多证书多数字签名在电子支付中的应用

吴国栋，李 旸
（安徽农业大学 信息与计算机学院，安徽 合肥 230036）

摘 要：电子支付的安全性是电子商务的核心与瓶颈，直接关系到网上电子商务活动能否顺利进行。在对安全电子支付协议(SET)进行分析的基础上，提出了利用多证书与多数字签名对SET协议在实际应用中进一步完善的方法，对提高网上电子交易的安全性具有一定意义。

关键词：多证书；多数字签名；SET；电子支付；安全性
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1673-629X(2007)05-0111-03

Application of Multi-Certificate & Multi-Digital Signature in Electronic Payment

WU Guo-dong, LI Yang
(Information and Computer College, Anhui Agricultural University, Hefei 230036, China)

Abstract: The security of electronic payment is the key and bottleneck in electronic commerce (EC), it restricted the development of EC. This paper advanced a means which use multi-certificate & multi-digital signature based on SET to improve electronic payment security. The model has to a certainty sense to promote the development of Internet payment.

Key words: multi-certificate; multi-digital signature; SET; electronic payment; security

0 引 言

电子支付的安全性是整个电子商务的核心与瓶颈，直接关系到网上电子商务活动能否顺利进行。尽管SET(安全电子商务交易)协议使用加密技术提供了信息的机密性，保证了支付的完整性，能对商家和持卡人的身份进行验证。但影响SET协议广泛使用的最重要的原因之一[1]就是其对加密方案的限制以及美国对加密算法出口的限制，所以能否在SET协议的基础上，加入一些自主的加密算法或其它各种加密算法，以进一步提高SET的安全性是一个很重要的问题。笔者试图在对SET进行分析的基础上，为采用自主加密算法，提出了利用多证书与多数字签名对SET协议在实际应用中进一步改进的方法。

1 SET协议的工作流程

SET协议定义了交易数据在用户、商家、发卡行和收单行之间的流通过程，也定义了各种支持这些交易的安全功能[2,3]。SET是基于卡的安全支付协议最典型的代表，也是目前世界上公认的最安全的电子支付协议之一。其工作流程如图1所示。

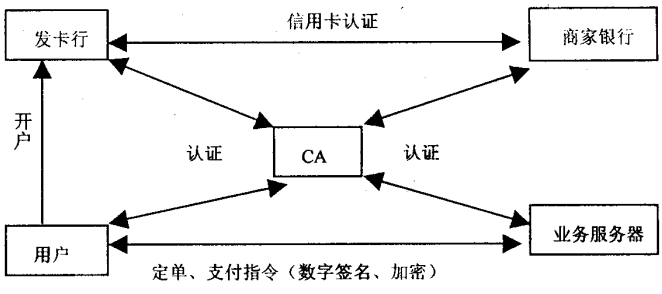


图1 SET模型的工作流程

其具体步骤主要有：(1)用户在银行开立信用卡账户，获得信用卡。(2)用户在商家的Web主页上查看商品目录选择所需商品，填写定单并通过网络传递给商家，同时附上付款指令，其中定单和付款指令要有用户的数字签名并加密，使商家无法看到用户的私人账户信息。(3)商家收到定单后，向发卡行请示支付认可；发卡行确认后，批准交易，并向商家返回确认信息。

收稿日期：2006-09-12
基金项目：安徽农业大学校长青年基金资助项目；安徽省教育厅自然基金资助项目(2006KJ075B)
作者简介：吴国栋(1972-)，男，安徽宿松人，硕士，讲师，CCF会员，研究方向为计算机网络、供应链与电子商务、信息安全等；李 旸，博士，副教授，研究方向为计算机网络、数据库等。

(4)商家发送定单确认信息给用户,并发货给用户。(5)商家请示银行支付货款,银行将货款由用户的账户转移到商家的账户。

SET 协议已成为电子商务中在线支付的一种主要模式,但由于在通用的 SET 协议模型中,其内部对加密方案的限制以及美国对加密算法出口的限制影响了 SET 协议的广泛使用,所以能否在 SET 协议的基础上,加入一些自主的加密算法或其它各种加密算法,以进一步提高 SET 的安全性,就显得比较重要。

2 改进的 SET 方案

该方案是在 SET 协议执行前,预先让交易双方进行协商,根据交易额的大小或该项交易的重要性选择不同的算法(最重要的是可以使用自主加密算法)进行一次加密过程,在 SET 协议结束时,再进行一次解密,从而完成整个交易过程。具体如图 2 所示。

由图 2 可知,发送方将所有加密算法和签名算法(含自主加密与签名算法)以列表的方式与接收方的算法列表进行协商,找到公共的加解密算法,然后以确认的公共算法对数据进行加密处理。

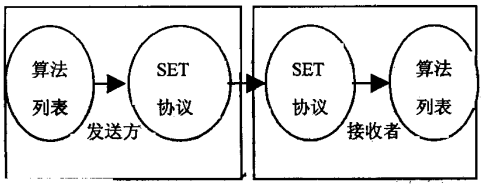


图 2 改进的 SET 协议

3 多证书和多数字签名的应用

为了保证改进的 SET 协议顺利地进行证书认证,必须确保每个参与者都支持多证书和多数字签名。

多证书:一个参与者拥有多个数字证书。在方案中,由于某个参与者可能支持几种不同的公开密钥算法,因此,对每种公开密钥算法都应有相应的数字证书来证明其公开密钥的有效性。多证书的生成可以采用两种方式[4,5]:(1)独立证书:对应每一种公钥加密算法或签名算法采用一个独立证书,即一个算法一张证书。证书申请方式与原来相同。发送其数字证书时,应根据算法协商情况,将相应的数字证书全部发送给接收者。(2)复合证书:同一数字证书包括多个公钥加密算法及签名算法。复合证书的引入,必对证书现有格式进行扩展,以便在证书中存贮多个公钥加密及签名算法标识。

根据 SET 证书格式,在用户自定义域中采用抽象符号(ASN.1)描述如下:

```
USERSDEF: : = SEQUENCE {
Hash Sequence Algorithm Identifier
Symmetry Sequence Algorithm Identifier
AymmetrySequence Algorithm Identifier
}
Algorithm Identifier: : = SEQUENCE{
Algorithm OBJECT IDENTIFIER,
Parameters ANY DEFINED BY algorithm OPTIONAL
}
```

多数字签名:在 SET 协议中数字签名只有一种,即采用 SHA-1 算法和 RSA 算法生成数字签名,而如果某个参与者支持几个单向哈希算法,在生成数字证书时,就要结合不同的单向哈希算法生成多数字签名。多数字签名有两种签名方法:一种是多次签名,即分别用单向哈希算法生成信息摘要,对消息摘要进行签名,其形式为:(Info,SIGx (HASHx(Info)),SIGy(HASHy (Info))…);另一种为多重签名,即本次签名根据上一次签名及信息一起生成信息摘要,再用本次公钥算法的私钥进行加密,生成本次签名。过程如图 3 所示。

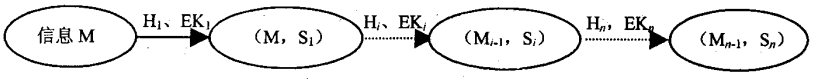


图 3 多重数字签名过程

其中:$S_i = EK_i(H_i(M + S_{i-1}))$, $(1 \leqslant i \leqslant N)$。发送信息为$(H, S_1, S_2, \cdots, S_n)$。

3.1 多数字签名的验证

对于多次签名,其验证方式与数字签名的验证方法一致,对每一次签名分别进行验证即可。为了提高处理效率,可以简化验证过程,即只对一次签名进行验证即可;对于多重签名,其验证过程为:从前向后或从后向前依次验证每一个签名,也可随机进行验证。若 $H_i(M + S_{i-1}) = Dk_i(S_i)$,则认为第 I 次签名被确认。

3.2 算法协商过程

该方案的核心是 SET 电子支付系统支持多种不同的加密和签名算法,具体实现方法是在实际信息交换之前,增加一个算法协商过程。协商过程分三步:

(1)发起者 A 根据自己的加密算法和 Hash 算法的算法标志符生成列表,在该列表中包含可采用的所有哈希函数、私钥加密算法和公钥加密算法的标志及用途,该列表的结构采用抽象符号(ASN.1)描述如下:

```
Algorism list: : = Sequence {AlgorithmID OBJECT IDENTIFIER
    Type AlgorithmType
    Function AlgorithmFunction
    }
Algorithm Type: : = CHOICE{Hash OCTET STRING,
    Symmetry OCTET STRING
```

Asymmetry OCTET STRING}

Algorithm Function::=CHOICE{Signature OCTET STRING,

Encryption OCTET STRING}

(2)接收者 B 在接收到 A 的算法列表以后,将该列表的的内容与其支持的算法进行比较。若在哈希函数,私钥加密算法和公钥加密算法都至少有一种算法与 A 的算法列表相一致,则 B 选择准备采用的算法,并将其修改后的算法列表返回给 A,如果上述条件不满足,则返回错误信息。

(3)A 在接收到 B 返回的信息后检查修改后的算法列表,根据算法列表的内容选择相应的算法进行下一步操作,若返回的是错误信息,则终止向 B 发送交易信息。

在协商过程中,由于用户对加密和签名算法的支持或喜好不同,协商可能要经过几次反复才能达成一致,具体实现时应当予以考虑。

4　加入多证书与多数字签名后的 SET 分析

4.1　交易流程

假设发起人 A 支持私钥加密算法 DES, IDEA,公开密钥算法 RSA 和 ELGamal,单向哈希算法有 MD5, SHA－1;B 是信息的接收者,它只支持 DES, RSA 和 SHA－1 三种算法;A, B 的数字认证中心所支持的算法与 A 一致。A 通过算法协商过程与 B 确定使用 DES, SHA－I 和 RSA 算法。若多数字签名采用多次签名,则 A 对应 RSA 的证书应该包含两个数字签名:

CERTA－RSA=(InfoCERT, DCA－RSA(HASHCA－SHA(InfocERT)),

DCA－RSA(HASHCA_MD5(Info Cert))

对应 ELGamal 算法的证书的数字签名为:

CERTA－ELG=(InfoCERT, DCA－ELG(HASHCA－SHA(InfoCERT)),

DCA－ELG(HASHCA-MD5(Info cert))

交易流程为[6]:

(1)算法协商过程:发起者 A 和接收者 B 协商并确定使用算法 DES, SHA－1, RSA。

(2)发起者 A 按照 SET 协议的信息生成过程,利用协商算法生成所需的消息摘要,签名后,附上证书发送给接收者 B。附上的数字证书应该是对应的公钥算法的证书。

(3)由于发起者 A 在生成数字证书时保证了其数字签名公钥算法与证书上的一致性,而且 B 也支持 A 所采用的公开密钥,因此,B 按照 SET 协议的解密过程将发起者 A 传送过来的信息进行解密,解密后,B 先验证 A 证书的有效性。由于 A 的证书中包括其所有支持的单向哈希算法生成的多数字签名,这就保证了 B 能够对 A 的证书的数字签名进行有效性验证。若证书有效,就用发起者 A 的证书上相应的公开密钥和 SHA－1 算法验证 A 的数字签名。

(4)根据验证结果选择下一步操作,若有效,则继续后面的交易过程;若无效,则终止交易。

4.2　性能分析

可以从以下几方面对采用多证书与多数字签名的 SET 协议进行简单分析。

(1)在工作效率方面:改进后的 SET 因为加入了算法协商过程,以及多数字签名的生成,工作效率有所下降。由于引入协商加解密方案带来了更高的安全性,通过采用加解密速度更快的算法和利用加密芯片来提高交易处理的效率,完全可以弥补增加的计算量对其效率的影响[7]。

(2)在适应性方面:由于协商加密方法的引入,在 SET 中可以采用的多种加密算法和 Hash 算法,解除了 SET 协议对加密算法的限制,提高了 SET 的适应性。

(3)在安全性方面:SET 电子支付系统的安全性主要由加密算法的安全性决定,在引入协商加密方法的 SET 协议中,由于可以采用的多种加密算法和 Hash 算法,因此,通过选取安全性更高的加密算法和 Hash 算法,就能够达到提高 SET 安全性的目的。

(4)在扩展性方面:由于协商加密方法的引入,SET 协议可以支持各种不同的加密算法和 Hash 算法,只要将新的加密算法和 Hash 算法引入系统,就可得到 SET 协议的支持,从而扩展了 SET 的应用范围,提高了 SET 的扩展性。

5　结　论

SET 协议提出以来,许多厂商开发出了符合 SET 协议的应用软件。利用多证书与多数字签名的方法,在 SET 协议中增加软件对多种算法的支持,这些算法可根据不同的情况进行选择,各个国家可以选择有自主知识产权的算法,在现有软件中加入实现各种算法的功能模块,再加入算法协商模块和在 CA 的软件中加入多证书和多数字签名的生成模块,就可以进一步提高 SET 交易的安全性。

参考文献:

[1] 袁姗姗,邱建雄. SET 的安全性与便捷性分析及改进措施[J]. 计算机工程与科学,2003,25(5):10－12.

[2] 陈　豫,陈喜阳. SET 协议的分析与改进[J]. 微型机与应用,2004,23(6):34－35.

[3] 吴建耀. SET 支付协议的形式化分析与改进[J]. 计算机工

(下转第 116 页)

产生 m 序列的初始值就是加密算法中的密钥，为避免产生输出的全 0 序列，就不能将寄存器的初始值全设为 0。

从 m 序列产生器可以看出只要初始值改变，m 序列就不同。这就满足随机性。以上初始值的运行结果为：111010110010001。

然后，将 m 序列与原图像像素的各位相异或，就能达到加密的效果，产生加密后的图像。

同样，图像解密是图像加密的逆过程。根据异或的特点 $A = A \oplus B \oplus B$，所以，解密就是将加密后的图像与 m 序列再异或一下就可以实现。运行结果就是加密前的图像。只要接收者使用此算法和密钥就可以实现解密，读出原图像。

3 基于 LSB 的图像嵌入与提取算法

选取原图像大小为：32 * 32（见图 4(a)）；选取载体图像大小为：128 * 128，如图 5(b)所示；隐藏 1～4 位后的图像如图 5(c)～(f)所示。信息隐藏比和峰值信噪比的计算如表 1 所示。

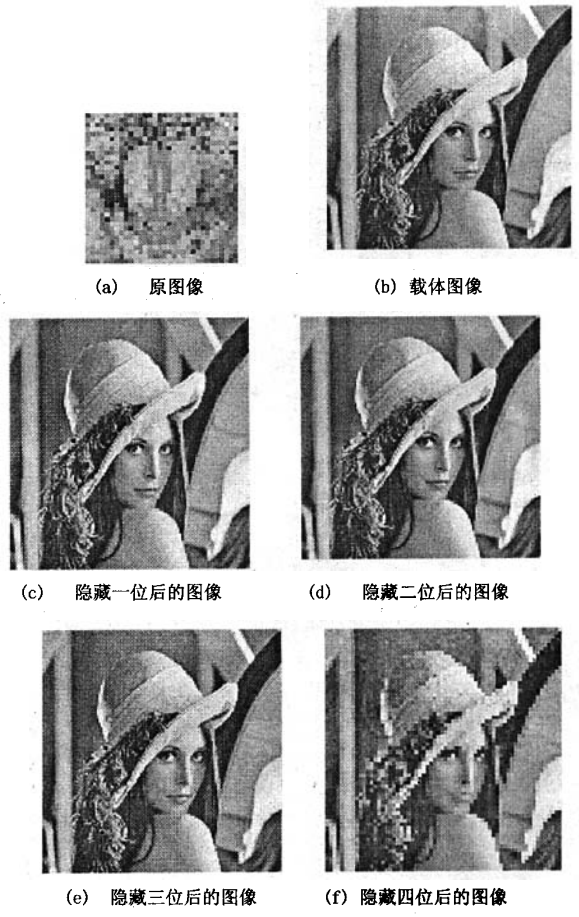
表 1 信息隐藏比和峰值信噪比计算结果

隐藏位数	信息隐藏比	峰值信噪比(PSNR)
1	0.125	75.4dB
2	0.25	69.4dB
3	0.375	58.2dB
4	0.5	33.8dB

由图 5 可以看出，隐藏 1～3 位后的图像与载体图像相比在视觉上没有什么差别或差别不大，而隐藏 4 位后的图像出现比较明显的伪轮廓。

4 结束语

图像信息隐藏技术和图像加密技术都是新兴的技术，具有极大的发展潜力，两者的结合可以克服目前的信息隐藏技术中的很多弱点。文中运用 Matlab 实现了基于空域 LSB(Least Significant Bit)的灰度图像隐藏与提取系统。由于在进行图像隐藏前对原始图像信息进行了置乱和加密处理，具有较高的安全强度，能满足隐蔽通信等应用要求。



(a) 原图像 (b) 载体图像 (c) 隐藏一位后的图像 (d) 隐藏二位后的图像 (e) 隐藏三位后的图像 (f) 隐藏四位后的图像

图 5 基于 LSB 的图像嵌入算法实验结果

参考文献：

[1] 韩杰思，汤光明，马晓煜. 基于图像的信息隐藏安全性分析[J]. 微计算机信息，2006，22(1－3)：19－21.

[2] Provos N, Honerman P. Hide and Seek: An Introduction to Steganography[J]. IEEE SECURITY & PRIVACY, 2003, 5/6:32－44.

[3] 汪小帆，戴跃伟，茅耀斌. 信息隐藏技术——方法与应用[M]. 北京：机械工业出版社，2001.

[4] 王聪丽，平西建. 矩阵编码的实现及其在图像信息隐藏中的应用[J]. 计算机工程与应用，2005(34)：146－148.

[5] 夏 煜，郎荣玲，戴冠中，等. 基于图像的信息隐藏分析技术综述[J]. 计算机工程，2003，29(7)：1－3.

(上接第 113 页)

程，2006，32(3)：164－166.

[4] Adi K, Debbabi M, Meiri M. A New Logic for Electronic Commerce Protocols[C]// AMAST 2000, LNCS. [s.l.]:[s.n.], 2000:499－513.

[5] 史国庆. 利用组合加解密方案改进 SET 协议的研究[J]. 计算机工程与应用，2002，38(2)：43－45.

[6] Shen Jau—Ji, Lin Iuon—Chang, Hwang Min—Shiang. A secure LITESET scheme[J]. Inst. Electron. Inf. & Commun. Eng, 2004(11):2509－2521.

[7] 何 胜. 电子商务中安全支付协议的对比及应用[J]. 计算机时代，2004(2)：29－30.