doi:10.3969/j.issn.1000-436x.2014.03.016

公平的多方并发签名方案

叶青[1,2]，杨赟[3]，郑世慧[2]，常利伟[2]，肖达[2]，杨义先[2,4]

(1. 河南理工大学 计算机科学与技术学院，河南 焦作 454000；2. 北京邮电大学 信息安全中心，北京 100876；
3. 铁道部信息技术中心，北京 100010；4. 北京邮电大学 灾备技术国家工程实验室，北京 100876)

摘 要：Tonien 等在 ISC2006 上首次提出了多方并发签名体制，但 Xie 和谭指出 Tonien 等的方案并不满足公平性，进而分别重新构造了多方并发签名方案。分别对 Xie 和谭的多方并发签名方案进行了分析，指出他们的方案也不满足公平性，进而正式定义了公平多方并发签名的安全模型，并基于双线性对及多方密钥协商技术重新构造了一个多方并发签名方案。分析表明，在随机预言模型下，假设 CDH 问题是难解的，新方案同时满足正确性、不可伪造性、模糊性、并发性和公平性，并且与同类方案相比，新方案在签名长度、计算量、通信代价方面效率较高。

关键词：多方并发签名；公平性；双线性对；随机预言模型

中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)03-0140-10

Fair multi-party concurrent signature scheme

YE Qing[1,2], YANG Yun[3], ZHENG Shi-hui[2], CHANG Li-wei[2], XIAO Da[2], YANG Yi-xian[2,4]

(1. College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454000, China;
2. Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China;
3. Information Technology Center, Ministry of Railways, Beijing 100010, China;
4. National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: Multi-party concurrent signatures were first proposed by Tonien *et al* at ISC2006, but Xie and Tan pointed Tonien *et al*'s scheme doesn't satisfy fairness and they reconstructed multi-party concurrent signature schemes respectively. Through analysis, the multi-party concurrent signature schemes proposed by Xie and Tan don't satisfy fairness either, so a formal security model of fair multi-party concurrent signatures was proposed and a multi-party concurrent signature scheme based on bilinear pairing and multi-party key agreement was also reconstructed. Analysis shows that the new scheme satisfies correctness, unforgeability, ambiguity, concurrency and fairness in the random oracle model assuming the CDH problem is intractable and highly efficient in signature size, computation cost and communication cost compared with other schemes of its kind.

Key words: multi-party concurrent signature; fairness; bilinear pairing; random oracle model

1 引言

并发签名是 2004 年 Chen 等[1]为了在电子商务中，在可信第三方不参与的情况下，公平高效地交换签名而提出的。自此以后，并发签名的研究成果层出不穷，但这些成果大部分都是研究两方并发签名[2~6]的情况，而对于用途更为广泛的多方并发签名，由于协议复杂、设计难度大等原因国内外的研究成果[7~10]并不多。

多方并发签名是 Tonien 等[7]在 ISC2006 上首次正式提出的。在这种签名体制中，每个交易参与方都需要选择一个秘密信息（个人密钥石），另外交易发起方还需选择一个群秘密信息（群密钥石）。各交易方首先产生并交换 n 个模糊（即签名者身份

收稿日期：2013-01-11；**修回日期**：2013-08-20

基金项目：国家自然科学基金资助项目(61003285, 61202082)；中央高校基本科研业务费专项基金资助项目(BUPT2012RC0219, BUPT2012RC0218)

Foundation Items: The National Natural Science Foundation of China (61003285, 61202082); The Fundamental Research Funds for the Central Universities(BUPT2012RC0219, BUPT2012RC0218)

不能确定）的签名，直到交易发起方公布群密钥石及其个人密钥石、其他参与方公布各自的个人密钥石，n 个模糊签名才与各自的签署方绑定成有效的签名。Tonien 等在文献[7]中，定义了这种签名体制应满足的安全属性，即正确性、不可伪造性、模糊性和公平性，并基于环签名[11]构造了第一个多方并发签名方案。

然而，Xie[8]指出 Tonien 等对于多方并发签名的模糊性和公平性定义存在问题，导致其设计的多方并发签名方案只要群密钥石和某个参与方 U_i 的个人密钥石一公布，U_i 的模糊签名即被绑定身份，而不必等到群密钥石和全部个人密钥石公布才被绑定。这种设计使得 U_j（$j\neq i$）在群密钥石和 U_i 的个人密钥石公布后，即得到了 U_i 的有效签名，那么接下来 U_j 完全有可能拒绝公布其个人密钥石而退出协议，这显然对 U_i 是不公平的。进而，Xie 修改了 Tonien 等对于多方并发签名模糊性和公平性的定义，并分别基于 RSA 签名和 Schnorr 签名重新设计了 2 个多方并发签名方案（Xie 方案 1 和 Xie 方案 2）。

Wang[9]注意到由于基于环签名[11]所设计，Tonien 等[7]方案中每个签名的长度与参与方的个数呈线性关系，即方案的签名总长度为 $O(n^2)$。进而，Wang 基于短环签名方案[12]设计了一个多方并发签名方案，该方案中每个签名的长度为常数，签名总长度仅为 $O(n)$。但是，Wang 并没注意到 Tonien 等方案存在的公平性问题，仍然沿用 Tonien 等的设计思路，即只要群密钥石和某个参与方 U_i 的个人密钥石一公布，U_i 的模糊签名即被绑定身份，所以 Wang 等的方案仍然存在和 Tonien 等相同的公平性问题。

谭肖[10]注意到了 Tonien 等方案存在的公平性问题，所以修改了 Tonien 等对于多方并发签名不可伪造性、模糊性、公平性的定义，并分别基于和谐签名体制[13]和分布式密钥生成[14]重新构造了 2 个多方并发签名方案（Tan 方案 1 和 Tan 方案 2）。

本文首先通过分析指出 Xie 对于多方并发签名的模糊性和公平性的定义是正确的，但其所提的 2 个方案却不满足其定义的模糊性和公平性，而谭不仅其所提的 2 个方案不满足公平性，而且其对多方并发签名的不可伪造性、模糊性和公平性的定义也都存在问题。进而，本文首次形式化定义了公平多方并发签名方案的安全模型，并基于双线性对和多方密钥协商技术[15]重新构造了一个多方并发签名方案。由于使用多方密钥协商技术取代环签名技术来构建方案，新方案不仅弥补了以往方案[7~10]的公平性缺陷，而且签名总长度仅为 $O(n)$，效率较高。

2　Xie、谭的多方并发签名方案及其公平性分析

2.1　Xie 的多方并发签名方案及其公平性分析

假设存在一组欲交换签名的用户 $U_1,U_2,\cdots,U_n$，每个 $U_i(i\in[1,n])$称为内部用户，$U_1,U_2,\cdots,U_n$ 以外的用户称为外部用户。Xie[8]提出的基于 RSA 签名的多方并发签名方案的基本算法如下。

1) 参数建立(Setup)：输入(l,n)，其中，l 为安全参数，n 为参与用户个数，该算法设置消息空间 $M=\{0,1\}^*$、密钥石空间 $K=Z$、密钥石固定空间 $\Phi=Z_l$；选取 3 个密码学散列函数 h_1：$\{0,1\}^*\rightarrow\Phi$，h_2，h_3：$K\rightarrow\Phi$，并令函数 Fgen=$h_2||h_3$；为每个用户 U_i 选择 2 个大素数 p_i, q_i(p_i 和 q_i 长度都为 l 位)，计算 $n_i=p_i q_i$，选择满足 $\gcd(e_i,\phi(n_i))=1$ 的整数 e_i，计算 $d_i=e_i^{-1}\bmod\phi(n_i)$，则 U_i 的私钥为 $sk_i=d_i$，公钥为 $pk_i=(n_i,e_i)$，其中，$1\leqslant i\leqslant n$。

2) 模糊签名算法(Asign)：输入$(m_i,f_1,f_2,\cdots,f_n,sk_i)$，其中，$m_i\in M$，$f_1,f_2,\cdots,f_n\in\Phi$，$sk_i$ 为用户 U_i 的私钥，该算法输出 U_i 关于消息 m_i 的签名 $\sigma_i=<v_i,x_i>$，其中，

$$v_i=h_1(m_i,r_i,f_1^{(L)},f_2^{(L)},\cdots,f_n^{(L)}),$$

$$x_i=(v_i\oplus r_i\oplus f_1^{(R)}\oplus f_2^{(R)}\oplus\cdots\oplus f_n^{(R)})^{d_i}\bmod n_i$$

其中，r_i 为在$[1,l-1]$上选取的随机数，$f_i^{(L)}=h_2(ik_i)$是 f_i 的左半部分，$f_i^{(R)}=h_3(ik_i)$是 f_i 的右半部分。

3) 内部验证算法(Iverify)：输入$(m_i,\sigma_i,pk_i,f_1,f_2,\cdots,f_n)$，其中，$m_i\in M$，$\sigma_i=<v_i,x_i>$，$pk_i$ 为用户 U_i 的公钥，$f_1,f_2,\cdots,f_n\in\Phi$，该算法计算

$$z_i=x_i^{e_i}\bmod n_i,$$

$$v_i'=h_1(m_i,z_i\oplus v_i\oplus f_1^{(R)}\oplus\cdots\oplus f_n^{(R)},f_1^{(L)},\cdots,f_n^{(L)})$$

检查如果 $v_i'=v_i$，则输出 accept，否则输出 reject，其中，$f_i^{(L)}=h_2(ik_i)$是 f_i 的左半部分，$f_i^{(R)}=h_3(ik_i)$是 f_i 的右半部分。

4) 绑定验证算法(Bverify)：输入$(pk_i,f_1,f_2,\cdots,f_n,ik_1,ik_2,\cdots,ik_n,(m_i,\sigma_i))$，其中，$pk_i$ 是用户 U_i 的公钥，$f_1,f_2,\cdots,f_n\in\Phi$，$ik_1,ik_2,\cdots,ik_n\in K$，$(m_i,\sigma_i)$是一对消息签名，该算法对所有的 $j=1,2,\cdots,n$，检查是否有 $f_j=$Fgen(ik_j)，如果前述验证有一项不通过，则输出 reject；否则，检查 Iverify$(m_i,\sigma_i,pk_i,f_1,f_2,\cdots,f_n)$=

accept，如果是，输出 accept，否则输出 reject。

基于 RSA 签名的多方并发签名方案的运作协议如下。

1) $U_1,U_2,\cdots,U_n$ 运行 Setup 算法，得到各自的公私钥对(pk_i,sk_i)和其他系统参数。

2) 每个用户 U_i 随机选择密钥石 $ik_i\in K$，并计算 $f_i=\text{Fgen}(ik_i)$，然后将 f_i 发送给所有其他参与方。

3) 每个 U_i 收集到所有 $f_1, f_2,\cdots, f_n$ 后，选择要签名的消息 $m_i\in M$，计算 $\sigma_i=\text{Asign}(m_i, f_1, f_2,\cdots, f_n, sk_i)$，并把$(m_i,\sigma_i)$发送给所有其他参与方。

4) 每个 U_i 收到其他参与方 U_j 的签名(m_j,σ_j)后，对于所有 $j=1,2,\cdots,n, j\neq i$，检查是否都有 $\text{iverify}(m_j, \sigma_j, pk_j, f_1, f_2,\cdots, f_n)=\text{accept}$，如果是，$U_i$ 公布 ik_i，否则 U_i 退出。

此时，任何收集到全部 ik 的人都可以通过检查是否 $\text{Bverify}(pk_i,f_1,f_2,\cdots,f_n,ik_1,ik_2,\cdots,ik_n,(m_i,\sigma_i))=$ accept 来绑定模糊签名(m_i,σ_i)的签署方。

由于 Xie 的基于 Schnorr 签名的多方并发签名方案与上述方案算法框架以及运作协议完全一样，区别仅在于基于的困难问题不同以及由此导致的算法实现细节的不同，所以在此不再介绍，详见文献[8]。

另外，在文献[8]中，Xie 要求公平的多方并发签名需要满足以下安全属性。

1) 正确性：模糊签名算法正确产生的签名，必然能通过内部验证算法和绑定验证算法的验证。

2) 不可伪造性：任何没有私钥 sk_i 的人不能伪造出能通过绑定验证算法验证的 U_i 的签名。

3) 模糊性：在所有参与方的密钥石 $ik_1,ik_2,\cdots,ik_n$ 未全部公布之前，任何外部用户不能识别出 U_i 签名的签署方。

4) 并发性：密钥石 $ik_1,ik_2,\cdots,ik_n$ 全部公布之后，所有模糊签名同时被绑定到各自的签署方。

5) 公平性：方案满足以上定义的正确性、不可伪造性、模糊性和并发性。

本文认为 Xie 关于多方并发签名的安全属性的定义，尤其模糊性和公平性的定义是正确的，但其提出的 2 个方案却不满足其定义的模糊性和公平性。原因在于 Xie 提出的 2 个方案的内部验证算法的输入参数中既无内部用户的私钥，也无其他的内部用户共享的秘密信息(f_i 在被 U_i 广播的过程中，可以被外部用户截获到，所以不是内部用户共享的秘密信息)，因此内部验证算法既可被内部用户正确调用执行，也可被外部用户正确调用执行。又由于内部验证算法具有识别模糊签名的签名者的功能（通过公钥的方式），所以在密钥石未公布之前，外部用户可以通过运行内部验证算法识别出模糊签名的签署方，从而方案不满足模糊性。假设某个 U_i 首先向其他参与方发出自己的签名，则由于此时 U_i 的签名已经与 U_i 绑定，其他参与方完全有可能拿到可绑定的 U_i 的签名后不再向 U_i 发出签名，这显然对 U_i 是不公平的，所以方案也不满足公平性。

2.2 谭的多方并发签名方案及其公平性分析

谭[10]提出的基于和谐签名体制的多方并发签名方案的基本算法如下。

1) 参数建立(Setup)：输入(l, n)，其中，l 为安全参数，n 为参与用户个数，该算法产生 2 个长度为 l 的大素数 p 和 q 满足 $q|p-1$；产生 Z_p^* 上的阶为 q 的生成元 g；设置消息空间 $M=\{0,1\}^*$、密钥石空间 $K=Z_q$、密钥石固定空间 $\Phi=Z_q\times Z_p$；选取 3 个密码学散列函数 $H_1:\{Z_p\}^n\times M\times Z_q\rightarrow Z_q$，$H_2: Z_p\times Z_p\times\{Z_q\}^n\rightarrow Z_p$，$H_3: Z_p\times M\rightarrow Z_q$；每个用户 U_i 的私钥 sk_i 随机从 Z_q 上选取，公钥 $pk_i=P_i=g^{ski}\bmod p$，其中，$1\leqslant i\leqslant n$，公钥组 $PK=(P_1, P_2,\cdots, P_n)$。

2) 密钥石产生算法(Kgen)：输入(m_i,PK)，其中，$m_i\in M$，PK 为用户公钥组，该算法随机选取密钥石 $ik_i\in K$，然后计算密钥石固定 $f_i=(s_i, t_i)$如下

$$s_i=H_1(PK\|m_i\|ik_i)$$

$$t_i=g^{iki}\bmod p$$

3) 模糊签名算法(Asign)：输入$(m_i,PK,f_1,f_2,\cdots,f_n, sk_i, ik_i)$，其中，$m_i\in M$，$PK$ 为用户公钥组，$f_1,f_2,\cdots, f_n\in\Phi$，$sk_i$ 是用户 U_i 的私钥，$ik_i\in K$，该算法计算 U_i 关于消息 m_i 的模糊签名 $\sigma_i=<u_i,v_i,(\varphi_{i,1}, \varphi_{i,2},\cdots, \varphi_{i,n})>$如下。

对 $j=1,2,\cdots,n$ 且 $j\neq i$，计算

$$\varphi_{i,j}=H_2(P_j^{iki}\|t_j^{ski}\|S)$$

然后计算

$$\varphi_{i,i}=P_i^{ik_i}/\prod_{j\neq i}\varphi_{i,j}$$

$$u_i=H_3(g^{r_i}(\prod_{j=1}^{n}\varphi_{i,j}), m_i)$$

$$v_i=(r_i-u_i)/sk_i\bmod q$$

其中，$S=(s_1, s_2,\cdots, s_n)$，r_i 是从 Z_q 上选取的随机数。

4) 外部验证算法(Overify)：输入$(m_i, \sigma_i, PK, f_1, f_2, \cdots, f_n)$，其中，$(m_i, \sigma_i)$是一对消息签名，$PK$ 是用户公钥组，$f_1, f_2,\cdots, f_n\in\Phi$，该算法检查是否 $u_i=$

$H_3(g^{u_i}P_i^{v_i}(\prod_{j=1}^{n}\varphi_{i,j}), m_i)$，如果等式成立，输出 accept；否则输出 reject。

5) 内部验证算法(iverify)：输入(m_i, σ_i, PK, f_1, f_2, …, f_n, sk_j, ik_j)，其中，(m_i,σ_i)是一对消息签名，PK 是用户公钥组，$f_1, f_2,\cdots, f_n\in\Phi$，$sk_j$ 是用户 U_j 的私钥，$ik_j\in K$，该算法对所有的 j=1,2,…,n, $j\neq i$，检查是否存在 $\varphi_{i,j}\neq H_2(t_i^{skj}\|P_i^{ikj}\|S)$，如果存在，输出 reject；否则，检查是否 $u_i=H_3(g^{u_i}P_i^{v_i}(\prod_{j=1}^{n}\varphi_{i,j}), m_i)$，如果等式成立，输出 accept；否则输出 reject，其中，$S=(s_1, s_2,\cdots, s_n)$。

6) 绑定验证算法(Bverify)：输入(PK,ik_1, ik_2,…, ik_n, $f_1, f_2,\cdots, f_n$, (m_1,σ_1), (m_2,σ_2),…,(m_n,σ_n))，其中 PK 为用户公钥组，$ik_1, ik_2,\cdots, ik_n\in K$，$f_1, f_2,\cdots, f_n\in\Phi$，($m_1$,$\sigma_1$), ($m_2$,$\sigma_2$),…, ($m_n$,$\sigma_n$)是一组模糊签名，该算法对于所有的 i = 1,2,…,n, 检查 $s_i=H_1(PK\|m_i\|ik_i)$是否成立，检查 $P_i^{ik_i}=\prod_{j=1}^{n}\varphi_{i,j}$ 是否成立。

对 j = 1, 2,…,n 且$j\neq i$，检查 $\varphi_{i,j}=H_2(P_j^{iki}\|P_i^{ikj}\|S)$ 是否成立，检查 $u_i=H_3(g^{u_i}\cdot P_i^{v_i}\cdot(\prod_{j=1}^{n}\varphi_{i,j}), m_i)$ 是否成立，如果上述检查均成立，则输出 accept；否则输出 reject，其中，$S=(s_1, s_2,\cdots,s_n)$。

基于和谐签名体制的多方并发签名协议如下。

1) $U_1,U_2,\cdots,U_n$ 运行 Setup 算法，得到各自的公私钥对(pk_i,sk_i)及 PK 等其他系统参数。

2) 每个用户 U_i 选择要签署的消息 $m_i\in M$，然后运行 Kgen(m_i,PK)产生自己的密钥石 ik_i 和对应的密钥石固定 f_i，并将 f_i 发送给所有其他参与方。

3) 每个 U_i 收集到所有 $f_1, f_2,\cdots, f_n$ 后，计算签名 σ_i =Asign(m_i,PK, $f_1, f_2,\cdots, f_n$, sk_i, ik_i)，并把(m_i,σ_i)发送给所有其他参与方；

4) 每个 U_i 收到其他参与方 U_j 的签名(m_j,σ_j)后，检查是否 Iverify(m_j,σ_j,PK,f_1,f_2,…,f_n,sk_i,ik_i)=accept，如果对于所有 j = 1,2,…,n, $j\neq i$，上述等式都成立，则 U_i 公布 ik_i，否则，U_i 退出。此过程中，外部用户可以通过检查是否 Overify(m_j,σ_j,PK,f_1,f_2,…,f_n) = accept 来验证签名(m_j,σ_j)的有效性。

所有的 ik 公布后，收集到全部 ik 的人都可以通过运行 Bverify(PK, ik_1, ik_2, …, ik_n, f_1, f_2, …, f_n, (m_1,σ_1), (m_2, σ_2),…, (m_n, σ_n))来绑定所有模糊签名的签署方。

谭提出的基于分布式密钥生成的多方并发签名方案的算法、协议与上述方案的算法、协议主体部分相同，不同之处在于前者由于利用分布式密钥生成协议[14]来解决 Tonien 方案的不公平问题，即 $U_1,U_2,\cdots,U_n$ 通过运行分布式密钥生成协议，使得每个用户 U_i 都掌握一个随机秘密 k 的影子碎片 ik_i，这样，当且仅当所有的 ik_i 都被正确公布，密钥 k 才得以恢复，模糊签名才得以绑定，任何一个用户 U_i 不公布其 ik_i，k 值都无法恢复，所有的模糊签名都无法绑定，所以导致了算法方面比后者增加了秘密分发和秘密重构的算法，协议方面比后者增加了秘密分发和秘密恢复的过程，详见文献[10]。

另外，在文献[10]中，谭要求公平的多方并发签名需要满足以下安全属性。

1) 正确性：模糊签名算法正确产生的签名，必然能通过内部验证算法、外部验证算法和绑定验证算法的验证。

2) 不可伪造性：对任意 2 个 U_u 和 U_v，任何其他用户无法向 U_u 伪造 U_v 的签名，即任何其他用户无法产生 U_v 的签名，并使该签名能通过 U_u 执行的内部验证算法的验证。

3) 模糊性：在 U_i 未公布其密钥石 ik_i 之前，任何外部用户不能证明 U_i 的签名是由 U_i 产生的。

4) 公平性：所有用户的密钥石产生算法和发布过程是相同的；如果存在用户 U_i 没有发布密钥石 ik_i，任何其他用户无法产生 ik_1, ik_2,…, ik_n 使得 Bverify (PK, ik_1, ik_2,…,ik_n, f_1, f_2,…, f_n, (m_1,σ_1), (m_2, σ_2),…, (m_n, σ_n))= accept；一旦所有用户发布了各自的密钥石，所有模糊签名将同时绑定身份。

本文认为谭关于公平多方并发签名安全属性的定义存在一些问题。具体地说，模糊性的定义方面，谭要求的是在 U_i 公布 ik_i 之前，任意外部用户无法绑定 U_i 的模糊签名的签署方，也就是说谭允许方案设计成一旦 U_i 公布 ik_i，即使其他用户 U_j 不公布 ik_j，U_i 的签名也可以被绑定。而这种设计和 Tonien 等的方案存在同样的公平性方面的问题，即若诚实的用户 U_i 公布了 ik_i，而不诚实的用户 U_j 拒绝公布 ik_j，那么不诚实的用户 U_j 手中将有诚实用户 U_i 的可绑定的签名，但诚实的用户 U_i 手中却没有可绑定的不诚实用户 U_j 的签名，这显然是不公平的。若想模糊性定义不会造成不公平的现象，应该使 U_i 签名的模糊与否与所有协议参与方的密钥石公布与否相关联，而不应只与 U_i 的密钥石公布与否相关联，即模糊性定义应改为“在所有参与方的密钥石 $ik_1,ik_2,\cdots,ik_n$ 未全部公布之前，任何外部用户不能识

别出 U_i 签名的签署方”；不可伪造性方面，举个反例，假设某个攻击者成功地向 U_u 伪造了 U_v 的签名，最差的后果是导致 U_u 公布 ik_u，但由于 U_v 不会公布 ik_v，所以（按照正确的模糊性定义）攻击者手中的 U_u、U_v 的模糊签名仍无法绑定，这对 U_u 和 U_v 并没有造成损失。即使这个攻击者也成功地向 U_v 伪造了 U_u 的签名，导致 U_v 也公布了 ik_v，进而导致攻击者手中的 U_u、U_v 的模糊签名都可以绑定到签署方，但由于此时 U_v 和 U_u 手中的签名也可绑定到签署方，所以这种情况对 U_v 和 U_u 也是没有损失的。以上例子说明谭关于多方并发签名不可伪造性的定义是不合适的，攻击者是否能伪造出通过内部验证算法验证的签名并不重要，重要的是保证攻击者无法伪造出能通过绑定验证算法验证的签名；公平性定义方面，应该将会影响到方案公平的各项指标都考虑进来，包括各参与方对密钥石的选择与公布应具有相等的控制权，方案应满足正确性、不可伪造性、模糊性以及在 $ik_1,ik_2,\cdots,ik_n$ 全部公布之后，所有的模糊签名应同时绑定。

另外，谭所提的 2 个方案也存在明显的模糊性和公平性方面的缺陷。首先其设计的在密钥石公布之前，供外部用户验证模糊签名的外部验证算法需要使用到签名者公钥 P_i，而并未使用其他用户公钥 $P_j(i,j\in\{1,2,\cdots,n\},j\neq i)$，这具有明显的区分性，这将造成在密钥石未公布之前，外部用户通过外部验证算法的验证过程即识别出模糊签名的签署方，所以签名方案并不满足模糊性，由 2.1 节中对 Xie 的多方并发签名方案公平性的分析可知，不满足模糊性的并发签名方案也不满足公平性。

3 公平的多方并发签名方案

借鉴前人[7~10]的经验，本文基于双线性对和多方密钥协商重新设计了一个公平的多方并发签名方案，在介绍具体方案之前，首先简单回顾双线性对的知识，至于多方密钥协商技术请参考文献[15]。

3.1 双线性对

设 G_1 是阶为素数 q、生成元为 P 的加法循环群，G_2 为具有相同阶 q 的乘法循环群。双线性对 $\hat{e}$：$G_1\times G_1\to G_2$ 具有下列性质的映射。

1) 双线性：对于所有的 $P,Q\in G_1$，$\alpha,\beta\in Z_q^*$，有 $\hat{e}(\alpha P,\beta Q)=\hat{e}(P,Q)^{\alpha\beta}$。

2) 非退化性：如果 P 是 G_1 的生成元，则 $\hat{e}(P,P)$ 是 G_2 的生成元。

3) 可计算性：对于所有的 $P,Q\in G_1$，存在有效的算法计算 $\hat{e}(P,Q)$。

在 G_1 中有以下数学困难问题定义。

计算性 Diffie-Hellman (CDH) 难题：已知(P,xP, yP)，其中，$x,y\in Z_q^*$且未知，计算 $xyP\in G_1$。

3.2 公平多方并发签名方案的形式化定义

公平的多方并发签名方案包含以下4个基本算法。

1) 参数建立：该算法为概率算法，输入(l,n)，其中，l 为安全参数，n 为参与用户个数，该算法设置消息空间 M，签名空间 Σ，密钥石空间 K，密钥石固定空间 Φ，密钥石固定加密空间 Φ'，Φ''，私钥空间 K_{sk}，并输出一个密钥石固定函数 Kgen：$K\to\Phi$，2 个密钥石固定加密函数 Enc_1：$\Phi\to\Phi'$，Enc_2：$\Phi\times\Phi\to\Phi''$，2 个密钥石固定解密函数 Dec_1：$\Phi\times K_{sk}\to\Phi$，Dec_2：$\Phi''\times\Phi\to\Phi$ 及其他系统参数 π。该算法同时输出每个参与用户的公钥 pk_i，每个用户自己保存私钥 sk_i，其中，$1\leqslant i\leqslant n$。

2) 模糊签名算法：该算法为概率算法，输入(m_i, sk_i, f_1, f_2, …, f_n)，其中 $m_i\in M$，sk_i 是用户 U_i 的私钥，f_1, f_2, …, $f_n\in\Phi$，该算法输出一个用户 U_i 关于消息 m_i 的模糊签名 $v_i\in\Sigma$。

3) 内部验证算法：该算法是确定算法，输入((m_i, v_i), pk_i, f_1, f_2,…, f_n)，其中，(m_i,v_i)是一对消息签名，pk_i 是用户 U_i 的公钥，f_1, f_2,…, $f_n\in\Phi$，该算法输出 accept 或者 reject。

4) 绑定验证算法：该算法是确定算法，输入(pk_i, ik_1, ik_2,…,ik_n, (m_i,v_i))，其中，pk_i 是用户 U_i 的公钥，ik_1,ik_2,…, $ik_n\in K$，(m_i,v_i)是一对消息签名，该算法输出 accept 或者 reject。

公平多方并发签名方案的运作协议如下。

1) U_1,U_2,…,U_n 运行 Setup 算法，得到各自的公私钥对(pk_i, sk_i)和其他系统参数。

2) 每个用户 U_i 随机选择密钥石 $ik_i\in K$，并计算密钥石固定 f_i=Kgen(ik_i)，然后计算 $r_i=\text{Enc}_1(f_i)$，并将 r_i 发送给 U_{i+1}（其中，U_n 将 r_n 发送给 U_1）。

3) 每个用户 U_i 收到 r_{i-1} 后，首先计算 $f_{i-1}=\text{Dec}_1(r_{i-1},sk_i)$，然后计算 $w_i=\text{Enc}_2(f_i,f_{i-1})$，并将 w_i 发送给所有其他参与方。

4) 每个用户 U_i 收到 $w_j(j\neq i)$后，分别计算 $f_{i+1}=\text{Dec}_2(w_{i+1},f_i)$，$f_{i+2}=\text{Dec}_2(w_{i+2},f_{i+1})$,…, 直到 U_i 拥有所有的 $f_1,f_2,\cdots,f_n$。

5) 每个 U_i 选择要签名的消息 $m_i\in M$，并计算对应的模糊签名 v_i =Asign(m_i, sk_i, f_1, f_2,…, f_n)，然后

把(m_i,v_i)发送给其他参与方。

6) 每个 U_i 收到其他参与方 U_j 的签名(m_j, v_j)后，检查是否 Iverify((m_j, v_j), pk_j, f_1, f_2,…, f_n)=accept，如果对于所有 j=1, 2,…, n, $j\neq i$，该等式都成立，则 U_i 公布 ik_i，否则，U_i 退出。

此时，任何收集到全部的 ik 的人都可以通过检查是否 Bverify(pk_i, ik_1, ik_2,…, ik_n, (m_i, v_i))=accept 来绑定模糊签名(m_i, v_i)的签署方，其中，$1\leqslant i\leqslant n$。

3.3 安全模型

1) 正确性

正确性要求模糊签名算法正确产生的签名，必然能通过内部验证算法和绑定验证算的验证，即：如果 v_i=Asign(m_i,sk_i, f_1, f_2,…, f_n)，则有 Iverify((m_i, v_i), pk_i, f_1, f_2,…, f_n)=accept；另外，如果对于 $1\leqslant j\leqslant n$，有 f_j=Kgen(ik_j), $ik_j\in K$，则有 Bverify(pk_i, ik_1, ik_2, …, ik_n, (m_i,v_i))=accept。

2) 不可伪造性

不可伪造性要求任何没有私钥 sk_i 的人不能伪造出能通过绑定验证算法验证的 U_i 的签名。下面通过一个攻击者 A 与挑战者 C 之间的游戏来定义多方并发签名方案的不可伪造性。

初始：C 输入某个给定的安全参数 l 运行 setup 算法，并将得到的系统参数以及参与用户的公钥 {pk_i}给 A。

接下来，A 可以对 C 进行以下询问。

私钥询问：A 可以询问任一参与用户的公钥 pk_i 对应的私钥，作为回应，C 返回 sk_i。

散列函数询问：A 可以询问任意输入的散列函数值，C 计算出该输入对应的散列函数值并将结果返回给 A。

密钥石固定询问：A 可以要求 C 选择一个密钥石 $ik_i\in K$，并返回 ik_i 对应的密钥石固定值 f_i=Kgen(ik_i)。A 也可以自己选择密钥石 $ik_i\in K$，然后对 ik_i 进行密钥石固定询问得到 f_i=Kgen(ik_i)。

密钥石询问：A 可以询问某个 $f_i\in\Phi$ 对应的密钥石，如果该 f_i 是以前某个密钥石固定询问的输出，C 返回对应的 ik_i，如果不是，C 返回 invalid。

签名询问：A 可以询问元组 (m,pk_i,f_1,f_2,…,f_n)对应的签名，其中，$m\in M$, pk_i 为签名者公钥，f_1, f_2,…, $f_n\in\Phi$，作为回应，C 首先对 pk_i 进行私钥询问，然后计算 v=Asign(m,sk_i,f_1,f_2,…,f_n)，并将 v 返回给 A。

输出：最终，A 输出一个元组(m_a,v_a)，其中，$m_a\in M$, $v_a\in\Sigma$，一组 ik_1, ik_2, …, $ik_n\in K$ 以及身份 a。如果 Bverify(pk_a,ik_1,ik_2,…,ik_n,(m_a,v_a))=accept，并且 A 没有对 pk_a 进行私钥询问，也从没对(m_a, pk_a, f_1, f_2,…, f_n)(其中，f_j=Kgen(ik_j))进行过签名询问，则称 A 赢得游戏。

定义 1　如果不存在多项式有界的攻击者以不可忽略的概率赢得以上游戏，则称一个多方并发签名方案在选择消息攻击下是存在不可伪造的。

3) 模糊性

模糊性要求在所有参与方的密钥石 ik_1, ik_2,…, ik_n 未全部公布之前，任何外部用户不能识别出 U_i 签名的签署方。下面通过一个攻击者 A 与挑战者 C 之间的游戏来定义多方并发签名方案的模糊性。

初始：同不可伪造性游戏。

阶段 1：A 进行了一系列的私钥询问、散列函数询问、密钥石固定询问、密钥石询问、签名询问，C 的回应方式与不可伪造性游戏中的相同。

挑战：A 选择一个挑战元组(pk_1, pk_2, …, pk_n, m)，其中 pk_1, pk_2,…, pk_n 是参与用户的公钥，$m\in M$，作为回应，C 随机选择 ik_1, ik_2,…, $ik_n\in K$，并且对于 $1\leqslant i\leqslant n$，计算 f_i= Kgen(ik_i)，然后 C 随机选择一个 $b\in$ {1, 2, …, n}，当 b=j 时，C 计算 v=Asign(m, sk_j, f_1, f_2,…, f_n)并输出 v。

阶段 2：A 可以对 C 再次进行阶段 1 中的一系列的询问，C 的回应方式同阶段 1。

输出：最终，A 输出 $b'\in$ {1,2,…, n}作为对 b 的估计值，如果 b'=b 且 A 没有对全部的 f_1, f_2,…, f_n 进行密钥石询问，则称 A 赢得游戏。

定义 2　如果不存在多项式有界的攻击者以不可忽略的大于 1/n 的概率赢得以上游戏，则称一个多方并发签名方案满足模糊性。

4) 并发性

并发性要求在密钥石 ik_1,ik_2,…,ik_n 全部公布之后，所有模糊签名同时绑定身份。下面仍然通过一个攻击者 A 与挑战者 C 之间的游戏来定义多方并发签名方案的并发性。

初始：同不可伪造性游戏。

私钥询问、散列函数询问、密钥石固定询问、密钥石询问、签名询问：C 回应这些询问的方式同不可伪造性游戏。

输出：最终，A 选择挑战公钥 pk_1, pk_2,…, pk_n，并输出一组 ik_1, ik_2,…, $ik_n\in K$，一组 f_1, f_2,…, $f_n\in\Phi$ 以及一组(m_1,v_1),(m_2,v_2),…,(m_n, v_n)，其中 $m_i\in M$, $v_i\in\Sigma$。如果对于某个元组(m_i, v_i)，有 Iverify((m_i, v_i), pk_i, f_1,

$f_2,\cdots, f_n$)=accept 且 Bverfiy(pk_i, ik_1, ik_2, …, ik_n, (m_i, v_i))= accept，而对于另一元组(m_j, v_j)，有 Iverify((m_j, v_j), pk_j, f_1, f_2, …, f_n)=accept，但 Bverfiy(pk_j, ik_1, $ik_2,\cdots,ik_n$, (m_j, v_j))=reject，则称 A 赢得游戏。

定义 3 如果不存在多项式有界的攻击者以不可忽略的概率赢得以上游戏，则称一个多方并发签名方案满足并发性。

5) 公平性

定义 4 如果一个多方并发签名方案中各参与方对密钥石的选择与公布具有相等的控制权，且方案满足以上定义的正确性、不可伪造性、模糊性、并发性，则称该方案为公平的多方并发签名方案。

3.4 一个公平的多方并发签名方案

本文基于双线性对提出一个具体的公平多方并发签名方案，该方案的算法如下。

1) Setup(l, n)

选择符合 3.1 节中定义的(G_1,G_2,$\hat{e}$,q,P)。

设置 M=K={0,1}*，Σ=G_1，Φ'=Φ''=Φ=Z_q，K_{sk}=Z_q^*。

随机选择 U_i 的私钥 $sk_i\in Z_q^*$，计算 U_i 的公钥为 pk_i= P_i= sk_iP，其中，$1\leqslant i\leqslant n$。

选取 3 个抗碰撞的散列函数 H_1：{0,1}$^*\rightarrow Z_q$，H_2：{0,1}$^*\times Z_q\rightarrow G_1$，$H_3$：$G_1\rightarrow Z_q$。

令 Kgen=H_1，$\mathrm{Enc}_1(f_i,k_i,P_{i+1})=f_i+H_3(k_iP_{i+1})$(其中，$k_i$ 为 Z_q^*上选取的随机数且 $K_i=k_iP$,P_{i+1} 是用户 U_{i+1} 的公钥)，$\mathrm{Enc}_2(f_i,f_{i-1})=f_i-f_{i-1}$, $\mathrm{Dec}_1(r_{i-1},sk_i,K_{i-1})=r_{i-1}-H_3(sk_iK_{i-1})$，$\mathrm{Dec}_2(w_{i+1},f_i)=w_{i+1}+f_i$。

2) Asign(m_i, sk_i, f_1, f_2,$\cdots$, f_n)：

v_i= $sk_iH_2[m_i\,\|\,(f_1+f_2+\cdots+f_n)]$

3) Iverify(m_i, v_i, p_i, f_1, f_2,$\cdots$, f_n)

如果 $\hat{e}(P,\ v_i)=\hat{e}(P_i,H_2[m_i\,\|\,(f_1+f_2+\cdots f_n)])$，则输出 accept，否则输出 reject。

4) Bverify(p_i,ik_1,ik_2,$\cdots$,ik_n,(m_i,v_i))

验证是否 $\hat{e}(P,v_i)=\hat{e}(P_i,H_2[m_i\|(H_1(ik_1)+H_1(ik_2)+\cdots+H_1(ik_n))])$，如果等式成立，则输出 accept，否则输出 reject。

4 安全性分析

下面用几个定理及其详细的证明来展示 3.4 节中所提方案满足 3.3 节中定义的正确性、不可伪造性、模糊性、并发性和公平性。

定理 1 所提方案满足正确性。

证明 假设模糊签名 v_i=Asign(m_i, sk_i, f_1, f_2,$\cdots$, f_n)，则有 $v_i=sk_iH_2[m_i\,\|\,(f_1+f_2+\cdots+f_2)]$，所以

$$\begin{aligned}\hat{e}(P,v_i)&=\hat{e}(P,sk_iH_2\left[m_i\,\|\,\left(f_1+f_2+\cdots+f_2\right)\right])\\&=\hat{e}(sk_iP,H_2\left[m_i\,\|\,\left(f_1+f_2+\cdots+f_2\right)\right])\\&=\hat{e}(P_i,H_2[m_i\,\|(f_1+f_2+\cdots f_n)])\end{aligned}$$

另外，如果对于 $1\leqslant j\leqslant n$，有 $f_j=H_1(ik_j)$，$ik_j\in K$，必然有 $\hat{e}(P,v_i)=\hat{e}(P_i,H_2\ [m_i\ \|(H_1(ik_1)+H_1(ik_2)+\cdots+H_1(ik_n))])$。

定理 2 假设 G_1 群上 CDH 难题是(ε',t')难解的，则所提方案在选择消息攻击下是(ε,t)存在不可伪造的。其中，ε, ε'表示概率，t, t'表示时间且 $\varepsilon\geqslant\varepsilon'(q_s+n)$，$t\leqslant t'-\mathrm{T_s}\,(q_2+2q_s+1)-T_m-T_i$，$q_s$ 表示攻击者最多可询问签名预言机的次数，q_2 表示攻击者最多可询问 H_2 的次数，n 为所提协议参与方个数，T_s 表示 G_1 群上标量乘法运算所花费的时间，T_m 表示 Z_q^*上乘法运算花费的时间，T_i 表示 Z_q^*上求逆运算所花费的时间。

证明 假设存在一个(ε,t)攻击者 A 赢得了 3.3 节中的不可伪造性游戏，接下来将展示存在另一个(ε',t')算法 C 能够利用 A 的攻击成果解决 G_1 群上 CDH 难题，即给定(P, xP, yP)，C 能计算出 xyP。令 X_a = {1,2,$\cdots$,n}\{a}。C 将模拟不可伪造性游戏中的挑战者与 A 交互如下。

初始：C 输入给定的参数(l,n)运行 Setup 算法。值得注意的是，对于每个用户 $U_i(i\in X_a)$，C 随机选择其私钥 $sk_i\in Z_q^*$，并计算其公钥 $P_i=sk_iP$，而对于用户 U_a，C 随机选择 $s\in Z_q^*$，并计算其公钥 $P_a=sxP$。C 将{P_1,P_2,$\cdots$,P_n}以及其他系统参数给 A。

接下来，C 回答 A 的各种询问如下。

1) 私钥询问：当 A 询问 $P_i(i\in X_a)$对应的私钥时， C 返回 sk_i，否则，C 返回 Invalid。

2) H_1、H_3 询问：关于 A 对 H_1 的询问，C 为其建立一个 H_1-list 列表。当 A 询问 H_1 时，C 随机选择 $t\in Z_q$，输出 t 并将输入和对应 t 值保存到 H_1-list 中；如果输入是 H_1-list 中已经记录的，则 C 在 H_1-list 中找到该输入对应的 t 值并输出。关于 A 对 H_3 的询问，C 也采用类似的操作方式。

3) H_2 询问：关于 A 对 H_2 的询问，C 为其建立一个元组为<m_i||K_i, t_i, c_i>的 H_2-list 列表，当 A 输入一个 m||K 时，其中 $m\in M$，$K\in Z_q$，C 操作如下。

① 查询 m||K 是否已存在于 H_2-list 的某个记录<m||K, t, c>中，如果存在，查看对应的 c 值是否为 0，如果是，则输出 tyP，如果为 1，则输出 tP；如不

存在，则继续。

② 产生一个随机的硬币 $c\in\{0,1\}$，并令 $\Pr[c=0]=1/(q_s+n)$。

③ 选择一个随机数 $t\in Z_q^*$，如果 $c=0$，输出 tyP，如果 $c=1$，输出 tP，并将$<m\|\|K,t,c>$存入 H_2-list 中。

4) 密钥石固定询问：C 为 A 进行该询问建立一个元组为$<ik_i,f_i>$的 I-list 列表。当 A 进行该询问时，C 随机选择一个密钥石 $ik_i\in K$ 并计算 $f_i=H_1(ik_i)$，输出 f_i 并将$<ik_i,f_i>$添加到 I-list 中。

5) 密钥石询问：当 A 询问某个 $f_i\in F$ 对应的密钥石时，C 查询 I-list 中是否存在某个元组$<ik_i,f_i>$，如果存在，C 返回 ik_i，如果不存在，C 返回 invalid。

6) 签名询问：当 A 输入$(m,P_i,f_1,f_2,\cdots,f_n)$进行签名询问时，其中 $m\in M$, P_i 为签名者公钥，$f_1,f_2,\cdots,f_n\in\Phi$，$C$ 操作如下：如果 $i\in X_a$，C 首先对 P_i 进行私钥询问，然后计算 $v=\text{Asign}(m,sk_i,f_1,f_2,\cdots,f_n)$，并将 v 返回给 A；如果 $i=a$，C 首先计算 $K=f_1+f_2+\cdots+f_n$，然后以 $m\|\|K$ 为输入进行 H_2 询问，假设得到对应的元组为$<m\|\|K,t,c>$，若 $c=0$，则 C 停止，即 C 不能够返回 U_a 的签名；若 $c=1$，则 C 返回 U_a 的签名为 $v=tP_a$。

假设 A 通过上述询问以及自己的计算伪造出了 U_a 的签名(m_a,v_a)以及一组密钥石 $ik_1,ik_2,\cdots,ik_n$ 满足 $\text{Bverify}(P_a,ik_1,ik_2,\cdots,ik_n,(m_a,v_a))=\text{accept}$，并且 A 没有对 P_a 进行私钥询问，也从没对 m_a, P_a, f_1, $f_2,\cdots,f_n$(其中 $f_j=H_1(ik_j)$)进行过签名询问。

由于 $\text{Bverify}(P_a,ik_1,ik_2,\cdots,ik_n,(m_a,v_a))=\text{accept}$，所以有 $\hat{e}(P,v_a)=\hat{e}(P_a,H_2[m_a\|(H_1(ik_1)+H_1(ik_2)+\cdots+H_1(ik_n))])$。由于 H_2 的输出是完全随机的，所以若要上述等式成立，A 必然需要借助于相关的签名询问或者 A 直接对 $m_a\|(H_1(ik_1)+H_1(ik_2)+\cdots+H_1(ik_n))$ 进行 H_2 询问。假设 A 进行过以 m_a 与一组密钥石 $f_1',f_2',\cdots,f_n'$ 为输入的签名询问，其中，$f_j'=H_1(ik_j')$，$\{ik_1',ik_2',\cdots,ik_n'\}$是不等于$\{ik_1,ik_2,\cdots,ik_n\}$的另外一组密钥石的集合，并假设 A 以$(m_a,f_1',f_2',\cdots,f_n')$为输入的签名询问，在 H_2-list 中产生的记录为$<m_a\|\|K_a,t_a,c_a>$，其中，$K_a=f_1'+f_2'+\cdots+f_n'$，由散列函数单向性可知，不可能由 K_a 反解出另外一组密钥石 $ik_1,ik_2,\cdots,ik_n$，使 $K_a=H_1(ik_1)+H_1(ik_2)+\cdots+H_1(ik_n)$，所以 A 能伪造成功不可能是借助于签名询问，因而推断 A 必然进行过以 $m_a\|\|K_a$ 为输入的 H_2 询问，其中 $K_a=H_1(ik_1)+H_1(ik_2)+\cdots+H_1(ik_n)$。假设该 H_2 询问，在 H_2-list 中产生对应的记录为$<m_a\|\|K_a,t_a,c_a>$。若 $c_a=1$，则 C 停止，即 C 不能解决 G_1 的 CDH 难题；若 $c_a=0$，则意味着对于 $m_a\|\|K_a$ 的询问，H_2 的返回值为 t_ayP，另外注意到 $P_a=sxP$，所以等式 $\hat{e}(P,v_a)=\hat{e}(P_a,H_2[m_a\|(H_1(ik_1)+H_1(ik_2)+\cdots+H_1(ik_n))])$ 相当于 $\hat{e}(P,v_a)=\hat{e}(sxP,t_ayP)$，即 $\hat{e}(P,v_a)=\hat{e}(P,st_axyP)$，进而 $v_a=st_axyP$，因为对于 C 来说，s 和 t_a 是已知的，所以 C 可计算出 $xyP=(st_a)^{-1}v_a$，即 C 解决了 G_1 群的 CDH 难题。

下面来讨论在上述游戏中，C 成功解决 CDH 难题的概率。首先定义下面 3 个事件。

ξ_1：A 的签名询问未造成 C 停止。

ξ_2：A 成功伪造出 U_a 的签名和对应的密钥石，并且 A 没有对 P_a 进行私钥询问，该签名也不是签名询问的输出结果。

ξ_3：ξ_2 发生，且 $c_a=0$。

C 解决 CDH 难题相当于以上 3 事件同时发生，所以 C 解决 CDH 难题的概率为 $\Pr[\xi_1\wedge\xi_2\wedge\xi_3]=\Pr[\xi_1]\Pr[\xi_2|\xi_1]\Pr[\xi_3|\xi_2\wedge\xi_1]$。

命题 1　A 的签名询问未造成 C 停止的概率大于等于 $[1-1/(q_s+n)]^{q_s}$，即 $\Pr[\xi_1]\geqslant[1-1/(q_s+n)]^{q_s}$。

证明　假设 A 对 C 进行了 $l(l\in[1,q_s])$次签名询问，令 $A_j(j\in[1,l])$表示事件“A 的第 j 次签名询问没造成 C 停止”，则事件“A 第 l 次签名询问后 C 不停止”等价于事件 $A_1,A_2,\cdots,A_l$ 同时发生，所以其发生概率等于 $\Pr(A_1\wedge A_2\wedge\cdots\wedge A_l)$。不失一般性，假设 A 每次签名询问输入的消息都是不同的，则 $A_1,A_2,\cdots,A_l$ 为相互独立事件，因而 $\Pr(A_1\wedge A_2\wedge\cdots\wedge A_l)=\Pr(A_1)\Pr(A_2)\cdots\Pr(A_l)$。由于每个 A_j 发生的概率即为 $c_j=1$ 的概率，所以 $\Pr(A_1\wedge A_2\wedge\cdots\wedge A_l)=\Pr(A_1)\Pr(A_2)\cdots\Pr(A_l)=\Pr[c_1=1]\Pr[c_2=1]\cdots\Pr[c_l=1]=[1-1/(q_s+n)]^l$。由于假设允许 A 最多可进行签名询问 q_s 次，所以 A 的签名询问未造成 C 停止的概率最小为 $[1-1/(q_s+n)]^{q_s}$，即 $\Pr[\xi_1]\geqslant[1-1/(q_s+n)]^{q_s}$。

命题 2　若 A 的签名询问没有造成 C 停止，则 C 提供给 A 的资源和实际攻击中 A 可获得的资源没有区别，因此，$\Pr[\xi_2|\xi_1]\geqslant\varepsilon$。

证明　略。

命题 3　在 A 进行成功的伪造后，C 不停止的概率等于 $1/(q_s+n)$，即 $\Pr[\xi_3|\xi_2\wedge\xi_1]=1/(q_s+n)$。

证明　前面分析过，若能伪造成功，A 必进行过以 $m_a\|\|K_a$ 为输入的 H_2 询问，其中，$K_a=H_1(ik_1)+H_1(ik_2)+\cdots+H_1(ik_n)$。假设该 H_2 询问，在 H_2-list 中产生对应的记录为$<m_a|K_a,t_a,c_a>$，则 C 不停止的概率即为 $c_a=0$ 的概率，所以为 $1/(q_s+n)$。

综上，C 解决 G_1 上 CDH 难题的概率为 $\Pr[\xi_1 \wedge \xi_2 \wedge \xi_3]=\Pr[\xi_1]\Pr[\xi_2|\xi_1]\Pr[\xi_3|\xi_2 \wedge \xi_1] \geqslant [1-1/(q_s+n)]^{q_s} \varepsilon [1/(q_s+n)]$。令 $[1-1/(q_s+n)]^{q_s} \varepsilon [1/(q_s+n)] \geqslant \varepsilon'$，解得 $\varepsilon \geqslant \varepsilon'(q_s+n)[(q_s+n)/(q_s+n-1)]^{q_s} \geqslant \varepsilon'(q_s+n)$。

算法 C 的运行时间等于 C 回应 A 各种询问所花费的时间、A 的运行时间以及 C 将 A 的伪造成果转化为 CDH 问题的解所花费的时间三者之和。C 回应每个 H_2 询问需要计算一次 G_1 上的标量乘法，回应每个签名询问需要计算两次 G_1 上的标量乘法。C 将 A 的伪造成果转化为 CDH 问题的解需要计算一次 Z_q^* 上的乘法、一次 Z_q^* 上的求逆运算、一次 G_1 上的标量乘法。用 T_s 表示 G_1 上的标量乘法运算所花费的时间，T_m 表示 Z_q^* 上的乘法运算所花费的时间，T_i 表示 Z_q^* 上求逆运算所花费的时间，则算法 C 的运行时间最长为 $t+T_s(q_2+2q_s+1)+T_m+T_i$。令 $t+T_s(q_2+2q_s+1)+T_m+T_i \leqslant t'$，解得 $t \leqslant t'-T_s(q_2+2q_s+1)-T_m-T_i$。定理 2 证毕。

定理 3 随机预言模型下，所提方案满足模糊性。

证明 假设存在一个多项式有界的攻击者 A 以不可忽略的大于 $1/n$ 的概率赢得了 3.3 节中的模糊性游戏。该游戏中，挑战者 C 的操作与定理 2 证明中不同的是：C 随机选择每个用户 U_i 的私钥 $sk_i \in Z_q^*$，计算 U_i 的公钥 $P_i=sk_iP$，其中，$1 \leqslant i \leqslant n$，并且 C 用相关用户的私钥来回答 A 的私钥询问和签名询问，用常规方式来回答 A 的其他询问。A 最终能以不可忽略的大于 $1/n$ 的概率赢得该游戏，则意味着 A 以不可忽略的概率找到了一组 $ik_1,ik_2,\cdots,ik_n \in K$ 满足 $H_1(ik_i)=f_i(1 \leqslant i \leqslant n)$，又由于仅允许 A 对 $f_1,f_2,\cdots,f_n$ 中的部分值进行密钥石询问，所以可以推断出：A 通过自己的计算（而不是通过密钥石询问）至少以不可忽略的概率找到一个 $ik_c \in K$ 满足 $f_c=H_1(ik_c)$ $(c \in \{1,2,\cdots,n\})$。而随机预言模型下，A 成功找到这样的 ik_c 的概率是可忽略的，这与假设 A 以不可忽略的概率赢得了模糊性游戏矛盾，因而方案满足模糊性。

定理 4 随机预言模型下，所提方案满足并发性。

证明 假设存在一个多项式有界的攻击者 A 以不可忽略的概率赢得了 3.3 节中的并发性游戏。在该游戏中，挑战者 C 产生用户公私钥以及回应 A 的各种询问的方式同定理 3 的证明。A 最终能输出某个签名 (m_i,v_i)，满足 $\text{Iverify}((m_i, v_i), pk_i, f_1, f_2, \cdots, f_n)=\text{accept}$ 和 $\text{Bverfiy}(pk_i, ik_1, ik_2,\cdots,ik_n,(m_i, v_i))=\text{accept}$，随机预言模型下，必然得出 $f_i=H_1(ik_i)(1 \leqslant i \leqslant n)$，又由于 A 输出另一个签名 (m_j, v_j) 满足 $\text{Iverify}((m_j, v_j), pk_j, f_1, f_2, \cdots, f_n)=\text{accept}$，那么必然有 $\text{Bverfiy}(pk_j, ik_1, ik_2,\cdots,ik_n,(m_j, v_j))=\text{accept}$，而这与假设中的 $\text{Bverfiy}(pk_j, ik_1, ik_2,\cdots, ik_n,(m_j, v_j))=\text{reject}$ 矛盾。因而，假设不成立，方案满足并发性。

定理 5 随机预言模型下，假设 CDH 问题是难解的，所提方案满足公平性。

证明 所提方案中每个协议参与方 U_i 可以选择自己的密钥石 ik_i，并可以自己决定 ik_i 的公布时间，而且由定理 1~定理 4 可得，方案满足公平性。

5 效率分析

表 1 将本文所提方案与 Tonien 等[7]、Xie[8]、谭肖[10]的方案以及 2012 年 Huang 等[16]提出的高效的乐观公平交换协议进行效率比较。这里的“签名总长度”比较的是方案中 n 个参与方产生的总签名长度。“签名计算量”和“内部验证计算量”比较的是方案产生一个签名和内部验证一个签名需要的计算量，“绑定验证总计算量”比较的是方案中绑定 n 个模糊签名的签署方需要的计算量，这里比较的运算主要包括耗时较长的乘幂运算(E)、G_1 群上的标量乘法运算(S)、双线性对运算(P)以及映射到

表 1 几种签名公平交换方案的效率比较

方案	签名总长度	签名计算量	内部验证计算量	绑定验证总计算量	通信代价
Tonien 方案	$O(n^2)$	$(n-1)$P+$(n-1)$E+$(n-1)$H+$(n+1)$S	3P+E+H+nS	4nP+nH+ (n^2+n)S	$O(n^2)$
Xie 方案 1	$O(n)$	E	E	nE	$O(n)$
Xie 方案 2	$O(n)$	E	2E	2 nE	$O(n)$
Tan 方案 1	$O(n^2)$	2nE	2nE	$(2n^2+n)$E	$O(n^2)$
Tan 方案 2	$O(n^2)$	2nE	2nE	2n^2E	$O(n^2)$
Huang 方案	$O(n)$	(2n+11)S	2P +nS	5nP + 2n^2S	$O(n)$
本文方案	$O(n)$	H+S	2P+H	2nP+nH	$O(n)$

点的散列运算(H)，相对于这些运算，其他普通运算可忽略不计。“通信代价”主要比较各方案中需要广播的数据长度，假设广播一个 ik_i 或 f_i 的通信代价为 1，广播一个签名的通信代价取决于签名的长度，例如，广播一个长度为 n 的签名的通信代价为 n。

从表 1 看出，在签名总长度和通信代价方面，Xie 的方案、Huang 等的方案和本文方案随着方案参与人数的增加呈线性增长，而其他方案则随着方案参与人数的增加呈二次方增长；在签名计算量和内部验证计算量方面，Xie 的方案和本文方案的计算量为常数，不随方案参与人数的增加而增加，而其他方案的计算量则随着参与人数的增加呈线性增长；在绑定验证总计算量方面，Xie 的方案和本文方案的计算量随着方案参与人数的增加呈线性增长，而其他方案的计算量则随着参与人数的增加呈二次方增长。因此，本文所提方案是一个效率较高的公平的多方并发签名方案。

6　结束语

Tonien 等在 ISC2006 上首次提出了多方并发签名体制，但 Xie 和谭指出 Tonien 等的方案并不满足公平性并分别重新构造了多方并发签名方案。本文对 Xie 和谭提出的方案分别进行了分析，指出他们的方案也和 Tonien 等的方案一样存在公平性方面的缺陷。进而，本文形式化定义了公平多方并发签名的安全模型，并基于双线性对和多方密钥协商技术重新设计了一个多方并发签名方案。经分析，随机预言模型下，假设 CDH 问题是困难的，该签名方案满足多方并发签名所要求的各种安全性质，并且与同类方案相比效率较高。

参考文献：

[1] CHEN L, KUDLA C, PATERSON K G. Concurrent signatures[A]. Eurocrypt 2004[C]. Spriger-Verlag, Berlin, 2004. 287-305.

[2] SUSILO W, MU Y, ZHANG F. Perfect concurrent signatures schemes [A]. ICICS’04[C]. Malaga, Spain, 2004. 14-26.

[3] WANG G L, BAO F, ZHOU J Y. The fairness of perfect concurrent signatures[A]. ICICS’06[C]. Springer, Berlin, 2006. 435-451.

[4] NGUYEN K. Asymmetric concurrent signatures[A]. ICICS’05[C]. Springer-Verlag, Beijing, 2005. 181-193.

[5] LI Z H, FAN K, LI H. Perfect concurrent signature scheme on conic curve over ring Z_n[J]. International Journal of Digital Content Technology and its Applications, 2012, 6(18): 10-16.

[6] ZHANG Z, XU S. Cryptanalysis and improvement of a concurrent signature scheme based on identity[A]. ICSESS 2011[C]. Beijing, 2011. 453-456.

[7] TONIEN D, SUSILO W, SAFAVI-NAINI R. Multi-party concurrent signatures[A]. ISC 2006[C]. Samos Island, Greece, 2006. 131-145.

[8] XIE J T. Fair multi-party concurrent signatures[D]. China, Taiwan: National Central University, 2008.

[9] WANG L L. Multi-party concurrent signatures based on short ring signatures[A]. WCNIS2010[C]. Beijing, China, 2010. 515 – 517.

[10] 谭肖. 具备非连接性的公平多方并发签名体制[D]. 上海: 复旦大学, 2010.
TAN X. Unlinkable Fair Multi-party Concurrent Signatures[D]. Shanghai: Fudan University, 2010.

[11] CHOW S S M, YIU S M, HUI L C. Efficient identity based ring signature[A]. ACNS’05[C]. New York, 2005. 499-512.

[12] WANG L L, ZHANG G Y, MA C G. ID-based deniable ring authentication with constant-size signature[J]. Frontiers of Computer Science in China, 2008, 2(1): 106-112.

[13] YUEN T H. Contributions to Pairing-based Cryptography[D]. Wollongong: University of Wollongong, 2010.

[14] FELDMAN P. A practical scheme for non-interactive verifiable secret sharing[A]. Proc of 28th FOCS[C]. IEEE, California, USA, 1987.427-437.

[15] JUST M, VAUDENAY S. Authenticated multi-party key agreement[A]. ASIACRYPT '96[C]. 1996. 36-49.

[16] HUANG Q, YANG G M, WONG D S, *et al*. A new efficient optimistic fair exchange protocol without random oracles[J]. International Journal of Information Security, 2012, 11(1): 53-63.

作者简介：

叶青（1981-），女，辽宁营口人，北京邮电大学博士生，主要研究方向为数字签名技术。

杨赟（1974-），女，江西宜春人，铁道部信息技术中心工程师，主要研究方向为信息系统的运行与维护。

郑世慧（1979-），女，山东济南人，北京邮电大学讲师，主要研究方向为密码方案的分析与设计。

常利伟（1986-），男，山西朔州人，北京邮电大学博士生，主要研究方向为密码学、信息安全。

肖达（1981- ），男，黑龙江绥化人，北京邮电大学讲师，主要研究方向为灾备技术、云存储和云安全。

杨义先（1961-），男，四川绵阳人，北京邮电大学教授、博士生导师，主要研究方向为密码学和网络安全。