基于超椭圆曲线的有序和广播多重盲签名

杨 青[1],辛小龙[2]
YANG Qing[1], XIN Xiaolong[2]

1.西安航空学院 基础部,西安 710077
2.西北大学 数学系,西安 710069
1.Department of Basic Courses, Xi'an Aeronautical University, Xi'an 710077, China
2.Department of Mathematics, Northwest University, Xi'an 710069, China

YANG Qing, XIN Xiaolong. Sequential and broadcasting blind multisignature scheme based on hyperelliptic curves. Computer Engineering and Applications, 2015, 51(2):99-102.

Abstract: As to the characteristics of multisignature and blind signature, this paper presents a new sequential blind multisignature scheme based on hyperelliptic curves, and its validity is proved. The signature structure is expanded, and some signature nodes are changed to broadcasting signature structure. A new broadcasting blind multisignature scheme is presented, and its correctness is proved. The safety and efficiency of the two schemes are analyzed.
Key words: hyperelliptic curve; reduced divisors; broadcasting; blind signature; multisignature

摘 要: 针对多重签名和盲签名的特点,提出新的基于超椭圆曲线的有序多重盲签名算法,并验证其有效性。扩展了签名结构,将某些签名节点拓展为广播签名结构,提出了广播多重盲签名算法并证明其正确性。对两种方案的安全性和高效性进行了分析。
关键词: 超椭圆曲线; 约化除子; 广播; 盲签名; 多重签名
文献标志码: A **中图分类号:** TP309 doi:10.3778/j.issn.1002-8331.1304-0044

随着网络应用的不断普及,数字签名技术也在不断发展。在一些特定的应用场合,签名者只是完成对文件的签名工作并不了解所签信息的内容,这就是盲签名,其广泛应用于电子投票系统和银行电子现金系统等。盲签名是一类特殊的签名,它具备盲性和不可追踪性,1983年chaum首次提出盲签名概念并给出了一个基于RSA的盲签名方案[1]。

多重签名是数字签名的一种,用于多人对同一电子消息进行签名。根据签名过程不同,多重签名分为有序多重签名和广播多重签名,前者要求所有的签名者按照串行的顺序进行签名,后者则对签名顺序没有要求。Harn L,Kiesler T.在1989年改进了基于RSA的数字签名方案,提出多重签名方案[2]。陆浪如等提出的基于离散对数的多重签名方案能够成功地避免多个签名者之间相互合作否认消息签名[3]。Harn等提出的基于ELGamal密码体系的结构化多重签名算法在签名长度和验证时间上具有高效性[4]。傅鹤岗等引入一个可信签名中心,提出了基于椭圆曲线的结构化多重数字签名算法[5]。陈逢林等提出的顺序多重盲签名[6],满足有序性和盲签名的特点。结构化多重签名是指签名团体按照某种特定的签名结构进行签名,签名结构可以是有序的,广播的,也可以是两者相结合的。

目前,盲签名和多重签名的实现有很多种方案,它们基本上是基于有限域上离散对数或是椭圆曲线上离散对数的困难性,在相同的安全强度下,RSA对应的基域为1 024 bit,椭圆曲线为160 bit而对于亏格为 $g=2$ 或3的超椭圆曲线来说各需要80 bit或54 bit的基域即可。密钥长度更短,所用基域更小,具有存储效率、计算

基金项目: 陕西省教育厅科研计划(No.11JK1070);西安航空学院基金项目(No.11XQ620,No.13XP19);陕西省科技厅计划项目(No.2013JM1019)。
作者简介: 杨青(1982—),女,讲师,主要从事密码学方面的研究;辛小龙(1955—),男,教授,博士生导师,主要从事信息与代数编码的研究。E-mail:45347981yq@163.com
收稿日期: 2013-04-03 **修回日期:** 2013-07-29 **文章编号:** 1002-8331(2015)02-0099-04
CNKI网络优先出版:2013-08-28, http://www.cnki.net/kcms/detail/11.2127.TP.20130828.1540.005.html

效率和通信宽带等方面的优势。本文参考文献[4-6],将盲签名和多重签名结合,并推广到超椭圆曲线密码系统上,提出了基于超椭圆曲线的有序多重盲签名算法和广播多重盲签名算法。

1 超椭圆曲线密码体制

定义1 设 F_q 是一个有限域,$\bar{F}_q$ 是它的代数闭包,定义在 F_q 上的亏格为 $g(g<4)$ 的超椭圆曲线(HC)可由方程:$y^2+h(x)y=f(x)$ 给出,其中 $f(x)\in F_q[x]$ 是次数为 $2g+1$ 的首一多项式,$h(x)\in F_q[x]$ 是次数至多为 g 的多项式,并且在HC上不存在点 $(x,y)\in\bar{F}_q\times\bar{F}_q$ 同时满足方程,及两个偏微分方程 $2y+h(x)=0$ 和 $h'(x)y-f'(x)=0$。HC上有唯一的一个无穷远点 ∞。特别地,当 $g=1$ 时,HC即为椭圆曲线。点 $p(x,y)$ 的反点为 $\bar{p}(x,-y-h(x))$,∞ 的反点为 ∞。限于篇幅,Mouford给出半约化除子的一个表示,可参考文献[7]。有关超椭圆曲线的Jacobian群和除子的概念,可参考文献[8]。Jacobian群上的运算主要是群加和倍除子,加法由Cantor算法给出,可参考文献[9],通过Cantor算法,可计算 m 个 D 的和 $D'=mD$,$m\in Z_n^*$。

2 基于超椭圆曲线的有序多重盲签名

2.1 系统参数设定

设 C 是有限域 F_q 上亏格为 $g(<4)$ 的超椭圆曲线,它的Jacobian群的阶为 $\#J(C;F_q)=hn$,n 是160 bit的大素数(或更大),h 是较小的余因子或等于1。D 为Jacobian群的一个基元,是阶为 n 的一个约化除子,即 $nD=div(1,0),div(1,0)$ 是群加法单位元。$D=div(a,b)$,$a(x)=\sum_{i=0}^{g}a_ix^i$,$b(x)=\sum_{i=0}^{g-1}b_ix^i$。构造一个映射函数 $\varphi:J(C;F_q)\to Z_{q^{2g}}$,$\varphi$ 是从超椭圆曲线的Jacobian群中的元素到有限整数集 $Z_{q^{2g}}=\{0,1,\cdots,q^{2g}-1\}$ 的单射函数,$\varphi(D)=a_{g-1}q^{2g-1}+\cdots+a_1q^{g+1}+a_0q^g+b_{g-1}q^{g-1}+\cdots+b_1q+b_0$ 构造这样的函数 φ 很多,如文献[10-11]。t 为签名者人数,假设有序多重盲签名算法签名者为:$A_1,A_2,\cdots,A_i,\cdots,A_t$,签名顺序为 $(A_1,A_2,\cdots,A_i,\cdots,A_t)$,密钥按照签名顺序的倒序生成,由后往前,从 A_t 开始,A_t 的私钥为 $x_t\in Z_n^*$,公钥为 $Y_t=x_tY_{t+1}$,$Y_{t+1}=D$,则消息签名者 A_i 的私钥为 $x_i\in Z_n^*$,$1\leqslant i\leqslant t$,公钥为 $Y_i=x_iY_{i+1}$。系统公开参数有超椭圆曲线 $C(F_q)$,φ,n,D,Y_i。

2.2 盲签名过程

盲签名过程可通过消息发送者 I,签名收集者 C 和 t 个有序消息签名者实现,步骤如下:

(1) A_i 随机选取 $k_i\in Z_n^*$,计算 $R_i=k_iY_{i+1}$,并发送给签名收集者 C。

(2) C 计算 $R=\sum_{i=1}^{t}R_i$,分别发送给 I 和 A_i 并广播签名顺序给每个参与者。

(3) I 任选 $\alpha,\beta\in Z_n^*$,计算 $T=\alpha R+\beta D$,对消息 m 盲化,计算 $m'=\alpha^{-1}\varphi(T)^{-1}\varphi(R)m \bmod n$ 和 $e=m'Y_1$,并发送 e 给消息签名者 A_i,发送 m' 给 A_1。

2.3 有序多重盲签名过程

t 个签名者 $A_1,A_2,\cdots,A_i,\cdots,A_t$,签名顺序为 $(A_1,A_2,\cdots,A_i,\cdots,A_t)$,则签名过程如下:

(1) A_i 计算 $s_i=x_is_{i-1}-k_i\varphi(R)\bmod n$,$Q_i=Q_{i-1}+R_i$,其中 $s_0=m'$,$Q_0=0$,$Q_t=R$,$1\leqslant i\leqslant t$。并传递数组 (s_t,Q_t) 给 A_{i+1},直到最后一个签名者 A_t。

(2) A_{i+1} 收到 A_i 的签名后,验证方程 $e=s_iY_{i+1}+Q_i\varphi(R)$ 是否成立,若成立,则按照上一步的方法继续签名;否则要求 A_i 重签或终止签名。

(3)每个 A_i 签名结束后,将最后一个签名者 A_t 的签名 (s_t,Q_t) 作为 m' 的有序多重盲签名发送给签名收集者 C。C 验证等式 $e=s_tD+Q_t\varphi(R)$ 成立,则盲签名有效,否则无效。若有效,则传递 s_t 给消息发送者 I 进行脱盲变换。

2.4 有序多重盲签名的脱盲和验证过程

消息发送者 I 接收到签名收集者 C 发来的签名后,对其进行脱盲变换,计算 $s=(m')^{-1}ms_t-\beta\varphi(T)$,验证方程:$mY_1=sD+T\varphi(T)$,若成立,则 I 发布消息 m 的签名 s。

2.5 算法正确性证明

定理1 若等式 $e=s_iY_{i+1}+Q_i\varphi(R)$ 成立,则 $A_1,A_2,\cdots,A_i$ 对盲消息 m' 签名有效。

证明 $\because s_i=x_is_{i-1}-k_i\varphi(R)\bmod n$

$x_is_{i-1}=s_i+k_i\varphi(R)\bmod n$

$\therefore x_is_{i-1}Y_{i+1}=s_iY_{i+1}+k_i\varphi(R)Y_{i+1}=s_iY_{i+1}+\varphi(R)R_i$

$\therefore s_{i-1}Y_i=s_iY_{i+1}+\varphi(R)R_i$,当 $i=1,2,\cdots$ 时有:

$$\begin{cases}s_0Y_1=s_1Y_2+\varphi(R)R_1\\ s_1Y_2=s_2Y_3+R_2\varphi(R)\\ \vdots\\ s_{i-1}Y_i=s_iY_{i+1}+R_i\varphi(R)\end{cases}$$

将左右两边相加得:

$s_0Y_1=s_iY_{i+1}+Q_i\varphi(R)$

$\because s_0=m'\therefore e=m'Y_1=s_iY_{i+1}+Q_i\varphi(R)$

定理2 若等式 $e=s_tD+Q_t\varphi(R)$ 成立,则 $A_1,A_2,\cdots,A_t$ 对盲消息 m' 的有序多重盲签名有效。

证明 在定理1中,已证 $A_1,A_2,\cdots,A_i$ 盲签名有效,可将 i 换成 t,且 $Y_{t+1}=D$,可证定理2。

定理3 若等式 $mY_1=sD+T\varphi(T)$ 成立,则原始消息 m 的有序多重盲签名有效。

证明 $\because s_i = x_i s_{i-1} - k_i \varphi(R) \bmod n$

$\therefore s_t = m' \prod_{i=1}^{t} x_i - (\sum_{i=1}^{t} k_i \prod_{j=i+1}^{t} x_j)\varphi(R) \bmod n$

$s = (m')^{-1} m s_t - \beta\varphi(T) = m\prod_{i=1}^{t} x_i -$

$(m')^{-1} m\varphi(R)\sum_{i=1}^{t} k_i \prod_{j=i+1}^{t} x_j - \beta\varphi(T) =$

$m\prod_{i=1}^{t} x_i - \varphi(T)(\alpha\sum_{i=1}^{t} k_i \prod_{j=i+1}^{t} x_j + \beta)$

$\therefore sD = m\prod_{i=1}^{t} x_i D - \varphi(T)(\alpha\sum_{i=1}^{t} k_i \prod_{j=i+1}^{t} x_j + \beta)D =$

$mY_1 - T\varphi(T)$

$\therefore mY_1 = T\varphi(T) + sD$

3　基于超椭圆曲线的广播多重盲签名

该算法有 $t-1+p$ 个签名者, $A_1, A_2, \cdots, A_{i-1}, A_{i+1}, \cdots, A_t, A_{i,1}, \cdots, A_{i,p}$。假设签名顺序为 $<A_1, A_2, \cdots, A_i, \cdots, A_t>$ 其中 A_i 是由 $A_{i,1}, A_{i,2}, \cdots, A_{i,p}$ 组成的虚拟签名节点,可称为虚拟签名者。$A_{i,1}, A_{i,2}, \cdots, A_{i,p}$ 为广播签名结构,并称 $A_{i,j}$ 为广播签名组成员。其余为有序签名结构。$A_1, A_2, \cdots, A_{i-1}$ 按前面的方法签名及验证,当签名到 A_i 时, $A_{i,j}$ 首先对 $A_1, A_2, \cdots, A_{i-1}$ 的有序签名进行验证,验证正确则进行自己的签名,否则重签或拒绝签名。只要 $A_{i,j}$ 中任何一个宣布签名无效,则拒绝签名。设 $A_{i,j}$ 的私钥为 $x_{i,j}$, 满足 $x_{i,j} \in Z_n^*$, 公钥为 $Y_{i,j} = x_{i,j} Y_{i+1}$, 其中 $j = 1, 2, \cdots, p$ 且 $Y_{t+1} = D$。A_i 的公钥为 $Y_i = Y_{i,1} + Y_{i,2} + \cdots + Y_{i,p}$。

3.1　广播多重盲签名过程

$A_{i,j}$ 签名过程如下:

(1) $A_{i,j}$ 随机选取 $k_{i,j} \in Z_n^*$, 计算 $R_{i,j} = k_{i,j} Y_{i,j}$ 并发送 R_{ij} 给签名收集者 C。

(2)签名收集者 C 收到所有 R_{ij} 后,计算 $R_i = R_{i,1} + R_{i,2} + \cdots + R_{i,p}$, 设 $k_i = \sum_{j=1}^{p} k_{i,j}$, 则 $R_i = k_i Y_{i+1}$, C 按2.2节中步骤(2)计算得到 R, 并发送给所有签名者和 I。

(3) $A_{i,j}$ 收到 R 后,计算 $s_{i,j} = x_{i,j} s_{i-1} - k_{i,j}\varphi(R) \bmod n$, 其中 $s_0 = m'$, $Q_{i,j} = Q_{i-1} + R_{i,j}$ 并将签名 $(s_{i,j}, Q_{i,j})$ 发送给签名收集者 C。

(4)签名收集者 C 收到签名 $(s_{i,j}, Q_{i,j})$ 后,验证等式 $\varphi(R)R_{i,j} = s_{i-1}Y_{i,j} - s_{i,j}Y_{i+1}$ 是否成立。若成立,则计算 $s_i = s_{i,1} + s_{i,2} + \cdots + s_{i,p} \bmod n$, $Q_i = Q_{i-1} + \sum_{j=1}^{p} R_{i,j}$ 并将 (s_i, Q_i) 作为虚拟签名节点 A_i 的签名发送给 A_{i+1};否则返回要求重签或终止签名。

(5)后续签名者 $A_{i+1}, A_{i+2}, \cdots, A_t$ 按照2.3节介绍的方法进行签名及验证。

(6)将最后一个签名者 A_t 的签名 (s_t, Q_t) 作为 m' 的广播多重盲签名,发送给签名收集者 C。C 的验证签名方程同2.3节步骤(3)。若有效,则传递 s_t 给消息发送者 I 进行脱盲变换。

3.2　广播多重盲签名的脱盲和验证过程

同2.4节。

3.3　算法正确性证明

定理4　若 $\varphi(R)R_{i,j} = s_{i-1}Y_{i,j} - s_{i,j}Y_{i+1}$ 成立,则 $A_{i,1}, A_{i,2}, \cdots, A_{i,p}$ 的广播签名有效。

证明 $\because s_{i,j} = x_{i,j} s_{i-1} - k_{i,j}\varphi(R) \bmod n$

$\therefore s_{i,j}Y_{i+1} = x_{i,j} s_{i-1} Y_{i+1} - k_{i,j}\varphi(R)Y_{i+1}$

$\therefore s_{i,j}Y_{i+1} = s_{i-1}Y_{i,j} - \varphi(R)R_{i,j}$

$\therefore \varphi(R)R_{i,j} = s_{i-1}Y_{i,j} - s_{i,j}Y_{i+1}$

另外,在广播多重盲签名方案中虚拟签名者 A_i 的满足条件与其他签名者相同。因为

$$\begin{cases} s_{i,1} = x_{i,1} s_{i-1} - k_{i,1}\varphi(R) \\ s_{i,2} = x_{i,2} s_{i-1} - k_{i,2}\varphi(R) \\ \quad\vdots \\ s_{i,p} = x_{i,p} s_{i-1} - k_{i,p}\varphi(R) \end{cases}$$

左右两边相加得:

$\sum_{j=1}^{p} s_{i,j} = s_{i-1}\sum_{j=1}^{p} x_{i,j} - \varphi(R)\sum_{j=1}^{p} k_{i,p}$

$\therefore s_i = s_{i-1}x_i - \varphi(R)k_i$

$\therefore s_{i-1}Y_i = s_i Y_{i+1} + \varphi(R)R_i$

因此由定理1可知,定理4是正确的。

4　方案分析

4.1　效率分析

用表格形式对比和分析本文的有序多重盲签名方案与文献[6]方案的效率(假设两种方案的公钥相同),两者计算所需时间,如表1所示。

表1　本文中有序多重盲签名方案与文献[6]方案的效率比较

签名过程	文献[6]方案	本文方案	本文节省计算时间
A_i 签名	$(t-1)T_A + tT_{MOD}$	$(t-1)T_A + tT_{MOD}$	相同
A_{i+1} 验证 A_i 的签名	$3(t-1)T_M + t(t-1)/2T_A$	$2(t-1)T_M + (t-1)T_A$	$(t-1)T_M + (t-1)(t-2)/2T_A$
C 验证签名	$3T_M + tT_A$	$2T_M + T_A$	$T_M + (t-1)T_A$
脱盲和验证	$3T_M + tT_A + T_{INV} + T_{MOD}$	$3T_M + T_A + T_{INV} + T_{MOD}$	$(t-1)T_A$

表1中符号说明：T_A 表示计算一次除子加运算所需时间，T_M 表示计算一次除子标量乘运算所需时间，T_{MOD} 表示计算一次取模运算所需时间，T_{INV} 表示计算一次取逆运算所需时间，t 表示签名者人数。

在盲签名过程中，本文方案比文献[6]多一个 T_M，其余运算量相同。因此，在整个有序多重盲签名过程中，本文方案在计算量上比文献[6]节省 $(t-1)T_M+(t-1)\times(t+2)/2T_A$。Lange[12]给出亏格为2的超椭圆曲线除子加法和倍点运算的高效计算公式，除子加法运算的运算量为1I+3S+22M，除子倍点运算的运算量为1I+5S+22M，其中I，S和M分别表示有限域上的求逆运算，平方运算和乘法运算。超椭圆曲线的各种除子运算的运算量可参考文献[13]，国际上约定的1I=30M，1S=0.8M[14]。以2倍点为例，本文方案在计算量上比文献[6]节省 $(t-1)\times T_M+(t-1)(t+2)/2T_A=(t-1)(1I+5S+22M)+(t-1)(t+2)\times(1I+3S+22M)/2=(27.2t^2+83.2t-110.4)M(t>1$时，单增)，所以本文的有序多重盲签名方案具有明显的高效性。

4.2 安全性分析

（1）方案满足盲性。每个签名者 A_i 都是对盲化后的消息 m' 进行签名，要求解 m 必须求解基于超椭圆曲线的离散对数问题，在计算上是不可行的，因此这两种方案都满足盲性。

（2）方案具有不可伪造性。有序多重盲签名中的 $s_i=x_is_{i-1}-k_i\varphi(R)\bmod n$，$R_i=k_iY_{i+1}$，若攻击者试图伪造签名者 A_i 的签名必须计算出私钥 x_i 和随机数 k_i，这又要求解超椭圆曲线离散对数问题。同理，广播多重盲签名算法也要求解此问题。所以，两方案具有不可伪造性。

（3）方案满足结构性。方案能够防止广播签名组成员内部串通，擅自改变签名顺序。由于签名收集者对收到的签名 $(s_{i,j},Q_{i,j})$ 分别进行验证，从而保证签名的结构性。

5 结论

本文提出一种新的基于超椭圆曲线的有序和广播多重盲签名方案，并证明该方案是正确的、安全的和高效的。广播多重盲签名算法适用于有多个虚拟签名者的结构。本文提出的两种方案在电子商务，电子选举等方面有广阔的应用前景和实用价值。

参考文献：

[1] Chaum D.Blind signatures system[C]//Proc of CRYPTO'83. New York,USA:Plenum Press,1983.

[2] Harn L,Kiesler T.New schem for digital multisignatures[J]. Electronics Letters,1989,25(15):1002-1003.

[3] 陆浪如，曾俊杰，匡友华，等.一种新的基于离散对数多重签名方案及其分布式计算[J].计算机学报，2002，25(12)：1417-1420.

[4] Harn L,Lin C Y,Wu C T.Structured multisignature algorithms[J].IEE Computers and Digital Techniques,2004,151(3):231-234.

[5] 傅鹤岗，陈滢.基于椭圆曲线的结构化多重数字签名算法[J].计算机应用，2009，29(1)：158-160.

[6] 陈逢林，胡万宝，孙广人.基于超椭圆曲线的顺序多重盲签名[J].计算机工程，2011，37(9)：160-162.

[7] Mumford D.Tata lectures on theta II:progress in mathematics 43[M].Berlin:Birkhauser,1984.

[8] Koblitz N.Algebraic aspects of cryptography[M].Berlin: Springer-Verlag,1998.

[9] Cantor D.Computing in the jacobian of A hyperelliptic curves[J].Mathematics of Computation,1987,48(1):95-101.

[10] You Lin,Sang Yongxuan.Effective generalized equations of secure hyperelliptic curve digital signature algorithms[J]. The Journal of China Universities of Posts and Telecommunications,2010,17(2):100-108.

[11] 游林.超椭圆曲线密码体制研究[D].辽宁大连：大连理工大学，2002.

[12] Lange T.Formulae for arithmetic on genus 2 hyperelliptic curves[J].Applicable Algebra in Engineering,Communication and Computing,2005,15(5):295-328.

[13] 郝艳华，许文丽，王育民.利用双基链计算超椭圆曲线标量乘[C]//密码学进展：中国密码学会2007年会论文集.成都：西南交通大学出版社，2007：102-108.

[14] Menezes A J,Oorschot P V,Vanstone S A.Handbook of applied cryptography[M].[S.l.]:CRC Press,Inc,1996.