适用于移动互联网的门限群签名方案

陈立全 朱 政 王慕阳 孙晓燕
(东南大学信息科学与工程学院 南京 210096)

摘 要 当前的移动互联网得到了快速的发展和应用,但是在这之上的信息易遭受窃听、篡改、伪造等威胁,这是当前信息安全研究的重要问题.在移动终端电子投票、移动合同签署、移动联合购物等应用场合中,门限群签名技术的应用能有效保证系统的安全.但是,现有基于可信中心的 ECC 门限群签名方案,缺乏成员对可信中心的反向认证机制,因此可信中心容易成为整个签名系统的安全隐患.针对这个问题,该文提出了一种新的适用于移动互联网的 ECC 门限群签名方案,并对方案中涉及到的签名初始化、成员注册、份额签名生成、签名合成、签名验证、签名打开以及签名成员撤销等步骤进行详细设计.提出了新门限群签名方案基于成员和可信中心共同生成成员密钥的思想,并且完成了成员和可信中心身份双向认证、密钥共同生成以及成员身份的两次盲化.经安全性证明,该文所提的方案具有正确性和安全性,能抵抗联合攻击和陷害攻击等.性能分析比较的结果也表明,在相同安全水平下,该文所提的方案签名长度更短,签名生成和签名验证的计算量更低.而适用性分析结果也表明,该文所提的方案实现了成员对可信中心的认证和二次盲化处理,降低了移动终端的通信及计算开销,能更好地适用于移动互联网环境中.最后,该文还基于随机预言机(ROM)模型完成了对所提出的门限群签名方案的形式化安全证明.

关键词 门限群签名;移动互联网;椭圆曲线密码;双向身份认证;可信中心
中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2018.01052

A Threshold Group Signature Scheme for Mobile Internet Application

CHEN Li-Quan ZHU Zheng WANG Mu-Yang SUN Xiao-Yan
(*School of Information Science and Engineering, Southeast University, Nanjing* 210096)

Abstract Nowadays, mobile Internet has gained fast development and application. However, the information in mobile Internet application is vulnerable in hacking, tampering, forgery and other threats. How to solve these security problems is one of key topics in information security research field. Currently, electronic voting in mobile devices, mobile contract signed in mobile terminals and mobile joint applications such as shopping have been implemented, the use of the threshold group signature technology can effectively ensure the security of these systems. There are two types of threshold group signature: one is without a trusted center; while the other one is with a trusted center. In those existing elliptic curve cryptography (ECC) threshold group signature schemes with a trusted center, the authentication of trusted center from group member is always lacked. Thus, the trusted center may become a security bottleneck of the whole signature system. If there is a fake trusted center which wants to cheat the group members, it will threat the security of the group member. Especially, for the mobile Internet application, the use of mobile or wireless communication channels will give more convenience for the attacker. In order to solve this problem, a threshold group signature scheme based on ECC and suitable for mobile Internet is proposed. The steps of the proposed scheme are presented. In the Setup step,

收稿日期:2016-07-04;在线出版日期:2017-04-05.本课题得到国家自然科学基金项目(61372103)、国家"八六三"高技术研究发展计划重点项目(2013AA014001)、中兴通讯产学研基金项目资助.**陈立全**,男,1976 年生,博士,副教授,博士生导师,主要研究领域为信息安全、移动互联网.E-mail: Lqchen@seu.edu.cn.**朱 政**,男,1991 年生,硕士研究生,主要研究方向为加密与签名技术、移动互联网.**王慕阳**,男,1992 年生,硕士研究生,主要研究方向为认证与签名技术.**孙晓燕**,女,1990 年生,硕士研究生,主要研究方向为信息安全、认证签名.

the parameters for signature are prepared. Member will do registration in the Registering step. The signature of different member is created in the Sign step. Then the threshold group signature is constructed based on the signatures of the group member in Combine step. The Signature is verified in the Verify step. If the administrator wants to find out who sign this signature, the Open step will do this job. By the way, if one member leaves the group, a new threshold group signature would be created by the Revoke processing. In this paper, the proposed scheme puts forward an idea that the group members and trusted center generate the members' secret keys together. Moreover, the group members and trusted center implement mutual identity authentication, while the key generation and twice blind processing of members' identities are used in the proposed scheme. Based on secure proof, the proposed scheme is proved to be correct and secure. It can resist the joint attack and trap attack, etc. According to the results of performance comparison, it is shown that the proposed scheme has short signature length and low computation for sign and verification at the same security level. The application analysis shows that the proposed scheme implements the authentication of trusted center and twice blind processing of members' identities, the overhead of communication and computation is reduced, it is suitable for mobile Internet application. Finally, based on random Oracle module, the security of the proposed threshold group signature scheme suitable for mobile Internet is semantically proved. Based on the proposed threshold group signature scheme, the security of the mobile Internet application is guaranteed. It is very important for the widely use of mobile terminals and mobile Internet applications.

Keywords　threshold group signature; mobile Internet; elliptic curve cryptography; mutual identity authentication; trusted center

1　引　言

作为移动通信与互联网的融合，移动互联网孕育而生并得到迅速的发展. 然而，人们在享受移动互联网带来的便捷的同时，信息遭受窃听、篡改、伪造等威胁也随之而来. 门限群签名是群签名的一种拓展签名，要求签名者不再是单独的个体，而是群体中的授权子集. 只有授权子集中的成员合作才能代表群体生成合法的签名. 研究适用于移动互联网的门限群签名方案，能够有效地解决用户隐私和用户行为保护的问题，防止消息的伪造和抵赖，有效地保证信息的来源和完整性. 在移动环境中，基于门限群签名的应用也在不断地增加，在移动战场指挥命令签署、移动终端电子投票、移动合同文本签署、移动联合购物等场合都有着实际的应用价值.

在移动战场指挥命令签署的场合中，由分布战场多地的多人联合代表指挥部签署战场指挥命令. 考虑到移动终端的计算能力较弱和缺乏对认证中心的反向认证，目前的门限群签名方案都不适合应用到移动环境中. 因为在移动和无线通信系统中，更容易出现中间人攻击或伪基站攻击等情况，移动环境下的门限群签名的安全机制有待提升. 另外，在移动终端电子投票和移动合同文本签署等应用场合，也存在分散各地的移动终端用户使用门限群签名的方法进行电子投票决策和合同文本签署. 此时，设计适合移动终端特点和需求的门限群签名就显得尤为重要.

下面给出移动互联网环境下具体门限群签名方案应用的一个实例. 某跨国公司业务十分繁忙，公司高层决策者们常常需要出差，但是公司总部常常会有重要的紧急会议需要各个决策者参与决策投票，为了实现快速有效的系统，并防止竞争对手的攻击带来巨额损失，需要设计一套移动互联网环境下的安全投票决策系统实现决策者移动无线投票. 整个系统如图 1 所示.

注册服务器提供群成员信息注册、密钥生成的服务，只有成功在注册服务器注册，才能加入决策组，获得投票的权利. 移动端决策者在注册完毕以后，可以使用各自的移动终端，例如智能手机、PDA、笔记本电脑等进行投票决策，各个决策的结果在投票服务器中汇总，形成最终的决定. 这是一个基于门限群签名的决策系统，若整个决策组一共

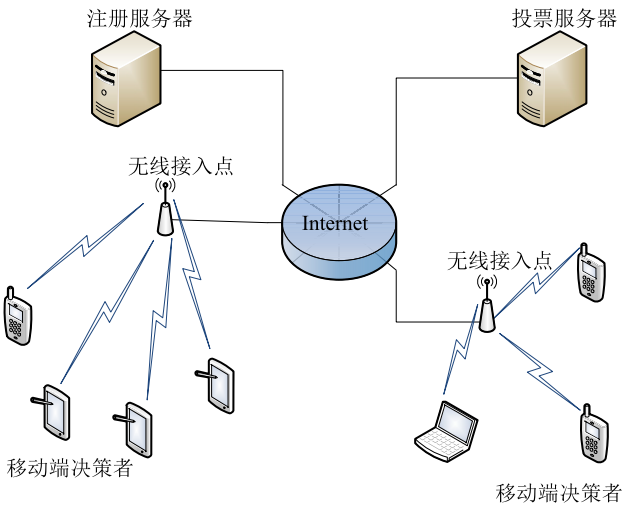


图 1 移动互联网下决策者远程投票系统

有 n 个决策者,决策门限为 t,其中 $t<n$,那么只有当大于等于 t 个决策者投票时,合成的投票结果才是有效的.

2 已有群签名方案分析

基于数学难题,门限群签名方案可以分为三类:(1)基于大数分解问题[1];(2)基于离散对数难题[2];(3)基于椭圆曲线或者超椭圆曲线难题[3-4].按照密钥分发方式的不同,现有的门限群签名方案可以分为两大类:有可信中心参与的门限群签名[4]和无可信中心参与的门限群签名[5-7].有可信中心参与的门限群签名方案中,成员只需参与部分计算;而无可信中心参与的门限群签名方案的计算量和通信量均依赖于群成员,成员的计算量和通信量均是有可信中心参与方案的 n 倍多,对群成员的计算能力和能源储存有较高要求.不过,现有可信中心参与的门限群签名方案缺乏用户对可信中心的反向认证,一旦可信中心不可信了,系统将被完全攻破;而无可信中心的门限群签名系统由于没有可信中心的参与,可以适用于用户互不信任的环境中.

研究适用于移动互联网的门限群签名,我们需考虑两个重要因素:(1)移动终端计算能力、电池容量有限;(2)移动互联网络环境更为复杂,安全性要求更高.这就要求设计的群签名方案具有以下特点:(1)对终端计算能力、能量资源的要求较低;(2)弱化可信中心的权力.理由如下:由上文的论述知,无可信中心群签名方案群成员的计算量和通信量比有可信中心群签名方案更高,因此,考虑到移动终端有限的资源,在移动互联网环境下,为了降低移动终端的计算与通信量,需要可信中心的参与.而考虑到可信中心被攻击的可能性,必须增加成员与可信中心的双向认证等方式弱化可信中心的权力,从而提升整个系统的安全性.因此,我们基于有可信中心参与的方案,利用椭圆曲线密码机制,设计有效安全的适用于移动互联网的门限群签名方案.

Hwang 等人提出了一个基于 RSA 问题的代理群签名方案[8].该方案能够满足代理签名的要求,能够抵御 equation attacks、insider forgery 和 direct forgery attacks 等攻击.但是,由文献[9]可知,相对于椭圆曲线密码体制,在获得相同级别的安全性下,RSA 密钥长度更长,计算量更大,处理速度更慢.1024 位 RSA 密钥获得的安全性与 160 位椭圆曲线密钥获得的安全性相近.

Yang 等人也提出了基于 RSA 问题的群签名方案[10].该方案与基于 ElGamal 的群签名方案相比,签名生成时间相近,但是签名验证时间快了约 10～40 倍.然而,由于 Yang 等人的方案也是基于 RSA 问题,因此相对于椭圆曲线方案,对计算资源、带宽资源有较高的要求,并不适用于资源有限的移动互联网中.

Lin 等人基于云计算编程模型 Map/Reduce 提出了一个门限秘密分享方案[11].该方案基于离散对数假设,能在消息的划分与整合中保证消息的保密性、完整性,并给出了认证机制.但是该方案应用于大规模高性能的分布式计算机集群中,对平台的计算能力要求高,并且没有用户身份盲化等机制,成员的私钥由一个 PKI VM 控制,一旦 PKI VM 被攻击,所有用户的私钥就会泄露.

可见,传统的基于大数分解问题和基于离散对数难题的群签名方案,相比于基于椭圆曲线的群签名方案,并不能够满足移动平台低计算能力、低能量资源、较低带宽的要求,因此并不适用于移动互联网中.而基于椭圆曲线的群签名方案,由于其更低的资源需求,可以适用于移动互联网.

目前,学术界对有可信中心参与的 ECC 门限群签名已经有了较多研究.2004 年,Chen 等人提出一个高效的门限群签名方案[12](简称 CHC 方案),该方案签名和验证过程中不涉及乘法运算和指数运算,运算量较低.但是,该方案没有给出身份追踪过程和撤销算法,并且不能抵抗联合攻击.基于 CHC 方案,彭娅提出了一个改进方案[13](简称 PY 方案)来解决不能抵抗联合攻击的问题,但是该方案证明过程

中默认 $f(x_i)=v_i$，而实际上 $x_{v_i}=v_i$，$(x_{v_i},y_{v_i})=f(x_i)G$. 此后，利用身份识别函数的思想，Xia 等人提出了一个动态门限群签名方案[14]（简称 XHGC 方案），谢冬等人提出了一种新的 ECC 门限群签名方案[15]（简称 XLS 方案）. 这两个方案均具有追踪性和撤销算法，但是 XHGC 方案不能够抵抗大于等于 t 个成员的合谋攻击. 以上四个方案均是基于 Shamir 的秘密共享技术，且大部分方案不能抵抗联合攻击. 为了弥补这一缺陷，出现了一些不使用 Shamir 秘密共享技术的门限群签名方案. 刘宏伟等人提出了基于身份密码体制的门限群签名方案[16]（简称 LXYZ 方案），该方案中 TC 选定群密钥 s，成员自选份额密钥 s_i，s 是以自选份额的模式分散到成员中.

同样，闫杰等人提出了新的 ECC 门限群签名方案[17]（简称 YYZ 方案），该方案中 TC 直接为成员选择私钥 x_i 并发送给成员，群私钥由成员私钥叠加而成. 这两个方案具备可追查性，给出了成员撤销过程. Chung 等人提出了基于 ECC 的群签名方案[18]，该方案具有匿名性、保密性、不可伪造性、不可否认性和前向安全，但是签名成员的私钥由可信中心生成并通过安全信道分发，一旦可信中心被攻破，成员的私钥就会泄露. 这些门限群签名方案的安全性都是基于对可信中心的完全信赖，一旦可信中心被攻破，由于可信中心知道群成员的所有信息，可以伪造成员签名，系统就丧失了安全性.

针对这种问题，本文提出了一种新的 ECC 门限群签名方案. 该方案设计的成员私钥由成员和可信中心共同生成. 同时，可信中心和用户通过 3 次身份信息交互，依次对成员身份进行两次盲化. 一方面，实现了身份的双向认证，有效防止可信中心和用户的欺诈行为；另一方面，利用盲化后的身份处理签名保证用户真实身份的隐蔽性，盲化身份和真实身份的一一对应关系保证对用户真实身份的可追踪性和用户的不可抵赖性. 此外，成员和可信中心对分配的私钥进行交互验证，弱化了对可信中心的绝对信赖，提高了系统的安全性. 该方案还能抵抗联合攻击和陷害攻击，同时具有较低的运算量和通信量，更适用于移动互联环境.

3　移动互联网 (t,n) 门限群签名方案（MI-(t,n)）

3.1　移动互联网 (t,n) 门限群签名（MI-(t,n)）模型

移动互联网 (t,n) 门限群签名（简称 MI-(t,n) 门限群签名）系统的参与方包括移动终端用户 User（U）、验证者 Verifier（V）、可信中心 Trust Center（TC）和签名合成者 Signature Combiner（SC）.

如图 2 所示，MI-(t,n) 门限群签名系统包括系统初始化、用户信息注册、份额签名生成、门限群签名生成、签名验证、签名打开和用户撤销七个部分. 每部分负责的任务如下：

（1）系统初始化过程中，TC 选定系统参数，并设定系统群密钥和 TC 自身密钥；

（2）用户注册信息过程是用户和 TC 交互的过程，主要包含身份信息的交互验证和密钥的交互验

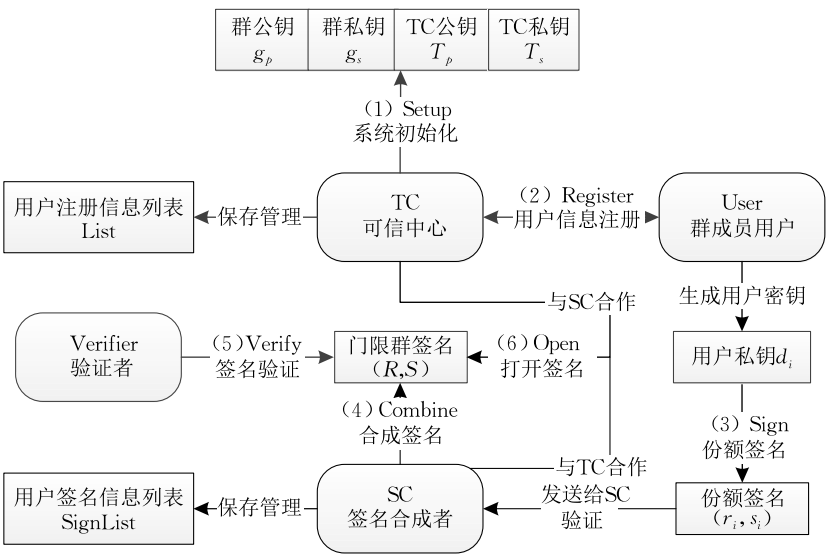


图 2　MI-(t,n) 门限群签名系统结构框图

证.该过程实现了双向认证.此过程生成了用户密钥和盲化后的用户身份,用于签名的处理;

(3)利用第2步生成的用户密钥和盲化后的身份,用户生成份额签名;

(4)SC验证份额签名合法后,合成门限群签名;

(5)利用群公钥,Verifier验证者对门限群签名进行合法性验证;

(6)SC和TC合作打开签名,揭示签名用户的真实身份.其中,SC查看用户签名信息列表SignList,TC查看用户注册信息列表List;

(7)一旦有用户离开群体,TC更新其他未撤销的用户密钥,并发布该用户离开群体的消息.

本方案中,TC与SC均作为可信的第三方存在,若能将这两者合并则能减小整个系统的通信开销,但是考虑到仅在产生纠纷时才需要合作打开签名,即打开签名这个操作发生的频率不高,因此在权衡安全性与通信性能之后,还是倾向于保留可信中心与签名合成者分开的设计.

3.2 移动互联网(t,n)门限群签名方案(MI-(t,n))设计

下面,具体描述MI-(t,n)门限群签名方案详细过程.表1给出了该方案涉及的符号及含义说明.

表1 MI-(t,n)门限群签名方案符号表示说明

符号	含义	符号	含义
TC	可信中心	ID_{i1}	用户一次盲化身份
U_i	群成员	ID_{i2}	用户二次盲化身份
SC	签名合成者	d_i	用户私钥
V	签名验证者	D_i	用户公钥
g_s	群私钥	P	t个成员的集合
g_p	群公钥	ID	t个成员的身份信息集合
T_s	可信中心私钥	List	TC保存的用户信息列表
T_p	可信中心公钥	SignList	SC保存的签名用户信息列表
ID_i	用户注册身份		

(1)系统初始化Setup(t,n)

可信中心TC执行系统创建过程,完成两个任务:设置(t,n)门限群签名系统的相关参数,搭建系统模型;生成TC自身的密钥及系统所需函数.具体过程如下:

①设置系统参数,生成椭圆曲线.具体过程如下:

首先,设定群的大小为n,门限值为t,其中$t<n$.接着,秘密选定一个大素数p,F_p表示有限域.随机选择$a,b\in F_p$,构造该有限域F_p上的椭圆曲线E:$y^2=x^3+ax+b$,其中a,b满足$4a+27b\neq 0(\mathrm{mod}\,p)$.最后,选择椭圆曲线$E$上的一个生成元$G$,它的阶$l$为一个大素数($l$的长度大于160bit).并且设$P_1,P_2$为椭圆曲线上的两个点,存在$k\in Z_p^*$,使得$P_1=kP_2$,由$k$和$P_2$计算$P_1$是可行的,但是通过$P_1$和$P_2$计算$k$是不可取的;

②可信中心TC设定相关密钥及参数.具体描述如下:

首先,设定TC私钥为$T_s=s$,TC公钥为$T_p=sG$,其中$s\in_R Z_p^*$.接着,秘密选定一个$t-1$次多项式:$f(x)=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+\cdots+a_2x^2+a_1x+a_0$,其中$a_i\in[1,p-1](i=0,1,2,\cdots,t-1)$的整数.那么群私钥为$g_s=f(0)=a_0$,群公钥为$g_p=f(0)G=a_0G$.最后,选择一个单向的哈希函数$h()$;

③公开参数a,b,G,g_p,p和$h()$,g_s和$f(x)$被TC秘密保存.

(2)用户注册信息Regist(T_s,T_p,U_i)

某个用户要加入群体成为群成员,需要与TC执行一个交互协议.这一交互过程包含了两个方面:一方面,TC对用户身份进行验证和盲化,同时用户对盲化后身份进行验证和二次盲化;另一方面,用户对TC为用户颁发部分密钥进行验证,TC对用户自己生成的部分密钥进行验证.交互协议的执行,实现了身份和密钥的双向认证,弱化了TC的绝对管理权力,加强了门限群签名系统的安全.具体执行过程如图3所示,具体流程如下:

①用户要加入群体成为群成员,先将用户身份信息ID_i发送给TC. TC验证该用户是否已经注册过.如果该用户注册过,TC拒绝其加入申请.否则,随机选择$u\in_R Z_p^*$,并计算

$$U=uG=(x_u,y_u) \tag{1}$$

$$ID_{i1}=(x_u+s)h(ID_i)+u\,\mathrm{mod}\,p \tag{2}$$

将(U,ID_{i1})发送给用户;

②用户接收到(U,ID_{i1})后,首先验证

$$ID_{i1}G=(x_uG+T_p)h(ID_i)+U \tag{3}$$

是否成立.如果不成立,用户重新发送申请.否则,选定自己部分私钥$x_i\in_R Z_p^*$,并计算$X_i=x_iG$.

随机选择$v\in_R Z_p^*$,并计算

$$V=vG=(x_v,y_v) \tag{4}$$

$$ID_{i2}=(x_v+x_i)h(ID_{i1})+v\,\mathrm{mod}\,p \tag{5}$$

将(X_i,V,ID_{i1},ID_{i2})发送给TC.其中,ID_{i2}作为用户的盲化身份参与签名的处理;

③收到(X_i,V,ID_{i1},ID_{i2})后,TC首先验证

$$ID_{i2}G=(x_vG+X_i)h(ID_{i1})+V \tag{6}$$

是否成立.如果成立,那么该用户成功加入群体,成为成员U_i.TC将用户的注册信息(X_i,ID_i,ID_{i2})添

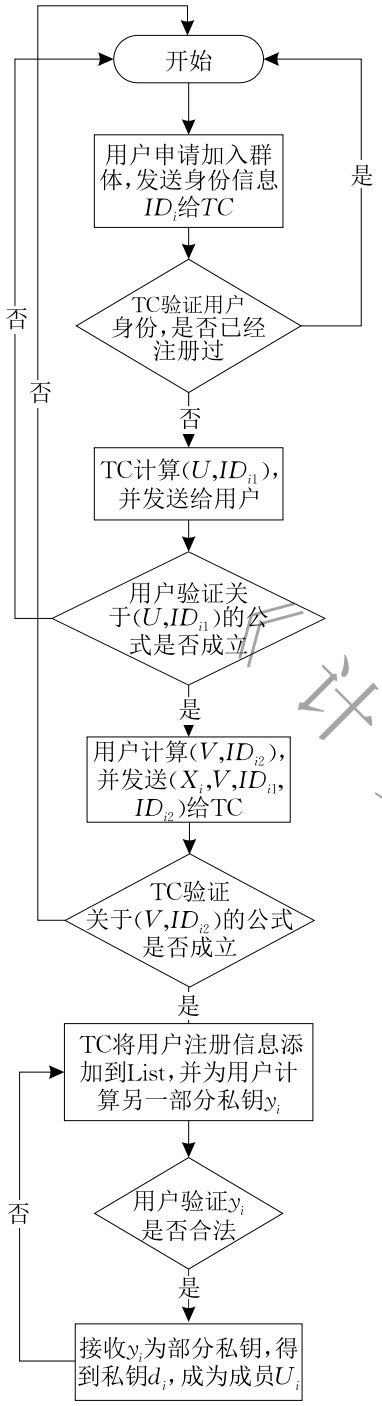


图 3　MI-(t,n)门限群签名用户注册流程图

加到用户信息列表 List 中，便于发生纠纷时进行真实身份的追踪. 否则，拒绝用户的加入申请，用户重新执行①～③的操作；

④ TC 为用户颁发另一部分私钥，这一过程需要用户和 TC 交互执行：

首先，TC 计算用户的另一部分私钥

$$y_i=f(ID_{i2}) \tag{7}$$

将 y_i通过秘密通道发送给相应的用户，并在用户群体中广播 a_iG 的值.

用户接收到私钥 y_i后，验证

$$y_iG=\sum_{i=0}^{t-1}a_iGID_{i2}^i \tag{8}$$

是否成立. 如果成立，用户则接收 y_i为其另一部分私钥；否则拒绝接收，要求 TC 重新生成另一部分私钥.

至此，用户生成了私钥 $d_i=x_i+y_i=x_i+f(ID_{i2})$，公钥 $D_i=d_iG$. 并公开用户公钥 D_i和用户身份信息 ID_{i2}.

(3) 用户生成份额签名 Sign(U_i,ID_{i2},d_i,m)

设门限群签名的参与成员为集合 $P=\{U_1,U_2,\cdots,U_t\}(t<n)$，对应的公开身份信息集合为 $ID=\{ID_{12},ID_{22},\cdots,ID_{t2}\}$. 每个成员 $U_i(i\in[1,t])$利用私钥 d_i，对消息进行签名，生成份额签名. 具体步骤包括：① 随机选择 $k_i\in_R Z_p^*$，计算 $r_i=k_iG=(x_{r_i},y_{r_i})$；② 计算消息的哈希值 $z=h(m)$；③ 计算份额签名 $s_i=k_ix_{r_i}-zd_iI_i \bmod p$，其中 $I_i=\prod_{i\neq j}\frac{ID_{i2}}{ID_{i2}-ID_{j2}}(i,j\in[1,t])$.

为了防止签名被敌手追踪，需要使用 SC 的公钥 PK_{SC}加密自身的身份，同时使用一个随机值 $RAND$ 使每次加密后的密文均不相同：

$$ID'_{i2}=E_{PK_{SC}}(RAND\,\|\,ID_{i2}).$$

由此，成员 U_i生成了份额签名 (r_i,s_i)，并将 (r_i,s_i)和 ID'_{i2}发送给签名合成者.

(4) 合成门限群签名 Combine (r_i,s_i,ID_{i2},D_i,m)

这一过程由签名合成者 SC 完成，包括份额签名的验证和签名的合成两个方面. 同时，SC 创建一张签名用户信息列表 SignList，保存签名用户的信息，便于配合 TC 进行成员身份的追踪.

在份额签名的验证方面，SC 收到成员 U_i的份额签名 (r_i,s_i)后，分别验证其正确性. 首先使用自身私钥 SK_{SC}解密 ID'_{i2}得到签名者的盲化身份 ID_{i2}，然后通过集合 ID，计算 I_i，$I_i=\prod_{i\neq j}\frac{ID_{i2}}{ID_{i2}-ID_{j2}}$；接着计算 z. 接着，证明等式 $s_iG+zD_iI_i=r_ix_{r_i}$是否成立. 如果成立，那么份额签名 (r_i,s_i)合法，否则拒绝该份额签名.

在签名的合成方面，当所有份额签名验证合法后，通过下述方法来合成门限群签名. 首先计算 $R=\sum_{i=1}^{t}r_ix_{r_i} \bmod p$，然后将所有份额签名合并，计算 $S=\sum_{i=1}^{t}s_i$，再计算 $W=\sum_{i=1}^{t}I_iX_i$并公开.

SC 生成门限群签名 (R,S)，并将其发送给验证者，同时将参与群体的用户签名信息 (r_i,s_i,ID_{i2})

及相应的群签名(R,S)添加到签名信息列表SignList中.

(5)签名验证 Verify(R,S,W,g_p,m)

签名验证者V接收到门限群签名(R,S)后,根据$z=h(m)$计算z,并验证$SG+z(g_p+W)=R$是否成立.如果成立则接收签名,否则拒绝该门限群签名.

(6)打开签名 Open

一旦发生纠纷,在任何合法的签名合成者SC和TC协助下,均能够揭示签名群体用户的真实身份.

①TC将签名(R,S)发送给SC.SC查询签名信息列表SignList,找到对应于(R,S)的(r_i,s_i,ID_{i2}).对于签名合成者SC来说,签名用户的盲化身份ID_{i2}是可见的,但是用户的真实身份ID_i是未知的;

②SC将参与签名的用户群体的盲化身份ID_{i2}集合发送给TC,TC查询用户信息列表,找到对应于盲化身份ID_{i2}的用户信息(X_i,ID_i,ID_{i2}),进而确定用户的真实身份ID_i.

(7)撤销成员 Revoke(U_i)

一旦某一个成员要离开签名群体,TC执行以下步骤删除成员U_i:

①重新秘密选定一个$t-1$次多项式:$f(x)=a'_{t-1}x^{t-1}+a'_{t-2}x^{t-2}+\cdots+a'_2x^2+a'_1x+a_0$;

②分别为成员重新计算部分密钥$y_i=f(ID_{i2})$,每个成员执行Register过程中的第4个步骤,确定是否接受部分密钥y_i.

通过这两个步骤,TC就删除了成员U_i.

4 MI-(t,n)门限群签名方案安全证明

4.1 正确性分析

MI-(t,n)门限群签名方案的正确性证明包括两个方面:一方面是用户注册信息过程中两次身份验证和密钥验证的正确性,另一方面是签名过程中份额签名和门限群签名的正确性验证.

(1)身份验证的正确性证明

在用户注册信息过程中,涉及到两次关于身份的验证:$ID_{i1}G=(x_uG+T_p)h(ID_i)+U$和$ID_{i2}G=(x_vG+X_i)h(ID_{i1})+V$.由$U=uG=(x_u,y_u)$及$ID_{i1}=(x_u+s)h(ID_i)+u$,得$ID_{i1}G=(x_uG+sG)h(ID_i)+uG=(x_uG+T_p)h(ID_i)+U$.同理,由$V=vG=(x_v,y_v)$和$ID_{i2}=(x_v+x_i)h(ID_{i1})+v$,得$ID_{i2}G=(x_vG+x_iG)h(ID_{i1})+vG=(x_vG+X_i)h(ID_{i1})+V$.

因此,两次身份的验证过程是正确的.

(2)密钥验证的正确性证明

用户注册信息的过程中,还包含了用户密钥的正确性验证:验证$y_iG=\sum_{i=0}^{t-1}a_iGID_{i2}^i$是否成立,决定是否接受$y_i$为部分用户密钥.由$f(x)=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+\cdots+a_2x^2+a_1x+a_0$,得$y_iG=f(ID_{i2})G=a_{t-1}ID_{i2}^{t-1}+a_{t-2}ID_{i2}^{t-2}+\cdots+a_2ID_{i2}^2+a_1ID_{i2}+a_0=\sum_{i=0}^{t-1}a_iGID_{i2}^i$

显然,关于密钥的验证过程也是正确的.

(3)份额签名的正确性证明

通过验证等式$s_iG+zD_iI_i=r_ix_{r_i}$是否成立,确定份额签名是否正确.由$s_i=k_ix_{r_i}-zd_iI_i$和$r_i=k_iG$,得$s_iG=k_ix_{r_i}G-zd_iI_iG=r_ix_{r_i}-zD_iI_i$.所以$s_iG+zD_iI_i=r_ix_{r_i}$得证.

(4)门限群签名的正确性证明

通过验证$SG+z(g_p+W)=R$是否成立,确定门限群签名是否正确.

$$\begin{aligned}SG&=\sum_{i=1}^{t}s_iG=\sum_{i=1}^{t}(k_ix_{r_i}G-zd_iI_iG)\\&=\sum_{i=1}^{t}r_ix_{r_i}-\sum_{i=1}^{t}z(x_i+f(ID_{i2}))I_iG\\&=R-\sum_{i=1}^{t}z(X_iI_i+f(ID_{i2})I_iG).\end{aligned}$$

由拉格朗日定理可知,$\sum_{i=1}^{t}f(ID_{i2})I_iG=\left(\sum_{j=1}^{t}f(ID_{i2})\prod_{i\neq j}\frac{ID_{i2}}{ID_{i2}-ID_{j2}}\right)G=f(0)G=g_p$.因此,$SG=R-z\left(\sum_{i=1}^{t}X_iI_i+g_p\right)=R-z(W+g_p)$,所以$SG+z(g_p+W)=R$.

4.2 安全性证明

(1)门限特性

门限签名的门限特性是指在一个(t,n)的门限签名方案中,签名密钥分散到n个成员的签名成员集合中,由不少于t个成员的成员子集使用各自所拥有的部分密钥共同产生最终的签名结果,而任何小于t个成员的子集都无法恢复密钥或者计算正确的签名结果.

根据3.2节的方案描述,门限群签名的产生过程包括份额签名的生成和门限签名的合成.其中,份额签名$s_i=k_ix_{r_i}-zd_iI_i$,合成的群签名为$S=\sum_{i=1}^{t}s_i=\sum_{i=1}^{t}k_ix_{r_i}-\sum_{i=1}^{t}z(x_i+f(ID_{i2}))I_i$.一个有效的

门限群签名必须通过验证者的验证，即证明 $SG+z(g_p+W)=R$ 成立.

在 4.1 节中，我们已经对 $SG+z(g_p+W)=R$ 予以证明. 证明过程应用了拉格朗日插值定理，$\sum_{i=1}^{t} f(ID_{i2})I_iG=\left(\sum_{j=1}^{t} f(ID_{i2})\prod_{i\neq j}\frac{ID_{i2}}{ID_{i2}-ID_{j2}}\right)G=f(0)G=g_p$. 该证明过程表明，只有 t 个或者多于 t 个群成员合作，才能恢复群私钥 $f(0)$，进而使得群签名合法. 若是少于 t 个成员合作生成份额签名并发送给 SC 予以合成，由于不能恢复群私钥，SC 合成的签名无法通过验证者的验证. 敌手若是希望通过恢复群私钥的方式得到一个合法的群签名，则需要通过群公钥 $g_p=f(0)G$ 解出 $f(0)$ 的值，此操作的难度相当于解开椭圆曲线上的离散对数问题(ECDLP)，而通常认为解开该问题是困难的.

因此，本文方案具有门限特性：至少 t 个合法的群成员才能生成有效的群签名.

(2) 不可陷害性证明

门限签名的不可陷害性是指任何群成员或者群管理者，都不可能以其他成员的名义生成合法的群签名.

对于该方案陷害攻击可以分为两种情况：情况 1，可信中心 TC 伪装为成员 U_i，对消息 m 进行签名，进而陷害成员 U_i；情况 2，某一成员 U_j 伪装为成员 U_i，对消息 m 进行签名，进而陷害成员 U_i. 对于这两种情形，门限群签名的参与成员身份集合 $ID=\{ID_{11},ID_{22},\cdots,ID_{t2}\}$ 均是公开的. 事实上，这两种攻击方式原理上与无证书签名体制中的两类攻击方式相同，情况 1 对应于无证书签名体制中的第一类攻击，即敌手能够获得系统主密钥的攻击(恶意可信中心攻击)；情况 2 对应于敌手不能获得系统主密钥，但可以使用自己选择的值替换任意用户的公钥(一般用户攻击).

下面，分别对两种情形的攻击予以分析.

(1) 情形 1. TC 伪造成员 U_i 的签名

对于 TC 来说，$f(x)$ 和 ID_{i2} 均是已知的.

TC 随机选择 $x_i'\in_R Z_p^*$，计算 $d_i'=x_i'+f(ID_{i2})$ 作为成员 U_i 的私钥，并计算 $X_i'=x_i'G$ 及公钥 $D_i'=d_i'G$.

此后执行份额签名 Sign 过程，生成份额签名 (r_i',s_i')，发送给签名合成者. 由于 D_i' 对应于 d_i'，该签名能通过 $s_i'G+zD_iI_i=r_i'x_{r_i}$ 的验证.

通过 SC 的验证后，SC 合成 t 个成员的份额签名，生成门限群签名 (R',S'). 计算 $R'=\sum_{j=1,j\neq i}^{t} r_jx_{r_j}+r_i'x_{r_j}'$，$S'=\sum_{j=1,j\neq i}^{t} s_j+s_i'$，$W'=\sum_{j=1,j\neq i}^{t} I_jX_j+I_iX_i'$，并公开 W'. 同样，由于 X_i' 对应于 x_i'，该签名 (R',S') 能通过签名验证者 $S'G+z(g_p+W')=R'$ 的验证.

但是，合法的成员 U_i 可以向仲裁机构提出申诉，并证明该签名不是其所签. 首先成员 U_i 将 (X_i,V,ID_{i1},ID_{i2}) 发送给仲裁机构，仲裁机构要求 TC 发送相应的值，那么 TC 发送 (X_i',V,ID_{i1},ID_{i2}). 由于 $ID_{i2}=(x_v+x_i)h(ID_{i1})+v$，$ID_{i2}G=(x_vG+X_i)h(ID_{i1})+V$ 只对于 X_i 唯一成立，因此 TC 要想成功伪造成员 U_i 的签名，必须保证 $x_i'=x_i$. 而对于 TC，要想得到 x_i，必须从 $X_i=x_iG$ 解到 x_i. 这等同于解决椭圆曲线上的离散对数难题，在计算上是不可行的.

(2) 情形 2. 成员 U_j 伪造成员 U_i 的签名

对于成员 U_j，只有 ID_{i2} 是已知的.

U_j 选定一个多项式 $f'(x)$，计算 $f'(ID_{i2})$. 随机选择 $x_i'\in_R Z_p^*$，计算 $d_i'=x_i'+f'(ID_{i2})$，并计算 $X_i'=x_i'G$ 及公钥 $D_i'=d_i'G$.

此后执行份额签名 Sign 过程，生成份额签名 (r_i',s_i')，发送给签名合成者. 由于 D_i' 对应于 d_i'，该签名能通过 $s_i'G+zD_iI_i=r_i'x_{r_i}$ 的验证.

SC 合成 t 个成员的份额签名，生成门限群签名 (R',S'). 计算 $R'=\sum_{j=1,j\neq i}^{t} r_jx_{r_j}+r_i'x_{r_j}'$，$S'=\sum_{j=1,j\neq i}^{t} s_j+s_i'$，$W'=\sum_{j=1,j\neq i}^{t} I_jX_j+I_iX_i'$，并公开 W'.

该门限群签名 (R',S') 要通过签名验证者的验证，使得 $S'G+z(g_p+W')=R'$，必须保证 $\sum_{i=1}^{t} f(ID_{i2})I_iG=\left(\sum_{j=1}^{t} f(ID_{i2})\prod_{i\neq j}\frac{ID_{i2}}{ID_{i2}-ID_{j2}}\right)G=f(0)G=g_p$. 对应地，即 $\sum_{j=1,j\neq i}^{t} f(ID_{j2})I_jG+f'(ID_{j2})I_jG=\left(\sum_{j=1}^{t} f(ID_{i2})\cdot\prod_{i\neq j}\frac{ID_{i2}}{ID_{i2}-ID_{j2}}\right)G=f(0)G=g_p$. 因此，$U_j$ 必须保证 $f'(ID_{j2})=f(ID_{j2})$，而 $f(x)$ 只有 TC 知晓. $f(x)=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+\cdots+a_2x^2+a_1x+a_0$，要想 $f'(ID_{j2})=f(ID_{j2})$，需有 $a_{t-1}=a_{t-1}'$，而 $a_i\in[1,p-1](i=0,1,2,\cdots,t-1)$ 的整数，因此 $f'(ID_{j2})=f(ID_{j2})$ 的概率为 $\frac{1}{(p-1)^t}$. 因此当 p 的值足够大时，敌手仅能以一个可以忽略的概率攻击成功.

即使 U_j 能够使 $f'(ID_{j2})=f(ID_{j2})$，进而通过签名的合法性验证. 合法的成员 U_i 可以向仲裁机构提出申诉，并证明该签名不是其所签. 该证明过程同于情形 1.

综上所述，MI-(t,n)门限群签名方案能够抵抗陷害攻击.

(3) 可追踪性证明

门限签名的可追踪性是指发生争执的时候，有且只有群管理者有权打开签名，确定签名者的真实身份.

签名合成者 SC 和可信中心 TC 合作能够追踪用户的真实身份. 群成员生成份额签名后，将(r_i,s_i,ID_{j2})发送给 SC. SC 验证份额签名为合法后再合成为门限群签名，并将成员签名信息(r_i,s_i,ID_{i2})和对应的(R,S)添加到签名信息列表 SignList 中.

一旦要追踪用户成员的真实身份，TC 将签名(R,S)发送给 SC，SC 查询 SignList，就能够找到参与签名的用户群体的盲化身份 ID_{i2}，并将其发送给 TC. TC 查询用户注册信息列表(X_i,ID_i,ID_{i2})，能够找到对应于 ID_{i2} 的身份 ID_i，揭示签名用户群体的真实身份.

由于 TC 不参与签名合成，即不具有具体的签名数据，而 SC 不具有用户的真实身份，因此他们任何一方均无法独立完成打开签名的操作；同时，由 4.2 节中的不可陷害性证明可知，签名用户的身份无法伪造，因此该方案具有可追踪性. 可追踪性的安全性基于不可陷害性的安全性，因此也是基于椭圆曲线上的离散对数难题. 因此，该方案具有可追踪性.

(4) 抗联合攻击

门限签名安全性中的抗联合攻击是指一个群体中的部分成员联合，不可能生成一个合法的签名使得群管理者无法追踪到.

攻击者的联合攻击分为两种情形：情形 1，多个群成员联合，生成有效的门限群签名；情形 2，多个群成员和可信中心 TC 联合，生成有效的门限群签名. 现假设两种情形下，均是联合冒充小组 $ID=\{ID_{11},ID_{22},\cdots,ID_{t2}\}$ 生成有效的门限群签名. 我们知道 $f(x)=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+\cdots+a_2x^2+a_1x+a_0$，含有 t 个未知数，如果知道 t 组$(ID_{i1},f(ID_{i1}))$，就能够恢复出 $f(x)$，得到群私钥 $f(0)$.

对于情形 1，如果联合的群成员个数大于等于 t，能够恢复 $f(x)$；如果联合的群成员个数小于 t，就不能够恢复 $f(x)$. 而对于情形 2，无论联合的群成员个数大于或小于 t，$f(x)$都是已知的.

因此，对于两种情形的证明分为两种情况：$f(x)$已知，包括联合的成员个数大于等于 t 时的情形 1 和情形 2；$f(x)$未知，即联合的成员个数小于 t 时的情形 1.

① $f(x)$已知

$f(x)$已知，即联合成员小组知晓小组 ID 内成员的部分密钥 $f(ID_{i2})$.

首先要生成小组 ID 内的每个成员的份额签名. 对于任意 $ID_{i1}\in ID$，随机选择 $x_i'\in_R Z_p^*$，计算 $d_i'=x_i'+f(ID_{i2})$作为成员 U_i 的私钥，$X_i'=x_i'G$ 及公钥 $D_i'=d_i'G$.

此后执行份额签名 Sign 过程，生成份额签名(r_i',s_i'). 由于 D_i'对应于 d_i'，该签名能通过签名合成者 $s_i'G+zD_iI_i=r_i'x_{r_i}$ 的验证. SC 合成份额签名，$R'=\sum_{i=1}^{t}r_i'x_{r_j}'$，$S'=\sum_{i=1}^{t}s_i'$，$W'=\sum_{i=1}^{t}I_iX_i'$，并公开 W'. 由于 $f(ID_{i2})$已知，X_i'对应于 x_i'，该签名(R',S')能通过签名验证者 $S'G+z(g_p+W')=R'$的验证.

但是，该签名无效. 我们知道 $ID_{i2}=(x_v+x_i)h(ID_{i1})+v$，对于 ID_{i2} 的验证 $ID_{i2}G=(x_vG+X_i)h(ID_{i1})+V$ 只对于唯一的 X_i 成立. 要想联合伪造的签名有效，必须保证对于任意 $ID_{i1}\in ID$，$x_i'=x_i$ 成立. 而实际上，要想得到准确的 x_i，等同于解决 t 个椭圆曲线上的离散对数难题.

② $f(x)$未知

$f(x)$未知，即联合成员小组不能得到小组 ID 内成员的部分密钥 $f(ID_{i2})$.

联合小组选定一个多项式 $f'(x)$. 对于任意$ID_{i1}\in ID$，随机选择 $x_i'\in_R Z_p^*$，计算 $d_i'=x_i'+f'(ID_{i2})$，$X_i'=x_i'G$ 及公钥 $D_i'=d_i'G$.

此后执行份额签名 Sign 过程，生成份额签名(r_i',s_i'). 由于 D_i'对应于 d_i'，该签名能通过 $s_i'G+zD_iI_i=r_i'x_{r_i}$ 的验证. SC 合成门限群签名(R',S')，计算 $R'=\sum_{i=1}^{t}r_i's_i'$，$S'=\sum_{i=1}^{t}s_i'$，$W'=\sum_{i=1}^{t}I_iX_i'$，并公开 W'.

门限群签名(R',S')要通过验证者的验证，必须满足 $\sum_{i=1}^{t}f'(ID_{i2})I_iG=\left(\sum_{j=1}^{t}f(ID_{i2})\prod_{i\neq j}\frac{ID_{i2}}{ID_{i2}-ID_{j2}}\right)G=f(0)G=g_p$，即保证 $f(x)=f'(x)$. $f(x)=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+\cdots+a_2x^2+a_1x+a_0$，$a_i\in[1,p-1](i=0,1,2,\cdots,t-1)$的整数，因此 $f'(ID_{j2})=f(ID_{j2})$的概率为 $\frac{1}{(p-1)^t}$.

此外，还需通过对 ID_{i2} 的验证. 同 $f(x)$ 已知的情况，须保证对于任意 $ID_{i2}\in ID$，$x_i'=x_i$ 成立. 这等同于解决 t 个椭圆曲线上的离散对数难题，在计算上是不可行的.

综述所述，MI-(t,n)门限群签名方案能够抵抗联合攻击.

(5) 匿名性证明

门限签名的匿名性是指对于一个给定的群签名，除了群管理者，任何人无法知晓签名者的真实身份.

该方案中，用户申请加入群体时，向 TC 提交了身份信息 ID_i. TC 对 ID_i 进行盲化，得到 $ID_{i1}=(x_u+s)h(ID_i)+u$. 通过对 ID_{i1} 的验证后，用户对身份进行二次盲化，得到 $ID_{i2}=(x_v+x_i)h(ID_{i1})+v$.

由计算公式可以看到，ID_{i2} 的计算需要用户的部分私钥 x_i 和 TC 的私钥 s，它们分别只有用户和 TC 本身知道. 任何其他恶意攻击者无法知晓 x_i 和 s，进而无法计算用户身份 ID_i 的盲化身份 ID_{i2}. 在此后的签名处理过程中，公开的用户身份信息为盲化后的身份 ID_{i2}. 根据 3.2 节用户信息注册 Regist 中的式(2)和(5)，ID_i 通过单向 hash 函数 h 计算得到 ID_{i2}，因此任何人不能够将 ID_{i2} 对应到用户的真实身份 ID_i. 只有 TC 和 SC 合作，才能追踪到用户的真实身份.

匿名性中需要重点关注的还有签名的关联性. 虽然以上论述说明了除了 TC 与 SC 合作以外并无得到用户真实身份的方法，但是注意到每次发出份额签名时，用户需要附带自己的二次盲化身份 ID_{i2}，虽然敌手得到 ID_{i2} 也不能计算出用户的真实身份，但是却能将所有 ID_{i2} 相同的份额签名关联起来，即实现签名的追踪. 为了杜绝此类攻击，每次用户发出自己的份额签名时，需要使用 SC 的公钥 PK_{SC} 加密自身的身份，同时使用一个随机值 $RAND$ 使每次加密后的密文均不相同：

$$ID_{i2}'=E_{PK_{SC}}(RAND\,\|\,ID_{i2}).$$

由此，成员 U_i 生成了份额签名 (r_i,s_i)，并将 (r_i,s_i) 和 ID_{i2}' 发送给签名合成者. 签名合成者 SC 使用自己的私钥解密得到份额签名对应的二次盲化身份，并记录在本地.

由以上分析可知，本文所述方案具有匿名性，并且不会被敌手关联签名.

4.3　基于随机预言模型的安全性证明

本文提供了 MI-(t,n)门限群签名方案的基于随机预言机模型的安全性证明，具体详见附录.

5　MI-(t,n)门限群签名方案性能

5.1　MI-(t,n)门限群签名方案性能分析和比较

下面，首先从计算量和通信量方面分析该方案的性能.

签名长度：MI-(t,n)门限群签名方案的设计是基于椭圆曲线上的离散对数难题. 而 160 比特椭圆曲线密码就可以达到 1024 比特 RSA 密码的安全强度. 在该方案份额签名生成阶段，每个成员将份额签名 (r_i,s_i) 和对应的盲化身份 ID_{j2} 发送给签名合成者. ID_{j2} 的发送用于签名合成者和可信中心合作揭示用户真实身份. 因此，每个成员签名需要占用 480 比特空间.

计算开销：

如表 2，首先介绍关于计算开销的几个符号的意义.

表 2　关于计算开销的符号表示说明

符号	含义
T_{MUL}	模乘法运算的时间开销
T_{EC_MUL}	椭圆曲线上乘法运算的时间开销
T_{EC_ADD}	椭圆曲线上加法运算的时间开销
T_{INV}	模的逆运算的时间开销
T_H	哈希运算的时间开销

根据文献[12]，对应于本章给出的椭圆曲线，有 $T_{EC\_MUL}\approx 29T_{MUL}$，$T_{EC\_ADD}\approx 0.12T_{MUL}$. 由于模加法和模减法的计算开销很低，因此忽略不计.

本文所提出的 MI-(t,n)门限群签名方案时间开销的计算包含三个部分：用户信息注册、签名生成和签名验证过程. 签名生成包含用户生成份额签名和合成门限群签名两个过程. 通过计算，总的时间开销如表 3 所示.

表 3　MI-(t,n)门限群签名方案的时间复杂度

过程	时间复杂度	合计
用户信息注册	$(3+t)T_{EC\_MUL}+(t+1)T_{EC_{ADD}}+2T_H$	$(87.12+29.12t)T_{MUL}+2T_H$
签名生成	$4tT_{EC\_MUL}+2(t-1)T_{EC_{ADD}}+3tT_{MUL}+(t+1)T_H$	$(119.24t-0.24)T_{MUL}+(t+1)T_H$
签名验证	$2T_{EC\_MUL}+2T_{EC_{ADD}}+T_H$	$58.24T_{MUL}+T_H$

其中，份额签名过程中每个用户的计算量为 $t_{sg}=T_{EC\_MUL}+T_H$.

为了突出 MI-(t,n)门限群签名方案的性能优势，下面从签名长度、计算量和安全性三个方面与现有方案进行比较，见表 4. 其中，现有方案均是基于椭圆曲线密码体制设计的，签名长度单位为比特，且

计算开销的方法与本文方案相同.由于各个方案用户注册过程不同,且有的方案没有用户与可信中心的交互,因此不对用户注册过程的计算量进行比较.

表 4 与现有门限群签名方案的性能比较

(a1) 签名长度和计算量的比较 I

性能 / 方案	密钥长度	签名长度	计算开销	
			签名生成	签名验证
MI-(t,n)	160	480	$(119.24t-0.24)T_{MUL}+(t+1)T_H$	$58.24T_{MUL}+T_H$
CHC[12]	160	320	$(90.24t-0.24)T_{MUL}+tT_{INV}+(t+1)T_H$	$(58.12+t)T_{MUL}+T_H$
PY[13]	160	320	$(88.24t-0.24)T_{MUL}+(t+1)T_H$	$58.12T_{MUL}+T_H$

(a2) 签名长度与性能比较 II

性能 / 方案	密钥长度	签名长度	计算开销	
			签名生成	签名验证
MI-(t,n)	160	480	$(119.24t-0.24)T_{MUL}+(t+1)T_H$	$58.24T_{MUL}+T_H$
HAA[19]	160	1440	$(209.36t-87.88)T_{MUL}+tT_{INV}+T_H$	$145.36T_{MUL}+T_H$
XHGC[14]	160	480	$(121.24t+0.88)T_{MUL}+tT_{INV}+(t+1)T_H$	$59.12T_{MUL}+T_H$
XLS[15]	160	480	$(235.12t-0.12)T_{MUL}+(t+1)T_H$	$87.24T_{MUL}+T_H$

(b) 安全性能的比较

性能 / 方案	可追踪	抗联合攻击	可撤销	完全依赖于对 TC 的信任
MI-(t,n)	是	是	是	否
HAA[19]	是	是	否	是
CHC[12]	否	否	否	是
PY[13]	否	是	否	是
XHGC[14]	是	否	是	是
XLS[15]	是	是	是	是
LXYZ[16]	是	是	是	是

如表(a1)和表(b)所示,就签名长度和计算量而言,虽然 PY 方案优于 MI-(t,n)方案,但是 PY 方案验证签名等式实际上并不成立,同时该方案安全性低,完全不符合表中的四个安全需求.CHC 方案签名长度均短于本文所提的 MI-(t,n)方案,但是 CHC 方案签名生成计算中包含模的逆运算,签名验证计算量和 MI-(t,n)方案相当,并且完全不符合表中的四个安全需求.

在表(a2)中,可以看到 HAA 方案由于无论在签名长度和计算量上,均明显高于 MI-(t,n)方案,并且 HAA 方案并没有可撤销的特点.XHGC 方案和 XLS 方案签名长度与 MI-(t,n)方案相当,但是签名生成和签名验证的计算量均高于 MI-(t,n)方案.

可见,MI-(t,n)方案克服了已有方案存在的安全问题,不仅具有可追踪性、可撤销性,能够抵抗联合攻击,同时加入了成员对 TC 的认证的特性,从而弱化了 TC 的管理权力,降低了 TC 被攻破时泄露成员私钥的概率,提升了系统的整体安全性能.综合安全性、计算量和通信量,MI-(t,n)门限群签名方案性能优于现有方案,签名长度短,计算量低,并且具有高的安全性.下面,将对该方案在移动互联网环境下的适用性进行分析.

5.2 MI-(t,n)门限群签名方案的适用性分析

针对移动互联网终端能力有限和网络环境复杂两个特点,本节将相应地对 MI-(t,n)门限群签名方案进行分析,以验证该方案能够适用于移动互联环境.

(1) 计算量

MI-(t,n)门限群签名方案基于椭圆曲线密码体制设计,占用的存储空间少,签名长度只有 480 比特.此外,根据 5.1 节对用户时间开销的计算过程,用户信息注册过程时间开销 $t_r=(3+t)T_{EC\_MUL}+(t+1)T_{EC_{ADD}}+2T_H$,份额签名过程中每个用户的计算量为 $t_{sg}=T_{EC\_MUL}+T_H$.

利用 crossbow 公司的无线传感器网络 MicaZ 节点,林玉炳测试了椭圆曲线上点乘的运算时间大约为 2.6 s[20],这里忽略哈希运算的实际开销.那么可以计算出该方案在单片机中用户的实际时间开销,如表 5(a)所示.在移动互联网终端中,以 Cortex A9 1.2GHz 微处理器为例,根据表 5(a),推算出该方案在移动智能终端中用户的计算时间开销,如表 5(b)所示.

表 5 MI-(t,n)门限群签名方案用户的计算时间开销

(a) 单片机中用户的计算时间开销

过程	时间开销/s
用户信息注册	$7.82+2.62t$
签名	2.6

(b) 移动智能终端中用户的计算时间开销

过程	时间开销/s
用户信息注册	$0.1043+0.0349t$
签名	0.0347

根据表 5(b)可以看出 MI-(t,n)门限群签名方案在移动智能终端中用户的计算时间开销比较低.如果换成在双核乃至四核处理器的移动智能终端上应用 MI-(t,n)门限群签名方案,它的实际时间开销将会更低.因此,MI-(t,n)门限群签名方案能够满足移动终端对于计算量和通信量的要求.

(2)增强安全性

首先，由 4.2 节的安全性证明，MI-(t,n)门限群签名方案满足门限特性，具有匿名性、可追踪性，能够抵抗联合攻击和陷害攻击. 4.1 节又将其与现有方案进行了比较，结果表明该方案的安全性能优于现有的方案.

其次，MI-(t,n)门限群签名方案执行用户注册信息过程时，用户和可信中心要实现双向认证. 这一双向认证包括两个方面：一方面是对身份信息的认证；另一方面是对密钥的认证.

如图 4，对身份信息的认证包括三次信息交互，实现用户和可信中心的互相认证：可信中心对用户身份进行验证，用户对可信中心盲化身份进行验证，可信中心对用户二次盲化身份的验证. 具体过程如下：

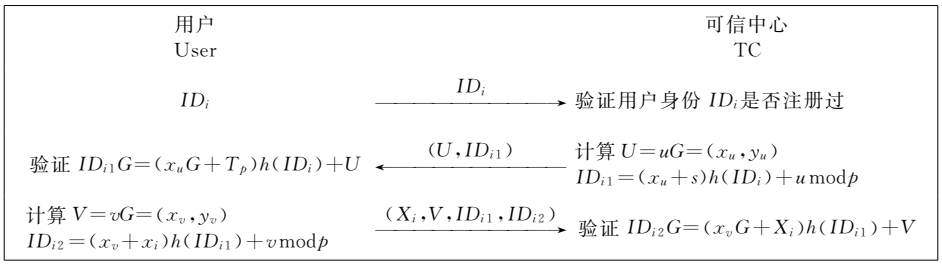


图 4　MI-(t,n)门限群签名身份信息的认证过程

(1)用户首先将身份信息 ID_i 发送给可信中心 TC. TC 接收后，首先验证用户身份的合法性，查看用户是否已经注册过. 如果没有注册，利用自己的私钥 s 对用户身份进行第一次盲化，计算得到盲化身份 ID_{i1}；

(2)用户接收到(U,ID_{i1})后首先验证盲化身份 ID_{i1}的合法性，即验证 $ID_{i1}G=(x_uG+T_p)h(ID_i)+U$ 是否成立. 我们知道 ID_{i1}是由 TC 私钥 s 生成，ID_i 是用户自己提交的. 如果该等式成立，那么用户有理由相信 ID_{i1}一定是 TC 对 ID_i的盲化身份. 用户自己选定用户部分私钥 x_i，利用 x_i第二次盲化身份，得到 ID_{i2}；

(3)TC接收到(X_i,V,ID_{i1},ID_{i2})后，验证$ID_{i2}G=(x_vG+X_i)h(ID_{i1})+V$ 是否成立判断 ID_{i2}的合法性. 由于 x_i是用户自己选定的，而 ID_{i1}是 TC 计算得到的，如果该等式成立，TC 完全相信 ID_{i2}是用户对 ID_{i1}的盲化身份.

至此，结束了三次身份信息验证和两次身份盲化. 三次身份信息的验证，确保了对方提供身份信息的准确性，有效防止了某一方的欺诈行为，提高了注册过程的安全性和系统的可靠性.

同时，如图 5 所示的 MI-(t,n)方案中，密钥的认证也是双向的，包括用户对可信中心颁发密钥的验证以及可信中心对用户自己选择密钥的验证. 具体过程如下：

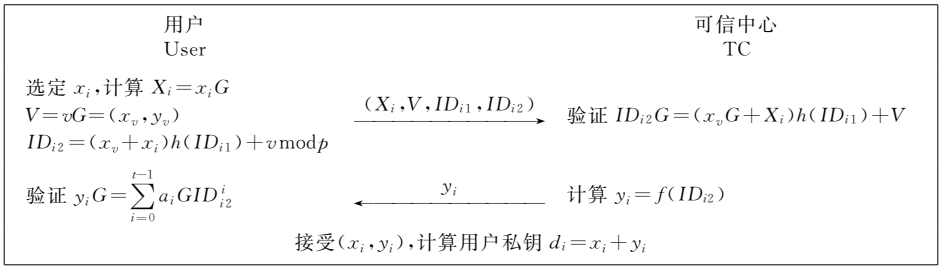


图 5　MI-(t,n)门限群签名密钥的认证过程

(1)用户自己选定密钥 $x_i\in_R Z_p^*$，计算 $X_i=x_iG$ 并公开. 利用 x_i盲化身份 ID_{i1}得到 ID_{i2}，并发送给 TC. TC 验证 $ID_{i2}G=(x_vG+X_i)h(ID_{i1})+V$ 是否成立判断是否接受 ID_{i2}. 由于 X_i对应于 x_i，ID_{i2}与 x_i绑定，那么如果该等式成立 TC 有理由相信 x_i为用户选择的部分私钥；

(2)TC 为用户颁发部分私钥 $y_i=f(ID_{i2})$，用户验证 $y_iG=\sum_{i=0}^{t-1}a_iGID_{i2}^i$ 是否成立决定 y_i是否是 TC 为其分配的秘密份额.

通过用户对可信中心颁发密钥的验证以及可信中心对用户自己选择密钥的验证，避免了 TC 颁发虚假密钥和用户提供虚假密钥的情况，保证了方案密钥分配的安全性.

最后，MI-(t,n)门限群签名方案并不完全依赖于对可信中心的信赖. 可信中心不能够陷害成员，威胁系统的安全性. 这主要通过下面两个方面得以保证：

(1)用户私钥由用户和可信中心共同生成，用户自己选定部分私钥 x_i，可信中心分配另一部分私钥 $y_i=f(ID_{i2})$. 并且对部分密钥进行交叉验证，防止欺诈行为；

(2)对用户身份进行两次盲化，第一次由可信中心通过自己的私钥生成，第二次由用户通过自己选择的私钥生成. 两次盲化处理，弱化了可信中心的绝对管理能力，防止可信中心伪造成员的盲化身份，陷害成员签名.

综上所述，MI-(t,n)门限群签名方案签名长度短，签名生成和签名验证的计算量低，安全性能优于现有门限群签名方案. 并且该方案实现了用户和可信中心的双向认证，确保了用户身份的合法性，避免了用户和可信中心的欺诈行为.

6 结束语

当前，移动互联网技术及应用得到了迅速的发展，而与此相对应的信息安全机制尤其是门限签名机制还没有有效的进展. 本文提出了一种新的适用于移动互联网的 ECC 门限群签名方案，通过用户和可信中心共同生成用户密钥来弱化可信中心的绝对权力，同时利用盲化后的身份处理签名保证用户真实身份的隐蔽性. 通过安全性证明和性能分析表明，本文所提出的 MI-(t,n)门限群签名方案能抵抗联合攻击和陷害攻击，克服了多种安全缺陷，同时具有较低的运算量和通信量. 经过适用性分析也验证了其适用于移动互联网的应用环境.

参 考 文 献

[1] Wang F, Zhou Y, Gu L, et al. Multi-policy threshold signature with distinguished signing authorities. Journal of China Universities of Posts and Telecommunications, 2011, 18(1): 113-120

[2] Zhang Z, Ye Y. A new ID-based threshold group signature scheme//Proceedings of the 8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM). Shanghai, China, 2012: 1-4

[3] Deng L, Zeng J. Two new identity-based threshold ring signature schemes. Theoretical Computer Science, 2014, 53(5): 38-45

[4] Hwang J Y, Kim H J, Lee D H, Song B. An enhanced (t,n) threshold directed signature scheme. Information Sciences, 2014, 275: 284-292

[5] Harn L. Group-oriented (t,n) threshold digital signature scheme and digital multisignature. IEE Proceedings-Computers and Digital Techniques, 1994, 141(5): 307-313

[6] Hong X. Efficient threshold proxy signature protocol for mobile agents. Information Sciences, 2009, 179(24): 4243-4248

[7] Li Hai-Feng, Lan Cai-Hui, Zuo Wei-Ping, et al. ID-based threshold group signature scheme without trusted party. Computer Engineering and Applications, 2012, 48(32): 89-93(in Chinese)
(李海峰，蓝才会，左为平等. 基于身份的无可信中心的门限群签名方案. 计算机工程与应用，2012，48(32)：89-93)

[8] Hwang M S, Lee C C. A new proxy signature scheme for a specified group of verifiers. Information Sciences, 2013, 227: 102-115

[9] Isern-DeyàA P, Huguet-Rotger L, Payeras-Capellà M M. On the practicability of using group signatures on mobile devices: Implementation and performance analysis on the android platform. International Journal of Information Security, 2014, 14(4): 335-345

[10] Yang C C, Chang T Y, Hwang M S. A new group signature scheme based on RSA assumption. Information Technology and Control, 2013, 42(1): 61-66

[11] Lin H Y, Hsieh M Y, Li K C. Secured map reduce computing based on virtual machine using threshold secret sharing and group signature mechanisms in cloud computing environments. Telecommunication System, 2015, 60(2): 303-313

[12] Chen T S, Hsiao T C, Chen T L. An efficient threshold group signature scheme//Proceedings of the Tencon IEEE Region 10 Conference. New York, USA, 2004, 167(1): 13-16

[13] Peng Ya. Research on Theory and Application of Threshold Digital Signature [M. S. dissertation]. Sun Yat-sen University, Guangzhou, 2010(in Chinese)
(彭娅. 门限数字签名理论及应用研究[硕士学位论文]. 中山大学，广州，2010)

[14] Xia Xiang-Sheng, Hong Fan, Geng Yong-Jun, et al. Efficient dynamic threshold group signature scheme based on elliptic curve cryptosystem. Journal of Southwest Jiaotong University, 2008, 16(1): 78-83

[15] Xie Dong, Li Jia-Jia, Shen Zhong-Hua. A new threshold signature scheme based on elliptic curve cryptosystem. Journal of Hangzhou Normal University (Natural Science Edition), 2013, 12(1): 57-60(in Chinese)
(谢冬，李佳佳，沈忠华. 一种新的基于椭圆曲线的门限群签名方案. 杭州师范大学学报(自然科学版)，2013，12(1)：57-60)

[16] Liu Hong-Wei, Xie Wei-Xin, Yu Jian-Ping. Efficiency identity-based threshold group signature scheme. Journal on Communications, 2012, 40(5): 54-60(in Chinese)

(刘宏伟，谢维信，喻建平. 基于身份密码体制的高效门限群签名方案. 通信学报，2012，40(5)：54-60)

[17] Yan Jie，Yin Xu-Ri，Zhang Wu-Jun. Research on group signature with threshold value based on elliptic curve. Journal of Southeast University (Natural Science Edition)，2008，38(A01)：43-46(in Chinese)
(闫杰，尹旭日，张武军. 基于椭圆曲线的带门限值的群签名研究. 东南大学学报(自然科学版)，2008，38(A01)：43-46)

[18] Chung Y F，Chen T L，Chen T S，Chen C S. A study on efficient group-oriented signature schemes for realistic application environment. International Journal of Innovative Computer and Information Control，2012，8(4)：2713-2727

[19] Dahshan H，Kamal A，RohiemA. A threshold blind digital signature scheme using ellipticcurve dlog-based cryptosystem// Proceedings of the 81st Vehicular Technology Conference. Glasgow，UK，2015：1-5

[20] Lin Yu-Bing. Design and Implementation of Identity Authentication Scheme Based on Elliptic Curve Cryptography on WSN [M. S. dissertation]. Zhejiang University of Technology，Hangzhou，2008(in Chinese)
(林玉炳. 无线传感器网络上基于椭圆曲线密码的认证方案设计与实现[硕士学位论文]. 浙江工业大学，杭州，2008)

附　录.　MI-(t,n)门限群签名方案的随机预言机模型(ROM)安全证明.

随机预言机模型(Random Oracle Module，ROM)是在理论情况下存在的一种模型，可将其视为 Hash 函数的理想化数学模型，其归约证明的思路为：首先形式化定义密码的安全性，假设攻击者能够以不可忽略的概率破坏协议的安全性(如破解加密信息或伪造签名)，然后虚拟一个模仿者 I，I 可以为攻击者提供一个与实际运行环境不可区分的模拟环境，I 回答攻击者所有的 oracle 询问，这样就可模拟攻击者能得到的所有信息，最后利用攻击者能够以不可忽略的概率破坏协议的安全性假设(如构造一个伪造签名)，设法解决某计算困难问题. 如果能够解决此计算难题，那么此协议安全性就归约到了解决此计算难题. 但实际上此计算难题到目前为止都是还没有有效解决，于是可以反证攻击者是不能以不可忽略的概率破坏所提方案的安全性. 那么由此可推出所要证明的门限群签名方案在实际应用环境中的安全性.

在本文中，我们首先给出 MI-(t,n)门限群签名方案的形式化模型：四个参与协议实体：移动终端用户 User(U)、验证者 Verifier(V)、可信中心 Trust Center(TC)和签名合成者 Signature Combiner(SC). MI-(t,n)门限群签名方案包括系统初始化、用户信息注册、份额签名生成、门限群签名生成、签名验证、签名打开和用户撤销七个部分.

若能证明 MI-(t,n)门限群签名在此形式化模型下是安全的，也就证明了实际中的 MI-(t,n)门限群签名是安全的.

本文利用随机预言机模型中的现实系统/理想系统模型，来证明形式化定义后的 MI-(t,n)门限群签名方案在随机预言机模型下是安全的.

首先简单介绍下理想系统/现实系统模型：现实系统中存在一些协议实体和控制了这些实体的攻击者 $\mathcal{A}$，另外还有环境 $\mathcal{E}$. 诚实实体之间按照协议过程操作，与环境 $\mathcal{E}$ 之间进行数据交互，环境 $\mathcal{E}$ 向诚实实体提供输入，同时接收其输出，环境 $\mathcal{E}$ 与攻击者 $\mathcal{A}$ 可任意交互，另外 $\mathcal{A}$ 控制了不诚实实体，所以也可与其他实体任意交互. 理想系统中，存在与现实系统中同样的协议实体以及一个可信第三方 T. 但这些协议实体并不像在现实系统中那样进行协议交互，而是向 T 输入数据，然后接受 T 的输出. T 执行的函数输出是所设计的安全协议预期要达到的功能. 理想系统中的实体不亲自完成协议过程，而通过 T 完成.

在这样一个理想系统/现实系统模型中，一个密码协议的安全性定义为：如果对于一个环境 $\mathcal{E}$ 和攻击者 $\mathcal{A}$，在理想系统中存在模拟者 I，I 与现实系统中的 $\mathcal{A}$ 控制着同样的实体，使得环境 $\mathcal{E}$ 不能区分它是在与现实系统中的 $\mathcal{A}$ 交互还是在与理想系统中的 I 交互. 若不能区分，则称此密码协议是安全的. 所以证明一个密码协议安全关键在于：先在理想系统中构建出可信方 T，然后构建模拟者 I，证明模拟者能够模拟 $\mathcal{A}$，使得环境 $\mathcal{E}$ 不能区分.

下面先给出 MI-(t,n)门限群签名协议的理想系统中可信方 T 的构建.

可信方 T 执行理想安全协议的功能，具体会执行以下几个操作：MI-(t,n)门限群签名的系统参数确立 Setup 协议；MI-(t,n)的用户注册信息 Regist 协议；MI-(t,n)的用户生成份额签名 Sign 协议；MI-(t,n)的合成门限群签名 Combine 协议；MI-(t,n)的签名验证 Verify 协议；MI-(t,n)的打开签名 Open 协议；MI-(t,n)的撤销成员 Revoke 协议.

T 的各个理想函数操作如下：

Setup 协议：

在可信中心 TC 执行系统创建过程中，T 设置(t,n)门限群签名系统的相关参数，搭建系统模型，并生成 TC 自身的密钥及系统所需函数.

Regist 协议：

T 接受用户的注册申请，通知 TC 随机生成 $u\in_R Z_p^*$，并计算：$U=uG=(x_u,y_u)$，$ID_{i1}=(x_u+s)h(ID_i)+u \bmod p$，将$(U,ID_{i1})$发送给用户. 用户接收到$(U,ID_{i1})$后，首先验证 $ID_{i1}G=(x_uG+T_p)h(ID_i)+U$，选定自己部分私钥 $x_i\in_R Z_p^*$，随机数 $v\in_R Z_p^*$ 发给 T，T 计算 $X_i=x_iG$，$V=vG=(x_v,y_v)$，$ID_{i2}=(x_v+x_i)h(ID_{i1})+v \bmod p$，然后将$(X_i,V,ID_{i1},ID_{i2})$发送给 TC，TC 首先验证 $ID_{i2}G=(x_vG+X_i)h(ID_{i1})+V$，然后通知 T 将用户的注册信息(X_i,ID_i,ID_{i2})添加到用户信息列表 List 中，TC 计算用户的另一部分私钥：$y_i=f(ID_{i2})$，通过 T 发送给用户，并在群里广播 a_iG，用户收到后验证 $y_iG=\sum_{i=0}^{t-1}a_iGID_{i2}^i$，生成了私钥 $d_i=x_i+y_i=x_i+f(ID_{i2})$，

公钥 $D_i=d_iG$. 并公开用户公钥 D_i 和用户身份信息 ID_{i2}.

Sign 协议：

每个群成员 U_i 利用私钥 d_i，对消息进行签名，生成份额签名，具体步骤为：U_i 随机选择 $k_i\in_R Z_p^*$ 并发送给 T，T 计算 $r_i=k_iG=(x_{r_i},y_{r_i})$，计算消息的哈希值 $z=h(m)$，计算份额签名 $s_i=k_ix_{r_i}-zd_iI_i \bmod p$，其中 $I_i=\prod_{i\neq j}\frac{ID_{i2}}{ID_{i2}-ID_{j2}}(i,j\in[1,t])$，计算 $ID'_{i2}=E_{PK_{SC}}(RAND\|ID_{i2})$，$T$ 将份额签名 (r_i,s_i) 和 ID'_{i2} 发送给签名合成者 SC.

Combine 协议：

SC 收到成员 U_i 的份额签名 (r_i,s_i) 后，分别验证其正确性，首先使用自身私钥 SK_{SC} 解密 ID'_{i2} 得到签名者的盲化身份 ID_{i2}，并发送给 T，然后 T 计算 $I_i=\prod_{i\neq j}\frac{ID_{i2}}{ID_{i2}-ID_{j2}}$；接着计算 z. 接着验证等式 $s_iG+zD_iI_i=r_ix_{r_i}$.

在签名的合成方面，当所有份额签名验证合法后 T 计算 $R=\sum_{i=1}^{t}r_ix_{r_i} \bmod p$，然后将所有份额签名合并，计算 $S=\sum_{i=1}^{t}s_i$，再计算 $W=\sum_{i=1}^{t}I_iX_i$ 并公开. SC 生成门限群签名 (R,S)，并通过 T 将其发送给验证者，同时将参与群体的用户签名信息 (r_i,s_i,ID_{i2}) 及相应的群签名 (R,S) 添加到签名信息列表 SignList 中.

Verify 协议：

签名验证者 V 接收到门限群签名 (R,S) 后，根据 $z=h(m)$ 计算 z，并验证 $SG+z(g_p+W)=R$ 是否成立.

Open 协议：

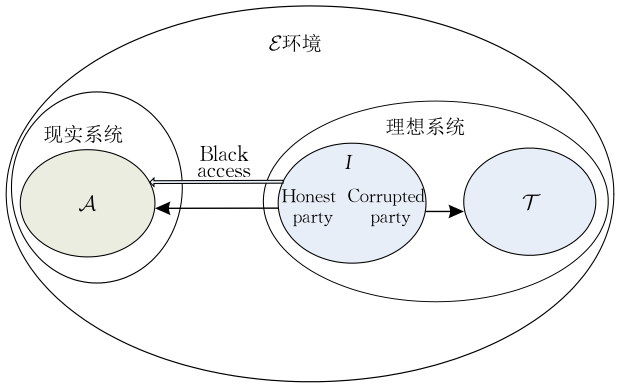
TC 将签名 (R,S) 发送给 SC. SC 查询签名信息列表 SignList，找到对应于 (R,S) 的 (r_i,s_i,ID_{i2})，SC 将盲化身份 ID_{i2} 发送给 TC，TC 查询用户信息列表，找到对应于盲化身份 ID_{i2} 的用户信息 (X_i,ID_i,ID_{i2})，进而确定用户的真实身份 ID_i.

Revoke 协议：

重新秘密选定一个 $t-1$ 次多项式：$f(x)=a'_{t-1}x^{t-1}+a'_{t-2}x^{t-2}+\cdots+a'_2x^2+a'_1x+a_0$ 并发送给 T，T 分别为成员重新计算部分密钥 $y_i=f(ID_{i2})$，每个成员执行 Register 过程中的第 4 个步骤.

下面给出模拟者 I 的构建：

模拟者 I 的作用有两个：(1) 使得攻击者 $\mathcal{A}$ 不能区分自身所处环境是理想系统还是现实系统，要达到这个要求，主要需要 I 在与 $\mathcal{A}$ 交互时，能成功模拟诚实实体. 现实系统中，I 通过对 $\mathcal{A}$ 的黑盒访问，获得 $\mathcal{A}$ 在协议的真实执行中发送的信息，然后，通过随机选择参数，利用强大的预言机功能，模仿诚实实体向 $\mathcal{A}$ 提供 $\mathcal{A}$ 期望接收到的信息，使 $\mathcal{A}$ 感觉依然处于现实环境中，而不是一个模拟环境；(2) 在理想系统与现实系统之间作为媒介，使两个系统的协议运行一致，使环境 $\mathcal{E}$ 不能区分身处哪个系统. 理想系统中，I 控制着现实系统中 $\mathcal{A}$ 所控制的那些实体，利用之前与 $\mathcal{A}$ 交互时从 $\mathcal{A}$ 那获取的有用信息模拟 $\mathcal{A}$，代表被攻陷实体请求 T 进行相应操作，使两个系统的参数输出计算不可区分. 模拟者 I 的原理示意图如附图 1.



附图 1 模拟者 I 的原理示意图

I 在 MI-(t,n) 门限群签名协议中的具体模拟过程如下：

Setup 模拟：现实系统中 I 模拟可信中心 TC，设置 (t,n) 门限群签名系统的相关参数，搭建系统模型，并将相关参数公布给 $\mathcal{A}$. 理想系统中 I 不做操作.

Regist 模拟：现实系统中，I 模拟 TC，接收 $\mathcal{A}$ 发送的 $u\in_R Z_p^*$，然后在模拟系统中，模拟被 $\mathcal{A}$ 控制的用户，用 $u\in_R Z_p^*$ 向 T 申请注册，T 计算：$U=uG=(x_u,y_u)$，$ID_{i1}=(x_u+s)h(ID_i)+u \bmod p$，将 (U,ID_{i1}) 发送给 I. I 接收到 (U,ID_{i1}) 后，在现实系统中将其发送给 $\mathcal{A}$. 随后 $\mathcal{A}$ 会验证 $ID_{i1}G=(x_uG+T_p)h(ID_i)+U$，选定自己部分私钥 $x_i\in_R Z_p^*$，随机数 $v\in_R Z_p^*$ 发给 I，I 在模拟系统中再转发给 T，由 T 计算 $X_i=x_iG$，$V=vG=(x_v,y_v)$，$ID_{i2}=(x_v+x_i)h(ID_{i1})+v \bmod p$，然后将 (X_i,V,ID_{i1},ID_{i2}) 发送给 TC，TC 首先验证 $ID_{i2}G=(x_vG+X_i)h(ID_{i1})+V$，然后通知 T 将用户的注册信息 (X_i,ID_i,ID_{i2}) 添加到用户信息列表 List 中，TC 计算用户的另一部分私钥：$y_i=f(ID_{i2})$，通过 T 发送给 I，并在群里广播 a_iG，I 在现实系统中将 y_i 发送给 $\mathcal{A}$，并广播 a_iG，$\mathcal{A}$ 收到后验证 $y_iG=\sum_{i=0}^{t-1}a_iGID_{i2}^i$，生成了私钥 $d_i=x_i+y_i=x_i+f(ID_{i2})$，公钥 $D_i=d_iG$. 并公开用户公钥 D_i 和用户身份信息 ID_{i2}.

Sign 协议：

在现实系统中，$\mathcal{A}$ 利用私钥 d_i，对消息进行签名，生成份额签名，具体步骤为：$\mathcal{A}$ 随机选择 $k_{i'}\in_R Z_p^*$ 计算 $r_{i'}=k_{i'}G=(x_{r_{i'}},y_{r_{i'}})$，计算消息的哈希值 $z=h(m)$，计算份额签名 $s_{i'}=k_{i'}x_{r_{i'}}-zd_{i'}I_{i'} \bmod p$，其中 $I_{i'}=\prod_{i'\neq j}\frac{ID_{i'2}}{ID_{i'2}-ID_{j2}}(i',j\in[1,t])$，计算 $ID'_{i'2}=E_{PK_{SC}}(RAND\|ID_{i'2})$，最后 $\mathcal{A}$ 将 $(r_{i'},s_{i'})$ 和 $ID'_{i'2}$ 发送给 I.

I 在模拟系统中检查份额签名 $(r_{i'},s_{i'})$，I 首先使用 SC 私钥 SK_{SC} 解密 $ID'_{i'2}$ 得到签名者的盲化身份 $ID_{i'2}$，然后验证 $ID_{i'2}=ID_{i2}$，如果不相等，则说明 $\mathcal{A}$ 模仿群里的其他成员 i' 签名，将份额签名 $(r_{i'},s_{i'})$ 发送给 T，T 将份额签名 $(r_{i'},s_{i'})$ 和 $ID'_{i'2}$ 发送给签名合成者 SC.

Combine 协议：

在现实系统中，I 模拟 SC 对份额签名进行验证：证明等式 $s_iG+zD_iI_i=r_ix_{r_i}$ 是否成立. 如果成立，那么份额签名

(r_i, s_i)合法，否则拒绝该份额签名. 如果在 Sign 协议中检测到$\mathcal{A}$模仿群里的其他成员签名，且份额签名(r_i, s_i)合法，则停止模拟，模拟失败 failure1，若没有检测到$\mathcal{A}$模仿群里的其他成员签名，且份额签名(r_i, s_i)合法，则 I 继续模拟 SC，完成门限群签名. 在模拟系统中，T 和 SC 合作完成门限群签名(R, S)，将参与群体的用户签名信息(r_i, s_i, ID_{i2})及相应的群签名(R, S)添加到签名信息列表 SignList 中.

Verify 协议：

I 在现实系统中模拟 V 对门限群签名(R, S)进行验证，首先根据 $z=h(m)$计算 z，并验证 $SG+z(g_p+W)=R$ 是否成立. 如果成立则接收签名，否则拒绝该门限群签名.

Open 协议和 Revoke 协议由模拟系统中的 T 完成，I 只需将结果返回给$\mathcal{A}$.

可以看出，只要 I 模拟过程中不会出现上述 failure1，I 就会成功模拟$\mathcal{A}$，使环境$\mathcal{E}$不可区分，从而可以证明 MI-(t, n)门限群签名协议的安全性.

下面只需要证明 I 在模拟过程中出现的 failure 发生概率可忽略即可. 证明方法使用 RO 模型中的归约证明方法.

假设 failure1 发生了，则模拟者 I 检测出攻击者$\mathcal{A}$伪造其他用户 i'的份额签名，且该签名通过了模拟者 I 的份额签名认证，分析该份额签名的认证过程，关键在于等式：$s_i G+zD_i I_i=r_i x_{r_i}$，其中$(r_i, s_i)$为份额签名.

$r_i=k_i G=(x_{r_i}, y_{r_i})$，而 k_i 为随机数 $k_i \in_R Z_p^*$，G 为系统公开参数，所以 r_i, x_{r_i} 都可由攻击者$\mathcal{A}$伪造且合法.

$s_i=k_i x_{r_i}-zd_i I_i \bmod p$，其中 p 为系统公开参数；$I_i=\prod_{i\neq j}\frac{ID_{i2}}{ID_{i2}-ID_{j2}}$，攻击者$\mathcal{A}$可计算获得；$z=h(m)$为消息哈希值，攻击者$\mathcal{A}$已知；$r_i=k_i G=(x_{r_i}, y_{r_i})$，而 k_i 为随机数 $k_i \in_R Z_p^*$，所以 k_i, x_{r_i} 都可由攻击者$\mathcal{A}$伪造且合法；而 $D_i=d_i G$，攻击者$\mathcal{A}$在只知道用户公钥 D_i 和参数 G 的情况下，求出私钥 d_i，这等同于解决椭圆曲线上的离散对数难题，在计算上是不可行的，所以可以反推出 failure 1 的发生概率可忽略.

综上所述，在一个 MI-(t, n)门限群签名协议中，当攻击者$\mathcal{A}$能够发生伪造签名的不合法行为时，模拟者 I 能够发现，并输出模拟失败，但 I 的模拟失败总是对应着一个密码学难题的攻破，所以 I 是不会模拟失败的. 当 I 能成功模拟时，$\mathcal{A}$在协议过程中所用的关键信息，都是 I 在模拟诚实实体时发送的，而另外一些信息，I 都能通过所控制预言机的强大功能知晓. 所以 I 在 MI-(t, n)门限群签名协议的理想系统中可成功模拟现实系统中攻击者$\mathcal{A}$的行为；另外由于 I 拥有随机预言机的强大功能以及可信第三方 T 的理想函数性，I 模拟过程中随机选择的参数输出将和真实协议中的输出计算不可区分，所以环境$\mathcal{E}$不能分辨自身是运行在理想系统中还是现实系统中. 根据随机预言机模型的安全性定义，可知 MI-(t, n)门限群签名协议在随机预言机模型下是安全的.

CHEN Li-Quan, born in 1976, Ph.D., associate professor, Ph. D. supervisor. His current research interests include information security and mobile Internet.

ZHU Zheng, born in 1991, M. S. candidate. His research interests include encryption and signature, mobile Internet.

WANG Mu-Yang, born in 1992, M. S. candidate. His research interests include authentication and signature.

SUN Xiao-Yan, born in 1990, M. S. candidate. Her research interests include information security, authentication and signature.

Background

Currently, security application in mobile Internet has gotten more attention than before. There are lots of open problems that need further investigation to make mobile Internet application more secure. Among them, the mobile applications based on threshold group signature such as mobile electronic voting system, mobile joint shopping are particularly urgent for security. However, there was not a good security solution put forward for this mobile application. In those existing elliptic curve cryptography (ECC) threshold group signature schemes with a trusted center, the authentication of trusted center from group member is always lacked. Thus, the trusted center may become a security bottleneck of the whole signature system.

In this article, a threshold group signature scheme based on ECC and suitable for mobile Internet is proposed. The proposed scheme puts forward an idea that the group members and trusted center generate the members' secret keys together. Moreover, the group members and trusted center implement mutual identity authentication, while the key generation and twice blind processing of members' identities are used in the proposed scheme. Based on secure proof, the proposed scheme is proved to be correct and secure.

This work was supported by the National Natural Science Foundation of China under Grant No. 61372103, the National High Technology Research and Development Program of China (863 Program) under Grant No. 2013AA014001, and the Joint Project between ZTE Corp. and Southeast University. All these projects focus on the researches on information security in mobile network and Internet of Things.