华东师范大学

硕士学位论文

盲签名的研究与应用

姓名：王静然

申请学位级别：硕士

专业：计算机应用技术

指导教师：钱海峰

20091101

论　文　摘　要

盲签名是数字签名的一种，它是为了实现电子商务中的电子货币技术而产生，和一般电子签名的不同是加入了对签名使用者隐私的保护，也就是说签名者对使用者要求的信息进行签名，但却不能获得信息的内容或者与其相关的可以辨认的知识。盲签名的发展已有20多年的历史，众多研究者们不断的对盲签名方案进行补充和扩展，但从盲签名方案的构造到盲签名在具体协议中的应用等方面仍然存在一些值得研究的问题。

针对此情况，本文提出了两个比较有效的盲签名方案，方案一：一个支持消息恢复的盲签名。这个盲签名使用了一个块比较小的分组密码来实现对签名的消息填充，把需要传输的消息冗余部分通过算法的执行包含在真正消息里面，从而减少传输消息的长度。而在算法执行过后，方案输出最终的签名时，任何人都可以通过简单的计算恢复出真正的消息，这减少了信息的储存和检测的消耗。这个方案可以使用一个真正的分组密码加以实现。我们也同时给出了对长消息的签名方案，这保证了算法的可用性和性能。方案二：无随机预言的盲签名方案。基于Boneh和Boyen的论文里提出的签名，本文给出了一个无随机预言的盲签名方案。不包括随机预言机，盲签名就是一个可实现的安全的标准方案。考虑到交互次数问题，该方案还可以引入公共参考串Common Reference String (CRS)来完成签名方的非交互零知识证明，使得盲签名算法仅包含两次交互，实现了轮优先round optimal，在此基础上也可以实现盲签名算法的并发执行。这个盲签名算法构造简单且计算复杂度比较低，比当前存在的盲签名方案更加的有效，节省了传输带宽，提高了传输效率。

对这两个盲签名方案，我们对它们的安全性: 盲性和不可伪造性都给出了具体的分析，考虑到算法的性能，我们还和一些类似的签名进行比较，并对算法的参数和具体实现也给出了相应的讨论。要特别指出的是，这两个算法有着各自的优越性和实现的合适条件，我们将在文中具体指出。

近些年来，除了电子货币，盲签名应用于电子选举，电子拍卖等更多的数字信息领域中，除了签名构造方法的设计和效率的提高，盲签名的具体应用也是一个值得研究的方面。本文在后面给出了我们提出的盲签名方案在电子现金和电子选举中的简单协议实现。

关键词: 盲签名, 盲性, 不可伪造性, RSA, BBS, 电子货币, 电子选举

ABSTRACT

Blind signature is a kind of digital signature used in e-cash technology in e-commerce. "Blind" means when the user require a signature of some information, they just want to gain legal signature, without let the signer know the content of the information or something related. In the last 20 years, many researchers have done a lot of work on it, but considering the construction of blind signature scheme and its protocol in specific implementation, there are still some problems to be studied.

We give two efficient blind signature in our paper, 1:An optimal blind signature with message recovery. We uses an ideal cipher with a smaller block size to design a secure two-move blind signature, put the message redundancy into the real message could shorter the length of the information transmission. Our blind scheme has the message recovery property with less bandwidth. This blind signature can be implemented with a truly real block cipher. Besides this, To ensure the availability and performance of the algorithm, we also give the scheme for longer message in our paper.

2: A blind signature with no random oracles. Boneh and Boyen gave a new encryption in a paper, our blind signature scheme is derived from their idea. We first give a blind signature without random oracles, with this property, the blind signature scheme is secure in standard model. Then, use Common Reference String to do non-interactive zero knowledge proof, we make the blind signature into only two moves to achieve round optimal, and the concurrency operation of blind signature can be reach by this.

Consider the security of blind signature: blindness and unforgeability, we provide the detail analysis. We also compare our blind signature scheme with the similar algorithm. To point out, these two schemes have their own advantage and appropriate conditions of implement way, we will describe it in the paper.

In recent years, besides e-cash, blind signatures were used in e-voting, electronic auctions and more fields of digital information. Its research direction is how to construct an efficient scheme and make it safe, as well as how to use it in the real application. In our paper, we also make the proposed blind signature scheme to be used in e-cash as an example.

KEY WORDS : Blind Signature, blindness, unforgeability, RSA, BBS, e-cash, e-voting

学位论文独创性声明

本人所呈交的学位论文是我在导师的指导下进行的研究工作及取得的研究成果。据我所知，除文中已经注明引用的内容外，本论文不包含其他个人已经发表或撰写过的研究成果。对本文的研究做出重要贡献的个人和集体，均已在文中作了明确说明并表示谢意。

作者签名：王静然　　日期：20091201

学位论文使用授权声明

本人完全了解华东师范大学有关保留、使用学位论文的规定，学校有权保留学位论文并向国家主管部门或其指定机构送交论文的电子版和纸质版。有权将学位论文用于非赢利目的的少量复制并允许论文进入学校图书馆被查阅。有权将学位论文的内容编入有关数据库进行检索。有权将学位论文的标题和摘要汇编出版。保密的学位论文在解密后适用本规定。

学位论文作者签名：王静然　　导师签名：

日　　期：20091201　　日　　期：2009.12.01

第一章　绪论

1.1　研究背景和意义

近几十年，随着现代通信技术的迅速发展和普及，由通信与计算机相结合而诞生的计算机互联网络迅速渗入到人们的日常生活和工作学习中，网络技术的发展及网上活动的日益频繁使得如何保证及加强信息安全成为国际社会普遍关心的重大问题。数字签名是一项重要的信息安全技术，如图 1.1，它是对传统文件手写签名的模拟，签名方案以电子形式存储消息签名，它既保证电子签名如手写签名一样可靠，同时又保证签名的完整和不可伪造性，也就是说，接受者可以确信消息的确来自签名者，并且没有在传输中被改动过，但接受者却不能伪造出一个合法的可以获得别人认可的签名。更形式的说，数字签名包含三个性质：

1. 签名者事后不可抵赖自己的签名。
2. 任何人不能伪造出合法的签名。
3. 若当事人双方对签名的真实性发生争执，可以在公正的仲裁者面前通过验证签名来确定真伪。

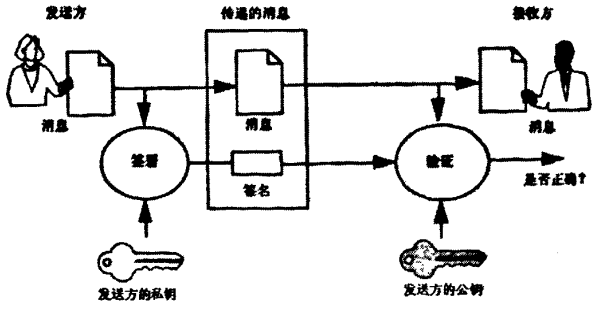

图 1.1: 数字签名

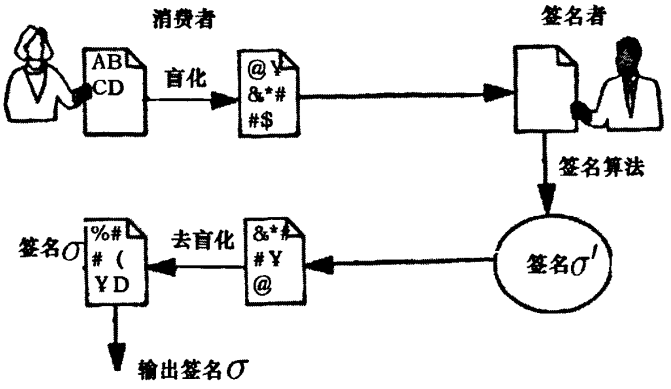

图 1.2: 盲签名

随着数字签名应用的不断扩展，又出现了很多不同形式的需要电子签名的领域，而签名的附加条件也多种多样起来。其中电子商务的发展，电子货币作为一个新型的网络货币的出现，使得盲签名应运而生。盲签名（如图 1.2）是这样一类特殊的数字签名，在满足数字签名的一般要求以外，还有自身的设置。一般的数字签名，签名者知道自己所签消息的内容，在电子货币中，使用货币的人希望能够成功的在银行领取电子现金，从而实现与商家的电子交易，但不希望银行知道自己账户变化的详情（花了多少钱）。盲签名就保证了这点，“盲”即意味着签名者对消息进行签名但又不知道消息的具体内容。这一特点除了应用在电子货币支付之外，还可以保证电子选举中消息的匿名性，它实现了签名使用者的私人信息不会被外界所获得。在注重个人隐私的现代社会中，网络使用的频繁使盲签名的应用方面越来越广泛，盲签名技术自从首次提出后，除了应用于电子支付、电子选举、电子拍卖等领域之外，在匿名证券交易、口令认证、遗嘱签署、证书的颁发和密钥分配等领域也有重要的应用。

下面举个实际中的例子说明盲签名的使用：在因特网上购买商品或服务已经是现在比较流行的消费手段，消费者要向供应商(由银行)付款，他们发出包含有他的银行帐号或者花费金额等方面的信息，由银行作出(电子)签名才能生效，但付款金额之类的信息又不希望泄露给签名者，以保证自己的隐私和使用安全。

盲签名方案的工作原理是这样的：消费者有消费信息m需要银行签署，但不需要让银行知道消息m的内容。设pk是银行的公开密钥，sk是私钥。消费者用他的安全通讯软件生成一个盲因子，将消息m盲化为m'发给银行系统，这样，银行收到的是被盲因子所“遮蔽”的值m'，并且它不可能从m'中获取有关m的信息。接着，银行系统生成针对m'的签名σ'并把它发给消费者，消费者接收到σ'之后，通过某种合适

的运算去除盲因子而获得真正的针对消息m的签名σ。可见，运用盲签名方案，消费者无法代替或冒充银行的签名，而银行则不知道他自己所签署的消息的真实内容。

1.2 盲签名研究和应用现状

盲签名的发展主要分为两个阶段：

第一阶段，1982年，D. Chaum首先提出了盲签名的概念，随后又提出了一个无法追踪支付系统中的盲签名方案。在此之后，盲签名便因为其潜在的应用价值得到了密码学界的极大关注。在这段时期里，研究者们陆续提出了一些性能良好的盲签名方案，如Okamato提出第一个基于Schonor签名协议的盲签名方案等。

第二阶段，上世纪90年代中期至今。盲签名的研究日益成熟。一方面，对盲签名的研究不断深入，研究者们提出了在各种特殊场合下的协议，如Brand提出的受限制的盲签名及其设计的电子货币方案等，另一方面，盲签名的研究也不断和其它密码协议或者方法交叉融合，如基于身份体系的引入，椭圆曲线算法的引入，群签名与盲签名结合的群盲签名，代理签名与盲签名结合的代理盲签名等。

Chaum[1]提出的第一个盲签名是基于RSA难解问题。后来，Juels[2] 和Pointcheval [3]给出了盲签名安全性的形式化证明。构造盲签名方案有两种基本的方法，一个是基于RSA算法，例如[4],[5],另外是基于双线性映射问题，例如[6],[3],[7]。考虑到盲因子的添加和去除，近些年来，基于双线性映射问题的盲签名方案由于计算复杂度小于基于因子分解的RSA问题而经常被研究者使用。在众多的双线性盲签名方案中，采用了Water签名方案的Okamoto方案是近些年提出的比较优秀的，它在签名方案的传输方式，对签名消息的盲化和去盲，以及对请求签名者身份的证明都很有效和成功，但此方案在消息的传输上仍然存在着计算复杂和传输消息较长的缺陷。另一方面，RSA 在构造算法上也存在着本身的优势，它的安全性比较高，算法设计思想简单，逻辑性比较强，在对安全度要求比较严格的环境中，例如银行系统与重点客户的签名协议，也会经常被采用，其中Chien[5] 的部分盲签名算法就是基于RSA问题，尽管在论文中它声称是低运算复杂度的，但从算法上面看，它是建立在RSA问题上的平方运算，而且生成的随机数也相对较多，存在可以改进的地方。

大部分安全的盲签名方案都使用了随机预言机[6],[7],[8]，随机预言模型是一般比较理想的模型，构造简单，在安全性证明上也形成了一套完整的体系。但是，随机预言模型不能用在标准模型中，而且在算法实现上也很困难，所以应用的时候，在保证算法的安全系数的前提下，可以使用伪随机预言机来产生随机预言机的效果。

与此同时，很多不包含随机预言机的盲签名方案在近些年也被陆续的提出来，比如[9],[10]. 前者[9]的解决方法远远比包含随机预言机的盲签名低效，而且它的构造也很复杂，包含许多次签名者和使用者的信息交互。Okamoto的盲签名方案要相对好些，但是在签名者和使用者的信息交互上面仍然需要占用很大的带宽，增加了传输消耗。

另外，在签名双方的身份证明中，很多方案引入了零知识证明Zero Knowledge Proof(ZIP)。零知识证明又分为交互零知识证明和非交互零知识证明，前者需要签名双方的多次交互信息而验证身份，比如说$\sum$ *protocols*。后者则在引入可信任第三方的基础上共享足够的信息而不需要双方的交互，比如公共参考串Common Reference String (CRS)方法。

这些年来，由于安全性和计算复杂性以及算法效率方面的考虑，盲签名方案的构造变得越来越复杂，比如[11],[9]。消息签名者和使用者之间的交互次数越来越多，算法的计算也很繁琐。如何选择合适的算法方案，构造少而有效的交互过程，精简运算复杂度，从而节省传输带宽，提高运算效率和资源消耗仍然是需要研究的问题。

现阶段盲签名的主要问题有：

1. 盲签名算法的构造和协议的交互过程有待继续分析，在带宽和计算环境的限制下，如何减少运算复杂度，提高传输效率并保证签名的安全性仍是一个需要不断改进的问题。

2. 对现有的盲签名的安全性的分析和证明仍有待规范化和形式化。

3. 对盲签名协议的具体应用的实现上仍然需要完善。

1.3 本论文的贡献

本论文的核心研究任务是：对已有的盲签名方案进行研究和分析，针对目前盲签名方案存在的主要问题，提出改进的方法。并在提出方案的基础上，给出具体的协议实现方式。

我们的论文主要做了下面的事情：

1. 根据已经存在的基于RSA问题的盲签名算法的研究，提出一个新的支持消息恢复的最优盲签名，这个方案有两个特点：一是对盲签名消息的填充，即是把要签名的消息和一部分冗余信息通过某种手段组织在一起，以节省消息长度；二是在已知消息签名时可以做出合适的计算，从签名里面恢复完整的消息。

2. 根据对双线性等其它问题的盲签名方案的研究和是否包含随机预言机的比较，提出了一个无随机预言机的盲签名方案，这是一个基于BBS问题的盲签名，与其它签名比较，有构造方法简单，交互次数较少等特点，而不包含随机预言机，也保证了它在协议实现上的有效性。

在提出两个盲签名方案之后，我们都给出了安全性分析和参数的讨论，也与其它类似的方案进行比较，分析了我们两个方案的特色。并且，紧跟其后，我们也给出了我们提出的盲签名在电子货币中的实际应用方式，加深了对盲签名方案的理解和可用性的检测。

1.4 论文结构和组织

本文研究盲签名，全文的结构如下：

第一章主要介绍盲签名的背景和意义，首先回顾了盲签名的发展历史，然后分析了盲签名的研究和应用现状，根据对现在各种比较有用的盲签名方案的分析，提出盲签名仍然存在的问题和可能解决的方法。

第二章介绍本文中需要用到的比较基本的数论知识和密码学知识，首先介绍了盲签名方案中一般会基于的三个难解问题：RSA问题，离散对数问题和双线性映射问题，同时描述了盲签名安全性证明中需要使用的概率多项式算法及衡量算法好坏的算法复杂度的定义；然后介绍了两个重要的密码学知识：Hash函数和陷门单向置换；最后给出了签名方案的一般定义。

第三章和第四章是本文的重心，我们提出的两个盲签名方案在这里进行介绍。两个章节的安排顺序是类似的：首先给出盲签名基于的问题和盲签名算法中会使用到的算法，然后具体描述了盲签名方案和其相应的安全性证明，最后给出盲签名的效率分析和参数讨论。

第四章是盲签名方案的具体应用，分别就电子货币和电子选举两个方面详细的给出了盲签名的应用方式。

第五章是对盲签名可能的发展做出一个展望和总结。

第二章　准备知识

2.1　数学难解问题

2.1.1　RSA问题

RSA难解问题是在1978年由Rivest, Shamir 和Adleman提出，其安全性是基于大整数素因子分解的困难性，而大整数因子分解问题是数学上的著名难题，至今没有有效的方法予以解决，也就确保了RSA算法的安全性。

定义2.1.1 (RSA问题). 设$n = pq$, 其中p和q为大的素数,$\Phi(n) = (p-1)(q-1)$. 令$\mathcal{K} = \{(n,p,q,e,d) : ed = 1 \pmod{\Phi(n)}\}$, 其中公钥是$pk = (n,e)$,私钥$sk = (p,q,d)$,定义

$$e_{pk}(x) = x^e \pmod{n}, \quad d_{sk}(y) = y^d \pmod{n}$$

其中

$$(x, y \in \mathbb{Z}_n).$$

在此基础上，如果不知道私钥，我们说解密y获得x是困难的。RSA密码体制的安全性是基于相信加密函数$e_{pk}(x) = x^e \pmod{n}$是一个单向函数，其中陷门是分解$n = pq$.

对RSA方案的分解因子方法的攻击现在有大量的算法，对于大整数最有效的三个算法是二次筛法（quadratic sieve）、椭圆曲线分解算法（elliptic curve factoring）和数域筛法（number field sieve）等等，自从1983年用二次筛法成功的分解了一个69位的十进制整数以来，人们不断的对更多数位的RSA算法发起挑战，而RSA-155包括一个512比他的二进制模，在包含6个国家的300台PC和工作站的8400MIPS年的技术时间[29]，所以，现在一般在采用的RSA算法的签名方案里面都会启用1024比特或者更长的数据来保证算法的安全性。

2.1.2　离散对数问题Discrete-Logarithm problem（DL）

令p是一个长度为n比特的素数，g是循环群$\mathbb{G}$的生成元。

定义2.1.2 (DL问题). *对任意随机选取长为n比特的素数p, 给出一个随机选择的数据$a \in \mathbb{G}$, 求解$b \in \mathbb{G}$满足下式是困难的:*

$$g^b = a \pmod{p}$$

求解DL问题是困难的，但其逆运算的指数运算可以使用平方乘的算法有效的计算出来。

2.1.3 双线性对

$\mathbb{G}$是阶数q的一个加法循环群，g是它的生成元，$\mathbb{G}_1$是阶数是q的乘法循环群，生成元也是g. 令$e(\mathbb{G} \times \mathbb{G}) \to \mathbb{G}_1$是满足下列性质的双线性对：

1. 双线性：如果对于所有的$u, v \in \mathbb{G}$和$a, b \in \{0, ..., p-1\}$，我们都有

$$e(u^a, v^b) = e(u, v)^{ab}$$

2. 非退化性：存在$e(g, g) \neq 1$

3. 可计算性：存在有效算法，对于所有的$u, v \in \mathbb{G}$，$e(u, v)$是可以计算的。

2.1.4 概率多项式算法(PPT)与算法复杂度

一个算法能在以输入规模为参变量的某个多项式的时间内给出答案，则称它为多项式时间算法。这里的多项式时间是指算法运行的步数。一个算法是否是多项式算法，与计算模型的具体的物理实现没有关系。

如果在算法的过程中引入随机数，使得该算法在执行的过程中随机选择下一个计算步骤，它最后可能导致结果也是不确定的。这就是概率算法。

而两者都具备的话就称为概率多项式算法（PPT），这是确定算法实际可行性的一个标准。

算法复杂度包含时间复杂度和空间复杂度：

时间复杂度：算法的时间复杂度是指算法需要消耗的时间资源。一般来说，计算机算法是问题规模n 的函数$f(n)$，算法的时间复杂度也因此记做$T(n) = \mathcal{O}(f(n))$。

空间复杂度: 算法的空间复杂度是指算法需要消耗的空间资源。其计算和表示方法与时间复杂度类似，一般都用复杂度的渐近性来表示。同时间复杂度相比，空间复杂度的分析要简单得多。

2.2 密码学知识

2.2.1 Hash函数和随机预言机

定义2.2.1 (Hash函数). *一个Hash函数是这样的映射簇:*

$$\mathcal{F}:\mathcal{K}\times\mathcal{D}\rightarrow\mathcal{R}$$

这里，$\mathcal{K}$是映射$\mathcal{F}$的密钥集，$\mathcal{D}$是定义域集，而$\mathcal{R}$是值域集。密钥和值域都是有限的，所有的集合也都非空.

对任意密钥$K\in\mathcal{K}$，定义映射$\mathcal{F}_K:\mathcal{D}\rightarrow\mathcal{R}$即$\mathcal{F}_K(x)=\mathcal{F}(K,Y)$,其中$x$是函数$\mathcal{F}_K$上的某个点.

在一个“理想的”Hash函数模型中，计算函数$\mathcal{F}_K$在点x处的值是得到$\mathcal{F}_K(x)$的唯一有效的方法，即使当其他的值$\mathcal{F}_K(x_1),\mathcal{F}_K(x_2),...$已经计算出来。

另外，Hash函数也可以设置成为一个不带密钥的函数。

由Bellare和Rogaway引入的随机预言模型（Random Oracle Model）提供了一个理想的Hash函数模型。在这个模型中，对于一个Hash函数$h:X\rightarrow Y$，我们仅允许随机预言机访问，这意味着不会给出一个公式或者算法来计算函数h的值。计算函数唯一的方法是访问随机预言机。对于随机预言模型下面的性质是成立的。

定理2.2.2 (随机预言模型). *假设$h:X\rightarrow Y$是随机选择的，当且仅当$x\in X$时，$h(x)$通过查询随机预言机被确定。那么对于所有的$x_i\in X/x$和$y_i\in Y$，有$Pr[h(x)=y_i]=1/M$，其中$|y|=M$。*

2.2.2 陷门单向置换

陷门单向置换是建立在单向函数的基础上的，我们先给出单向函数的定义。简单的说，单向函数就是一种容易计算而难于求逆运算的函数。

定义2.2.3 (单向函数). *函数$f:\{0,1\}^*\rightarrow\{0,1\}$如果满足下列条件，我们就称其为（强）单向函数:*

1. *易于计算: 存在一个确定的多项式时间算法，使得输入为x时输出是$f(x)$。*
2. *难于求逆: 对于一个概率多项式算法(PPT)$\mathscr{A}$，每一个正多项式$p(\cdot)$和所有足够大的n，都有:*

$$\Pr[\mathscr{A}(f(x),1^n)=f^{-1}(f(x))]<\frac{1}{p(n)}$$

简单的说，陷门单向置换就是一些具有附件属性的单向函数f_i，f_i一旦给定一个辅助输入作为指标i的陷门，就可以有效的对其求逆。指标i的陷门记为tk_i，不能由i求得，但可以有效的产生相应的序对(i, tk_i).

定义2.2.4 (陷门单向置换). 定义在集合$I \in \{0,1\}^*$上的置换集合称为陷门单向置换，如果它满足:

1. 在多项式算法时间（PPT）内存在一个算法可以输出指标i和对应的陷门信息tk_i.
2. 给定指标i，则$f(i)$是一个确定性算法，即随机选取x，计算$f(x)$是一个多项式算法.
3. 给定指标i，和对应的陷门信息tk_i，$f(x)$是可逆的，即对于$y = f(x)$可以唯一高效的计算$f^{-1}(y)$.
4. 在没有知道陷门tk_i的情况下，任意的多项式算法$\mathscr{A}$想计算出$f^{-1}(y)$是不可行的,即f不可逆。

这里我们可以发现，RSA难解问题是一个典型的陷门单向置换。

2.2.3 签名方案

签名方案又称数字签名，一个签名方案包含三个算法：密钥产生算法，签名算法和验证算法，密钥产生算法生成签名方案所需要的公钥和私钥，签名者使用签名算法和私钥对消息进行签名，签名结果可以使用公开的验证算法得到验证。给定数据消息和其对应的签名，验证算法可以判断签名是否合法并返回对应的true或者false。下面我们给出更准确的定义。

定义2.2.5. 一个签名方案包含一组PPT算法$(KeyGen, Sign, Vrfy)$满足下列性质:

1. $KeyGen$是一个随机的密钥生成算法，输入的安全参数是1^k，产生一组密钥对：公钥pk和私钥sk.
2. 签名算法$Sign$使用输入密钥sk和消息m，输出一个签名σ。我们记作$\sigma \leftarrow Sign_{sk}(m)$.
3. 验证算法$Very$的输入是公钥pk和消息m，以及签名σ，输出一个比特b，如果签名合法，则$b = 1$，否则$b = 0$。我们记作$b = Vrfy_{pk}(m, \sigma)$.

第三章　支持消息恢复的最优盲签名

3.1　盲签名体制

3.1.1　盲签名定义

盲签名方案是数字签名的扩展，其过程比一般的签名方案多了一个盲化消息和去盲化的过程，从而保证消息不会被签名者所知道。

定义3.1.1 (盲签名). 一个盲签名方案包含两个交互方签名者和使用者(S,U)和一组算法$(KeyGen, Sign, Vrfy)$。

1. $KeyGen$是一个概率多项式算法，以安全参数1^k作为输入，输出一对公钥和私钥(pk, sk)。

2. S和U是一对多项式交互概率图灵机，输入是公钥pk。sk是S私有的，而消息m是U拥有的并通过算法或者S对其的签名。

   在算法$Sign$中，U首先把消息m盲化为m'，再把它发给签名者S。S对消息m'进行签名，得到结果σ'并把它发给使用者U。U最后对签名去盲化生成针对消息m的签名σ。算法$Sign$最终输出(σ, m)或者$fail$。

3. $Vrfy$也是一个多项式时间算法，它的输入是(pk, m, σ)，经验证如果σ是消息m的签名，那么它输出$accept$，否则输出$reject$。

3.1.2　安全性定义

盲签名的安全性包含两点：盲性和不可伪造性

1. 盲性(blindness)：签名者对所签名的消息是盲的，即签名者不知道签名的消息的内容，即使公布消息及其签名，签名者也无法追踪签名和消息的对应关系。

定义3.1.2 (盲性). 如果任何PPT算法S在下面攻击中成功的概率是可以忽略的，那么盲签名算法就满足盲性:

(a) S输出公钥pk和一对相同长度的消息m_0, m_1。

(b) 随机选择一个比特b, S与两个诚实的使用者进行交互，

$$U_b = U_{pk}(m_b), U_{\bar{b}} = U_{pk}(m_{\bar{b}}),$$

当交互算法执行完后，签名σ_0, σ_1定义为:

如果任何一个使用者U_b或者$U_{\bar{b}}$终止了，那么$(\sigma_0, \sigma_1) = (\perp, \perp)$。否则，令$\sigma_0$(或者$\sigma_1$)是$U_0$(或者$U_1$)的输出。

(c) 最后，S输出一个比特b'。

定义S成功的概率是

$$Adv_S^{blind} = \Pr[b' = b] - 1/2.$$

2. 不可伪造性(unforgebility): 除去签名者自己以外，给出一个消息，任何人(包括合法的U)都不可以伪造出对应的签名。

定义3.1.3 (不可伪造性). 对任意攻击者F如果满足下面实验得到的成功概率是可忽略的，那么盲签名方案就是不可伪造的:

(a) 密钥生成算法$KeyGen$生成(pk, sk)，F可以得到公钥pk。

(b) F可以和诚实的签名者执行多项式次盲签名算法，得到n个签名$\sigma_1, ..., \sigma_n$。

(c) 最后F输出一组消息和其对应的签名

$$(m_1, \sigma_1), ..., (m_{n+1}, \sigma_{n+1}).$$

定义F成功的概率是。

$$Adv_F^{unforg} = \Pr[\forall 1 \leq i \leq n+1, Vrfy(pk, (m_i, \sigma_i)) = 1]$$

3.1.3 典型的盲签名方案

大多数的盲签名方案都是基于签名方案为基础的，下面我们介绍两个盲签名方案的典型例子。其中签名者和使用者分别用S和U表示。

RSA盲签名

Chaum于1982年提出盲签名的概念，并给出了第一个基于RSA难解问题的盲签名方案。

1. 密钥产生算法$KeyGen$产生满足RSA问题的公钥$pk = (n, e)$和私钥$sk = (p, q, d)$。

2. 签名算法$Sign$:

   - U获得公钥随机选择$r \in \mathbb{Z}_n$，把消息m盲化为$m' = mr^e \pmod n$发给S。
   - S拥有私钥sk，对消息m'签名$\sigma' = m'^d \pmod n$ 然后把σ'发给U.
   - U对σ'去盲化处理，$\sigma = \sigma'/r \pmod n$.

3. 验证算法$Vrfy$验证等式$m = \sigma^e \pmod n$是否成立，如果成立，输出签名σ，否则输出$fail$.

基于Schnorr的盲签名方案

下面介绍的这个盲签名方案是基于Schnorr的协议[33]的。

1. 密钥产生算法$KeyGen$: 令群$\mathbb{G}$序是n生成元是g，其中n是一个足够大的素数。随机选择$x \in \mathbb{Z}_n$为私钥，公钥为$h = g^x$。

2. 签名算法$Sign$:

   - S随机选择$u \in \mathbb{Z}_n$，计算$a = g^u$并把a发给U。
   - U随机选择$v, w \in \mathbb{Z}_n$，计算$a' = ag^v h^w, c' = H(a', m), c = c' - w$，其中$H$是一个Hash函数。$U$把$c$发给$S$.
   - S计算$r = u + cx$并发给U.
   - U首先验证等式$g^{r'} = a'h^{c'}$是否成立，如果成立，计算$r' = r + v$，输出签名$\sigma = (c', r')$，否则算法终止。

3. 验证算法$Vrfy$验证等式$m = H(g^{r'}h^{-c'}, m)$是否成立，如果成立，输出签名σ，否则输出$fail$.

3.2 基本问题

定义3.2.1 (RSA求逆问题(Chosen-target Inversion Problem): RSA-ACTI). 令k是安全参数，有下面的实验$Exp_{\mathscr{A}}^{rsa-acti}$:

1. *RSA* 密钥产生算法$KeyGen$: 输入k，选择两个不同的奇素数p,q，计算$N = pq$并且$2^{k-1} \leq N \leq 2^k$; 选择e满足$gcd(e,\phi(N)) = 1$，计算d满足$ed \equiv 1 \pmod{\phi(n)}$。于是我们得到公钥$pk = (e,N)$和私钥$sk = (d,p,q)$.

2. 攻击者$\mathscr{A}$可以得到公钥$pk = (e,N)$，它可以访问*RSA*求逆预言机$(\cdot)^d \pmod N$并且可以不超过q次询问预言机$\mathcal{O}_N$，最终它会输出$(\pi : x_1,...,x_m)$满足下列三个条件:

   - $\pi : \{1,...m\} \to \{1,...,n\}$是单射的。
   - 对任意$i \in \{1,...m\}$都有$x_i^e \equiv y_{\pi(i)} \pmod N$。
   - 算法$\mathscr{A}$对$(\cdot)^d \pmod N$的访问不超过m次。

3. 如果上述三点都成立那么输出1，否则输出0.

我们定义攻击者$\mathscr{A}$成功可能是:

$$Adv_{\mathscr{A}}^{rsa-acti} = \Pr[Exp_{\mathscr{A}}^{rsa-acti} = 1]$$

Bellare在论文 [12]中指出RSA-ACTI问题是困难的当且仅当RSA-CTI 问题是困难的，而RSA-CTI 问题又可以规约到RSA问题，这也就意味着RSA-ACTI问题是困难的当且仅当RSA 问题是困难的（归纳推理），我们将使用这一点来证明后面要提出方案的不可伪造性。

3.3 具体的盲签名方案

这一部分，我们将具体描述一个支持消息恢复的最优盲签名方案。首先给出相对于有限长度消息的盲签名方案构造，然后我们将把它扩展成一个可以为更长的消息进行签名的方案。

令$(KeyGen, Sign, Vrfy)$是三个组成盲签名方案的算法，下面给出它的具体描述:

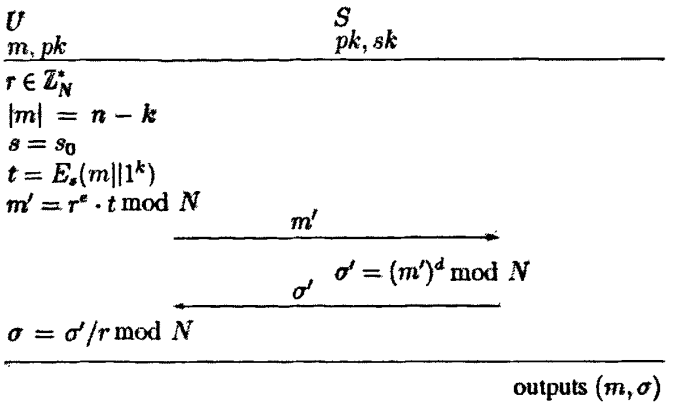

图 3.1: 短消息的盲签名方案

- 密钥生成算法$KeyGen$: 盲签名方案运行签名算法产生公钥$pk = (e, N)$和私钥$sk = (d, p, q)$，这些参数的产生类似于RSA算法，这里不再详述。另外，密钥产生算法也生产一个公共字符串$s_0 \in \{0,1\}^l$作为初始参数。

- 签名算法$Sign$: 这个算法需要使用一个分组密码$E(\cdot) : \{0,1\}^l \cdot \{0,1\}^n \rightarrow \{0,1\}^n$。

  - 对消息m的盲化: 使用者U首先随机选择$r(r \in \mathbb{Z}_N^*)$。令$|m| = n - k$，U计算

    $$s = s_0, t = E_s(m||1^k), m' = r^e \cdot t \pmod{N}$$

    并把m'发送给签名者。

  - 签名者S计算$\sigma' = (m')^d \pmod{N}$并把签名$\sigma'$发给使用者。

  - 在签名算法的最后，U去盲化签名，计算$\sigma = \sigma'/r \pmod{N}$并输出$(m, \sigma)$作为此算法的盲签名。

- 验证算法$Vrfy$: 对$s = s_0$，通过验证等式

  $$s = s_0,\ \sigma^e =^? E_s(m||1^k)$$

  是否成立，任何人都可以验证此签名。

我们在图 3.1里列出了这个盲签名方案。

盲签名正确性: 对上面的算法方案，我们可以通过下面的方法来判断它的正确性，这里$|m| \leq n$ 并且$s = s_0$:

$$\begin{aligned} \sigma^e &= (\sigma'/r)^e \pmod N \\ &= ((m')^d/r)^e \pmod N \\ &= ((r^e \cdot t)^d/r)^e \pmod N \\ &= t \pmod N \\ &= E_s(m||1^k) \pmod N. \end{aligned} \tag{3.1}$$

消息恢复: 使用者可以很容易根据盲签名算法的签名恢复原始的消息：通过计算

$$s = s_0, E_s(m||1^k) = \sigma^e \pmod N, (m^*||1^k) = E_s^{(-1)}(\sigma^e)$$

然后最终得到$m = m^*$.

如果这个等式成立的话，它将接受σ是消息m的有效签名，否则，算法失败。当验证成功之后，它也可以仅保留签名而不保留消息，下次使用时，则可直接从签名中恢复消息。

3.4 安全性分析

盲性

正如Juels [2]所说，盲性是盲签名方案的一个很重要的属性，我们的算法使用了和Chaum [1]的论文相同的算法（一个盲因子r的引入）保证了方案的盲性。

定理3.4.1. *上述提出的支持消息恢复的最优盲签名方案是满足盲性的.*

证明. 令S^*是一个概率多项式算法，它按下面方式执行盲签名游戏：对$i = 0, 1$，S^*在和诚实的使用者U执行签名算法的时候可以获得$pk_i, sk_i, m_i', \sigma_i'$，它要输出一个比特$b$实现对$i$的猜测。

假设S^* 在执行盲签名游戏[定义3.1.2]在第二步得到$\perp$而终止的话，我们很容易看出S^*赢得这个游戏的概率不会比1/2大，也就是说它只能对b进行随机猜测。

否则，假设S^*在与U交互后可以获得两个签名σ_0 和σ_1，我们回顾盲签名算法，可以发现除非知道盲因子r，否则S不能获得任何有用的信息。我们还可以看到，无论$pk_i, sk_i, m_i', \sigma_i'$是什么，$r$始终是存在的。因此，在这个盲签名算法中，$pk_i, sk_i, m_i', \sigma_i'$一直保持着等价的关系，这就意味着即使是非常强大的攻击者算法S^* 也只能随机的猜测b的值，就像抛硬币一样，它成功的可能性不会大于1/2。 □

不可伪造性

下面，我们将证明，上面的盲签名方案是基于RSA-ACTI的不可伪造的。也就是说，如果我们可以成功的伪造一个此盲签名的合法签名，那么我们就可以以概率多项式算法（PPT）时间赢得$Adv_{\mathscr{A}}^{rsa-acti}$攻击游戏。这会直接导致对RSA求逆问题 [12]的成功攻击。

下面我们开始做[定义3.2.1]里RSA求逆问题的攻击游戏。附加的条件是攻击者可以已知$E(\cdot)$的逆运算。我们通过维护一个列表E-List来模拟理想的分组密码预言机E。每当询问这个预言机的时候，首先检查在列表E-List是不是已经有了相关的数据，如果有，那么直接回答这个数据，否则，随机选择$y \in \mathbb{Z}_N^*$，在列表中创建$E_s(M) = y$并把y作为答案返回。

现在我们可以给出这个盲签名方案的不可伪造性证明。

定理3.4.2. *如果RSA-ACTI问题是难解的，那么我们的支持消息恢复的最优盲签名也是多项式安全的。换句话来说，对应本盲签名方案的攻击者$\mathscr{F}$，必有一个RSA-ACTI的攻击算法$\mathscr{A}$并且存在满足下式:*

$$Adv_{\mathscr{F}} \leq Adv_{\mathscr{A}}^{rsa-acti}.$$

Proof. 攻击者$\mathscr{A}$ 使用盲签名攻击算法$\mathscr{F}$来达成对RSA-ACTI问题的成功攻击。下面游戏执行的时候，它需要为$\mathscr{F}$提供预言机的回答。

攻击算法$\mathscr{A}^{(\cdot)^d \pmod N, \mathcal{O}_N}(N, e, k)$ 按照下面的步骤执行游戏：

1. 提供输入N, e, k，$\mathscr{A}$运行盲签名攻击算法$\mathscr{F}$，并按照下面所述提供预言机的回答：

   当$\mathscr{F}$ 向分组密码E提交消息M_i时，如果$E_s(M_i)$还没有定义，那么随机选择$E_s(M_i) \leftarrow \mathcal{O}_N$，在表格$E$-List创建一个$E_s(M_i)$并把它作为回答返回。

   如果$\mathscr{F}$提交一个RSA逆运算（RSA-inversion）的询问y，算法$\mathscr{A}$把y提交给RSA求逆预言机$(\cdot)^d \pmod N$并返回它的回答。

   用这种方式，$\mathscr{F}$ 执行[定义3.1.3]中的不可伪造性实验并输出一组数据

   $$((M_1, x_1), ..., (M_m, x_m)).$$

2. 算法$\mathscr{A}$ 得到上面的一组数据，计算$\pi(i) \leftarrow Find(x, x_i)$。在这一步中，$Find$是一个子程序，它的功能是在一组给定的数据中寻找请求的某个值。它的输入是一组值x_i，然后返回一个目标值x，这个x已知是在此组数据中的。$Find$最后将输出索引i满足$x = x_i$。

3. 算法$\mathscr{A}$最后输出$(\pi, x_1, ...x_t)$，这组数据满足定义3.2.1中的条件。

□

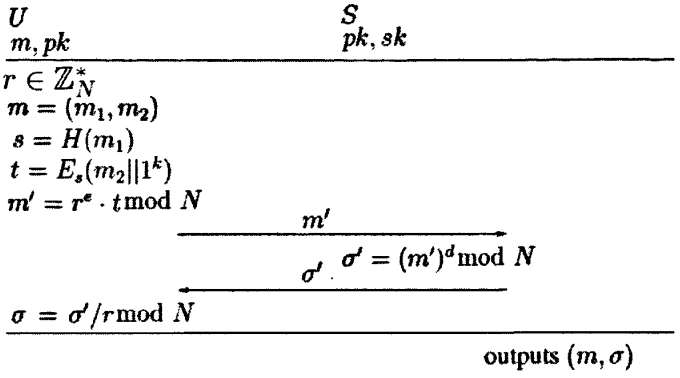

图 3.2: 长消息的盲签名算法协议

3.5 长消息的盲签名方案

我们现在给出时候长消息的盲签名方案。

密钥产生算法$KeyGen$: 运行密钥产生算法得到基于RSA问题的密钥对：公钥$pk = (e, N)$和私钥$sk = (d, p, q)$，这个过程和上面的短消息盲签名是相同的。

盲签名算法$Sign$: 在这步中，需要使用一个Hash函数$H : \{0,1\}^* \to \{0,1\}^l$ 和一个分组密码$E(\cdot) : \{0,1\}^l \times \{0,1\}^n \to \{0,1\}^n$。

1. 要签名的消息是m，盲签名使用者U 首先随机选择$r(r \in \mathbb{Z}_N^*)$给消息m做盲化处理。

   当$|m| > n$时，令$m = (m_1, m_2)$，它的长度空间是$\{0,1\}^{s-n} \times \{0,1\}^{n-k}$，使用者$U$计算$s = H(m_1)$ 和$t = E_s(m_2||1^k)$，然后盲化消息m得到$m' = r^e \cdot t \pmod N$。U把m'发给签名者。

2. 签名者S计算$\sigma' = (m')^d \pmod N$，然后把签名σ' 发给使用者。

3. 在签名算法的最后，U首先去盲化签名，计算$\sigma = \sigma'/r \pmod N$，然后输出$\sigma$作为本盲签名算法的实际签名。

验证算法Vrfy: 任何人都可以按照下面方法来验证签名：计算$s = H(m_1)$，验证等式

$$\sigma^e =^? E_s(m_2||1^k)$$

是否成立，其中$m = (m_1, m_2)$，m的消息长度空间是$\{0,1\}^{s-n} \times \{0,1\}^{n-k}$。

我们在图 3.2中列出了此盲签名算法。

3.6 参数讨论

为了协议实现的安全，n 必须比冗余信息k要大得多，一般情况下，如果单向陷门函数是$2k$比特安全的，我们就可以设计一个k比特安全的盲签名方案，其冗余信息（消息扩展）也不超过k比特。根据论文 [13]中的定理所述，我们的消息填充实现了一个最优（optimal）的盲签名。

由于本部分的盲签名方案是基于RSA难解问题的，而关于RSA安全参数的设置，根据Lenstra-Verheul论文 [14]中的说法，如果RSA是(t,ε)安全的，那么$t/\varepsilon \geq 2^{80}$。因此，这个盲签名方案的参数可以设置为$n = 1024, k = 81$，这样我们可以得到一个80比特安全的盲签名协议。

盲签名方案中我们还用到一个Hash函数$H : \{0,1\}^* \rightarrow \{0,1\}^{256}$，它可以看作一个随机预言机(例如SHA-256)。另外我们可以选择一个分组密码，比如说NUSH来实现密钥的运算部分$E(\cdot) : \{0,1\}^l \times \{0,1\}^n \rightarrow \{0,1\}^n$，而考虑到消息的长度问题我们可以使用分组密码链接模式Cipher Block Chaining Mode(CBC)把分组密码构造成多轮的加密方案。

3.7 和其他方案的比较

近些年来，研究者们提出了很多盲签名，很多方案由于冗余信息很长，而产生更长的签名。我们的最优盲签名填充把签名的消息和冗余信息巧妙的绑定在一起，极大的缩短了前面的长度。另外，我们的消息也是可以恢复的，这为签名者和使用者都提供了方便。

下面我们把这个有消息恢复的盲签名填充方案和几个类似的方案进行对比，具体的细节列在了下面的表格中，这里用h表示哈希算法，用m表示标量乘，用e表示指数算法，用p表示双线性算法，从表中可以看出，本文和Chien的算法相比，同样采用了RSA问题，但在指数运算和乘运算上面都小了很多，而和SH的算法相比，乘运算上面小了一些，但由于对方采用的是双线性问题，因此没有指数运算，但引入了双线性运算，双线性运算构造复杂，且条件约束也较多，在某些安全系数要求比较高的场合中，本部分的方案更有优势。因此，和其它类似的方案相比，我们的方案有着相应的计算或者安全上的优势，因此我们改进了盲签名的算法。

表 3.1: 和其它方案的比较

方案	消息恢复	基于问题	签名算法	验证算法
Our	Yes	RSA	$2h+2e+m$	$2e+h+m$
SH's [6]	Yes	双线性	$8m+2p+h$	$p+m$
Chien's [5]	No	RSA	$13m+8e+2h$	$2m+2h+e$

3.8 小结

这个章节中提出了一个可以实现的最优盲签名，此方案还有可以消息恢复的性质。与其它的类似方案对比，我们的盲签名消息长度比较短，这样大大节约了传输带宽和网络负担。而基于RSA的难解问题，也使得这个盲签名方案足够有效和安全。

第四章　无随机预言模型的盲签名

和上面介绍盲签名的顺序一样，我们也先介绍盲签名所依据的基本问题。

4.1　基本问题

4.1.1　BBS问题

Boneh和Boyen[16]构造了一个算法，Qian[15]在最近的一篇论文中证明了它，并把它改为一个不包含随机预言机的安全的模型，本文的盲签名方案的安全性则基于这个BBS问题，下面我们给出它的定义。

定义4.1.1 (BBS问题). 令$e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$是如上所述的双线性映射，随机选择$x, u_0, u_1 \in \{0, ..., p-1\}$，我们有$X = g^x, U_0 = g^{u_0}, U_1 = g^{u_1}$和$y = e(g,g)^x = e(X,g)$，这里我们把$(x, X)$作为私钥，$U_0, U_1, y$作为公钥。

当输入消息m，算法随机选择$r \in \{0, ..., p-1\}$，计算$\sigma_1 = X(U_0 U_1^m)^r, \sigma_2 = g^r$，输出$\sigma = (\sigma_1, \sigma_2)$。

在不知道私钥的情况下，根据签名σ求解m是不可解的。

4.2　零知识证明

为了证明签名的双方是诚实的，我们的方案里还包含了零知识证明的部分。

零知识证明Zero Knowledge Proof(ZK)，是由Goldwasser等人在20世纪80年代初提出的，证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄漏任何关于被证明消息的信息，如图[4.1]所示。在Goldwasser等人提出的零知识证明中，证明者和验证者之间必须进行交互，这样的零知识证明被称为交互零知识证明。80年代末，Blum等人进一步提出了非交互零知识证明的概念，用一个公共参考串Common Reference String(CRS)代替交互过程并实现了零知识证明。

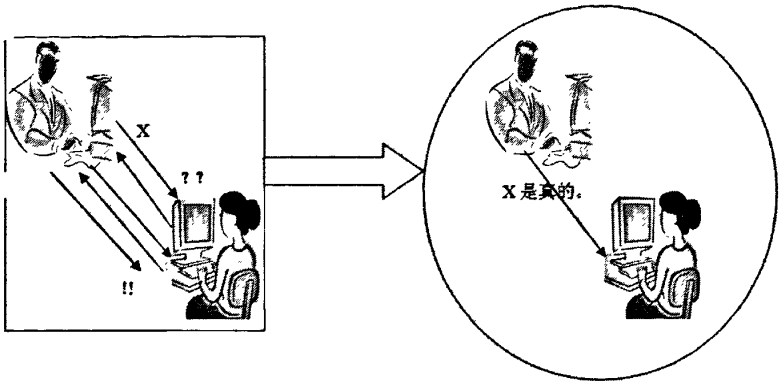

图 4.1: 零知识证明

实现零知识证明的协议有很多，比如$\Sigma - Protocols$等。我们的盲签名方案既可以使用交互零知识证明：根据需要构造一个交互的证据不可区分Witness-Indistinguishable Proof(WIP)以完成交互式零知识证明；同时也可以使用非交互零知识证明：公共参考串CRS，下面我们将分别介绍。

4.2.1 证据不可区分性证明Witness-Indistinguishable Proof(WIP)

构造WIP的方法很多，例如[17],[18]，主要是实现两个功能：

1. 验证者不能得到任何有关证据（witness）的信息：保证盲签名方案里对消息m盲化。
2. 无论在验证前还是验证后，被验证者是不能对证据进行更改：保证c一定是由t和m生成（c的产生见后文）。

我们这里给出一个比较简单的方法，从而不对盲签名算法复杂度造成影响。

- 使用者首先随机选择$\alpha, \beta \leftarrow^r \{0, ..., p-1\}$，计算$y = g^{-\alpha} U_1^{-\beta}$，然后把$y$同$c$一起发给签名者。在这里可以看到，$y$和$c$的长度是相同的，这保证了没有提高盲签名算法的复杂度。
- 签名者随机选择$a \leftarrow^r \{0, ..., p-1\}$发给使用者。
- 使用者计算$T = t + a\alpha, S = m + a\beta$并把$T, S$发给签名者。
- 签名者验证等式$c = g^T U_1^S y^a$是否成立，如果成立，则WIP执行成功，盲签名算法继续进行，否则算法终止。

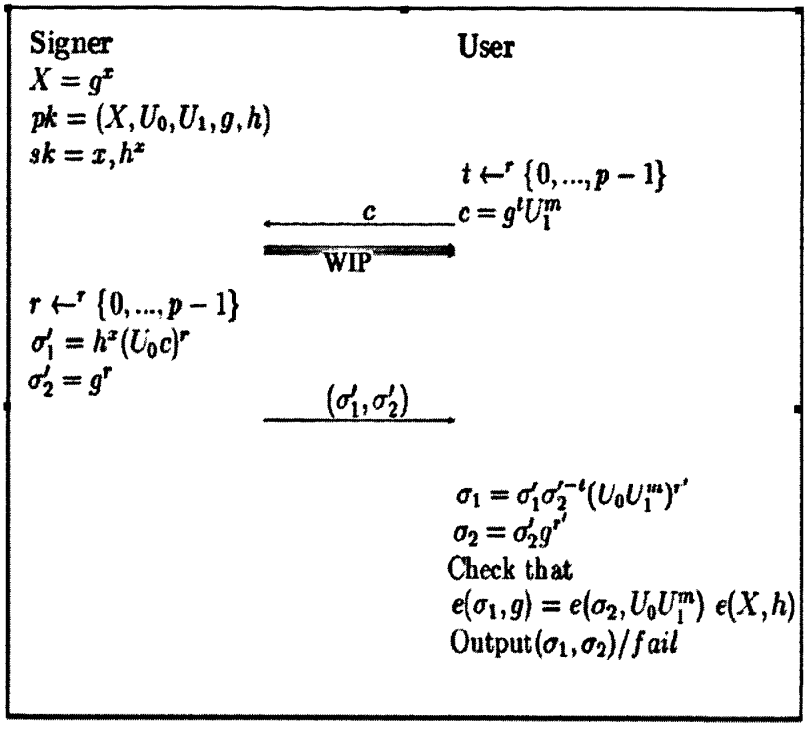

图 4.2: 无随机预言模型的盲签名算法协议

4.2.2 公共参考字符串Common Reference String(CRS)

在公共参考字符串中，我们假设交互的双方都可以访问一个公共的字符串，并且，协议的双方在交互的过程中都不知道产生这个字符串的陷门，这个陷门是在安全性证明中被模拟器所获得。在实际使用中，一个可信任的第三方可以通过CRS生成算法$K : (CRS, \tau) \leftarrow K(1^\lambda)$产生一个CRS，然后丢掉陷门$\tau$。公共参考字符串CRS是公开的，交互的双方都可以得到它。在下面的盲签名方案里面，可以将签名使用者的要证明的信息包含在这个公共参考串中，以实现非交互的零知识证明。

4.3 盲签名方案

图片 4.2里面给出了协议的实现图表。

我们的方案包含两个交互方签名者和使用者(S, U)和一组算法$(KeyGen, Sign, Vrfy$

1. 密钥产生算法$KeyGen$：令$\mathbb{G}, \mathbb{G}_1$是序为p的双线性群，$e: \mathbb{G}\times\mathbb{G} \to \mathbb{G}_1$是安全的双线性映射，算法随机选择$g, h \in \mathbb{G}$和$x \in \{0, ..., p-1\}$，然后选择$U_0, U_1 \in \mathbb{G}$。输出一对公钥$pk = (X, U_0, U_1, g, h)$和私钥$sk = x, h^x$，其中$X = g^x$。

2. 签名算法$Sign$：U通过下面的步骤获得对消息m的签名：

   - U随机选择$t \leftarrow^r \{0, ..., p-1\}$，计算$c = g^t U_1^m$并把$c$发给签名者$S$。
   - 为了证明U没有欺骗签名者，S和U之间要执行一个证据不可区分WIP的零知识证明，具体的证明按照上文所述，如果这个证明失败了，那么U会在这里终止算法。另外，这个证明是非常短而有效的，而我们的安全性证明也不依赖于这个算法，所以我们可以仅仅把它当做一个“黑盒子”来处理。
   - S和U零知识证明验证成功后，随机选择$r \leftarrow^r \{0, ..., p-1\}$，并使用密钥$sk$计算$\sigma_1' = h^x(U_0 c)^r$和$\sigma_2' = g^r$，然后把签名$(\sigma_1', \sigma_2')$发给$U$。
   - U首先验证签名(σ_1', σ_2')，如果不成功，那么终止算法。否则，U随机选择$r' \leftarrow^r \{0, ..., p-1\}$并计算$\sigma_1 = \sigma_1' \sigma_2'^{-t}(U_0 U_1^m)^{r'}$和$\sigma_2 = \sigma_2' g^{r'}$，产生对应消息$m$的真正签名$(\sigma_1, \sigma_2)$。

3. 要验证对应消息m的签名(σ_1, σ_2)，只需要检查等式

$$e(\sigma_1, g) = e(\sigma_2, U_0 U_1^m)\, e(X, h)$$

   是否成立，如果成立，输出$\sigma = (\sigma_1, \sigma_2)$，否则输出$fail$。

在此方案的基础上，WIP的任务是完成使用者对c一定是由t和m生成的证明，而改成以CRS为基础的非交互式零知识证明，则是通过可信任第三方的帮助，使得盲签名算法只包含两次交互，从而实现轮优先。我们在上文对CRS的使用做了说明，Hazay[19]的论文给出了非交互零知识证明的更详细的构造方法。

4.4 安全性分析

1. 盲性

   假设存在一个攻击者S^*，对$i = 0, 1$，S^*作为一个不可信的签名者与一个诚实的使用者U 执行盲签名算法，获得数据$pk_i, sk_i, m_i, \sigma_{i1}, \sigma_{i2}$，攻击算法执行完后，$S^*$输出$b$实现对$i$的猜测，如果猜测成功，那么我们说算法成功，否则失败。后面我们将通过几个实验，来讨论S^*成功的可能不会大于$1/2 + \epsilon$，其中ϵ是一个可忽略的概率。

- 实验G_0：S^*仅仅执行盲签名算法获得数据$pk_i, sk_i, m_i, \sigma_{i1}, \sigma_{i2}$，此时$S^*$猜测$b$成功的概率是$1/2$。
- 实验G_1：S^*在获得c_i时尝试对b进行猜测，由于t_i是随机选取的，而我们盲签名中的WIP 是安全的“黑盒子”，所以S^*无法比试验U_0中获得更多的可用的消息。
- 试验G_2: S^*在获得U最终给出的签名σ_{i1}, σ_{i2}时尝试对$\sigma'_{i1}, \sigma'_{i2}$与$\sigma_{i1}, \sigma_{i2}$对应关系的猜测，这一步，由于$U$在给出最终的签名前对$\sigma'_{i1}, \sigma'_{i2}$去盲化并做了一个随机处理，$r'$是随机选取的，这也保证了这一步签名中$S^*$得不到更多的信息。

从上面的3步试验可以看出，无论$pk_i, sk_i, m_i, \sigma_{i1}, \sigma_{i2}$是什么，随机值$r, r'$都是存在的，因此每一次盲签名算法的执行，$pk_i, sk_i, m_i, \sigma_{i1}, \sigma_{i2}$都会存在相同的对应关系，也就是说，攻击者$S^*$是无法比随便猜测$b$的值更大的概率来完成攻击实验的。所以我们的盲签名方案可以满足盲性。

2. 不可伪造性

本文的盲签名方案的签名部分是基于BBS问题的，通过 4.2可以很容易看出如果存在一个攻击者U^*可以成功伪造一个签名实现对盲签名签名方案的攻击，那么BBS问题就不是难解的，这也就说我们的盲签名方案是满足不可伪造性的。

首先，假设有攻击者U^*可以与签名者S进行交互，在只允许不超过n次执行盲签名算法的基础上最后产生$n+1$个合法的签名

$$(m_1, \sigma_1,), (m_2, \sigma_2), ..., (m_{n+1}, \sigma_{n+1}).$$

由于攻击者U^*是不诚实的，那么在与签名者交互的过程中，则可以保留一个存储数据的表格，对应的存储$m_i, t_i, c_i, \sigma'_i, r'_i, \sigma_i$，这样，在$n$次的询问后，我们可以得到多于$n+1$次的表格数据，于是，我们可以成功的通过盲签名算法的逆运算得到$n+1$个满足BBS问题的(m_i, σ_i)，而其中至少一个不是通过询问盲签名算法方案得到的，这样就完成了对BBS问题的攻击。

4.5 效率分析

和上一个方案一样，下面我们将从所使用的难解问题，是否包含随机预言机，是否是轮优先的，签名算法、验证算法复杂度，是否可以并行实现等方面和本文中所提到的现在已经存在的盲签名算法进行比较。

表格1里列出了几个算法的对比，其中用h表示哈希算法，用m表示标量乘，用e表示指数算法，p表示双线性算法,为了方便比较，我们还把Okamoto里面的$\sum_protocol$部分不列入复杂度计算里面。从表格可以看出，我们的盲签名算法是不包含随机预言机的轮优先的方案，在算法的实现，算法效率，算法复杂度等方面都有了相应的提高，对本文开头提出的问题给出了解决方案。

表 4.1: 几个盲签名方案的对比

Tab. 4.1: comparison of Blind Signature Schemes

盲签名方案	包含随机预言机	轮次	签名算法	验证算法	是否可以并行
Han[6]	是	4	$8m+2p+h$	$m+p$	否
Okamoto[10]	否	5	$12e+5m+p$	$m+p$	是
Ours	否	2	$8e+5m+p$	$p+m+e$	是

4.6 小结

本章基于BBS问题提出了一个新的不包含随机预言模型的盲签名方案，与已经提出的盲签名相比较,该方案计算复杂的相对较低，需要传输信息比较少，在引入非交互式零知识证明之后，还实现了轮优先这一属性。因此在算法构造和实现上都实现了对当前盲签名算法的改进。

第五章　盲签名应用

正如第一章中所说，盲签名的实际应用很广泛，而如何把盲签名设计成为一个在生活中可以真正使用的方案也是一个研究的方向。这里我们仅仅根据上面提出的盲签名方案，做出它在电子货币中使用的最简单的方式，具体实现细节和系统实现仍有待继续研究。

5.1　电子商务模型

电子商务支付系统是电子商务系统的重要组成部分，它指的是消费者、商家和金融机构之间使用安全电子手段交换商品或服务，即把新型支付手段（包括电子现金（E-Cash）、贷记卡（CreditCard）、借记卡（Debit Card）、智能卡等）的支付信息通过网络安全传送到银行或相应的处理机构，来实现电子支付。

电子商务网上购物流程如图 5.1所示：

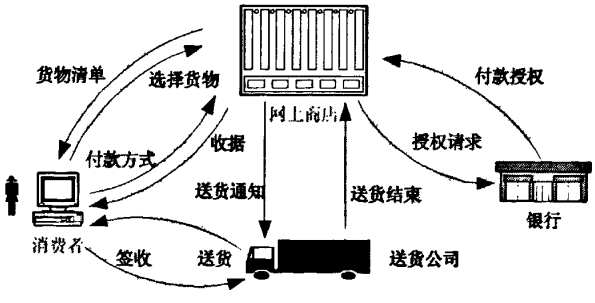

图 5.1: 电子商务网上购物流程

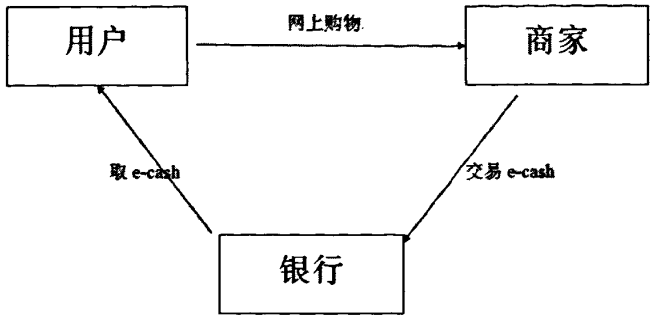

图 5.2: 电子现金使用流程

5.1.1 电子货币

电子现金(E-cash)是以电子化数字形式存在的现金货币，它可以被看作是现实货币的电子或数字模拟，电子现金以数字信息形式存在，通过网络流通。它比现实货币更加方便、经济。第一个电子现金方案是由Chaum[22]在1982年提出，他利用盲签名技术来实现，可以完全保护用户的隐私权。

电子现金在其生命周期中要经过取款、支付和存款三个过程，涉及用户、商家和银行等三方。电子现金的基本流通模式如图 5.2：用户与银行执行提取协议从银行提取电子现金；用户与商家执行支付协议支付电子现金；商家与银行执行存款协议，将交易所得的电子现金存入银行。

根据[32]中所述，电子现金应具备以下性质:

1. 独立性:电子现金的安全性无法依靠物理上的安全来保证，而是通过电子现金自身使用的各项密码技术和协议双方的交互和协商来保证电子现金的安全。
2. 不可重复花费:电子现金只能使用一次，重复花费能被容易地检查出来。
3. 匿名性：电子现金的使用不能跟踪，银行和商家联系起来也无法将电子现金的用户的购买行为联系到一起，从而隐蔽电子现金用户的个人信息隐私。
4. 不可伪造性：对应于现实中的用户不能伪造合法的货币。
5. 可传递性：用户能将电子现金与商家交易用户之间彼此转让，但这种转让时不可跟踪的。
6. 可分性：电子现金不仅能作为整体使用，还应能被分为更小的部分多次使用，只要各部分的面额之和与原电子现金面额相等，就可以进行任意金额的支付。

这些性质也就保证了电子现金可以像现实货币那样被方便而有效的使用。而使用合适的加密和签名技术，也保证了电子现金的安全性和可靠性，[32]也给出了这一点的描述。

电子现金设计的基本流程如下：

1. 注册和身份验证：用户向银行注册自己的身份ID和密码，并通过某种协议来验证自己的ID是诚实可信的。

2. 取款协议（Withdrawal Protocol）：用户在匿名的前提下可以从银行帐户提取合法的电子现金。为了保证这一点用户将与银行交互执行盲签名协议，同时银行必须确信电子现金上包含必要的用户身份。

3. 支付协议（Payment Protocal）：用户使用电子货币购买物品，分为两步：

   - 电子货币签名的验证，用于确认电子货币是合法的。
   - 用户需要向商家发送部分有关自己的身份的信息，这一步是用于防止用户多次使用该电子货币。

4. 存款协议（Deposit Protocal）：用户及商家将电子货币存入到银行账户上。在这一步中银行将检查存入的电子货币是否是合法的。如果不合法，银行可以适当的查出非法用户的身份，对其进行惩罚。

在众多的电子货币方案中，Brands[23]方案是目前公认的比较有效的电子支付系统，它具有不可跟踪，不可重复等优点已经被广泛运用在现实生活中。下面我们使用上文提出的基于RSA的盲签名技术给出一个简单的在线电子支付系统的描述，图 5.3中也给出了具体的协议交互过程：

用户注册

1. 系统的初始化：银行B首先生成RSA参数满足$n = pq, ed = 1 \pmod{(p-1)(q-1)}$。$B$随后扔掉$p$和$q$。

2. 用户注册和认证：用户U使用自己的个人ID和密码在银行提供的可信通道上注册成功，然后它就可以访问银行网页。U把自己的ID封装好后作为公共信息发送给银行B以证明自己的真实身份。

取款协议

在这一步中，U和B之间将执行盲签名协议获得它的合法电子现金e-cash.

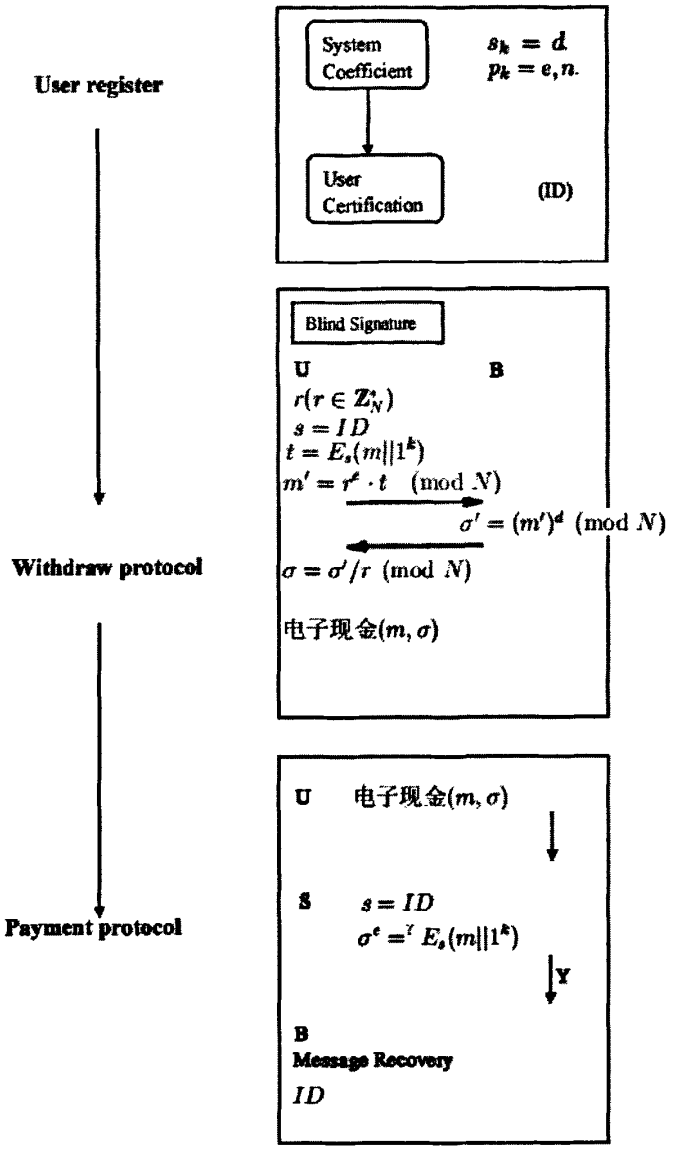

图 5.3: 基于RSA盲签名的电子现金协议

1. U随机选择长度是$n-k$的消息m，然后再随机选择$r(r \in \mathbb{Z}_N^*)$，开始计算

$$s = ID, t = E_s(m||1^k), m' = r^e \cdot t \pmod{N}$$

并把m'发给银行B.

2. 银行B计算$\sigma' = (m')^d \pmod{N}$，并把签名$\sigma'$发给用户。

3. 用户U计算$\sigma = \sigma'/r \pmod{N}$。

最终，通过上面的几步，用户就得到他的电子现金(m, σ).

付款协议

1. 用户把从银行得到的合法签名的电子现金(m, σ) 发给商家S.

2. S 首先验证电子现金的合法性：

$$s = ID, \sigma^e =^? E_s(m||1^k).$$

如果这个等式成立，那么它会把这组数据发给银行B.

3. 银行B通过这组数据恢复消息，并得到用户的身份ID信息，如果这个信息是合法的并且从来没有使用过，那么它就会给出这个电子现金的真实性的肯定并接受这部分现金并把它存到商家的账户上，于是商家就和用户达成交易。

从上面的这三个协议，我们把用户的个人身份信息封装后放入到传输的消息上面，由于对传输消息的有效的填充，考虑到现在网络的负担，我们在电子现金协议上面做出了一定的贡献，我们的盲签名有着消息恢复的机制，所以可以比较容易的恢复用户的身份ID，这样就减少了用户、银行、商家之间的交互次数，因为我们对电子现金的实现方面做出了一定的优化。

5.2 电子选举模型

电子选举也是盲签名的另一个重要应用，运用计算机和网络技术来实现投票、计票功能。与传统的选举方式相比，它不仅具有更高的效率和更大的灵活性，而且可以节省大量的人力、物力、财力。例如,选举委员会不必像传统选举那样进行人工的选票发放和选票统计工作。投票人也不必到一个固定的投票地点去投票等。

与传统选举系统相似，电子选举系统的主要参与者是投票者和选举中心。系统通常要求投票者和选举中心能够执行一些必须的多项式次计算并通过公共信道通信。

电子选举的研究开始于80年代中期，但直到1992年，Fujiola, Okamoto, Ohta[30]提出了一个实用的适用于大规模选举的方案后，电子选举方案得到了实质上的突破。

一个安全的电子选举协议需要满足一定的性质和采用相应的安全技术，论文[31]中给出了详尽的描述，如下：基本性质：合法性、完备性、匿名性、不可重复性、公正性、可验证性、无收据性。

主要安全技术的应用：

1. 盲签名技术

   电子选举的投票过程中使用盲签名技术，可以保证选票在得到鉴别的同时，能以某种办法切断投票者与选票的关系，实现了在认证的同时不泄露内容。

2. 位承诺

   电子选举中，当计票中心收集完选票后，通过位承诺保证投票者提交出与最初选择内容相同的选票。

3. 同态加密

   电子选举中使用同态加密函数加密选票，通过对加密选票进行某种运算，但不解密获得选票结果，不需要对选票解密保证了选票内容的保密性。

使用盲签名方案的电子选举很多，1992年Fujioke，Okamoto和Ohta三人提出了一个比较实用的方案[24]，后来的Sensus系统既是有这个方案演化而来，这个Sensus系统由投票人、验票机构、统计机构三个部分组成，整个投票流程由注册登记、验证选票、投票和结果公布四个步骤组成，具体流程如图 5.4所示：

1. 注册ID:选民V向注册机构R申请身份注册,得到注册号$R(ID_i)$。

2. 申请选举: 选民V用注册号$R(ID_i)$向认证机构A申请空白选票t_i。

3. ID认证:认证机构A与注册机构R之间运行认证协议，判定$R(ID_i)$的合法性。

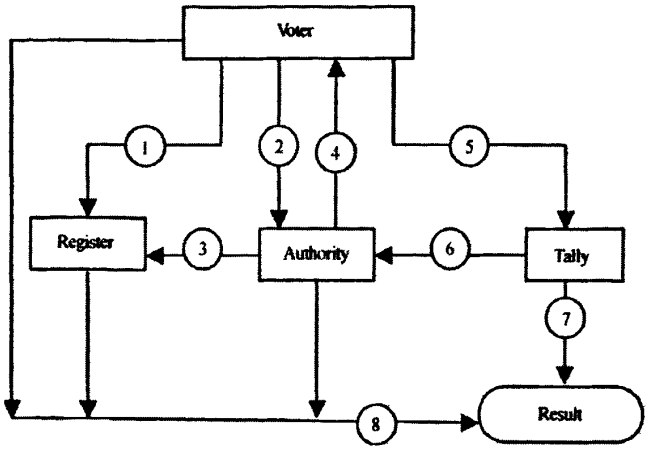

图 5.4: 电子选举流程

4. 签发选票: 认证机构A为合法选民$R(ID_i)$签发空白选票$A(t_i)$。

5. 投票: 合法选民V将自己的选票v_i发送给计票中心T。

6. 判定选票唯一性: 计票中心T与认证机构A对v_i的唯一性进行认证，接收合格选票$T(v_i)$。

7. 统计机构计算合格的选票的和: $Result = \sum_{i=1}^{n} T(v_i)$。

8. 选民、注册机构、认证机构均可以对选举结果进行验证，确认选举结果的正确性。

第六章　结束语

自从1983年Chaum 提出了首个盲签名方案之后，对盲签名定义的完善和安全性的研究到如今已有二十多年，随着签名技术的发展，构造盲签名的技术也不断更新。而通信技术的发展和网络的快速普及，又使得盲签名在实际应用中越来越重要。随着网络拓补结构的不断扩大，为了保证签名算法的性能，算法的构造也越来越复杂。这样就给安全性和算法性能带来了挑战，计算机技术的发展和计算能力的不断加强，也迫使盲签名安全强度更大，与此同时，运算时间和运算复杂度也要更加简短和方便。这些都依赖于算法的选择和具体的操作方式，以及签名双方可信度的测试。

另外，随着盲签名应用条件的扩展，盲签名和其他的签名方式不断结合，产生了花样繁多的混合签名，并且由简单的两种方案的混合（代理盲签名，群盲签名等）向多个方案结合发展（群代理盲签名，基于身份的部分盲签名等等）。这些都是盲签名的可能研究方向。

在实际应用方面，盲签名是当前广泛应用的数字签名技术的重要组成部分之一。现今，已经提出的应用主要集中在电子支付和电子现金两方面。同时，在金融合同的签署、遗嘱签署、CA 证书的颁发等方面也有重要的应用。将盲签名具体实施到实际应用中，并仍然确保现实状态下盲签名的安全，也是盲签名的一个研究方向。

参考文献

[1] Chaum D. Blind signatures for untraceable payments. Advances in Cryptology. Proceedings of Crypto, Prenum Publishing Corporation, 1982, pp.199-2004.

[2] Juels A, Luby M, Ostrovsky R. Security of blind digital signatures. Lecture Notes in Computer Science, Springer-Verlag, 1997, pp.150-164.

[3] Pointcheval D, Stern J. Provably secure blind signature schemes. Lecture Notes in Computer Science, Asiacrypt, Springer-Verlag, 1996.

[4] CHAUM D. Blind signatures for untraceable payments. Advances in Cryptology. Proceedings of Crypto, Prenum Publishing Corporation, 1982, pp.199-204.

[5] Hung-Yu Chien,Jinn-Ke Jan,Yuh-Min Tseng. RSA-Based Partially Blind Signature with Low Computation. Eighth International Conference on Parallel and Distributed Systems (ICPADS'), 2001.

[6] Han Song, Chang E. A Pairing-based Blind Signature Scheme with Message Recovery. Inernational Journal of Information Technology, 2(4),2005.

[7] Gjosteen K, Krakmo L. Round-Optimal Blind Signatures from Waters Signatures. Lecture Notes in Computer Science 5324, Springer-Verlag, 2008, pp.112-126.

[8] Bellare M, Namprempre C, Pointcheval D etal. The Power of RSA Inversion Oracles and the Security of Chaum's RSA-Based Blind Signature Scheme. Lecture Notes in Computer Science 5324, Springer-Verlag, 2002, pp.319-338.

[9] Camenisch J, Koprowski M, Warinschi B. Efficient Blind Signatures without Random Oracles, Forth Conference on Security in Communication Networks, Lecture Notes in Computer Science, Springer-Verlag, 2004.

[10] Okamoto T. Efficient Blind and Partially Blind Signatures Without Random Oracles. Lecture Notes in Computer Science 3876, Springer-Verlag, 2006, pp.80-99.

[11] Kiayias A, Zhou Hong-Sheng. Concurrent Blind Signatures Without Random Oracles. Lecture Notes in Computer Science 4116, Springer-Verlag, 2006, pp.49-62.

[12] Bellare M. The one-more-rsa-inversion problems and the security of chaums blind signature scheme. Financial Cryptography01, LNCS 2339, pp.319-338, 2001.

[13] Louis G. Short signatures in the random oracle model. ASIACRYPT 2002.Berlin:Springer-Verlag, pp.364-378, 2002.

[14] Lenstra A and Verheul E. Selecting cryptographic key sizes. PKC00, LNCS 1751, pp.446-465, 2000.

[15] Qian Hai-feng. Random-Oracle-Free Signatures and Sequential Aggregate Signatures with Short Keys. 未发表.

[16] Boneh D, Boyen X. Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles. Eurocrypt, Lecture Notes in Computer Science 3027, Springer-Verlag, 2004. pp.223-238.

[17] Feige U, Shamir A. Zero Knowledge Proofs of Knowledge in Two Rounds. Lecture Notes in Computer Science 435, Springer-Verlag, 1990, pp.526-544.

[18] Dwork C, Naori M. Zaps and Their Applications. Foundations of Computer Science, 2000. Proceedings. 41st Annual Symposium on , 2002, pp.283-293.

[19] Hazay C, Kztz J, Koo C etal. Concurrently-Secure Blind Signatures without Random Oracles or Setup Assumptions. Lecture Notes in Computer Science 4392, Springer-Verlag, 2007, pp.323-341.

[20] Bellare M, Namprempre C, Pointcheval D etal. The Power of RSA Inversion Oracles and the Security of Chaum's RSA-Based Blind Signature Scheme. Lecture Notes in Computer Science 5324, Springer-Verlag, 2002, pp.319-338.

[21] Boneh D, Lynn B, Shacham H. Short Signatures from the Weil Pairing. Lecture Notes in Computer Science, Springer-Verlag, 2001, pp.297-319.

[22] Chaum D. Blind Signatures for Untraceable Payments. Advances in Cryptology, ProcofCrypto 82. SantaBarbara, California: Springer Verlag, 1983, pp.199～203

[23] Brands S. Off-Line Cash Transfer by Smart Cards. Centre for Mathematics and Computer Science (CWI), 1994.

[24] Atsushi Fujioka, Tatsuaki Okamoto, Kazuo Ohta. A practical secret voting scheme for large scale elections. Lecture Notes in Computer Science, Springer Verlag, 1993, pp.244-251.

[25] Abe M, Fujisaki E. How to Date Blind Signatures. Advances in Cryptology2Asiacryptp96 Proceedings. Berlin : Springer Verlag , 1996, pp.244-251.

[26] Mambo M, Usuda K, Okamoto E. Proxy Signatures: Delegation of the Power to Sign Messages. IEICE Transactions on Fundamentals, 1996, 79(9): pp.1338-1354.

[27] Shamir A. Identity based cryptosystems and signature schemes. Advances in Cryptology Crypto′ 84. NewYork: Springer Verlag, 1984.

[28] Lysyanskaya A，Ramzan Z.Group blind digital signature：a scalable solution to electronic cash[C]//Proc of the 2nd Financial Cryptography. Conf，1998, pp.184-197.

[29] Wenbo Mao. Modern Cryptography: Theory and Practice. Prentice Hall PTR. July 25, 2003.

[30] Fujiola A, Okamoto T, Ohta K. A Practical Secret Votiing scheme for Large Scale Elections. Advances in Cryptology: AUSCRYPT'92, Lecture Notes in Computer Science 718, Springer Verlag, 1993, pp.615-619.

[31] 万涛，曾辉.电子选举中安全技术的应用. 中国市场. 2008年第十期. pp.91-92.

[32] 朱月珍.一类基于身份无可信中心的离线电子现金方案. 计算机应用与软件. 2009年第六期. pp.108-110.

[33] Schnoir C.P. Efficient Signature Generation by Smart Cards. Journal of Cryptology, 1991, pp.161-174 .

致　　谢

在论文结束之际，我首先要衷心感谢我的导师钱海峰副教授的谆谆教诲和悉心指导，在攻读硕士学位期间和论文写作过程中，他都给了我非常大的帮助。

感谢所有任课教师对我悉心的指导，他们的帮助使我圆满完成了各门专业课的学习任务，使我在掌握知识的深度和广度上都有长足的进步。

感谢各位师兄师姐师弟师妹们对我的帮助和鼓励，与他们进行的学术上有益的探讨以及生活上的友好相处使我受益匪浅，在此表示诚挚的谢意。

三年艰苦而充实的求学历程中，我的家人和我的朋友在背后给我始终如一的默默支持，在心灵上和生活上给予我温暖和鼓励。我学业的顺利完成与他们的无私奉献是分不开的，愿我的成绩能够给他们带去欢欣和骄傲。

再一次向所有关心和帮助过我的师长、亲人和朋友们表示诚挚的谢意！并同时也感谢各位评审老师的辛苦工作，谢谢！

王　静　然

二零零九年十月

在读期间完成的论文目录

[1]Jingran Wang, Haifeng Qian. An optimal blind signature padding with message recovery. Fifth International Conference on Information Assurance and Security (IAS09),2009,pp.673-677.

[2]王静然，钱海峰. 一个无随机预言模型的盲签名方案。计算机应用研究，2010年第4期-第5期月刊。

盲签名的研究与应用

作者：王静然
学位授予单位：华东师范大学