面向对象的数字签名在公文传送中的应用研究①

Study on The Application of Object – oriented Digital Signature in Document Transmission

蔡平胜 闫乐林 （山东省教育学院 计算机科学与技术系 山东济南 250013）

摘 要： 本文把面向对象的思想引入数字签名之中，并在网络公文传送中应用。通过分析公文处理各阶段相关因素，设计出安全对象的属性和方法，建立了基于面向对象的公文传送模型。同时，简要分析了应用安全对象进行数字签名对公文安全性保护的原理和过程，解决了公文网络传送中的安全问题。

关键词： RSA 面向对象 公文传送 数字签名

1 引言

办公自动化系统(OA)是一个综合的信息系统，具备多种办公信息处理功能。随着 OA 的快速发展，许多单位和部门都采用了 OA 技术来提高办公效率和质量，其中的网上公文传送具有阶段性强、多角色参与、读取公文权限差异大的特点，是 OA 公文管理中使用频率最高、功能要求完备的一个重要组成部分。在公文网络传送的过程中需要建立良好的协同控制机制，对访问权限、数据私有性和完整性等要有很好的控制，否则会出现公文内容被修改、恶意篡改会签顺序、批示冒签等安全问题。

针对公文网络传送中存在的安全问题，本文试图利用面向对象的思想，将安全属性、访问控制表、加密算法等加入到文档中构成安全对象，并用加密和数字签名技术对安全属性进行保护，使非授权用户不能查看和修改文件的内容及访问控制表等，从而达到公文网络安全传输的目的。

2 安全对象

安全对象是在普通对象的基础上扩展而来的，安全对象中除包含一般对象中包含对象的一般属性和方法外，还包含用于对象安全控制所需的安全属性和安全方法。通常情况下，安全对象由加密的对象内容、对象的安全属性和方法、对象的访问控制表、以及用户对对象的签名组成。对象的安全属性及方法包括对象的安全有效期，对象所采取的安全服务机制的实现算法、密钥长度属性和判断用户拥有访问权限的方法。对象的访问控制表包括对象创建者、被授权访问对象的组和用户的存取权限和规则。对象的加密和签名包括对被授权用户所分配的对称密钥的加密方式、对修改部分的签名和对象创建者对整个对象的签名。在安全对象中的访问控制表、安全属性、文件内容等都应用数字签名予以保护，防止了非法修改，保证了内容的正确性、完整性。

3 公文传送中的对象签名

3.1 公文传送中安全对象的设计

公文传送的流程简单概括为：撰稿人首先起草公文，然后交上层各主管审阅，经修改交各主管部门会签，再呈报批示，最后公文发布执行并存档。公文从起草到发布全过程在网络交换中完成，其安全主要涉及用户、文件内容、文件的处理阶段等因素。因此，在安全对象中，除设置一般属性和方法外，还增加了相应的安全属性和方法。

(1) 用户属性。在安全对象中设置用户属性，用不同的编号分别代表公文的撰稿者、会签者、批示者、归

① 基金项目：山东省教育厅自然科学基金资助项目(J05G55)

档者、公文查询者。为分析方便，定义用户 C 为撰稿者、用户 A 为会签者、用户 B 为批示者、用户 D 为归档者、组 G1 为文件查询者。

(2) 文件属性。不同的用户读取公文不同的部分，故把文件分成标题区、摘要区、正文区、会签区、批示区等几个部分，对不同类型的用户设置对公文操作权限。操作权限分为 Read Only、Write、None，其关系见表 1。相应的安全属性和文件内容设置在公文安全对象中。

表 1　用户权限与公文内容的对应关系

	标题	摘要	正文	会签	批示
用户 C	R/W	R/W	R/W	R	R
用户 A	R	R	R	W	R
用户 B	R	R	R	R	W
用户 D	R	R	/	/	R
组 G1	R	R	/	/	/

(3) 安全属性和方法。为保证网络传输中公文的安全性、完整性、公正性，对公文处理的每个阶段均采用文件加密和数字签名，要在公文安全对象中设置对象的数字签名属性。安全对象中设置的加密方法、签名方法、验证方法以及权限检查方法等用来保证文件的安全、正确的传送以及数据完整性的确认。

3.2 安全对象的访问控制原理

网络访问控制分为任意访问控制和强制访问控制。在强制访问控制中，主体和客体均有固定的安全属性，这些属性在网络系统中使用，以决定某个主体是否可以访问某个客体，这些强制性的安全属性有管理部门或有操作系统自动严格按照规划来设置，任何主体和客体都不能随意更改。在这些控制方法中，常用的是访问控制矩阵，即对每一个主体使用一张表，表中列出该主体访问的所有客体，以及每个客体的访问权限。只要控制策略一定，把主体和相应受控客体放在一张表个考虑，就形成了一个访问控制矩阵。

网络公文中的表和签名属性都由文件的创建者生成，同时还分别生成用于加密文件的基本数据区、会签区、批示区、附件数据区等对应的会话密钥 Ki。起控制原理就是利用会话密钥 Ki 对相应的数据区进行加密，然后由创建者对拥有不同访问权限的用户，通过用户的 RSA 公开密钥 PKi 存取文件的会话密钥进行加密授权。同时用程序对用户存取文件的属性进行控制，达到合理、正确控制用户访问权限的目的。

由公开密钥算法的特点可知：创建者用任意用户(比如 A)的公开密钥对会话密钥 Ki 进行加密，只有拥有自身秘密密钥的用户(A)才能对加密的数据进行解密。拥有了对各个数据区进行操作的会话密钥 ki 后，用户即可以对自己相应的数据区进行读写操作。

3.3 网络公文传送的控制流程

文件发起人(即用户 C)、用户 A、用户 B、用户 D、用户组 G1 已经在本地机产生了公开密钥对 PKi 和 SKi (i=A,B,C,D,G1)。且发起人 C 已从网络获得了各自的 PKi。利用用户的 RSA 公开密钥 PKi 对存取文件的会话密钥 Ki 进行加密授权。

将一个文件 DOC1 具体划分为：标题 S1、摘要 S2、正文 S3、会签 S4、批示 S5 五部分，则会话密钥 Ki 加密的文件内容 S1、S2、S3、S4、S5。而 DOC1 的安全属性是发起人 C 在生成对象的同时所决定的，它同时受到所采用的安全算法的制约。文件访问控制表和安全属性都是由文件的创建者签名保护，防止修改和伪造。文件的各个部分传送至不同的用户手中时，各种访问权限不同的用户所见到的界面和操作权限是不同的。如"批示者(用户 B)"在接到"会签者(用户 A)"传来的文件时，能看到会签意见栏，可读却无更改的权利。

文件在实际传送时，除了本身的内容外，还将包含：访问控制表、安全属性表、控件属性设置等内容。当文件通过网络送达时，各用户将自动的调用 API 函数，检查访问控制表、控件当前的属性等的设定值，恢复出它所需的规定权限的内容。

3.4 安全对象中数字签名实现

为保证文件的来源和内容的完整性，所有对文件的修改和增加的内容都要经过作者的数字签名，并随原文件一起保存。签名时首先用 MD 函数对所需签名的内容求 Hash 摘要，然后用私有密钥对摘要进行加密，即产生了签名。因为公文从撰稿、传阅、会签、批示到最后的成文需要经过多次文本的变更，所以对每一次的变更都应由变更人进行签名保护。而每位用户接到上一位用户传来的文件后，先对不同用户在不同阶段所做的数字签名进行验证。若发现文件有改变将拒绝接受，其工作如图 1。

在图中，D1 = S1(Hash(公文草稿))，它是由撰稿者完成签名的。D2 = Hash(会签)，D5 = S(Hash(D1, D2))；它是由会签者结合撰稿者的签名和他的修改

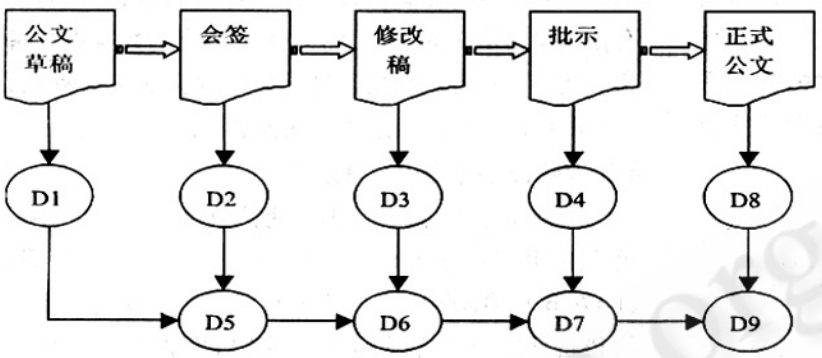

图 1　公文签名流程图

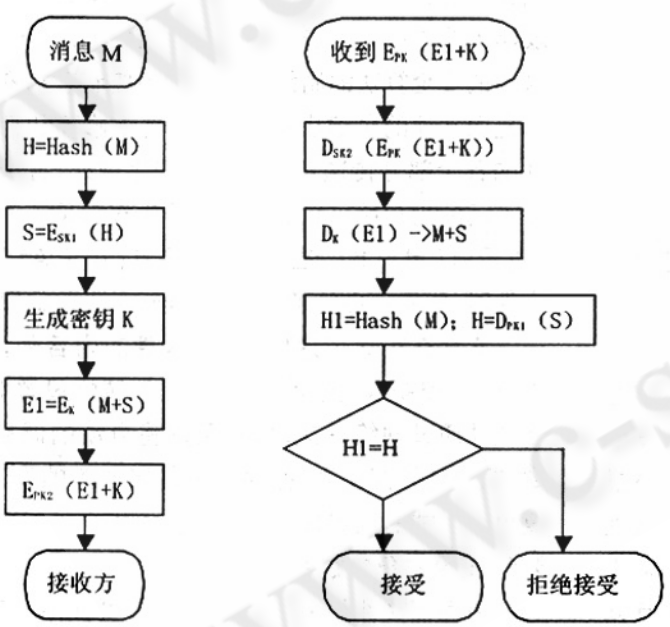

图 2　公文传送中的加密和签名的验证

(会签意见)一起求新的签名。同理，D3 = Hash(修改稿)，D6 = S(Hash(D5, D3))，D7 = S(Hash(D6, D4))，D8 = S(正式稿)；随公文对象一起保存的签名为 D1, D5, D6, D7, D9 等以及操作者相应的身份，任何有权使用该文件的用户都可以通过公文的签名来验证公文的完整性和各操作阶段作者的身份。

在文件传送中，消息的加密、签名和验证过程见图 2。

为防止将来可能出现的用户抵赖和文件纠纷的情况，当文件传送完成后，可以将包含 D1, D5, D6, D7, D9 等以及操作者相应身份的文件传送至信息中心保存起来，以便日后仲裁之用。

4　结语

本文介绍了安全对象的概念，并把安全对象应用于网络公文传送，通过设计安全对象的安全属性和方法，实现了网络公文传送中的数据加密和数字签名，保障了公文传送的安全性、有效性和完整性。

参考文献

1　卢开澄，计算机密码学[M]，北京：清华大学出版社，1999.
2　朱麟、杨季文，基于 Notes 的办公自动化系统中日志文件的应用[J]，苏州大学学报，2003，23(5)：44—48.
3　张大陆、时慧，电子公文中数字签名的设计与实现[J]，计算机应用研究，2001，(6)：78—80.
4　张江辉、李长云、马睿，电子政务解决方案——公文审批系统[J]，包装工程，2002，23(5)：59—60.
5　阮耀平，电子邮件的安全措施与实现[J]，计算机工程，1999，(10).
6　Zheng Dong, Chen Kefei. Multi - item fair exchange scheme. Journal of electronics (china), 2002, 19(4): 363 - 368.