无模逆运算的椭圆曲线数字签名算法

肖 帅[1,2],王绪安[1,2],潘 峰[1,2]
1.武警工程大学 网络与信息安全武警部队重点实验室,西安 710086
2.武警工程大学 密码工程学院,西安 710086

摘 要:经典的椭圆曲线数字签名(ECDSA)在签名和验证过程各使用了1次求逆运算,复杂费时的求逆运算制约着数字签名效率的提升。针对目前ECDSA的局限性,业界提出了很多改进方案,然而一些改进方案仅仅从ECDSA计算效率的提高入手,但却未能将诸如伪造签名攻击的问题考虑在内。在对经典ECDSA方案分析的基础上,兼顾椭圆曲线数字签名的安全性和计算效率,提出了一种改进的椭圆曲线数字签名新方案,并通过理论分析和仿真实验证明了新方案的安全性和高效性。研究结果表明,改进的方案通过引入双参数以及在签名和验证阶段回避求 Zp^* 逆运算,既提高了数字签名的计算效率又能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;安全性;模逆运算
文献标志码:A **中图分类号:**TP391 doi:10.3778/j.issn.1002-8331.1911-0456

肖帅,王绪安,潘峰.无模逆运算的椭圆曲线数字签名算法.计算机工程与应用,2020,56(11):118-123.
XIAO Shuai, WANG Xu'an, PAN Feng. Elliptic curve digital signature algorithm without modular inverse operation. Computer Engineering and Applications, 2020, 56(11):118-123.

Elliptic Curve Digital Signature Algorithm Without Modular Inverse Operation

XIAO Shuai[1,2], WANG Xu'an[1,2], PAN Feng[1,2]
1.Key Laboratory for Network and Information Security of Chinese Armed Police Force, Engineering University of Chinese Armed Police Force, Xi'an 710086, China
2.Institute of Cryptology Engineering, Engineering University of Chinese Armed Police Force, Xi'an 710086, China

Abstract: The classic ECDSA scheme uses one inversion operation in the process of signature and verification, and the complex and time-consuming inversion operation restricts the efficiency of digital signature. In view of the limitations of ECDSA, many improvement schemes have been put forward in the industry. However, some improvement schemes only start from the improvement of ECDSA computing efficiency, but they fail to take into account such issues as forgery signature attack. Based on the analysis of the classical ECDSA scheme, taking into account the security and calculation efficiency of the elliptic curve digital signature, an improved new scheme of the elliptic curve digital signature is proposed and the security and efficiency of the new scheme are proved through theoretical analysis and simulation experiments. The results show that the improved scheme can not only improve the efficiency of digital signature calculation, but also prevent the forgery attack of digital signature by introducing two parameters and avoiding the inverse operation in the signature and verification phase.

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

1 引言

数字签名算法(DSA)是1991年8月由美国国家研究所(NIST)提出的标准和技术[1-3],它的安全性是基于离散对数(DL)在 Zp^* 的素数阶子群中的计算不可追溯

基金项目:国家自然科学基金(No.61772550,No.U1636114,No.61572521);陕西省自然科学基础研究计划项目(No.2018JM6028);国家密码发展基金(No.MMJJ20170112);国家重点研发计划(No.2017YFB0802000)。
作者简介:肖帅(1992—),男,硕士,研究领域为数字签名,E-mail:756617001@qq.com;王绪安(1981—),男,博士,副教授,硕士生导师,研究领域为密码学,信息安全;潘峰(1967—),男,教授,硕士生导师,研究领域为对称密码。
收稿日期:2019-11-29 **修回日期:**2020-03-13 **文章编号:**1002-8331(2020)11-0118-06
CNKI**网络出版:**2020-03-18, http://kns.cnki.net/kcms/detail/11.2127.tp.20200317.1457.006.html

性的问题(DLP)。作为信息与数据安全的核心技术之一，它可以实现身份认证、数据完整性保护、防篡改、防冒充和不可否认性等数据传输中的重要需求[4]。Johson等人[2]在2001年提出了椭圆曲线数字签名(Elliptic Curve Digital Signature，ECDSA)算法，它是通过2次模逆运算、3次标量乘运算来实现数字签名的过程的。椭圆曲线数字签名是重要的信息保护技术之一，它通过为信息增加签名，有效保护了信息的完整性、不可否认性、认证性、不可伪造性，目前这一算法得到了广泛认可和应用[5]。图1显示的是ECDSA的发展历程。

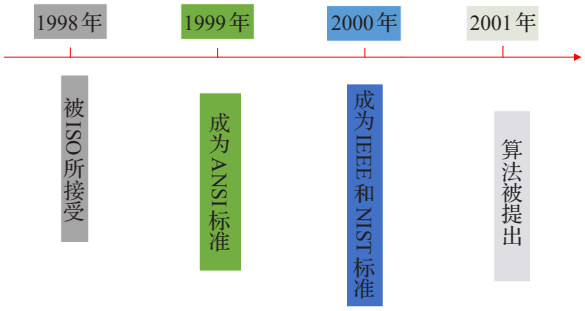

图1　ECDSA发展历程

椭圆曲线数字签名算法(ECDSA)是对数字签名算法(DSA)的模拟。椭圆曲线密码(ECC)由Koblitz N[6]和Miller V[7]于1985年发明，是目前安全性最高的公钥加密算法，它是基于椭圆曲线的一种公钥体制。相较其他公钥体制，椭圆曲线密码的单位比特强度要高一些。椭圆曲线密码体制的主要优势是计算参数更小，密钥更短[8]，运算速度更快，签名也更加短小[9]，效率也更高[10]。因此椭圆曲线密码性能优良，应用广泛，尤其适用于存储空间、处理能力、带宽及功耗受限的场合[11]。

表1显示的是基于公钥密码的数字签名体制的分类：在这三种分类中，ECDLP是最难解的，除几类特殊椭圆曲线外，至今仍没有ECDLP的有效求解算法。

表1　基于公钥密码的数字签名体制分类

根据困难问题分类	典型例子
大整数分解问题(IFP)	RSA
离散对数问题(DLP)	ElGamal，DSA等
基于椭圆曲线离散对数问题(ECDLP)	ECDSA

数字签名应用广泛，电子商务和网络安全认证的核心技术就是数字签名，最近大火的区块链技术，其底层技术之一就是数字签名。由于数字签名方案是许多保密协议的核心构造块，因此提高数字签名方案的效率是非常重要的[12]。

在对ECDSA的深入研究过程中，一般一致认为影响ECDSA签名耗时主要有两个计算因素[13]：一是标量乘法运算[14]，标量乘法运算是已知椭圆曲线上两个点：基点 G 和随机数 k，求 kG 的运算过程。另外一个也是最主要的运算就是模逆运算，由于在乘法运算中至少要进行1次求逆运算，而模逆运算所需要消耗的时间是乘法运算的10倍[2]，所以耗时主要由求逆运算产生。针对ECDSA计算的耗时问题，对求逆运算和标量乘运算的各种改进的方案[15-21]相继被提出，详见表2。

表2　对求逆运算和标量乘运算的各种改进的方案

改进方案	主要内容
文献[15]	在签名和验证过程中完全避免求逆运算，并使用Hamming重量代替Hash值
文献[16]	提出一种无求逆的数字签名新算法，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
文献[17]	指出文献[16]通过减少求逆运算来提升签名效率会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
文献[18]	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
文献[19]	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
文献[20]	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
文献[21]	分析了文献[20]存在的局限性，指出文献[20]虽然提高计算效率，但易遭受伪造攻击
文献[13]	针对ECDSA的耗时和伪造攻击的问题，结合Hamming距离提出了ECDSA数字签名的改进方案，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

本文在分析研究经典的椭圆曲线密码理论的基础上，针对经典ECDSA方案中存在的耗时和伪造攻击的问题，通过引入双参数和避免求逆运算，提出了一种改进的能实现高效率的数字签名方案。

2　预备知识

2.1　方案参数与释义说明

本文方案描述所涉及的参数符号及释义如表3所示。

表3　参数符号与释义

参数	释义	参数	释义
U	签名方	s	数字签名
M	消息明文	k	随机整数
p，q	大素数	k^{-1}	k的逆运算
$H()$	哈希函数	R	与k相关的量
G	椭圆曲线上的基点	n	模数
mod	模运算	V	验证方
d_u	用户私钥	T	椭圆曲线域参数
e	哈希值		

2.2　椭圆曲线密码体制

椭圆曲线密码体制可以看作是旧的离散对数(DL)的椭圆曲线类似物，Z_P* 的子群被有限域上椭圆曲线上的点群所代替。以下是ECC的一般结构：

设 $P\in(F_P)$，点 Q 是 P 的倍数，即存在正整数 X，使得 $q=Xp$，然后用给定的 p 和 q 定义ECDLP。基于

椭圆曲线离散对数问题,产生了椭圆曲线密码体制。

设 E 为椭圆曲线, p 为 E 上的一个点,如果存在正整数 N ,使得 $NP=0$,则 n 是点 P 的阶数,其中 O 是无穷大点。

椭圆曲线公钥密码(ECC)体制的构造如下:

选择域 Fp ,椭圆曲线 E ,选择点 $P(x_p,y_p)$, n 为 E 上的素数阶。公开信息:有限域 F_p ,曲线方程 E ,点 P 及其阶 n ,计算 $Q=dP$,取 Q 点为公钥,整数 D 为密钥。

要向Alice发送秘密信息 M ,需要执行以下步骤:

(1)在域 Fp 中将明文 M 表示为元素 M ;

(2)随机选取 $[1,n-1]$ 中的整数 k ;

(3)计算点 $(x_1,y_1)=kP$;

(4)计算点 $(x_2,y_2)=kQ$,如果 $x_2=0$,则重新选择 k ;

(5)计算 $c=mx_2$;

(6)发送 (x_1,y_1,c) 给Alice。

当Alice接收到密文时,使用密钥 D 计算密文。

$$D(x_1,y_1)=dkP=k(dP)=kQ=(x_2,y_2)$$

然后计算 $cx_2^{-1}=m$ 得到明文 m 。

这里 $Q=dP$ 是公开的。如果破译者能够解决椭圆曲线上的离散对数问题,就可以从 dP 中还原出 d ,完成解密[22]。

2.3　椭圆曲线离散对数问题(ECDLP)

椭圆曲线离散对数问题是对于椭圆曲线 $E\left(GF(q)\right)$ 上任意两点 G 和 Q ,有 $Q=dG$,在已知 G 和 Q 的前提下求出小于 q 的正整数 d 。已知 d 和 G 计算 Q 比较容易,但是已知 Q 和 G 计算 d 则很困难,这便是椭圆曲线加密体制的核心。椭圆曲线密码体制的安全性基于椭圆曲线离散对数问题,也就是求解ECDLP算法的时间复杂度。

3　ECDSA数字签名原理与方案分析

3.1　ECDSA数字签名方案描述

ECDSA是ECC与DSA的结合,整个签名过程与DSA类似,所不一样的是签名中采取的算法为ECC,最后签名出来的值也是分为 r,s 。

(1)方案建立

U 为签名者, V 为验证者:

① U 构建椭圆曲线城参数 $T=(p,a,b,G,n,h)$;

② U 建立密钥对 (d_u,Q_u) ,且有 $Q_u=d_uG$;

③ U 选择一个hash数;

④ U 将hash函数和椭圆曲线域参数 T 传给 V 。

(2)签名算法

① 选择一个临时密钥对 (k,r) ,其中 $R=kG=(x_R,y_R)$ 和域参数 T 相关。

② 令 $r=x_R \bmod n$,如果 $r=0$,返回1。

③ 计算待签消息的hash值 $H=H(m)$,将 H 转换成整数 e 。

④ 计算 $s=k^{-1}(e+rd_u)(\bmod n)$,如果 $s=0$,返回1。

⑤ 输出 $S=(r,s)$ 为数字签名。

(3)验证算法

V 通过验证从 U 发来的数字签名来判断所接收消息以及对方身份的真伪。

① 如果 $r,s\notin[1,n-1]$,验证不通过。

② 计算待签消息的hash值 $H=Hash(M)$,将 H 转换成整数 e 。

③ 计算 $u_1=es^{-1}(\bmod n),u_2=rs^{-1}(\bmod n)$ 。

④ 计算 $R=\left(x_R,y_R\right)=u_1G+u_2Q_u$,如果 $R=0$,验证失败。

⑤ 令 $v=x_R(\bmod n)$,如果 $v=r$,验证成功,否则验证失败。

3.2　ECDSA数字签名方案分析

在ECDSA方案中,公钥的产生算法是 $Q_u=d_uG$,在签名的生成和验证过程中需要分别计算 $k^{-1} \bmod n$ 和 $s^{-1} \bmod n$,即需要进行模逆运算。若模乘运算的数据规模为 n ,则一次模乘运算的复杂度为 $O(n^2 \ln n)$ 。表4分析了ECDSA方案的算法复杂度。

表4　ECDSA算法复杂度分析

运算	签名算法			验证算法		
	点积	模逆	模乘	点积	模逆	模乘
运算次数	1	1	2	2	1	2
总运算量	$(\ln n+11)n^2$			$(2\ln n+11)n^2$		

可以看到,签名算法和验证算法运算很复杂,都有模逆运算。前文中已经提到,在现有的椭圆曲线加密或者签名过程中,主要的运算负担来自求逆运算,求逆是最复杂费时的操作,一次求逆的时间大约相当于80次点乘运算。如果可以减少甚至是避免模逆运算无疑有助于数字签名效率的提升。

4　改进的ECDSA方案

由以上分析可知,在签名或者验证阶段,如果可以减少甚至是避免模逆运算无疑有助于数字签名效率的提升。但在着力提高运算效率的同时也应兼顾安全问题,基于此,本文提出了一种新的ECDSA的改进方案。

4.1　改进方案的算法描述

设ECC参数为 $T=\{a,b,G,n,h\}$,用户使用私钥 $A(d,Q)$ 对消息 m 进行签名,图2显示了签名和验证的具体过程。

(1)A随机选择一个整数 k , $k\in[1,n-1]$;

(2)计算 $kG=\left(x_1,y_1\right)$,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 $k=\alpha r+\beta m$;

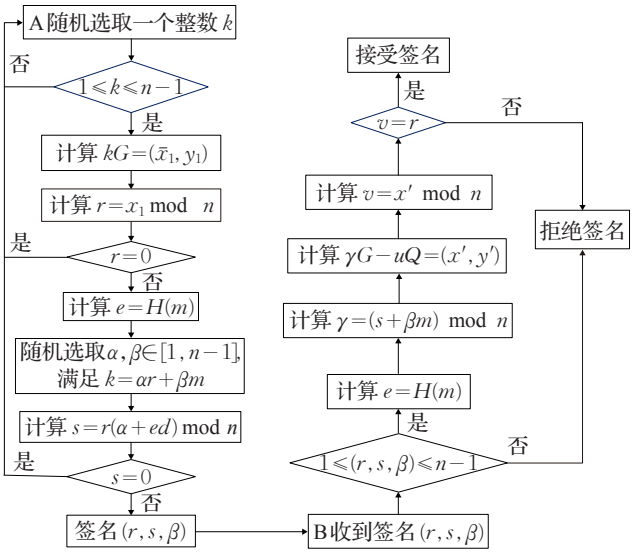

图2　改进的算法流程图

(4)计算待签名的消息 m 的哈希值 e，$e=H(m)$；

(5)计算 $r=\bar{x}_1 \bmod n$；其中若 $r=0$，则跳转到(1)；

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

(7) (r,s,β) 即为签名 m 的信息. 用户B收到 m 和 (r,s,β) 后，对签名进行如下验证：

① 验证 r,s,β 是否属于区间 $[1,n-1]$ 内的整数，若三者中任何一个参数验证失败，则拒绝签名；

② 计算 $e=H(m)$；

③ 计算 $\gamma=(s+\beta m)\bmod n$，$u=er \bmod n$；

④ 计算 $\gamma G-uQ=(x',y')$；

⑤ 计算 $v=x' \bmod n$；

⑥ 若 $v=r$，则验证签名成功。

在以上改进方案的算法描述细节部分，步骤(1)至步骤(3)中关于随机数 k 的选取，进行分析说明，以表明方案中随机数选取的合理性和随机性。

通过(1)，确定了一个整数 k，k 是在 $[1,n-1]$ 区间随机选取的，在(3)中，等式的两边都要进行模 n 运算，由于 n 为素数，r,m 为已知信息，k 被随机选取后，再从 $[1,n-1]$ 区间任意选取一个 α，则一定存在一个满足等式 $k=\alpha r+\beta m$ 的整数 β，且 $\beta\in[1,n-1]$，所以改进方案的构造具有合理性和随机性。

对改进算法的正确性证明如下，若 (r,s,β) 是对 m 的签名信息，则：

$$\gamma=(s+\beta m)\bmod n=(\alpha r+edr+\beta m)\bmod n=(k+erd)\bmod n$$

$$k=(\gamma-erd)\bmod n$$

因此

$$(x,y)=kG=(\gamma-erd)G=\gamma G-uQ=(x',y')$$

所以有 $v=x'=x=r \bmod n$

4.2　改进方案的算法分析

(1)抗替换信息的伪造攻击

A发送 (r,s,β) 信息给接收方C后，接收方C可以用伪造消息 m' 来代替 m 进行签名。

C伪造签名过程如下：

① 由于 s,e，r 为已知量，C由 $s=r(\alpha+ed)\bmod n$ 可计算出 $(\alpha+ed)\bmod n$；

② 使用替换的消息 m'，计算 $e'=H(m')$；

③ 计算满足条件 $k=\alpha r+\beta m$ 的 α,β；

④ 计算 $s'=r(\alpha+e'd)\bmod n$；

⑤ 伪造签名计算 $s'=r(\alpha+e'd)\bmod n$，(r,s',β) 为 m' 的签名数据。

B收到 (r,s',β) 签名信息后，进行如下签名验证，计算：

$$\gamma'=(s'+\beta m')\bmod n=(\alpha r+e'rd+\beta m')\bmod n\neq(k+erd)\bmod n$$

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，可以伪造随机数 k' 来代替 k 进行签名。C伪造签名过程如下：

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

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 $e=H(m)$；

⑦ 计算 $s'=r'(\alpha'+ed)\bmod n$。

B收到 (r',s',β') 签名信息后，进行如下签名过程：

计算 $\gamma'=(s'+\beta' m)\bmod n=(\alpha' r'+er'd+\beta' m)\bmod n\neq(x_1,y_1)$，因此签名无效，通过以上分析可知，改进的ECDSA算法可以有效抵御接收者伪造签名。

4.3　改进方案的性能分析

4.3.1　安全性分析

方案的构造通常不难，但首要的是要考虑到它的安全性，否则即使数字签名计算效率再高，也毫无意义。在本文的改进方案中，即使非法用户设法得到了A或B的私钥，也很难获取到会话密钥。由 $Q_A=d_A G$ 可知，如果攻击者在窃取 Q_A 和 G 后推出了 d_A，那么就意味着他解决了离散对数难题，而这是不可能的，因此攻击者无法获得私钥。具体安全性有以下几个方面。

(1)抗伪造攻击

对于发送方A和接收方B，虽然 $e,r',\alpha',(\alpha+ed)\bmod n$ 是公开已知的，但是接收方B验证出来的 x' 与 x 不同，所以可以有效地抵抗伪造攻击。

(2)防数据篡改

通过对消息进行哈希运算可以实现数据的完整性，一旦数据遭到篡改，哈希数值将会发生变化，从前述步

骤中可以看出,如果哈希值不相同,则签名无法通过。

(3)抗中间人攻击

在传统的通信过程中,公钥是公开的,私钥可以是随机数 r 或分发给用户的 d 。攻击者选取随机数 $r_c\in[1,n-1]$,截获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 对信息进行加密,非法用户截获之后进行解密,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,而事实上A和B是不知情的,这样正常的密钥协商就受到了影响。因此,在不清楚对方真实身份的情况下,通信双方建立的密钥会话易遭受中间人攻击。在本文方案中通信的双方实现了身份的双向认证,非法用户不能伪装成任何一方,从而有效地防止了中间人攻击。

(4)抗抵赖性

接收方根据发送方发送的 (r,s,β) ,防止发送方事后抵赖。

4.3.2　效率分析

在本文的方案中,签名和验证过程均没有模逆运算,通过具体的数值来分析改进方案的效率变化。在数字签名过程中耗时主要集中在乘法、逆运算和标量乘运算,可分别简记为 $[l],[i],[h]$,鉴于加法等运算对耗时的影响因素较小,故可忽略不计。1次求逆运算约相当于10次乘法运算,即 $[i]=10[l]$,根据文献[18],标量乘运算是满足在163b下 $[h]=75[i]+173[l]=750[l]+173[l]=923[l]$,设模乘运算的数据规模为 m ,表5是改进后的新方案与经典的ECDSA方案的耗时对比,由表5分析可知,本文改进的方案在签名上的计算效率比经典的ECDSA方案提高了0.96%,在验证上的计算效率比ECDSA方案提高了50.2%。

表5　两种方案耗时对比

方案	乘法		标量乘运算		求逆运算		总计	
	签名	验证	签名	验证	签名	验证	签名	验证
ECDSA	2	2	1	2	1	1	935[l]	1 858[l]
本文方案	3	2	1	1	0	0	926[l]	925[l]

4.3.3　仿真实验

在本文的改进方案中,签名和验证过程均没有求逆运算,理论上无疑会极大提升数字签名的效率,使用MATLAB编程模拟仿真来进行验证,检测效率如图3所示,从图中可以直观地看到两种方案的运算复杂度与数据规模的关系。

由图3可看到,相较经典的ECDSA方案,在同等的数据规模下,本文的改进方案中数据复杂度始终较低,

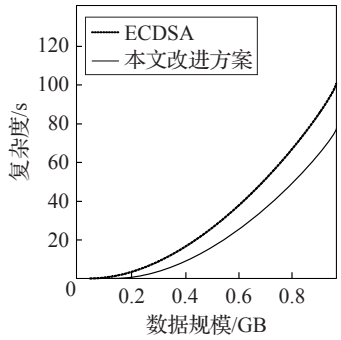

图3　复杂度与数据规模对比

实验仿真结果与本文的理论分析相吻合,即本文的改进方案可以提高数字签名的计算效率。

5　改进的ECDSA方案在电子商务中的应用

信息化网络时代,电子商务的飞速发展使得人们足不出户就可以享受方便快捷的服务。电子商务对信息的保密性、数据完整性、不可否认性有较高要求。人们在享受网上交易带来的便捷服务的同时,也日益关注信息安全。RSA签名算法曾被广泛使用来保护交易信息的安全,随着MD5算法被破解,SHA-1算法受到挑战和ECDSA在理论上的日益成熟,ECDSA算法的优越性日益凸显,电子商务的安全越来越需要ECDSA来保证。

将改进的ECDSA方案与时下飞速发展的电子商务进行结合,在交易信息的加解密模型中通过构建Meneses-Vanstone密码体制来对数据进行加解密操作。基于改进的椭圆曲线Meneses-Vanstone(MV)密码体制构造数据加解密模型。

数据加密模型如图4所示。

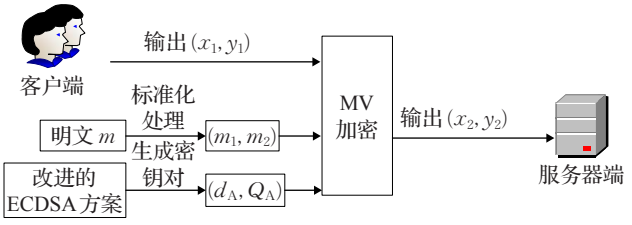

图4　电子数据加密模型

在电子商务交易过程中主要是客户端与服务器端的互动,客户端即加密的一方,为电子商务中数据信息的发送方。

(1)客户端将待发送传输的数据信息格式化处理生成消息串 (m_1,m_2) 。

(2)用数据信息的接收方服务器端的公钥 Q_B 和客户端的私钥 d_A 按照MV密码体制对 (m_1,m_2) 进行加密形成密文 (x_2,y_2) 。

(3)客户端将自己的公钥 Q_A 和加密信息 $\left(Q_A,(x_2,y_2)\right)$ 一起发送给接收方服务器端。

MV加密过程如下:

(1)获得服务器端的公钥Q_B，计算$(x_1,y_1)=d_AQ_B$，如果$x_1,y_1=0$，则客户端重新选择私钥d_A，同时生成新的公钥。

(2)计算$x_2=m_1x_1 \bmod p,\ y_2=m_2y_1 \bmod p$。

MV解密过程如下：

(1)获得客户端的公钥Q_A，计算$(x_1,y_1)=d_BQ_A$。

(2)计算$m_1=x_2x_1^{-1} \bmod p, m_2=y_2y_1^{-1} \bmod p$。

数据解密模型如图5所示。

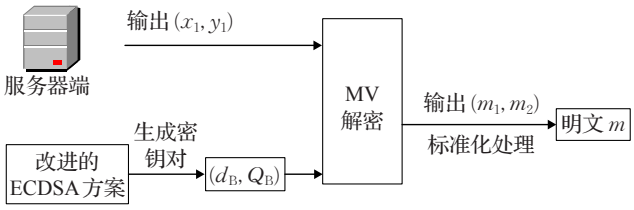

图5　电子数据解密模型

服务器端即解密方，为电子商务交易中数据信息的接收方。服务器端接收到客户端发送过来的加密信息(x_2,y_2)，首先使用客户端的公钥Q_A和服务器端的私钥d_B对加密信息按照MV密码体制进行解密生成(m_1,m_2)，然后再将其逆向转换为客户端明文消息。

MV加密体制并没有限制消息明文必须嵌入椭圆曲线上，这种体制的优点是不需要将待加密的数据进行数据类型转换操作，从而降低了成本，同时提高了数据加解密效率。无模逆的椭圆曲线数字签名算法，使运算负担减少，从而加快数字签名和验证签名的速度，进而使电子商务交易过程安全高效。

6　结束语

本文在对经典的椭圆曲线数字签名进行分析的基础上，指出其存在的局限性，由此进行了方案的改进。改进的方案引入了双参数，进行标量乘运算2次，在签名和验证过程中均没有使用模逆运算，理论分析证明了本文方案的安全性，仿真实验证明了改进方案提高了数字签名的计算效率。最后将改进的方案应用到电子商务中，构建了电子商务交易过程中电子数据的加解密模型。

参考文献：

[1] Hankerson D，Menezes A，Vanstone S.椭圆曲线密码学导论[M].张焕国，译.北京：电子工业出版社，2005.

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

[3] Menezes A，Orschot P，Vanstone S.Handbook of applied cryptography[M].London：CRC Press，1996：454-459.

[4] Seo J H.Efficient digital signatures from RSA without random oracles[J].Information Sciences，2019.

[5] 丛林虎，方轶.数字签名技术在导弹数据数字化登记中的应用[J].兵器装备工程学报，2020，41(1)：153-156.

[6] Koblitz N.Elliptic curve cryptosystems[J].Mathematics of Computation，1987，48：203-209.

[7] Miller V.Uses of elliptic curves in cryptography[C]//Advances in Cryptology(Crypto'85)，1985：387-398.

[8] Gura N，Patel A，Wander A，et al.Comparing elliptic curve cryptography and RSA on 8-bit CPUs[C]//Cryptographic Hardware and Embedded Systems(CHES 2004).Berlin，Heidelberg：Springer，2004：119-132.

[9] Lenstra A K，Verheul E R.Selecting cryptographic key sizes[J].Journal of Cryptology，2001，14(4)：255-293.

[10] Potlapally N R，Ravi S，Raghunathan A，et al.A study of the energy consumption characteristics of cryptographic algorithms and security protocols[J].IEEE Trans on Mobile Comput，2006，5(2)：128-143.

[11] 杨晓元，魏立线.计算机密码学[M].西安：西安交通大学出版社，2015.

[12] 丁黎明.基于椭圆曲线数字签名算法的软件注册码智能绘制方法[J].自动化与仪器仪表，2019(6)：95-98.

[13] 陈亚茹，丛培强，陈庄.一种椭圆曲线数字签名的改进方案[J].信息安全研究，2019，5(3)：217-222.

[14] Guajardji J，Paar C.Efficient algorithms for elliptic curve cryptosystems[C]//Proc of Eurocrypt'97.Berlin：Spring，1997：342-356.

[15] 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.

[16] 陈亮，游林.椭圆曲线数字签名算法优化与设计[J].电子器件，2017，34(1)：89-93.

[17] 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)，2018，7(4)：32-33.

[18] 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.

[19] 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)，2018，34(2)：1-3.

[20] 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，2008，29(17)：4425-4427.

[21] 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，2018，25(3)：44-47.

[22] Bellare M，Canetti R，Krawczyk H.A modular approach to the design and analysis of authentication and key exchange protocols[C]//Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing，1998：419-428.