基于椭圆曲线的门限盲签名方案分析

Analysis of Threshold Blind Signature Scheme Based on Elliptic Curve

王亚楠 WANG Ya-nan;刘丽梅 LIU Li-mei
(渭南师范学院数理学院数学系,渭南 714099)
(Department of Mathematics,School of Mathematics and Physics,Weinan Normal University,Weinan 714099,China)

摘要: 椭圆曲线的密码体制是密码学的研究热点之一,而作为现如今最重要的数字密码系统数字签名是一种单向不可逆的公开密钥系统,在资源的处理中逐渐取代了 RSA 的地位。进而它在电子商务和网络安全通信方面有着至关重要的作用。本文通过对椭圆曲线密码学及数字签名的研究分析,给出了几点改进和优化的建议。

Abstract: The cryptosystem of elliptic curve is one of the hotspots of cryptography research. As the most important digital cryptosystem, digital signature system is a one-way irreversible public key system, and it has gradually replaced the status of RSA in the process of resource processing, also it has a vital role in e-commerce and cybersecurity communications. In this paper, through the analysis of elliptic curve cryptography and digital signature, it gives some suggestions for improvement and optimization.

关键词: 椭圆曲线密码体制 数学签名 门限体制

Key words: elliptic curve cryptosystem ;mathematical signature ;threshold system

中图分类号:TN918.1 **文献标识码:**A **文章编号:**1006-4311(2017)22-0204-02

DOI:10.14018/j.cnki.cn13-1085/n.2017.22.083

0 引言

作为密码学的核心,公钥密码在信息安全中担负着密钥协商、数字签名、消息认证等重要角色。目前信息安全领域的核心体制是基于椭圆曲线的椭圆曲线密码体制,简称 ECC,它是一类以椭圆曲线的数学理论为核心公钥密码体制。这种体制是在 1985 年由 Neal Koblitz 和 Victor Miller 分别独立提出的,进而一步一步发展为椭圆曲线在密码学。随着其不断完善和成熟,应用十分广泛。这是因为和其他公钥密码体制相比较而言,这类新的椭圆曲线密码体制的最大优点是短密钥和计算效率高。而其安全的主要依据是建立在由其定义的某类椭圆曲线点群上的离散对数问题求解的困难性的基础之上,这些椭圆曲线上离散对数的求解问题的难易程度要远远大于经典的离散对数问题。

随着密码学的发展和需要,数字签名方案体系随之而出并成为密码学的一个新的分支,特别是现在已经成为当今网络信息安全中的核心技术之一。它在身份认证、数据完整性评价、不可否认性和匿名性验证等信息安全应用领域中都有着重要的应用。它要求签名者用自己的私钥对给定的消息进行签名,而同时验证者需要利用签名者预先给定的公钥并结合消息来检验他的签名是否有效。因此数字签名方案成为开展电子商务信息安全的重要保障,并在实现客户身份认证、重要机密数据完整性和系统不可抵御性等领域都有重要的应用前景。

本文的目的在于通过对已有的椭圆曲线密码体制及数字签名方案的研究分析,进而从构造可验证性、盲性、不可伪造性的一种新型的可验证的门限盲签名方案入手,给出这种签名体系改进和进一步优化的几点建议,以供设计者甄别。

基金项目: 渭南师范学院大学生创新创业训练计划项目资助(15ZXK018)。

作者简介:王亚楠(1984-),女,陕西汉中人,主要从事数学与信息安全研究。

1 椭圆曲线数字签名方案设计

在 ISO7498—2 标准中,数字签名方案的定义是附加在数据单元上的一些数据,或者是对一些数据单元所作的密码新变换,这种数据和变换允许数据单元的接收者利用并用以确认数据单元的来源和数据单元的完整性,进而保护数据安全,以防止被人(例如接收者)进行伪造。

在上述的数字签名方案中,要求加密变换使用的密钥和解密变换使用的密钥必须是完全相同的一串密钥,而这个公共的密钥必须以某种非常安全的方式告诉解密的一方。这就是所谓的公钥密码体制。它使用的密钥被人们分解为一对,即就是一把公钥密码和一把私钥密码。要求私钥安全保密就可以了,公钥密码是可以公开的,也可以将其发到因特网等公开地方供别人查询和下载使用。

1.1 基于椭圆曲线的数字签名方案

数字签名的过程如图 1 所示。

1.2 椭圆曲线数字签名算法(ECDSA)

研究者开始只是使用椭圆曲线算法对数字签名算法进行模拟实验。直到 1999 年,ECDSA 才被 ANSI 确定为一种新的数字签名标准 ANSI X9.62-1998,这是由于基于椭圆曲线离散对数问题的数字签名算法要远远难于经典的离散对数问题,而且基于椭圆曲线的密码系统的单位比特强度也是要远远高于经典离散对数系统的,因此,其安全性更高、更可靠。

避免求 k 逆的签名过程如图 2 所示。

2 基于椭圆曲线的新型门限签名方案

一种签名方案如果能够实现其秘密共享效果就可以发展为一种新的门限签名方案,也就是说,如果人们不能简单地把秘密共享方案和签名方案结合起来则其就是门限签名方案。因为若要根据秘密共享方案分割密钥的话,等到用时再将其合成,则这种方法固然是不可取的。因此,一个科学的门限签名方案是每一个成员需要对消息使用自己的子密钥签名从而得到部分签名,而签名机构每次即

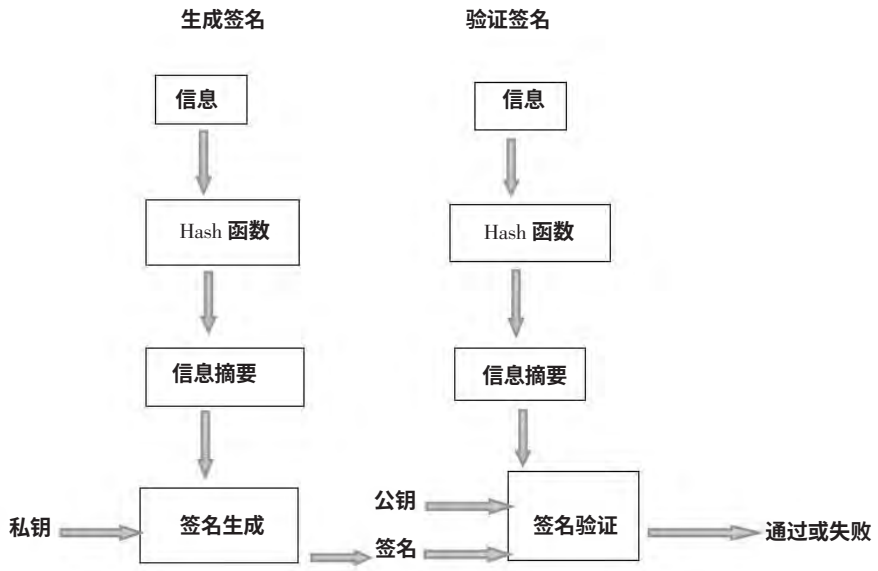

图 1

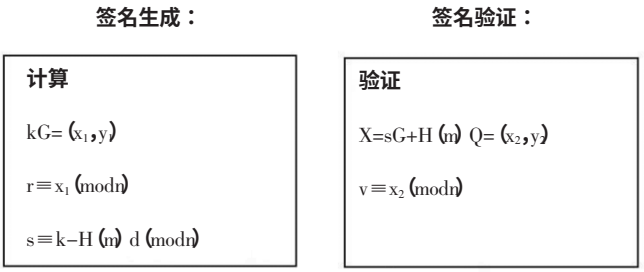

图 2

就是使用 N 个部分签名也无法获得整个签名的任何真实信息，并且由已知的部分签名不能获得密钥和子密钥的任何相关信息。

截止目前，和门限签名方案研究相关的新的研究方向有：向前安全的门限签名方案、动态门限签名方案和可证安全的门限签名方案。

就向前安全的门限签名方案而言，主要是尽量减少由于可能的密钥泄露而带来的对签名安全的直接影响和相应损失，即就是如果对手已经在窃取了群体当前时段的一些签名密钥的假设下，他也不能伪造此群体这一时段的数字签名，进而保障数字签名的安全性。

而动态门限签名方案主要是基于门限签名的理论基础，但却极大的减少了算法系统对其中诚实成员数量的假设要求，在这个签名方案中，改系统的生命期被设计者分成了若干个不定的时间段，同时要求在每个确定的时间段内非诚实成员要数量少于开始的门限值。在实际问题中，这种签名方案能够解决由签名文件的重要性决定签名者的数目的条件性问题。例如，一个非常重要的文件需要较多的签名者以增强其安全性，而一个普通文件则只需要较少的签名者而已。

最后，可证安全的门限签名方案则主要是解决以往门限签名方案中可能存在的可公开验证性和成员诚实性热点问题，它的密钥生成则只要求成员之间协商完成即可，而不需要由可信中心来协调，解决了以往方案中过分依赖于可信中心和可信中心权力过大核心问题。因此，该方案是健壮的和具有对适应性选择消息攻击是不可伪造的特征。

3 安全性分析与建议

3.1 需进一步增强签名的盲性特征

在整个门限签名方案的设计过程中，要求用户和每个签名者都需要将其事先协商好的公共信息嵌入到已有的签名过程中去，这样就可以首先保证签名的部分性特征，而且一旦用户将盲化因子引入到已有的签名中的话，其他可能的人（这包括签名群体中的每个签名者）想试图求出参数值是困难的，因而，试图由盲消息得到原消息的内容也是十分困难的。这里，可以引入数学中的模型和特殊群的结构设计加以优化，所以增加数字签名方案的盲性设置和进一步优化方案设计都可以增强方案的安全性。

3.2 不断提高签名的不可伪造性

在已有的门限签名方案中，我们假设方案最大能够容忍入侵度为 T-1，即就是攻击者至多可勾结 T-1 个秘密分享者进行攻击。假设若 A 要假冒 B 中的某个用户对消息进行部分签名的话，他需要构造出被验证方接受的密钥信息，但是在他不知道中心私钥或 B 中任何子成员的子密钥的情况下，他要求解参数间的等价问题和求解对应的椭圆曲线的离散对数问题，都是是十分困难的，若我们能够找到数学中的一些特殊结构的椭圆曲线来刻画这一问题，就可以提高算法的安全性。因此，研究者提高中心密钥的不可伪造性及其选取合适的椭圆曲线是提高签名的不可伪造性的有效途径。

4 结论

我们知道，数字签名的目的就是想通过数字方式实现在实际通讯中通信双方的身份验证问题，保证互通消息的真实性和完整性。但是在现代社会的实际问题中若需要多个人同时参与才能生成签名的情况下，则我们发现门限签名是较好的选择。门限签名可以满足很多实际应用的要求，具有广泛的应用前景和市场。

参考文献：

[1]宋震等.密码学[M].中国水利水电出版社，2002：129-135.

[2]Stinso D R 著，冯登国.译.密码学原理与实践[M].电子工业出版社，2003：87-90.

[3]张伟.ECDSA 算法实现及其安全性分析[J].信息与电子工程，2003，1 (2)：26-33.

[4]罗浩，黄双庆，刘金龙，乔秦宝.椭圆曲线签名方案[J].理学版武汉大学学报，2003，49 (1)：17-23.

[5]Koblitz N. Elliptic curve cryptosystems Mathematics of Computation[M].世界图书出版社，1987：98-109.

[6]Koblitz N. Introduction to Elliptic curves and Modular Forms[M].世界图书出版社，2003:32-55.