一种新型在线证书状态响应方案

敖显林[1,2],杨 林[2],杨 峰[2],申志军[2]
(1. 解放军理工大学 指挥自动化学院,江苏 南京 210007;
2. 总参第 61 研究所,北京 100039)

摘 要:证书撤销信息的发布成为了 PKI 系统大规模化的瓶颈,传统的证书撤销方案因为存在可扩展性差、实时性不强、交换数据量大等原因,不能适用于大型 PKI 系统中。针对以上问题,从理论上提出了一种新的证书撤销方案 OLMiniCRL,新方案使用在线查询响应模式,采用 MiniCRL 压缩策略和 NOVOMODO 预签名方案,以精简的证书段的状态作为一个证书状态查询的响应。与传统的在线查询响应模式相比,新方案使用数字签名保障了数据的安全完整性,使用单向的 Hash 函数链保证了通信的实时性,大量减少数字签名的次数和数据处理量,降低服务器资源消耗,采用预签名方案能够提高用户查询的响应速度,具有较好的实时性、精简性和可扩展性,能够适用于对实效要求较高的大型 PKI 系统中。

关键词:公钥基础设施;证书撤销;MiniCRL 技术;证书段
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2013)10-0130-04
doi:10.3969/j.issn.1673-629X.2013.10.033

A New Online Certificate Status Response Scheme

AO Xian-lin[1,2], YANG Lin[2], YANG Feng[2], SHEN Zhi-jun[2]
(1. Institute of Command Automation, PLA University of Science and Technology, Nanjing 210007, China;
2. The 61st Institute of General Staff, Beijing 100039, China)

Abstract: The publishing of the certificate revocation information is the bottleneck problem for the development of the Public Key Infrastructure (PKI) system. The conventional schemes of certificate revocation cannot apply to the large-scale PKI system due to its bad expandability, low real-time performance, large switched data and so on. In view of the questions mentioned above, a new certificate revocation scheme is proposed called OLMiniCRL. The new certificate revocation scheme used an on-line inquiry-response mode based on the MiniCRL compression strategies and the NOVOMODO pre-signature scheme with an efficient and simple message of certificate segment as a response to an inquiry. Compared with conventional on-line inquiry-response mode, the new certificate revocation scheme using the digital signature ensures the data security and integrity, applying the one way Hash function guarantees the real-time performance, which reduces drastically the number of digital signature so as to slow down the server resource consumption. Besides, the pre-signature scheme improves the speed of a response, has a good real-time performance, suitable expandability, which is applicable to the large-scale PKI system with a high demand of real-time performance.

Key words: PKI; certificate revocation; MiniCRL; certificate segment

0 引 言

公钥基础设施(Public Key Infrastructure, PKI)以公钥证书为基础,实现了网络通信的保密性、完整性和不可抵赖性[1]。公钥证书的有效性是保证 PKI 系统能够正常运行的前提条件。一般情况下,证书的有效性由证书中的有效日期所限定,然而,现实中的一些情况可能使得证书在有效期内变得无效(如密钥丢失等)。当一个证书被提前过期时,PKI 系统应当尽最大努力将证书撤销的信息发布给系统中有可能用到该证书的所有用户,以保证用户通信的安全可靠。证书撤销信息的发布是 PKI 系统中的关键操作。

当前,随着网络的发展和网络安全的需求,PKI 系统的普遍化和大型化已经成为了一种发展趋势。然而,撤销信息的发布是 PKI 系统中消耗资源最大的操作[2],证书撤销方案的优劣直接影响着系统能否正常运行。

收稿日期:2012-12-19 **修回日期**:2013-03-25 **网络出版时间**:2013-07-24
基金项目:军内科研项目(2011ALZ026)
作者简介:敖显林(1984-),男,硕士研究生,研究方向为网络信息安全、计算机应用技术;杨 林,研究员,研究方向为网络信息安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20130724.0954.024.html

1　传统的证书撤销方案

目前,在理论和实现中有很多证书撤销的方案,这些方案主要分为两种:一种是 CA 周期发布证书撤销信息,另一种是用户在线查询证书状态。

1.1　周期性发布证书撤销信息

CRL 也称证书黑名单,是 PKIX 工作组在 RFC2459 中提出的证书撤消方法[3],在这个方法中,CA 定期发布一个签名的数据结构——证书撤消列表(Certificates Revocation List,CRL),这个列表中包含了所有被提前撤消证书的序列号和相关信息以及 CRL 的有效期。用户根据一个证书序列号是否在 CRL 中来判断当前证书是否被撤销。在这种方案中,CRL 的规模会随着撤销信息的增多而变得非常庞大,CRL 的验证周期将变得越来越长,大量用户同时更新可能会引起网络拥塞,使客户无法得到 CRL 信息。用户与服务器之间的数据交换会成为系统运行的巨大负担[4]。为了解决这个问题,许多基于 CRL 的改进方案被提出[5-6]。由于证书撤销请求到达是随机的,而信息的发布是定时的,导致 CRL 不能实时反映证书撤销信息。周期发布证书撤销信息不能使用于对实时性要求较高的 PKI 系统。

1.2　在线查询证书状态

在线证书状态响应协议(OCSP)是 PKIX 工作组在 RFC2560 中提出的协议[7],作为 CRL 的补充和完善,它为用户提供了一种名为 OCSP 响应器的可信第三方获取在线撤消信息的手段。它是目前使用最广泛的证书状态查询机制。在这种机制中,用户每次和 CA 交互的只是一个或多个证书的状态信息,而不再是完全的证书撤销信息,减少了用户和 CA 的数据交换量。相对 CRL 而言,OCSP 具有更强的实时性。OCSP 协议采用的是请求响应实时应答模式,当系统规模变大时,用户基数很大,OCSP 服务器负担会变得越来越大,及时地向用户反映撤销证书状态成为系统瓶颈,OCSP 需要对确定的回复进行数字签名,数字签名对资源的占用较多,尤其是当请求数量比较大的时候,服务器可能会耗尽资源无法完成正常工作[8]。

1.3　Novomodo

为了解决 OCSP 数字签名时占用系统资源多的问题,一些学者提出用其他方法取代数字签名,减少系统消耗。Novomodo 是 Silvio Micali 在 1997 年提出的一种预签名方法,这种方法用 Hash 函数的单向性保证数据的安全[9]。在这种方案中,当 CA 为用户颁发一个证书时为证书设置两个值 Y_{365}(以一个证书的有效期为 365 天为例)和 N_1,其中 N_1 来源于随机数 N_0 过一次 Hash 变换所得,Y_{365} 源于随机数 Y_0 经过 365 次 Hash 变换所得。CA 将 $N_0, Y_0, Y_1, \cdots, Y_{364}$ 保密,并将 Y_{365}, N_1 与证书信息绑定并公开。当用户向服务器发送证书状态申请时,服务器根据当前时间(以证书发布后的第 i 天为例)和证书的当前状态向用户发送 Y_{365-i}(表示当前有效)或 N_0(表示证书已被撤销)。用户接收到服务器响应后将所得数值经过一次 Hash 变换后与 N_1 比较,如相同,则判定证书已无效;或将数值经过 i 次 Hash 变换后与 Y_{365} 比较,如相同,则判定证书此时有效。在这种方法中,响应器不需要对每次的回复进行数字签名,可有效地缩短系统的响应时间和系统的资源消耗。尽管 Novomodo 这种证书撤销方案没有被广泛使用在 PKI 系统中,但是它提出的单向 Hash 链的使用方法被用在了其他的改进方案中[10-11]。

2　MiniCRL

MiniCRL 是一种精简的撤销信息存储结构,它是美国 Corestreet 公司研究的证书撤销方案,曾在 2010 年运用于美国国防部 PKI 系统中,将证书撤销信息从 175 M 压缩至 4 M,压缩比例大于 30∶1[12]。考虑到在大多数情况下,用户在使用证书时,所关心的只是证书的有效性,对证书的撤销日期、原因等信息并不关心。MiniCRL 除去了证书撤销日期、原因等信息,仅用一个 Bit 位表示一个证书的状态,最大限度地减少撤销信息数据量。在一个使用 MiniCRL 的 PKI 系统中,要求 CA 按照一定的顺序颁发证书序列号(如按照递增的顺序颁发证书序列号),使得系统能够根据一个证书序列号推出它之后的下一个证书序列号。基于这样的证书顺序,只需要一个开始证书序列号,就可以使用偏移位数表示开始序列号之后的证书序列号,用 0/1 比特位表示证书是否是有效的状态。一个 MiniCRL 结构包含 3 个部分:Header、Segment、Signature,其中 Header 是传统 CRL 的部分字段,主要存储有 CA 标识、算法标识、有效日期等信息;Segment 中包含一个开始序列号和一序列的 0/1 比特位,它表示从开始序列号证书开始后的一段状态,在一个 PKI 系统中可以根据需求将证书分为多个段;Signature 部分是对 Header 和所有的 Segment 进行的数字签名,保证其完整性和安全性。

3　新型在线证书查询机制

MiniCRL 仅使用一个 Bit 位存储一个证书的状态,相对于传统的撤销信息存储结构,它在数据量精简上占有显著优势,而且 MiniCRL 证书段中包含了所有已颁发的证书状态,数据量不会随着撤销证书的增多而增大。然而,MiniCRL 和 CRL 一样属于周期性发布的撤销信息的方案,周期性发布决定了它存在撤销信息实时性不强的缺陷,使得它不能适用于那些对实时性要求较高的 PKI 系统。

在线查询是解决实时性问题较好的方法,MiniCRL 具有高精简的特征,适当调整 MiniCRL 证书段的大小,可将一个证书段作为一个证书状态查询请求的回复。一个证书段包含的是一段证书的状态,可作为证书段中所包含的所有证书的状态查询的响应,大大减少了服务器的负担。传统的在线证书状态查询机制,为了保证数据的安全性和实时性,服务器要对用户每次查询的响应加入时间信息并进行数字签名。数字签名是占用资源较大的操作。为了减轻服务器的负担,新方案结合 MiniCRL 的压缩方案和 Novomodo 预签名方案,只在撤销信息发生改变时或最大生存时间到期时进行数字签名,在保证数据安全完整和实效性的基础上,大量减少服务器数字签名次数。

3.1 新方案描述

为了能够使用 MiniCRL 的压缩策略,新方案需要 CA 按照递增的顺序颁发证书序列号,将颁发的证书按照序列号的顺序分为多个证书段。PKI 系统设置多个证书状态查询响应器,将如图 1 所示的证书段分发到各个响应器上作为用户在线证书状态查询的响应。一个新型证书段表示的是包含在该段中的所有证书当前是否有效的状态。

当系统需要撤销证书时,CA 首先找到该证书所在段,修改表示证书状态的所在位,并对修改后的证书段进行数字签名,生成单向 Hash,并设置系统定时器。服务器收到用户的申请时,首先判断要查询的证书所在证书段,后将该段作为响应发送给客户。客户得到响应后解析证书段得到证书相关信息。

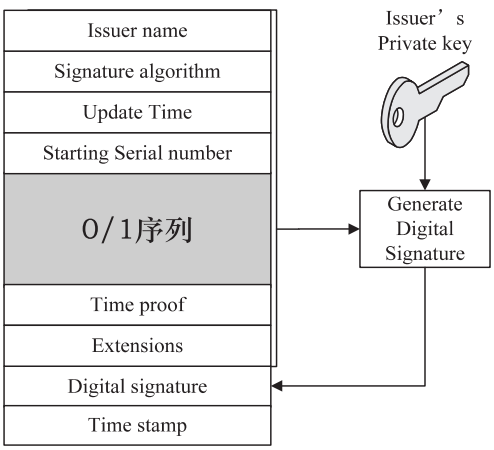

图 1 改进后的证书段结构

在图 1 所示的证书段结构中,Issuer name、Signature algorithm 和传统的 CRL 一样,是对 CRL 颁发者、加密算法的描述。

Update Time 表示的是证书段数字签名的时间。

Starting Serial number 是证书段的开始序列号,0/1 序列表示从开始序列号开始后的一段证书是否有效的状态。

Time proof 是系统在证书段数字签名时对随机数 R_0(R_0 不公开) 进行 d 次散列运算 $H^d(R_0)$ 所得。(其中 d 表示该证书段在数字签名后的最大生存时间段数)。

Extensions 是证书段的扩展字段,用户或开发人员可根据需求填入相关内容。

Digital signature 是上述几个字段的数字签名,作为用户验证,保证其安全完整。

Time stamp 用来与 Time proof、Update Time 字段指明响应的实时性。系统根据证书段的定时器时间在该证书段数字签名后的第 i 个周期点上,响应器将 $H^{d-i}(R_0)$ 填入 Time stamp 字段中。

用户在使用一个证书时,首先向服务器发送证书状态的请求,以判断证书的状态。当收到一个来自服务器的响应时,用户根据数字签名判断其安全性和完整性,根据数字签名时间 Update Time 和当前时间判断当前位于发布后的第 i 个时间周期内,将 Time stamp 进行 i 次 Hash 变换后与 Time proof 比较,如相同,判断此为当前所颁发,否则重新向服务器提出申请。

3.2 新方案性能分析

图 2 是传统的 OCSP 与新方案的简单流程对比图。在传统的 OCSP 中,当证书撤销发生时,系统将撤销信息存放于 CRL 中。当查询请求到达时,服务器从 CRL 中查找该证书,如查找成功,则证明该证书已经被撤销,否则,证明该证书当前有效,然后将证书是否被撤销的信息加入时间信息并进行数字签名后对用户的请求进行响应。

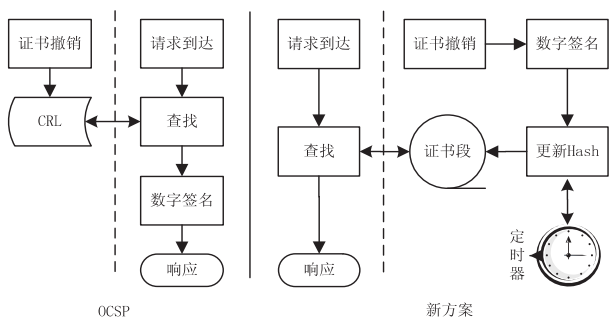

图 2 传统 OCSP 与新方案简单流程对比图

在新方案中,当有证书撤销发生时,系统查找该证书所在证书段,修改表示该证书的 Bit 位,进行数字签名,生成单向 Hash 链,并设置系统定时器,此后,系统根据定时器的时间更新证书段的 Hash 链(Time stamp)。当证书状态请求到达时,系统根据证书序列号查找该证书所在的证书段,并将其作为证书状态查询请求的响应。

(1)可扩展性:在传统的 OCSP 中,系统需要为每个到达的证书状态请求的响应进行数字签名,显然,当有大量证书状态同时到达时,系统的响应速度会受到

大量的数字签名的影响,甚至可能耗尽资源而无法工作。新方案采用 MiniCRL 压缩策略,以一个 Bit 位存储一个证书的状态,结构非常精简,同时证书段可以作为证书段中所包含的所有证书的状态查询响应,降低了服务器的数据处理量。当有证书状态请求到达时,系统将该证书所在的证书段作为响应传递给用户,而不需要进行数字签名。因此,当 PKI 系统增大时,新方案能够有效减轻系统的负担,具有较好的可扩展性。

(2)安全性:新方案使用数字签名保证数据的安全完整性。单向的 Hash 函数具有不可逆的特征,新方案使用 Hash 函数的单向性能够保证通信的实效性。

(3)实时性:在传统的 OCSP 中,当有证书请求到达时,系统在 CRL 中查找该证书,因此 CRL 的更新策略影响着消息的及时性。在一些实际的系统中,OCSP 作为 CRL 补充撤销方案,OCSP 就是在定期更新 CRL 中查找证书,而定期更新的 CRL 不能保证撤销信息的实时性。在新方案中,当有证书撤销发生时,服务器对该证书所在的证书段和相应位进行更新并重新进行数字签名,保证证书撤销信息实时性、周期性地发布单向 Hash 函数保证通信的实时性。从理论上说,在新方案中用户使用证书时查询所得到的响应就是该证书的当前状态。

(4)响应速度:当一个证书查询到达时,OCSP 服务器经过查找、数字签名后响应,在新方案中,服务器只需查找到证书所在的证书段,不用数字签名即可响应。OCSP 服务器在 CRL 中查找证书,随着 PKI 系统的增大,CRL 随之增大,查找证书的时间变得越来越长,极大影响了服务器响应速度,新方案中的证书段按序存储着所有已颁发的证书的状态,不会随着撤销证书的数量增多而增大,因此当证书查询到达时,服务器是在一个按顺序排列的数据中查找证书段。相较而言,新方案在响应速度方面更具有优势。

3.3　实验结果

为了测试新方案的实际性能,依托实验室搭建实验平台,实验环境如下:在 Windows 环境下,采用 OpenLDAP 作为证书状态数据库,服务器/客户端均使用 Delphi 语言开发,所使用机器均为 P4 3.0 GHz 处理器,内存为 1 GB 的普通 PC 机,连接环境为一小型局域网。

实验室中,拟在一个证书序列号连续递增的包含 100 W 个证书 PKI 系统中,每个证书段包含 1 000 个已签发证书状态。分别测试撤销证书数量为 1 k ~ 100 k,传统 OCSP 与新方案服务器的响应时间,每种情况进行 100 次试验求平均值,得到的试验结果如图 3 所示。

从图 3 可以看出,新方案的响应速度在整体性能上优于传统 OCSP,当系统规模增大时(撤销证书数量增多),传统 OCSP 的响应时间随之增长,新方案的响应时间基本上不变。实验结果表明,新方案较之传统 OCSP 具有更好的性能,当系统增大时具有良好的可扩展性。

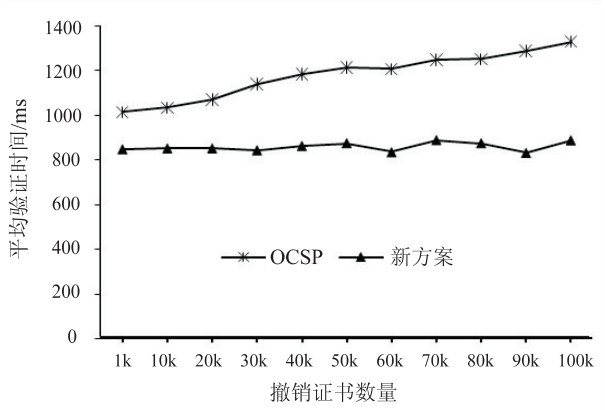

图 3　新方案与 OCSP 响应时间对比图

4　结束语

随着网络的发展和网络安全的需求,PKI 系统的普及和大型 PKI 系统的建立成为了一种发展趋势,撤销信息的发布是大型 PKI 系统中消耗资源最大的操作,性能良好的证书撤销机制对于大型 PKI 系统有着非常重要的意义。文中通过分析传统证书撤销机制的不足,结合 MiniCRL 压缩方案和 Novomodo 预签名方案从理论上提出了一种新的证书撤销方案。通过理论分析和实验结果可以看出,新的方案在保证数据安全性和实时性的基础上可有效地减少服务器的负担,从整体上提高系统的响应速度,改善了系统性能,具有较好的可扩展性。新方案适用于规模较大对实时性要求较高的 PKI 系统。

参考文献:

[1]　余　堃,郑方伟. PKI 原理与技术[M]. 成都:电子科技大学出版社,2007.

[2]　Berkovits S, Chokhani S, Furlong J A, et al. Public key infrastructure study[R]. [s. l.]: MITRE Corporation for NIST, 1994.

[3]　Internet X. 509 public key infrastructure certificate and CRL profile[S]. RFC 2459, 1999.

[4]　陈水霞. PKI 中证书撤销机制分析与研究[D]. 太原:太原理工大学,2010.

[5]　郑志勇,余舟华,徐　蕾. 一种基于分段 CRL 的改进方案[J]. 计算机应用与软件,2009,26(12):271-272.

[6]　牟　颖,全太锋,袁　丁. 一种新型的证书撤销列表[J]. 计算机工程,2007,33(12):169-171.

[7]　X. 509 internet public key infrastructure online certificate status protocol OCSP[S]. RFC 2560, 1999.

(下转第 166 页)

从该直方图可以看出,零出现的次数非常多,故有理由认为该计数数据出现了零膨胀现象。同时从图 3 可以看出图像类似于零膨胀的泊松分布统计直方图。在上述分析的基础上,文中对该实际数据考虑零膨胀泊松回归模型并对其进行分析,具体的,用极大似然估计算法得到相应的参数估计值 $a = -3.34$, $b = 1.84$, $\omega = 0.10$, 同时根据(7)式可得 score 检验统计量 $S = 448.67$,对应 $\chi^2_{1,0.01} = 6.637$,则拒绝原假设认为该数据存在明显的零点膨胀。因此,对上述实际数据考虑 ZIP 回归模型是合理的。

根据参数估计值可知当车流量控制在 1.8 万辆/日以内交通事故发生的概率几乎为零,当车流量达到 1.8 万辆/日以上交通事故发生的频率会明显增加,并会随着车流量的继续增加而导致交通事故的发生频数不断增大。所以当车流量即将超过 1.8 万辆/日时有关部门就应采取相应的措施,在极端天气出现时,更应及时控制好车流量并提醒驾驶员保持车距。

此外,文中还从贝叶斯方法的角度对该数据进行了分析,得到参数估计结果见表 2,该结果和前述极大似然估计结果是一致的。

表 2 各参数的估计值和相应的标准差以及 MC 误差

node	mean	sd	MC error
a	-3.375	0.219 3	0.007 368
b	1.838	0.117 4	0.003 94
ω	0.102	0.009 918	1.339E-4

4 结束语

文章针对实际生活中所研究的存在过多零的计数数据的普遍情况,先回顾了该类情况下常使用的零膨胀泊松混合分布模型,并提出 score 检验方法来检验是否存在零膨胀。在精确的参数估计问题上采用了极大似然估计和贝叶斯方法。实例说明零膨胀回归模型对高速公路交通事故的分析和预测有很好的可靠性和实用性,是控制交通事故发生所采用的措施和决策的有力根据。另外,对于二维数据的分析,同样也可以将该方法推广到三维甚至多维的情形。

参考文献:

[1] Lambert D. Zero-inflated Poission regression with an application to defects in manufacturing[J]. Technometrics, 1992, 34(1): 1-14.

[2] Ridout M, Demetrio C G B, Hinde J. Models for count data with many zeros[C]//Proc of the Nineteenth International Biometrics Conference. Cape Town: [s. n.], 1998: 179-192.

[3] Bohning D. Zero-inflated Poisson models and C. A. Man: a tutorial collection of evidence[J]. Biometrical Journal, 1998, 40(7): 833-843.

[4] 马昌喜. 高速公路交通安全对策研究[J]. 中国公共安全, 2008(3): 168-170.

[5] 阚伟生. 路侧事故预测模型的统计分析方法研究[J]. 道路交通与安全, 2006(12): 18-21.

[6] 钟连德, 孙小端, 陈永胜, 等. 高速公路事故预测模型[J]. 北京工业大学学报, 2009, 35(7): 966-971.

[7] 陈 敏, 于静涛, 陆 建. 道路交通事故多元回归预测模型研究[J]. 公路交通科技(应用技术版), 2012(1): 175-179.

[8] 崔立志. 高速公路交通事故的灰色预测模型[J]. 科学技术与工程, 2012, 12(19): 4843-4846.

[9] Shankar V, Milton J, Mannering F. modeling accident frequencies as zeroaltered probability processes: an empirical inquiry[J]. Accident Analysis and Prevention, 1997, 29(6): 829-837.

[10] van den B J. A score test for zero-inflation in a Poission distribution[J]. Biometrics, 1995, 51(2): 738-743.

[11] Jansakul N, Hinde J P. Score test for zero-inflated Poission models[J]. Computational Statistics and Data Analysis, 2002, 40(1): 75-96.

[12] 孙大飞, 陈志国, 刘文举. 基于 EM 算法的极大似然参数估计探讨[J]. 河南大学学报(自然科学版), 2002, 32(4): 35-41.

(上接第 133 页)

[8] 张 茜, 朱艳琴, 罗喜召. OCSP 协议的改进和实现[J]. 计算机工程, 2007, 34(23): 167-169.

[9] Micali S. Novomodo: scalable certificate validation and simplified PKI management[C]//Proc of 1st Annual PKI Research Workshop. [s. l.]: [s. n.], 2002.

[10] 王 政, 赵 明, 斯雪明, 等. 基于局部签名 Hash 表的证书撤销列表方案[J]. 计算机工程, 2009, 35(1): 36-39.

[11] 李景峰, 潘 恒, 祝跃飞. 基于单向散列链的公钥证书撤销机制[J]. 小型微型计算机系统, 2006, 27(4): 642-645.

[12] Wikipedia. Common access card[EB/OL]. 2013-08. http://en.wikipedia.org/wiki/Common_Access_Card.

一种新型在线证书状态响应方案

作者： 敖显林， 杨林， 杨峰， 申志军， AO Xian-lin， YANG Lin， YANG Feng， SHEN Zhi-jun

作者单位： 敖显林,AO Xian-lin(解放军理工大学 指挥自动化学院，江苏 南京 210007; 总参第61研究所，北京 100039)， 杨林,杨峰,申志军,YANG Lin,YANG Feng,SHEN Zhi-jun(总参第61研究所,北京,100039)

刊名： 计算机技术与发展

ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2013(10)