第 35 卷 第 9 期 计 算 机 工 程 2009 年 5 月
Vol.35 No.9 Computer Engineering May 2009
·安全技术· 文章编号：1000—3428(2009)09—0174—02 文献标识码：A 中图分类号：N945

基于 AVL 搜索树的证书吊销系统

周海岩，赵建洋
(淮阴工学院计算机工程系，淮安 223001)

摘 要：针对公钥基础设施中的证书吊销问题，提出一种基于 AVL 搜索树的解决方案，该方案在查询与更新时的最大时间复杂度始终保持在 $O(\text{lb}n)$量级。实验结果表明，该方案是有效的，且对工程实现具有一定指导意义。

关键词：公钥基础设施；证书权威；证书吊销；二叉搜索树；AVL 搜索树

Certificate Revocation System Based on AVL Search Tree

ZHOU Hai-yan, ZHAO Jian-yang
(Dept. of Computer Engineering, Huaiyin Institute of Technology, Huai'an 223001)

【Abstract】 Aiming at certificate revocation problem in Public Key Infrastructure(PKI), a solution scheme based on AVL Search Tree(AVLST) is proposed. The time complexity of searching and updating of the scheme is $O(\text{lb}n)$. A novel certificate management method is also introduced. Experimental results show this scheme is effective, and has referential value to the PKI engineering practice.

【Key words】 Public Key Infrastructure(PKI); Certification Authority(CA); certificate revocation; binary search tree; AVL Search Tree(AVLST)

1 概述

随着电子商务的推广，安全性问题已经受到人们越来越多的关注。电子商务安全支付中的一个重要课题是对各个实体身份的认证，而对实体身份的认证是通过公钥基础设施(Public Key Infrastructure, PKI)技术来实现的，即将某一实体与其所持的公钥证书捆绑在一起。这样对实体身份的认证，实际上是对其所持有的公钥证书的认证。公钥证书是由公钥基础设施中具有公共信任资格的证书权威(Certification Authority, CA)签名的一组信息。该组信息除了含有该公钥持有人的身份信息及公钥参数等数据外，还有该证书编号及证书有效期限等。公钥基础设施通过公钥证书链来传递信任，进而实现对各个实体身份进行认证的目的。

当证书颁发之后，其有效性通常由有效期加以限制。但是经常由于密钥泄露或是怀疑密钥泄露或证书持有人的工作岗位变动等原因，有些证书需在其失效期前吊销。信誉卡系统是这方面的一个典型例子，当一个卡被盗或丢失时，卡的持有人报告信誉卡管理中心，管理中心必须在该卡失效前予以吊销。持有证书只是证明该证书有效的必要条件而非充分条件。因此，需要建立一种证书吊销及证书有效性查询的机制，以维护系统的安全运行[1]。

目前，关于证书吊销问题的解决方案主要有 X.509 证书系统的证书吊销列表(Certificate Revocation List, CRL)、Micali 的证书吊销系统(Certificate Revocation System, CRS)、kocher 的证书吊销树(Certificate Revocation Tree, CRT)、Naor-Nissim 的 2-3 证书吊销树 2-3CRT 以及王尚平等的证书吊销的线索二叉排序 Hash 树解决方案(Certificate Revocation Threaded Binary Sorted Hash Tree, CRTBSHT)。

本文在 CRT, 2-3CRT, CRTBSHT 及文献[2]系统思想的基础上，提出证书吊销问题的一个新的解决方案——AVL 搜索树解决方案(Certificate Revocation AVL_Search Tree, CRAVLST)。该方案继承了 CRT 及 CRTBSHT 的优点，即证明一个证书的状态不需要整个线索二叉树，而只需要其中相关路经的部分(约为所有节点数的对数个数值)。同时，在更新该树时，不需要对整棵树重新计算，仅需计算相关路经，且保留了二叉树的结构，该方案克服了 CRTBSHT 方案及文献[2]给出的证书吊销解决方案中叶节点到根节点的路径长度不统一，有的叶节点到根节点路径很短，有的则很长的问题。该方案中叶节点到根节点的路径长度始终保持在 $O(\text{lb}n)$，其中，n 为树中所有节点数。即该方案对查询、插入与删除的最大时间复杂度始终保持在 $O(\text{lb}n)$量级，较好地解决了证书吊销问题。据此策略本文还给出基于 AVL 搜索树的证书管理方案。设共发放 m 个证书，则该方案在查询证书的状态以及插入、删除操作其最大时间复杂度都保持在 $O(\text{lb}m)$量级。

2 AVL搜索树

2.1 AVL搜索树的基本概念

定义 1 二叉搜索树[3](binary search tree)是棵可能为空的二叉树，一棵非空的二叉搜索树满足以下特征：

(1)每个元素有一个关键值，并且没有任意 2 个元素有相同的关键值，因此，所有的关键值都是唯一的。

(2)根节点左子树的关键值(如果有的话)小于根节点的关键值。

(3)根节点右子树的关键值(如果有的话)大于根节点的关键值。

(4)根节点的左右子树也都是二叉搜索树。

定义 2 空二叉树是 AVL 树，如果 T 是一棵非空的二叉树，T_L 和 T_R 分别是其左子树和右子树，那么当 T 满足以下条件时，T 是一棵 AVL 树。

基金项目：江苏省科技攻关计划基金资助项目(BE2006357)
作者简介：周海岩(1957－)，男，教授，主研方向：信息安全，数据挖掘，智能决策，算法设计与分析，数据库；赵建洋，副教授、博士
收稿日期：2008-10-30 **E-mail：**zhy_5703@163.com

(1)T_L 和 T_R 是 AVL 树；

(2)$|h_L-h_R|\leqslant 1$，h_L 和 h_R 分别为左子树和右子树的高度。

AVL 搜索树(AVL_Search Tree)既是二叉搜索树，又是 AVL 树。

命题 1 有 n 个节点的一棵 AVL 树，其树高为 $O(\text{lb}n)$。

2.2 AVL搜索树的插入与删除

对于 AVL 搜索树，经插入或删除节点后可能不再是 AVL 搜索树，所以，插入或删除节点后，需要调整原 AVL 搜索树，使其保持平衡。这种操作称为平衡调整。

由于在 AVL 搜索树上插入节点而失去平衡的最小子树的根节点为 a(即 a 是离插入节点最近的，且平衡因子绝对值超过 1 的祖先节点)则失去平衡后进行调整的规律可归纳为下列 4 种情况：(1)*LL* 型平衡旋转；(2)*RR* 型平衡旋转；(3)*LR* 型平衡旋转；(4)*RL* 型平衡转。其中，(1)和(2)对称；(3)和(4)对称。旋转的正确性由“遍历所得中序序列不变”证明。以下给出 AVL 搜索树插入算法的简单描述。AVL 搜索树的插入与删除算法详见文献[3]。AVL 搜索树插入算法描述如下：

(1)沿着从根节点开始的路径对具有相同关键字的元素进行搜索，以找到插入新元素的位置。在此过程中，寻找最近的，平衡因子为-1 或 1 的节点，令其为 A 节点。如果找到了相同关键字的元素，那么插入失败，返回。

(2)如果没有这样的节点 A，那么从根节点开始再遍历一次，并修改各有关节点的平衡因子，返回。

(3)如果 $A.Bf$=1，并且新节点插入到 A 的右子树中或者 $A.Bf$=-1 并且新节点插入到 A 的左子树中，那么 A 的新平衡因子是 0。这种情况下，修改从 A 到新节点途中的平衡因子，然后终止。

(4)确定 A 的不平衡类型并执行相应的旋转，在从新子树根节点至新插入节点途中，根据旋转需要修改相应节点的平衡因子。

3 基于AVL搜索树的证书吊销系统

先给出证书吊销问题的抽象化模型。这里采用文献[1]中的定义。一个全集，S 是 U 的一个子集，$S\subseteq U$ 设 D_s 是代表 S 的一个数据结构。

(1) 〈e〉代表对 $e\in S$ 的成员查询，其回答为 〈a〉，$a\in$ {YES,NO}，分别对应于 $e\in S$ 或 $e\notin S$。若其回答为 〈a, p〉，其中，a 同上且 p 是由 CA 签名的一个关于 a 的证明，则称这样的查询为成员认证查询。

(2)更新运算是指如下 2 种运算：

1) 〈*Insert*,e〉，其中，$e\in U\backslash S$，则插入 e 后的数据结构为 $D_{S'}$，这里 $S'=S\cup\{e\}$；

2) 〈*Remove*,e〉，其中，$e\in U$，则删除后的数据结构为 $D_{S'}$，这里 $S'=S\backslash\{e\}$。

下面设 U 是 CA 发行的全部证书编号集，S 是 CA 吊销的证书编号集，用 AVL 搜索树来构造数据结构 D_s，并讨论其认证查询以及插入、删除运算。

3.1 基于AVL搜索树的证书吊销模型

先设 CA 吊销的证书编号集为 $S=\{n_1,n_2,\cdots,n_m\}$，其中，被吊销的证书编号可按吊销的顺序任意排列。下面以证书编号为关键字，对 S 构造 AVL 搜索树。设 AVL 搜索树中节点的结构为：

Lchild	Num	*Bf*	Parent	Rchild

其中，Num 为被吊销的证书的编号；Lchild, Rchild 分别是指向其左右子树的根节点的指针；Parent 为指向其父节点的指针；*Bf* 为平衡因子。*Bf* 是为了在构造 AVL 搜索树时及在 AVL 搜索树中简化插入和删除操作所设置的参量。给定节点 X，X 的平衡因子定义为

$$X.Bf=h_{xl}-h_{xr}$$

其中，h_{xl}, h_{xr} 分别是节点 X 的左右子树的树高。从 AVL 搜索树的定义易知，平衡因子的可能取值为-1, 0 和 1。

可以调用 AVL 搜索树的插入算法建立证书吊销 AVL 搜索树 T。该树的每个节点对应于一个被吊销的证书。这样得到的树反映了被吊销的证书的信息，类似于 CRT，证明某证书被吊销只需要给出该证书所对应的节点到根节点的路径及相关节点的有关信息即可。查询者在收到证明以后，可以利用 CA 的公钥与证明中 CA 对根节点的签名验证名录服务应答证明的有效性。由于 n 个节点的一棵 AVL 搜索树其树高始终保持在 $O(\text{lb}n)$量级，因此对被吊销证书的查询及插入与删除操作其最大时间复杂度都保持在 $O(\text{lb}n)$量级。

以文献[1]所给出的被吊销证书编号集 S={50, 12, 5, 99, 20, 13, 15}为例，以被吊销证书编号为关键字，构成的 AVL 搜索树如图 1 所示。其中，节点旁边的数字表示对应节点的平衡因子的值。

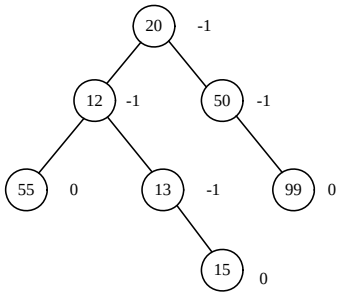

图 1 证书吊销 AVL 搜索树示例

给定一个证书编号，若要查询该编号的证书是否被吊销只需利用一般二叉搜索树的搜索算法查询 AVL 搜索树中是否存在该编号的节点即可得到问题的答案。

3.2 基于AVL搜索树的证书管理系统

可以基于 AVL 搜索树为数据结构建立证书管理系统，设 $U=\{u_1,u_2,\cdots,u_m\}$是 CA 发行的全部证书编号集，下面以证书编号为关键字，对 U 构造 AVL 搜索树。设 AVL 搜索树中节点的结构为

Lchild	Num	*Bf*	Parent	*Zt*	Rchild

其中，Num 为被吊销的证书的编号；Lchild, Rchild 分别是指向其左右子树的根节点的指针；Parent 为指向其父节点的指针；*Bf* 为平衡因子；*Zt* 是证书的状态，*Zt*=0 表示证书有效，*Zt*=1 表示证书被吊销。同样，可以调用 AVL 搜索树的插入算法建立证书管理 AVL 搜索树 T。该树的每个节点对应于 CA 发行的一个证书。这样得到的树反映了 CA 发行的全部证书的信息，设 CA 共发行 m 个证书，则证书管理 AVL 搜索树 T 共有 m 个节点，于是证书管理 AVL 搜索树 T 的高度为 $O(\text{lb}m)$，因而证书管理 AVL 搜索树 T 的查询、修改(这里指的是修改某证书对应节点得状态 *Zt* 等的值)与更新(即插入与删除)的最大时间复杂度都保持在 $O(\text{lb}n)$量级。由此可见，AVL 搜索树是用于数据管理的一类好的数据结构。

（下转第 178 页）