基于公钥密码算法的数字签名系统分析①

向 猛, 谢立靖

(湖南商务职业技术学院 实训部, 长沙 410205)

摘 要: 数字签名系统是电子商务,电子政务等不可缺少的安全技术. 通过探讨信息在网络传输中所面临的主要安全隐患, 并详细说明了基于公开密钥密码算法的数字签名系统的实现原理, 着重分析数字签名如何解决信息传输所面临的各种安全隐患的, 最后将数字签名和数字证书结合起来讨论 Internet 信息安全传输过程.

关键词: 公开密钥密码算法; Hash 函数; 数字摘要; 数字签名; 认证机构; 数字证书

Analysis of PKC-Based Digital Signature System

XIANG Meng, XIE Li-Jing

(Hunan Vocational College of Commerce, Training Department, Changsha 410205, China)

Abstract: Digital Signature System is an indispensible Information Safety Technology for E-commerce, E-government etc. The thesis probed main information safety hazard in the course of information transmission, emphatically explained PKC-based Digital Signature System's realization principle and selective analysised the Digital Signature System how to solve all kinds of potential safety hazard for network information. Finally, through combining Digital Signature with Digital Certificate, elaborated basic process of Internet Information secure transmission.

Key words: public key cryptographic algorithm; hash function; digital abstract; digital signature; certification authority; digital certificate

随着信息技术的迅猛发展, 电子商务、电子政务、电子银行等网络应用成为人们日常生活中必不可少的内容. 然而, 电子信息的安全性保证一直是人们所关注的焦点. 数字签名系统作为一种保证信息的完整性、机密性、抗否定性的核心安全技术, 在信息安全等级要求高的电子政务、电子政务、网上银行等应用系统的设计和实施过程中, 有着举足轻重的作用. 然而, 信息安全技术由于其多学科性、复杂性、抽象性, 导致企业或政府部门在实施这些对人们日常生活、对国家经济、社会秩序等有着重要影响的信息系统时困难重重, 有时甚至付出惨痛的代价. 本文去除或简化了信息安全管理中晦涩难懂密码算法、复杂的 PKI 体系结构, 具体的数字签名系统实现代码等一些深奥复杂的东西, 直接深入细致的探讨数字签名系统保证信息安全的整个过程, 使设计人员快速掌握高安全信息系统设计的基本架构.

1 信息网络传输过程中可能存在的一些安全隐患

1.1 信息传输过程中易受到第三方攻击

信息在网络传输过程中可能遭受到第三方的非法攻击, 攻击手段包括: 非法获取信息的内容(泄密)、篡改、重放、延迟、通信流量模式分析等等.

目前, 广泛采用“消息认证”来保护网络信息免于第三方非法攻击. 消息认证是收发双方通过产生消息认证码(MAC)来验证消息的真实性(的确是由所声称的实体发送过来的)和完整性(信息未被篡改), 同时还用于验证消息的顺序性和时间性(抗位重排,重放,延迟).

目前, 密钥相关的哈希运算消息认证码(HMAC keyed-Hash message authentication code)是实现消息认证的重要工具. 已经成为事实上的 Internet 标准, 包括 IPSec 协议在内的一些安全协议都使用了 HMAC 算法.

① 收稿时间:2012-12-19;收到修改稿时间:2013-01-11

它利用已有的Hash函数，在一个通信双方事先共享密钥的控制下，对所传输的信息进行计算，得到固定长度的信息摘要．目前主要的 Hash 函数有 MD5 和 SHA-1，其对应的 HMAC 记为 HMAC-MD5 和 HMAC-SHA1.

具体生成 HMAC 的算法较复杂，可以将 HMAC 的产生简单理解为：$h_K(x)=h(K\|x)$.

其中 h 是 hash 函数，K 是双方共享的密钥，x 是信息，产生定长的输出 hk(x).

采用 HMAC 进行消息认证的基本过程如图 1 所示:

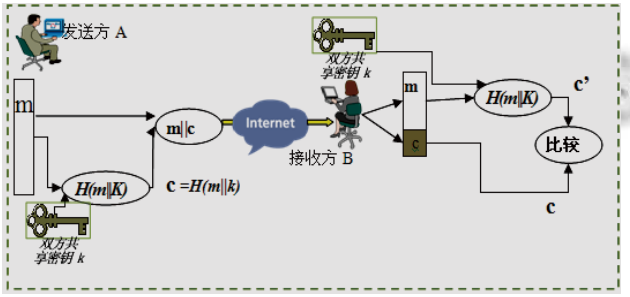

图 1　HMAC 消息认证过程

用户 A 需要将信息 m 发送给用户 B，于是 A 与 B 事先通过某种方式共享一个秘密密钥K. 首先用户 A 在共享密钥K的控制下使用选定的Hash函数来计算m的信息摘要(即计算 HMAC)得到 c=H(m||k)，然后将信息摘要追加到信息 m 的最后，一起发送给 B. B 接收到数据后，分离出信息 m 和摘要信息 H(m||k)，对于信息 m，B 使用相同的hash函数并应用两者共享的密钥K，自己计算其信息摘要(即计算 HMAC)得到 c'=H(m||k)，并将自己计算出的c'=H(m||k)与分离出来的c=H(m||k)相比较. 如果两者相等 c=c'，则 B 确定消息 m 是来自于用户 A，因为只有A才知道他们之间的共享密钥K. 并且能够发现信息在传输过程中是否被篡改过(保证了信息的完整性)，这是由于 hash 函数的不可逆运算特性决定的. 即：找出满足 H(m)=H(m')且 m≠m'的明文在计算不可行，简单的讲就是，如果报文不同，使用相同HASH函数计算出的数字摘要肯定不同. 如果再结合加密算法，就能够保证信息的机密性.

1.2 通信双方之间也存在着多种形式的欺骗行为

但不幸的是，通信双方之间也可能有多种形式的欺骗行为. 比如：发送方抵赖、接收方伪造等等. 然而消息认证却不能保护通信双方中的一方被另一方的欺骗.

在图 1 所示使用 HMAC 进行消息认证的过程中，由于发送方和接受方事先通过某种方式共享同一个的密钥 k，于是双方可能存在以下问题.

1) B 伪造一个消息并使用与 A 共享的密钥 K 产生该消息的认证码，然后声称该消息来自 A(即接收方伪造).

2) 由于 B 有可能伪造 A 发送的消息，所以 A 就可以对自己发送的消息予以否认，声称自己实际发送的消息是 B 伪造的(即发送方抵赖)，同样 A 也可以对发送的内容进行抵赖.

以上两种欺骗在现实的网络信息传输中都有可能发生，比如在电子资金传输中，接收方伪造了一个较小资金数目，然后使用与发送方共享的密钥产生该消息的认证码，并称该消息是发送方发送过来的，这就是第一种欺骗；又比如某个客户通过电子邮件向其股票经纪人发送购买某种股票的指令，但是以后这种股票大副下跌，要赔钱了，客户就否认曾经发送过相应的购买指令，说股票经纪人有伪造的能力，这个购买消息肯定是他伪造的. 这属于第二种欺骗.

除了上面提到的第三方攻击和双方之间的欺骗之外，图 1 所示使用 HMAC 进行消息认证的过程还存在着诸如：共享密钥管理交换困难、通信双方身份认证困难、无加密功能等等问题. 所以在通信双方未能建立起完全的信任关系且存在利害冲突的情况下，仅能防止第三方篡改而不能防止通信双方之间相互欺骗、不能进行身份认证的网络信息安全解决方案是明显不够的.

2　数字签名系统

数字签名系统就是解决上述一些安全问题的综合性解决方案. 可以有效解决上述两种通信双方之间的欺骗行为，同时又提供一些防止第三方攻击/欺骗的安全服务. 具体来说，数字签名能够提供 身份认证、数据完整性、抗抵赖性、防伪造 这几种安全服务.

实现数字签名系统的技术很多，这里主要讨论采用公开密钥密码技术实现的数字签名系统. 其在目前电子商务、电子政务、电子银行等安全管理中广泛采用，其基本实现过程如图 2 所示.

这里假设通信双方通过某种方式相互知道了对方的公钥(具体的公钥管理及分配参考下面第 4 小节：公钥密码体制的密钥管理—数字证书(公钥证书)).

(1) 发送方 A 将任意长度的明文信息使用 SHA-1 或 MD5 等 HASH 函数产生固定长度(如 HMAC-MD5 产生 128 位,HMAC- SHA-1 产生 160 位)的摘要 m1=H(m).

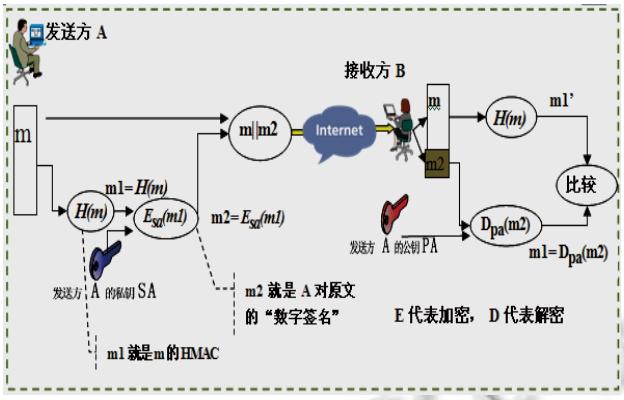

图 2 基于公钥密码技术的数字签名系统实现原理

(2) 然后A用自己的私有密钥SA对这个固定长度的信息摘要进行加密运算,就形成了数字签名 Esa(m1).

(3) 在发送时, A 将这个数字签名加到原文的后面, 一起通过网络传输给接收方 B.

(4) 接收方 B 收到原始明文和数字签名后, 分离出原文 m 和加在原文后面的数字签名 Esa(m1), 然后使用发送方A的公钥PA对数字签名进行解密运算, 得到m1, 同时对分离的原文采用相同的HASH函数计算数字摘要, 得到 m1'.

(5) B 将解密后的摘要 m1 同计算得到的摘要 m1' 进行比较, 如果m1= m1', 则说明消息在传输过程中没有被破坏或篡改过. 如果 m1≠m1', 就说明消息在传输的过程中, 被破坏或篡改过.

3 数字签名系统安全服务分析

数字签名系统是如何提供上面所说的数据完整性, 抗抵赖性, 身份认证和抗伪造性的呢?

3.1 对于第三方攻击者而言

在图 2 中, 假设文件在传输过程中, 被第三方的攻击者篡改了, 由于对于已知明文 m, 要找到另一个明文 m', 且 m≠m',使得这两者的数字摘要相同在计算上是不可行的. 那么接收方使用发送方的公钥对数字签名解密后的数字摘要与由篡改后文件计算出来的数字摘要肯定不同, 所以接收方很快就可以检测到文件被第三方篡改, 这保证了数据的完整性. 如果把发送方的明文和数字签名整体使用公钥密码算法(如 RSA)或对称密码算法(如 DES)加密, 还可以实现通信的保密性, 就防止了第三方非法获得信息的内容.

3.2 对于通信的双方而言

假设接收方 B 伪造了文件 m'(创建新文件或篡改原文件内容), 由于接收方 B 不知道发送方 A 的私钥, 无法以发送方的名义对 m'进行数字签名, 所以接收方 B 无法伪造报文, 因此具有抗接收方伪造报文的特性.

同时, 接收方为了防止发送方事后对发送文件这件事或者对文件的内容进行抵赖, 小心的保存接收到的文件 m 以及对文件 m 的签名, 当发送方抵赖时, 将收到的文件 m 以及该文件签名 Esa(m1)一起交给第三方权威机构(比如法院法官或某个权威机构), 第三方权威机构简单的使用发送方公钥解密文件的数字签名, 同时对明文 m 使用相同的 HASH 函数进行计算, 然后比较解密出的数字摘要和计算出来的数字摘要, 如果相等, 表明发送方 A 确实发送了明文 m, 因为包括接收方 B 在内的其他人无法获得发送方 A 的私钥, 进而不可能用这个私钥对 m 进行签名, 可以肯定, 这是发送方的行为. 所以保证了发送方的不可抵赖性. 同时也可以使用文件的数字签名认证发送方的身份, 因为只有他才能产生这样的签名.

所以, 图 2 基于公钥密码技术的数字签名系统既防止了第三方对信息的篡改、发送方的抵赖以及接收方的伪造, 同时还能够认证发送方的身份.

4 公钥密码体制的密钥管理—数字证书(公钥证书)

在图 2 中, 有一个关键性的假设, 就是假设通信双方事先通过某种方式相互知道了对方的公钥, 但是通信双方到底通过什么方式知道对方的公钥以及如何认证该公钥呢? 这通常是通过给用户颁发数字证书来实现的.

4.1 数字证书

在公开密钥密码体制中, 无论发送方还是接收方都有两个密钥, 一个是公钥(公布给别人, 常用于少量数据的加密以及解签名,), 一个是私钥(自己秘密保存, 常用于少量数据的解密以及签名). 为了保证公钥拥有者身份的真实性, 目前 Internet 上普遍做法是使用一个第三方权威机构 CA(certificate authority), 为每个用户

发放一个数字证书. 用于证明某一主体(如人、服务器等)的身份以及公钥的合法性.

4.2 公钥密码体制中公钥的管理

在以公钥密码算法实现的信息安全技术中, 通信双方公钥的管理, 目前多是利用数字证书进行密钥管理以及公钥交换. 数字证书管理公钥的方式如图 3.

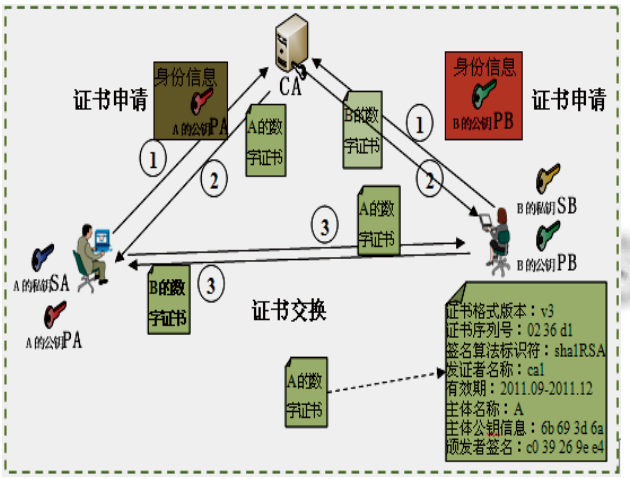

图 3 数字证书申请、颁发及交换的简单过程

首先 A 在本地产生自己的公钥私钥对, 其私钥自己秘密保存, 将自己的公钥以及其他一些身份信息发送到信任的 CA 进行证书申请, CA 在验证用户真实身份后, 将执行一些必要的步骤, 以确信请求确实由该用户发送而来. 然后, CA 给用户发送一个 X.509 格式的数字证书, 证书中包含证书持有人的名称、证书有效期、证书的发行机构、证书的签名算法、和用户的公钥信息以及 CA 使用自己的私钥对证书的签名(即 CA 对上述信息计算信息摘要, 然后使用 CA 自己的私钥进行加密, 形成签名). 可以这样说, 数字证书就是经过 CA 认证的公钥, 其将公钥同实体绑定在一起.

如果 A 想和 B 进行安全通信, 于是 A 向 B 提出会话请求. B 响应请求, 并给 A 发送自己的数字证书(根据公钥管理方式的不同, A 也可以直接向给 B 颁发数字证书的 CA 请求 B 的证书). 当 A 得到 B 的数字证书后, 使用 CA 的公钥对证书的签名进行验证, 如果签名是有效的, 就承认证书中的公钥确实是 B 的公钥. B 经过相同的过程得到和验证 A 的数字证书. 此后双方便可以使用自己的数字证书进行相关的各种活动.

现实信息系统中公钥的管理、认证等要比图 3 复杂许多, 需要采用以 CA 为核心的 PKI 公钥基础设施来处理数字证书的认证、存储、吊销、更新等方方面面的事情.

5 利用公钥密码系统来安全传输对称密钥

密码算法的共享密钥

由于公钥加密计算复杂, 耗用时间长, 比对称密钥加密算法慢很多. 所以通常使用公钥密码系统来安全传输对称密钥密码算法的共享密钥, 使用对称密钥密码算法来实现信息加密. 通信双方通过前面提到的方式相互得到对方的数字证书后, 由发送方产生一个供对称密钥密码算法所使用的临时会话密钥 KS. 然后通过公钥密码系统将此临时会话密钥 KS 安全的传输给接收方. 此后发送方的明文信息将使用此临时的会话密钥 KS 以及双方协商的一个对称密钥密码算法(如 DES、3DES)进行加密.

利用公钥系统安全传输临时会话密钥的简单过程:

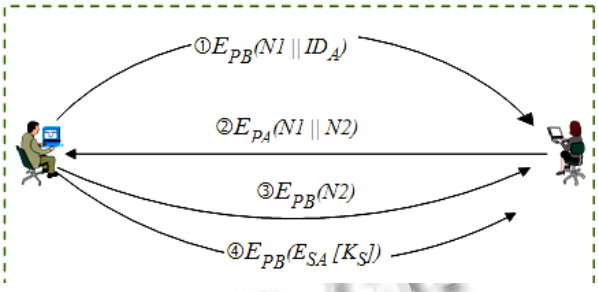

图 4 利用公钥密码系统安全产生双方共享临时密钥的过程

(1) A 用 B 的公钥加密 A 的身份信息和自己确定的一个一次性随机数 N1 后发送给 B;

(2) B 用自己的私钥解密信息得到 N1, 并用 A 的公钥加密 N1 和另外一个由自己产生的随机数 N2 发送给 A;

(3) A 用自己的私钥解密得到 N2, 然后 A 用 B 的公钥加密 N2 后发送给 B;

(4) 接着 A 产生一个会话密钥 Ks, 用自己的私钥加密此会话密钥后再用 B 的公钥加密, 发送给 B.

(5) B 用 A 的公钥和 B 的私钥解密得 Ks. 自此通信双方都知道了临时会话密钥, 可以使用此密钥结合对称密码算法进行信息的加解密.

其中步骤(1)、(2)、(3)主要用于身份认证、防中间人攻击、防重放攻击等. 通过上述步骤通信双方便可

以安全获得一个用于加密大量数据的对称秘密算法的临时密钥.

6 数字签名与数字证书的综合使用案例

在分析了数字签名系统实现原理、通信双方公钥的交换、认证问题以及临时会话密钥安全传输等一系列问题后, 便对目前绝大多数高安全等级要求应用系统的安全保证机制有了一个完整的了解. 大部分企业都是把数字签名和数字证书两者综合起来同时又加上一些自己的特性, 一起保障网络信息安全. 其完整过程大致如下:

比如 A 要向 B 发送机密数据. 通过图 3 所示过程, A 和 B 相互得到并认证了对方的数字证书(公钥). 再如(图四)所示的步骤, 利用公钥密码系统安全产生、交换用于大量数据加密的对称密码算法的临时共享密钥. 然后其安全通信过程如图 5 所示, 图 5 相比于图 2 所示过程, 增加使用了对称密码算法加密信息的功能, 保证了信息的机密性.

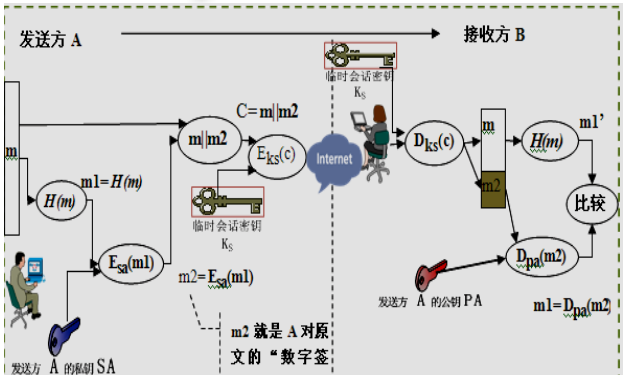

图 5 具有加密、完整性保护、抗抵赖、防伪造完整的数字签名系统

以国家税务管理信息系统—“金税工程”的出口退税审核子系统为例, 该系统采用 J2EE 平台来实现. 在出口退税管理的最后一个阶段—正式审核阶段, 退税审核部门审核操作人员向征税管理部门提交审核汇总表数据的过程中, 为了保证信息传输的安全, 在退税审核部门的审核操作人员登录出口退税系统审核端时需要由出口退税系统服务器对其身份进行验证. 并且当退税审核系统服务器接收审核操作人员提交的审核汇总表数据时对数字签名进行验证, 同时为了保证数据的机密性, 还需要审核汇总表数据采用对称密钥算法进行加密. 其基本任务流程如图 6 所示.

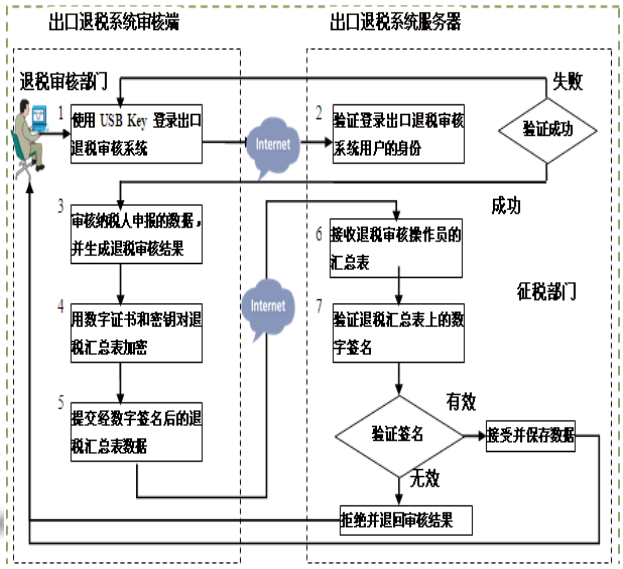

图 6 出口退税系统工作流程图

这里仅对退税审核操作人员与征税部门之间安全传输审核汇总表数据的过程进行分析, 整个过程就是前面论述的基于公钥密码算法的数据签名系统的实现过程, 其过程如下:

退税审核部门操作人员端的处理:

(1) 退税审核人员对退税审核汇总表数据进行 HASH 运算, 获得审核结果汇总表的数字摘要.

(2) 用退税审核人员的私钥对审核结果汇总表进行数字签名.

(3) 使用系统随机生成的对称密钥 K 和双方都同意的对称密钥算法(3DES)对退税审核汇总表进行加密, 形成密文.

(4) 用征税部门的公钥对审核人员用于加密审核汇总表的对称密钥 K 进行加密, 形成临时会话密钥 KI.

(5) 将审核汇总表密文、数字签名以及形成的会话密钥进行封装一起通过 Internet 发送给征收部门.

征税部门服务器端的处理:

(6) 信息到了征税部门服务器后, 用征税部门私钥解开会话密钥, 得到对称密钥 K.

(7) 对接收到的密文用对称密钥 K 进行解密, 得到审核汇总表原文.

(8) 利用退税部门审核人员的公钥对其发送的数字签名进行解密, 得到退税审核人员生成的数字摘要.

(9) 对征收管理部门私钥解密后的审核汇总表原文, 进行 HASH 运输, 将得出的数字摘要与用退税部

(下转第 57 页)

次迁移过程中，采用在线迁移的技术，只在迁移结束后，对目标系统刷新缓存或重新启动应用. 从而大大降低源系统和目标系统的中断时间.

② 数据风险

迁移的数据风险主要包括数据遗漏、数据不完整、数据不一致、数据泄密等等.

针对数据遗漏，根据迁移日志和数据库比对，验证数据迁移范围；针对数据不完整和不一致，主要通过严格分析数据迁移规则，对迁移前后数据进行预览，测试等；针对数据泄密，通过中间文件加密操作，从而保障传输的过程安全可靠.

③ 可靠性风险

数据迁移可靠性风险主要包括业务连续、出错恢复等.

数据迁移的业务连续风险主要指业务流程信息的连续性. 一方面，通过技术手段保障数据的一致完整；另一方面，从业务上规定当前未处理完成的流程数据的迁移规则，如迁移后将根据省公司的流程定义重新启动新的业务流程. 数据迁移的出错恢复，主要通过分析数据迁移日志，对迁移错误数据进行恢复重导或直接纠正等.

5 结语

数据迁移是在信息化发展过程中保障信息化建设成果的必要手段. 在迁移过程中，为确保数据完整无误、业务流程连贯，应充分分析源系统和目标系统迁移的需求和差异，坚持工具化，使迁移过程有据可查，同时迁移后的用户验证也是不可或缺的关键步骤.

本文在论述了数据迁移的相关要素和技术方法，结合电力生产系统数据迁移方案实施经验，提出基于工具化自动迁移方案，对风险进行了详尽分析，以保障迁移环节顺利进行. 相关数据迁移方法论在国家电网公司“三集五大”建设实践中得到了充分论证.

参考文献

1 李喆,万小健.企业级信息系统数据迁移方法.计算机系统应用,2011,20(1):182–184.

2 楼宏良,胡建,殷云飞.海量数据库迁移与升级,2012,28(6):152–154.

3 赵钦,周丹.政府办公自动化信息系统数据迁移解决方案,2008,(4).

(上接第 35 页)

门公钥解密得到的数字摘要进行比较验证，如果一致，则认为审核的汇总表确实是安全的，没有遭受到攻击以及相互的欺骗.

由于该退税审核子系统是税务管理信息系统的一个子系统，整个子系统都建立在前期工程的 PKI 架构之上. 因此公钥证书的管理相对容易.

7 总结语

随着计算机网络的发展，过去依赖于手工签名的各种业务在网络上都可以使用电子数字签名代替，它是实现电子政务、电子商务、电子出版等系统安全的重要保证. 在网络安全应用中发挥着越来越重要的作用.

参考文献

1 胡铮.网络与信息安全.北京:清华大学出版社,2006.

2 Tanenbaum A.S.计算机网络.潘爱民.第 4 版.北京:清华大学出版社,2004.

3 贺雪晨.信息对抗与网络安全.北京:清华大学出版社, 2006.

4 杨波.网络安全理论与应用.北京:电子工业出版社,2002.

5 曹建国,王丹,王威.基于 RSA 公钥密码安全性的研究.计算机科技与发展,2007,17(1):172–173.

6 叶生勤.公钥密码理论与技术的研究现状及发展趋势.计算机工程,2006,32(17):4–6.

7 高鹏飞.PKI 安全体系在电子公文系统中的应用研究.信息与电脑,2011,(9):84–85.

8 石志坚,谭全权,段海龙.RSA 算法实现数字签名的研究与应用.微型电脑应用,2008,24(6):50–51.

9 易红军,余名高.MD5 算法与数字签名.计算机与数字工程,(34):44.

10 陆宗跃.基于公钥基础设施技术 CA 认证中的密钥算法分析与认证.湖北第二师范学院学,2011,28(8):51–53.