文章编号:2095-476X(2013)02-0100-03

基于身份的数字签名在数字图书馆中的应用

杨清兰

(郑州轻工业学院 图书馆, 河南 郑州 450002)

摘要:在图书文档传递中采用基于身份的加密和数字签名,实现了对图书电子文档进行合法性和完整性校验, 给出了基于公钥证书的数字签名技术,使其在数字图书馆成功应用. 在图书电子文档传递过程中,采用基于身份的数字签名可以省去对公钥证书的管理和维护的代价,无需传递文档发送者的数字证书, 电子文档接收者也无需验证公钥证书的合法性, 从而节约了带宽,减少了计算量,大大方便了数字图书馆的用户.

关键词:数字图书馆;安全;基于身份的数字签名;公钥证书

中图分类号:TP309 **文献标志码**:A DOI:10.3969/j.issn.2095-476X.2013.02.023

The application of ID-based signature scheme in digital library

YANG Qing-lan

(*The Library of Zhengzhou University of Light Industry*, *Zhengzhou* 450002, *China*)

Abstract: the validity and integrality of the document were verified using ID-based digital signature and encryption during the transmision of E-books and the digital documents, and the application of ID-based signature scheme in digital library was proposed. The results showed that the cost of the management and maintain of certificates for public key users can be omitted duiring the transmission of E-books and the digital documents. During sending a digital document, it does not to transmit the sender's public key certificate, and the receiver of the digital document does not to verify the validity of the public key certificate, so it saves the width and reduces many computation, which provides more convenience for the users of digital library.

Key words: digital library; security; ID-based digital signature; public key certificate

0 引言

图书馆的数字化是图书馆建设的一个重要内容,特别是随着计算机技术和现代通信网络的发展,虚拟数字化图书馆系统发展受到了广泛的关注. 数字签名技术是现代密码学研究的一个重要内容. 数字签名是在数据单元后面附加上一些校验数据, 这些数据需要利用加密技术对数据单元进行加密变换才能产生. 数字签名具备以下主要特点[1]:不可伪造性;保证消息的完整性;不可否认性. 数据的接收者能够根据数字签名验证数据单元的来源、数据的完整性, 并能防止恶意用户伪造校验数据. 任何人都可以通过用户的公钥验证数字签名的合法性, 并验证电子文档的完整性,实现对数据源的

收稿日期:2013-01-07

基金项目:国家自然科学基金项目(61272525)

作者简介:杨清兰(1973—),女,河南省邓州市人,郑州轻工业学院助理馆员,主要研究方向为数字化图书馆和信息资源共享.

认证. 由于数字签名有以上特点, 其在电子商务、电子政务、网络通信、信息安全中有着广泛的应用. 数字签名可分为 2 类:基于公钥证书的数字签名[2-3]和基于身份的数字签名[4]. 与基于公钥证书的数字签名方案相比, 基于身份的数字签名方案有明显的优势,即不需要公钥证书, 从而大大简化了公钥管理的过程; 另外, 用户在对电子文档进行数字签名验证时,无需传递和验证公钥证书,从而节约了带宽,减少了计算量. 目前, 数字签名技术主要是通过公钥密码技术实现的. 许多学者对图书馆数字化的理论和实践进行了有益的探索. 例如,张建中[5]以中南工业大学图书馆电子阅览室为例, 给出了图书馆多功能电子阅览室网络系统的设计与实现;董晓霞等[6]利用面向对象和远程控制技术对网络和数据库操作进行了封装, 给出了一种新的电子阅览室管理系统;安琳等[7]利用 RSA 加密算法对数字图书进行加密,实现了数字图书内容的安全性和流通范围的有效控制;董理文[8]给出了基于公钥证书的数字签名技术在数字图书馆中的应用, 以实现对图书电子文档传递的完整性、认证性.

文献[8]的方案需要使用公钥证书, 这就需要一个证书生成机构为所有的用户生成公钥证书, 系统需要对公钥证书目录进行管理和维护, 这会增加系统的代价. 另外, 在向用户发送图书电子文档时, 需要同时将发送者的公钥数字证书发给读者, 这不可避免地会增加带宽的需要, 而且读者在打开图书电子文档前,需要先通过发送者的公钥证书验证公钥的合法性, 这也无疑增加了计算量.

为保证图书文档传递的保密性, 控制图书的流通范围,还可以引入基于身份的加密算法, 对传递的电子文档利用用户的公钥(即用户的身份 ID)进行加密, 使得只有合法的用户(即身份为 ID 的用户)才能利用自己的私钥解密电子文档阅读相关的内容. 比如, 可采用 D. Boneh 等[9]提出的基于身份的加密技术,或者采用文献[10 - 11]中所讨论的基于身份的加密技术对电子文档进行加密. 鉴于此, 本文将基于身份的数字签名引入数字图书馆,以期方便数字图书馆的用户.

1　使用基于身份的数字签名实现图书电子文档的安全传递

基于身份的数字签名应用在数字图书馆中,用于图书电子文档的安全传递, 保证电子文档传递的完整性、认证性、不可篡改性. 用图书馆的名字 library 代表图书馆的公钥,用 key_library 代表图书馆的私钥,由于是在基于身份的环境下构建, 因此无需设立额外的证书管理机构 CA. 数字图书馆的用户 user 在使用图书馆的资源之前,需先获得自己的私钥, 而用户的个人身份信息(如姓名、E-mail、电话等)可以用作自己的公钥.

假定 user 代表一个用户的身份信息,即在这里用 user 来代表用户的公钥,为获得自己的私钥, 用户需向 KGC 注册申请自己的私钥, KGC 通过一个安全的信道将用户的私钥 key_user 发送给用户.

合法的用户 user 可以向数字图书馆 library 申请图书电子文档 document. library 作为图书电子文档的发送端,执行以下步骤:

1)为限制 document 的流通范围, library 利用 user 公钥和基于身份的加密技术对 document 进行加密得到密文 ciphertext.

2)对 ciphertext 进行压缩得到消息摘要,用 message 代表消息摘要.

3)library 利用自己的私钥 key_library 对 message 进行基于身份的数字签名, 得到签名 signature.

4)library 将 signature 和 ciphertext 发送给申请图书资源的用户.

在接收端, 合法的用户通过以下步骤获得 document, 并对其进行校验:

1)用户在接收到 signature 和 ciphertext 后, 需要先利用数字图书馆的公钥 library 验证数字签名 signature 的合法性:如果不合法, 则拒绝接收;若合法,说明 ciphertext 没有受到篡改, 并保持了图书电子文档的完整性, 则用户执行以下步骤.

2)用户利用自己的私钥 key_user 解密 ciphertext 而得到原始的图书电子资源 document.

3)用户阅读电子文档, 并向 library 传送接受确认签名书.

在上述的方案中需要用到基于身份的加密和数字签名, 而这些技术可以采用文献[9 - 11]中提出的基于身份的签名和加密方案.

以上的注册申请私钥过程、发送端和接收端的工作步骤见图 1.

2　效率和安全分析

1)本文采用了基于身份的数字签名技术来对文档进行完整性校验和合法性检验. 由于不需要公

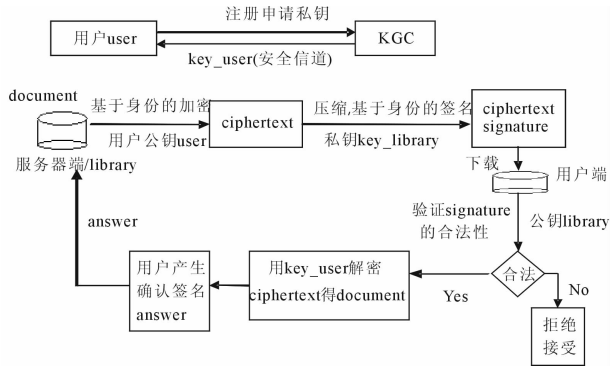

图 1 基于身份的数字签名实现
图书电子文档的安全传递结构图

钥证书,用户传送电子文档无需传递验证公钥证书,接收端也无需验证公钥证书,从而节约了带宽和计算量,方便了用户. 另外,基于身份的环境省去了对公钥证书目录的管理和维护,从而节约了成本和代价.

2)在图书电子文档传递过程中,传递的是 document 的密文 ciphertext. 只有合法的用户 user 才能利用自己的私钥 key_user 解密 ciphertext 得到 document. 即使 ciphertext 在网络传递过程中被非法用户截获,由于不知道 key_user 而无法解密 ciphertext 得到可阅读电子文档. 因此,这就控制了 document 的流通范围.

3)在 library 给 user 发送电子文档时,将自己的签名 signature 发送给用户. 这样,如果 ciphertext 在网络传递中被他人篡改、删除,都会导致 signature 无法通过用户的验证. 这种措施保证了文档在网络传递过程中的完整性,并能保证 document 认证及其正确来源.

3 结语

本文利用基于身份的数字签名和加密技术,在图书电子文档传递中采用基于身份的加密和数字签名,保证了图书电子文档在传递中能够进行合法性和完整性校验,实现了基于身份的数字签名技术在数字图书馆的应用. 结果表明,与基于公钥证书的数字签名在数字图书馆中的应用相比,在图书电子文档传递中采用基于身份的数字签名和加密技术,不仅能够保证图书文档具有完整性和可校验性,而且可以有效控制图书电子文档的流通范围,具有更高的安全性,而且节约了带宽,减少了计算量,省去了对公钥证书目录的管理和维护,从而大大方便了数字图书馆的用户.

参考文献:

[1] 辛向军. 几种具有附加性质的数字签名体制的研究[D]. 西安:西安电子科技大学,2007.

[2] Schnorr C P. Efficient signature generation by smart cards [J]. Journal of Cryptology,1991,4(3):161.

[3] Xin X J,Tong Y Z,Li J L. Pairing-based signature scheme with strong security and tight reduction [J]. Journal of Computational Information Systems, 2011, 7(5): 1508.

[4] Sato C,Okamoto T,Okamoto E. Strongly unforgeable ID-based signatures without random oracles [C]//ISPEC 2009, Berlin: Springer-Verge,2009:35 - 46.

[5] 张建中. 图书馆多功能电子阅览室网络系统的设计与实现[J]. 图书情报工作,1999(3):37.

[6] 董晓霞, 马自卫. 数字时代电子阅览室管理系统的设计和实现[J]. 现代图书情报技术,2004(2):29.

[7] 安琳,武学师,刘玉珍. 基于改进式 RSA 加密算法的高校网络数字化图书阅览系统的研究[J]. 高校图书馆工作, 2010(3):50.

[8] 董理文. 数字签名技术在数字图书馆中的应用[J]. 图书馆论坛,2004, 24(5):111.

[9] Boneh D, Boyen X. Efficient selective identity-based encryption without random oracles [J]. J Cryptol, 2011, 24:659.

[10] 杨波. 现代密码学[M]. 北京:清华大学出版社, 2007.

[11] Stinson D R. 密码学原理与实践 [M]. 北京:电子工业出版社, 2003.