第34卷 第3期 工 程 数 学 学 报 Vol. 34 No. 3
2017年06月 CHINESE JOURNAL OF ENGINEERING MATHEMATICS June 2017

doi: 10.3969/j.issn.1005-3085.2017.03.003 文章编号: 1005-3085(2017)03-0247-15

改进的超椭圆曲线结构化多重盲签名*

杨 青[1], 辛小龙[2], 李小光[1]

(1- 西安航空学院理学院，西安 710077; 2- 西北大学数学学院，西安 710069)

摘 要: 安全高效的多重盲签名方案在电子商务和电子现金系统有很多重要的应用．本文对已有的结构化多重签名方案进行了分析和改进，提出快速和高效的基于超椭圆曲线的结构化多重盲签名方案．我们将签名结构从二层扩展为三层，使有序和广播更好的结合，并给出各种情形下的具体算法．最后，比较和分析了改进方案的复杂度和安全性，与已有文献比较，改进方案的运算量减少了 $(3n+2)TH+(273.8n+32.2)TML$．结果表明，改进方案具有运算量低，所需时间少，安全性高且易于实现等优点．

关键词: 超椭圆曲线；约化除子；盲签名；结构化；多重签名

分类号: **AMS**(2010) 11G05; 14H52 **中图分类号**: TP309 **文献标识码**: A

1 引言

在超椭圆曲线上建立密码体制是 Koblitz[1] 在 1989 年提出的，它的安全性是建立在超椭圆曲线的 Jacobian 群离散对数问题上的．与椭圆曲线密码体制相比，超椭圆曲线的安全性更高，所用基域更小．例如，在相同的安全强度下，RSA 所用的基域为 1024 比特，椭圆曲线所用的基域为 160 比特，而对亏格为 2 的超椭圆曲线所用基域为 80 比特，对亏格为 3 的超椭圆曲线所用基域约为 55 比特．为了满足我们的安全需求[2]，在超椭圆曲线上建立阶为 2^{160} 大小的群．当亏格 $g>3$ 时，超椭圆曲线密码体制的安全性有所降低．当亏格为 3 时，也要选择安全的超椭圆曲线以避免攻击[3]．

盲签名是指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．盲签名除了满足一般数字签名的基本特征外，还必需满足以下几个性质：

1) 盲性，签名人不知道所签文件或消息的具体内容；

2) 不可追踪性，即签名人无法将有效的签名和被签名的消息联系起来[4,5]．

多重签名是指多个人合作对同一份消息进行签名，2010 年，Har 和 Ren[6] 提出多重签名方案，是基于身份的数字签名方案．由于签名过程的不同，有序多重签名和广播多重签名统称为多重签名，签名者按照串行的顺序进行签名称为有序多重签名，而广播多重签名对签名顺序没有要求．所有签名者按照某种特定的签名结构进行签名称为结构化多重签名，签名结构可以是有序的、广播的，或者是两者相结合的．人们将双线性对用于多重签

收稿日期: 2015-12-18. **作者简介**: 杨青 (1982年7月生)，女，讲师. 研究方向：信息与代数编码.

*基金项目: 陕西省科技厅项目 (2013JM1019; 2014K05-43)；陕西省教育厅项目 (14JK1310)；西安航空学院项目 (2015KY1218).

名方案，例如文献 [7–9]．将盲签名和多重签名结合起来形成具有特殊功能的多重盲签名方案．它同时具有两个签名的特性，用来满足特殊的应用要求．多重盲签名对于具有匿名性要求的网络通信具有独特的地位和作用．它被广泛应用于匿名电子投票系统，智能网中的电话投票业务，网上电子银行、数字现金等．例如，应用在电子现金需银行多个部门同时进行盲签名后才可生效的情形中．

本文对 Harn 等[10] 提出的结构化多重签名方案进行了分析和改进，提出了更为快速和高效的基于超椭圆曲线的结构化多重盲签名方案．首先，我们将有序多重签名和广播多重签名及盲签名相结合；其次，扩展了签名结构，使签名结构具有三层：第一层任一个有序签名者可以是单个签名者，也可以是虚拟签名者 (依据实际而定)，而每一个虚拟签名者又是由第二层的某些广播签名者组成；第二层的任一个广播签名者可以是单个签名者，也可以是虚拟签名者，若是虚拟签名者又可由第三层某些有序签名者组成．分析签名结构，给出具体签名算法和验证算法．再次，证明了算法的正确性和安全性．最后，比较和分析了改进方案的安全性和复杂度，并应用于超椭圆曲线密码系统．该算法具有快速、高效且易于实现的特点．在有序签名结构中，签名者的公钥按照签名顺序的倒序生成，由后往前依次生成，可以避免在生成公钥时出现重复，节省计算量．

本文第 1 节介绍超椭圆曲线的基本概念和多重盲签名的定义及安全模型；第 2 节提出改进的超椭圆曲线结构化多重盲签名方案；第 3 节证明新算法的正确性；第 4 节比较和分析了改进方案的安全性和复杂度；最后一节对本文进行总结，并探讨进一步的工作．

2 超椭圆曲线密码系统

2.1 超椭圆曲线的概念

本节将简要介绍超椭圆曲线的有关概念，具体内容可参考文献 [11,12]．给定有限域 F_q，它的代数闭包 $\bar{F}_q$，首先定义亏格为 g $(g<4)$ 的超椭圆曲线

$$C(F_q): y^2+h(x)y=f(x),$$

其中 $f(x)$ 是首一多项式，次数为 $2g+1$．$h(x)$ 是多项式，次数至多为 g，并且不存在点 (x,y) 同时满足 $y^2+h(x)y=f(x)$，及偏微分方程

$$2y+h(x)=0,\quad h'(x)y-f'(x)=0.$$

超椭圆曲线上有唯一的一个无穷远点 ∞．其次，建立超椭圆曲线上的 Jacobian 群．限于篇幅，超椭圆曲线 $C(F_q)$ 上的 Jacobian 群，记为 $J(C;F_q)$．Jacobian 群上的每个元素，都可用唯一的约化除子来表示．群加和倍除子是 Jacobian 群上的两种主要运算．Jacobian 群的阶为 $\#J(C;F_q)=hn$，n 是 160 比特的大素数 (或更大)，h 是较小的余因子或等于 1．D 是阶为 n 的约化除子，是 Jacobian 群的一个基元．$\mathrm{div}(1,0)$ 是群加法单位元．

$$D=\mathrm{div}(a,b),\quad a(x)=\sum_{i=0}^{g}a_ix^i,\quad b(x)=\sum_{i=0}^{g-1}b_ix^i,$$

当 $g=2$ 时

$$D=\mathrm{div}(a_2x^2+a_1x+a_0,b_1x+b_0),\quad x\in Z_n.$$

构造一个映射函数 φ[13]：$J(C;F_q)\longrightarrow Z_{q^{2g}}$，$\varphi$ 是一个从超椭圆曲线的 Jacobian 群中的元素到有限整数集的单射函数

$$Z_{q^{2g}}=\{0,1,\cdots,q^{2g}-1\},$$

$$\varphi(D)=a_{g-1}q^{2g-1}+\cdots+a_1q^{g+1}+a_0q^g+b_{g-1}q^{g-1}+\cdots+b_1q+b_0.$$

2.2　多重盲签名的定义

定义 1　多重盲签名方案中有 3 个参与者：消息发送者、签名者集合，签名收集者．一个多重盲签名算法主要过程如下：

1)　系统参数设置算法：输入安全参数 k，生成系统参数 params；

2)　密钥生成算法：输入系统参数 params，生成所有签名者 A_i 的公私钥对 (x_i,Y_i)；

3)　多重盲签名算法：消息发送者对消息 m 执行盲化处理，输出盲化消息 m'，所有签名者按照约定的签名顺序进行盲签名和对部分盲签名验证，输出盲签名 s；

4)　多重盲签名的脱盲和验证算法：输入消息发送者，签名收集者和所有签名者的公钥及盲签名 s 进行脱盲和验证．若签名有效，则算法输出 1，否则输出 0．

定义 2　CDH (computational diffie-Hellman) 问题：对于任意未知的整数 $a,b\in Z_n^*$，已知 D, aD, $bD\in G$，求解 $abD\in G$ 是困难的．

CDH 假设：若不存在多项式时间算法在时间 t 内以至少 ε 的概率求解 CDH 问题，那么称 (ε,t)-CDH 假设在 G 上成立．

2.3　多重盲签名方案的安全模型

一个安全有效的多重盲签名方案必需满足盲性和不可伪造性．盲性是指签名者不能将签名过程和最终的签名结果相对应，也不能实现对盲签名消息的跟踪．本文形式化地定义敌手 A 与挑战者 B 之间的游戏来模拟改进方案的盲性．

定义 3 (盲性)　如果存在多项式时间敌手 A 以可忽略的优势

$$Adv(A)=\left|2Pr[\gamma=\gamma']-1\right|$$

赢得测试 1，则改进方案满足盲性．

测试 1　①　系统建立：挑战者 B 选取系统安全参数，运行算法，输出系统公共参数 params，并发送给敌手 A；

②　准备：敌手 A 选取两个可区分且相同长度的消息 m_1, m_2 及签名者提交给挑战者 B；

③　挑战：挑战者 B 随机选择比特位 $\gamma\in[0,1]$ 请求 A 分别运行对盲化后的消息 m_1', m_2' 签名．随后，挑战者 B 运行去盲算法，并返回对 m_1 的最终盲签名给敌手 A；

④　应答：敌手 A 输出对 γ 的猜测 γ'，如果等式 $\gamma=\gamma'$ 成立，则敌手 A 赢得游戏．

下面讨论多重盲签名的不可伪造性，方案主要包括 2 类敌手：第一类敌手 A1 只能访问公开参数；第二类敌手 A2 除访问公开参数外，还可访问签名者的私钥．可见，A2 蕴

含了 A1，即多重盲签名方案应该在 A2 敌手攻击下可证明安全．基于文 [14–16] 的签名模型，本文定义敌手 $\mathrm{A} \in \{\mathrm{A1}, \mathrm{A2}\}$ 与挑战者 B 之间的游戏来模拟改进方案的不可伪造性．

定义 4 (不可伪造性) 对于任意多项式有界的敌手 A，如果 A 赢得测试 2 的概率是可忽略的，则称改进方案在适应性选择消息攻击下具有不可伪造性．

测试 2 ① 系统参数设置：挑战者 B 运行系统参数生成算法，得到系统参数 params 并发送给敌手 A；

② 签名询问：若敌手 A 攻破 k 个签名者的私钥并能伪造他们的部分签名．敌手 A 为获得未被攻破签名者的部分签名，向挑战者 B 发起询问，包括用户生成询问、私钥询问及签名询问，并得到输出；

③ 伪造：敌手 A 输出对应消息 m'^* 的多重盲签名 s'^*．如果 s'^* 未在签名询问中出现过，且为按照签名顺序对 m'^* 的有效签名，则敌手 A 赢得游戏．

3 改进的结构化多重盲签名方案

本文首先结合有序与广播签名的特征，将签名结构进一步扩充成三层．有序签名中嵌套广播签名，而广播签名中又嵌套有序签名，如图 1 这样更符合实际中的应用．其次将多重签名和盲签名结合，给出不同情况下，具体算法．最后推广到超椭圆曲线密码系统上，提高了安全性能和效率．

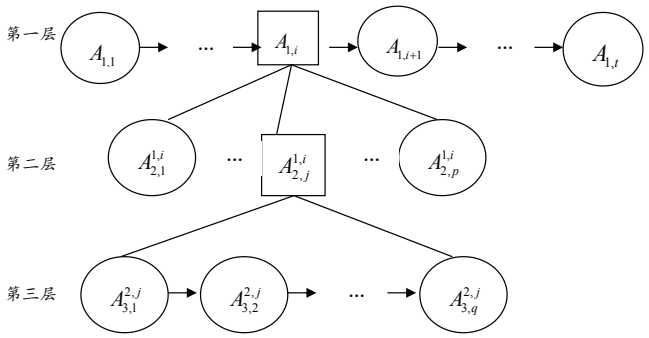

图 1: 签名结构

3.1 系统参数的设定

该算法有 $t+p+q$ 个签名者 (也称签名节点)，其中含 2 个虚拟签名者，签名过程可由消息发送者 I，签名收集者 C 和 $t+p+q$ 个签名者实现．

签名结构为如图 1 所示的三层结构．节点 $A_{3,q}^{2,j}$ 的含义：$(2,j)$ 指该节点的父节点 (上一层) 位于第二层，第 j 个；$(3,q)$ 是指该结点位于第三层，第 q 个．$A_{1,i}$ 指该节点位于第一层，第 i 个，无父节点．其他签名节点含义类同．签名顺序为 $(A_{1,1}, \cdots, A_{1,i}, \cdots A_{1,t})$，其中任一签名节点 $A_{1,i}$ 可以由 p 个广播签名者 $A_{2,1}^{1,i}, \cdots, A_{2,p}^{1,i}$ 组成，这 p 个签名者可同时进行签名，不必遵循先后次序；而任一节点 $A_{2,j}^{1,i}$ 又可由 q 个有序签名者 $A_{3,1}^{2,j}, \cdots, A_{3,q}^{2,j}$ 组成，按照串行的顺序进行签名．由多个签名者组成的节点称为虚拟节点．

3.2　签名者公钥的生成

有序签名者的公钥按照签名顺序的倒序生成，广播签名者的公钥可依据它后续签名者的公钥生成，若无后续签名者，则可由超椭圆曲线上的Jacobian群的一个基元D生成. 所有签名者的公钥和私钥生成如下：

第三层有序签名者$A_{3,1}^{2,j},\cdots,A_{3,q}^{2,j}$的密钥：按照签名顺序$(A_{3,1}^{2,j},\cdots,A_{3,q}^{2,j})$的倒序生成，由后往前，从$A_{3,q}^{2,j}$开始，$A_{3,q}^{2,j}$的私钥为$x_{3,q}^{2,j}\in Z_n^*$，公钥为

$$Y_{3,q}^{2,j}=x_{3,q}^{2,j}Y_{3,q+1}^{2,j},\quad Y_{3,q+1}^{2,j}=Y_{1,i+1},\quad i=t,\quad Y_{1,t+1}=D,$$

则签名者$A_{3,w}^{2,j}$的私钥为$x_{3,w}^{2,j}\in Z_n^*$, $1\le w\le q$，公钥为$Y_{3,w}^{2,j}=x_{3,w}^{2,j}Y_{3,w+1}^{2,j}$.

第二层广播签名者$A_{2,1}^{1,i},\cdots,A_{2,p}^{1,i}$的密钥：若是单个签名者，则公钥分别为

$$Y_{2,1}^{1,i}=x_{2,1}^{1,i}Y_{1,i+1},\cdots,Y_{2,p}^{1,i}=x_{2,p}^{1,i}Y_{1,i+1},\quad i=t,\quad Y_{1,t+1}=D,$$

私钥分别为$x_{2,1}^{1,i},\cdots,x_{2,p}^{1,i}\in Z_n^*$. 公钥不能相同，若相同则重新选择私钥计算公钥. 若$A_{2,j}^{1,i}$是虚拟签名者，则公钥为

$$Y_{2,j}^{1,i}=Y_{3,1}^{2,j}=x_{3,1}^{2,j}Y_{3,2}^{2,j}=\prod_{w=1}^{q}x_{3,w}^{2,j}Y_{1,i+1},$$

此公钥为组成该虚拟节点的第一个有序签名者的公钥，私钥为

$$x_{2,j}^{1,i}=\prod_{w=1}^{q}x_{3,w}^{2,j}\in Z_n^*.$$

第一层有序签名者$A_{1,1},\cdots,A_{1,i},\cdots,A_{1,t}$的密钥：若是单个签名者，则按照签名顺序$(A_{1,1},\cdots,A_{1,i},\cdots,A_{1,t})$的倒序生成，由后往前，从$A_{1,t}$开始，$A_{1,t}$的私钥为$x_{1,t}\in Z_n^*$，公钥为$Y_{1,t}=x_{1,t}Y_{1,t+1}$, $Y_{1,t+1}=D$，则签名者$A_{1,i}$的私钥为$x_{1,i}\in Z_n^*$, $1\le i\le t$，公钥为$Y_{1,i}=x_{1,i}Y_{1,i+1}$. 若$A_{1,i}$是虚拟签名者，则公钥为

$$Y_{1,i}=Y_{2,1}^{1,i}+Y_{2,2}^{1,i}+\cdots+Y_{2,j}^{1,i}+\cdots+Y_{2,p}^{1,i},$$

私钥为

$$x_{1,i}=\sum_{j=1}^{p}x_{2,j}^{1,i}.$$

当所有签名者的公钥生成完后，系统公布签名结构和所有签名者的公钥，每个签名者保存自己的私钥，并且系统公开参数还有超椭圆曲线$C(F_q)$, φ, n, D.

3.3　生成R

从第三层开始依次倒序计算(若第三层存在)，具体步骤如下：

1)　从第三层开始，每个有序签名者$A_{3,w}^{2,j}$ $(w=1,2,\cdots,q)$随机选取$k_{3,w}^{2,j}\in Z_n^*$，计算$R_{3,w}^{2,j}=k_{3,w}^{2,j}Y_{3,w+1}^{2,j}$，其中$Y_{3,q+1}^{2,j}=Y_{1,i+1}$，并发送$R_{3,w}^{2,j}$给签名收集者C；

2)　签名收集者C收到所有$R_{3,w}^{2,j}$后，计算

$$R_{2,j}^{1,i}=\sum_{w=1}^{q}R_{3,w}^{2,j},$$

并发送 $R_{2,j}^{1,i}$ 给第三层每个签名者 $A_{3,w}^{2,j}$ 和消息发送者I. $R_{2,j}^{1,i}$ 与第二层广播虚拟签名者 $A_{2,j}^{1,i}$ 对应;

3) 第二层每个广播单个签名者 $A_{2,j}^{1,i}$ 随机选取 $k_{2,j}^{1,i} \in Z_n^*$，计算 $R_{2,j}^{1,i} = k_{2,j}^{1,i} Y_{1,i+1}$，当 $i = t$ 时，$Y_{1,t+1} = D$，并发送 $R_{2,j}^{1,i}$ 给签名收集者C;

4) 签名收集者C收到所有 $R_{2,j}^{1,i}\,(1 \le j \le p)$ 后，计算 $R_{1,i} = R_{2,1}^{1,i} + \cdots + R_{2,p}^{1,i}$，若 $A_{2,j}^{1,i}$ 是虚拟签名者，则可由步骤2)计算得 $R_{2,j}^{1,i}$，若 $A_{2,j}^{1,i}$ 是广播单个签名者，则可由步骤3)计算得 $R_{2,j}^{1,i}$. 签名收集者C发送 $R_{1,i}$ 给所有第二层签名者 $A_{2,j}^{1,i}$ 和I;

5) 第一层每个有序单个签名者 $A_{1,i}$，随机选取 $k_{1,i} \in Z_n^*$，计算 $R_{1,i} = k_{1,i} Y_{1,i+1}$，并发送 $R_{1,i}$ 给签名收集者C，$Y_{1,t+1} = D$;

6) 签名收集者C收到所有 $R_{1,i}$ 后，计算 $R = \sum_{i=1}^{t} R_{1,i}$，其中若 $A_{1,i}$ 是虚拟签名者，则可由步骤4)计算得 $R_{1,i}$，若 $A_{1,i}$ 是有序单个签名者，则可由步骤5)计算得 $R_{1,i}$，签名收集者C发送 R 给所有签名者和I.

根据签名结构图，所有签名者和签名收集者C在生成 R 时，若无第三层，则可由步骤3)开始进行；若无第二层，则由步骤5)开始进行.

3.4 盲签名的生成和验证

3.4.1 消息 m 的盲化

由3.3节可知，消息发送者I收到签名收集者C发送的 R 后，I任选 $\alpha, \beta \in Z_n^*$，计算 $H = \alpha R + \beta D$，对消息 m 盲化，计算 $m' = \alpha^{-1}\varphi(H)^{-1}\varphi(R)m \bmod n$ 和 $e = m'Y_{1,1}$，并发送 e 给所有签名者，发送 m' 给 $A_{1,1}$.

3.4.2 验证并生成签名

每一个签名者收到前一签名者的签名后，首先验证此签名是否有效. 若之前签名有效，则继续签名，然后将自己的签名发送给下一位签名者；否则拒绝签名.

从 $A_{1,1}$ 开始，按照系统公布的签名顺序和签名结构依次进行：

1) 若 $A_{1,i}$ 是单个签名者，则继续如下步骤：

① $A_{1,i}$ 收到 $A_{1,i-1}$ 的签名后，验证方程 $e = s_{1,i-1}Y_{1,i} + \varphi(R)Q_{1,i-1}$ 是否成立，若成立，则继续下一步骤，否则要求 $A_{1,i-1}$ 重签或拒绝签名，$A_{1,1}$ 不需验证;

② $A_{1,i}$ 计算

$$s_{1,i} = x_{1,i}s_{1,i-1} - k_{1,i}\varphi(R) \bmod n, \quad Q_{1,i} = Q_{1,i-1} + R_{1,i},$$

其中 $s_{1,0} = m'$, $Q_{1,0} = 0$, $Q_{1,t} = R\,(1 \le i \le t)$，并传递数组 $(s_{1,i}, Q_{1,i})$ 给 $A_{1,i+1}$，若 $A_{1,i+1}$ 是虚拟签名者，则传递给签名收集者C，C验证签名的有效性.

2) 若 $A_{1,i}$ 是虚拟签名者，即由第二层的 p 个广播签名者 $(A_{2,1}^{1,i}, \cdots, A_{2,p}^{1,i})$ 组成，而任一 $A_{2,j}^{1,i}\,(1 \le j \le p)$ 又可由第三层的 q 个有序签名者 $A_{3,1}^{2,j}, \cdots, A_{3,q}^{2,j}$ 组成. 签名收集者C验证由 $A_{1,i-1}$ 发送的签名数组 $(s_{1,i-1}, Q_{1,i-1})$，验证方程

$$e = s_{1,i-1}Y_{1,i} + \varphi(R)Q_{1,i-1}$$

是否成立. 如果成立，那么签名收集者C将数组 $(s_{1,i-1}, Q_{1,i-1})$ 分别发送给 $A_{2,1}^{1,i}, \cdots, A_{3,1}^{2,j}$,

$A_{2,j+1}^{1,i},\cdots,A_{2,p}^{1,i}$ ($A_{3,1}^{2,j}$ 接收 C 发送给虚拟签名者 $A_{2,j}^{1,i}$ 的数组) 后继续下一步骤，其中 $s_{1,0}=m'$, $Q_{1,0}=0$，否则签名终止.

① 若 $A_{2,j}^{1,i}$ 是单个签名者，则继续如下步骤：

(a) $A_{2,j}^{1,i}$ 收到签名收集者 C 发送的 R, $(s_{1,i-1},Q_{1,i-1})$, $R_{1,i}$ 后，计算

$$s_{2,j}^{1,i}=x_{2,j}^{1,i}s_{1,i-1}-k_{2,j}^{1,i}\varphi(R)\ \bmod n,$$

其中 $s_{1,0}=m'$，并将签名 $s_{2,j}^{1,i}$ 发送给签名收集者 C；

(b) 签名收集者 C 收到广播单个签名者 $A_{2,j}^{1,i}$ 发送的签名 $s_{2,j}^{1,i}$ 后，验证

$$\varphi(R)R_{2,j}^{1,i}=s_{1,i-1}Y_{2,j}^{1,i}-s_{2,j}^{1,i}Y_{1,i+1}$$

是否成立. 若成立，则宣布签名有效，否则要求重签或宣布无效.

② 若 $A_{2,j}^{1,i}$ 是虚拟签名者，由 q 个有序签名者 $A_{3,1}^{2,j},\cdots,A_{3,q}^{2,j}$ 组成，继续如下步骤：

(a) $A_{3,1}^{2,j}$ 收到签名收集者 C 发送的 R, $(s_{1,i-1},Q_{1,i-1})$, $R_{1,i}$ 后，从 $A_{3,1}^{2,j}$ 依次开始，$A_{3,w}^{2,j}$ 计算

$$s_{3,w}^{2,j}=x_{3,w}^{2,j}s_{3,w-1}^{2,j}-k_{3,w}^{2,j}\varphi(R)\ \bmod n,$$

当 $w=1$ 时

$$s_{3,0}^{2,j}=s_{1,i-1},\quad Q_{3,0}^{2,j}=0,\quad 1\le w\le q,\quad Q_{3,w}^{2,j}=Q_{3,w-1}^{2,j}+R_{3,w}^{2,j},$$

并将签名 $(s_{3,w}^{2,j},Q_{3,w}^{2,j})$ 发送给下一位 $A_{3,w+1}^{2,j}$；

(b) $A_{3,w+1}^{2,j}$ 收到签名 $(s_{3,w}^{2,j},Q_{3,w}^{2,j})$ 后，验证等式

$$s_{1,i-1}Y_{3,1}^{2,j}=s_{3,w}^{2,j}Y_{3,w+1}^{2,j}+\varphi(R)Q_{3,w}^{2,j}$$

是否成立. 若成立，则按照步骤 (a) 继续签名；否则，要求 $A_{3,w}^{2,j}$ 重签或拒绝签名. 当 $w=q$ 时，$Y_{3,q+1}^{2,j}=Y_{1,i+1}$，直到最后一个签名者 $A_{3,q}^{2,j}$ 将其签名 $(s_{3,q}^{2,j},Q_{3,q}^{2,j})$ 发送给签名收集者 C；

(c) 签名收集者 C 收到签名 $(s_{3,q}^{2,j},Q_{3,q}^{2,j})$ 后，验证等式

$$s_{1,i-1}Y_{3,1}^{2,j}=s_{3,q}^{2,j}Y_{1,i+1}+\varphi(R)R_{2,j}^{1,i}$$

是否成立. 若成立，则宣布签名有效，并将签名 $(s_{3,q}^{2,j},Q_{3,q}^{2,j})$ 作为是虚拟签名者 $A_{2,j}^{1,i}$ 的签名

$$s_{2,j}^{1,i}=s_{3,q}^{2,j},\quad R_{2,j}^{1,i}=Q_{3,q}^{2,j}=\Sigma_{w=1}^{q}R_{3,w}^{2,j},\quad Q_{2,j}^{1,i}=Q_{2,j-1}^{1,i}+R_{2,j}^{1,i},$$

否则终止签名.

③ 签名收集者 C 收到第二层所有 $A_{2,j}^{1,i}$ 的签名 $s_{2,j}^{1,i}$ 且验证有效后，计算

$$s_{1,i}=s_{2,1}^{1,i}+\cdots+s_{2,p}^{1,i}\ \bmod n,\quad Q_{1,i}=Q_{1,i-1}+R_{1,i},$$

其中 $R_{1,i}=\sum\limits_{j=1}^{p}R_{2,j}^{1,i}$ (见 3.3 节)，则公布虚拟签名者 $A_{1,i}$ 的签名 $(s_{1,i},Q_{1,i})$，并发送签名给下一位 $A_{1,i+1}$，否则终止签名.

3) 对于后续签名者 $A_{1,i+1},\cdots,A_{1,t}$，按照本节 3.4.2 介绍的方法进行签名及验证. 将第一层最后一位签名者 $A_{1,t}$ 的签名 $(s_{1,t},Q_{1,t})$ 作为 m' 的结构化多重盲签名，发送给签名收集者 C. 若 $A_{1,t}$ 是单个签名者，则 C 验证等式 $e=s_{1,t}D+\varphi(R)Q_{1,t}$ 是否成立. 若成立，则宣布签名有效，否则无效. 若 $A_{1,t}$ 是虚拟签名者，则按照 3.4.2 的步骤 2) 的方法进行签名和验证 (当 $i=t$ 时).

最后，C 验证 $A_{1,t}$ 的签名有效后发送签名 $s_{1,t}$ 给 I 进行脱盲变换，否则终止签名.

3.4.3 盲签名的脱盲和验证过程

消息发送者 I 收到签名收集者 C 发送的签名 $s_{1,t}$ 后，计算 $s=(m')^{-1}ms_{1,t}-\beta\varphi(H)$. 若等式 $mY_{1,1}=sD+\varphi(H)H$ 成立，则 I 宣布消息 m 的盲签名 s 有效，否则无效.

4 正确性证明

定理 1 若等式 $e=s_{1,i}Y_{1,i+1}+\varphi(R)Q_{1,i}$ 成立，则有序单个签名者 $A_{1,1},\cdots,A_{1,i}$ 的签名有效.

证明 由

$$s_{1,i}=x_{1,i}s_{1,i-1}-k_{1,i}\varphi(R)\ \bmod n,\quad x_{1,i}s_{1,i-1}=s_{1,i}+k_{1,i}\varphi(R)\ \bmod n,$$

可得

$$x_{1,i}s_{1,i-1}Y_{1,i+1}=s_{1,i}Y_{1,i+1}+k_{1,i}\varphi(R)Y_{1,i+1},\quad s_{1,i-1}Y_{1,i}=s_{1,i}Y_{1,i+1}+\varphi(R)R_{1,i}.$$

当 $i=1,2,\cdots$ 时，有

$$\begin{cases} s_{1,0}Y_{1,1}=s_{1,1}Y_{1,2}+\varphi(R)R_{1,1},\\ s_{1,1}Y_{1,2}=s_{1,2}Y_{1,3}+\varphi(R)R_{1,2},\\ \cdots,\\ s_{1,i-1}Y_{1,i}=s_{1,i}Y_{1,i+1}+\varphi(R)R_{1,i}, \end{cases}$$

上述等式左右两端相加，得 $s_{1,0}Y_{1,1}=s_{1,i}Y_{1,i+1}+\varphi(R)Q_{1,i}$，又因 $s_{1,0}=m'$，所以

$$e=m'Y_{1,1}=s_{1,i}Y_{1,i+1}+\varphi(R)Q_{1,i}.$$

定理 2 若等式 $s_{1,i-1}Y_{3,1}^{2,j}=s_{3,q}^{2,j}Y_{1,i+1}+\varphi(R)R_{2,j}^{1,i}$ 成立，则第二层广播虚拟签名者 $A_{2,j}^{1,i}$，第三层有序签名者 $A_{3,1}^{2,j},\cdots,A_{3,q}^{2,j}$ 的签名有效.

证明 因为

$$s_{3,w}^{2,j}=x_{3,w}^{2,j}s_{3,w-1}^{2,j}-k_{3,w}^{2,j}\varphi(R)\ \bmod n,\quad x_{3,w}^{2,j}s_{3,w-1}^{2,j}=s_{3,w}^{2,j}+k_{3,w}^{2,j}\varphi(R)\ \bmod n,$$

所以

$$x_{3,w}^{2,j}s_{3,w-1}^{2,j}Y_{3,w+1}^{2,j}=s_{3,w}^{2,j}Y_{3,w+1}^{2,j}+k_{3,w}^{2,j}\varphi(R)Y_{3,w+1}^{2,j},$$

$$s_{3,w-1}^{2,j}Y_{3,w}^{2,j}=s_{3,w}^{2,j}Y_{3,w+1}^{2,j}+\varphi(R)R_{3,w}^{2,j}.$$

当 $w=1,2,\cdots,q$ 时，有

$$\begin{cases} s_{3,0}^{2,j}Y_{3,1}^{2,j}=s_{3,1}^{2,j}Y_{3,2}^{2,j}+\varphi(R)R_{3,1}^{2,j},\\ s_{3,1}^{2,j}Y_{3,2}^{2,j}=s_{3,2}^{2,j}Y_{3,3}^{2,j}+\varphi(R)R_{3,2}^{2,j},\\ \cdots,\\ s_{3,q}^{2,j}Y_{3,q+1}^{2,j}=s_{3,q}^{2,j}Y_{3,q+1}^{2,j}+\varphi(R)R_{3,q}^{2,j}, \end{cases}$$

将上述等式左右两端相加，得

$$s_{3,0}^{2,j}Y_{3,1}^{2,j}=s_{3,q}^{2,j}Y_{3,q+1}^{2,j}+\varphi(R)\sum_{w=1}^{q}R_{3,w}^{2,j},$$

又因

$$s_{3,0}^{2,j}=s_{1,i-1},\quad R_{2,j}^{1,i}=Q_{3,q}^{2,j}=\sum_{w=1}^{q}R_{3,w}^{2,j},\quad Y_{3,q+1}^{2,j}=Y_{1,i+1},$$

所以

$$s_{1,i-1}Y_{3,1}^{2,j}=s_{3,q}^{2,j}Y_{1,i+1}+\varphi(R)R_{2,j}^{1,i}.$$

定理3　若等式 $\varphi(R)R_{2,j}^{1,i}=s_{1,i-1}Y_{2,j}^{1,i}-s_{2,j}^{1,i}Y_{1,i+1}$ 成立，则第二层广播单个签名者 $A_{2,j}^{1,i}$ 的签名有效.

证明　因为

$$\begin{aligned} s_{2,j}^{1,i}&=x_{2,j}^{1,i}s_{1,i-1}-k_{2,j}^{1,i}\varphi(R)\ \bmod n,\\ s_{2,j}^{1,i}Y_{1,i+1}&=x_{2,j}^{1,i}s_{1,i-1}Y_{1,i+1}-k_{2,j}^{1,i}\varphi(R)Y_{1,i+1},\\ s_{2,j}^{1,i}Y_{1,i+1}&=s_{1,i-1}Y_{2,j}^{1,i}-\varphi(R)R_{2,j}^{1,i}, \end{aligned}$$

所以

$$\varphi(R)R_{2,j}^{1,i}=s_{1,i-1}Y_{2,j}^{1,i}-s_{2,j}^{1,i}Y_{1,i+1}.$$

实际上，当 $A_{2,j}^{1,i}$ 是虚拟签名者时，公钥为 $Y_{2,j}^{1,i}=Y_{3,1}^{2,j}$，签名为 $s_{2,j}^{1,i}=s_{3,q}^{2,j}$，因此，在定理2和定理3中，广播签名者 $A_{2,j}^{1,i}$ 的签名验证等式的形式可统一写为

$$\varphi(R)R_{2,j}^{1,i}=s_{1,i-1}Y_{2,j}^{1,i}-s_{2,j}^{1,i}Y_{1,i+1},$$

但二者签名方法不同.

定理4　若等式 $mY_{1,1}=sD+\varphi(H)H$ 成立，则原始消息 m 的结构化盲签名 s 有效.

证明　由定理1和定理4的证明可知，总有式 $s_{1,i-1}Y_{1,i}=s_{1,i}Y_{1,i+1}+\varphi(R)R_{1,i}$ 成立，所以

$$e=m'Y_{1,1}=s_{1,i}Y_{1,i+1}+\varphi(R)Q_{1,i},$$

当$i=t$时，$m'Y_{1,1}=s_{1,t}Y_{1,t+1}+\varphi(R)Q_{1,t}$，又因$Y_{1,t+1}=D$, $Q_{1,t}=R$，所以$m'Y_{1,1}=s_{1,t}D+\varphi(R)R$，又因$m'=\alpha^{-1}\varphi(H)^{-1}\varphi(R)m \bmod n$，所以

$$\alpha^{-1}\varphi(H)^{-1}\varphi(R)mY_{1,1}=s_{1,t}D+\varphi(R)R,$$

$$s_{1,t}D=\alpha^{-1}\varphi(H)^{-1}\varphi(R)mY_{1,1}-\varphi(R)R.$$

又因$s=(m')^{-1}ms_{1,t}-\beta\varphi(H)$，所以

$$s=\alpha\varphi(H)\varphi(R)^{-1}s_{1,t}-\beta\varphi(H),$$

$$sD=\alpha\varphi(H)\varphi(R)^{-1}s_{1,t}D-\beta\varphi(H)D=mY_{1,1}-\alpha\varphi(H)R-\beta\varphi(H)D$$

$$=mY_{1,1}-\varphi(H)(\alpha R+\beta D)=mY_{1,1}-\varphi(H)H,$$

所以$mY_{1,1}=sD+\varphi(H)H$.

5 方案分析

5.1 安全性分析

1) 盲性分析

定理5 本文提出的改进的多重盲签名方案满足盲性.

证明 给定任意一个有效的多重盲签名(m,e,s)和在盲签名过程中产生的任意视图$(H,m',s_{1,t})$，总存在唯一的一对盲因子$\alpha,\beta\in Z_n^*$. 因为盲因子$\alpha,\beta\in Z_n^*$是随机数，所以多重盲签名方案必然满足盲性，并且有下列等式成立：

① $H=\alpha R+\beta D$;

② $m'=\alpha^{-1}\varphi(H)^{-1}\varphi(R)m$;

③ $s=(m')^{-1}ms_{1,t}-\beta\varphi(H)$.

由②知存在唯一的$\alpha\in Z_n^*$，使得$\alpha=\varphi(H)^{-1}\varphi(R)m(m')^{-1}$. 同时，由③知也必然存在唯一的$\beta\in Z_n^*$，使得$\beta=\varphi(H)^{-1}[m(m')^{-1}s_{1,t}-s]$. 下面证明$\alpha,\beta\in Z_n^*$也满足式①，由于盲签名是有效的，所以$mY_{1,1}=sD+\varphi(H)H$成立(定理4). 因此，$H=(mY_{1,1}-sD)\varphi(H)^{-1}$，再由定理4的证明知$sD=mY_{1,1}-\varphi(H)(\alpha R+\beta D)$，所以有$H=\alpha R+\beta D$.

由以上可知，在多重盲签名方案中，总存在$\alpha,\beta\in Z_n^*$，签名过程中产生的视图与任何有效的盲签名均无关联. 因此，即使是一个具有无限计算能力的敌手A输出正确值的概率是0.5. 根据定义3，故敌手A输出$\gamma=\gamma'$的概率是$Pr[\gamma=\gamma']=0.5$. 所以敌手A赢得测试1的优势$Adv(A)=|2Pr[\gamma=\gamma']-1|$是可忽略的，从而改进方案满足盲性.

2) 改进方案满足不可伪造性

定理6 在多重盲签名的标准安全模型下，如果敌手A能够以不可忽略的概率伪造出多重盲签名，则挑战者B能够解决CDH问题.

证明 当敌手A在多项式时间t内以不可忽略的概率ε攻破改进方案，则挑战者B能够解决CDH问题(即就是B已知$D,D_1=aD,D_2=bD$能输出abD). 实例过程如下：

① 系统参数设置：假设签名者有t个，A已获得$i\,(1\le i\le t-1)$个签名者的私钥．为伪造多重盲签名，敌手A需要伪造$A_{1,t}$的签名．B选择安全参数，生成系统参数$C(F_q)$, φ, n, D，签名结构及所有签名者的公钥并发送给敌手A．B维护表L_k, L_R为对应私钥和R的询问；

② 私钥和R的询问：A询问签名者$A_{1,i}$的私钥$x_{1,i}, R_{1,i}$和R．B首先计算$R=\sum\limits_{i=1}^{t}R_{1,i}$，然后查询表$L_k, L_R$得到$x_{1,i}, R_{1,i}$，最后返回$(A_{1,i}, x_{1,i}, R_{1,i}, R)$给A；

③ 签名的询问：A询问签名者$A_{1,i}$对消息m'的签名．B在表L_k, L_R中分别查找对应$A_{1,i}$的私钥$x_{1,i}$和$R_{1,i}$，然后计算签名

$$s_{1,i}=x_{1,i}s_{1,i-1}-k_{1,i}\varphi(R)\mod n,\quad Q_{1,i}=Q_{1,i-1}+R_{1,i},\quad 1\le i\le t-1,$$

其中$s_{1,0}=m'$, $Q_{1,0}=0$，并返回数组$(s_{1,i}, Q_{1,i})$给A；

④ 伪造签名：敌手A在多项式时间t内以概率ε输出一个从未被询问过的消息m'^*的有效多重盲签名$(m'^*, s'^*_{1,t}, Q_{1,t})$．然后，B再次利用A得到一个从未被询问过的消息$\overline{m}^*$的有效多重盲签名$(\overline{m}^*, \overline{s}^*_{1,t}, \overline{Q}_{1,t})$．根据一般分叉引理[17]，B以不可忽略的概率得到对m'^*的2个伪造多重盲签名$(m'^*, s'^*, Q_{1,t})$和$(m'^*, \overline{s}^*_{1,t}, Q_{1,t})$．接着，B计算$R_{1,t}=D_2+tD$，由于$s'^*_{1,t}=x_{1,t}s'^*_{1,t-1}-k_{1,t}\varphi(R)$．假定签名者$A_{1,t}$的公钥可表为$Y_{1,t}=x_{1,t}D=D_1+tD$，则由方程组

$$\begin{cases} s'^*_{1,t}R_{1,t}=x_{1,t}s'^*_{1,t-1}R_{1,t}-k_{1,t}\varphi(R)R_{1,t},\\ \overline{s}^*_{1,t}R_{1,t}=x_{1,t}\overline{s}^*_{1,t-1}R_{1,t}-k_{1,t}\varphi(R)R_{1,t},\end{cases}$$

求得

$$abD=\frac{s'^*_{1,t}-\overline{s}^*_{1,t}}{s'^*_{1,t-1}-\overline{s}^*_{1,t-1}}(D_2+tD)-t(D_1+D_2+tD).$$

所以，若A能成功伪造有效多重盲签名，则挑战者B能够解决CDH困难问题，与定义2矛盾．由定义4，方案满足不可伪造性．

3) 任一签名者$A_{1,i}$是虚拟签名者时，等式$e=s_{1,i}Y_{1,i+1}+\varphi(R)Q_{1,i}$也是成立的．因为，虚拟签名者$A_{1,i}$的签名为$s_{1,i}=s^{1,i}_{2,1}+\cdots+s^{1,i}_{2,p}\bmod n$，若$A^{1,i}_{2,j}$是虚拟签名者，其公钥为$Y^{1,i}_{2,j}=Y^{2,j}_{3,1}$，签名为$s^{1,i}_{2,j}=s^{2,j}_{3,q}$．因为$\varphi(R)R^{1,i}_{2,j}=s_{1,i-1}Y^{1,i}_{2,j}-s^{1,i}_{2,j}Y_{1,i+1}$，所以$s_{1,i-1}Y^{1,i}_{2,j}=s^{1,i}_{2,j}Y_{1,i+1}+\varphi(R)R^{1,i}_{2,j}$，当$j=1,2,\cdots,p$时，有

$$\begin{cases} s_{1,i-1}Y^{1,i}_{2,1}=s^{1,i}_{2,1}Y_{1,i+1}+\varphi(R)R^{1,i}_{2,1},\\ s_{1,i-1}Y^{1,i}_{2,j}=s^{1,i}_{2,j}Y_{1,i+1}+\varphi(R)R^{1,i}_{2,j},\\ \cdots,\\ s_{1,i-1}Y^{1,i}_{2,p}=s^{1,i}_{2,p}Y_{1,i+1}+\varphi(R)R^{1,i}_{2,p},\end{cases}$$

将上述等式两端左右相加，得

$$s_{1,i-1}\sum_{j=1}^{p}Y^{1,i}_{2,j}=Y_{1,i+1}\sum_{j=1}^{p}s^{1,i}_{2,j}+\varphi(R)\sum_{j=1}^{p}R^{1,i}_{2,j},$$

又因

$$Y_{1,i}=\sum_{j=1}^{p}Y_{2,j}^{1,i},\quad R_{1,i}=\sum_{j=1}^{p}R_{2,j}^{1,i},$$

所以

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

这与定理1中等式相同，所以$e=s_{1,i}Y_{1,i+1}+\varphi(R)Q_{1,i}$成立．另外，当$i=t$时，若$A_{1,t}$是单个签名者，则C验证签名等式为$e=s_{1,t}D+\varphi(R)Q_{1,t}$；若$A_{1,t}$是虚拟签名者，则签名的安全性由定理2和定理3验证．

5.2 效率分析

本文的有序多重盲签名方案、广播多重盲签名方案分别与文献[10,18–21]的方案进行了效率分析，如表1和表2所示．我们的操作平台是Pentium IV 3GHZ，512 MB RAM和Windows XP操作系统．在有限域$F_q=F_{p^{113}}$上，选取亏格为2的超椭圆曲线$C(F_q):y^2=x^p-a_1x-a_2$，$C(F_q)$上的Jacobian群的阶$\#J(C;F_q)=1+5^{226}$，取$p=5$．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可参考文献[11,12,22]，除子加法的运算量为$1I+3S+22M$，除子倍点的运算量为$1I+5S+22M$，其中I, S, M分别表示有限域上的求逆、平方和乘法，$1I=30M$, $1S=0.8M$, $1T_{EX}=240T_{ML}$, $1T_{HEM}=56T_{ML}$, $1T_{HEA}=55.4T_{ML}$．为便于比较计算量，假定签名者人数均为n．计算结果见表2，本文的有序多重盲签名方案(结构图中第一层，算法见3.4.2节1)及3.4.3脱盲过程)总的运算量为$(223.8n+169)T_{ML}$．与文献[19]的有序签名比较，本文的运算量减少$2nT_H+(257.2n-169)T_{ML}$．本文的广播多重盲签名方案(结构图中的第二层，算法见3.4.2节2)①(a), (b)及③和3.4.3脱盲过程)总的计算量为$(224.4n+280.8)T_{ML}$．与文献[19]的广播签名比较，本文的运算量减少$(n+2)T_H+(16.6n+201.2)T_{ML}$．因此，本文总的运算量共减少$(3n+2)T_H+(273.8n+32.2)T_{ML}$．由表2易见，与其他文献[10,18,20,21]相比，本文提出的方案具有最少的运算量，所需时间最短，且易于实现等优点．

表1: 各种密码体制下的操作运算转换关系

名称	含 义
T_H	执行Hash函数的时间复杂度
T_{EX}	执行模幂运算的时间复杂度
T_{ML}	执行模乘运算的时间复杂度
T_{HEM}	在超椭圆曲线上执行除子标量乘运算的时间复杂度
T_{HEA}	在超椭圆曲线上执行除子加法运算的时间复杂度

表 2: 已有文献和本文方案的运算量及运算时间复杂度的比较

方 案	运算量
文献 [10]	$4nT_{EX}+3nT_{ML}$
文献 [18] (有序)	$(0.5n^2+1.5n)T_H+6nT_{EX}+(1.5n^2+6.5n)T_{ML}$
文献 [18] (广播)	$3nT_H+(6n+3)T_{EX}+(11n-2)T_{ML}$
文献 [20]	$(4n+2)T_{EX}$
文献 [21]	$(2n+2)T_{EX}$
文献 [19] (有序)	$2nT_H+2nT_{EX}+nT_{ML}$
文献 [19] (广播)	$(n+2)T_H+(n+2)T_{EX}+(n+2)T_{ML}$
本文方案 (有序)	$(2n+3)T_{HEM}+2nT_{HEA}+(n+1)T_{ML}$
本文方案 (广播)	$(3n+3)T_{HEM}+(n+2)T_{HEA}+(n+2)T_{ML}$
方 案	运算时间复杂度
文献 [10]	$963nT_{ML}$
文献 [18] (有序)	$(0.5n^2+1.5n)T_H+(1.5n^2+1446.5n)T_{ML}$
文献 [18] (广播)	$3nT_H+(1451n+718)T_{ML}$
文献 [20]	$(960n+480)T_{ML}$
文献 [21]	$(480n+480)T_{ML}$
文献 [19] (有序)	$2nT_H+481nT_{ML}$
文献 [19] (广播)	$(n+2)T_H+(241n+482)T_{ML}$
本文方案 (有序)	$(223.8n+169)T_{ML}$
本文方案 (广播)	$(224.4n+280.8)T_{ML}$

6 结论

本文改进了文献 [10] 提出的结构化多重签名方案，将单一的有序多重签名和单一的广播多重签名相结合，提出改进的结构化多重盲数字签名方案．将签名结构从二层推广至三层，使有序和广播两者更好的结合，并给出各种情况下的具体算法，更符合实际应用中的签名结构．最后，在多重盲签名的安全模型下证明其安全性和盲性，并且分析和比较了改进方案与已有文献的计算效率，得出改进方案具有运算量低，所需时间少，且易于实现等优点．同时，改进方案具有高安全性能．

参考文献：

[1] Koblitz N. Hyperelliptic cryptosystems[J]. Journal of Cryptology, 1989, 1(3): 139-150

[2] Avanzi R, Cohen H, Doche C, *et al*. Handbook of Elliptic and Hyperelliptic Curve Cryptography[M]. Boca Raton: Chapman & Hall, 2005

[3] 李明，孔凡玉，朱大铭. 超椭圆曲线上Montgomery标量乘的快速计算公式[J]. 软件学报，2013, 24(10): 2275-2288
Li M, Kong F Y, Zhu D M. Fast addition formulae for Montgomery ladder scalar multiplication on hyperelliptic curves[J]. Journal of Software, 2013, 24(10): 2275-2288

[4] Li F G, Zhang M W, Takagi T. Identity-based partially blind signature in the standard model for electronic cash[J]. Mathematical and Computer Modeling, 2013, 58(1): 196-203

[5] Sergiu B, Hubert C L, Stephanie D. Deducibility constraints and blind signatures[J]. Information and Computation, 2014, 238(11): 106-127

[6] Harn L, Ren J. Efficient identity-based RSA multisignatures[J]. Computers & Security, 2010, 27(3): 12-15

[7] Islam S H, Biswas G P. Certificateless short sequential and broadcast multisignature schemes using elliptic curve bilinear pairings[J]. Journal of King Saud University–Computer and Information Sciences, 2014, 26(1): 89-97

[8] Wang B, Yang X D, Yang G. An Identity-based multisignature scheme from the weil pairing[C]// Proceedings of the 2010 International Conference on Computer Design and Applications (ICCDA 2010), 2010: 585-587

[9] Islam S H, Biswas G P. Certificateless strong designated verifier multisignature scheme using bilinear pairings[C]// Proceedings of the International Conference on Advances in Computing Communications and Informatics (ICACCI-2012), 2012: 540-546

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

[11] Yang S M, Wu H F, Li J Y. Access structures of hyperelliptic secret sharing schemes[J]. Finite Fields and Their Applications, 2016, 37(1): 46-53

[12] Tang C M, Xu M Z, Qi Y F. Faster pairing computation on genus 2 hyperelliptic curves[J]. Information Processing Letters, 2011, 111(10): 494-499

[13] You L, Sang Y X. 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

[14] Zhang D D, Ma Z F, Niu X X, *et al*. Secure and efficient anonymous proxy signature scheme in the random Oracle model[J]. The Journal of China Universities of Posts and Telecommunications, 2013, 20(4): 87-92

[15] 秦艳琳，吴晓平. 高效的无证书有序多重签名方案[J]. 通信学报，2013, 34(7): 105-110
Qin Y L, Wu X P. Efficient certificateless sequential multi-signature scheme[J]. Journal on Communications, 2013, 34(7): 105-110

[16] 许艳，黄刘生，田苗苗，等. 可证安全的高效无证书有序多重签名方案[J]. 通信学报，2014, 35(11): 126-131
Xu Y, Huang L S, Tian M M, *et al*. Provably secure and efficient certificateless sequential multi-signature scheme in random oracle model[J]. Journal on Communications, 2014, 35(11): 126-131

[17] David P, Jacques S. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396

[18] Hang H F, Chang C C. Multisignatures with distinguished signing authorities for sequential and broadcasting architectures[J]. Computer Standards & Interfaces, 2005, 27(2): 169-176

[19] Chu H W, Zhao Y L. Two efficient digital multisignature schemes[C]// Proceedings of the International Symposium on Computational Intelligence and Design (ISCISD' 08), 2008: 258-261

[20] Giri D, Srivastava P D. An improved efficient multisignature scheme in group communication sys-tems[C]// Proceedings of the 2007 International Conference on Advanced Computing and Communications (ICACC' 07), 2007: 447-543

[21] Yang F Y, Lo J H, Liao C M. Improvement of an efficient ID-based RSA multisignature[C]// Proceedings

of the International Conference on Complex, Intelligent and Software Intensive Systems, 2010: 822-826

[22] You L, Yang Y, Gao S, *et al*. Fast scalar multiplications on the curve $v^2 = u^p - au - b$ over the finite field of characteristic p[J]. Fundamenta Informaticae, 2014, 129(4): 395-412

Improved Structured Blind Multisignature Schemes Based on Hyperelliptic Curves

YANG Qing[1], XIN Xiao-long[2], LI Xiao-guang[1]

(1- Faculty of Science, Xi'an Aeronautical University, Xi'an 710077;
2- School of Mathematics, Northwest University, Xi'an 710069)

Abstract: Secure and efficient blind multisignature schemes have a number of important applications in electronic commerce and electronic cash systems. Structured multisignature algorithms by reference are analyzed and improved in this paper. We present fast and efficient structured blind multisignature schemes based on hyperelliptic curves. The signature structure is expanded from two levels to three levels, so both sequential and broadcast are better integration. And a variety of specific algorithms are given. Finally, the complexity and security of improved schemes are compared and analyzed. Comparing with current approaches, improved schemes reduce computation costs by $(3n + 2)TH + (273.8n + 32.2)TML$. The results show that improved schemes have the advantages of low computation complexity, low computation time, high security and easy to implement.

Keywords: hyperelliptic curve; reduced divisors; blind signature; structured; multisignature

Received: 18 Dec 2015. **Accepted:** 06 Sep 2016.

Foundation item: The Foundation of Science and Technology Department of Shaanxi Province (2013JM 1019; 2014K05-43); the Foundation of Shaanxi Provincial Education Department (14JK1310); the Research Program of Xi'an Aeronautical University (2015KY1218).