椭圆曲线数字签名的两种改进算法

李明株,刘瑞芹

(华北科技学院 理学院,北京 东燕郊 065201)

摘 要:数字签名技术是信息安全领域中研究的热点问题之一。在研究椭圆曲线密码体制和经典数字签名过程的基础上,针对明文用哈希函数变换成一个整数和明文嵌入到椭圆曲线上点的不同情况,提出了两种数字签名的改进算法,并进行了正确性验证和安全性分析。改进后的算法加密和验证过程中不需要进行模逆的运算,减少了运算量,降低了对计算机软硬件的要求。

关键词:椭圆曲线密码体制;哈希函数;数字签名

中图分类号:TP301.6 **文献标识码**:A **文章编号**:1672-7169(2020)05-0084-04

Two improved algorithms for elliptic curve digital signature

LI Mingzhu, LIU Ruiqin

(*School of Science, North China Institute of Science and Technology, Yanjiao*, 065201, *China*)

Abstract: The digital signature technology is one of hot topics in the information security domain. Based on the elliptic curve cryptosystem and the classical digital signature process, we analyze the different situations of using hash function to transform plain text into integer and plain text into points on elliptic curve, and propose two kind of digital signature improvement algorithm. The correctness verification and security analysis is carried out. The improved algorithm does not need modular inversion in the process of encryption and verification. Reduces the amount of computation. The algorithm reduces the requirements of computer hardware and software.

Key words: elliptic curve cryptosystem; hash function; digital signature

0 引言

上世纪九十年代,通用的是 RSA 公钥密码体制,密钥长度一般为 512bit。1999 年 RSA-512 被破解,之后只能用加长密钥保证信息的安全性,导致运行速度更加缓慢。1985 年,Koblitz[1] 和 Miller[2] 提出将椭圆曲线用于公钥密码学的思想,标志着椭圆曲线密码体制(ECC,Elliptic Curve Cryptography)的诞生。ECC 是建立在基于椭圆曲线上的点构成的 Abelian 加法群的离散对数问题上的密码体制。研究表明:基于有限域上椭圆曲线的离散对数问题运算位数远小于传统离散对数的运算位数,它可以使用较短的密钥达到较高的安全性,且计算速度快、存储量小、带宽要求低[3]。

数字签名在网络环境中可以代替传统手写签名或印章,是实体签名的信息化实现。使用数字

收稿日期:2020-09-29

基金项目:2019 年国家级大学生创新创业训练计划(065D12)

作者简介:李明株(1998-),女,山西长治人,华北科技学院理学院在读大学生,研究方向:密码学与信息安全。E-mail:1453770644@qq.com

通讯作者:刘瑞芹(1965-),女,河北保定人,硕士,华北科技学院理学院教授,研究方向:应用数学、密码学与信息安全。E-mail:2175740634@qq.com

签名技术能够使得发送者事后不能否认发送的签名信息、接收者能够核实但不能伪造或篡改发送者的签名信息。数字签名是提供身份认证、确保信息完整性、不可伪造性、不可否认性的重要信息技术。Jonhson 和 Menezes 于 1999 年提出了基于椭圆曲线的数字签名算法(ECDSA)。椭圆曲线数字签名算法也成为目前研究的热门问题[4-6]。

1　椭圆曲线密码体制

1.1　有限域上的椭圆曲线

椭圆曲线密码体制[7,8]的有效实现主要用到两种类型的有限域,它们是素数域 $GF(p)$ 和二元域 $GF(2)$ 上的扩域 $GF(2^m)$。

素数域 $GF(p)$:设 p 是一个大素数,$GF(p)=\{0,1,2\cdots,p-1\}$。

二进制扩域 $GF(2^m)$:由二元域 $GF(2)$ 上所有次数小于 m 的多项式组成,即:

$GF(2^m)=\{a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots a_1x+a_0\}$,$a_i=\{0,1\}$。

域元素$(a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_1x+a_0)$通常用长度为 m 的二进制串$(a_{m-1},a_{m-2},\cdots,a_1,a_0)$表示,则 $GF(2^m)=\{(a_{m-1},a_{m-2},\cdots,a_1,a_0)\}$,$a_i=\{0,1\}$。扩域 $GF(2^m)$中包含 2^m 个元素。

(1) 有限域 $GF(p)$上的椭圆曲线是对于给定 a,b $(4a^3+27b^2)\bmod p\neq 0$,满足方程:

$$y^2=x^3+ax+b\bmod p$$

的所有解(x,y)构成的点集,外加无穷远点 O 构成的一个群 $E(F_p)$。其中 a,b,x,y 均在有限域 $GF(p)=\{0,1,2\cdots,p-1\}$中取值,$E(F_p)$称为椭圆曲线群。

(2) 有限域 $GF(2^m)$上的椭圆曲线满足方程:

$$y^2+xy=x^3+ax^2+b$$

的所有解(x,y)构成的点集,外加无穷远点 O 构成一个椭圆曲线群 $E(F(2^m))$。

其中 a,b,x,y 均在有限域 $GF(2^m)$中取值。

在椭圆曲线群中,使 $nG=0$ 的最小正整数 n 称为点 G 的阶数。

椭圆曲线上的离散对数问题:在曲线上两个点 P 和 Q 满足 $Q=kP$,其中 k 为常数。已知 k 和 P 求 Q 容易,已知 P 和 Q 求 k 的问题是离散对数问题,求解却很困难,是建立椭圆曲线密码体制的数学依据。

1.2　椭圆曲线加解密算法

椭圆曲线密码体制是将加密问题转换为椭圆曲线群中元素的计算问题,采取非对称的公、私双秘钥方式进行加解密运算。下面以素数域上的椭圆曲线为例介绍一种利用椭圆曲线群实现加、解密的方法。

首先选定椭圆曲线 $y^2=x^3+ax+b\bmod p$。寻找一个阶数为 n 的点 G,要求 n 为一个大素数,称为基点。把要发送的明文 m 嵌入到群 $E(F_p)$上的点 P_m[9,10],然后对消息 P_m 进行加、解密:

用户 A,选取一个整数 d_A 作为私钥,对应的公钥为 $p_A=d_AG$。

用户 B,选取一个整数 d_B 作为私钥,对应的公钥为 $p_B=d_BG$。

用户 A 向用户 B 发送信息 P_m,进行秘密传输。

1.2.1　加密过程

(1) 用户 A 随机选取一个正整数 $k\in[1,n-1]$;

(2) 计算点 $P_k=kG$;

(3) 利用用户 B 的公钥 p_B,计算点 kp_B;

(4) 计算点 P_m+kp_B;

(5) 形成密文 $C=(P_k,P_m+kp_B)$,由一对椭圆曲线群 $E(F_p)$中的点组成。

1.2.2　解密过程

(1) 用户 B 接收到密文 $C=(P_k,P_m+kp_B)$;

(2) 用私钥 d_B 计算点 d_BP_k;

(3) 计算点$(P_m+kp_B)-d_BP_k$,得到消息 $P_m=(P_m+kp_B)-d_BP_k$。

事实上,$(P_m+kp_B)-d_BP_k=(P_m+kd_BG)-d_BkG=P_m$。

上述过程表明,用户 A 通过将 kp_B 与 P_m 相加来伪装消息 P_m,实现加密。因为 k 是用户 A 随机选取的,只有用户 A 知道,加解密过程中的主要计算是点的倍乘运算,其他人无法从 $P_k=kG$ 中解出 k,就无法消除伪装,提高了加密的安全性。

2　椭圆曲线密码数字签名的算法

数字签名算法包括两个部分,即签名算法和

验证算法。发送者签名时用私钥对明文或消息摘要实施加密运算,然后把加密的数据传给接受者,因他人无法知道私钥,故不能伪造签名。接收者验证签名时利用发送者的公钥进行验证,将结果与消息或者摘要进行比较,当且仅当两者相同,就接收签名。

在 SEC(Standards for Efficient Cryptography)制定的 ECC 工作草案中[11],定义椭圆曲线参数的形式是一个六元偶,记作:$R=\{q,a,b,G,n,h\}$

其中:

(1) 整数 q 表示椭圆曲线基域 $F(p^m)$ 中域元素的个数;

(2) a,b 表示椭圆曲线方程的系数;

(3) G 是椭圆曲线点群的一个基点;

(4) n 是椭圆曲线基点 G 的阶;

(5) h 是余因子,利用 h 可以较快地找到基点 G。

椭圆曲线数字签名 ECDSA(Elliptic Curve Digital Signature Algorithm)是不带有消息恢复功能签名方案[12],需要使用的参数有:椭圆曲线参数六元偶;待签名消息 m;签名者 A 的密钥对(d,Q),其中 $Q=dG$,d 是私钥、Q 是公钥。

签名生成过程:

输入:$R=\{q,a,b,G,n,h\}$,私钥 d、消息 m

输出:(r,s)

(1) 随机地选取一个整数 $k\in[1,n-1]$

(2) 计算 $kG=(x_1,y_1)$,$r=x_1 \bmod n$,如果 $r=0$ 则返回到 1;

(3) 计算 $e=SHA-1(m)$;

(4) 利用签名者 A 的私钥计算 $s=k^{-1}(e+dr) \bmod n$,如果 $s=0$ 则返回 1;

(5) (r,s)是 A 对消息 m 的签名。A 发送给接收者 B 消息 m 及签名(r,s)。

签名验证:

输入:$R=\{q,a,b,G,n,h\}$,公钥 Q、消息 m

输出:验证(r,s)是对消息 m 的签名是否正确。

(1) 验证(r,s)是$[1,n-1]$中的整数;

(2) 计算 $e=SHA-1(m)$;

(3) 计算 $w=s^{-1} \bmod n$;

(4) 计算 $u_1=ew \bmod n$,$u_2=rw \bmod n$;

(5) 利用签名者 A 的公钥计算 $X=u_1G+u_2Q=(x_2,y_2)$;

(6) 判定:如果 $X=O$ 则拒绝签名,否则计算 $v=x_2 \bmod n$,当 $v=r$ 时接受这个签名。

签名验证的证明:

因为(r,s)是签名者 A 对消息 m 的签名,

则 $s=k^{-1}(e+dr) \bmod n$,

从而

$k=s^{-1}(e+dr)=s^{-1}e+s^{-1}dr=we+wdr=u_1+u_2d$

所以 $X=u_1G+u_2dG=(u_1+u_2d)G=kG$ 即 $v=r$。

从上述算法知道,A 是利用随机数 k 和私钥 d,对消息 m 进行的签名,B 是利用 r 和公钥 Q 对签名进行验证。这个过程中无法通过 r 和公钥 Q 来计算 k 和私钥 d,这就使得 ECDSA 算法非常安全。

3 两种改进的数字签名算法

在数字签名前,对于待签明文 m 的处理有两种方法,一种方法用密码杂凑函数即哈希函数计算 $e=H(m)$,并转化为一个整数。另一种方法是把明文 m 与椭圆曲线上的点建立对应关系,利用嵌入算法把明文用椭圆曲线上的点 P_m 来表示[13,14]。对哈希函数值 e 和椭圆曲线上点 p_m 的签名就是对明文消息 m 的签名。根据这两种情况对数字签名算法进行了改进。

3.1 明文 m 利用哈希函数处理的数字签名改进算法

3.1.1 签名生成过程

输入:$R=\{q,a,b,G,n,h\}$,私钥 d、明文 m

输出:(r,s)

(1) 随机地选取一个整数 $k\in[1,n-1]$;

(2) 计算 $kG=(x_1,y_1)$;

(3) 计算 $e=SHA-1(m)$;

(4) 计算 $r=(x_1+e) \bmod n$,如果 $r=0$ 则返回 1;

(5) 利用签名者 A 的私钥计算 $s=(k-dr) \bmod n$,如果 $s=0$ 则返回到 1;

(6) (r,s)是 A 对消息 m 的签名。A 发送给接收者 B 消息 m 及签名(r,s)。

3.1.2 签名验证

输入:$R=\{q,a,b,G,n,h\}$,公钥 Q、消息 m

输出:验证(r,s)是对消息 m 的签名是否

正确。

(1) 验证(r,s)是$[1,n-1]$中的整数;

(2) 计算 $e=SHA-1(m)$;

(3) 利用签名者 A 的公钥计算:

$$X=sG+rQ=(x_2,y_2)$$

(4) 判定:如果 $X=O$ 则拒绝签名。否则计算 $v=(x_2+e)\bmod n$,当 $v=r$ 时接受这个签名。

3.1.3　签名验证的证明

因为(r,s)是签名者 A 对消息 m 的签名,则 $s=(k-dr)\bmod n$,从而

$$X=sG+rQ=(k-dr)\bmod nG+rd\bmod nG=kG$$

所以 $v=r$。

3.2　明文 m 用椭圆曲线上的点 P_m 来表示的数字签名改进算法

3.2.1　签名生成过程

输入:$R=\{q,a,b,G,n,h\}$,私钥 d、消息 P_m

输出:(r,s)

(1) 随机地选取一个整数 $k\in[1,n-1]$

(2) 计算 $P_m+kG=(x_1,y_1)$;

(3) 计算 $r=x_1\bmod n$,如果 $r=0$ 则返回到 1;

(4) 利用签名者 A 的私钥计算 $s=(k-dr)\bmod n$,如果 $s=0$ 则返回到 1;

(5) (r,s)是 A 对消息 m 的签名。A 发送给接收者 B 消息 m 及签名(r,s)。

3.2.2　签名验证

输入:$R=\{q,a,b,G,n,h\}$,公钥 Q、消息 P_m

输出:验证(r,s)是对消息 m 的签名是否正确。

(1) 验证(r,s)是$[1,n-1]$中的整数;

(2) 利用签名者 A 的公钥计算:

$$X=P_m+sG+rQ=(x_2,y_2)$$

(3) 判定:如果 $X=O$ 则拒绝签名,否则计算 $v=x_2\bmod n$,当 $v=r$ 时接受这个签名。

3.2.3　签名验证的证明

因为(r,s)是签名者 A 对消息 m 的签名,则 $s=(k-dr)\bmod n$,从而

$$X=P_m+sG+rQ=P_m+[(k-dr)\bmod n]G+[rd\bmod n]G=P_m+kG$$

所以 $v=r$。

3.3　改进的 ECDSA 算法安全性分析及其特点

安全性分析:

(1) 签名算法中 $s=(k-dr)\bmod n$,一个方程中包含随机数 k 和私钥 d 两个量,攻击者无法求解;

(2) 从验证方程 $X=sG+rQ$ 和 $X=P_m+sG+rQ$ 中无法求得私钥,保证了消息的真实性;

(3) 如果签名是伪造的,验证方程不能通过,签名不能否认。

改进的数字签名方案对 *Hash* 值 e 应用模 n 做了约简,具有以下几方面的特点:

(1) 签名算法的生成和验证过程比较简单;

(2) 避免了求模逆的运算,提高了计算速度,对计算机硬软件的要求更低;

(3) 算法能够保证签名文件的安全。

4　结论

(1) 本文对椭圆曲线密码体制和数字签名算法进行了研究,给出了一种明文 m 利用哈希函数处理的数字签名改进算法;给出了一种明文 m 用椭圆曲线上的点 P_m 来表示的数字签名改进算法。

(2) 两种改进的数字签名算法,能够保证签名的安全性,避免了求模逆的问题,减少了运算量,对系统要求更低。研究具有一定的理论意义和实际应用价值。

(3) 从安全性和算法有效性的角度来看,数字签名算法有进一步改进的可能,下一阶段将继续研究。

参考文献:

[1] KoblitzN. Elliptic curve cryptosystems[J]. Mathematics of Computation,1987,48(177):203-209.

[2] MillerVS. Use of elliptic curves in cryptography [C]. Advances in Cryptology (Crypto'85). Lecture Notes in Computer Science,Springer Verlag,1985(128):417-426.

[3] 汪朝晖,陈建华,涂 航,李莉. 素域上椭圆曲线密码的高效实现[J]. 武汉大学学报(理学版),2004,50(3):335-338.

[4] 张方国,王常杰,王育民.基于椭圆曲线的数字签名和盲签名[J]. 通信学报,2001,22(8):22-27.

[5] 崔文军,贾志娟,胡明生,公 备,王利朋. 基于椭圆曲线的签密方案[J]. 计算机应用与软件,2020,37(3):304-309.

[6] 殷骏,张颖超. 一种基于椭圆曲线的有向门限群签名方案[J]. 计算机工程与应用,2005(8):146-148.

(下转第 102 页)

故原因调查及防范措施[J]. 中国应急管理,2016 (2): 44-57.
[6] 刘建川,邓利民,侯映天. 危险化学品公共安全技术信息管理系统研究进展[J]. 中国安全生产科学技术,2011,7(11):97-102.
[7] 曲艳东,李瑞勇,翟诚等. 国内外危险化学品安全管理体系探讨[J]. 中国安全生产科学技术,2009,5(5):42-45.
[8] 魏广庆,张景钢,宋国强,索诚宇. 危险化学品安全监管现状及对策研究[J]. 华北科技学院学报,2015,12(3):73-77.
[9] 方堃. 我国化学品安全生产问题与对策[J]. 华北科技学院学报,2004(2):22-24.
[10] 郭帅,郭宗舟,石燕燕等. GHS 背景下危险化学品登记数据的应用[J]. 中国安全生产科学技术,2013,9(2):130-134.
[11] 张兴全. 危险化学品安全生产现状与对策探讨[J]. 中国石油和化工标准与质量,2019,39(17):21-22.
[12] 高建明,曾明荣. 我国危险化学品安全生产现状与对策[J]. 中国安全生产科学技术,2005(3):52-55.
[13] 陈晶,李方,周中华. 浅谈我国危险化学品安全生产管理现状及对策[J]. 科技创新导报,2015,12 (28): 187-188.
[14] 易高翔. 北京市危险化学品企业安全生产风险评估分级研究[J]. 中国安全生产科学技术,2010,6(6):93-97.
[15] 周琦. 危险化学品安全监管信息化的研究[D]. 镇江:江苏大学,2005.
[16] 王晓宁,王明贤,陈万金. 现代信息技术对我国危险化学品监管体系的影响[C]. 煤炭工业出版社:第二届中国国际安全生产论坛论文集,2004. 9:171-174.
[17] 于洋. 危险化学品企业重大危险源管理现状及对策研究[J]. 中国安全生产科学技术,2012,8(12):114-119.
[18] 曾明荣,王浩水,魏利军. 论危险化学品安全生产长效机制构[J]. 中国安全生产科学技术,2009,5(2): 112-116.
[19] 许代红,王琪. 大庆油田云数据中心建设思路[J]. 通信管理与技术,2013(3):19-23.

(上接第 87 页)

[7] 刘建伟 王育民. 网络安全—技术与实践[M]. 清华大学出版社,2014.
[8] 卢昌荆,周厚勇,史开泉. 图像安全的椭圆曲线加密实现[J]. 山东大学(工学版),2004,34(3),33-36.
[9] 赵君卫,王保保.椭圆曲线密码体制中明文嵌入的研究[J]. 微机发展,2003,13(10):69-70.
[10] 卢忱,妙全兴,卞正中. 嵌入明文到椭圆曲线上一点的算法设计与实现[J].纺织高校基础科学学报,2004,17(1):63-67.
[11] SEC1, Elliptic Curve Cryptography group, working draft[EB/OL], http://www. secg. org/, 1999-02-12.
[12] ANSI X 9. 62 62-99, Public key cryptography for the financial services industry. Elliptic curve digital signature algorithm (ECDSA)[S]1999-02-12.
[13] 高伟,张国印,王欣萍.一种改进的椭圆曲线数字签名算法[J].黑龙江大学自然科学学报,2010,27(3):396-402.
[14] 韩笑,施荣华. 一种高效的椭圆曲线数字签名方案[J]. 微计算机信息,2012,28(9):395-396.