周克元, 王丽. 无模逆椭圆曲线数字签名方案研究[J]. 智能计算机与应用,2026,16(5):102-105. DOI:10.20169/j.issn.2095-2163.24072403

无模逆椭圆曲线数字签名方案研究

周克元, 王 丽
(宿迁学院 文理学院, 江苏 宿迁 223800)

摘 要: 对椭圆曲线数字签名张庆胜方案及其改进方案栗亚敏方案进行分析,指出了栗亚敏方案存在的错误。通过构建椭圆曲线数字签名中的参数 k 与参数 r,m 的关联关系,推导签名方程与验证方程,提出张庆胜方案的两种新的改进方案,改进方案中倍乘和模逆的运算次数分析低至 3 次和 0 次,将改进方案与已有方案进行复杂度比较,结果显示新方案复杂度更低。

关键词: 椭圆曲线; 数字签名; 伪造攻击; 模逆
中图分类号: TP309.7 **文献标志码**: A **文章编号**: 2095-2163(2026)05-0102-04

Research on ECDSA without modular inverse operation

ZHOU Keyuan, WANG Li
(School of Arts and Sciences, Suqian University, Suqian 223800, Jiangsu, China)

Abstract: The elliptic curve digital signature scheme of Zhang Qingsheng and the Li Yamin improved scheme are analyzed, and the errors in Li Yamin's scheme are pointed out. By relating the parameter k to the parameters r and m, and deriveing the signature and verification equations, two new improved schemes of Zhang Qingsheng's scheme are presented, in which, the number of scalar multiplications and modular inverses reached the minimum values of 3 and 0, respectively. The complexity comparison with existing schemes is also given, showing that the new schemes have lower complexity.

Key words: elliptic curve; digital signature; forgery attack; modular inverse

0 引 言

椭圆曲线密码体制是离散对数密码体制在椭圆曲线上的平移,椭圆曲线密码体制具有更小的密钥量、更快的速度和更高的安全性等优点[1]。数字签名是当前网络安全领域的研究热点,其作为保障网络信息安全的核心机制,可以解决签名的伪造、抵赖、冒充和篡改问题[2]。

目前对椭圆曲线数字签名的改进有以下两个方向:一是在保证安全性的基础上对算法复杂度进行改进,给出复杂度更低的方案,主要是对算法中的模逆运算进行改进[3-5],例如文献[5]中的方案将模逆运算次数优化至 0 次;二是在数字签名功能的基础上增加新的功能,如前向安全、消息恢复[6-8]、数字签密[9-11]、代理签名[12-13]、盲签名[14-16]、群签名[17-19]等。

张庆胜[20]对椭圆曲线数字签名算法(Elliptic Curve Digital Signature Algorithm, ECDSA)进行分析,提出了新的方案,在 ECDSA 的基础上减少了一次倍乘运算。栗亚敏[21]指出张庆胜方案可被伪造签名攻击,同时给出了改进方案。本文分析发现栗亚敏改进方案存在安全缺陷,同时根据其改进思路给出两种新的改进方案,新方案将模拟运算次数优化至 0 次,达到理论最小值,并证明了其正确性和安全性。

1 张庆胜对 ECDSA 的改进方案[20]

1)参数

设有限域 GF(p),E 是有限域 GF(p) 上的椭圆曲线。选择 E 上一点 $G \in E$,G 的阶为满足安全要求的素数 n, 即 $nG = O$(O 为无穷远点)。选择随机数 d,$d \in [1, n-1]$, 计算 $Q = dG$, 公钥为 (n, Q), 私钥为 d。

2)签名算法

基金项目: 国家自然科学基金(12101441)。

作者简介: 周克元(1978—),男,硕士,讲师。主要研究方向:信息安全。Email: zhoukeyuan2001@163.com。

收稿日期: 2024-07-24

签名者 A 对消息 m 的签名过程如下：

(1)随机选取整数 $k \in [1,n-1]$，计算 $kG=(x_1,y_1)$，$r=x_1 \bmod n$，若 $r=0$，则重新选取 k；

(2)计算 $e=h(m)$，其中 h 为安全的 Hash 函数；

(3)计算 $s=(er)^{-1}(k+d) \bmod n$；

则 A 对消息 m 的签名为 (r,s)。

3)验证算法

B 接收到 A 的签名，验证的步骤如下：

(1)计算 $e=h(m)$，h 为安全的 Hash 函数；

(2)计算 $w=ers \bmod n$；

(3)计算 $wG-Q=(x_2,y_2)$，$v=x_2 \bmod n$；

若 $v=r$，则接受该签名；否则不接受。

栗亚敏[21]对张庆胜方案进行了分析，指出可用另一消息 m' 替换原有消息 m 进行伪造签名攻击，过程如下：

已知 s,e,r，由 $s=(er)^{-1}(k+d) \bmod n$ 可求得 $(k+d) \bmod n$，然后计算 $e'=h(m')$，则可以计算出 $s'=(e'r)^{-1}(k+d) \bmod n$，得 m' 的伪造签名 (r,s')。该签名可通过验证，正确性证明如下：

$$e'r \cdot s'G-Q=e'r(e'r)^{-1}(k+d)G-Q=(k+d)G-dG=kG$$

因此 $v=r$，签名通过验证。

栗亚敏对张庆胜方案进行了改进，改进方案如下。

2　栗亚敏改进方案[21]

1)参数

同张庆胜方案。

2)签名算法

签名者 A 对消息 m 签名的过程如下：

(1) 随机选取整数 $k \in [1,n-1]$，计算 $kG=(x_1,y_1)$，$r=x_1 \bmod n$，若 $r=0$，则重新选取 k；

(2)计算 $e=h(m)$，h 为安全的 Hash 函数；

(3)计算 $s=(ke-rde^2) \bmod n$；

则 A 对消息 m 的签名为 (r,s)。

3)验证算法

B 接收到 A 的签名，验证的步骤为：

(1)计算 $e=h(m)$，h 为安全的 Hash 函数；

(2)计算 $w=ed \bmod n$；

(3)计算 $w^{-1}sQ+rwG=(x_2,y_2)$，$v=x_2 \bmod n$；

若 $v=r$，则接受该签名；否则不接受。

上述接收者 B 验证过程 $w=ed \bmod n$ 的计算中，用到了签名者 A 的私钥 d。数字签名方案中，签名者 A 的私钥不允许泄漏，故栗亚敏方案不可行。

3　本文改进方案

文献[5]给出了一种椭圆曲线数字签名无求逆方案，本文在其基础上进行改进，给出张庆胜方案的两种新的改进方案。

3.1　改进方案 1

1)参数

同张庆胜方案。

2)签名算法

签名者 A 对消息 m 签名的过程如下：

(1)随机选取整数 $k \in [1,n-1]$，计算 $kG=(x_1,y_1)$，$r=x_1 \bmod n$，若 $r=0$，则重新选取 k；

(2)计算 $e=h(m)$，h 为安全的 Hash 函数；

(3)选择一组整数 $\alpha,\beta \in [1,n-1]$，满足 $k=(\alpha r+\beta m) \bmod n$；

(4)计算 $s=(\alpha r+ed) \bmod n$；

则 A 对消息 m 的签名为 (r,s,β)。

3)验证算法

B 接收到 A 的签名，验证的步骤为：

(1)计算 $e=h(m)$，h 为安全的 Hash 函数；

(2)计算 $(s+\beta m)G-eQ=(x_2,y_2)$，$v=x_2 \bmod n$；

若 $v=r$，接受该签名；否则不接受。

4)正确性证明

$$\begin{aligned}&(s+\beta m)G-eQ\\=&(\alpha r+ed+\beta m)G-edG\\=&(\alpha r+\beta m)G\\=&kG\end{aligned}$$

所以 $v=r$。

5)安全性证明

(1)抗替换消息 m 伪造攻击

签名者 A 发送 $(r,s,\beta;m)$ 给 B，r、s、β、m、e 是已知量。B 用 m' 代替 m 进行签名，计算 $e'=h(m')$。方程组

$$\begin{cases}k=(\alpha r+\beta m) \bmod n\\s=(\alpha r+ed) \bmod n\end{cases}$$

其中，未知量 k、α、d 无法求出，故 m' 签名方案对应的参数 α、β、r、s 只能使用原有参数值，即 m' 的伪造签名为 (r,s,β)。

验证过程中，

$$(s+\beta m')G-e'Q=(\alpha r+ed+\beta m')G-e'dG=(\alpha r+\beta m')G+(ed-e'd)G$$

由于 $\alpha r + \beta m' \neq k, ed - e'd \neq 0$，故上式 $(s + \beta m')G - e'Q \neq kG$，则 $v \neq r$，验证失败。

(2) 抗替换随机数 k 伪造攻击

任取 $k' \in [1, n-1]$，计算 $k'G = (x', y')$，$r' = x' \bmod n$。计算一组整数 $\alpha', \beta' \in [1, n-1]$，满足 $k' = (\alpha' r' + \beta' m') \bmod n$。签名方程 $s' = (\alpha' r' + e'd) \bmod n$ 中，攻击者无法得到签名者的私钥 d，故替换随机数 k 伪造攻击无法成功。

3.2 改进方案 2

1)参数

同张庆胜方案。

2)签名算法

签名者 A 对消息 m 签名的过程如下：

(1)随机选取整数 $k \in [1, n-1]$，计算 $kG = (x_1, y_1)$，$r = x_1 \bmod n$，若 $r = 0$ 转到(1)重新计算；

(2)计算 $e = h(m)$，h 为安全的 Hash 函数；

(3)选择一组整数 $\alpha, \beta \in [1, n-1]$，满足 $k = (\alpha r + \beta m) \bmod n$；

(4)计算

$s = (\alpha r + rd) \bmod n = r(\alpha + d) \bmod n$；

则 A 对消息 m 的签名为 (r, s, β)。

3)验证算法

B 接收到 A 的签名，验证的步骤为：

(1)计算 $e = h(m)$，h 为安全的 Hash 函数；

(2)计算 $(s + \beta m)G - rQ = (x_2, y_2)$，$v = x_2 \bmod n$；

若 $v = r$，接受该签名；否则不接受。

4)正确性证明

$$(s + \beta m)G - rQ = (\alpha r + rd + \beta m)G - rdG = (\alpha r + \beta m)G = kG$$

所以 $v = r$。

5)安全性证明

(1)抗替换消息 m 伪造攻击

签名者 A 发送 $(r, s, \beta; m)$ 给 B，r、s、β、m、e 是已知量。B 用 m' 代替 m 进行签名，计算 $e' = h(m')$。方程组

$$\begin{cases} k = (\alpha r + \beta m) \bmod n \\ s = (\alpha r + rd) \bmod n \end{cases}$$

其中，未知量 k、α、d 无法求出，$\alpha + d$ 可求出，故 m' 对应的参数 α、β、r、s 只能使用原有参数值，即 m' 的伪造签名为 (r, s, β)。

验证过程中，$(s + \beta m')G - rQ = (\alpha r + rd + \beta m')G - rdG = (\alpha r + \beta m')G \neq kG$，则 $v \neq r$，验证失败。

(2)抗替换随机数 k 伪造攻击

任取 $k' \in [1, n-1]$，计算 $k'G = (x', y')$，$r' = x' \bmod n$。计算一组整数 $\alpha', \beta' \in [1, n-1]$，满足 $k' = (\alpha' r' + \beta' m') \bmod n$。签名方程 $s' = (\alpha' r' + r'd) \bmod n$ 中，攻击者无法得到签名者的私钥 d，故替换随机数 k 伪造攻击无法成功。

另外，若使用求出的 $\alpha + d$ 计算 $s' = r'(\alpha + d) \bmod n$，此时签名为 (r', s', β')，验证过程中：$(s' + \beta' m')G - r'Q = (\alpha r' + r'd + \beta' m')G - r'dG = (\alpha r' + \beta' m')G \neq k'G$，则该替换随机数 k 伪造攻击无法成功。

4 复杂度分析

椭圆曲线数字签名算法的运算主要有点积、倍乘、模逆和 Hash 函数运算，一般来说对椭圆曲线数字签名运算时间影响最大的是倍乘运算和模逆运算，点积运算相对于模乘和模逆运算来说复杂度较低，同时模逆运算所需时间是倍乘运算的 10 倍[22]，故算法的复杂度主要考虑模逆运算的次数。

目前椭圆曲线数字签名最新的改进方案为文献[5]和[8]中的方案，将本文改进方案与上述两个方案复杂度进行比较，结果见表 1。

表 1 三种方案时间复杂度比较

Table 1 Comparison of time complexity of three schemes

	点积运算		倍乘运算		模逆运算		Hash 运算	
	签名	验证	签名	验证	签名	验证	签名	验证
肖帅方案[5]	2	2	1	2	0	0	1	1
周克元方案[8]	3	1	1	2	0	0	1	1
本文方案 1	2	1	1	2	0	0	1	1
本文方案 2	1	1	1	2	0	0	1	1

上述 4 种方案中，Hash 函数运算在签名和验证中均只有 1 次；模逆运算在签名和验证中均为 0 次；倍乘运算在签名和验证中均为 1 次和 2 次；点积运算相对于倍乘和模逆来说计算量较小，本文给出的

两个改进方案的点积运算次数少于肖帅方案周克元方案，因此本文的两个改进方案复杂度更低。

5　结束语

本文对椭圆曲线数字签名的改进方案进行了分析，指出了栗亚敏改进方案的错误，同时给出了两个新的改进方案，证明了改进方案的正确性和安全性。改进方案中模逆运算次数为 0 次，与其他方案进行了复杂度比较，改进方案复杂度更低。

参考文献

[1] 王丽君，付春宝，董诗娟. 椭圆曲线在多重盲签名中的应用[J]. 计算机应用与软件，2008，25(1)：253-255.

[2] 任中岗，翟东海. 有限域 GF(q) 上安全椭圆曲线的选取[J]. 信息与电子工程，2009，7(5)：493-496.

[3] 侯爱琴，高宝建，张万绪，等. 基于椭圆曲线的一种高效率数字签名[J]. 计算机应用与软件，2009，26(2)：58-59.

[4] 杨青，王昊轩. 改进的椭圆曲线数字签名方案及实例分析[J]. 计算机应用与软件，2023，40(1)：327-330.

[5] 肖帅，王旭安，潘峰. 无模逆运算的椭圆曲线数字签名算法[J]. 计算机工程与应用，2020，56(11)：118-123.

[6] 杨迎辉，任俊峰，袁喜凤. 改进的具有消息恢复签名方案[J]. 计算机技术与发展，2011，21(4)：168-170.

[7] 张平，栗亚敏. 前向安全的椭圆曲线数字签名方案[J]. 计算机工程与应用，2020，56(1)：115-120.

[8] 周克元. 快速椭圆曲线消息恢复数字签名方案[J]. 西北师范大学学报(自然科学版)，2015，49(5)：54-56.

[9] 肖鸿飞，刘长江. 一种基于身份的改进高效签密方案[J]. 计算机工程，2011，37(24)：126-128.

[10] 王彩芬，樊睿，白荷芳. 前向安全的签密方案[J]. 兰州大学学报(自然科学版)，2006，42(6)：84-87.

[11] 周克元. 公开验证和前向安全数字签密方案的分析与改进[J]. 西北师范大学学报(自然科学版)，2015，51(6)：50-53.

[12] 杨青，辛小龙，戢伟. 基于椭圆曲线的数字签名和代理数字签名[J]. 计算机工程，2008，34(23)：147-149.

[13] 李方伟，万丽，闫少军. 基于椭圆曲线的盲代理盲签名方案[J]. 计算机工程，2012，38(3)：139-140.

[14] 黄秀菊，杜云飞，李子臣. 种理想格上高效盲签名方案[J]. 计算机应用研究，2022，39(11)：3461-3464.

[15] 张硕英，刘锋. 一个可证安全和前向安全的群盲签名方案[J]. 计算机应用与软件，2024，41(3)：308-312.

[16] 饶金涛，崔喆. 基于 SM2 门限盲签名电子选举方案[J]. 计算机应用，2024，44(2)：512-518.

[17] 汤永利，李元鸿，张晓航，等. 格上基于身份的群签名方案[J]. 计算机研究与发展，2022，59(12)：2723-2734.

[18] 张明武，夏禹轩，张语荻，等. 一种基于群签名的许可区块链匿名背书方案[J]. 密码学报，2022，9(3)：496-510.

[19] 张学旺，张豪，姚亚宁，等. 基于群签名和同态加密的联盟链隐私保护方案[J]. 信息网络安全，2023，23(3)：56-61.

[20] 张庆胜，郭宝安，徐树民，等. 快速椭圆曲线签名验证算法[J]. 计算机工程与设计，2008，29(17)：4425-4427.

[21] 栗亚敏，张平. 一种改进的椭圆曲线数字签名方案[J]. 计算机应用与软件，2020，37(12)：304-308.

[22] JOHNSON D，MENEZES A，VANSTONE S. The elliptic curve digital signature algorithm(ECDSA)[J]. International Journal of Information Security，2001，1(1)：36-63.