钥(以下用 E_C 代替)和自己的数字证书(私有密钥,以下用 D_T 代替)。 D_C 是每个发电厂(企业)的身份证明,必须妥善保管,不能泄露。

图 1 为使用公开密钥的数字签名的过程。

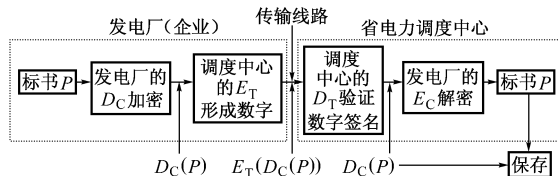


图 1 使用公开密钥的数字签名的过程
Fig. 1 The process of digital signature by using the public secret-key

使用公开密钥的数字签名过程的算法如下:

a. $E_T(D_C(P))$ 在通信线路上传输,有可能被截取或窃听。但窃听者没有调度中心的私钥和各个发电厂(企业)的公钥,则不可能从加密后的标书中得到任何有效信息,也不可能篡改标书内容;而且由于每份标书都加上了时间戳,也不会受到重发攻击的影响,保密的强度非常高,达到了 1 024 bit,因此无法破解。

b. 如果发电厂(企业)否认曾经发送过标书 P 给调度中心,发生纠纷需要法院裁决时,调度中心可

以出示标书 P 和 $D_C(P)$, 法院只需使用 E_C , 就能轻易证明调度中心确实收到了一条用 D_C 加密的有效标书。由于调度中心不知道各个电厂的私有密钥 D_C , 调度中心不可能自己生成这样一条由 D_C 加密的有效标书, 因此只能是由发电厂(企业)发送过来。这样可以得到法律认可的证据。

c. 所有的算法都是公开的。如果需要, 所有的过程都可再现和反复验证, 没有给任何使用者以任何的“后门”, 保证了算法的“公正、公平、公开”。

3 结语

湖南电网发电竞价信息加密系统采用了算法公开的对称密钥数字签名的加密、解密、身份验证和证据保全等技术, 其加密强度达到了世界先进水平。近1年的运行表明, 系统运行稳定, 发布信息及时准确, 安全可靠, 创造了较大的经济效益, 有效地降低了用户电价, 为电力市场的发展提供了有力的支持。

参考文献

- 1 姚建刚, 章建(Yao Jiangang, Zhang Jian). 电力市场分析(Power Market Analysis). 北京: 高等教育出版社(Beijing: Higher Education Press), 1999
- 2 Horng Gwoboa, Yang C S. Key Authentication Scheme for Cryptosystems Based on Discrete Logarithms. Computer Communication, 1996, (19): 848~472
- 3 Shao Zuhua. Signature Scheme Based on Discrete Logarithm Without Using One-Way Hash Function. Electronic Letters, 1998, 34(11): 1079~1080
- 4 ELGamal T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Trans Inform Theory, 1985, 31(4): 469~472

姚建刚, 男, 教授, 系主任, 主要从事电力市场、配电系统自动化和新型输电方式的研究。

罗滇生, 男, 博士, 讲师, 主要从事计算机通信技术与电力市场的研究。

陈亮, 男, 硕士研究生, 主要从事电力市场方面研究。

DEVELOPMENT OF INFORMATION ENCRYPTION SYSTEM FOR HUNAN ELECTRICITY BIDDING MARKET

Yao Jiangang¹, Luo Diansheng¹, Chen Liang¹, Yin Chelai², Fu Weisheng², Chen Qingqi²

(1. Hunan University, Changsha 410082, China)

(2. Hunan Electric Power Dispatching and Communication Center, Changsha 410007, China)

Abstract: The implementing of electricity bidding is an important action during the realization of electricity market. Based on the characteristics of electricity bidding and the demands of encryption techniques, the electronic commercial information technology is introduced into electricity bidding system. The 1024-bit public secret-key arithmetic RSA is adopted in this paper, which forms the integrated techniques of encoding, decoding, ID-checking and evidence-saving from damage. So it provides a powerful technical support for a fair and open electricity bidding market.

Keywords: electricity bidding; encryption technique; ID-checking