基于 RSA 的叛逆者追踪方案的设计与分析

齐亚莉
(北京印刷学院 信息与机电工程学院, 北京 102600)

摘 要: 叛逆者追踪方案是版权保护中的重要工具。基于 RSA 算法的安全性,设计叛逆者追踪方案,数据分发者分别为每个用户进行初始化,使每个用户都具有标志性的用户信息,可准确地追踪到叛逆者。对方案进行分析后得出结论:为保证安全性,需要不断增加密钥长度,但其不可否认性和防诬陷性使该追踪算法的应用受到一定限制。

关键词: 叛逆者;RSA;黑盒测试;可撤销性
中图分类号: TN918.4 **文献标志码**: A
文章编号: 1004-8626(2012)02-0055-02

The Analysis and Design of Traitor Tracing Scheme Based on RSA

QI Ya-li
(School of Information & Mechatronic Engineering, Beijing Institute of Graphic Communication, Beijing 102600, China)

Abstract: Traitor tracing technology is an important measure to data copyright protection. This paper designs a traitor tracing scheme based on RSA, which dispatches special information for every users respectively. The information for one user is the label of him. The scheme has the advantages of tracing traitor and revoking traitor successfully. But it is restrained by non-repudiation and full frameproof to application.

Key words: traitor; RSA; black box testing; revoking traitor

叛逆者指的是恶意的授权用户,为了某种利益,将自己的解密密钥泄漏给未授权用户,或者与别的用户共谋产生一个新的解密密钥。一旦发现这样的盗版解码器,数据发布者或者可信代理就可以利用追踪算法,找出至少一个参与共谋的用户。叛逆者追踪对盗版行为具有一种威慑作用,对保护版权具有重要的意义[1]。

1 RSA 加解密算法

RSA 算法是由 Ron Rivest、AdiShamir 和 Leonard Adleman 共同发明的[2]。RSA 的安全性依赖于大数分解。公钥和私钥都是两个大素数(大于 100 个十进制位)的函数。

密钥对的产生首先选择两个大素数,p 和 q,计算:$M=p\times q$。然后随机选择加密密钥 e,要求 e 和 $(p-1)\times(q-1)$ 互质。最后,利用欧几里得算法计算解密密钥 d,满足 $e\times d=1(\mathrm{mod}(p-1)\times(q-1))$,其中 M 和 d 也要互质。数 e 和 M 是公钥,d 是私钥。

加密信息 m 时,首先把 m 分成等长数据块 $m_1,m_2,\cdots,m_i$,块长 s,其中 $2\wedge s\leqslant n$,s 尽可能的大。对应的密文是:

$$c_i = m_i \wedge e(\mathrm{mod}\ n) \quad (1)$$

解密时作如下计算:

$$m_i = c_i \wedge d(\mathrm{mod}\ n) \quad (2)$$

在图 1 中,选择质数 11 和 7,得出 M 为 60,加密信息为 75,加密后信息为 26。当然,在实际应用中,选择的质数应该尽可能大,据猜测,从一个密钥和密文推断出明文的难度等同于分解两个大素数的积。

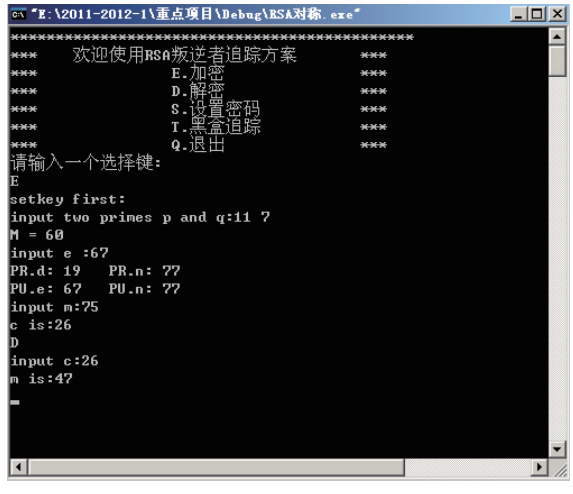

图 1 基于 RSA 的加解密实验

收稿日期: 2011-11-22
基金项目:北京市属高等学校人才强教计划资助项目(PXM2010_014223_095557);北京印刷学院重点项目(Ea2011005)

2 基于 RSA 叛逆者追踪方案的设计

2.1 数据供应商初始化

数据供应商先生成 RSA 模数 $M=pq$,其中 p,q 是两个安全的大素数,满足 $(p-l)/2$ 和 $(q-l)/2$ 都是素数。然后,数据供应商随机选择一个 L 长的向量 $E=\{e_1,e_2,\cdots,e_L\}$ 作为在模 M 下的加密密钥。

最后,数据供应商将参数 L 和 M 公开,将 p,q,$\varphi(M)$,$E=\{e_1,e_2,\cdots,e_L\}$ 秘密保存,其中,$\varphi(M)$ 是欧拉函数。

2.2 用户初始化

当一个用户被加入到授权用户集中,数据供应商按如下方式生成用户的解密密钥并通过安全信道分发给该用户。

1)对于用户 i,随机生成一个 L 维的布尔向量 v^i,向量中的每个元素以概率 α 取值为 1,以 $1-\alpha$ 的概率取值为 0。同时 $\boldsymbol{v}^i$ 中的分量不能全为 0,且没有两个向量是完全相同的。重复选择下去,直到符合条件的 $\boldsymbol{v}^i$ 被找到,它满足 $\sum_{j=1}^{L} v_j^{(i)} e_j$ 与 $\varphi(M)$ 互素。

2) 使用欧几里得扩展算法,计算解密密钥中的解密参数 d_i:

$$d_i = \left(\sum_{j=1}^{L} v_j^{(i)} e_j\right)^{-1} \bmod \varphi(M)$$

如果 d_i 是概率上的素数,则继续执行以下步骤,否则返回步骤 1)。

3)通过安全信道将解密密钥 $DK_i=(v_i,d_i,M)$ 传送给用户 i。

2.3 加密、传输和解密

1)加密。为了把明文消息 P 安全地广播给授权用户,数据供应商用加密密钥 $E=\{e_1,e_2,\cdots,e_L\}$ 中的每一个分量对 P 执行 L 次 RSA 加密运算。加密后得到密文 $C=P^{e_1} \bmod M,\cdots,P^{e_l} \bmod M$。为保证语义安全,在加密之前,对所有的明文消息 P 采用优化的非对称加密填充作预处理。

2)传输。数据供应商把密文 C 广播给所有的用户。

3)解密。收到密文 C 后,授权用户使用其解密密钥 $DK_i=(v_i,d_i,M)$ 解密密文 $P=\left(\prod_{j=1}^{L}(c_j)^{v_j^i}\right)^{di} \bmod M$,其中 $c_j=P^{e_j} \bmod M$。

3 黑盒追踪分析

当没收一个盗版解码器后,数据供应商利用追踪算法来识别参与盗版的叛逆者用户。叛逆者追踪的黑盒追踪算法可识别出全部的叛逆者[3]。在黑盒追踪算法中,采用随机的数据作为密文输入到盗版解码器中来识别叛逆者[4-5]。由于使用每一个授权用户的解密密钥对随机数据解密将产生不同的可以预测的结果,因而,可以识别出叛逆者。假定用户 i 的解密密钥为 $DK_i=(v_i,d_i,M)$,黑盒追踪算法的过程如下。

Step1,随机生成一个含有 L 个分量的向量 $\boldsymbol{c}=\{c_1,c_2,\cdots c_L\}$,$\boldsymbol{c}$ 中每一个分量为$\lceil \log_2 M \rceil$比特长。

Step2,对每一个授权用户 i,执行以下步骤:

1)随机地选择一个整数 z,满足 $v_z^i=1$;

2)构造向量 $\boldsymbol{c}'=\{c_1',c_2',\cdots c_L'\}$,使得当 $j=z$ 时,有 $\boldsymbol{c}'=\boldsymbol{c}$,否则 $\boldsymbol{c}_j'=1$;

3)将 $\boldsymbol{c}'$ 发送给盗版解码器作为输入值观察其输出结果 P';

4)判断如果 $P'=P_{\text{test}}=\left(\prod_{j=1}^{L}(\boldsymbol{c}_j)^{v_j^i}\right)^{di} \bmod M$ 成立,那么用户 i 就是叛逆者。

如果参与盗版行为的用户不超过 k 个,那么,重复执行上述黑盒追踪算法,就可以检测出所有的叛逆者。

4 可撤销性分析

若确定 i 用户是叛逆者,则可以通过改变 L 维长的向量随机向量 $E=\{e_1',e_2',\cdots,e_L'\}$,对于已经发送给用户 i 的 $DK_i=(v_i,d_i,M)$ 来说,等式 $d_i=\left(\sum_{j=1}^{L} v_j^{(i)} e_j'\right)^{-1} \bmod \varphi(M)$ 不再成立,也就是说对于新的产品,即使 i 用户得到新的加密密文,也不会用原来的密钥进行解密。对于叛逆者可以进行有效的授权撤销。

5 结 语

RSA 的安全性依赖于大数的因子分解,RSA 算法的特点是数学原理简单、在工程应用中比较易于实现。通过对每个用户设计独特的解密信息,使得在获得解码器后,可以准确追踪到叛逆者,并对其进行授权撤销。当然,与其他叛逆者追踪方案相比,由于其性能受到大数因子分解的制约,RSA 的速度比同样安全级别的对称密码算法要慢很多倍。随着破译技术的发展,为了保证安全性,要求密钥长度不断增加,随着保密级别的提高,其密钥长度

(下转第 59 页)

件。Proficy Machine Edition 是一个集人机界面、运动和控制应用于一体的通用开发环境,提供一个统一的工作空间和工具集,具有用户友好的结构和标准化的用户界面,支持项目需要的多组件的编辑功能。系统控制程序主要完成以下任务:控制模式的选择与切换,太阳方位信息的采集与处理,监控显示以及步进电机动作的控制等。主程序框图如图 4 所示,系统初始化后,先对硬件进行检测,如果不正常,启动手动控制排除故障;若无故障,系统进行自动控制。控制过程中,实时检测太阳是否达到光强,若是,则程序存储位置信息,并进行比较,进行跟踪控制;若不是,工作模式切换到定时工作模式,利用内部时间,对跟踪装置进行调整控制,待光强达到一定强度时,系统会自动调整为自动光电跟踪控制,实现对太阳能位置的跟踪。

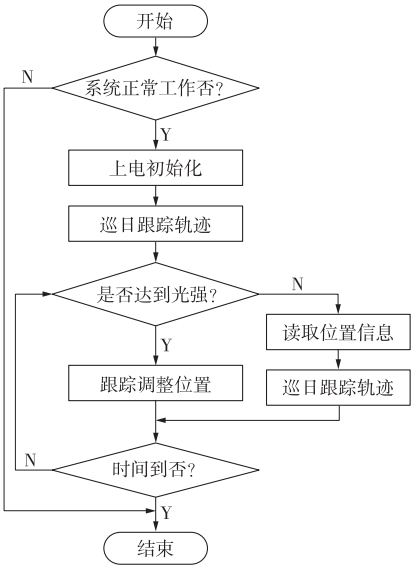

图 4　主程序控制流程

3　实验测试

采用 3 块太阳能电池板安装在跟踪控制系统支架上,用一个强光电筒连续移动模拟太阳光源的变化轨迹,将其中一块太阳能电池板调至最佳倾斜角度固定,另外 2 块太阳能电池板设置成自动跟踪模式,当太阳光照射轨迹变化时,采用跟踪模式的太阳能电池板比固定式安装的太阳能电池板的辐照量增加明显。在模拟天气光照强度良好时,本控制装置可以实现自动跟踪太阳轨迹运行,在光照强度较弱如阴雨天或夜间时进入待机状态,待光照强度良好时,系统能及时自动确定方位,自动跟踪太阳的运行。

4　结　论

本系统设计的双轴太阳跟踪控制系统采用视日运动轨迹跟踪和光电跟踪相结合的跟踪方式,实现了对太阳能电池板的方位角和高度角的实时自动跟踪控制,具有系统结构简单、成本低、可靠性强等特点,既可用于独立的太阳能光伏发电装置设备上,也可用于串并联的大型光伏发电系统的现场总线控制系统。

参考文献:

[1] 赵争鸣,刘建政,孙晓英,等. 太阳能光伏发电及其应用[M]. 北京:科学出版社,2005.

[2] 王淼,王保利,焦翠坪,等. 太阳能跟踪系统设计[J]. 电气技术,2009(8):100-103.

[3] 戴训江,晁勤. 太阳能单轴跟踪系统的 PLC 设计[J]. 可再生能源,2008,26(3):60-62.

[4] 陈向军,潘宇,于荣金. 太阳能自动跟踪系统的研究[J]. 电子技术,2007(9):121-122.

[5] 张兴磊,杨丽丽,张东风. 一种太阳自动跟踪系统的设计[J]. 青岛农业大学学报:自然科学版,2008,26(4):315-318.

[6] 郁汉琪,王华. 可编程自动化控制器(PAC)技术及应用:基础篇[M]. 北京:机械工业出版社,2010.

(责任编辑:邱林华)

(上接第 56 页)

增加非常快。另外,其不可否认性和防诬陷性使得基于 RSA 的叛逆者追踪算法应用受到了一些限制。

参考文献:

[1] ChorB, FiatA, NaorM. Tracing Traitors [C]. Advancesin CryPtology-CRYPTO, 94, LNCS839, SPringer-Verlag, 1994, 257-270.

[2] 马华,曹正文. 基于 RSA 加密算法的叛逆者追踪方案[J]. 西安电子科技大学学报,2004,31(4):611-613.

[3] 马华,杨波. 改进的基于修改 RSA 的叛逆者追踪方案[J]. 西安电子科技大学学报,2006,33(3):422-424.

[4] John Patrick McGregor, Yiqun Lisa Yin, Ruby B. Lee, A Traitor Tracing Scheme Based on RSA for Fast Decryption[C]. ACNS 2005, New York City, LNCS 3531, SPringer-Verlag, 2005:56-74.

[5] 李勇,杨波,华翔. 一种高效非对称的动态公钥叛逆者追踪方案[J]. 西安电子科技大学学报,2003,30(3):394-398.

(责任编辑:邱林华)