一种椭圆曲线数字签名的改进方案

陈亚茹　丛培强　陈　庄
（重庆理工大学计算机科学与工程学院　重庆　400054）
（642200814@qq.com）

An Improved Scheme for Elliptic Curve Digital Signature

Chen Yaru, Cong Peiqiang, and Chen Zhuang
(*School of Computer Science and Engineering, Chongqing University of Technology, Chongqing* 400054)

Abstract　The existing problems of elliptic curve digital signature (ECDSA) are briefly described, the improved scheme for the existing problems of ECDSA is studied, although the scheme improves the computational efficiency of ECDSA, the forgery signature attack is not considered. Based on the security and computational efficiency of elliptic curve digital signature, an improved scheme for elliptic curve digital signature is proposed, the safety and efficiency of the proposed scheme are proved by theory and simulation experiments. The results show that the improved scheme improves the computational efficiency of digital signature and prevents forgery attacks by scalar multiplication twice and inversion once.

Key words　ECDSA; forgery attack; scalar multiplication; inverse operation; computing time

摘　要　阐述了目前椭圆曲线数字签名(elliptic curve digital signature, ECDSA)存在的问题，针对ECDSA存在的问题提出了改进的方案，并分析了该方案虽然提高了ECDSA的计算效率，但未考虑伪造签名攻击的问题. 从椭圆曲线数字签名的安全性和计算高效性出发，提出了一种椭圆曲线数字签名的改进方案，通过理论和仿真实验证明了方案的安全性和高效性. 研究结果表明，改进的方案通过标量乘运算2次和逆运算1次，提高了数字签名的计算效率和防止数字签名伪造攻击.

关键词　椭圆曲线数字签名；伪造攻击；标量乘运算；逆运算；计算耗时

中图法分类号　TP309

Miller[1]和Koblitz[2]提出了椭圆曲线算法(ECC)，并指出椭圆曲线的安全性取决于离散对数问题求解的困难性(ECDLP). Johson等人[3]在2001年提出了椭圆曲线数字签名(elliptic curve digital signature, ECDSA)算法，通过2次逆运算、3次标量乘运算实现数字签名的过程. 随着对ECDSA的深入研究，业界提出了影响ECDSA签名耗时的2个主要计算因素：一是求逆运算，文献[3]提出求逆的时间消耗是乘法的10倍；二是标量乘法运算[4]，标量乘法运算是已知椭圆曲线1个点G和1个随机数k，求kG的运算过程. 由于在乘法运算中至少要进行1次求逆运算，所以耗时

收稿日期：2018-12-14
基金项目：重庆市研究生科研创新基金项目(CYS18312)

集中在求逆运算上. 针对 ECDSA 计算的耗时问题,业界提出了对逆运算和标量乘运算的各种改进的方案[5-6]. 陈亮等人[7]提出了一种无求逆的数字签名新算法,该算法在签名和验证中避免求逆运算,并且在签名和验证过程中各进行 1 次模乘运算,提高运算速度. 宋凡[8]提出了文献[7]通过减少求逆运算来提升签名效率引起伪造签名的安全问题,在改进 ECDSA 效率问题的同时应该考虑安全问题. 曹欣等人[9]提出一种改进的 ECDSA 算法,通过使用 SHA-256 算法有效避免了求逆运算来提高效率. 白国强等人[10]提出了一次性计算 $kP+IQ$ 的方法,使 kP,IQ 计算量减少到 25%,并适用于无线网络中. 张庆胜等人[11]提出一种改进的 ECDSA 方案,通过模乘运算 2 次,模逆运算 1 次,提高了签名的速度. 伍红梅[12]分析了文献[11]存在的局限性,提出文献[11]虽然提高计算效率但遭受伪造攻击,文献[13]提出 Hanmming 距离和哈希值的关系.

针对 ECDSA 的耗时和伪造攻击的问题,本文结合 Hanmming[13]提出了 ECDSA 数字签名的改进的方案,通过标量乘运算 2 次和逆运算 1 次,提高了数字签名的计算效率和防止数字签名伪造攻击.

1 张庆胜等人[11]方案分析

ECDSA[14]是 DSA 在椭圆曲线上的移植. ECDSA 包括数字签名和签名验证 2 个过程[15]. 设椭圆曲线参数为 $T=(p,a,b,G,n)$,定义椭圆曲线为 $y^2=(x^3+ax+b)\bmod p$,其中 p 是一个大素数,F_p 为有限域,a,b 是整数,G 是 $E(F_p)$ 上的基点,n 为素数,是基点 G 的阶数,用户 A 的私钥为 d,公钥 $Q=dG$,k 是选取的随机整数,e 是消息 m 的哈希运算的数值,r 是椭圆曲线上点 (x,y) 中 x 对 n 的取余. 文献[11]提出一种改进的 ECDSA 方案,通过签名方程形式 $s=er+rd$ 推导出 $s=(er)^{-1}(k+d)$.

1.1 ECDSA 签名过程

用户 A 对消息 m 签名,步骤如下:

① 用户 A 随机选择一个整数 k,使得 $k\in[1,n-1]$;

② 计算 $kG=(x_1,y_1)$ 及 $r=x_1 \bmod n$;其中若 $r=0$,则调转到①;

③ 计算待签名的 m 的哈希值 e,$e=H(m)$;

④ 计算 $s=(er)^{-1}(k+d)\bmod n$;

⑤ (r,s) 是对 m 的签名数据.

用户 B 收到用户 A 的签名数据 (r,s) 后,要验证用户 A 在消息 m 上的签名,需要如下步骤:

① 验证 r,s 是在区间 $[1,n-1]$ 内的整数;

② 计算 $e=H(m)$;

③ 计算 $w=(er)s \bmod n=(k+d)\bmod n$;

④ 计算 $wG-Q=(kG+dG)-dG=(x_1,y_1)$;

⑤ 计算 $v=x_1 \bmod n$.

若 $v=r$,接受签名,否则丢弃.

张庆胜等人[11]在改进的 ECDSA 方案中签名过程只进行 1 次标量乘法运算,验证签名也只进行 1 次运算,因此比传统的 ECDSA 验证签名时间减少一半,提高了 ECDSA 算法的签名速度.

1.2 伪造签名攻击

在文献[11]改进的方案中 k,d 只有发送方拥有,接收方只可以计算 $(k+d)\bmod n$,却无法推导出 k,d,在一定程度上起到对私钥的保护作用. 但是,虽然接收方 C 推导不出 k,d,但是可以进行消息 m 和随机数的 k 伪造签名,进行伪造攻击. 伪造过程如下:

1) 替换消息 m 伪造攻击

接收方 C 收到签名消息 (r,s) 后,可以用消息 m' 代替 m 进行签名.

C 伪造签名如下:

① 由于 s,e,r 已知,B 由 $s=(er)^{-1}(k+d)\bmod n$ 计算出 $(k+d)\bmod n$;

② 使用替换的消息 m',计算 $e=H(m')$;

③ 计算 $s'=(e'r)^{-1}(k+d)\bmod n$;

④ (r,s') 为 m' 的签名数据.

B 收到 C 的伪造签名信息 (r,s') 后,进行签名验证如下:

① 验证 $r\in[1,n-1]$;

② 计算 $e=H(m')$;

③ 计算 $w'=(e'r)s' \bmod n=(k+d)\bmod n$;

④ 计算 $w'G-Q=(kG+dG)-dG=(x_1',y_1')$;

⑤ 计算 $v=x_1' \bmod n$;

显然若 $v=r$,接受签名.

2) 替换随机数的伪造攻击

接收方 C 收到签名消息 (r,s) 后,可以用替换

的随机数 k' 代替 k 进行签名.

C 伪造签名过程如下：

① 由于 s,e,r 已知，C 由 $s=(er)^{-1}(k+d) \bmod n$ 计算出 $(k+d) \bmod n$；

② 随机生成一个整数 t，计算 $k'=k+t$，其中 k',k 都是未知的；

③ 计算 $k'G=(k+t)G=kG+tG=(x',y')$；

④ 计算 $r'=x' \bmod n$；

⑤ 计算 $e=H(m)$；

⑥ 计算 $s'=(er')^{-1}(k'+d)=(er')^{-1}(k+t+d) \bmod n$；

⑦ (r',s') 即是消息 m 伪造的信息.

B 收到 C 的伪造签名信息 (r',s') 后，进行签名验证如下：

① 验证 $r' \in [1,n-1]$；

② 计算 $e=H(m)$；

③ 计算 $w'=(er')s' \bmod n=(k'+d) \bmod n$；

④ 计算 $w'G-Q=(k'G+dG)-dG=(x',y')$；

⑤ 计算 $v'=x' \bmod n$；

显然，$v'=r'$，签名有效.

综上所述，伪造方 C 窃取签名信息 (r,s) 后，虽然 k,d 未知，但是根据已知数据 s,e,r 可以计算出 $(k+d) \bmod n$，之后利用替换信息 m、随机数 k 进行伪造攻击. 为了避免数字签名的伪造攻击，k，d 需要是不同的系数值.

2 改进的 ECDSA 方案

为了提高 ECDSA 数字签名的运算效率和防伪造攻击，在数字签名过程可以采用哈希值的 Hamming[13] 重量来代替哈希值实现签名的过程. 以 MD5 为例，哈希数值为 128 b 的二进制数，而 Hamming 重量为 7 b 二进制数. Hamming 值对消息变化很敏感，若消息发生变化，Hamming 值发生变化的概率在 92% 以上. 基于此，本文提出了一种新的 ECDSA 的改进方案.

2.1 改进的算法描述

设 ECC 参数为 $T=\{a,b,G,n,h\}$，用户私钥 $A(d,Q)$ 对消息 m 签名，签名和验证过程如图 1 所示：

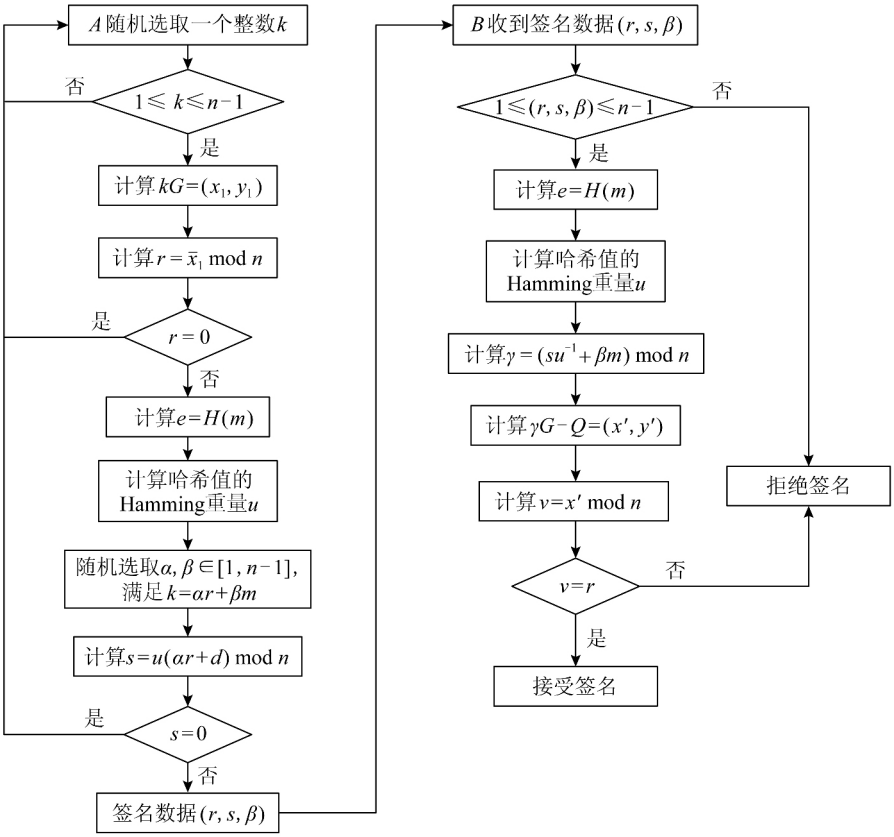

图 1 改进的 ECDSA 算法流程

① A 随机选择一个整数 k，$k\in[1,n-1]$；

② 计算 $kG=(x_1,y_1)$，并将 x 转换成整数 $\bar{x}$；

③ 随机选择 1 组 $\alpha,\beta\in[1,n-1]$，α,β 满足条件 $k=\alpha r+\beta m$；

④ 计算待签名的消息 m 的哈希值 e，$e=H(m)$，并求哈希值的 Hanming 重量 u；

⑤ 计算 $r=\bar{x}_1 \bmod n$；其中若 $r=0$，则调转到步骤①；

⑥ 计算 $s=u(\alpha r+d)\bmod n$；若 $s=0$，则跳转到步骤①；

⑦ (r,s,β)即为签名 m 的信息.

用户 B 收到 m 和 (r,s,β)后，对签名的验证过程如下：

① 验证 r,s,β 是否在区间$[1,n-1]$内的整数，若任何一个验证失败，则拒绝签名；

② 计算 $e=H(m)$，并求哈希值的 Hamming 重量 u；

③ 计算 $\gamma=(su^{-1}+\beta m)\bmod n$；

④ 计算 $\gamma G-Q=(x',y')$；

⑤ 计算 $v=x' \bmod n$；

⑥ 若 $v=r$，则验证签名成功.

之后，对改进算法的证明如下：

若(r,s,β)是对 m 的签名信息，则 $\gamma=(su^{-1}+\beta m)\bmod n=(k+d)\bmod n$，$k=(\gamma-d)\bmod n$. 因此，$(x,y)=kG=(\gamma-d)G=\gamma G-dP=rG-Q=(x',y')$，所以有 $v=x'=x=r \bmod n$.

2.2 改进的算法分析

1）抗替换信息的伪造攻击

接收方 C 收到 A 发送的(r,s,β)信息后，可以用另外的消息 m'代替 m 进行签名.

C 伪造签名如下：

① 由于 s,u,r 已知，C 由 $s=u(\alpha r+d)\bmod n$ 计算出$(\alpha r+d)\bmod n$；

② 使用替换的消息 m'，计算 $e'=H(m')$，并计算 e'的 Hamming 重量 u'；

③ 计算满足条件 $k=\alpha r+\beta m$ 的α,β；

④ 计算 $s'=u'(\alpha r+d)$；

⑤ 伪造签名计算 $s'=u'(\alpha r+d)$；

(r,s',β)为 m'的签名数据.

B 收到(r,s',β)签名信息后，进行签名验证如下：

计算 $\gamma'=[s'u'^{-1}+\beta m]\bmod n$，$\gamma'=(\alpha r+\beta m'+d)\bmod n\neq(k+d)\bmod n$. 因此签名无效.

2）替换随机数的伪造攻击

接收方 C 收到签名消息(r,s,β)后，可以用替换的随机数 k'代替 k 进行签名.

C 伪造签名过程如下：

① 由于 s,u,r 已知，B 由 $s=u(\alpha r+d)\bmod n$ 计算出$(\alpha r+d)\bmod n$；

② 随机生成一个整数 t，计算 $k'=k+t$，其中 k',k 都是未知的；

③ 计算 $k'G=(k+t)G=kG+tG=(x',y')$；

④ 计算 $r'=x'\bmod n$；

⑤ 计算满足条件 $k'=\alpha' r'+\beta' m$ 的α',β'；

⑥ 计算 $e=H(m)$，并求哈希值的 Hamming 重量 u；

⑦ 计算 $s'=u(\alpha' r'+d)\bmod n$.

B 收到(r',s',β') 签名信息后，进行签名过程如下：计算 $\gamma=(s'u^{-1}+\beta m)\bmod n=(\alpha' r'+d+\beta m)\bmod n\neq(x_1,y_1)$，因此签名无效.

由上分析可知，改进的 ECDSA 算法可以抵御接收者伪造签名.

3 改进方案的性能分析

3.1 安全性分析

1）抗伪造攻击

发送方 A 和接收方 B 虽然知道 e,r',a'，$(\alpha r+d)\bmod n$，但是接收方 B 验证出来的 x'与 x 不同，所以可以有效地抵御伪造攻击.

2）防止数据篡改

数据的完整性是通过对哈希值和 Hamming 使用实现的，一旦数据被篡改，Hamming 将得到不同的数值，如果 Hamming 值不相同，从步骤中可以看出签名不通过.

3）抗中间人攻击

在传统的通信中，公钥是公开的，私钥可以是随机数 r 或分发用户的 d. 攻击者选择随机数 $r_c\in[1,n-1]$，截取 A 发给 B 的 $Q_A=d_AG$，B 发给 A 的 $Q_B=d_BG$，将 d_AG,d_BG 修改成 r_cG，协商之后，A 与非法用户共享密钥 d_Ad_BG，A 误认为 B 是共享的，B 与非法用户共享 d_Ad_BG，而 B 认为 A 是共享的，实际 A 和 B 没有共享密钥. 当 A 发送信息给 B 时用 d_Ar_cG 进行信息加密，非法用户截取之后进行解密，伪造信息，用 d_Ad_BG 加密后发送给

B，这样就欺骗了用户 A 和 B，A 和 B 是不知情的，这样就影响了正常的密钥协商. 因此，通信双方在不清楚对方身份的情况下进行的密钥会话的建立，容易遭受中间人攻击. 本方案通过数字签名技术实现身份的双向认证，非法用户不能冒充任何一方，防止中间人攻击.

4）向前安全性

假设非法用户得到 A 或 B 的私钥，很难得到会话密钥. 因为 $Q_A=d_AG$，由离散对数难题，攻击者窃取 Q_A，G 也很难推出 d_A，无法获得私钥. 因此，方案具有向前安全性.

5）抗抵赖性

接收方根据发送方发送的(r,s,β)，防止发送方事后具有不可抵赖性.

将改进后的方案与现有的方案进行了安全性对比，从 5 个方面分析系统安全性. 如表 1 所示：

表 1　安全性对比

方案	抗伪造安全	防止数据篡改	抗中间人攻击	前向安全性	抗抵赖性
陈亮[7]	否	否	否	否	否
白国强等人[10]	否	是	否	否	否
张庆胜等人[11]	否	是	是	是	是
本文方案	是	是	是	是	是

3.2　效率分析

在签名过程中耗时要集中在乘法、逆运算和标量乘运算，记作$[l]$，$[i]$，$[h]$，加法等运算影响较小，忽略不计. 1 次逆运算约等于 10 次乘法运算，得到$[i]=10[l]$，文献[10]指出标量乘运算是满足在 163 b 下$[h]=75[i]+173[l]$. 设模乘运算的数据规模为 f，表 2 是新方案与传统的 ECDSA 的耗时对比，同时对签名采用 Matlab 编程进行仿真，检测效率如图 2 所示. 图 2 表示这 3 种方案的运算复杂度与数据规模的关系.

表 2　改进的算法与传统的 ECDSA 算法耗时对比

方案	乘法		求逆运算		标量乘运算		总计	
	签名	验证	签名	验证	签名	验证	签名	验证
ECDSA	2	2	1	1	1	2	935$[l]$	1 858$[l]$
张庆胜等人[11]改进的方案	2	2	1	0	1	1	935$[l]$	925$[l]$
本文方案	3	2	0	1	1	1	926$[l]$	935$[l]$

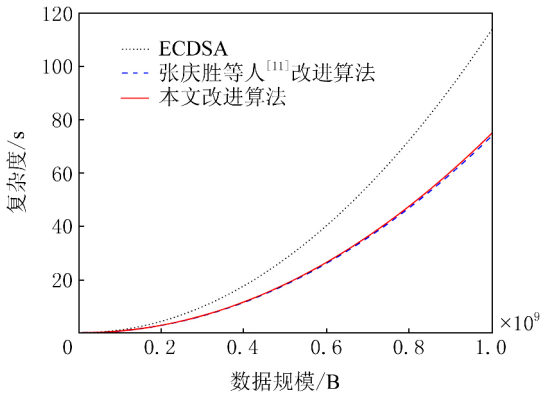

图 2　复杂度与数据规模的对比

从上面分析可知，本文改进的方案在签名上的耗时比 ECDSA 提高了 0.96%，比文献[11]提高了 0.96%，在验证上比 ECDSA 提高了 49.6%，比文献[11]慢了 1%，但是实现了抗伪造攻击.

4　结束语

本文分析了快速椭圆曲线签名验证方案[11]的不足，并结合 Hamming（汉明文距离）进行了方案的改进. 改进的方案通过标量乘运算 2 次和逆运算 1 次，实验的仿真证明了本方案提高了数字签名的计算效率，理论上证明了可以防止数字签名伪造攻击.

参 考 文 献

[1] Miller V. Uses of elliptic curves in cryptography [G] // LNCS 218: Advances in Cryptology. Berlin: Springer, 1986: 387-398

[2] Koblitz N. Elliptic curve cryptosystems [J]. Mathematics of Computation, 1987, 27(48): 203-209

[3] Johson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm (ECDSA) [J]. International Journal of Information Security, 2001, 41(1): 36-63

[4] Guajardji J, Paar C. Efficient algorighms for flliptic curve cryptosytems [C] //Proc of Eurocrypt'97. Berlin: Spring, 1997: 342-356

[5] 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)：58-60

[6] 赵泽茂，刘凤玉，徐慧. 基于椭圆曲线密码体制的签名方程的构造方法[J]. 计算机工程，2004，30(19)：96-97

[7] 陈亮，游林. 椭圆曲线数字签名算法优化与设计[J]. 电子器件，2011，34(1)：89-93

[8] 宋凡. 关于改进 ECDSA 的安全问题研究[J]. 贵阳学院学报：自然科学版，2012，7(4)：32-33

[9] 曹欣，魏仕民. 一种改进的椭圆曲线数字签名算法[J]. 淮北师范大学学报：自然科学版，2013，34(2)：1-3

[10] 白国强，黄谆. 椭圆曲线数字签名算法中的快速验证算法[J]. 清华大学学报：自然科学版，2003，43(4)：564-568

[11] 张庆胜，郭宝安，程登峰. 快速椭圆曲线验证算法[J]. 计算机工程与设计，2008，17(29)：4425-4427

[12] 伍红梅. 基于椭圆曲线的 ELGamal 数字签名方案[J]. 楚雄师范学院学报，2010，25(3)：44-47

[13] 孙建梅. 基于内容的图像认证技术研究[D]. 西安：西北大学，2005

[14] Xu Jiawei, Wang Keda, Wang Chao. Byzantine fault-tolerant routing for large-scale wireless sensor networks based on fast ECDSA [J]. Tsinghua Science and Technology, 2015, 20(6): 627-633

[15] 王国才，刘美兰. 基于椭圆曲线的高效分级群签名[J]. 计算机应用研究，2014，31(2)：586-589

陈亚茹

硕士研究生，主要研究方向为信息安全.

642200814@qq.com

丛培强

硕士研究生，主要研究方向为大数据.

1539397039@qq.com

陈　庄

教授，研究生导师，主要研究方向为企业信息化管理、网络与信息安全.

cz@cqut.edu.cn