基于散列算法的 RSA 盲签名方案设计

魏长明

（中南大学信息科学与工程学院，湖南 长沙 410081）

摘 要：盲签名方案中，消息的内容对签名者是不可见的，签名被泄露后，签名者不能追踪其签名。笔者利用散列函数的单向性，基于 RSA 算法的基础上，设计了一种不可跟踪的盲签名方案，并对其安全性进行了分析。

关键词：盲签名；哈希算法；RSA

中图分类号：TN918.1 **文献标识码：**A **文章编号：**1003-9767(2015)05-105-02

一般的数字签名中，总是要先知道文件内容而后才签署。但有时需要某人对一个文件签名，而又不让他知道文件内容，称为盲签名，它是由 Chaum 在 1983 年最先提出的。在此之后，人们做了许多努力去构造各种盲签名方案，并将盲签名技术应用于电子货币和电子投票等许多安全应用系统。一般来说，一个好的盲签名应该具有以下性质：不可伪造性、不可抵赖性、盲性、不可跟踪性，满足上面几条性质的盲签名，被认为是安全的。祁明按照不同参数以及盲化的强度，将盲签名方案分为盲参数签名、弱盲签名和强盲签名三类。盲签名方案中，签名者仅知道盲消息 M 的签名 sign（M），而不知原始消息 m 及其签名 sign（m），sign（m）是签名收方利用 sign（M）所求得。如果签名者存储 sign（M）或其它有关数据，待 sign（m）公开后，签名者可以找到 sign（M）和 sign（m）的内在联系，从而达到对消息拥有者的跟踪，即为弱盲签名，若签名无法将 sign（M）和 sign（m）进行联系，则是强盲签名方案。笔者分别利用散列函数的单向性，随机性，对盲因子进行改进，设计一种不可跟踪的盲签名方案。

1 基于散列算法的 RSA 盲签名方案设计

1.1 散列函数

散列函数又称哈希函数或杂凑函数，是现代密码学的核心之一。一个好的散列函数 h=H（m），其中 H 为散列函数，m 为输入串，h 为散列值，长度是固定的。它有如下特性：

性质一，给定 m，很容易计算 h，即实用有效性；

性质二，给定 h，不能计算 m，即抗原象攻击；

性质三，给定 m，很难找到另一个输入串 m1 并满足 H（m1）= H（m），即抗碰撞攻击；

正因于散列函数的这些特性，在现代密码学中，散列函数有众多方面的应用：如在数字签名中，散列函数用来产生“消息摘要”，在需要随机数的密码学应用中，散列函数被广泛地用做实用的伪随机函数等。

1.2 散列函数与 AES 算法结合产生盲因子

盲因子产生过程如下：

1）用户 A 选择一随机数序列 r 和 K，并秘密保存，n 初值为 0；

2）计算 r1’=H（r）；

3）k1=H（k）；

4）r1=Ek1（r’1）

r1 即为当次盲签名因子。E 表示加密，k1 为密钥，下一次盲签名因子的产生，即以 r1’代替 r，k1 代替 k，重复 2） 3） 4）步，即可产生新的盲因子 r2，随机盲因子产生，见图 1。

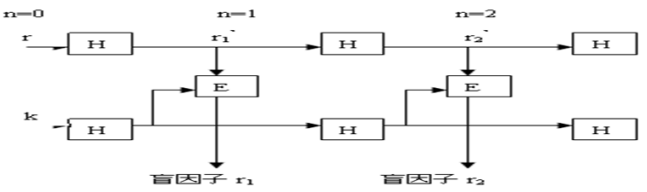

图 1 随机盲因子产生

国际上广泛应用的散列函数 MD5、加密算法 AES 具有很好的安全性，上述盲因子产生中用 MD5 作为散列算法，AES 作为加密算法以保证其安全性。

1.3 RSA 盲签名方案

盲签名方案有如下三个阶段：

盲化阶段：A 方选取随机数序列 r，选择一随机序列为加密密钥 K，按上述方法产生本次签名盲因子 r1；

（下转第 110 页）

作者简介：魏长明（1974-），男，湖南长沙人，讲师。研究方向：计算机网络。

计算机操作人员进行软硬件的组装和相关网站的维护管理。而这无疑与中职计算机专业学生的基本操作职能相吻合，为中职计算机学生的毕业发展提供了广阔的空间。所以中职教育机构应该对当地城镇化建设程度和水平进行调研，明确城镇化发展中各地经济形势的主要变化和这种变化带来的人才需求，进而按照人才需求对课程设置进行适当的调整，培养符合当地需要的计算机专业人才，拓展学生的岗位适用面。

2.6 提升教师的职业素质

在提升教师的职业素质方面，教育机构可以借鉴“双师型”教师师资队伍构建的方法，在保证教师的知识传授职能的同时为教师计算机技能的更新制定相应的资源培训平台，并定期为教师提供进入到相关企业参与实训的机会，通过对教师实践能力的坚固，提升教师实践教育的素质，从而培养学生的动手操作能力。

3 结 语

综上所述，只有真正将就业作为教学活动的导向，在中职计算机课堂教学中不断对教学理念、教学方式和教学模式加以探索，才能真正培养出具有独立学习能力、创新能力的社会实用型人才，为学生的发展和社会主义建设做出相应的贡献。

参考文献

[1] 林友山 . 实训教学在中职计算机专业的应用探究 [J]. 课程教育研究，2013（24）.

[2] 刘川蛟 . 中职计算机教学有效性的探究 [J]. 读写算，2013（4）.

[3] 刘文森，王玉玲 . 立足学生就业实际改革中职计算机课堂教学 [J]. 中国现代教育装备，2010（16）.

[4] 王耀菊 . 提高中职计算机课堂教学有效性的策略 [J]. 才智，2012（29）.

[5] 王倩 . 如何培养学生的创新能力 -- 对中职计算机 Flash 动画制作教学的探讨 [J]. 中学课程辅导，2014（20）.

[6] 郭芳 . 管窥如何提高中职计算机课堂的有效性 [J]. 新课程，2013（11）.

[7] 罗炯彪 . 中职计算机课堂“学案导学”教学模式探究 [J]. 中国科教创新导刊，2013（17）.

（上接第 105 页）

将签名信息 m 盲化 M=m r1e mod n 将 M 发送给盲签名者 B；（e，n 为 B 的公钥）

签名阶段：B 将信息 M 签名 s ’ =（M）d mod n ，得到签名 s ’，发送 s ’给 A;（d、n 为 B 的私钥）

脱盲阶段：A 计算 s=s ’ r-1 mod n ，得到签名 s

判断验证等式 m=（s）e mod n 是否成立，由此可确定签名是否有效。RSA 签名体制的安全性依赖分解大数的难易程序。分解 n 是最常用的攻击方法，攻击者只要能分解 n，求出签名者的私钥是轻而易举的事，因此，n 的取值要尽可能大些。

3 方案安全性分析

3.1 不可伪造性

由于 RSA 算法的安全性是基于大数分解的困难性，A 很难伪造另一个有效的签名 S，使得 m=（S）e mod n 成立。

3.2 盲性

信息 m 经过了 M`=m re mod n 的变换，Bob 只能看到 M，从而 m 对 Bob 是不可见的。

3.3 不可跟踪性

待 sign（m）公开后，签名者即算能找到 sign（M）和 sign（m）的内在联系，即盲因子 r1，由于散列算法的性质二，AES 加密与散列函数的一次一盲因子，由 r1 无法推导出前一次和后一次的盲因子，从而保证了盲签名的不可跟踪性，又使请求签名方只需保存初始量 r、k 及 n，能找出每次签名的盲因子，实现其记录特点。

3.4 有效性

由于采用的是散列算法及对称加密算法 AES，其计算量不大，并未增加太多的签名计算量。

4 结 语

本文利用散列函数的单向性、随机性与 RSA 算法相结合，构造了一种不可跟踪的盲签名方案，并使用户只须秘密保存盲因子产生的初始量，使此签名方案具有较强的不可跟踪性及有效性。

参考文献

[1] 祁明，张凌 . 盲参数签名及其应用 [J]. 计算机工程与应用，2001（14）.

[4]Radia Perlman. 网络安全 [M]. 北京：电子工业出版社，2004：52-57.