维普资讯 http://www.cqvip.com

基于XML的多人数字签名技术研究与实现

李凤银
(曲阜师范大学计算机科学学院　山东日照 276826)

摘　要　本文基于XML提出一种新的多人数字签名方案,能够实现多人数字签名以及多方的不可否认性,基于该多人数字签名方案用Java实现了一个电子公文签发系统。

关键词　XML,数字签名,电子公文

1 引言

数字签名技术是建立在公开密钥加密体制基础上、经多次验证的较为理想的认证技术,是一种反事后抵赖的手段。传统的数字签名技术是对需要签名的信息用私有密钥进行运算,得到该信息的签名并附加在原信息上,以此来保证数据的完整性、消息来源的认证性以及消息发送方的不可否认性。这种签名方案只适合一对一通信时的签名和验证,对于有多个参与者均需签名的应用,这种签名方案无能为力。文[1]提出一种多人签名的实现方案,这种方案存在以下不足:(1)必须事先对所有的参与者人为地规定一种先后顺序,即使对签名顺序没有任何要求,参与者也必须严格按照这种顺序依次签名,所以这种方案不支持同时签名,给用户带来不便;(2)需要最后一位签名人在签名完成后将最终消息和最终签名一起发送出去,具体实现时很难要求签名者做到这一点,因为签名者一般只负责签名,不负责最终文档的发送。另外,有很多应用场合,某些参与者要求在另外一些特定参与者(不一定是全部参与者)的签名之后签名,而且这种要求不是永久的,是动态变化的,文[1]没有给出相应的解决方案。

本文基于XML提出一种新的多人数字签名方案,这种数字签名方案不仅能够有效解决上述问题,而且能够实现对文档进行部分签名,能够实现只保证文档的某一部分的完整性,其余部分保持公开留给用户修改,常规数字签名无法做到这一点,因为常规数字签名是对整个文档签名,后来用户对文档的任何改动都将使签名验证失败,签名实效。

2 数字签名技术

数字签名是指附加在数据单元上的一些数据,或是对数据单元所作的密码变换,这种数据或变换能使数据单元的接收者确认数据单元的来源和数据的完整性,并保护数据,防止被人(例如接收者)进行伪造。

传统数字签名技术是利用公开密钥加密算法中私有密钥的保密性来实现的,因为这个私有密钥除拥有者本人外无任何人知道,所以可以用它来唯一标识这个用户。用私有密钥加密的信息只能用相对应的公开密钥才能解密,从而可以实现签名的认证,保证该签名的不可否认性和不可伪造性[2]。

为了保证信息的确是发送方的原信息,没有被非法改动,可采取信息摘要算法:发送方使用一个单向函数(如SHA或MD5)从明文消息中产生一个固定长度的信息摘要,并用自己的私有密钥加密摘要,创建一个数字签名,将其与消息一起发送给接收方。接收方收到消息后用发送方的公开密钥解密签名得到真正的摘要,同时他用原来的单向函数作用于收到的消息得到另一个信息摘要,通过比较这两条信息摘要来验证消息的完整性。

在实际应用中,为实现信息的保密性,往往将数字签名技术与加解密技术相结合,发送方将签名结果加密后再发送给接收方,而接收方对接收到的信息解密后再验证签名,这种数字签名的实现步骤可描述如下:

(1)发送方A用单向函数(如SHA)从要发送的报文(P)中产生一个信息摘要M(P)。

(2)A用自己的私有密钥D_A来加密(签名)信息摘要M(P),得到数字签名$D_A(M(P))$。

(3)A利用接收方B的公开密钥E_B对得到的数字签名$D_A(M(P))$和报文(P)加密,得到$E_B(D_A(M(P)),P)$并发送给B。

(4)B接收到$E_B(D_A(M(P)),P)$后,先用自己的私有密钥D_B解密,得到签名$D_A(M(P))$和报文(P)。

(5)B用A的公开密钥E_A验证签名$D_A(M(P))$,得到信息摘要M(P)。

(6)B再用同样的单向函数对解密得到的报文P进行运算,得到信息摘要$M_1(P)$。

李凤银　硕士,研究方向:计算机网络安全技术及应用。

维普资讯 http://www.cqvip.com

(7)若 $M_1(P) = M(P)$,说明收到的报文是正确的,而且因为 M(P)是用 A 的公开密钥解密得到的,这说明它是用 A 的私有密钥加密的,而 A 的私有密钥只有他自己知道,从而验证了 A 的签名,保证了发送方 A 的不可否认性(见图 1)。

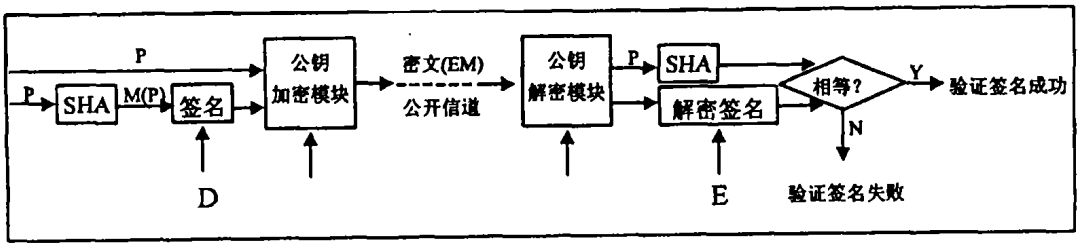

图 1 数字签名技术的实现

3 基于 XML 的多人数字签名技术

为讨论方便,我们假设签名群体中的实体(包括个人)用户共有 n 个,用 Unit1, Unit2, …, Unitn 表示,需要签名文档的用户用 User 表示。针对某个特定的文档,必须在某个签名实体之前签名的所有签名实体称为该签名实体针对该特定文档的前导实体,简称前导实体。

3.1 多人数字签名技术

在需要多人签名的场合,有些场合多个签名之间没有顺序,谁先谁后或是同时签名都是允许的;而另外有一些场合,有一些签名实体具有一个或多个前导实体,具有前导实体的签名实体必须等待其所有的前导实体都签名完成才能实施签名,缺一不可(类似于部门老总,只有看到所有相关分管领导的签名后才肯放心的签名)。于是这些签名实体形成了一种偏序关系,具有先后关系的签名实体必须严格按照先后顺序进行签名,而没有先后顺序的签名实体可以按任意顺序或同时进行签名。显然,没有签名顺序要求的情况是有签名顺序要求的一个特例,不失一般性,我们只讨论有特定签名顺序要求的情况。

假设用户 User 有一份文档 P 需要 Unit1, Unit2, Unit3, Unit4, Unit5 共 5 个签名实体的签名,其中 Unit2 和 Unit3 是 Unit1 的前导实体,而 Unit5 是 Unit3 的前导实体,其他人的签名没有顺序要求。签名步骤描述如下:

(1)用户 User 首先将源文档 P 发送给 Unit2、Unit5 以及没有顺序要求的 Unit4 请求签名;

(2)Unit2、Unit5 和 Unit4 这三个签名实体同时对源文档进行签名,生成三个签名文档 Signature2、Signature5 和 Signature4 并发送回 User;

(3)User 再将 Signature5 和源文档 P 一起发送给 Unit3 签名实体请求签名;

(4)Unit3 检查其前导实体 Unit5 的签名 Signature5 是否存在,若存在则验证 Signature5,只有验证通过才对源文档进行签名并将签名结果 Signature3 发送回 User,否则拒绝签名,并给出要求其前导实体 Unit5 先签名的提示信息,多人签名异常终止;

(5)User 将 Signature2、Signature3 以及源文档 P 发送给 Unit1 请求签名;

(6)Unit1 检查其所有前导实体(Unit2、Unit3)的签名是否都存在,并依次验证,所有前导实体的签名都验证通过才对源文档进行签名得到 Signature1 发送回 User,否则拒绝签名并给出要求其前导实体 Unit2、Unti3 先签名的提示信息,多人签名异常终止;

(7)用户 User 将接收到的所有签名实体的签名以任意的顺序整理成签名文档,并和源文档一起发送给特定的接收用户,或者在一定范围内广播给特定的接收者,从而实现了多人签名。

接收方收到多人签名的文档后,可以阅读该文档并可验证该文档的任何一份签名,从而保证了签名任何一方的不可否认性。

3.2 基于 XML 的多人数字签名文档结构

一个基于 XML 的多人数字签名文档结构描述如下:

```
<? xml version="1.0"? >
<SignatureDoc>
  <Signature-Unit1>
  </Signature-Unit1>
  <Signature-Unit2>
  </Signature-Unit2>
    …
  <Signature-Unitm>
  </Signature-Unitm>
</SignatureDoc>
```

其中 <Signature-Uniti> … </Signature-Uniti>(i=1,2,…,m)代表第 i 个签名实体 Uniti 对源文档的签名,每个签名实体的签名采用以下文档结构:

```
<Signature>
  <SignedInfo>
    <CanonicalizationMethod> … </CanonicalizationMethod>
    <SignatureMethod> … </SignatureMethod>
    <Reference URL="…">
```

维普资讯 http://www.cqvip.com

```
<Transforms> … </Transforms>
<DigestMethod> … </DigestMethod>
<DigestValue> … </DigestValue>
<SignatureValue> … </SignatureValue>
</Reference>
</SignedInfo>
<KeyInfo> … </KeyInfo>
<Object> … </Object>
</Signature>
```

其中，<Reference>…</Reference>为签名描述单元，根据需单独签名的文档段的个数，该组成部分可以有多个。

XML多人数字签名的正确性基于传统数字签名技术的正确性，已经得到证明和广泛的认可[3]。

4 基于XML的多人数字签名技术的实现

本文将多人数字技术应用到电子政务系统中，实现了一个电子公文签发系统(见图2)，该系统由数字签名管理(DSM)模块、签名实体用户Unit和普通用户User三类实体组成。DSM(由服务器充当)负责为系统中所有用户提供多人签名服务，并将签名成功的文件连同签名一起发送给一个或多个最终用户。签名实体用户有为其他用户签名的特权，普通用户没有签名的权利，但可以申请DSM对文件进行多人签名。系统中所有用户之间相对固定的前导关系，存到前导实体数据库中并由DSM在实现多人签名过程中动态更新。

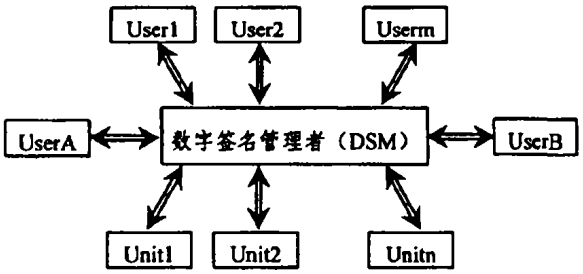

图2 电子公文签发系统结构图

在该系统中，如果用户UserA需要签发电子公文，则UserA首先生成一份XML请求签名文档，其中给出源文档、签名要求以及签名文档的接收方等信息的描述，然后将该请求签名文档提交给签名文档管理员(DSM)，由DSM负责进行文档的签名和发送工作。

该系统中，DSM是整个系统的核心，其内部由接收、发送、签名验证、签名请求分析处理和签名重组五个功能模块和前导实体数据库组成(见图3)。

接收模块负责接收所有用户的签名请求和签名实体用户的签名，并分别交给签名分析处理模块和签名验证模块进行处理。还可以接收签名实体用户的拒签信息，若是因为前导关系错误拒签，则调整前导数据库，通过签名请求分析处理模块重新提出签名请求；若是不同意源文档的观点拒绝签名，则将源文档附上拒签信息通过发送模块退还给原请求签名用户。

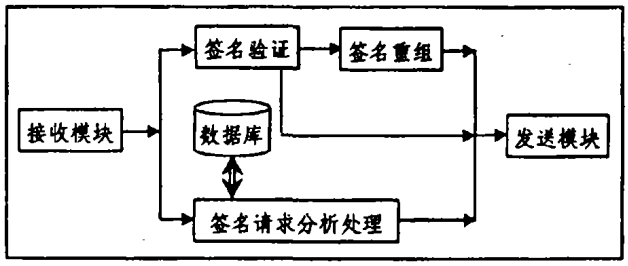

图3 DSM组成结构图

签名请求分析处理模块负责分析用户的签名请求，将合法签名请求发送一份给签名重组模块，并根据请求文档中的签名要求，生成多个单签名请求文档发送给各签名实体请求签名。

签名验证模块验证由各签名实体发送回来的签名的有效性，验证不通过则生成签名失败信息，经由发送模块发送回签名实体，要求签名实体重签名；验证通过则将该签名发送给签名重组模块。

签名重组模块负责接收由验证模块传来的各签名实体的合法签名，根据签名请求文档的描述，在某份文档的所有签名到齐后，将该源文档、相对应的所有签名以及最终用户的描述重组成一份签名的XML文档交给发送模块。

发送模块负责所有文档的发送工作，将签名失败信息发给签名实体要求重签名，将由签名重组模块发来的成功签名的XML文档发送给最终用户(可以是多个)。

前导实体数据库中存放着签名群体中各签名实体间的相对固定的前导关系，该数据库由签名请求分析处理模块在签名过程中进行动态更新。

DSM中，只有签名验证模块要进行签名验证的计算工作，其他模块只是进行XML签名文档的接收、重组和发送等简单的管理工作，其负担的增加是非常有限的。

该系统是基于WWW访问模式实现的，用户端需要配备有PC机，安装支持XML的浏览器(Internet Explore 5.0或Netscape Navigator 5.0或以上版本)。整个系统的签名算法采用RSA算法。用户端的摘要算法、签名算法、XML文档的生成算法用Java Applet实现，服务器端(DSM)的接收、发送、签名验证、签名重组、签名请求分析处理等功能模块及相关算法用Java Servlet实现，签名实体数据库用Microsoft SQL Server 2000实现。该实现方案的特点是：对用户端的硬件要求比较低，用户端的加解密的计算量比较小。实验结果表明这一方案在实际应用中是可行的。

(下转第114页)

维普资讯 http://www.cqvip.com

密碎片 $s^j_{k-1,i}$给 P_i，广播 $h^{c^j_{k-1,i}}$。P_i 如下验证收到的碎片 $s^j_{k-1,i}$是否正确：

$$h^{c^j_{k-1,i}} = v_{k-1,i} h^{c^i_{k-1,0}} (h^{c^i_{k-1,1}})^j \cdots (h^{c^i_{k-1,t}})^{j^t} \pmod p, j \in M \quad (5)$$

如果等式成立，则收到的碎片 $s^j_{k-1,i}$是正确的；否则，则不正确。P_i 利用至少 $t+1$ 个正确的碎片可以重构 $s_{k-1,i}$的共享多项式 $d^i_{k-1}(x) = c^i_{k-1}(x) + g_{k-1}(x)$，因为 $d^i_{k-1}(j) = c^i_{k-1}(j) + g_{k-1}(j) = w^j_{k-1,i} + s_{k-1,j} = s^j_{k-1,i}(j \in M)$，且 $d^i_{k-1}(i) = c^i_{k-1}(i) + g_{k-1}(i) = 0 + s_{k-1,i} = s_{k-1,i}$。这恢复了 P_i 的秘密碎片 $s_{k-1,i}$。

现在我们将方案组合为一个完整的方案如下：在时间周期 $k=0$，秘密分发者进行秘密碎片的产生和分发；在时间周期 $k(=1,2,\cdots)$，顺序执行秘密碎片检测、损坏秘密碎片恢复和秘密碎片更新；当系统需要重构秘密时，执行秘密重构。

容易看出，在秘密碎片检测和损坏秘密碎片恢复过程中，攻击者要获取相关秘密信息，也必须解离散对数问题。因此，整个方案的安全性是基于离散对数问题的难解性的。即使在一个时间周期内，$n-k-1$ 个秘密碎片被敌手毁坏或丢失，其余 $k+1$ 个秘密碎片完好无损但有 k 个被敌手偷听，我们的方案仍然可以安全地进行下去。

结论 基于离散对数问题的难解性，提出一个周期更新的可验证秘密共享方案，方案在秘密信息保持不变的情况下，定期对秘密碎片进行更新。参与者可以对自己的秘密碎片和其他成员出示的秘密碎片进行验证。为了保证秘密的完整性和可用性，方案还具有检测损坏的秘密碎片和恢复正确的秘密碎片的功能。方案最大可以预防在一个时间周期内，$n-k-1$ 个秘密碎片被敌手毁坏或丢失，其余 $k+1$ 个秘密碎片完好无损但有 k 个被敌手偷听。由于方案始终有一个可信的分发者参与，与文[3]相比，我们方案的通信量很小，有效性大大提高。

参考文献

1 Shamir A. How to share a secret. Communications of the ACM, 1979, 22(11): 612~613

2 Blakley G R. Safeguarding cryptographic keys. In: Proc. of the National Computer Conf. 1979. Vol. 48 of American Federation of Information Processing Societies Proceedings. 1979. 313~317

3 Herzberg A, Jarecki S, Krawczyk H. Proactive secret sharing or how to cope with perpetual leakage. in Advances in Cryptology: Coppersmith D. In: Proc. of Crypto'95 (vol. 963 of Lecture Notes in Computer Science). Springer-Verlag, 1995. 339~352

4 Gennaro R, Jarecki S, Krawczyk H, Rabin T. Secure distributed key generation for discrete-log based cryptosystems. in Advances in Cryptology: Stern J. In: Proc. of Euro-crypt '99 (vol. 1592 of Lecture Notes in Computer Science). Springer-Verlag, 1999. 295~310

5 张建中，肖国镇. 可防止欺诈的秘密共享方案. 通信学报，2000, 21(5): 81~83

6 张建中，肖国镇. 一个可防止欺诈的秘密分享方案. 电子科学学刊，1999, 21(4): 516~521

7 许春香，魏仕民，肖国镇. 定期更新防欺诈的秘密共享方案. 计算机学报，2002, 25(6): 666~669

(上接第 111 页)

结束语 本文基于 XML 多人数字签名方案实现的电子公文签发系统，已在某市建设规划委员会的电子办公系统中试运行，运行结果表明该多人数字签名方案能够实现多方签名和多方的不可否认性，而且支持同时签名、按任意顺序签名、对部分文档签名。但因为在整个系统内部，所有用户数据信息均以明文形式进行传输，所以本文提出的方案不具有保密功能，对系统内部人员公开。在"电子公文签发系统"中以明文形式传输用户数据，基于两个方面的考虑：(1)如果对全部的用户数据进行加密，势必会增加整个系统的负荷，降低系统的性能；(2)在一般部门的局域网电子办公系统中，电子公文的签名主要是提供电子公文的真实性、权威性，无需对内部人员保密。

如果将该系统扩展到 Internet 上或是应用到某些高度机密的国家安全部门，则可以考虑对明文数据进行加密，使其以密文的形式传送，进一步提高系统的整体安全性。具体方法可选用对称密钥算法中的 DES(或 AES)算法，任何一次通信，都是由发方生成会话密钥，用该密钥对用户数据进行加密生成数据密文，再用接收方的公开密钥(基于 RSA 算法)对会话密钥加密生成密钥密文，然后将得到的密钥密文和数据密文一起发送给接收方。接收方用自己的私有密钥解密密钥密文得到会话密钥，然后再用会话密钥解密数据密文得到用户数据信息，从而实现了数据的保密传输，提高了系统的安全性。

随着 Internet 的发展，数字签名技术的广泛应用以及 XML 文档描述语言的日趋普及，XML 多人数字签名技术将得到进一步的应用与发展。

参考文献

1 陈晋大，郑纪蛟. 用数字签名保护网络通信安全. 计算机应用研究，2000, 9: 43~44

2 王志巍，吴丽红，王天青. 两方间收方不可否认的数字签名. 计算机工程，2001, 27(7): 107~108

3 李凤银，鞠宏伟，刘培玉. 基于 XML 的数字签名技术研究. 山东师范大学学报(自然科学版)，2003, 18(1): 21~23

4 Laurent S S. XML 基础教程[M]. 北京：电子工业出版社，