Pure Mathematics 理论数学, 2019, 9(5), 596-600
Published Online July 2019 in Hans. http://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2019.95079

Hans汉斯

Construction of Blind Signature Scheme Based on Quadratic Residue

Jing Luo, Ziqiang Fan

School of Mathematics and Big Data, Anhui University of Science and Technology, Huainan Anhui
Email: 847083264@qq.com

Received: Jun. 30th, 2019; accepted: Jul. 18th, 2019; published: Jul. 25th, 2019

Abstract

Blind signature was proposed based on the privacy of protected information in 1982. It plays an important role in cryptography. Based on the difficulty of quadratic residue and integer decomposition, a new blind signature scheme is proposed in this paper. By using Hash function and blind factor to blind signature information, it makes the content of the information has not been seen by the signer, thus protecting the user's information. Meanwhile, it is proved that the signature is blind and cannot be forged.

Keywords

Blind Signature, Quadratic Residue, Decomposition of Large Composite Numbers

基于二次剩余构造的盲签名方案

罗　婧，范自强

安徽理工大学数学与大数据学院，安徽　淮南
Email: 847083264@qq.com

收稿日期：2019年6月30日；录用日期：2019年7月18日；发布日期：2019年7月25日

摘　要

盲签名是在1982年基于对保护信息的私密性而提出的签名方案，在密码学中占据着重要的地位。本文以二次剩余和整数分解的困难性为理论基础，提出了一种新的盲签名方案。通过利用Hash函数以及盲因子让待签名信息盲化，使签名者不知所签名的具体信息，从而保护了用户信息。同时，还证明了该签名的盲性以及不可伪造性。

文章引用: 罗婧, 范自强. 基于二次剩余构造的盲签名方案[J]. 理论数学, 2019, 9(5): 596-600.
DOI: 10.12677/pm.2019.95079

关键词

盲签名，二次剩余，分解大合数

1. 引言

随着计算机科学技术的发展，电子商务、电子金融等系统得到了广泛的应用，数字签名的问题就显得更加突出、更加重要。1982 年 Chuam [1]为实现不可跟踪的支付系统，也就是电子现金，首次提出了盲签名的概念。盲签名与普通签名相比有两个显著特点：第一，签名者不知道所签署的数据内容。第二，在签名被接收者泄漏后，签名者不能追踪签名内容[2]。为了满足这样的条件，用户首先将待签名的数据进行盲变换，然后把变换后的盲数据发送给签名者，经过签名者签名后再发给用户。用户对签名进行去盲变换，得到的是签名者对原数据的盲签名。

盲签名可以有效地保护用户的隐私，因而被广泛的应用于需要保护个人隐私的地方。文献[3]提出了一个基于二次剩余的盲签名方案，但是没有给出它的不可伪造性。文献[4]提出了一种基于 RSA 体制的盲签名，但是计算效率较低。2011 年，文献[5]提出一种基于 Schnorr 盲签名的向前安全盲签名方案。之后，文献[6]指出文献[5]不满足可验证性和不可伪造性，并对其进行改进。本文基于二次剩余提出了一个新的盲签名方案，并且对该方案进行分析，证明了它满足盲性和不可伪造性。

2. 基本定义与相关定理

二次同余式求解问题可以归结到讨论形如 $x^2 \equiv a(\mathrm{mod}\, m)$ 的同余式，在密码学中应用很广泛，它是本文所构造的概率密码体制的数学理论基础之一。

设 n 是正整数集， $Z_n = \{x \mid 0 \le x < n, n \in N\}$， $Z_n'' = \{x \mid x \in Z_n, (x,n) = 1\}$。

定义 2.1 [7]：若 $a \in Z_n''$，且存在 x 满足二次同余式 $x^2 \equiv a \bmod n$，则称 a 为模 n 的二次同余，称 x 为模 n 下 a 的平方根，模 n 的所有二次同余的集合记为 Q_n；若 $a \in Z_n''$ 且 $a \notin Q_n$，称 a 为模 n 非二次同余 $\overline{Q}_n$。

定义 2.2：若 $n = p \cdot q$，其中 p 和 q 为两个互不相同的素数，并且满足 $p \equiv q \equiv 3 \bmod 4$，则称 n 为 Blum 数。

定理 2.1 [7]：(欧拉定理)若 $(a,n) = 1$，则 $a^{\phi(n)} \equiv 1 \bmod n$。

定理 2.2 [7]：(欧拉判别条件)若 $(a,p) = 1$，则 a 是模 p 的平方剩余的充分必要条件是 $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p)$；而 a 是模 p 的平方非剩余的充分必要条件是 $a^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\, p)$。

定理 2.3 [8]：设 p 和 q 为两个互不相同的素数，$n = p \cdot q$，则对任一整数 $a \in Z_n^*$，有 $a \in Q_n$，等价于 $a \in Q_p$ 且 $a \in Q_q$。

定理 2.4 [8]：p 为素数且 $p \equiv 3 \bmod 4$， $a \in Q_P$ (Q_p 为模 p 的所有二次同余的集合)，则 $x^2 \equiv a \bmod p$ 在模 p 下有且仅有两个平方根，分别为 $x \equiv \pm a^{\frac{p+1}{4}} \bmod p$。

引理 1 [8]：设 $N = p \cdot q$ 为 Blum 数， $a \in Q_n$， 则 $a^{\frac{\phi(n)}{4}} \equiv 1 \bmod N$。

定理 2.5 [8]：设 $N=p\cdot q$ 为 Blum 数， $a\in Q_n$ ，则对于 $x^2\equiv a \bmod N$ 有：

1) 在模 N 下有 4 个平方根。

2) 这 4 个平方根有且仅有一个属于 Q_n ，且 $x\equiv a^{\frac{\phi(N)+4}{8}} \bmod N$ 。

定理 2.6：设 $N=p\cdot q$ ，其中 p 和 q 为两个互不相同的奇素数，则分解 N 计算上等价于求模 N 的平方根。

3. 签名与验证过程

3.1. 参数生成阶段

Step1：签名者找出两个较大的素数 p、q(不能公开)，使得 $p\equiv q\equiv 3 \bmod 4$ ，同时需要计算 Blum 数 $N=p\cdot q$ ，将 N 作为验证密钥，将 p、q 作为签名密钥。

Step2：签名者选择一个结果为平方项的 Hash 函数：H：$(0,1)^*\to Z_N^*$ 。并计算 $d=(N-p-q+5)/8$ ，公开(N,H)，保密(d,p,q)。

Step3：对于明文信息 $M=(a_0,a_1,\cdots,a_n)$ ，计算 $H(a_i),i=0,1,\cdots,n$ ，再选择一个盲因子 $k\in Z_n^*$ ，计算 $M'\equiv k^2H(a_i) \bmod N$ ，得到 $M'=(a_0',a_1',\cdots,a_n')$ 。

3.2. 签名过程

Step1：用户选取随机数 b， $b\in Z$， $x_0\equiv b^2 \bmod N$ ，并把 x_0 以及待签名信息 $M'=(a_0',a_1',\cdots,a_n')$ 发送给签名者。

Step2：签名者收到用户所发送的信息后，根据 d 分别做如下计算：

$$\begin{aligned}x_1&\equiv x_0^d \bmod N\\ x_2&\equiv x_1^d \bmod N\\ &\vdots\\ x_{n+1}&\equiv x_{n+2}^d \bmod N\end{aligned}$$

得到序列 $A=(x_1,x_2,\cdots,x_{n+1})$ 。

Step3：根据待签名信息 $M'=(a_0',a_1',\cdots,a_n')$ ，签名者分别计算：$y_0=a_0'\times x_1,y_1=a_1'\times x_2,\cdots,y_n=a_n'\times x_{n+1}$ ，得到序列 $Y=(y_0,y_1,\cdots,y_n)$ 。

Step4：签名者得到 $Sign(M')\equiv Y^d \bmod N$ ，并将 $(Sign(M'),x_{n+1})$ 发送给用户，用户收到 $(Sign(M'),x_{n+1})$ 后，计算 $s\equiv sign(M')/k(\bmod N)$ ，对 M 的签名是 (s,M,x_{n+1}) 。

3.3. 签名验证过程

验证者验证的具体步骤如下：

Step 1：根据 x_{n+1} ，分别计算：

$$\begin{aligned}x_{n+1}^2&\equiv x_n \bmod N\\ x_n^2&\equiv x_{n-1} \bmod N\\ &\vdots\\ x_2^2&\equiv x_1 \bmod N\end{aligned}$$

得到序列 $A=(x_1,x_2,\cdots,x_{n+1})$ ，并计算 $T\equiv H(a_i)x_{i+1}^2 \bmod N$ 。

Step 2：验证 $s^2\equiv T \bmod N$ 是否成立，如果成立则签名有效；否则签名无效。

4. 签名方案的分析

4.1. 有效性分析

$Y=(y_0,y_1,\cdots,y_n)$，$y_i=a_i'x_{i+1}^2=k^2H(a_i)x_{i+1}^2$，$i=0,1,2,\cdots,n$。又因为$T=H(a_i)x_{i+1}^2$，$Sign(M')=Y^d \bmod N$，$s=sign(M')/k(\bmod N)$。验证$s^2\equiv T \bmod N$，即$\frac{Sign(M')^2}{k^2}\equiv H(a_i)x_{i+1}^2 \bmod N$，$Sign(M')^2\equiv k^2H(a_i)x_{i+1}^2 \bmod N\equiv Y \bmod N$，说明签名$Sign(M)=(s,M,x_{n+1})$是一个有效签名。

4.2. 盲性

盲性是盲签名的主要安全需要，它可以确保被签名消息的安全性。要证明我们的方案是盲的，只要证明方案中存在随机值，可以在签名过程中有效地保护原信息，使得签名者对所签消息一无所知。由于签名者只知道$M'=(a_0',a_1',\cdots,a_n')$，而$M'=(a_0',a_1',\cdots,a_n')$是用户经过盲因子盲化之后以及 Hash 函数计算之后所得的数据，签名者不能从盲化后的消息$M'=(a_0',a_1',\cdots,a_n')$中推出原消息的 Hash 值$H(M)$，更不能推出原消息$M$。所以，这个签名方案是满足盲性的。

4.3. 不可伪造性

攻击者想要通过公开的验证密钥N求出保密的签名密钥p，q是不可行的，因为这是基于大合数分解的困难问题。因此，该方案是可以抵御一般性的伪造攻击。如果攻击者想要伪造签名者对盲化后的$M'=(a_0',a_1',\cdots,a_n')$进行签名，需要先破获$x_0$。其次，攻击者需要求出$d$，而这是不可行的，因为$d=(N-p-q+5)/8$，想要求出$d$，必须要先求出$p$，$q$，这仍然是基于大合数分解的困难问题。所以，我们的盲签名方案满足不可伪造性。

4.4. 性能分析

本方案与文献[3]的方案同为利用二次剩余进行盲签名，但在签名方式上各不相同，故签名运算所用时间有所差异。在模运算中，模幂、模逆与模乘运算占用了大部分时间，在签名阶段本方案的运算效率高于文献[3]。而在参数生成阶段时，文献[3]需要多次计算 Jacobi 符号也会花费时间。可以看出就整个签名方案而言，本方案的计算效率更高。

5. 结束语

盲签名因为具有盲性，它使得盲签名能有效地保护用户的隐私，所以在电子商务和电子选举等领域有着广泛的应用[9]。本文提出一个基于二次剩余的盲签名方案，并证明了这个盲签名方案满足盲性和不可伪造性这两个基本安全需求。

参考文献

[1] Chaum, D. (1983) Blind Signatures for Untraceable Payments. In: *Proceedings of CRYPTO*, Plenum Press, New York, 199-203. https://doi.org/10.1007/978-1-4757-0602-4_18

[2] Mao, W. 现代密码学理论与实践[M]. 北京: 电子工业出版社, 2004: 135-153.

[3] Fan, C.I. and Lei, C.L. (1996) Low-Computation Blind Signature Schemes Based on Quadratic Residues. *Electronics Letters*, **32**, 1569-1570. https://doi.org/10.1049/el:19961084

[4] Cao, Z.F., Zhu, H. and Lu, R. (2006) Provably Secure Robust Threshold Partial Blind Signature. *Science in China*, **49**, 604-615. https://doi.org/10.1007/s11432-006-2013-7

[5] 张席, 杭欢花. 一种改进的前向安全盲签名方案[J]. 武汉大学学报: 理学版, 2011, 57(5): 434-438.

[6] 何俊杰, 王娟, 祁传达. 一个改进的前向安全盲签名方案[J]. 计算机工程, 2012, 38(11): 133-135.

[7] 闵嗣鹤, 严士健. 初等数论[M]. 北京: 高等教育出版社, 2003: 88-91.

[8] 王小非, 崔国华, 李俊, 等. 一个数据膨胀率为 1 的概率公钥密码系统[J]. 计算机科学, 2007, 34(1): 117-119.

[9] 孙芳, 张雪峰, 袁小转. 一个前向安全盲签名方案的分析与改进[J]. 信阳师范学院学报(自然科学版), 2014(3): 444-446.