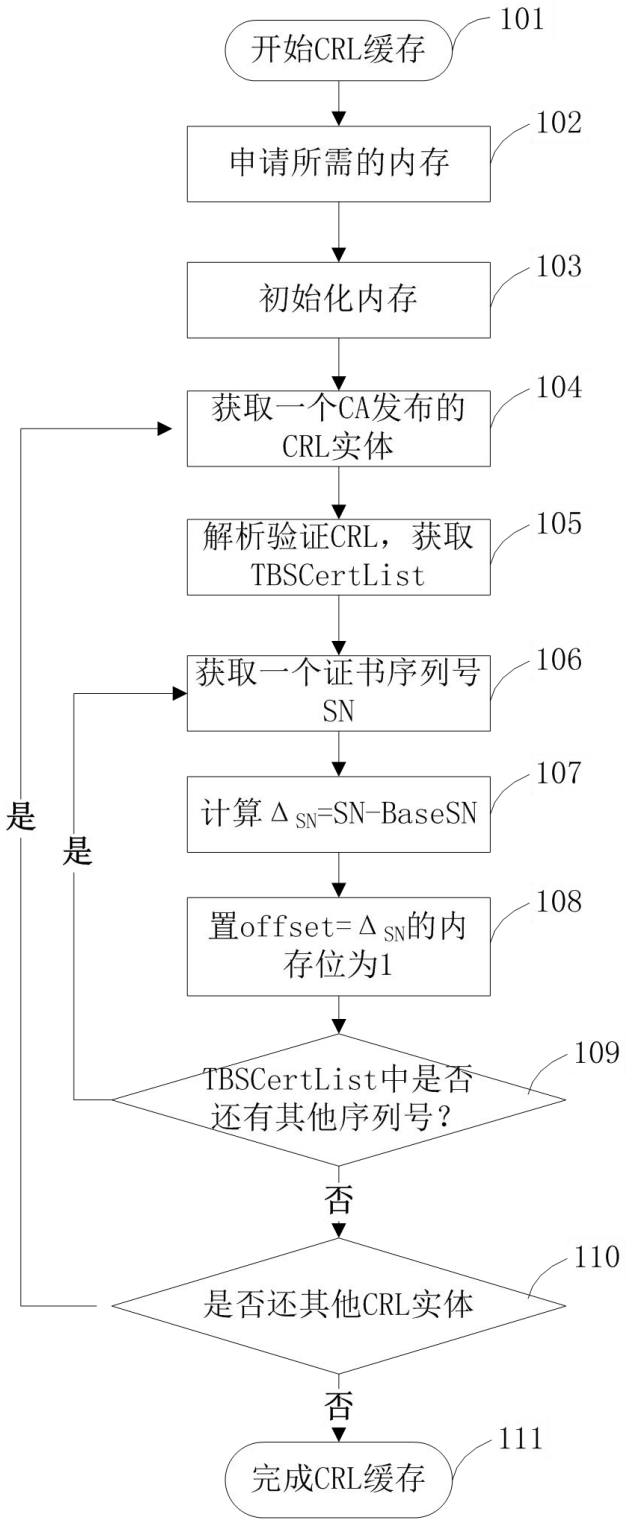
说　明　书　摘　要

本发明公开了一种数字证书的证书吊销列表缓存及查询方法，包括：A、设置一个起始值 BaseSN；B、分配一段用于储存证书吊销列表(CRL)的内存，并进行初始化，将 CRL 的缓存区内容清零；C、从 CA 获取一个最新发布的 CRL；D、解析所述的 CRL，从中得到 TBSCertList；E、从 TBSCertList 中获得一个数字证书的序列号(SN)；F、计算 SN 与 BaseSN 的差值 Δ_{SN}；G、设 Δ_{SN} 为偏移量，将 CRL 缓存区中相应的二进制位置 1；H、判断 TBSCertList 中是否还有其他数字证书的 SN，若没有，则执行步骤 I；否则，则返回步骤 E；I、步骤 I：进一步判断是否还有其他 CRL 实体，若有，则返回步骤 C；否则，结束所述 CRL 的缓存过程。采用本发明，能够提高从缓存中检索 CRL 的效率。

摘　要　附　图


开始CRL缓存
101
申请所需的内存
102
初始化内存
103
获取一个CA发布的CRL实体
104
解析验证CRL，获取TBSCertList
105
获取一个证书序列号SN
106
计算 Δ SN=SN-BaseSN
107
置offset= Δ SN的内存位为1
108
TBSCertList中是否还有其他序列号？
109
是
是
否
是否还其他CRL实体
110
否
完成CRL缓存
111

权　利　要　求　书

1、一种数字证书的证书吊销列表缓存方法，其特征在于，该方法包括：

A、根据数字证书的策略和实际情况，设置一个证书序列号的起始值BaseSN；

B、向系统申请分配一段用于储存证书吊销列表CRL的内存，并对该段内存进行初始化，将CRL的缓存区内容清零；

C、从数字证书颁发机构获取一个最新发布的CRL；

D、解析所述的CRL，从CRL中得到TBSCertList；

E、从TBSCertList中获得一个数字证书的序列号；

F、计算所述序列号与BaseSN的差值Δ_{SN}；

G、设所述Δ_{SN}为偏移量，将所述CRL缓存区中相应的二进制位置1；

H、判断所述TBSCertList中是否还有其他数字证书的序列号，若没有，则执行步骤I；否则，则返回步骤E；

I、步骤I：进一步判断是否还有其他CRL实体，若有，则返回步骤C；否则，结束所述CRL的缓存过程。

2、根据权利要求1所述数字证书的证书吊销列表缓存方法，其特征在于，所述数字证书序列号的起始值BaseSN与在内存中的位置无关。

3、根据权利要求1所述数字证书的证书吊销列表缓存方法，其特征在于，步骤D所述TBSCerList为CRL中的一个字段，该字段为一个序列，含有数字证书发行者的名字、发行日期、下一个CRL的发行日期、 吊销证书列表和可选CRL的扩展。

4、根据权利要求1所述数字证书的证书吊销列表缓存方法，其特征在于，所述CRL缓存区中相应的二进制的位置为1或0，用以指示对应该位置的数字证书的状态是否被吊销。

5、一种验证权利要求1～4所述数字证书状态的查询方法，其特征在于，包括：

a、获得数字证书的序列号 SN；

b、计算 SN 与数字证书序列号的起始值 BaseSN 的差值，即计算 Δ_{SN}=SN-BaseSN；

c、取证书吊销列表 CRL 缓存区中 Δ_{SN} 位置上的二进制值 b；

d、判断该二进制位的 b 值是否为 1，若为 1，则证明该证书已被吊销；否则，b 不为 1，则证明该证书有效。

说　　明　　书

数字证书的证书吊销列表缓存及查询方法

技术领域

本发明涉及信息安全和数字证书技术，尤其涉及一种数字证书的证书吊销列表缓存及查询方法。

背景技术

基于数字证书的应用，通常需要访问证书颁发机构（CA）获取证书吊销列表（CRL）来检查证书状态。应用软件通常将 CRL 缓存，并按预设的策略进行更新。随着数字证书数量的快速增长，CRL 缓存的空间开销和检索证书是否被吊销的时间开销也变得越来越大。因此，亟待发展一种能够提高缓存和检索 CRL 效率的技术。

目前，传统的 CRL 缓存方式是缓存 CRL 的实体，或使用线性表、哈希表结构在存储 CRL 中标记“已吊销”的数字证书序列号。

现有的 CRL 缓存方式下，缓存一个数字证书序列号大约需要 20 字节，缓存 N 个 CRL 中被吊销的证书序列号，则需要的空间约为 N×序列号包含字节数。

在传统的 CRL 缓存方式下，检索一个指定的数字证书序列号（SN）是否包含在吊销列表中，对缓存的数据结构进行检索需要进行多次比对，才能确认缓存中是否包含了序列号（SN）。对于数据条数假设为 n 的缓存而言，查找的时间复杂度为 O(n)，如果采用二分法进行查找，则所需的时间复杂度为 O(log(n))。

因此，采用传统方式在数字证书数量和被吊销证书的数量达到百万至千万数量级之后，所需的存储空间和检索所需的时间，都会迅速增长，这将会对系统的运行效率和响应的及时性产生较严重的影响。

发明内容

有鉴于此，本发明的主要目的在于提供一种数字证书的证书吊销列表（CRL）缓存及查询方法，在使用海量的数字证书和数字证书的CRL的场景下，供使用数字证书的应用软件或密码设备进行验证使用，以大幅降低CRL缓存的开销和提高CRL的检索效率。

为达到上述目的，本发明的技术方案是这样实现的：

一种数字证书的证书吊销列表缓存方法，该方法包括：

A、根据数字证书的策略和实际情况，设置一个证书序列号的起始值BaseSN；

B、向系统申请分配一段用于储存证书吊销列表CRL的内存，并对该段内存进行初始化，将CRL的缓存区内容清零；

C、从数字证书颁发机构获取一个最新发布的CRL；

D、解析所述的CRL，从CRL中得到TBSCertList；

E、从TBSCertList中获得一个数字证书的序列号；

F、计算所述序列号与BaseSN的差值Δ_{SN}；

G、设所述Δ_{SN}为偏移量，将所述CRL缓存区中相应的二进制位置1；

H、判断所述TBSCertList中是否还有其他数字证书的序列号，若没有，则执行步骤I；否则，则返回步骤E；

I、步骤I：进一步判断是否还有其他CRL实体，若有，则返回步骤C；否则，结束所述CRL的缓存过程。

其中，所述数字证书序列号的起始值BaseSN与在内存中的位置无关。

步骤D所述TBSCerList为CRL中的一个字段，该字段为一个序列，含有数字证书发行者的名字、发行日期、下一个CRL的发行日期、 吊销证书列表和可选CRL的扩展。

所述CRL缓存区中相应的二进制的位置为1或0，用以指示对应该位置的数字证书的状态是否被吊销。

一种验证权利要求 1～4 所述数字证书状态的查询方法，包括：

a、获得数字证书的序列号 SN；

b、计算 SN 与数字证书序列号的起始值 BaseSN 的差值，即计算 Δ_{SN}=SN-BaseSN；

c、取证书吊销列表 CRL 缓存区中 Δ_{SN} 位置上的二进制值 b；

d、判断该二进制位的 b 值是否为 1，若为 1，则证明该证书已被吊销；否则，b 不为 1，则证明该证书有效。

本发明所提供的数字证书的证书吊销列表缓存及查询方法，具有以下优点：

在海量数字证书和海量数字证书吊销列表的情况下，基于数字证书的应用或设备，出于效率原因，需要缓存吊销列表的情况下，使用本发明的技术，能够有效降低缓存 CRL 所需的内存要求，并且，能够提高从缓存中检索 CRL 的效率。

附图说明

图 1 为本发明对数字证书的证书吊销列表进行缓存的过程示意图；

图 2 为本发明采用二进制位保存数字证书是否被吊销的信息的数据结构存储状态示意图；

图 3 为本发明验证数字证书（CA）状态的查询过程示意图。

具体实施方式

下面结合附图及本发明的实施例对本发明的方法作进一步详细的说明。

图 1 为本发明对数字证书（CA）的证书吊销列表（CRL）进行缓存的过程示意图。在本发明中，采用 1 个二进制位来保存 1 个证书是否被吊销的信息（参考图 2）。

如图 1 所示，对证书吊销列表进行缓存的过程包括如下步骤：

步骤 101：根据数字证书的策略和实际情况，设置一个证书序列号的起始值 BaseSN（参考图 2）。

这里，所述数字证书的实际情况，主要是指证书大小、存储空间等。

步骤 102：向系统申请分配一段用于储存证书吊销列表（CRL）的内存。

步骤 103：对所述的一段内存初始化，将证书吊销列表（CRL）的缓存区内容清零。

步骤 104：从数字证书颁发机构获取一个最新发布的证书吊销列表（CRL）。

步骤 105：解析所述的证书吊销列表（CRL），从证书吊销列表（CRL）中得到 TBSCertList。

这里，所述 TBSCerList 为 CRL 中的一个字段，该字段是一个序列，含有数字证书发行者的名字、发行日期、下一个证书吊销列表（CRL）的发行日期、吊销证书列表和可选 CRL 的扩展。其中，吊销证书列表是由一连串的数字证书序号、撤销日期和可选 CRL 入口扩展组成。

步骤 106：从 TBSCertList 中获得一个数字证书的序列号（SN）。

步骤 107：计算所述序列号（SN）与 BaseSN 的差值，即根据下述公式：

Δ_{SN}=SN-BaseSN。

步骤 108：设所述 Δ_{SN}=SN-BaseSN 为偏移量（offset），将证书吊销列表（CRL）缓存区中相应的二进制的位置为 1（参考图 2）。

步骤 109：判断所述 TBSCertList 中是否还有其他数字证书的序列号（SN），若没有，则执行步骤 110；否则，则返回步骤 106；

步骤 110：进一步判断是否还有其他证书吊销列表（CRL）实体，若有，则返回步骤 104；否则，执行步骤 111。

步骤 111：完成所述证书吊销列表（CRL）的缓存过程。

图 2 为本发明采用二进制位保存数字证书是否被吊销的信息的数据结构存储状态示意图。如图 2 所示，每个二进制位指示 1 个数字证书是否被吊销的状态。其中，二进制位“0”表示该对应的数字证书目前有效；二进制位“1”表示该对应的数字证书被吊销。如图 1 所示的步骤 108 中，偏移量（offset）Δ

$_{SN}$=SN-BaseSN，此时，须在证书吊销列表（CRL）缓存区中相应的二进制位赋值 1。反之，在 CRL 缓存区相应的二进制位赋值 0。

图 3 为本发明验证数字证书（CA）状态的查询过程示意图。在验证某个数字证书的状态时，需验证该证书的序列号（SN）是否包含在证书吊销列表（CRL）中，如果已经包含在吊销列表中，则认为该证书已被吊销；否则认为该证书状态为正常。如图 3 所示，该过程包括如下步骤：

步骤 301：开始数字证书状态验证。

步骤 302：获得证书的序列号 SN。

步骤 303：计算 SN 与数字证书序列号的起始值 BaseSN 的差值，即计算 Δ$_{SN}$=SN-BaseSN。

步骤 304：取 CRL 缓存区中，Δ$_{SN}$ 位置上的二进制值 b。

步骤 305：判断该二进制位的 b 值是否为 1，若为 1，则执行步骤 306；否则，执行步骤 307。

步骤 306：b 为 1，则证明该证书已被吊销，返回。

步骤 307：b 不为 1，则证明该证书有效。

下面，结合具体实施例对缓存数字证书的过程和查询即验证数字证书是否有效的过程分别进行说明。

例如，某证书认证机构颁发的证书，序列号是从下面的证书序列号开始，逐个递增，我们将该序列号定义为 CRL 缓存的 BaseSN。

64 3F 7D 55 30 87 94 41 22 00 00 00 00 00 00 00 00 00 00 01。

根据当前证书认证机构的证书容量和预期一个时间内的证书容量，我们预设 CRL 缓存大小为 64 M，分为 64 个区段，每个区段 1M。其定义如下：

CRL 缓存程序按照自己的缓存更新策略，到 CA 获取 CA 最新发布的 CRL，进行 CRL 的完整性验证，此后，从 CRL 的 TBSCertList 中获取所有被吊销的序列号，对每一个序列号 SN，采用如下步骤处理。

步骤 a：计算 Δ$_{SN}$=SN-BaseSN。

步骤 b：计算该 SN 所对应缓存的段 segment = Δ$_{SN}$ / (1024 * 1024 * 8);

步骤 c：计算该 SN 所对应缓存的字节位置 position = (Δ_{SN} % (1024 * 1024 * 8))/8；

步骤 d：计算该 SN 所对应缓存的二进制位 long offset2 = position % 8。

步骤 e：置该二进制位的值为 1。

其验证证书状态的过程如下：

步骤 A：解析数字证书，取得数字证书序列号 SN。

步骤 B：计算 Δ_{SN}=SN-BaseSN。

步骤 C：计算该 SN 所对应缓存的段 segment = Δ_{SN} / (1024 * 1024 * 8)。

步骤 D：计算该 SN 所对应缓存的字节位置 position = (Δ_{SN} % (1024 * 1024 * 8))/8。

步骤 E：计算该 SN 所对应缓存的位 long offset2 = position % 8。

步骤 F：取该位的二进制值 b，若 b 为 1，则返回该证书已被吊销，否则返回该证书状态有效。

在有海量数字证书（CA）和海量证书吊销列表（CRL）的情况下，基于数字证书的应用或设备出于效率原因，需要缓存吊销列表的情况下，使用本发明的技术，能够有效降低缓存 CRL 所需的内存要求，并且，能够提高从缓存中检索 CRL 的效率。

反映在需要的存储空间大小方面：

一般情况下，考虑数字证书的序列号空间，证书颁发机构会采用 10～20 字节的序列号，这种情况下，设想一个数字证书量为 10 亿的系统，按照 1/5 被吊销的估计值来分析，使用传统的缓存方式，需要的缓存空间约为：

缓存空间≈10 亿* 1/5 * 20 字节=40 亿字节≈4G 字节。

而使用本发明的方案，所需的缓存空间约为：

缓存空间≈10 亿* 1 比特 =10 亿比特≈125M 字节。

可见，采用本发明的方法，能够大大减少对存储空间的需求。

反映在检索效率方面：

采用本发明的方法，查询一个数字证书是否被吊销。只需要通过计算序列

号 SN 和 BaseSN 的差值，就可以直接获得偏移量（offset），根据对应的二进制位的值即可获得其证书是否是吊销状态。其计算的时间复杂度为常数 O（1）。相比传统方式采用线性表组、哈希表方式的检索 O(n)和 O(log(n))的计算复杂度，大大降低了从缓存中获取证书状态的计算量，从而可使证书验证过程的效率能够大幅度得到提高。

以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。

说　明　书　附　图

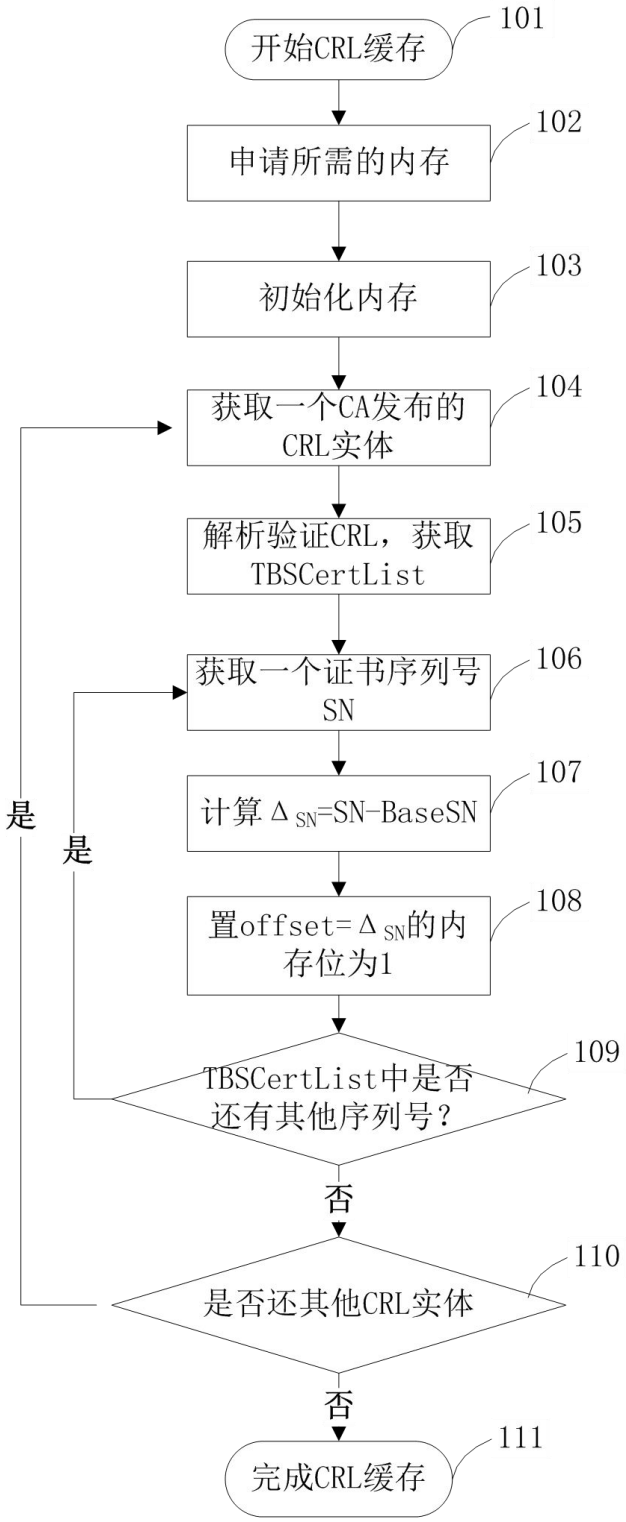

开始CRL缓存
101
申请所需的内存
102
初始化内存
103
获取一个CA发布的CRL实体
104
解析验证CRL，获取TBSCertList
105
获取一个证书序列号SN
106
计算 Δ SN=SN-BaseSN
107
置offset= Δ SN的内存位为1
108
TBSCertList中是否还有其他序列号？
109
是
否
是否还其他CRL实体
110
是
否
完成CRL缓存
111

图 1

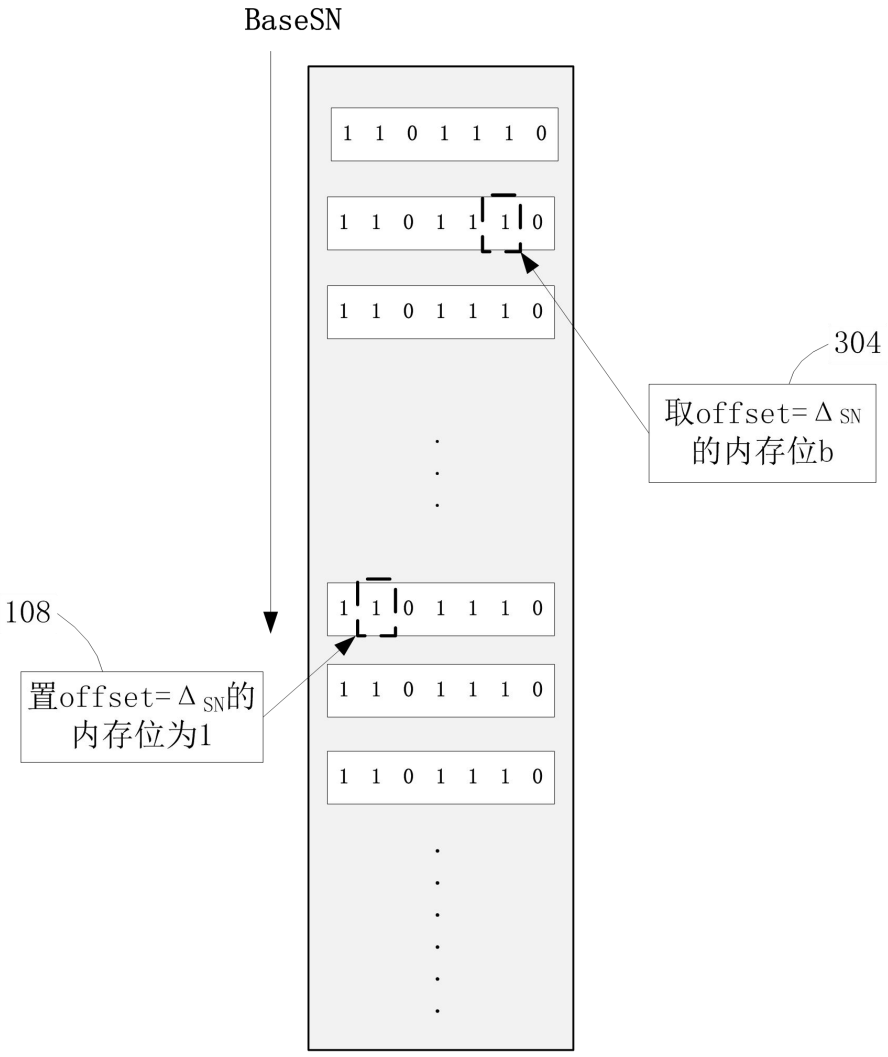

BaseSN
1 1 0 1 1 1 0
1 1 0 1 1 1 0
1 1 0 1 1 1 0
304
取offset=Δ SN
的内存位b
108
置offset=Δ SN的
内存位为1
1 1 0 1 1 1 0
1 1 0 1 1 1 0
1 1 0 1 1 1 0

图 2

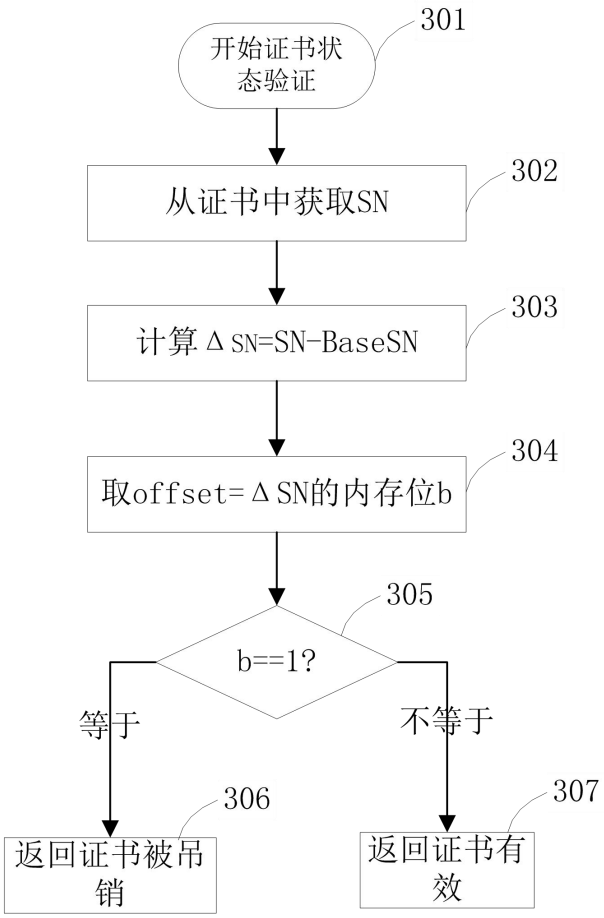

301
开始证书状态验证
302
从证书中获取SN
303
计算ΔSN=SN-BaseSN
304
取offset=ΔSN的内存位b
305
b==1?
等于
不等于
306
返回证书被吊销
307
返回证书有效

图 3