# 一种基于数字加密与信息隐藏的电子签名技术改进方案

周启海 黄 涛 张 乐
(西南财经大学经济信息工程学院 成都 610074)

**摘 要** 阐述了电子商务系统的安全性需求,以及作为安全保障中必不可缺的电子签名关键技术的实现过程;指出现行电子签名实现过程中存在的不足;给出了基于数字加密与信息隐藏相结合的电子签名技术改进思路及几种实现方案;提出了用"安全/速度比"数字签名强度理论指导签名技术方案选择的创新思想;指出了电子商务安全技术的发展方向。

**关键词** 电子商务,电子签名,数字加密,信息隐藏,安全/速度比,数字签名强度

## An Improved Scheme for E-signature Techniques Based on Digital Encryption and Information Hiding

ZHOU Qi-Hai HUANG Tao ZHANG Le
(School of Economic Information Engineering, Southwestern University of Finance and Economics, Chengdu 610074)

**Abstract** In this paper, the demand of an e-commerce system security and the realizing process of an e-signature technology as the essential key technology in the safety control are elaborated; the insufficiency in current e-signature realizing process is pointed out; based on digital encryption and information hiding, an improving thinking and some realizing schemes for the techniques of e-signature are given; a creative new idea to guide the selection among the e-signature technical schemes with a "safety/speed ratio" digital signature strength theory is proposed; and the developing direction of an e-commerce security technology is pointed out.

**Keywords** E-commerce, E-signature, Digital encryption, Information hiding, Safety/speed ratio, Digital signature strength

## 1 引言

计算机技术、通信技术、网络技术(尤以 Internet 为代表)的迅猛发展与广泛应用,对传统工作方式和商务模式产生了巨大冲击,也促成了电子商务方式、模式、系统的应运而生。电子商务,比传统商务模式具有便捷、低成本、更高效的优势,这使它在如今经济贸易中的作用越来越重要,影响越来越深广。但也应清醒地看到,社会各界关注热点和研究课题之一是"当今世界通过电子商务渠道完成的贸易额为什么仍只占同期全球贸易额的一小部分?",其所以如此的一个基本原因,就是电子商务系统安全已成为制约电子商务发展的核心问题和主要瓶颈之一。显然,电子商务系统高度依赖计算机网络技术,而互连网所具有的自由、开放则不可避免地使电子商务系统面临着网上各种各样的安全隐患与威胁。为了有效保障商务各方正当权益,人们理所当然地迫切要求电子商务系统必须具有高可靠性、强安全性,以确保所传输商务数据的完整性、安全性、及时性、私密性、不可否定性。数字签名技术作为电子商务交易中验证身份真伪以及交易不可否认的核心技术,是电子商务安全性保障的重要组成部分,正越来越受到社会各界的广泛关注。

## 2 电子商务系统安全控制的基本要求

电子商务系统的安全控制(包括电子签名)[1,2],其基本要求是:

(1)通信过程必须保证交易数据完整。

(2)提供对通信双方的身份认证机制,确保电子商务交易双方身份的可靠性和合法性。例如:①实现系统对用户身份的有效确认;②对私有密钥和口令进行有效保护;③对非法攻击能实时防范;④防止假冒身份在网上交易、诈骗,等等。

(3)确保商务信息的保密性。例如:怎样保证用户的信用卡号不被窃取、如何保证货源订单等信息不被竞争对手获悉等等。

(4)电子商务系统应防止对交易信息的随意改动,防止数据传输过程中交易信息的丢失和重复,并保证信息传递次序和内容的统一。

(5)保证电子订单等商务信息的不可否认性。即:电子商务系统应能有效防止商业欺诈行为,保证商业信用和行为的不可否认性,保证交易各方对已做交易无法抵赖,等等。

## 3 数字签名定义及实现过程

实现电子商务信息保密的最基本方法是数据加密,但是要确保电子交易的不可否认性、交易双方身份的确认性和订单的不可修改性,仅仅依靠数据加密是解决不了的。在传统交易过程中,通常交易双方采用亲自手书签名(包括:手写或盖章)来保证文件的可靠性及法律效力。如果通过网络进行交易,就需要设计一种能够代替交易双方亲自手书签字的方案,使签字的文件从一方通过网络安全地传送到另一方。这就需要所谓的数字签名技术。

**周启海** 教授,博(硕)士生导师,主要研究方向:财经计算,算法研究与应用,计算几何,同构化信息处理等。**黄 涛** 讲师,主要研究方向:计算机应用。**张 乐** 硕士研究生,主要研究方向:电子商务,计算机应用。

### 3.1 数字签名定义

数字签名是相对于手书签名而言的，签名主要起到认证、核准和生效的作用，是指采用一定的数据交换协议，使用密码算法对待附加在交易信息上的一些数据，或是对交易信息所作的密码变换，这种数据和变换允许交易信息的接收者用以确认交易信息来源和交易信息的完整性，并保护交易信息，防止被人（例如对方接收者）进行伪造。数字签名是一种基于加密技术的信息认证技术，它作为电子商务安全性保障的重要组成部分，必须满足下述基本特性：

（1）不可伪造性，即数字签名只能由发送方自己签发，其他任何人都不能伪造出发送方的数字签名，这有利于保护发送方的权益。

（2）不可否认性，即接收方收到数字签名后能够确认该签名是由发送方签发的，同时发送方不能否认发送消息给接收方。

（3）不可篡改性，即一旦有第三方截获并篡改了消息，接收方能够轻易地检验出来。

（4）不可重用性，即保证消息是新的，而不是已用过的消息的重用，若重用旧消息时，发送方和接收方都能检验出来，这就要求数字签名具有自毁功能。

（5）可鉴别性，即一旦发、送双方发生争议时，第三方（仲裁机构）能够凭借发送方的消息，通过一个公开的验证算法，来验证数字签名是否为发送方签发的。

### 3.2 数字签名的现行过程

消息摘要是数字签名的基础。单向杂凑函数（HASH 函数）是生成消息摘要的快速加密算法。单向杂凑函数并不使用密钥，它只是一个比较复杂的公式，但它可以将任何长度的明文转化为一个消息摘要——16 位的字符串。这样，无论用户输入多少字符所构成的串，最后得到的总是 16 位的一个串，从而使每一条明文产生一个随机的消息摘要。据此，简易数字签名的实现过程[3~5]，可概述为（如图 1 所示）：

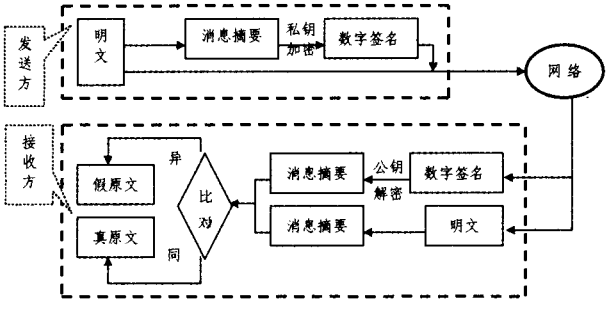


图 1 简易数字签名实现过程示意图

（1）发送方随机生成一个消息摘要。

（2）发送方用自己的私钥对消息摘要进行加密，生成发送方的一个数字签名。

（3）发送方将数字签名和明文发送给接收方。

（4）接收方收到消息后：①接收方用发送方的公钥对数字签名进行解密得到消息摘要；如果能够解开，说明该明文确实是发送方发送的，从而验证了发送方身份的真实性。②接收方再用相同的 HASH 函数对明文进行计算得到消息摘要，并与第①步解密得到的发送方的消息摘要作比对：如果相同，则说明所收到该明文为真原文（即在传送途中没有被篡改或伪造），否则为假原文，从而实现了收、发双方消息传递完整性的监控。

## 4 数字签名存在的问题及改进

### 4.1 数字签名存在的问题及信息隐藏技术简介

应当看到：上述简易数字签名实现过程中，存在着“拦截窃读”的隐患——由于发送方是把数字签名和明文一齐发送给接收方，而明文却没有采取任何加密措施；故该数字签名过程虽可认证发送方身份的真实性、防止其抵赖以及检测明文被篡改，倘若传输途中有第三方进行拦截窃读（即只是读取明文内容而不对明文做任何篡改），则明文中所含的消息就会泄露，而收、发双方可能对“明文已被非法读取”毫不知情，从而给收、发双方带来巨大损失。

简易数字签名的这种拦截窃读隐患，可通过对明文进行加密来解决。然而现行加密方式的不可破解是靠密钥长度来保证的。随着计算机运算速度的不断提高，攻击方完全有可能通过穷举算法破解出密文，并且现行加密方式存在一个致命弱点，即密文存放的位置比较明显，容易引起攻击方的注意，从而引起其攻击。对于加密方式存在的这种致命隐患，我们可以通过信息隐藏技术加以解决。

传统的密码编码学研究的是如何将明文通过一定的算法形成不为外人所识别的密文，然后进行传输；而信息隐藏技术研究的是如何将一段秘密信息隐藏于一段公开的信息（载体信息）中，然后通过载体信息的传输来实现秘密信息的传输。密码编码学与信息隐藏技术都用于秘密通信，但两者之间存在明显差别。前者传输的信息一旦被攻击方截获并被解密，则密文完全变成明文；后者在传输途中即使信息被截获，由于信息隐藏技术隐蔽性强的特点，攻击方往往很难从公开信息的表面发觉有秘密信息隐藏于其中，从而更谈不上提取其中的秘密信息了。这样，无异于后者比前者多了一层强化保护，使得秘密信息由“看不懂”变为“看不见”，从而大大提高了信息传输的安全性。

信息隐藏系统的一般模型可概述为（如图 2 所示）[6]：

（1）密钥生成器生成嵌入密钥以及提取密钥（两个密钥是相同或相关的）。

（2）发送方通过嵌入密钥将秘密信息嵌入到载体信息中形成隐藏载体。

（3）发送方将隐藏载体发送给接收方。

（4）接收方接收到隐藏载体后通过提取密钥将秘密信息提取出来。

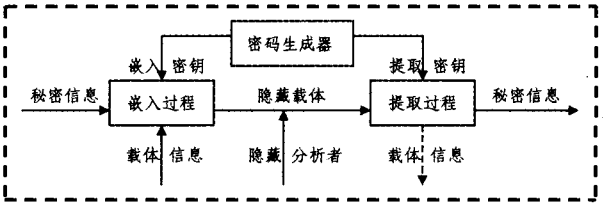


图 2 信息隐藏系统的一般模型

在上述信息隐藏模型中可以看到，如果我们仅局限于用已知的信息隐藏算法对秘密信息进行隐藏，一旦攻击方截取到隐藏载体，在不知道密钥的情况下，只要使用已知的信息隐藏算法对其进行蛮力攻击，秘密信息完全有可能被提取出来。如果我们在隐藏信息前对秘密信息进行置乱处理，使得秘密信息失去其原来面目，则其安全性就会提高许多。即使秘密信息被提取出来也会由于其是杂乱无章的“图书”，而使得攻击方无法分辨出在置乱处理前的原秘密信息的具体内容。但

也正由于经过置乱后的秘密信息是杂乱无章的，容易引起攻击方的注意，因此，我们使用信息分存技术，将经过置乱处理后的秘密信息随机分布在载体信息中，使得攻击方难以从视觉上发现有秘密信息隐藏于其中，降低攻击方的注意，减少遭受攻击的可能性，从而很大程度上提高了秘密信息传送的安全性。

### 4.2 高强度数字签名方式

简易数字签名所存在的种种隐患，可通过对明文进行加密、并与信息隐藏技术相结合的方法来解决。一种可行的全密数字签名解决方案，可设计如下（如图 3 所示）：

(1)发送方随机生成一个消息摘要；用发送方私钥对消息摘要进行加密，生成发送方的数字签名。

(2)发送方对数字签名进行置乱处理得到置乱签名。

(3)发送方再随机生成一个对称密钥，用此对称密钥对明文进行加密，并用接收方公钥加密该对称密钥（称之为密化对称密钥）。

(4)发送方使用嵌入密钥以及信息分存技术将置乱签名、加密过的明文、密化对称密钥随机隐藏于载体信息中，得到隐藏载体；然后，将隐藏载体发送给接收方。

(5)接收方收到发送方信息后：

①接收方通过提取密钥将隐藏载体中的秘密信息提取出来。

②接收方将置乱签名进行还原，得到发送方的数字签名。

③接收方用发送方公钥对其数字签名进行解密，得到消息摘要；如果能够解开，说明该明文确实是发自于发送方，从而验证了发送方身份的真实性。

④接收方用己方私钥，解密已经过发送方加密的对称密钥，得到发送方的对称密钥。

⑤接收方用发送方的对称密钥解开密文，从而得到明文。

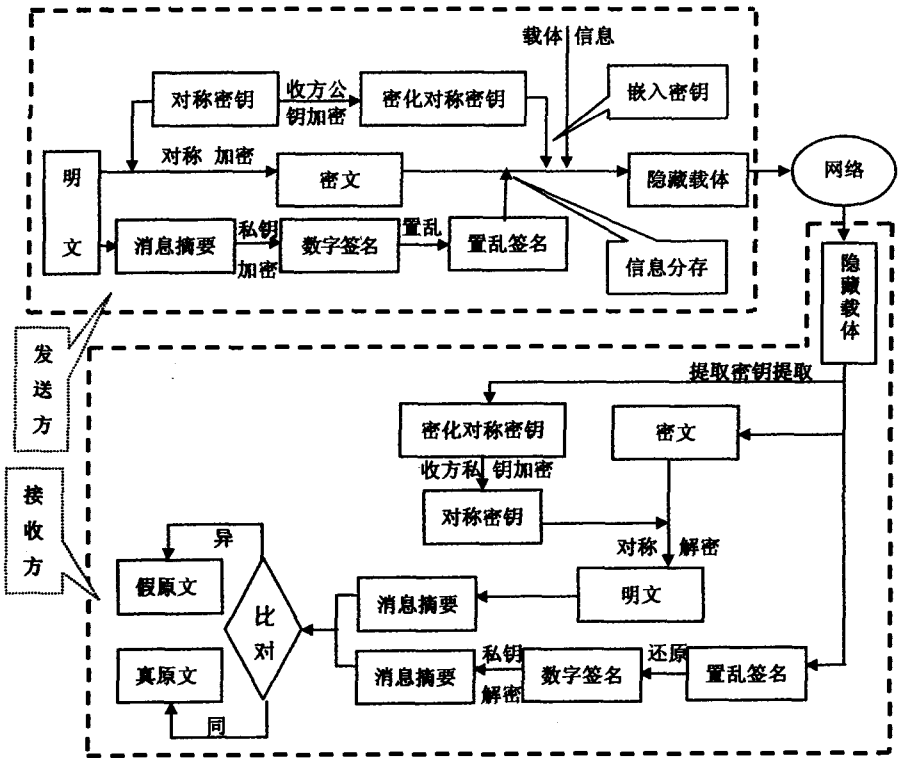


图 3 全密数字签名实现过程示意图

⑥接收方再用相同的 HASH 函数对明文进行计算得到消息摘要，并与第①步解密得到的发送方的消息摘要作比对：若完全相同，则说明该明文在传送途中没有被篡改或伪造，否则为假原文。

据此，便可实现和强化收、发双方对消息传递安全性与完整性的监控。

### 4.3 中强度数字签名方式

由上述全密数字签名的实现过程，可以看出其安全性得到了充分保障；但我们也必须清醒地认识到由于其对明文进行整体加密，其解密过程所耗费的时间比较长。而电子商务是以便捷著称的，网上交易其金额大多是数额较小的小支付、微支付。因此，小支付、微支付的交易双方在要求较高安全性的同时，必然更要求交易的时间尽可能短。鉴于此，我们提出了另一种改进方案——局密数字签名，其具体实施过程如下（如图 4 所示）：

(1)发送方随机生成一个消息摘要；用自己的私钥对消息摘要进行加密，生成发送方的数字签名。

(2)发送方对数字签名进行置乱处理得到置乱签名。

(3)发送方按事先约定的某一算法将明文随机分配比例得到头文、中文、尾文，使其头文、中文、尾文各占全文长度的 $\alpha$、$\beta$、$1-\alpha-\beta$（其中：$0<\alpha$，$0<\beta$，$\alpha+\beta<1$）。

(4)发送方从头文、中文、尾文中各抽取一部分使用接收方公钥进行加密后，再与余下的部分共同形成局部加密新密文。

(5)发送方使用嵌入密钥以及信息分存技术将置乱签名与局部加密新密文隐藏于载体信息中，得到隐藏载体，然后将隐藏载体发送给接收方。

(6)接收方收到隐藏载体后：

①接收方通过提取密钥将隐藏载体中的秘密信息提取出来。

②接收方将置乱签名进行还原，得到发送方的数字签名。

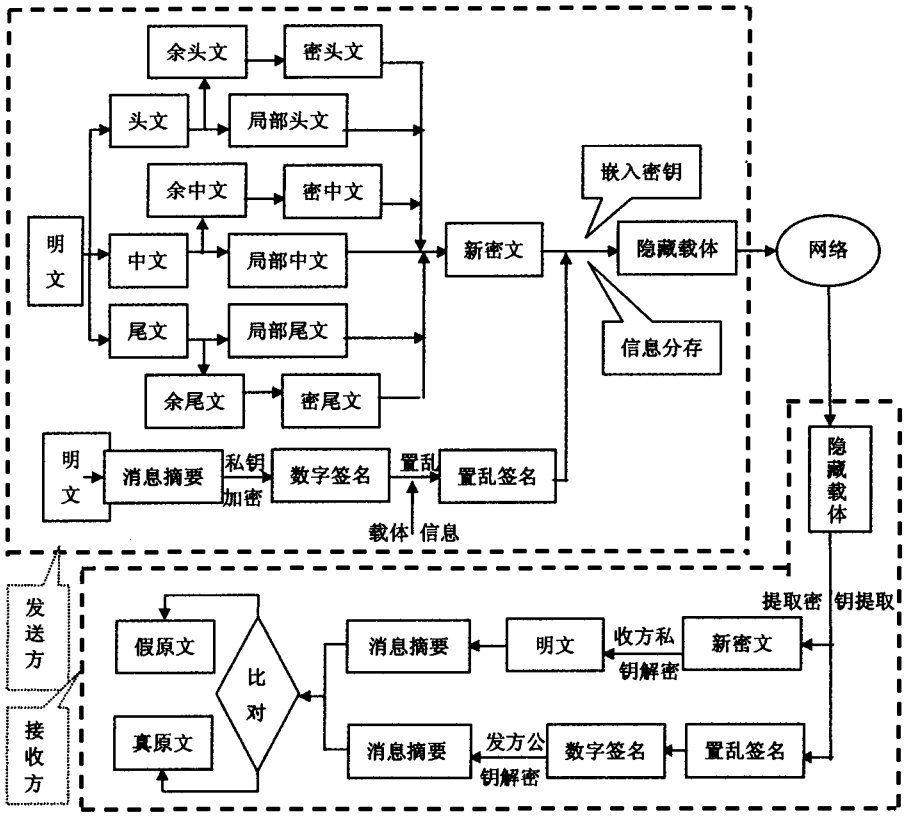


图 4　局密数字签名实现过程示意图

③接收方用发送方的公钥对其数字签名进行解密，得到消息摘要；如果能够解开，说明明文确实是发自发送方，从而验证了发送方身份的真实性。

④接收方使用同一算法的逆算法，将局部加密新密文转换成明文。

⑤接收方通过 HASH 函数使明文转换成消息摘要，与第①步中所得到的消息摘要相比对：如果两者完全相同，则说明消息在传递过程中未被篡改或伪造，否则为假原文。

### 4.4　两种数字签名改进方式的评价及选择机制

由上述改进过的数字签名实现过程可以看到：第一种全密数字签名改进方法，其全文加密方式使得加密强度较大、安全系数较高；但正因为它是对整个明文进行加密，实现过程复杂，耗费时间长，故这种方法较适合于交易数额巨大、交易重视程度比较高的“大支付”场合。第二种局密数字签名改进方法，其局文加密方式使得加强强度适中；且由于只对明文的一部分进行加密，故节约了一定的时间，提高了交易速度；同时在消息的传输途中，即使存在着“拦截窃读”的隐患，也会由于所窃取的消息是残缺不全的，得到的是毫无价值的信息而不会造成重大的损失，从而兼顾了一定的安全性。因此，后一方法更适用于交易数额较小的、重要程度一般的“小支付、微支付”场合。

据此，我们可以根据“安全/速度比”来选择加密强度适当的加密方式。即：应统筹兼顾、全面权衡、认真比较“安全与速度两大因素在交易过程中的重要性程度”，来选择合适的加密方式：若安全的重要性大于速度的重要性时，则选择第一种改进方法的高强度加密方式；若交易中更重视速度因素同时又兼顾一定的安全性时，则选择第二种改进方法的中强度加密方式；当交易中最重视速度因素而只需一般安全性时，则选择普通简易方法的低强度加密方式。

**结束语**　电子商务安全问题，是阻碍电子商务发展的主要瓶颈之一。数字签名技术，具有良好的防伪造、防篡改、防拒认的功能，而我国最新颁布的《电子签名法》使它在电子商务领域中更具备了替代传统人工签名的权益，现在它正成为保障电子商务安全的关键技术之一。可以断言：只有进一步改进包括数字签名、信息隐藏在内的各种电子商务安全技术，才能为电子商务的可持续、跨越式发展提供强有力的技术支撑。

## 参 考 文 献


1　肖存涛. 数字签名技术与电子商务安全性研究[J]. 网络安全技术与应用，2005,7:67～69

2　彭岚，廖仁全. 电子商务安全中的数字签名技术[J]. 中国金融电脑，2004,1:74～76

3　纪志凤，丁鹏. 电子商务系统安全和数字签名技术[J]. 经济师，2004，8:110

4　夏露. 我国电子签名安全问题及解决办法[J]. 特区经济，2004，8:99～100

5　马涛. 电子签名的安全性问题[J]. 经济论坛，2002，24:42～43

6　张书真. 信息安全中的信息隐藏技术[J]. 电脑知识与技术，2005，18:75～77