第 35 卷 第 1 期 计 算 机 工 程 2009 年 1 月
Vol.35 No.1 Computer Engineering January 2009
·博士论文· 文章编号：1000—3428(2009)01—0036—04 文献标识码：A 中图分类号：TP311

基于局部签名 Hash 表的证书撤销列表方案

王 政，赵 明，斯雪明，韩文报
(解放军信息工程大学信息工程学院，郑州 450002)

摘 要：在大规模应用环境中，不合理的证书撤销方案会带来巨大的运算量和网络传输负担。该文分析几类主要的证书撤销列表(CRL)机制，提出 PSHT-CRL 方案，综合分段 CRL、重定向 CRL 和重复颁发 CRL 方案的特点，采用 Hash 表、局部签名和链接等方法，在确保安全性的基础上，提高用户查询和证书更新时的效率，以解决其他证书撤销方案中遇到的问题。对 PSHT-CRL 方案的安全性和效率进行分析，与其他 CRL 方案作了比较。

关键词：公钥基础设施；哈希表；公钥证书；证书撤销列表

Certificate Revocation List Scheme Based on Partial Signature Hash Table

WANG Zheng, ZHAO Ming, SI Xue-ming, HAN Wen-bao
(Institute of Information Engineering, PLA Information Engineering University, Zhengzhou 450002)

【Abstract】 Large scale environment, unreasonable certificate revocation management will bring enormous operations and burden of network transmission. This paper analyzes some kinds of CRL mechanisms, puts forward a maintenance scheme of certificate revocation list named PSHT-CRL, which inherits the character of segment-CRL, redirect-CRL and over issue-CRL. PSHT-CRL uses Hash table, partial signature, and link method to ensure the scheme's security, to reduce the cost of user request response and certificate updating. PSHT-CRL solves the problems of other revocation schemes. The security and capability of this scheme are analyzed and PSHT-CRL compared with other CRL scheme.

【Key words】 Public Key Infrastructure(PKI); Hash table; certificate; Certificate Revocation List(CRL)

公钥基础设施(Public Key Infrastructure, PKI)[1]以公钥证书为基础，实现身份认证、通信保密、抗抵赖等安全机制。公钥证书的安全关系到整个系统的安全性，对公钥证书生存期中每一个环节的安全保障都十分重要。在PKI中，由证书权威机构(CA)为用户进行公钥证书的颁发和撤销。一般情况下，可以通过证书的有效期控制公钥证书的使用期限，但在实际应用中，由于私有密钥泄露、用户更新等原因，需要对有效期内的公钥证书进行撤销，因此需用合适的证书撤销方案来实现。证书撤销方案的优劣会影响整个系统的运行效率，甚至影响PKI的实际应用。因此，研究与设计安全、高效、灵活、实用的证书撤销方案是PKI研究的重要组成部分。

1 已有的 CRL 证书撤销方案

证书撤销方案的基本模型如图 1 所示。

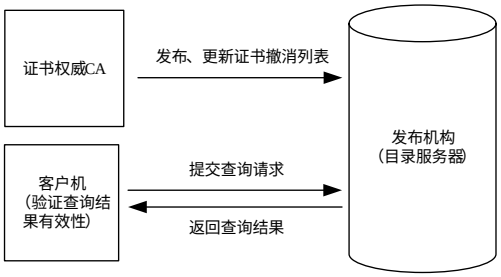

图 1 证书撤销方案基本模型

证书撤销方案包括 3 个主体：证书权威机构(CA)，发布机构(目录服务器)，用户。公钥证书的撤销信息由CA提供，由目录服务器发布。用户通过查询目录服务器判断相应的公钥证书是否有效。在安全性讨论中，往往认为发布机构是不可信的。证书撤销有多种实现机制，如证书撤销列表(Certificate Revocation List, CRL)[2-3]，CRS(Certificate Revocation System)[4]，CRT(Certificate Revocation Tree)[5-7]，在线证书验证机制[3,8]和短期证书机制[3,9-10]。由于CRL方案简单、易用，因此目前普遍采用的方法是周期性地发布CRL，这是本文所设计的证书撤销方案的基础。PKIX 工作组在RFC2459[2]中对CRL作了详细描述。证书验证者查询和下载CRL，根据CRL中是否包含所查证书序列号判断证书的有效性。

CRL方案的应用主要面临4个问题：

(1)CRL的规模[3,11]。在大规模网络环境中，CRL的大小正比于该CA域的用户规模、证书的生命期和证书撤销的概率。而撤销信息必须在已颁证书的整个生命期里存在，这就可能导致在某些CA域内的CRL发布变得非常庞大。

(2)CRL中撤销信息的实时性[3]。CRL是定期发布的，而撤销请求的到达是随机的，从接收撤销请求到下一个CRL发布之间的时延将带来证书状态在CRL上和现实中的不一致。

基金项目：国家自然科学基金资助项目(60503011)；国家“863”计划基金资助项目(2006AA01Z425)；国家“973”计划基金资助项目(2007CB807902)

作者简介：王 政(1975－)，男，博士研究生，主研方向：密码学，信息安全；赵 明，助理工程师、硕士；斯雪明，副研究员、博士研究生；韩文报，教授、博士

收稿日期：2008-06-05 **E-mail：**file_wang@sina.com

(3)网络带宽。用户与发布机构之间、CA与发布机构之间存在繁重的通信量。随着用户规模逐渐增大，撤销的证书也逐渐增多，用户为了检查一个证书的有效性，必须下载整个撤销列表，造成通信带宽的浪费。

(4)计算资源。CA在更新CRL时要进行大量数据的签名运算，造成对CA峰值的计算压力过大。

为了缓解这些问题，产生了一些对CRL机制的改进方案。

1.1 基本 CRL

CRL是一个带签名信息的列表(一般由CA签发)，其中包含了所有被CA撤销的公钥证书的序列号、更新生效的时间以及有效期，具体结构如图2所示。

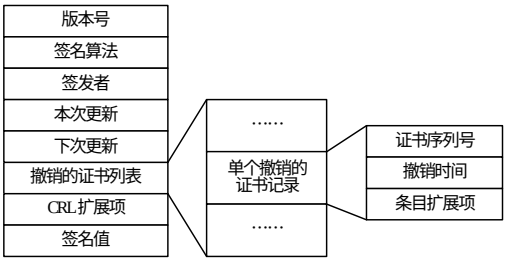

图 2 基本 CRL 结构示意图

在到达有效期限时，即使证书撤销列表没有任何变化，CA 也必须签发新的列表来代替旧的。CRL 通过发布机构(目录服务器)进行发布，如果一个用户需要检查一个证书是否已经被撤销，需要到发布机构下载整个 CRL 来确定证书是否已经被撤销。当已撤销的证书过期时，在以后发布的 CRL 中就不会再出现该证书的记录信息。

由于CRL具有简单和易于实现的特点，因此成了目前应用最广泛的证书撤销机制。同时，为了提高证书撤销列表管理的效率，一些CRL的改进方案被提了出来，主要包括增量CRL(Delta-CRL)[3,11]、分段CRL(Segment-CRL或CRL Distribution Points)[3,12]、重复颁发CRL(Over-issued CRL)[12]、重定向CRL(Redirect-CRL)[3,13]、间接CRL(Indirect-CRL)[3]。

1.2 增量 CRL(Delta-CRL)

缩短CRL的颁发周期可以减少CRL时延给用户带来的风险，但频繁发布庞大的CRL给CA和用户都带来了沉重的负担。解决CRL时延问题的一种新的机制是增量CRL。

增量CRL包含2种类型的CRL：基准CRL和增量CRL。基准CRL发布注销的证书信息，增量CRL在每2次基准CRL更新期间，以较小的时间间隔颁发自上一次基准CRL颁发以来新增加的注销证书供用户下载。Delta-CRL提高了CA发布注销证书的频率，同时减小了用户下载尺寸，但是每一次Delta-CRL的发布也会出现类似CRL的峰值请求高峰；而且在用户请求完一次Delta-CRL时，若本地没有基准CRL，还需请求基准CRL，增加了用户的平均请求率。

1.3 分段 CRL

按照某种分类方式将CRL分段发布，可以减小CRL长度。如按照地区分段，用户只需下载该地区的CRL段，无须下载全部CRL。每段CRL的存放地点可以在颁发证书时，在扩展字段中指明。但是，证书一旦颁发，CRL段的存放地址就已经固定。为了改变这种不利于扩展的局限性，提出了重定向CRL。

分段CRL可以发布在不同的证书库中，它减少了用户下载的CRL长度，将峰值请求分散到各个分段的存放地址，但在用户需要查询多个段时，反而增加了用户的平均请求率和等待时间。分段CRL还有一个问题是，一旦颁发了证书，在整个证书的生命期里，CRL分段的位置就固定了。

1.4 重定向 CRL

重定向CRL即在证书扩展项中不是指明CRL分段的存放地址，而是指出可以找到CRL分段存地址的地址。这种方法也称为动态分段CRL。

重定向CRL可以用来解决分段CRL中位置不能改变的问题，一个重定向CRL可以指向多个CRL，能指出到哪里去找到每个CRL分段。重定向CRL能提供比标准分段CRL更灵活的分段位置信息，通过定义一种新的CRL扩展来实现，这种新扩展允许在不影响现有证书撤销机制的情况下，改变撤销信息的分段的分布位置。

在重定向CRL中有多个范围声明，它们指出了多个CRL分段中证书的范围或类型。范围信息可以基于证书序列号或者其他标识符。重定向CRL的位置可以在证书的CRL分段中指出，或用其他方式告知用户。这样，用户就可以检索重定向CRL，然后根据范围声明找出相应的CRL分段信息存放的位置。

1.5 重复颁发 CRL(Over-issued CRL)

将 CRL 交叉颁发，即在旧的 CRL 还未到期时就发布新的 CRL，使用户缓存中的 CRL 在不同时间到期来降低峰值请求。如第 1 个 CRL 在 0∶00 发布，24∶00 到期，隔 6 h，再发布一次新的 CRL，即 6∶00 发布，次日 6∶00 到期，依此类推，用户下载 CRL 后将其缓存，只有在 CRL 过期时，才会下载新的 CRL。

1.6 间接 CRL

间接CRL使得在一个CRL中可以发布多个CA的撤销信息。间接CRL的使用可以减少用户在证书验证过程中需要检索的CRL总数。例如一个PKI域中可能会有多个CA，尤其强迫一个用户去检索多个CRL(每个CRL 对应一个CA)，不如把整个域里的证书撤销信息集中到一个间接CRL中，以提高效率。这种机制在域间情况下也很有效，可以减少流量负载和降低成本。

间接CRL是基于普通CRL的、通过CRL扩展值来确定的。采用这种机制的前提是，集中了所有的撤消信息后，间接CRL不会变得太庞大而降低系统性能。另外，间接CRL的签发者很可能不是证书的签发者，所以，用户必须信任间接CRL的签发者，就像信任CA一样。

1.7 衡量证书撤销方案的主要性能指标

一个良好的证书撤销体系应该在安全性、可扩展性、服务器性能、用户查询代价方面满足实际应用需求。

(1)安全性。首先要保证所发布的消息安全可靠，不会遭到不可信证书库篡改或伪造，保证撤销信息的新鲜度。

(2)可扩展性。当 PKI 规模扩张时，容易扩展适应新的规模。

(3)服务器性能。这主要是指峰值请求和网络带宽。

(4)用户查询代价。这是指用户所需下载的 CRL 大小、请求响应延迟等。

2 基于 Hash 表的证书撤销方案

通过上述分析可以看出，虽然前述的各类方案解决了公钥证书撤销中的某些问题，但是每种方案都有其自身的局限性。由此，本文提出了一种基于局部签名 Hash 表的证书撤销列表方案，它是分段 CRL 的一种改进，在保证简单、易用的基础上，通过采用 Hash 表和局部签名的方式进一步提高各个

CRL 分段的均匀分布，降低 CA 与发布机构、发布机构与用户之间的通信量，降低用户验证时的计算量。分析表明，此方案在适当增加 CA 发布 CRL 时所需计算量的情况下，几项重要的性能指标都有一定的提高，确保了 CA 签名的安全性。

2.1 局部签名 Hash 表的建立

方案中证书的撤销管理基于局部签名 Hash 表机制，采用带表头节点的 Hash 表进行证书撤销列表的存储。方案中使用 2 个 Hash 函数：*Hash*1()和 *Hash*2()，前者用于构造 Hash 表，满足 Hash 值均匀分布即可(可根据需求设计)；后者用于构造局部签名，应满足 Hash 值均匀分布和强碰撞自由条件(如 SHA-1)。PSHT-CRL 数据结构建立步骤如下：

(1)首先建立Hash表的所有表头节点，每个表头节点包含以下内容：表头节点在Hash表中的地址a；与表头节点对应的数据区中数据单位的个数n_a；数据区内容的Hash值h_a，$h_a = Hash2(ID_{a1} \| ID_{a2} \| \cdots \| ID_{an_a})$，若$n_a$＝0，则 $h_a = Hash2(\phi)$；当前表头节点对应CRL数据区的签发时间t_{a1}以及下次更新时间t_{a2}；对应的CRL数据区存储地址*laddr*(可以采用URL地址)及对以上信息的签名信息S_{CA}。Hash表的大小可根据证书用户规模确定，若证书系统最大用户规模为N，则Hash表的大小可定为 $\sqrt{N}$，即对任意ID都有 $0 \le Hash1(ID) \le \sqrt{N}$。

(2)CRL数据区中每个数据单位就是一个撤销的证书序列号ID_i。在表头节点中存放着与该表头节点对应的CRL数据区中数据单位的个数n。若n=0，表示在该表头节点下无撤销的证书。

(3)对撤销证书的序列号 ID 进行 *Hash*1()运算，确定其在 Hash 表中的地址 a＝*Hash*1(ID)，取出地址 a 处存放的表头节点，根据表头节点中的重定向地址 *laddr* 确定与其相关的 CRL 分段的数据区(允许存放在其他发布点上，可采用 URL 定位)，由 CA 在数据区中插入新 ID(在 ID 对应的证书到期时也可执行删除老 ID 的操作)，并对表头节点的内容进行更新与发布。由于 Hash 表的元素定长、有序且带有重定向地址，因此便于查询(可通过地址计算直接定位元素)和分布式存放(即将经过重定向的 CRL 分段存储到若干个不同的发布机构中，以降低发布机构的访问压力)。

(4)CA 按照上述规则建立 Hash 表后，对每一个表头节点中的内容和相应数据区中的数据使用 CA 的私钥进行签名，即 $S_{CA} = Sign_{CA}(a, n_a, h_a, laddr_a, t_1, t_2)$。对表头节点中任何数据(如有效期)和相应 CRL 数据区中任何数据的篡改，都能通过验证 CA 签名信息发现。对于所有表头节点的内容，CA 都要进行签名，包括数据区为空的表头节点。

在建立 Hash 表时需要做以下工作：

(1)为不同的表头节点设定不同的更新时间，将各个表头节点对应的CRL分段到期时间错开，以降低CA和发布机构之间、发布机构与用户之间信息传输的峰值带宽[11,14]，以及CA的峰值计算压力(主要指签名运算)。

(2)针对分布式的发布机构，可将Hash表对应的CRL分段进行分布式存储，以减少每个发布机构存储CRL所占用的空间及访问量[11,14]。用户可根据需要到特定的发布机构下载链表。应该注意的是，每个CRL上都应有一份完整的Hash表(可以不含CRL数据区)。

(3)为提高方案的效率，*Hash*1()运算得到的地址应该在Hash表中分布均匀，以更好地实现负载均衡[11,14]。

图 3 是本文的 Hash 表结构，其中，每一个节点由证书序列号、Hash 值及下一节点指针组成。

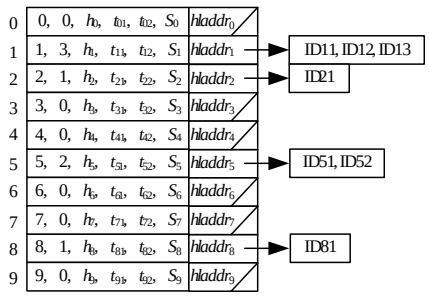

图 3 局部签名 Hash 表结构

2.2 证书的查询与判断

在进行证书撤销情况的查询时，用户首先检查本地有无缓存信息，若有，则检查缓存信息是否过期；若没过期，则使用缓存信息进行后面的查询与判断。若没有已过期的缓存信息或缓存信息，则将要查询的证书序列号 ID 发送给发布机构(目录服务器)，发布机构根据证书序列号 ID 计算其在 Hash 表中的地址 a＝*Hash*1(ID)，之后将该地址对应的表头节点发送给用户。

用户根据返回的信息判断所查询证书是否被撤销(检验算法)：

(1)通过检验表头节点中CA签名的正确性，确保表头节点内容的新鲜度和完整性，若验证出错，则报错，转步骤(8)；若通过验证，则继续。

(2)判断表头节点中的地址a是否等于*Hash*1(ID)；若不相等，则报错，转步骤(8)；若相等，则继续。

(3)检查表头节点中的 CRL 数据单元计数 n，若 n=0，则说明所查询 ID 号对应的证书未被撤销，报告结果，转步骤(8)；若 $n \neq 0$，则用户根据表头节点中 *laddr* 指向的位置获取对应的 CRL 分段的数据区。

(4)在取得 CRL 分段的数据区后，先判断数据区中的证书 ID 数目是否和表头节点中的计数 n 相等，若不相等，则报错，并转步骤(8)；若相等，则继续。

(5)计算 CRL 分段的数据区中所有 ID 的 Hash 值，$Hash2(ID_{a1} \| ID_{a2} \| \cdots \| ID_{an_a})$并与表头节点中的 Hash 值 h 进行比较，若不相等，则报错，转步骤(8)；若相等，则继续。

(6)通过查询数据区中的所有证书ID，判断所查ID号对应的证书是否被撤销，若在数据区中找到所要查询证书序列号 ID，则该证书已被撤销；若未找到，则该证书未被撤销。

(7)根据需要对表头节点和数据区进行缓存，以提高多次查询的效率。

(8)结束。

2.3 撤销列表的更新

撤销列表更新时，由于在表头节点中设置了不同的更新周期，CA只要向发布机构传送整个Hash表的部分节点(达到更新时间的节点)。更新的具体过程如下：

(1)若对应地址的表头节点到达有效期，但对应的CRL分段数据区的证书数目和内容未改变，则CA根据新的有效期重新计算表头节点中的签名信息，并将表头节点信息发送给所有分布式发布机构进行更新。

(2)若对应的CRL分段数据区的证书数目或内容发生改变，则CA根据新的数据区内容计算Hash值h*，更新表头节点中的数据区Hash值h和CRL证书计数值n，重新设置有效期，

计算表头节点中的签名信息，并将表头节点信息发送给所有分布式发布机构进行更新，同时，把新的CRL分段的数据区传送到*laddr*指向的发布位置。

(3)若CRL分段的数据区存放位置发生改变，则用新的位置信息*laddr**更新表头节点中的*laddr*，重新计算表头节点中的签名信息，并将表头节点信息发送给所有分布式发布机构更新，同时，把CRL分段的数据区存放到新的发布位置。

3 方案的安全性和效率

3.1 安全性

CA对所有表头节点的信息进行签名，其中包括CRL分段数据区生成的Hash值。假设所采用的Hash函数是安全的，则所有对CRL分段数据区中数据单元的篡改都会被发现。因此，CRL分段数据区中的证书ID的完整性可以得到保证。

无论是不可信发布机构还是攻击者，对返回的查询结果进行任何修改都会被发现。例如，删除CRL数据区中的一个证书ID(图4)，虽然可以通过2.2节检验算法中的第(1)步CA签名的检查，但在第(5)步就将被发现，无法通过Hash值检验。

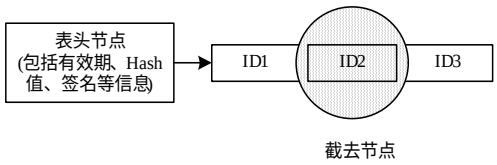

图 4 非法截短的链表

若不可信发布机构或攻击者通过返回Hash表中其他表头节点或过期的表头节点来欺骗查询者，在检验算法中也将被发现，因为CA的签名信息中包含了表头节点对应的地址和有效期。

由此可知，本方案可以抵抗来自发布机构外部以及不可信发布机构的篡改和替换攻击。

3.2 效率

在下面的讨论中，设证书系统的用户规模为N，撤销的证书个数为n，Hash表的容量为m(*Hash*1()函数输出最大值)，证书的序列号长度为l_{id}，*Hash*2()函数的输出值长度为l_h，CA签名信息长度为l_s，时间参数的长度为l_t，表头节点地址的长度为l_a，CRL数据区位置信息的长度为l_l。

采用本方案时，若使用k个分布式证书发布机构，则总空间开销为$O(km+n)$。每个证书发布机构的空间开销为$O(m+n/k)$。

对于每一次用户请求，发布机构查询时间为$O(1)$。

若*Hash*1()函数的输出在[0,m]上均匀分布，且用户查询的证书ID是随机的，则用户收到服务器返回的平均信息长度为$O(1+n/m)$，本地的平均查询时间为$O(1+n/m)$。该结论由以下事实保证：

假设共有n个需要撤销的证书存储到m个表中，则m个表的平均节点数等于n/m。

因此，对于每一次用户请求，发布机构向用户传输的数据量为：$l_s+l_h+l_a+l_l+2l_t+l_{id}\cdot(n/m)$，约为：$O(1+n/m)$。

此外，本方案还具有以下特点：

(1)对分段CRL、重定向CRL、重复颁发CRL方案进行了综合，使本方案同时具备三者的优点。

(2)Hash表对应的CRL分段进行分布式存储，可以降低每一个发布机构的访问流量和存储空间的要求。

(3)证书更新采用了局部更新的方式，可以减少撤销列表的更新开销，降低因延时带来的风险，无须每次更新发布庞大的撤销列表。

(4)表头节点中可以定义不同的发布时间和下次更新时间，实现重复颁发CRL的功能，使用户缓存的链表在不同时间到期，降低了峰值请求。

(5)支持离线、在线2种方式，用户可根据自身环境选择是否存储撤销链表。

(6)对表头节点的下载和验证使用户有一个预判过程，可以减少不必要的CRL分段下载。

表1是PSHT-CRL方案与基本CRL方案的性能比较。

表 1 PSHT-CRL 方案与基本 CRL 方案性能比较

	基本CRL	PSHT-CRL
空间开销	$O(n)$	$O(km+n)$
查询时间	$O(n)$	$O(n/m)$
传输开销	$O(n)$	$O(n/m)$

从表1可以看出，适当增加总存储空间可以大大降低相应的查询时间和传输开销。由于存储空间是分布到k个发布机构上的，每个发布机构的存储只有$O(m+n/k)$，这与基本CRL的单发布机构存储量相差不大。

表2是PSHT-CRL方案与其他CRL方案的综合比较。

表 2 PSHT-CRL 方案与其他 CRL 方案的综合比较

方案	访问量与峰值	合时性	扩展性	安全性	用户端要求
普通CRL	流量高,存在峰值问题	周期性发布撤销信息,周期较长	适合小规模或撤销频率低的系统	由CA签名保证安全性	支持离线使用
增量CRL	相对CRL访问率和流量有改善	经常发布新的撤销信息,合时性较高	相对CRL有所改善	与CRL相同	支持离线使用,需经常下载撤销信息
分段CRL	单个分布CRL的访问率和流量减少	周期性发布撤销信息,周期较长	适合大规模,高撤销频率系统	与CRL相同	不适合离线使用
重复颁发CRL	解决峰值问题,性能显著改善	周期性发布撤销信息,周期较短	相对CRL有所改善	存在多个信息源的签名信息与验证	支持离线使用
PSHT-CRL	解决峰值问题,性能显著改善	周期性发布撤销信息,周期较短	适合大规模,高撤销频率系统	存在多个信息源的签名信息与验证	支持离线使用

可以看出，PSHT-CRL 综合了大部分 CRL 方案的优势，在保证合时性、安全性的前提下，对性能、扩展性作了改善，是一种较为理想的证书撤销方案。

4 方案的进一步改进

本文在讨论方案性能时采用了 2 个假设：(1)*Hash*1()函数的输出在[0,m]上均匀分布；(2)用户查询的证书 ID 是随机的。

在 PKI 等证书系统的实际应用过程中，不同证书的使用次数会有很大的差异，有的证书 ID 可能会被经常查询，而有的则很少被查询。针对这种情况，可根据证书的使用频率对*Hash*1()进行调整，使经常被查询的证书 ID 所在的表头节点对应的 CRL 分段数据单元数目最少(最优情况是取值为 0)，这样可以节约网络传输带宽和用户的本地查找时间。同时，在考虑 CRL 分段的分布式存储时，可根据 CRL 分段的访问频率调整 *Hash*1()，尽量做到负载平衡。

（下转第 42 页）