ECMLR 数字签密方案的改进①

李田清 [1] 刘建辉 [2] (1.辽宁工程技术大学 研究生院 辽宁 葫芦岛 125105;
2.辽宁工程技术大学 电子与信息工程学院 辽宁 葫芦岛 125105)

摘 要: ECMLR 签密方案是指基于椭圆曲线的具有消息链接恢复的签密方案，该方案采用递推的方式构造消息分块的签名，把前一个参数作为后一个参数的输入，这样恢复消息时只需要进行递推的运算就可以一个一个地恢复全部消息了，从而大大地减少了通信运输量。但是通过分析可以发现，该方案的安全性必须建立在消息密钥的互异上，通过研究，对其进行了改进，并给出了证明。

关键词: 数字签名；数字签密；消息链接恢复；ECMLR

Improvement of ECMLR Digital Signcryption Scheme

LI Tian-Qing [1], LIU Jian-Hui[2]
(1.Institute of Graduate, Liaoning Technical University, Huludao 125105, China;
2.School of Electronic and Information Engineering, Liaoning Technical University, Huludao 125105, China)

Abstract: ECMLR is a sincryption scheme with message recovery and message linkage recovery based on the elliptic curve crypto system. The message's block is constructed in recursive mode, taking the present parameter as the input of the next parameter. By doing this, the whole message can be recovered recursively one by one. And the communicate traffic is reduced significantly. But in the research, it is found that this scheme's security is based on the different message key. So an improvement is given with proof.

Keywords: digital signature; digital singcryption; message linkage recovery; ECMLR

数字签名是电子商务安全的一个重要的分支，是实现电子交易安全的核心技术之一。它在实现身份认证，数据完整性，不可否认等功能方面都有重要的应用，尤其在大型网络安全通信中的密钥分配,公文安全传输以及电子商务和电子政务等领域有重要的应用价值。

数字签名的过程可以用图 1[1]简要的概括,数字签名的实现基础是加密技术，一般使用公钥加密算法与散列函数。常用的数字签名算法有 RSA，DSS， ECDSA，ElGamal，Schnorr 等; 还有一些用于特殊用途的数字签名，如盲签名，群签名，代理签名，环签名等[2]，而签密方案是在签名的基础上增加了保密性。

ECMLR 签密方案,是指基于椭圆曲线的具有消息链接恢复的签密方案[3]。基于椭圆曲线的签名方案见文献[4,5]，消息恢复的签名方案参见文献[6,7]。

ECMLR 采用递推的方式构造消息分块的签名，把前一个参数作为后一个参数的输入，这样恢复消息时只需要进行递推的运算就可以一个一个地恢复全部消息了，从而大大地减少了通信传输量。

本文首先介绍数字签名的基础,然后给出 ECMLR 签密方案及安全性分析，最后给出改进方案和证明。

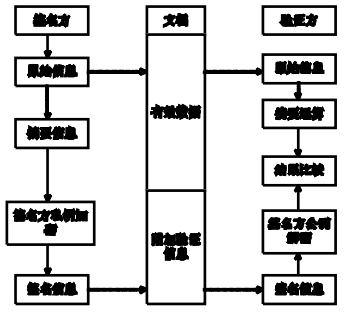

图 1 数字签名过程

① 收稿时间:2009-06-08

1　基本原理

1.1 定义 1　群

设一个非空集合G，在G上定义了一个二元运算“$\bullet$”符,满足如下条件：

(1) 封闭性：对于任意$a,b\in G$，有$a\bullet b\in G$。

(2) 结合律：对任何的$a,b\in G$，有$a\bullet b\bullet c=(a\bullet b)\bullet c=a\bullet(b\bullet c)$。

(3) 单位元：存在一个元素$1\in G$，称为单位元，对任意元素，有$a\bullet 1=1\bullet a=a$。

(4) 逆元：对任意$a\in G$，存在一个元素$a^{-1}\in G$，称为逆元，使得$a\bullet a^{-1}=a^{-1}\bullet a=1$。

把满足上述条件的集合G称为群，记为$\{G,\bullet\}$。

(5) 交换律：对任意$a,b\in G$，有$a\bullet b=b\bullet a$。

如果一个群满足交换律,则称其为交换群(或 Abel 群)。如果一个群的元素是有限的,则称该群为有限群，否则称为无限群。

(6) 循环群：

如果群中每一个元素都是某一个元素$a\in G$的幂$a^k\in G$（k为整数)，则称该群是循环群。

1.2 有限域 GF(p)

定义 1．域

域由一个非空集合F组成,在集合F中定义了两个二元运算符：“+”(加法)和“$\bullet$”(乘法),并满足：

(1) F 关于加法“+”是一个交换群,其单位元“0”，a的逆元为$-a$；

(2) 关于乘法“$\bullet$”是一个交换群，其单位元为“1”，a的逆元为a^{-1}；

(3) (分配律)对任何$a,b,c\in F$，有$a\bullet(b+c)=(b+c)\bullet a=a\bullet b+a\bullet c$；

(4) (无零因子)对任何$a,b\in F$，如果有$a\bullet b=0$，则$a=0$或$b=0$。这样的一个集合F称为域，记为$\{F,+,\bullet\}$。

如果F中包含有限个元素，则称其为有限域。有限域中元素的个数称为有限域的阶。

定理 1．每个有限域的阶必须为素数的幂。

定理 2．对任意素数P与正整数n，存在p^n阶域，记为$GF(p^n)$。当$n=1$时，有限域$GF(p)$也称为素数域。

2　ECMLR签密方案

2.1 方案描述

2.1.1 初始化过程

(1) 选取定义在有限域$GF(p)$上的一条安全的椭圆曲线E，使得E上的有理点群的阶被一个大素数n整除，保证有理点群上的离散对数问题是难解的。

(2) 选取一个基点$G=(x_G,y_G)\in E$，G的阶为n，即有$nG=O$，O表示一个无穷点，基点G公开。

(3) 设 A 和 B 为系统的两个用户，A 的私钥为$k_A\in Z_n^*$，$P_A=k_AG\in E$，P_A作为 A 的公钥。同样地 B 选择$k_B\in Z_n^*$，$P_B=k_BG\in E$，P_B作为 B 的公钥。它们的公钥P_A和P_B在系统内公开，并记$P_A=(x_A,y_A),P_B=(x_B,y_B)$。

2.1.2 签名过程

签名者 A 利用上面的域参数及信息接收者 B 的公钥对消息$m=\{m_1,m_2,...,m_t\}$进行签名，其中$m_i\in Z_n^*$，步骤如下：

(1) 选取随机数或伪随机数$k\in Z_n^*$，令$r_0=0$；

(2) 计算$R=kP_B=(x,y),r_B=x\bmod n$，若$r_B=0$，则返回到第(1)步；

(3) 计算$r_i=m_ih(r_{i-1}\oplus r_B)^{-1}\bmod n$，$i=1,2,...,t,r=h(r_1\|r_x\|...\|r_t)$；

(4) 计算$s=k+rk_A\bmod n$，如果$s=0$，则返回到第一步；

(5) A 对消息 m 的签名是$(r,s,r_1,r_2,...,r_t)$。

2.1.3 消息恢复及验证过程

B 收到 A 的签名$(r,s,r_1,r_2,...,r_t)$后,首先获取系统的域参数和 A 的公钥,然后做以下的操作进行验证：

(1) 验证$r,s,r_1,r_2,...,r_t$是$[1,n-1]$中的整数；

(2) 计算$r'=h(r_1\|r_2\|...\|r_t),r'\neq r$，则签名不成立；

(3) 计算$X=sG-rP_A=(x',y')$，$r_B'=k_Bx'\bmod n$，$m_i=r_ih(r_{i-1}\oplus r_B')\bmod n$，即恢复原消息串$m=\{m_1,m_2,...,m_t\}$。若$x'=0$，则拒绝这个签名。否则，通过计算出的消息串的冗余位进行身份认证，若正确，接受签名，否则拒绝接受。

2.2 安全性分析

(1) 攻击者从用户的公钥P_A获取其私钥k_A是不可能的，因为他面临求解椭圆曲线离散对数难题。同样从签名过程$s=k+rk_A\bmod n$中获取私钥也是不可能的。因为在签名方程中含有另一个未知数k。

(2) 攻击者截取签名$(r,s,r_1,r_2,...,r_t)$后，因不知道接收者的私钥k_B，虽然可以计算$X=sG-rP_A=(x',y')$，但是无法计算$r_B'=k_Bx'\bmod n$，从而不能计算$m_i=r_ih(r_{i-1}\oplus r_B')\bmod n$，因此也无

法恢复消息。

(3) 若攻击者获取了明文， $m=\{m_1,m_2,...,m_t\}$ 的签名，因为 $h(r_{i-1}\oplus r_B)^{-1}=m_i r_i^{-1} \bmod n$，Hash 函数 $h(\bullet)$ 是一个安全的函数,使用160位的Hash值，保证了已知明文的攻击是困难的，也就是说不可能从中求得 $r_B^{'}$。

(4) 消息密钥 k 不能重复使用，即不同的消息签名应使用不同的消息密钥,否则,私钥 k_A 将可能恢复。例如，对不同的消息 m_1,m_2，若使用相同的消息密钥 k，产生两个消息签名 $(r_1,s_2,r_{11},r_{12},...,r_{1t}),(r_2,s_2,r_{21},r_{22},...,r_{2t})$ 此时： $s_1=k+r_1k_A \bmod n, s_2=k+r_2k_A \bmod n$， $s_1-s_2=(r_1-r_2)k_A \bmod n$ 如果 $r_1\neq r_2$，则有 $k_A=(r_1-r_2)^{-1}(s_1-s_2)\bmod n$，从而攻击者可以恢复 k_A。

3 ECMLR的改进

由于并不应该把签名的安全性建立在消息密钥的互异性上，每次签名的时候不用和上一次的消息密钥进行比较，每次签名都应该是独立的，本次签名的安全性建立在以前签名的基础上是不可取的，基于此，对原来的方案作了如下的改进。

3.1 改进方案简单描述

3.1.1 签名过程

(1) 选取随机数或伪随机数 $k\in Z_n^*$，令 $r_0=0$;

(2) 计算 $R=kP_B=(x,y),r_B=x \bmod n$，若 $r_B=0$，则返回到第(1)步;

(3) 计算 $r_i=m_i h(r_{i-1}\oplus r_B)^{-1} \bmod n$， $i=1,2,...,t, r=h(r_1\|r_2\|...\|r_t)$;

(4) 计算 $s=k_A k+r \bmod n$，如果 $s=0$，则返回到第一步;

A 对消息 m 的签名是 $(r,s,r_1,r_2,...,r_t)$。

4 ECMLR改进方案的证明

4.1 签名方案的验证

$rk=1+k_A s \bmod n$，

$R=kP_B=k_B kG=k_B(r^{-1}G-r^{-1}sP_A)$

$=k_B(x^{'},y^{'})$

所以 $r_B=k_B x \bmod n$，从而 $m_i=r_i h(r_{i-1}\oplus r_B^{'}) \bmod n$。

4.1.2 改进方案安全性证明

(1) 攻击者从用户的公钥 P_A 获取其私钥 k_A 是不可能的，因为他面临求解椭圆曲线离散对数难题。同样从签名过程 $rk=1+k_A s \bmod n$ 中获取私钥也是不可能的。因为在签名方程中含有另一个未知数。

(2) 攻击者截取签名 $(r,s,r_1,r_2,...,r_t)$ 后，因不知道接收者的私钥 k_B，虽然可以计算 $X=r^{-1}(G-sP_A)=(x^{'},y^{'})$，但是无法计算 $r_B^{'}=k_B x^{'} \bmod n$，从而不能计算 $m_i=r_i h(r_{i-1}\oplus r_B^{'}) \bmod n$，因此也无法恢复消息。

(3) 若攻击者获取了明文， $m=\{m_1,m_2,...,m_t\}$ 的签名 $(r,s,r_1,r_2,...,r_t)$，因为 $h(r_{i-1}\oplus r_B)^{-1}=m_i r_i^{-1} \bmod n$，Hash 函数 $h(\bullet)$ 是一个安全的函数,使用 160 位的 Hash 值,保证了已知明文的攻击是困难的,也就是说不可能从中求得 $r_B^{'}$.

5 结语

随着经济全球化的进一步深化,电子商务将成为主要的经济活动载体,其安全性至关重要.而电子商务的核心是数字签名.数字签名的核心是密码,其安全性字节关系到经济活动的安全与稳定.下一步准备进一步研究数字签名的安全性.

参考文献

1 赵泽茂.数字签名理论.北京:科学出版社, 2007.4－6.

2 蔡勉,卫宏儒.信息系统安全理论与技术.北京:北京工业大学出版社, 2006.145－145.

3 赵泽茂,徐慧,刘凤玉.具有消息链接恢复的椭圆曲线认证加密方案.南京理工大学学报, 2005,29(1):81－83.

4 张方国,王常杰,王育民.基于椭圆曲线的数字签名与盲签名.通信学报, 2001,22(8):22－28.

5 Johnson D, Menezes A. The elliptic curve digital signature algorithm. Waterloo: Technical Report, Department of Combination and Optimization, University of Waterloo, 1999.

6 李子臣,李中献.具有消息恢复签名方案的伪造攻击.通信学报, 2000,21(5):84－87.

7 李子臣,杨义先.具有消息恢复的数字签名方案.电子学报, 2000,28(1):125－126.