

轻量级门限群签名方案的改进

竺智荣^{1,2}, 吕佳玉^{1,2}, 叶帼华^{1,2}, 姚志强^{1,2}

(1. 福建师范大学数学与信息学院, 福建 福州 350117;

2. 福建省公共服务大数据挖掘与应用工程技术研究中心, 福建 福州 350108)

摘要: 为了提高门限群签名在 5G 环境下的安全性和效率, 提出一个新的解决方案。核心思想是通过引入消息令牌和动态身份, 提高认证信息的新鲜性, 加大敌手攻击难度; 同时精简参与各方的交互次数, 并将部分计算任务迁移至服务器, 减少成员部分计算开销。经过安全分析, 所提方案可抵抗包括重放攻击在内的多种攻击; 经过性能分析, 所提方案比同类方案减少了两次与可信中心的交互, 签名占用空间缩小 30%, 具有更短的执行时间, 适用于 5G 网络下的资源受限设备。

关键词: 门限群签名; 5G 网络; 轻量级; 重放攻击

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020048

Improvement of lightweight threshold group signature scheme

ZHU Zhirong^{1,2}, LYU Jiayu^{1,2}, YE Guohua^{1,2}, YAO Zhiqiang^{1,2}

1. School of Mathematics and Information, Fujian Normal University, Fuzhou 350117, China

2. Fujian Engineering Research Center of Public Service Big Data Mining and Application, Fuzhou 350108 China

Abstract: In order to improve the security and efficiency of threshold group signature in 5G environment, a new scheme was proposed. The core idea was to introduce message token and dynamic identity to improve the freshness of authentication information and increase the difficulty of enemy attacks. At the same time, the number of interactions between the participating parties was simplified, and some computing tasks were migrated to the server to reduce the computing overhead of the member part. After security analysis, the proposed scheme can resist multiple attacks including replay attack. After performance analysis, the proposed scheme can reduce the interaction with the trusted center twice compared with similar schemes, reduce the signature space by 30%, and have shorter execution time, which is suitable for resource-constrained devices under 5G network.

Key words: threshold group signature, 5G network, light weight, replay attack

收稿日期: 2020-02-25; 修回日期: 2020-05-19

通信作者: 姚志强, yzq@fjnu.edu.cn

基金项目: 国家自然科学基金 (61872090, 61972096)

Foundation Item: The National Natural Science Foundation of China (61872090, 61972096)

论文引用格式: 竺智荣, 吕佳玉, 叶帼华, 等. 轻量级门限群签名方案的改进[J]. 网络与信息安全学报, 2020, 6(4): 120-129.

ZHU Z R, LYU J Y, YE G H, et al. Improvement of lightweight threshold group signature scheme[J]. Chinese Journal of Network and Information Security, 2020, 6(4): 120-129.

1 引言

5G网络作为新一代移动通信技术,引发了各国学术界和工业界的普遍关注。5G运用超密集网络结构、D2D通信以及一系列空中接口技术进一步提高了频谱利用率,同时极大地提升了数据的传输速度,增强了用户体验。为了适应不断增长的数据总量和多样化的业务需求,要求5G网络具备高速率、低延时、低能耗、安全可靠的特点,由此催生了一系列对传输延迟和数据安全有较高要求的新应用,如移动医疗、自动驾驶以及智慧城市等。随着物联网技术的不断发展,5G网络主要的服务对象是数量庞大的移动终端用户,虽然目前移动设备的计算能力已有长足进步,但其能量资源依然有限,为保证设备处理较大量信息时能长久续航,且进一步提高传输速率和绿色计算能力,应继续轻量化5G应用。

为达到轻量化的效果,针对会议投票、合同签署以及共享资源管理等具体应用场景,本文在陈立全等^[1]的研究成果之上提出一个新的轻量级门限群签名方案,旨在适应5G网络带来的新变化:5G网络的频段提升,达到全覆盖,必然增多基站数量和增大密集化程度,同时增加数据在传输过程中被敌手窃听和篡改的风险,于是要求新的方案能够抵抗包括重放攻击在内的各种攻击,并且减少参与各方的信息交互次数,以达到减少时延的同时降低被攻击的风险。此外,需要在方案中合理分配计算任务,在保证安全性的前提下达到轻量化的效果。

2 相关工作

有关门限群签名或秘密共享的研究成果,可以依据是否有可信中心区分为两类。Jia等^[2]提出一种基于中国剩余定理的无可信中心的秘密共享方案,其核心是一个素数矩阵,可以配合公共广播信道随时激活不同的阈值,但方案中缺少成员之间的相互认证,容易被敌手利用,不适合5G网络的复杂环境。Rui等^[3]提出一种针对电子健康档案系统的多权限安全签名方案,其中没有可信中心或权限生成者,避免了托管问题,该方案可以抵抗伪造攻击以及合谋攻击;Sun等^[4]提出一

种应用于医疗系统的签名方案,该方案基于线性秘密共享机制,可以在不暴露签名者身份的情况下,有效验证签名者的属性,并且分散属性的签名特性使其适用于分布式区块链系统,具有借鉴意义,只是在健康档案管理的应用场景实例中,若想打开档案以确认患者身份,必须由患者同意,这样自然限制应用场景的拓广。

以上是无可信中心的解决方案,考虑到移动设备的资源限制,需要将部分计算任务迁移至第三方服务器,进而出现有可信中心的解决方案,Yu等^[5]提出的门限群签名方案将椭圆曲线短密钥的特点与门限方法相结合,在一定程度上降低了计算复杂度,但在方案中没有提供追踪成员和撤销成员的方法;Xia等^[6]提出动态的门限群签名方案,加入了对于成员追踪和撤销的方法,但该方案无法抵抗合谋攻击;Hwang等^[7]提出的签名方案可以在出现问题时由签名者或指定验证者帮助验证签名,同时作者证明了该方案可以抵抗流氓攻击(rogue-key attack),但方案缺乏签名者对于可信第三方的反向验证,存在复制攻击的风险;Li等^[8]提出一种新的群签名方案用以保护移动用户的位置隐私,他们将群签名与蜂窝网络中的区域概念相结合,使位于同一区域的收集器具有可识别性,从而实现了收集器的匿名性和位置隐私性,该方案具有较低的计算复杂度和较高的安全性,但在方案中没有给出签名打开的方法,无法在发生争议时确定相关责任人;Dan等^[9]提出一种将阈值功能添加到非阈值加密方案的通用方法,可以将密钥拆成若干份,交由多方保管,该方案构造的门限签名具有很高的安全性,但是由于计算复杂度,只适合短距离的大型加密系统,不适合长距离的5G通信。

针对5G网络的新特性,本文提出一个更加快速、轻量和安全的解决方案,以适应未来的新环境,主要贡献如下。

(1) 提出一个新的门限群签名方案,加入了令牌和动态身份,并精简了交互次数和签名长度。

(2) 经过分析比较,证明了本文方案相比现有方案,具有更高的安全性和更低的计算复杂度。

3 设计目标和威胁模型

3.1 设计目标

本文方案的设计目标如下。

(1) 基本要求：需要保证门限特性、成员匿名性以及可追踪性等门限群签名方案的基本特性。

(2) 抵抗攻击：不仅能抵抗陷害攻击和联合攻击等常见攻击，还能抵抗重放攻击。

(3) 高效节能：可实现更快的处理速度和更低的计算复杂度。

3.2 威胁模型

在实现门限群签名的同时，5G 网络由于环境的开放性，将会遭遇敌手对于传输数据的窃听和捕获，或参与成员的陷害与合谋，进而产生各种类型的攻击，主要包括以下几种。

(1) 重放攻击：敌手捕获参与者发送过的数据包，对其进行重新发送，借此达到欺骗目标系统的目的。

(2) 复制攻击^[10]：广义的复制攻击指外部敌手通过公开信息冒充合法成员参与通信；狭义的复制攻击指外部敌手通过某种未知的方法，在某一时刻获得合法成员的一个或几个秘密参数，再冒充成员参与通信。

(3) 陷害攻击：分为两种情况，情况①是内部成员 U_z 利用已知信息冒充内部成员 U_x 参与签名；情况②是可信中心利用已知信息冒充成员 U_x 参与签名。

(4) 联合攻击：组织中的部分成员联合，企图生成一个合法的签名，以通过各项验证。这里将联合攻击分为 3 种情况：情况①是联合人数少于门限值 t ；情况②是联合人数大于或等于门限值 t ；情况③是可信中心与部分成员联合。

4 方案构造

4.1 方案流程

如图 1 所示，门限群签名方案主要由三方组成：组织成员、可信中心和群签名验证者。

(1) 组织成员：分为注册成员和非注册成员，若想要参与决策，需要先向可信中心进行注册，注册成功后才可以产生有效的部分签名。

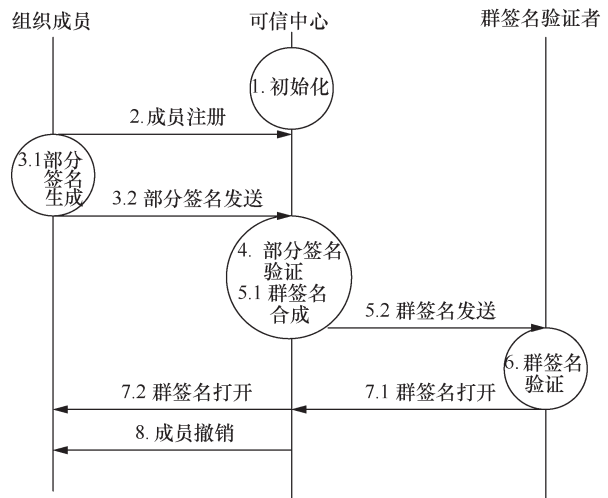


图1 门限群签名系统流程
Figure 1 Threshold group signature system flow

(2) 可信中心：主要负责成员的注册、部分签名的验证以及群签名的合成。

(3) 群签名验证者：主要负责群签名的验证，以及发生争议时的仲裁。

系统的整个流程包括 8 个部分：系统初始化、成员注册、部分签名生成、部分签名验证、群签名合成、群签名验证、群签名打开和成员撤销。其中，系统初始化是在第一次使用系统时进行，成员注册是在非注册成员第一次申请注册时进行，而群签名的打开和成员的撤销是在发生争议时进行。

4.2 具体设计

本文以抗重放攻击、提高安全性、折中安全与效率之间关系为主，在以下 4 个环节加以改进：① 加入令牌以预防重放攻击；② 采用动态身份和注册凭证以提高安全性；③ 优化交互次数和签名空间以提高效率；④ 完善细节使方案达到安全与效率的平衡。

接下来，阐述改进方案的具体设计。为了便于理解，先以表格的形式给出在本文中出现的符号及其含义，如表 1 所示。

(1) 系统初始化

首先，确定注册成员规模为 n ，门限值为 t ($t < n$)，均为正整数。

接着，构造椭圆曲线。选定两个大素数 p 和 q ，构造有限域 F_p 上的椭圆曲线 $y^2 = x^3 + ax + b$ ，其中 a, b 满足 $4a^3 + 27b^2 \neq 0 \pmod{p}$ ，选定阶为

q 的基点 P 构成加法循环群 G 。选择两个单向函数 $H_1: \{0,1\}^* \rightarrow Z_q^*$, $H_2: \{0,1\}^* \times G \rightarrow Z_q^*$, 其中 H_2 是将椭圆曲线上的点映射到数值的哈希函数, 运算方法为先做椭圆曲线上的点乘运算, 再将得到结果的横纵坐标值相加, 接着模 q 完成哈希运算。

表 1 符号说明
Table 1 Notations and their meanings

符号	含义
n	群大小
t	门限值
p, q	大素数
P	基点
G	循环群
H_1, H_2	哈希函数
g_s	群私钥
g_p	群公钥
TC	可信中心
T_s	可信中心私钥
T_p	可信中心公钥
$\beta_{U_i}, A_{U_i}, F_{U_i}$	验证信息
M_{U_i}	注册凭证
c_0, c_1, c_2	伪随机数
ID_i	成员身份标识
DID_{i1}	成员动态身份
x_i	成员部分私钥
y_i	成员部分私钥
d_i	成员完整私钥
D_i	成员公钥
sig_i	部分签名
Sig	群签名
I_i	插值系数
T_{U_i}	消息令牌

最后, 对系统参数做初始化。秘密选择一个 $t-1$ 次多项式 $f(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \dots + a_2x^2 + a_1x + a_0$, 其中 $a_i \in [1, q-1] (i = 0, 1, \dots, t-1)$ 均为整数。设置群私钥为 $g_s = f(0) = a_0$, 群公钥 $g_p = f(0)P = a_0P$ 。选择可信中心 TC 的私钥 $T_s \in Z_q^*$, 计算公钥 $T_p = T_sP$ 。

公开参数 P, T_p, g_p, q, H_1, H_2 。

(2) 成员注册

非注册会员想要加入组织获得决策权, 需要先向 TC 进行注册。

首先, 成员发送注册信息。成员选择 $x_i \in Z_q^*$ 作为自己的部分私钥, 并计算 $X_i = x_iP$; 选择随机数 $c_0 \in Z_q^*$, 并计算 $\beta_{U_i} = H_1(ID_i \| X_i \| c_0)$, 其中, 当点遇到级联操作时, 是先将横纵坐标相加后再进行的; 成员将 $\{ID_i, X_i, \beta_{U_i}\}$ 发送给 TC。

接着, TC 处理注册信息。TC 首先判断成员是否注册, 有则跳过; 没有则选择随机数 $c_1 \in Z_q^*$, 并计算 $A_{U_i} = c_1P$ 和注册凭证 $M_{U_i} = H_2(A_{U_i}, \beta_{U_i}) \cdot T_s \bmod q + c_1$, 再计算注册成员的另一部分私钥 $y_i = f(ID_i)$ 和动态身份 $DID_{i1} = H_1(ID_i \| c_1)$, 建立关联表 $\{ID_i, DID_{i1}, X_i\}$ 。TC 用 X_i 对 y_i 和 DID_{i1} 进行加密, 将 $\{E_{X_i}(y_i \| DID_{i1}), M_{U_i}, A_{U_i}\}$ 发送给成员。

最后, 成员对 TC 进行反向认证。成员在收到 TC 的回复后, 验证 $M_{U_i} \cdot P = H_2(A_{U_i}, \beta_{U_i}) \cdot T_p \bmod q + A_{U_i}$ 是否成立, 验证失败则重新申请, 若连续失败多次需发出警报; 验证成功则结合两个部分私钥计算注册成员完整的私钥 $d_i = x_i + y_i = x_i + f(ID_i)$ 和公钥 $D_i = d_iP$, 注册成功。

(3) 部分签名生成

成员在注册成功之后, 即可对消息 m 生成自己的部分签名。

首先, 选择随机数 $c_2 \in Z_q^*$, 并计算 $F_{U_i} = c_2 \cdot P$ 。

接着, 生成用于保证消息新鲜性的令牌 $T_{U_i} = H_2(m, F_{U_i})$ 。

最后, 生成部分签名 $\text{sig}_i = d_i I_i + M_{U_i} T_{U_i}$ 。其中, I_i 通过每位注册成员的公开身份集合

$ID = \{ID_1, ID_2, \dots, ID_t\}$ 计算, 即 $I_i = \prod_{j=1, i \neq j}^t \frac{-ID_j}{ID_i - ID_j}$ 。

每位成员将 $\{DID_{i1}, \text{sig}_i, T_{U_i}\}$ 发送给 TC。

(4) 部分签名验证

TC 在合成群签名之前, 需要先验证部分签名的合法性。

首先, 验证动态身份。为了防止复制攻击或其他不知名的攻击, TC 需要通过查表确定 DID_{i*} 。

是否是由 TC 之前所派发并记录在关联表中, 顺便确定签名者身份。若无记录, 则签名无效; 若有记录, 则继续进行下一步验证, 并重新计算动态身份 $DID_{i2} = H_1(DID_{i1} \| c_3)$, 其中, 随机数 $c_3 \in Z_q^*$ 。将新的动态身份加密后发给用户, 更新关联表 $\{ID_i, DID_{i1}, DID_{i2}\}$, 其中, 旧的动态身份保留到下一次该成员产生可验证的部分签名为止。

接着, 验证消息令牌。为了防止重放攻击, TC 需要比较成员发送的令牌 T_{U_i} 是否与上一次产生变化。若相同, 则签名无效, 要求重发 (动态身份验证失败不能重发, 令牌验证失败可以重发); 若不同, 则验证通过, TC 用新令牌更换关联表 $\{ID_i, DID_{i1}, T_{U_i}\}$ 中的旧令牌。

如果该成员是第一次参与签名, 则无须进行上述比较, 只需要进行相应的更改和替换。

最后, 验证部分签名。TC 验证等式 $\text{sig}_i \cdot P = (d_i I_i + M_{U_i} T_{U_i})P = D_i I_i + H_2(A_{U_i}, \beta_{U_i}) T_p T_{U_i} \bmod p + A_{U_i} T_{U_i}$ 是否成立。若不成立, 则拒绝; 若成立, 则接收, 并将部分签名加入关联表 $\{ID_i, \text{sig}_i\}$ 。

(5) 群签名合成

TC 对验证成功的部分签名进行合成。

首先, 将部分签名合并 $\text{Sig} = \sum_{i=1}^l \text{sig}_i$ 。

接着, 计算验证信息 $W = \sum_{i=1}^l I_i X_i$, $Y = \sum_{i=1}^l H_2(A_{U_i}, \beta_{U_i}) T_p T_{U_i}$, $Z = \sum_{i=1}^l A_{U_i} T_{U_i}$ 。

最后, 将群签名 Sig 加入关联表 $\{ID_i, \text{sig}_i, \text{Sig}\}$, 并将 $\{\text{Sig}, W, Y, Z\}$ 发送给群签名验证者。

(6) 群签名验证

群签名验证者对 TC 发送的群签名进行验证。验证者验证等式 $\text{Sig} \cdot P = W + g_p + Y + Z$ 是否成立。若成立, 则群签名有效; 若不成立, 则拒绝接收签名和相关信息。

(7) 群签名打开

群签名验证者可以在 TC 的帮助下将群签名打开, 确认签名者的真实身份。

首先, 群签名验证者将 Sig 发送给 TC, 请求打开群签名, 确认签名者身份。

接着, TC 根据 Sig 通过查找关联表, 确认参

与签名的人群。

最后, 通过关联表中的 $\{ID_i, \text{sig}_i\}$ 进一步确认签名者的真实身份。

(8) 群成员撤销

当组织中有成员需要离开时, TC 会进行相应的处理, 避免该行为对组织造成不良的影响。

首先, TC 重新选择一个秘密的 $t-1$ 次多项式

$$f'(x) = a'_{t-1}x^{t-1} + a'_{t-2}x^{t-2} + \cdots + a'_2x^2 + a'_1x + a_0$$

接着, TC 对除了离开组织外的每位注册成员重新计算部分私钥 $y'_i = f'(ID_i)$ 。

最后, 成员重新执行上一步骤中对 TC 的反向验证, 确认是否接收 y'_i 。验证成功后, 重新计算完整私钥 $d'_i = x_i + y'_i = x_i + f'(ID_i)$ 。

当以上步骤全部完成时, 成功将成员撤销。

5 方案安全性分析

5.1 有效性分析

(1) 成员对 TC 反向验证的有效性证明

在成员注册阶段, 成员通过验证等式 $M_{U_i} \cdot P = H_2(A_{U_i}, \beta_{U_i}) \cdot T_p + A_{U_i}$ 是否成立, 来判断 TC 是否可信。由 $M_{U_i} = H_2(A_{U_i}, \beta_{U_i}) \cdot T_s + c_1$, $T_p = T_s P$ 和 $A_{U_i} = c_1 P$ 可得等式两边相等; 又因为 T_s 是 TC 的私钥, 当等式成立时可以证明对方是 TC。

(2) 验证部分签名的有效性证明

验证部分签名阶段, TC 通过验证等式 $\text{sig}_i \cdot P = D_i I_i + H_2(A_{U_i}, \beta_{U_i}) T_p T_{U_i} + A_{U_i} T_{U_i}$ 是否成立来判断部分签名是否可信。由 $\text{sig}_i = d_i I_i + M_{U_i} T_{U_i}$ 和 $D_i = d_i P$, 加上有效性分析 (1) 中的证明, 可以得出等式两边相等; 又因为 d_i 是成员的私钥, 并且部分签名的组成中包含 TC 的私钥, 当等式成立时可以证明这是一个合法的部分签名。

(3) 验证群签名的有效性证明

验证群签名阶段, 群签名验证者通过验证等式 $\text{Sig} \cdot P = W + g_p + Y + Z$ 成立来判断群签名是否可信。

$$\begin{aligned} \text{Sig} \cdot P &= \sum_{i=1}^l \text{sig}_i \cdot P = \sum_{i=1}^l (d_i I_i + M_{U_i} T_{U_i}) P = \\ &= \sum_{i=1}^l [(x_i + y_i) I_i + H_2(A_{U_i}, \beta_{U_i}) \cdot T_s \cdot T_{U_i} + c_1 \cdot T_{U_i}] P = \end{aligned}$$

$$\begin{aligned} & \sum_{i=1}^t x_i P I_i + \sum_{i=1}^t y_i I_i P + \sum_{i=1}^t H_2(A_{U_i}, \beta_{U_i}) \cdot T_s P \cdot T_{U_i} + \\ & \sum_{i=1}^t c_i P T_{U_i} = \sum_{i=1}^t X_i I_i + \sum_{i=1}^t (f(\text{ID}_i) I_i P) + \\ & \sum_{i=1}^t H_2(A_{U_i}, \beta_{U_i}) T_p T_{U_i} + \sum_{i=1}^t A_{U_i} T_{U_i} \end{aligned} \quad (1)$$

由拉格朗日插值定理可得

$$\begin{aligned} & \sum_{i=1}^t (f(\text{ID}_i) I_i P) = \\ & \left(\sum_{i=1}^t (f(\text{ID}_i)) \prod_{j=1, j \neq i}^t \frac{-\text{ID}_j}{\text{ID}_i - \text{ID}_j} \right) P = f(0) P = g_p \end{aligned} \quad (2)$$

又因为

$$\begin{aligned} W &= \sum_{i=1}^t X_i I_i, \\ Y &= \sum_{i=1}^t H_2(A_{U_i}, \beta_{U_i}) T_p T_{U_i}, \quad Z = \sum_{i=1}^t A_{U_i} T_{U_i} \end{aligned}$$

可知等号两边相等。

5.2 安全性分析

(1) 抗重放攻击证明

根据 3.2 节威胁模型 (1) 分析方案抵抗重放攻击的能力。现对本文方案中各方的交互进行逐条分析。①第一条交互信息是成员对 TC 发送的注册信息。若该数据包被重复发送, TC 会因检测到该成员已经注册而跳过, 不会造成任何危害。②第二条交互信息是 TC 发送注册信息和部分私钥给对应成员。若该数据包被重复发送, 成员会重新计算私钥 $d_i = x_i + y_i$, 但由于各部分私钥没有发生变化, 所以不会造成任何危害。③第三条交互信息是成员给 TC 发送部分签名。若该数据包被重复发送, TC 会通过查表的方式检测到数据中所包含的令牌 T_{U_i} 重复, 要求重发; 多次重复后, TC 会发出警报, 有效杜绝了重放攻击。其中, 令牌组成包含了消息和随机数, 极大降低了重复的概率。

(2) 抗复制攻击证明

根据 3.2 节威胁模型 (2) 分析方案抵抗复制攻击的能力。对于敌手而言, 只有 ID 是已知的, 但在与 TC 进行通信时需要出示 TC 分配给每位注册成员的动态身份, 若是动态身份与关联表中的不一致, TC 会拒绝接收该成员的消息和签名。

动态身份的分配, 是用成员公钥对其进行椭圆曲线上的加密, 若敌手想要恢复, 在不知道私钥的情况下相当于求解椭圆曲线上的离散对数问题, 这在计算上是不可行的。假设敌手通过某种未知的方式, 试出了某位成员在某一时刻的动态身份, 但由于动态身份在每次成员发送完部分签名之后都会产生变化, 所以除非敌手可以及时分析出成员每次的动态身份, 否则无法假冒成员与 TC 进行通信。

(3) 抗陷害攻击证明

根据 3.2 节威胁模型 (3) 分析方案抵抗陷害攻击的能力。

情况①是常见的复制攻击。根据安全性分析 (2) 中可以得出, 由于敌手不知道 TC 分配给成员 U_x 的动态身份, 所以敌手的部分签名会被 TC 拒绝; 若是敌手想要恢复成员的动态身份, 相当于求解椭圆曲线上的离散对数问题, 这在计算上是不可行的。

情况②是 TC 冒充成员进行签名。在这种情况下, TC 自己选择一个 $x'_x \in Z_q^*$ 作为部分私钥, 计算 $X'_x = x'_x P$ 、 $d'_x = x'_x + f(\text{ID}_x)$ 和 $D'_x = d'_x P$, 生成部分签名 $\text{sig}'_x = d'_x I_x + M'_{U_x} T'_{U_x}$, 再合成群签名 $\text{Sig}' = \sum_{i=1, i \neq x}^t \text{sig}_i + \text{sig}'_x$, 同时计算验证信息 W' 、 Y' 、 Z' 。因为 X'_x 对应 x'_x , 所以该群签名可以通过群签名验证者的验证, 并且满足门限特性。

但是, 成员 U_x 可以向群签名验证者提出仲裁, 请求证明该签名不是其所签。验证者接受仲裁并要求成员 U_x 和他的冒充者 (TC) 提交他们的个人信息 $\left\{ \text{ID}_x, \frac{X_x}{X'_x} \right\}$ 。因为 $X_x = x_x \cdot P$, X_x 由 x_x 唯一确定, 所以若 TC 想要成功冒充成员 U_x 签名, 必须保证 $x'_x = x_x$, 而想要从 $X_x = x_x \cdot P$ 中恢复出 x_x , 相当于求解椭圆曲线上的离散对数问题, 这在计算上是不可行的。

(4) 抗联合攻击证明

根据 3.2 节威胁模型 (4) 分析方案抵抗联合攻击的能力。

情况①, 联合人数少于门限值 t 。敌手想要生成一个合法签名, 必须依托在某个注册成员之下,

假设随机选择一个注册成员 U_x ，设法生成一个合法的签名，若敌手不知道 U_x 的动态身份，那情况和抗复制攻击证明的复制攻击以及抗陷害攻击证明的第一种情况相同。当假设加强，敌手通过某种方法得到了成员 U_x 最新的动态身份，并且知晓了成员 U_x 的注册凭证 M_{U_x} （注册凭证由 TC 颁发并且唯一标识一个注册成员，但因为它在传播过程中没有进行加密并且不会改变，安全性低于动态身份，所以不单独进行分析讨论）。敌手选择一个 $x'_x \in Z_q^*$ 作为部分私钥，计算 $X'_x = x'_x P$ ，由于不知道秘密多项式 $f(x)$ ，所以重新选定一个多项式 $f'(x)$ ，同时计算 $d'_x = x'_x + f'(\text{ID}_x)$ 和 $D'_x = d'_x P$ ，生成部分签名 $\text{sig}'_x = d'_x I_x + M_{U_x} T'_x$ ，因为 D'_x 对应 d'_x 并且知晓认证凭证 M_{U_x} ，所以该部分签名能够通过 TC 的验证。接着 TC 合成群签名

$$\text{Sig}' = \sum_{i=1, i \neq x}^t \text{sig}_i + \text{sig}'_x, \quad \text{同时计算验证信息}$$

$$\text{Sig}' \cdot P = W' + g_p + Y' + Z' \text{ 成立, 即 } \sum_{i=1, i \neq x}^t f(\text{ID}_i) I_i P +$$

$$f'(\text{ID}_x) I_x P = \left(\sum_{i=1}^t f(\text{ID}_i) \prod_{j=1, j \neq i}^t \frac{-\text{ID}_j}{\text{ID}_i - \text{ID}_j} \right) P = f(0) P = g_p$$

成立，必须保证 $f'(\text{ID}_x) = f(\text{ID}_x)$ ，又因为联合人数少于门限值 t ，所以无法恢复多项式 $f(x)$ ；再假设联合人数达到 $t-1$ ，根据 $t-1$ 次多项式的组成结构 $f(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \dots + a_2x^2 + a_1x + a_0$ ，其中， $a_i \in [1, q-1] (i=0, 1, \dots, t-1)$ 均为整数。可得

$$f'(\text{ID}_x) = f(\text{ID}_x) \text{ 的概率是 } \frac{1}{(q-1)^t}, \text{ 所以, 只要 } q$$

足够大，敌手就只能以一个很小的概率攻击成功。

情况②，联合人数大于或等于门限值 t 。当假设加强，敌手通过某种方法得到了成员 U_x 最新的动态身份和注册凭证，并且因为联合人数达到门限值 t ，所以可以恢复出秘密多项式 $f(x)$ 。敌手选择 $x'_x \in Z_q^*$ 作为部分私钥，计算 $X'_x = x'_x P$ ，同时计算 $d'_x = x'_x + f(\text{ID}_x)$ 和 $D'_x = d'_x P$ ，生成部分签名 $\text{sig}'_x = d'_x I_x + M_{U_x} T'_x$ ，因为 D'_x 对应 d'_x 并且知晓认证凭证 M_{U_x} ，所以该部分签名能够通过 TC 的验证。接着 TC 合成群签名 $\text{Sig}' = \sum_{i=1, i \neq x}^t \text{sig}_i + \text{sig}'_x$ ，同

时计算验证信息 W' 、 Y' 、 Z' 。因为 $f(\text{ID}_x)$ 已知，并且 X'_x 对应 x'_x ，所以该群签名能够通过群签名验证者的验证，满足门限特性。但该签名无法通过签名验证者的仲裁，一旦有人提出异议，就需要成员提供个人信息，而 X_x 又由 x_x 唯一确定，若敌手希望伪造的签名无法被追踪，则需要保证 $x'_x = x_x$ ，这相当于求解椭圆曲线上的离散对数问题，在计算上是不可行的。

情况③，TC 与部分成员联合。这与情况②类似，不做赘述。

(5) 门限特性证明

门限群签名中的门限指只有当签名人数达到门限要求时，群签名才有效，对应该方案中的门限是 t ，即只有当有效的部分签名数量不少于 t 时，群签名才有效。

负责检验群签名是否有效的任务，是由群签名验证者承担的，而群签名验证者通过验证等式 $\text{Sig} \cdot P = W + g_p + Y + Z$ 成立来判断群签名是否有效，其中的关键在于能否通过群签名恢复出群私钥 $g_s = f(0) = a_0$ ，进而计算出群公钥 $g_p = f(0)P = a_0P$ 。由 5.1 节有效性分析 (3) 中可得，通过拉格朗日插值定理，当参数 ID_i 数量不少于 t 时，由式(2)可以计算出群公钥，即对于 t 个互不相同的插值节点 $x_i (1 \leq i \leq t)$ ，由 $t-1$ 次插值多项式的唯一性可以唯一确定一个多项式 $f(x)^{[1]}$ ，进而求出 $f(0)$ 。对应于具体的场景为：当参与签名的有效人数不少于 t 时，通过秘密多项式可以恢复群私钥，证明群签名有效；当签名人数少于 t 时，由于他们组成的群签名无法恢复出群私钥，故而会被验证者拒绝，以此来保证门限特性。

若有敌手想要通过其他方式来恢复私钥，则只有通过公钥 $g_p = f(0)P = a_0P$ 反解出 $f(0)$ ，这相当于求解椭圆曲线上的离散对数问题，在计算上是不可行的。

(6) 匿名性证明

匿名性是门限群签名需要具备的一个重要特性^[12]。匿名性指对于给定的部分签名，在签名被打开之前除了本人和 TC 之外没有人知道签名者是谁。

在本文方案中，注册阶段成员将自己的 ID 发

送给 TC 进行注册,注册成功 TC 返回给成员一个动态身份,在之后的交互中,成员的信息都是依附于 TC 所颁发的动态身份,真实的 ID 不会在信道中传输。敌手即使捕获了部分签名,也无法得知是哪位成员所签。若敌手想要从动态身份中恢复出成员的真实身份,则只能从计算式 $DID_{i1} = H_1(ID_{i1} || c_1)$ 中恢复, H_1 是单向的哈希函数,恢复出 ID_i 在计算上是不可行的。假设敌手以极小的概率恢复出了成员的身份,但动态身份在每次生成部分签名之后都会发生变化,即使敌手下次捕获了同一个成员的部分签名,敌手也无法分辨,因为那时动态身份已经发生了变化。

综上所述,本文方案具有抵抗重放攻击、复制攻击、陷害攻击和联合攻击的能力,并且具有匿名性和门限特性。

6 方案性能分析和比较

本文方案是基于 160 bit 密钥长度的椭圆曲线上的离散对数问题,在安全性上可以达到 1 024 bit RSA 的安全性^[13]。取部分签名 sig_i 长度 160 bit,加上注册成员在生成 sig_i 时由哈希函数产生 160 bit 消息令牌,即成员部分签名及其参数所占用的签名空间为 320 bit。

因为文献[1]的 MI 方案优于 HAA^[14]、XLS^[15]和 PY^[16]等,本文仅与 MI 方案实验结果比较分析。实验数据涉及成员注册、部分签名生成以及群签名合成中所采用的运算类型和数量,其中 T_{ECC_MUL} 表示椭圆曲线上乘法运算的执行时间, T_{ECC_ADD} 表示椭圆曲线上加法运算的执行时间, T_{MUL} 表示普通模乘运算的执行时间, T_H 表示哈希函数的执行时间,参照文献[1], $T_{ECC_MUL} \approx 29T_{MUL}$, $T_{ECC_ADD} \approx 0.12T_{MUL}$ 。

注册阶段,成员在计算 X_i 时进行了 1 次椭圆

曲线乘法,计算 β_{U_i} 时进行了 1 次哈希运算;接着 TC 在计算 A_{U_i} 时进行了 1 次椭圆曲线乘法,计算 M_{U_i} 时进行了 1 次哈希运算和 1 次模乘运算,计算 DID_{i1} 时进行了 1 次哈希运算;最后成员在进行验证时进行了 2 次椭圆曲线乘法、1 次哈希运算和 1 次椭圆曲线加法,计算 D_i 时进行了 1 次椭圆曲线乘法。忽略模加和模减,成员在注册阶段共进行了 4 次椭圆曲线乘法,2 次哈希运算和 1 次椭圆曲线加法,即 $4T_{ECC_MUL} + 2T_H + T_{ECC_ADD} = 116.12T_{MUL} + 2T_H$; TC 在注册阶段共进行了 1 次椭圆曲线乘法,2 次哈希运算和 1 次模乘,即 $T_{ECC_MUL} + 2T_H + T_{MUL} = 30T_{MUL} + 2T_H$ 。同样,部分签名 sig_i 生成和群签名合成阶段的计算复杂度示如表 2 所示(其中非成员部分所承担的计算统称为外部)。

从表 2 中可以看出,本文的成员部分和外部的计算复杂度总和分别为 $147.1T_{MUL}$ 和 $117T_{MUL}$,而 MI 的总和分别为 $177.2T_{MUL}$ 和 $117.2T_{MUL}$ (忽略哈希函数计算),即各部分的计算复杂度是小于 MI 方案的。深入对比成员注册阶段和部分签名生成阶段,本文的成员部分和外部的数值均小于 MI;另外,群签名合成阶段的主要计算任务由 TC 承担而非成员自身,当部分计算任务迁移至服务器使成员部分减负时(如图 2 所示,成员部分的计算量占比下降),并没有对移动终端设备的有限资源带来负荷,这正是本文方案中的一项优化。此外,本文方案减少了 2 次与可信中心的交互,签名占用空间缩小 30%。反之,MI 方案在执行过程中需要使用 1 次秘密信道,增加了实施成本。从安全方面考虑,经分析,MI 方案无法抵抗重放攻击,无注册成功后的认证凭证和动态身份,安全性低于本文方案。

表 2 与同类方案的计算复杂度比较
Table 2 Comparison of computational complexities with similar schemes

方案	密钥长度	签名空间	成员注册			部分签名生成			群签名合成		
			成员部分	外部	总和	成员部分	外部	总和	成员部分	外部	总和
本文方案	160	320	$116.1T_{MUL} + 2T_H$	$30T_{MUL} + 2T_H$	$146.1T_{MUL} + 4T_H$	$31T_{MUL} + T_H$	0	$31T_{MUL} + T_H$	0	$87T_{MUL} + T_H$	$87T_{MUL} + T_H$
MI	160	480	$145.2T_{MUL} + 2T_H$	$87.2T_{MUL} + 2T_H$	$232.4T_{MUL} + 4T_H$	$32T_{MUL} + T_H$	0	$32T_{MUL} + T_H$	0	$30T_{MUL}$	$30T_{MUL}$

有关加密操作的执行时间是采用 MIRACL 来计算,许多环境中的密码操作通常使用这个著名的密码库^[17]。文献[18]给出了相关加密操作在 I7-4700 处理器、4 GB 内存和 Win7 操作系统下的执行时间: $T_{ECC_MUL} \approx 0.442$ ms, $T_{ECC_ADD} \approx 0.0018$ ms, $T_H \approx 0.0001$ ms。

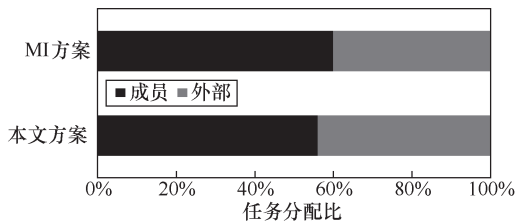


图2 不同方案的计算任务分配对比
Figure 2 The comparison of computing task assignment of different schemes

图3是表2数据的条形图表示,从中可以看出本文方案在除合成群签名阶段以外均快于MI方案,因此总时间花费减少了。群签名合成及后续阶段的计算均由TC负责,表明成员体验性得到提升,合成阶段的时间增长不会对成员的体验造成负面影响。由于成员生成部分签名阶段,本文方案的执行时间与MI方案相近,所以由文献[1]可以估算出本文方案该阶段在移动终端的执行时间约为0.034 s。无论是在PC端还是在移动端,本文方案的执行时间都是可以接受的。

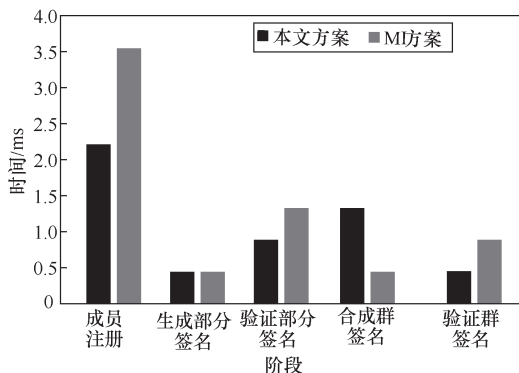


图3 不同方案在各阶段的执行时间对比
Figure 3 The comparison of the execution time of different schemes in each stage

不可否认,最耗时的是成员注册阶段,含有椭圆曲线上的1次点加运算、2次哈希运算和占时最大的4次椭圆曲线标量乘法^[19]。根据文献[20],构建有限域 F_p 上的椭圆曲线的计算复杂度为 $4O(N_{sc-ecc}^3)$, N_{sc-ecc} 为素数 p 的比特数,它在

5G 网络下是可接受的。

综上所述,本文方案具备门限群签名的基本特性,能够抵抗包括重放攻击在内的多种攻击,并且从性能分析中可以得出,本文方案在各种终端上的执行时间都是可以接受的,同时适用于5G网络。

7 结束语

为在新一代高速网络中使资源有限设备之间更安全、更高效、低延时地进行认证互通,本文针对门限群签名的各过程提出改进和轻量化:通过成员和TC的双向认证确保相关人员的有效参与;动态身份设计既为成员提供隐私保护又防范复制攻击;添加令牌有效地提高交互信息的新鲜性。下一步的研究方向为:①研究如何在保证安全性的前提下,进一步减少参与方之间的交互次数;②当出现成员撤销时,如何降低对原有成员的影响。

参考文献:

- [1] 陈立全,朱政,王慕阳,等.适用于移动互联网的门限群签名方案[J].计算机学报,2018,425(5):86-101.
CHEN L Q, ZHU Z, WANG M Y, et al. Threshold group signature scheme for mobile Internet application[J]. Chinese Journal of Computers, 2018, 425(5): 86-101.
- [2] JIA X, WANG D, NIE D, et al. A new threshold changeable secret sharing scheme based on the Chinese Remainder Theorem[J]. Information Sciences, 2019:13-30.
- [3] RUI G, SHI H, ZHAO Q, et al. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems[J]. IEEE Access, 2018, 6: 11676-11686.
- [4] SUN Y, ZHANG R, WANG X, et al. A decentralizing attribute-based signature for healthcare blockchain[C]//2018 27th International Conference on Computer Communication and Networks (ICCCN). 2018.
- [5] YU Y L, CHEN T S. An efficient threshold group signature scheme[J]. Applied Mathematics and Computation, 2005, 167(1): 362-371.
- [6] XIA X S, HONG F, GENG Y J, et al. Efficient dynamic threshold group signature scheme based on elliptic curve cryptosystem[J]. Journal of Modern Transportation, 2008, 16(1): 18-23.
- [7] HWANG J Y, KIM H J, LEE D H, et al. An enhanced (t,n) threshold directed signature scheme[J]. Information Sciences, 2014, 275: 284-292.
- [8] LI Y, CHENG S. Privacy preserved mobile sensing using region-based group signature[J]. IEEE Access, 2018: 61556-61568.
- [9] DAN B, GENNARO R, GOLDFEDER S, et al. Threshold cryptosystems from threshold fully homomorphic encryption

- tion[C]//Annual International Cryptology Conference. 2018: 565-596.
- [10] LI S, WANG W, ZHOU B, et al. A (M, m) authentication scheme against mobile sink replicated attack in unattended sensor networks[J]. IEEE Wireless Communication Letters, 2017.
- [11] 谭亦夫, 李子臣. 基于 Shamir 门限秘密分享的图像可视加密算法[J]. 网络与信息安全学报, 2018, 4(7): 73-80.
TAN Y F, LI Z C. Image visualization encryption algorithm based on Shamir threshold secret key sharing[J]. Journal of Network and Information Security, 2018, 4(7): 73-80.
- [12] 张兴兰, 崔遥. 基于群签名的属性加密方案[J]. 网络与信息安全学报, 2019, 5(1): 15-21.
ZHANG X L, CUI Y. Attribute-based encryption schema with group signatures[J]. Journal of Network and Information Security, 2019, 5(1): 15-21.
- [13] ISERN D, ANDREU P, HUGUET L, et al. On the practicability of using group signatures on mobile devices: implementation and performance analysis on the android platform[J]. International Journal of Information Security, 2015, 14(4): 335-345.
- [14] DAHSHAN H, KAMAL A, ROHIEM A. A threshold blind digital signature scheme using elliptic curve dlog-based cryptosystem[C]//2015 IEEE 81st Vehicular Technology Conference. 2015.
- [15] 谢东, 李佳佳, 沈忠华. 一种新的基于椭圆曲线的门限群签名方案[J]. 杭州师范大学学报(自然科学版), 2013, 12(1): 57-60.
XIE D, LI J J, SHEN Z H. A new threshold signature scheme based on elliptic curve crypt system[J]. Journal of Hangzhou Normal University (Natural Science Edition), 2013, 12(1): 57-60.
- [16] 彭娅. 门限数字签名理论及应用研究[D]. 广州: 中山大学, 2010.
PENG Y. Research on Theory and Application of Threshold Digital Signature[D]. Guangzhou: Sun Yat-sen University, 2010.
- [17] Shamus Software Ltd. MIRACL Library[EB].
- [18] HE D, ZEADALLY S, XU B, et al. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad-hoc networks[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(12): 2681-2691.
- [19] HE, D, ZEADALLY S, XU B, et al. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular Ad Hoc networks[J]. IEEE Trans Information Forensics Security, 2015, 10 (12): 2681-2691.
- [20] YING B, NAYAK A. Lightweight remote user authentication pro-

ocol for multi-server 5G networks using self-certified public key cryptography[J]. Journal of Network and Computer Applications, 2019, 131: 66-74.

[作者简介]



竺智荣 (1993-), 男, 浙江宁波人, 福建师范大学硕士生, 主要研究方向为大数据安全与隐私保护。



吕佳玉 (1995-), 女, 辽宁盖州人, 福建师范大学硕士生, 主要研究方向为大数据安全与隐私保护。



叶幅华 (1976-), 女, 福建霞浦人, 福建师范大学副教授, 主要研究方向为大数据安全隐私保护、信息安全。



姚志强 (1967-), 男, 福建莆田人, 博士, 福建师范大学教授、博士生导师, 主要研究方向为大数据安全隐私保护、多媒体安全、应用安全。