基于群签名的慈善捐赠身份隐私安全保护方案

刘飚，王治中，袁喜琴，封化民
（北京电子科技学院信息安全重点实验室，北京 100070）

摘　要：为了解决慈善捐赠中数字用户隐私泄露及平衡匿名性与可追责性的问题，提出了一种基于群签名的慈善捐赠身份隐私安全保护方案。具体而言，提出了可追踪群签名方案，根据捐赠场景下的用户需求设计了轻量化的认证协议，并提出了动态哈希图谱存储结构优化物资管理以及电子捐赠证书发放的解决方法。结合随机预言机模型，证明所提方案具有有效抵御选择消息攻击（EUF -CMA）的安全性，并解决了现有方案中存在的用户匿名、信息隐私等多项安全问题。理论分析和测试表明，该方案的用户请求和捐赠机构效率分别达到现有最新慈善捐赠方案的12倍和1.5倍，在计算效率与时间开销上具有显著优势。

关键词：慈善捐赠；身份认证；隐私保护；群签名；哈希图谱
中图分类号：TP309.7
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025125

Identity privacy and security protection scheme for charitable donations based on group signatures

LIU Biao, WANG Zhizhong, YUAN Xiqin, FENG Huamin
Key Laboratory of Information Security, Beijing Electronics Science and Technology Institute, Beijing 100070, China

Abstract: To address digital privacy leakage and balance anonymity with accountability in charitable donations, the identity privacy and security protection scheme for charitable donations based on group signatures was proposed. Specifically, a traceable group signature framework was proposed, a lightweight authentication protocol tailored to donor requirements in charitable scenarios was designed, and a dynamic Hash graph storage architecture was introduced to optimize supply chain management alongside a digital certificate distribution mechanism. Security analysis conducted under the random oracle model demonstrated that existential unforgeability against chosen message attacks (EUF-CMA) was achieved, resolving multiple security vulnerabilities in existing systems including user anonymity flaws and information privacy leakage. Theoretical analysis and experimental evaluation revealed that the proposed scheme improved efficiency by up to 12 times for user requests and 1.5 times for donor institutions. This approach significantly reduces computational and time overhead compared to current charitable donation mechanisms.

Keywords: charitable donation, authentication, privacy protection, group signature, Hash graph

0　引言

慈善捐赠具有产生深远社会影响的潜力，是公平分配社会资源的重要渠道。慈善捐赠不仅是第三次分配的核心载体，更是实现共同富裕目标的关键路径。“十四五”规划和2035年远景目标纲要明确要求，要完善慈善激励机制，推动慈善捐赠与乡村

收稿日期：2025–04–30；修回日期：2025–06–30
通信作者：刘飚，liubiao@besti.edu.cn
基金项目：国家重点研发计划基金资助项目（No.2024YFB3108103）；中央高校基本科研业务费专项资金资助项目（No.3282024012）
Foundation Items: The National Key Research and Development Program of China (No.2024YFB3108103), The Fundamental Research Funds for the Central Universities（No.3282024012）

振兴、教育医疗等民生领域深度融合，构建现代化慈善服务体系。通过定向捐赠、慈善信托、志愿服务等多元形式，慈善事业可以有效帮扶困难群体，优化资源配置，增进社会凝聚力，是公平分配社会资源的重要渠道[1]。

然而，近年来出现了一系列现实的问题。首要问题集中于信息透明度与问责机制的缺失，部分慈善组织存在潜在的数据操纵风险，导致捐赠流程中的诚信危机。此外，物资流动和使用的不透明性使追踪从捐赠到预期受益人的轨迹的能力变得复杂，造成捐赠者和受益者之间脱节。鉴于这些问题，如何增强现有的协议，以提高慈善事业的透明度和问责制，从而增强公众对慈善组织的信心成为慈善捐赠领域的热门话题[2-3]。

为了解决上述问题，人们提出了许多基于区块链的解决方案[4-6]。文献[4]基于以太坊网络设计了一个去中心化物资运输平台，文献[5]中利用可信执行环境解决物资运输问题，文献[6]中基于联盟区块链设计了一种可追踪物资分发系统。此类方案解决了包括慈善组织和捐赠物资分配的不透明性等问题。然而，目前这些基于区块链的解决方案，虽然可以有效解决慈善捐赠中物资分配不透明等问题，但同时也面临着隐私和安全挑战[7-10]，例如，文献[7]存在捐赠信息泄露的风险，文献[8]存在捐赠者和受赠者身份暴露的风险，文献[9]存在身份验证安全问题，文献[10]缺少方案安全性分析。

针对隐私保护问题，现有研究主要采用加密算法构建隐私保护机制[11-13]。文献[11]提出基于零知识证明的匿名凭证系统，文献[12-13]则开发了动态令牌生成方案。虽然这些加密方法在部分情况下提供了解决措施，但仍然存在尚未解决的问题：1) 如何在确保参与者身份可验证性的前提下防范伪造捐赠等欺诈行为；2) 如何构建条件隐私保护机制以平衡用户隐私权与恶意行为追责需求；3) 现有方案多数都聚焦于企业等团体捐赠场景，缺乏对普通家庭闲置物品处置需求的适应性设计。事实上，当下普通家庭中可能存在大量物资处理的捐赠需求，高效处理和利用闲置物品，不仅可以有效实现资源的合理配置，更响应资源循环利用的可持续发展时代趋势。

在隐私保护技术方面，群签名机制展现出独特优势。自 Chaum 等[14]提出群签名理论以来，该技术已被广泛应用于条件隐私保护认证系统[15-19]。例如，在车辆网络通信研究中，文献[17]提出了一种结合群签名的认证方案，该方案使用了群签名技术和基于身份的密码学，减少了系统中车辆信息的存储开销和证书管理负担，但该方案没有提供撤销机制，无法撤销恶意非法车辆。

为了解决上述问题，本文结合基于国密算法 SM9 的群签名算法[20]提出了一种基于群签名的慈善捐赠身份隐私安全保护方案来保护用户隐私安全，解决慈善捐赠场景下匿名性与可追责性的平衡难题。具体而言，本文通过设计适用于家庭级捐赠场景的轻量化认证协议，包含 6 个核心模块：系统初始化、捐赠认证、证书发放、受捐认证、物资存储和匹配、身份公开，满足普通捐赠用户需求，并提出了动态哈希图谱存储结构以解决捐赠物资管理问题。本文阐述了慈善捐赠场景下的安全目标并证明了方案的安全性。理论分析表明，本文方案相比最新的捐赠认证方案具有较低的时间开销和更高的安全性，为完善现代慈善服务体系提供了重要技术支持。

1 预备知识

1.1 双线性群

设 λ 为安全参数，p 为与 λ 相关的大素数，G_1、G_2、G_T 均为素数 p 阶的乘法循环群，P_1、P_2 分别为群 G_1 和群 G_2 的生成元，存在双线性映射，e: $G_1 \times G_2 \rightarrow G_T$ 满足以下条件。

1)双线性。对于任意元素 $P_1 \in G_1, P_2 \in G_2$，a，$b \in Z_p$，都有 $e(P_1^a, P_2^b) = e(P_1, P_2)^{ab}$。

2)非退化性。至少存在元素 $P_1 \in G_1, P_2 \in G_2$，满足 $e(P_1, P_2) \neq 1$。

3)可计算性。对于任意的 $P_1 \in G_1$，$P_2 \in G_2$，存在有效算法计算 $e(P_1, P_2)$。

1.2 群签名

群签名方案通常包含以下几个过程。

初始化（Setup）：生成系统安全参数，创建群公钥（公开用于验证签名）和群私钥（由群管理保管，用于必要时追踪签名者身份）。

成员加入（Join）：新成员通过交互协议加入群组，生成唯一的成员私钥和成员证书，确保每个成员的私钥独立且不可伪造。

签名（Sign）：群成员使用自己的私钥和待签名消息生成群签名，该签名隐藏签名者身份，仅证明其属于合法群组。

验证（Verify）：任何人可验证签名的有效性，确认消息确实由群内成员签署，但无法追踪到具体签名者。

打开（Open）：在争议或违规情况下，群管理可使用私钥“打开”签名，揭示签名者的真实身份，实现监管与隐私的平衡。

1.3　双线性碰撞攻击假设（k-BCAA 1）[21]

对于整数 k 和随机选取的 $x \in Z_q^*$，$P_2 \in G_2^*$，$P_1 = \psi(P_2)$，$\hat{e}: G_1 \times G_2 \to G_T$，且 $h_i \in Z_q^*$，给定 $\left(P_1, P_2, xP_2, h_0, \left(h_1, \frac{1}{h_1 + x} P_2\right), \cdots, \left(h_k, \frac{1}{h_k + x} P_2\right)\right)$，其中 $0 \leqslant i \leqslant k$，计算 $\hat{e}(P_1, P_2)^{\frac{1}{x + h_0}}$ 是困难的。

1.4　基于国密 SM9 的群签名方案

文献[20]提出了基于身份的多密钥生成中心（KGC）高效无证书群签名方案，对现有 SM9 算法进行适当优化，实现了对交易过程和用户身份的隐私保护，具有良好的效率与安全性，可应用于大量需要验证用户身份的场合，如房屋租赁、实物交易等。以下是该群签名方案具体流程。

创建：群管理员（GM, group manager）的身份为 $\mathrm{ID_{GM}}$，需要向所有 KGC 申请建立群，KGC 在核实 GM 身份后，将 $\mathrm{ID_{GM}}$ 记录，以便之后 KGC 对新加入的成员生成并发放群私钥。申请群成功后，该群的公钥为 $\mathrm{ID_{GM}}$，私钥则由签名算法生成并交由 GM 保存。

入群：当节点 A 想加入群时，则由 GM 或 KGC 核实 A 的身份 $\mathrm{ID_A}$，核对通过后，将 $\mathrm{ID_A}$ 通过改进的 SM9 算法进行签名后，利用安全信道发送至 KGC。KGC 对 GM 的签名进行验证后提取出 $\mathrm{ID_A}$，商定 $\mathrm{ks} \in [1, N-1]$ 以及每个 KGC 各自持有 $\mathrm{ke}_j \in [1, N-1]$。首先，计算 $d_1 = [H_1(\mathrm{ID_{GM}} \| \mathrm{hid}, N) + \mathrm{ks}]^{-1} \bmod N$，$d_2 = [H_1(\mathrm{ID_A} \| \mathrm{hid}, N) + \mathrm{ks}]^{-1} \bmod N$，得出 $\mathrm{ds}'_{\mathrm{A}} = [d_2] P_1$。然后，每个 KGC 计算 $\mathrm{ds}_{\mathrm{A}j} = [\mathrm{ke}_j] \mathrm{ds}'_{\mathrm{A}}$，A 将每个 KGC 的 $\mathrm{ds}_{\mathrm{A}j}$ 相加，即可得到签名私钥 $\mathrm{ds_A} = [d_2] \left[\sum_{j=1}^{k} \mathrm{ke}_j\right] P_1$。最后，A 将结果重新发送给所有 KGC，KGC 重新计算 $\mathrm{ds}'_{\mathrm{AG}} = [d_2] \left[\sum_{i=1}^{k} \mathrm{ke}_j\right] \cdot \mathrm{ke}_j \cdot [d_1] \cdot P_1$ 并发送给 A，由 A 计算 $\mathrm{ds_{AG}} = \sum_{j=1}^{k} \mathrm{ds}'_{\mathrm{AG}} = [d_2] \left[\sum_{j=1}^{k} \mathrm{ke}_j\right] \left[\sum_{j=1}^{k} \mathrm{ke}_j\right] [d_1] P_1$，可得到 A 的群私钥 $\mathrm{ds_{AG}}$。至此，节点 A 入群成功，其群密钥对为 $(\mathrm{ds_A}, \mathrm{ds_{AG}}, \mathrm{ID_A}, \mathrm{ID_{GM}})$，其中，$\mathrm{ds_A}$、$\mathrm{ds_{AG}}$ 为私钥，由 A 保存，$\mathrm{ID_{GM}}$ 为群签名的唯一标识。

群签名：若群中节点 A 要对消息 M 进行群签名，则其需要首先计算 $g = e(P_1, P_{\mathrm{pub-e}})$，并选取随机数 $r_1 \in [1, N-1]$ 与 $r_2 \in [1, N-1]$，计算 $w = g^{r_1}$，之后计算 $h = H_2(M \| w, N)$，$S_1 = (r_2^{-1}) \cdot (r_1 - h) \cdot \mathrm{ds_A}$ 与 $S_2 = (r_2^{-1}) \cdot (r_1 - h) \cdot \mathrm{ds_{AG}}$，最后计算 $h_1 = H_1(\mathrm{ID_A} \| \mathrm{hid}, N)$，$P_{3'} = [h_1] P_2 + P_{\mathrm{pub-s}}$，$P_3 = [r_2] P_{3'}$。得出节点 A 对消息 M 的群签名 (h, P_3, S_1, S_2)。

验证：对于接收到的消息 M' 与其群签名 (h', P'_3, S'_1, S'_2)，群中节点 B 若想验证其是否属于群 $\mathrm{ID_{GM}}$，则需要先计算 $h_1 = H_1(\mathrm{ID_{GM}} \| \mathrm{hid}, N)$，接着计算 $P = [h_1] P_2 + P_{\mathrm{pub-s}}$，之后计算 $u_1 = e(S_2, P)$ 与 $u_2 = e(S_1, P_{\mathrm{pub-e}})$，若 $u_1 \neq u_2$，则验证不通过；否则，继续计算 $u = e(S_1, P_3)$，$g = e(P_1, P_{\mathrm{pub-e}})$ 与 $t = g^{h'}$，最后计算 $w' = u \cdot t$，得到 $h = H_2(M \| w', N)$。对比 h' 与 h，一致则验证通过，至此可证明该消息由群 $\mathrm{ID_{GM}}$ 中某个成员所签名。

打开：当需要核实信息签名来源时，KGC 可根据所持有的用户信息 $\mathrm{ID_A}$ 找到该用户所属密钥，并查看是否已被撤销或更新，以确定交易产生的时间以及交易的合法性。

系统维护与成员撤销：当 GM 需要撤销群成员节点时，在将要撤销的成员信息中记录“已作废”标记；当系统参数需要更新时，KGC 可重新生成系统参数，并且更新用户信息，分发给群成员新的密钥对。同时保留曾经使用的系统参数。

本文针对慈善捐赠的具体场景在文献[20]的基础上简化了方案复杂的协商流程，加入部分批量认证提高计算效率，重新设计了方案的公开与成员撤销操作，并为改进后群签名方案的不可伪造性和隐私保护提供了正确性和安全性证明。

2　系统模型

2.1　系统模型

系统模型主要由可信机构（TA, trust author-

ity)、捐赠机构、捐赠者、受捐者 4 个实体组成。

可信机构：一个功能强大的实体。其职责是初始化整个系统、注册捐赠者和受捐者、生成公共参数和分发密钥。同时，TA 在需要公开捐赠者身份或者发生争议时，可以追踪目标用户的身份。

捐赠机构：接收捐赠者的捐赠请求以及受理受捐者的受捐请求，负责捐赠物资的存储，并将所有物资的物流运输外包给物流公司，每个捐赠机构作为一个 GM。

捐赠者：有意向捐赠物资的用户。在进行捐赠时根据需求选择是否匿名捐赠，例如有捐赠抵扣纳税需求可以选择公开捐赠获得捐赠证书，以及是否追溯捐赠结果。本文将捐赠者和受捐者统称为“用户”。

受捐者：可以是个人也可以是集体。注册时需受捐者首先按照相关要求获得受捐资格的证明文件（如贫困证明、灾情报告等），成功注册后获得群成员身份，在有限时间内可以通过验证发送受捐请求来获得相应物资。

系统模型如图 1 所示，其中捐赠者、受捐者、捐赠机构与可信机构间通过安全信道进行注册，捐赠和受捐流程通过外部不安全信道进行，捐赠机构通过内部信道对物资进行存储匹配，并通过物流运输分配物资。

2.2　威胁模型

可信机构是完全可信的，不会被任何对手破坏，且可信机构与捐赠机构间存在安全通信通道。假设捐赠机构、捐赠者和受捐者是诚实但充满好奇的，这意味着他们会严格遵循预先设计的方案，但也可能试图从可用信息中窥探他人的隐私。

捐赠机构可能对用户身份或捐赠信息感兴趣，还可能兜售用户隐私信息牟利。但因为捐赠机构需要对用户和捐赠物资核查以及负责物资的运输，所以本文方案允许其获得用户的部分信息（如联系方式），同时，大部分用户不会经常更换联系方式和寄件地址，因此捐赠机构很容易通过 2 条不同的请求链接到同一用户。本文不考虑可能存在的物理攻击，例如快递公司在取件派件时对用户拍照等侵犯身份隐私的行为。

捐赠者提交捐赠请求但实际不进行捐赠或者存在捐赠物资与实际不符，同时与捐赠机构勾结来伪造捐赠结果。

受捐者试图获取其他受捐者的身份，短时间内重复发送捐赠请求来获取超出自身实际需求的物资。

外部攻击者可以窃听通信信道以捕获传输的消息并侵犯隐私。此外，外部对手可能试图冒充受捐者，诱骗捐赠物资。

2.3　设计目标

用户认证：在发送捐赠或受捐请求之前，应该对用户进行身份认证，使得对手无法冒充合法用户。

用户匿名与不可链接：用户的合法身份受到

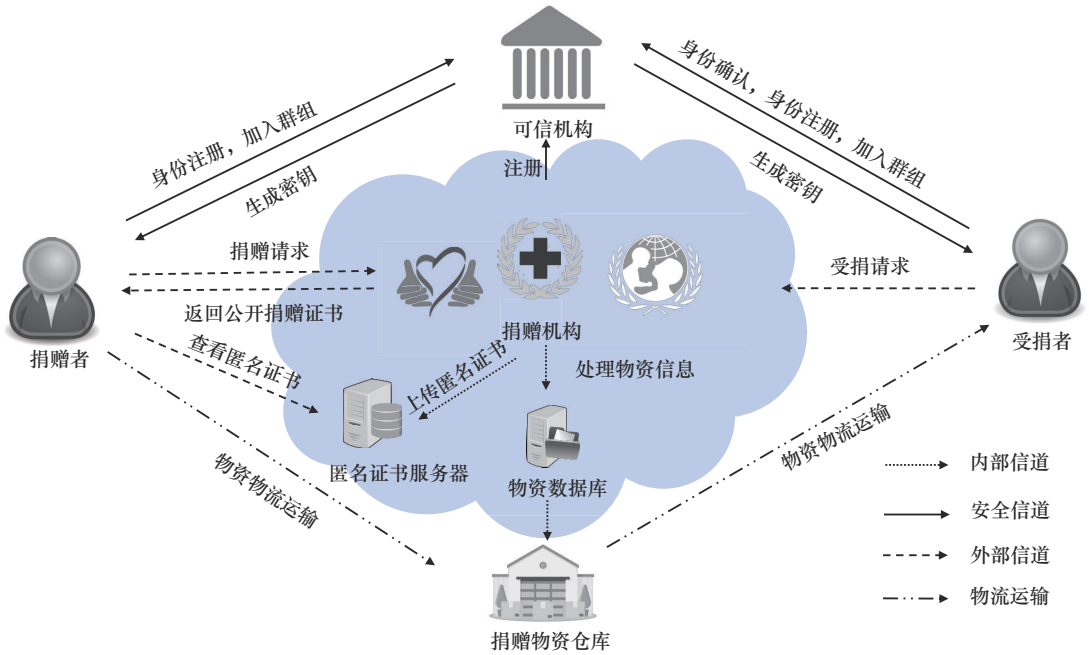

图 1　系统模型

保护，不受服务器、其他用户和外部对手的影响。同时，给定来自一个用户的2个捐赠/受捐请求，除捐赠机构外没有人可以将它们链接到同一个用户。

不可伪造：用户的签名不可被伪造，为捐赠者发放的捐赠证书也同样不可伪造。

抗联合勾结：防止捐赠者与捐赠机构联合勾结，来伪造捐赠记录牟利。

数据机密性和完整性：保护所有请求报告的内容不受服务器、其他用户和外部对手攻击，并且内容不被非法修改。

可追溯性：TA可以在发生纠纷时追踪行为不当用户的真实的身份，并撤销群组中用户身份。

快速结果检索：存储捐赠物资后，捐赠机构应该有效地为受捐者分配物资。

2.4　安全模型

基于上述提及的安全风险与密码学理论中的随机预言模型，本文方案应满足有效抵御选择消息攻击（EUF-CMA）安全性[22]。

定义1　EUF-CMA。该安全性由挑战者$\mathcal{C}$与攻击者$\mathcal{A}$之间的游戏定义，并且由随机预言机模拟恶意节点控制的设备，包括哈希随机预言机和群签名随机预言机，游戏过程分为以下3个阶段。

1)初始化

挑战者$\mathcal{C}$使用系统初始化生成系统参数params和主私钥s，将params发送给攻击者$\mathcal{A}$。

2)询问

①哈希询问。$\mathcal{A}$询问哈希结果，$\mathcal{C}$可以通过查询哈希随机预言机得到相关内容的哈希值H_1、H_2、H_3。

②签名询问。$\mathcal{A}$询问消息M与对应用户身份ID_i，$\mathcal{C}$可以通过查询签名随机预言机从而生成用户ID_i对消息M的群签名结果σ并返回。

3)伪造

在$\mathcal{A}$从未询问过任意用户的签名私钥，也从未询问过对消息的M^*签名的前提下，$\mathcal{A}$可以成功伪造合法用户基于身份的$\mathrm{ID_A}$对消息M^*的合法群签名σ^*。如果$\mathcal{A}$伪造的签名σ^*能通过验证，则$\mathcal{A}$赢得游戏。定义$\mathcal{A}$赢得该游戏的优势为$\mathrm{Adv}_{\mathcal{A}}=\Pr[\mathrm{Verify}(M^*,\mathrm{ID_A},\sigma^*)=\mathrm{valid}]$。如果对于任意攻击敌手$\mathcal{A}$，在多项式时间内该优势是可以忽略的，则称该群签名方案是EUF-CMA安全的。

3　方案设计

本文慈善捐赠隐私保护方案包含6个核心模块：系统初始化、捐赠认证、证书发放、受捐认证、物资存储和匹配、身份公开，其中的系统参数如表1所示。

表1　**系统参数**

参数	含义
$\mathrm{id_A}$	用户A伪身份
W_{A}	用户A捐赠/所需的物资种类编号
q_{A}	用户A捐赠/所需的物资数量
L_{A}、L_{p}	取件场地、物资存储仓库编号
t_1、t_2、tt_1	捐赠时间、捐赠取件时间、受捐取件时间
b_1、b_2	公开捐赠选择、追溯捐赠结果选择
C_{A1}、C_{A2}	传输密文
Pw	受捐者可披露个人信息
Cert	捐赠证书
Array()	数组序列
Res	物资存储结果
Enc()	公钥加密算法
Dec()	公钥解密算法

3.1　系统初始化

首先，TA确定方案的安全参数k，选取群的阶数为$N>2^k$，$G_1\times G_2\to G_T$为双线性映射，选择G_1和G_2的生成元为$P_1\in G_1,P_2\in G_2$，满足ψ:$G_2\to G_1$然后设定$s\in[1,N-1]$作为主私钥，计算主公钥$P_{\mathrm{pub}}=sP_2$，并选择散列函数$H_1()$、$H_2()$、$H_3()$。最后，核查所有提交申请的捐赠机构信息，随机选择$x_{\mathrm{group}}\in[1,N-1]$作为群私钥，计算群公钥$P_{\mathrm{group}}=x_{\mathrm{group}}P_2$，为通过的捐赠机构生成群唯一身份$\mathrm{ID_{GM}}$，将$(\mathrm{ID_{GM}},x_{\mathrm{group}})$发送给对应群管理员。TA记录所有群信息。并广播群签名参数。公共参数params为

$$\{G_1,G_2,G_T,e,N,P_1,P_2,P_{\mathrm{pub}},P_{\mathrm{group}},H_1(),H_2(),H_3(),\mathrm{ID_{GM}}\}\tag{1}$$

其次，入群。当新的捐赠者U_{A}想要加入标识为$\mathrm{ID_{GM}}$的群时，TA首先确认U_{A}的标识$\mathrm{ID_A}$是否合法，然后随机选择$t_{\mathrm{A}}\in[1,N-1]$，$T_{\mathrm{A}}=t_{\mathrm{A}}P_1$，计算

$$d_1=[H_1(\mathrm{ID_{GM}})+s]^{-1}\bmod N\tag{2}$$

$$d_2=[H_1(\mathrm{ID_A})+s]^{-1}\bmod N\tag{3}$$

$$x_{\mathrm{A}}=[t_{\mathrm{A}}\cdot d_2]P_1 \tag{4}$$

$$r_{\mathrm{A}}=[d_1\cdot t_{\mathrm{A}}\cdot d_2]P_1 \tag{5}$$

$$k_{\mathrm{A}}=[d_2\cdot s]P_1 \tag{6}$$

其中，x_{A}为成员U_{A}的个人私钥，r_{A}为群私钥。至此，U_{A}成功加入群组。TA将$(\mathrm{ID_A},\mathrm{ID_{GM}},x_{\mathrm{A}},r_{\mathrm{A}},t_{\mathrm{A}},k_{\mathrm{A}})$发给$U_{\mathrm{A}}$。TA存储$U_{\mathrm{A}}$成员证书$(\mathrm{ID_A},\mathrm{ID_{GM}},T_{\mathrm{A}},k_{\mathrm{A}})$。

TA对于受捐者U_{B}额外生成t_{d}，代表其受捐身份有效截止时间。同理，TA将$(\mathrm{ID_B},\mathrm{ID_{GM}},x_{\mathrm{B}},r_{\mathrm{B}},t_{\mathrm{B}},t_{\mathrm{d}},k_{\mathrm{B}})$发送给$U_{\mathrm{B}}$，TA存储成员证书信息$(\mathrm{ID_B},\mathrm{ID_{GM}},t_{\mathrm{B}},t_{\mathrm{d}},k_{\mathrm{B}})$。

最后，TA为所有捐赠机构生成信息用于证书发放中机构进行签名。随机选择$t_{\mathrm{K}}\in[1,N-1]$，$T_{\mathrm{K}}=t_{\mathrm{K}}P_1$，计算

$$d_1=[H_1(\mathrm{ID_{TA}})+s]^{-1}\bmod N \tag{7}$$

$$d_2=[H_1(\mathrm{ID_{GM}})+s]^{-1}\bmod N \tag{8}$$

然后计算$x_{\mathrm{K}}=[t_{\mathrm{K}}\cdot d_2]P_1$和$r_{\mathrm{K}}=[d_1\cdot t_{\mathrm{K}}\cdot d_2]P_1$。捐赠机构$\mathrm{ID_{GM}}$的签名密钥为$(x_{\mathrm{K}},r_{\mathrm{K}})$，TA存储$\mathrm{ID_{GM}}$成员证书信息$(\mathrm{ID_{GM}},T_{\mathrm{K}},k_{\mathrm{K}})$。

3.2 捐赠认证

当新入群的捐赠者或捐赠者U_{A}想再次进行捐赠时，向捐赠机构GM发送捐赠请求。捐赠者利用智能手机生成基本捐赠信息，具体包括个人伪身份$\mathrm{id_A}=H_3(\mathrm{ID_A})$，捐赠物资类型$W_{\mathrm{A}}$，捐赠数量$q_{\mathrm{A}}$，期望取件场地$L_{\mathrm{A}}$，捐赠时间$t_1$，取件时间$t_2$，是否公开捐赠$b_1$，是为1，否为0，以及是否需要追溯物资捐赠情况$b_2$，是为1，否为0。

随机选取$r_0\in[1,N-1]$，加密消息M_{A}:$(\mathrm{id_A},W_{\mathrm{A}},q_{\mathrm{A}},L_{\mathrm{A}},b_1,b_2)$，$m=(\mathrm{id_A}\|W_{\mathrm{A}}\|q_{\mathrm{A}}\|L_{\mathrm{A}}\|b_1\|b_2)$。预计算$e\left(P_1,P_2\right)$与$e\left(P_1,P_{\mathrm{group}}\right)$

$$C_{\mathrm{A1}}=r_0P_1 \tag{9}$$

$$C_{\mathrm{A2}}=e\left(r_0P_1,P_{\mathrm{group}}\right)\cdot m=e\left(P_1,P_{\mathrm{group}}\right)^{r_0}\cdot m \tag{10}$$

U_{A}随机选择$r_1,r_2\in[1,N-1]$，计算

$$w=e(P_1,P_2)^{r_1} \tag{11}$$

$$h=H_2(w,\mathrm{id_A},W_{\mathrm{A}},q_{\mathrm{A}},L_{\mathrm{A}},b_1,b_2) \tag{12}$$

$$S_1=(r_2^{-1})\cdot(t_{\mathrm{A}}^{-1})\cdot(r_1-h)\cdot x_{\mathrm{A}} \tag{13}$$

$$S_2=(r_2^{-1})\cdot(t_{\mathrm{A}}^{-1})\cdot(r_1-h)\cdot r_{\mathrm{A}} \tag{14}$$

$$P_3=r_2(H_1(\mathrm{ID_A})P_2+P_{\mathrm{pub}}) \tag{15}$$

$$P_4=t_{\mathrm{A}}P_1-(r_2^{-1})\cdot(r_1-h)\cdot k_{\mathrm{A}} \tag{16}$$

输出消息M_{A}的群签名$\sigma=(h,P_3,P_4,S_1,S_2)$。最终输出捐赠请求$\mathrm{Que_A}=(\mathrm{ID_{GM}},C_{\mathrm{A1}},C_{\mathrm{A2}},t_1,t_2,h,P_3,P_4,S_1,S_2)$。

捐赠机构接收到用户的捐赠请求$\mathrm{Que_A}=(\mathrm{ID_{GM}},C'_{\mathrm{A1}},C'_{\mathrm{A2}},t_1,t_2,h',P'_3,P'_4,S'_1,S'_2)$后。首先解密$C'_{\mathrm{A1}},C'_{\mathrm{A2}}$

$$s_k=e\left(C'_{\mathrm{A1}},x_{\mathrm{group}}P_2\right) \tag{17}$$

$$(\mathrm{id_A}\|W_{\mathrm{A}}\|q_{\mathrm{A}}\|L_{\mathrm{A}}\|b_1\|b_2)=C'_{\mathrm{A2}}\cdot s_k^{-1} \tag{18}$$

验证：当捐赠机构接收多个验证请求，对于同属一个$\mathrm{ID_{GM}}$的请求可以批量验证，计算

$$P=H_1(\mathrm{ID_{GM}})P_2+P_{\mathrm{pub}} \tag{19}$$

$$U_1=e\left(\sum_{i=1}^{n}S'_{2,i},P\right) \tag{20}$$

$$U_2=e\left(\sum_{i=1}^{n}S'_{1,i},P_2\right) \tag{21}$$

如果$U_1=U_2$，批量认证通过；否则，对每个签名单独计算

$$u_1=e(S'_2,P) \tag{22}$$

$$u_2=e(S'_1,P_2) \tag{23}$$

首先验证$u_1=u_2$，然后计算

$$u=e(S'_1,P'_3) \tag{24}$$

$$w'=u\cdot e(P_1,P_2)^{h'} \tag{25}$$

$$h_3=H_2(w',\mathrm{id_A},W_{\mathrm{A}},q_{\mathrm{A}},L_{\mathrm{A}},b_1,b_2) \tag{26}$$

如果$h_3=h'$，证明群签名是由捐赠机构GM中的合法用户生成的。

验证通过后，由捐赠机构指派物流公司到指定地点L_{A}接收捐赠物资，并暂时保留捐赠请求$\mathrm{Que_A}$，用于后续证书发放，在该物资确认完毕后，为本次捐赠生成唯一捐赠序列号K，将捐赠请求与序列号保存到捐赠机构数据库中。

3.3 证书发放

捐赠机构在确认物资情况正确后，根据获得签名中的b_1信息，为捐赠者提供匿名捐赠证明或者公开捐赠证书。

1)匿名捐赠证明

当$b_1=0$，代表捐赠者选择不公开个人身份信息的匿名捐赠，捐赠机构$\mathrm{ID_{GM}}$对捐赠请求用自身公钥P_{group}进行加密。

$$\mathrm{Enc}_{P_{\mathrm{group}}}(\sigma,w,\mathrm{id_A},W_{\mathrm{A}},q_{\mathrm{A}},L_{\mathrm{A}},b_1,b_2,t_1) \tag{27}$$

在一段时间内（如一天），将加密结果、对应捐赠时间t_1、唯一捐赠序列号K按捐赠时间顺序上传到公共捐赠服务器之中保存，供所有人查阅。

捐赠者可以在当天结束后，同样用式(27)加密自身捐赠信息以及捐赠请求Que_A，在对应捐赠机构的匿名捐赠服务器中结合捐赠时间t_1进行对应，如果对应成功，表明自己匿名捐赠成功。此外，捐赠者可自行保存捐赠序列号K以用于日后获取自己当时的捐赠记录。

2)公开捐赠证书发放

首先，捐赠机构GM将捐赠请求Que_A发送给TA，TA对捐赠请求使用用户揭露从而获得用户成员证书信息$(\mathrm{ID}_\mathrm{A},\mathrm{ID}_\mathrm{GM},T_\mathrm{A},k_\mathrm{A})$。

TA使用当前时间戳Time为捐赠者生成捐赠证书$\mathrm{Cert}=(\mathrm{ID}_\mathrm{A},M_\mathrm{G},\sigma,t_1,\mathrm{Time},h_\mathrm{cert})$，$M_\mathrm{G}$为捐赠物资信息，$h_\mathrm{cert}=H_3(\mathrm{ID}_\mathrm{A},M_\mathrm{G},\sigma,t_1,\mathrm{Time})$，TA将证书保存在证书数据库中，并将证书$(\mathrm{Cert},T_\mathrm{A})$通过安全通道发送给捐赠机构。

捐赠机构随机选择$r_1,r_2\in[1,N-1]$，$w=e(P_1,P_2)^{r_1}$，$h=H_2(w,\mathrm{Cert})$，计算$S_1=(r_2^{-1})\cdot(t_\mathrm{A}^{-1})\cdot(r_1-h)\cdot x_\mathrm{A}$，$S_2=(r_2^{-1})\cdot(t_\mathrm{A}^{-1})\cdot(r_1-h)\cdot r_\mathrm{A}$，$P_3=r_2(H_1(\mathrm{ID}_\mathrm{A})P_2+P_\mathrm{pub})$，输出消息$M_\mathrm{G}$的群签名：$\sigma=(h,P_3,S_1,S_2)$。捐赠机构用$T_\mathrm{A}$加密$\mathrm{Enc}_{T_\mathrm{A}}(\mathrm{Cert},\sigma,h_\mathrm{Cert})$发送给捐赠者。

捐赠者首先用自身t_A解密$\mathrm{Dec}_{t_\mathrm{A}}(\mathrm{Cert},\sigma,h_\mathrm{Cert})$，计算$P=H_1(\mathrm{ID}_\mathrm{GM})P_2+P_\mathrm{pub}$，$u_1=e(S_2',P)$，$u_2=e(S_1',P_2)$，验证$u_1=u_2$。计算$u=e(S_1',P_3')$，$t=e(P_1,P_2)^{h'}$。最后，设$w'=u\cdot t$，$h_3=H_2(w',\mathrm{Cert})$，如果$h_3=h'$证明签名是由TA生成的，则接受捐赠证书。

3.4　受捐认证

如果有受捐者或者受捐群体U_B想要获得捐赠，则通过匿名认证向服务器发送受捐请求。受捐者利用相应智能设备生成基本供应信息，包括伪身份id_B，$\mathrm{id}_\mathrm{B}=H_3(\mathrm{ID}_\mathrm{B})$想要获得捐赠物资类型$W_\mathrm{B}$、数量收件$q_\mathrm{B}$、场地$L_\mathrm{B}$、取件时间tt，另外由于部分捐赠者有追溯物资捐赠情况的需求，因此还需要受捐者选择性披露个人信息Pw（如职业、所在省份），用于向捐赠者反馈捐赠情况。

类似于3.2节，随机选取$r_0\in[1,N-1]$，加密消息M_B:$(\mathrm{id}_\mathrm{B},W_\mathrm{B},q_\mathrm{B},L_\mathrm{B},\mathrm{Pw})$，$C_{\mathrm{B}1}=r_0P_1$，$C_{\mathrm{B}2}=e\left(P_1,P_\mathrm{group}\right)^{r_0}\cdot(\mathrm{id}_\mathrm{B}\|W_\mathrm{B}\|q_\mathrm{B}\|L_\mathrm{B}\|\mathrm{Pw})$，$U_\mathrm{B}$随机选择$r_1,r_2\in[1,N-1]$，$w=e(P_1,P_2)^{r_1}$，$h=H_2(w,\mathrm{id}_\mathrm{B},W_\mathrm{B},q_\mathrm{B},L_\mathrm{B},\mathrm{tt})$，计算$S_1=(r_2^{-1})\cdot(t_\mathrm{B}^{-1})\cdot(r_1-h)\cdot x_\mathrm{B}$，$S_1=(r_2^{-1})\cdot(t_\mathrm{B}^{-1})(r_1-h)\cdot r_\mathrm{B}$。$P_3=r_2(H_1(\mathrm{ID}_\mathrm{B})P_2+P_\mathrm{pub})$，$P_4=t_\mathrm{B}P_1-(r_2^{-1})\cdot(r_1-h)\cdot k_\mathrm{B}$，输出消息$M_\mathrm{B}$的群签名$\sigma=(h,P_3,P_4,S_1,S_2)$。最终输出捐赠请求$\mathrm{Que}_\mathrm{B}=(\mathrm{ID}_\mathrm{GM},C_{\mathrm{B}1},C_{\mathrm{B}2},\mathrm{tt},h,P_3,P_4,S_1,S_2)$。

在受捐者管理机制中，捐赠机构采用双表结构进行动态管控：捐赠记录表$(\mathrm{id}_\mathrm{B},K_1,t_1,K_2,t_2,K_n,t_n,h)$，用于记录物资序列号集合$\{K_i\}$、对应捐赠时间戳$\{t_i\}$及验证哈希值$h=H_3(K_1,t_1,K_2,t_2,K_n,t_n)$；过期受捐者表$(\mathrm{id}_\mathrm{B},T)$，用于管理受捐者休眠周期参数$T$，其中$T>0$表示暂停捐赠的冷却时间，$T=-1$标记身份失效需重新注册的不可逆状态。

TA维护证书数据库，将受捐者证书参数$(\mathrm{ID}_\mathrm{B},\mathrm{ID}_\mathrm{GM},t_\mathrm{B},t_\mathrm{d},k_\mathrm{B})$按失效时间$t_\mathrm{d}$进行优先级排序。当$t_\mathrm{d}$触发过期条件时，TA向全网捐赠机构广播$\mathrm{id}_\mathrm{B}=H_3(\mathrm{ID}_\mathrm{B})$的失效通知，捐赠机构据此执行记录迁移操作：将目标实体从捐赠记录表移除，并归档至过期受捐者表。

对于捐赠请求$\mathrm{Que}_\mathrm{A}=(\mathrm{ID}_\mathrm{GM},C_{\mathrm{B}1},C_{\mathrm{B}2},\mathrm{tt},h,P_3,P_4,S_1,S_2)$，首先进行状态核查：若请求者存在于过期受捐者表且$T>0$，立即拒绝请求并维持冷却状态，若$T=-1$，则返回身份失效通知，要求重新注册。通过初筛后，系统执行捐赠频次评估：若近期捐赠累计次数（如最近周期内≥3次）超过预设阈值，则拒绝当前请求，同时将该受捐者移入过期受捐者表并设置合理休眠参数T。

接着解密$C_{\mathrm{B}1}',C_{\mathrm{B}2}'$，$s_k=e\left(C_{\mathrm{B}1}',x_\mathrm{group}P_2\right)$，$(\mathrm{id}_\mathrm{B}\|W_\mathrm{B}\|q_\mathrm{B}\|L_\mathrm{B}\|\mathrm{Pw})=C_{\mathrm{B}1}'\cdot s_k^{-1}$。

验证过程同捐赠请求验证过程相同。

捐赠机构为用户进行物资匹配，在物资成功匹配后，将对应受捐者捐赠记录表中添加对应捐赠物资序列号K_i，受捐时间t_i，并更新h。

3.5　物资存储和匹配

如图2所示，物资管理架构包含以下关键组件。

分类哈希映射：将全部物资划分为M个主类别（如医疗用品、书籍、电子产品），并为每个物资实例分配唯一分类编码W。通过哈希函数$H_3(W)$生成整型哈希值h，并取模运算$h \bmod M$将其映射至

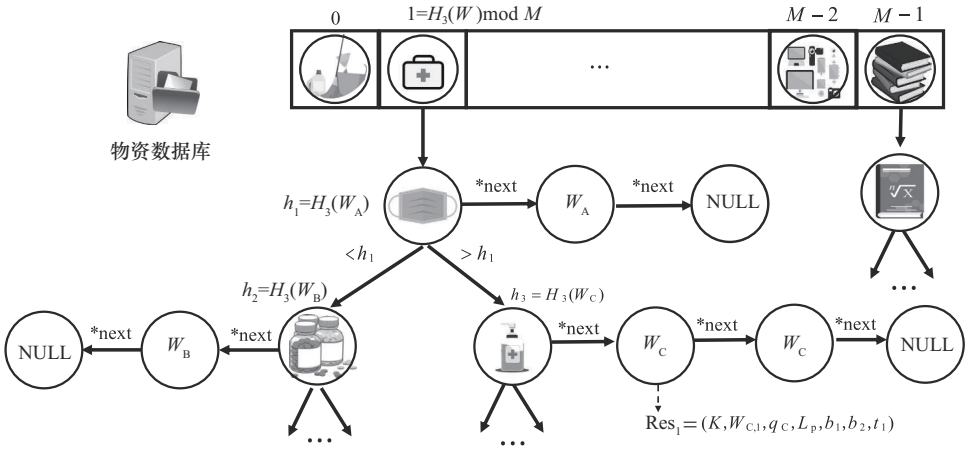

图2 物资管理架构

对应主类存储节点。

复合树状存储结构：哈希表由M个二叉查找树（BST）根节点构成数组。每个BST节点存储主类元数据，其子节点管理子类信息，遵循左子节点值小于父节点、右子节点值大于父节点的排序原则。具体物资信息以兄弟节点链表形式存储于叶节点。

1)物资存储算法流程：当新增物资W_A入库时，首先计算$h=H_3(W_A)$并定位根节点，$T=\text{Array}[h \bmod M]$，然后在BST中递归查找$h$。若存在目标节点，将物资元组$(K,W_A,q_A,L_p,b_1,b_2,t_1)$插入兄弟节点链表；若不存在，创建新叶节点并初始化链表。

2)物资检索算法流程：收到物资请求W_B时，同样计算$h=H_3(W_B)$，定位根节点T，若T为空树，返回空集；否则执行BST搜索，遍历匹配节点的兄弟链表，生成候选集$\text{Res}=(K,W_A,q_A,L_p,b_1,b_2,t_1)$。最后按$L_p$与请求者的地理距离升序排列，返回前5个记录。

3)物资匹配策略包含2种特殊处理：当物资数量不足即$q_A<q_B$时，系统自动累加后续记录直至满足$\sum q_A \geqslant q_B$。当数量超额即$q_A>q_B$时，更新库存数据为$q'_A=q_A-q_B$，并将受捐者部分身份信息Pw_i追加至元组，形成新纪录。

此外，系统还需检测Res中b_2，若$b_2=1$，代表该物资捐赠者希望追溯物资捐赠情况，此时捐赠机构通过捐赠序列号K与自身保存的捐赠信息获取捐赠者的捐赠请求Que_A，并将受捐者选择性披露的个人信息Pw发送给捐赠者进行通知。

3.6 身份公开

当捐赠机构发现捐赠者声称的物品与实际不符、捐赠者企图虚假捐赠或获取其他用户信息，或者受捐者存在不正当行为时，就会发生纠纷。因此，TA应该能够跟踪目标用户。

具体来说，根据群签名，TA可以利用用户U_A的签名$\sigma=(h,P_3,P_4,S_1,S_2)$追踪用户的真实身份。计算

$$S_3=s\cdot S_1 \tag{28}$$

$$T_A=P_4+S_3 \tag{29}$$

根据存储的成员信息$(\text{ID}_A,\text{ID}_{GM},T_A)$，可以找到签名对应的$\text{ID}_A$。将匹配的$(\text{ID}_A,\text{ID}_{GM},T_A)$插入TA的黑名单中，并将$H_3(\text{ID}_A)$广播给所有捐赠机构。如果该非法用户再次提交请求，所有机构都可以通过用户伪身份id_A与黑名单中$H_3(\text{ID}_A)$对应，从而识别撤销用户U_A。

4 安全性分析

4.1 正确性证明

分别将u_1中的S_2、P和u_2中的S_1按定义展开

$$u_1=e(S_2,P)=e((r_2^{-1})\cdot(r_1-h)\cdot u\cdot d\cdot P_1,$$
$$[h_2]P_2+[s]P_2)=e(P_1,P_2)^{(r_2^{-1})\cdot(r_1-h)\cdot d}$$

$$u_2=e(S_1,P_2)=e\left((r_2^{-1})(r_1-h)\cdot d\cdot P_1,P_2\right)=$$
$$e(P_1,P_2)^{(r_2^{-1})(r_1-h)\cdot d}=u_1$$

由此可得$u_2=u_1$。同理，将u中S'_1与P'_3按定义展开，可得

$$u=e(P_1,P_2)^{\left(r_2^{-1}\right)(r_1-h)\cdot d\cdot r_2\cdot\left[H_1(\text{ID}_A)+s\right]}=$$

$$e(P_1,P_2)^{(r_1-h)}$$

$$w'=u\cdot t=e(P_1,P_2)^{(r_1-h)}\cdot e(P_1,P_2)^{H_2(M\|w)}=e(P_1,P_2)^{r_1}$$

由 $w=e(P_1,P_2)^{r_1}$ 可得 $w'=w$，与方案中认证一致。批量认证时，将 i 条消息中的 $S'_{2,i}$ 和 $S'_{1,i}$ 展开并加和

$$U_1=e\left(\sum_{i=1}^{n}S'_{2,i},P\right)=e\left(\sum_{i=1}^{n}\left(\left(r_{2,i}^{-1}\right)\cdot\left(r_{1,i}-h\right)\cdot u\cdot d_i\cdot P_1\right),P\right)=e(P_1,P_2)^{\sum_{i=1}^{n}\left((r_2^{-1})\cdot(r_{1,i}-h)\cdot d_i\right)}$$

$$U_2=e\left(\sum_{i=1}^{n}S'_{1,i},P_2\right)=e(P_1,P_2)^{\sum_{i=1}^{n}\left((r_2^{-1})\cdot(r_{1,i}-h)\cdot d_i\right)}=U_1$$

因此，本文群签名是正确的。

4.2　不可伪造性

定理 1　由于 k-BCAA 1 困难问题在群 G_1、G_2、G_T 上是存在的，则捐赠者或受捐者的群签名满足存在不可伪造性，能够有效抵御选择消息攻击。

证明　假设存在攻击者 $\mathcal{A}$ 使用多项式时间概率攻击算法，能以不可忽略的优势 ε 成功伪造的签名内容。还存在挑战者 $\mathcal{C}$ 通过与 $\mathcal{A}$ 交互后，可以成功解决 k-BCAA 1 困难问题，解决该问题的优势为 $\varepsilon_1\geqslant\dfrac{\varepsilon}{q_{H_1}}$，其中 q_{H_1} 为 H_1 查询次数。

1) 初始化。$\mathcal{C}$ 生成系统参数 $\{G_1,G_2,G_T,e,N,P_1,P_2,P_{\text{pub}},P_{\text{group}},H_1(),H_2(),H_3(),\text{ID}_{\text{GM}}\}$。随机选择 $i'\in[1,q]$，对于 $i\neq i'$，$\mathcal{C}$ 生成私钥 $\left(h_i,\dfrac{1}{h_i+x}P_2\right)$。

2)哈希询问。$\mathcal{C}$ 为每个随机预言机维护一个列表，将它们分别用于记录对 $\mathcal{A}$ 提供的答案。L_1、L_2、L_3 分别记录 3 个预言机 H_1、H_2、H_3 的哈希询问，L_s 记录签名询问。

①H_1 查询。假设攻击者 $\mathcal{A}$ 提供的身份是 ID_i，如果查询的 ID_i 已经在 L_1 中，则 $\mathcal{C}$ 返回值 h_i；否则 (ID_i,h_i) 记录为新的第 i 个查询，特别当 $i=i'$ 时，令 $H_1(\text{ID}_{i'})=h_{i'}$ 并发送到 $\mathcal{A}$。

②H_2 查询。$\mathcal{C}$ 收到 $\mathcal{A}$ 的 (M_i,w_i) 询问时，如果列表 L_2 中不包括 (M_i,w_i)，则设置 $H_2(M_i,w_i)=d_i$ 并更新列表 L_2，将结果发送给 $\mathcal{A}$，否则直接将 (M_i,w_i) 送给 $\mathcal{A}$。

③H_3 查询。$\mathcal{C}$ 收到 $\mathcal{A}$ 的 (ID_i) 询问时，如果列表 L_3 中不包括 $(\text{ID}_i,\text{id}_i)$，则设置 $H_3(\text{ID}_i)=\text{id}_i$ 并更新列表 L_3，将结果发送给 $\mathcal{A}$，否则直接把 id_i 发送给 $\mathcal{A}$。

3)签名查询。将 (M_i,ID_i) 设置为第 i 个消息标识对，其中对于捐赠者 $M_i=(\text{id}_\text{A},P_\text{A},W_\text{A},q_\text{A},L_\text{A},b_1,b_2)$，对于受捐者 $M_i=(\text{id}_\text{B},P_\text{B},W_\text{B},q_\text{B},L_\text{B},\text{Pw})$，如果 $i\neq i'$，返回正常签名；如果 $i=i'$，$\mathcal{C}$ 随机选择 $S_1,S_2\in G_1$，$k\in Z_N^*$，$t_\text{A},r_1,r_2\in[1,N-1]$，计算 $P_3=r_2\left(h_i'P_2+P_{\text{pub}}\right)$，$P_4=t_\text{A}P_1-(r_2^{-1})\cdot k_\text{A}\cdot(r_1-k)$，$w=e(S_1,P_3)e(P_1,P_2)^h$，$H_2(M,w)=h$，将结果 (S_1,h) 发送给 $\mathcal{A}$。

4)伪造签名。$\mathcal{A}$ 可以成功伪造关于 (M_i,ID_i) 的签名元素 (M_i,h,S_1)，因此根据分叉引理[23]，最终可以输出 2 种签名元素 (M_i,h,S_1) 和 (M_i,h^*,S_1^*)。基于此，2 种签名元素可以计算为

$$e(S_1,P_3)\cdot e(P_1,P_2)^h=e(P_1,P_2)^{r_1}\tag{30}$$

$$e(S_1^*,P_3)\cdot e(P_1,P_2)^{h^*}=e(P_1,P_2)^{r_1}\tag{31}$$

$$\frac{e(S_1,P_3)}{e(S_1^*,P_3)}=e(P_1,P_2)^{h^*-h}\tag{32}$$

$$\frac{S_1-S_1^*}{h^*-h}=\frac{1}{r_2(x+h_{i'})}P_1\tag{33}$$

$$e\left(\frac{S_1-S_1^*}{h^*-h},r_2P_2\right)=e(P_1,P_2)^{\frac{1}{x+h_{i'}}}\tag{34}$$

因此，k-BCAA 1 困难问题得以解决，$\mathcal{A}$ 的优势为 $\varepsilon>\dfrac{q(q_s+1)(q_s+q_{h_1})}{2^k}$，其中 q_s、q_{h_1}、q 分别代表签名询问次数，H_1 询问次数和自然数。证毕。

4.3　用户匿名

用户发送请求时使用群签名方案来证明自身的身份，首先，存在椭圆曲线上求解离散对数难题，使服务器无法知道用户的真实的身份。其次，用户使用随机数 r_0、r_1、r_2 来对信息以及签名结果随机化，使同一个用户每次生成的签名与信息结果并无显性联系，并将伪身份 $\text{id}_\text{A}=H_3(\text{ID}_\text{A})$ 作为重要信息加密传输，由于数据的机密性，id_A 也不可能被对手获得。存在椭圆曲线上求解离散对数难题，对手仅凭请求中 ID_{GM} 或时间的显性信息很难判断 2 个不同的签名是否来自同一个用户。因此，身份隐私得到了保障。

此外，即使捐赠机构通过用户信息链接到同一用户，用户的匿名性仍然可以得到保证，即捐赠机构只拥有用户的伪身份 id_A 而无法获得用户真实身份 ID_A，因此确保不可信的捐赠机构尽可能拥有较少的用户信息。

最后，当用户选择公开捐赠时，因需发放实名制证书（可用于纳税抵扣），代表用户放弃部分匿名，捐赠机构最后在服务器中公开捐赠结果时使用用户伪身份 id_A，所有人都可以将捐赠结果链接到同一用户的伪身份 id_A。

4.4 数据机密性与完整性

对于捐赠/受捐请求，由于包含大量用户隐私信息，本文采用基于有限域的离散对数公钥密码（Elgamal）加密方案[24]对其进行加密。即在捐赠请求中发送的 $(\mathrm{id}_A\|P_A\|W_A\|q_A\|L_A\|b_1\|b_2)$ 和 $(\mathrm{id}_B\|P_B\|W_B\|q_B\|L_B\|\mathrm{Pw})$ 由临时公钥 r_0 和捐赠机构的私钥 x_{group} 保护。由于 Elgamal 加密方案已被证明是安全的，因此本文方案捐赠请求与受捐请求具有良好的机密性，避免遭受其他用户和外部对手的攻击。捐赠和用户之间的消息使用群签名方案进行认证，从而保证了消息的完整性。

4.5 可追溯性和高效撤销性

发生纠纷时，TA 可以追踪发出捐赠请求的捐赠者或得到捐赠的受捐者的真实的身份。使用接收到的签名 $\sigma=(h,P_3,P_4,S_1,S_2)$，TA 可以计算 $S_3=s\cdot S_1$，$T_A=P_4+S_3$，根据 TA 存储的成员信息 $(\mathrm{ID}_A,\mathrm{ID}_{GM},T_A)$，获得用户的真实身份。通过将匹配的 $(\mathrm{ID}_A,\mathrm{ID}_{GM},T_A)$ 插入 TA 黑名单实现高效撤销用户，将 $H_3(\mathrm{ID}_A)$ 发送给所有捐赠机构。如果该非法用户再次提交请求，所有机构都可以通过用户伪身份 id_A 与黑名单中 $H_3(\mathrm{ID}_A)$ 对应，从而识别撤销用户。

4.6 抗联合勾结攻击

本文方案的捐赠机构负责用户认证，管理捐赠物资以及分发捐赠证书。由于捐赠机构拥有以上特殊权限，他们可能联合捐赠者以谋取私利，例如捐赠者联合捐赠机构伪造捐赠结果。为了防止这种情况，本文方案采取审计日志来监管捐赠机构行为。具体来说，TA 会定期审计捐赠机构服务器中的捐赠结果、物资存储服务器中物资存储情况、实际存储仓库物资情况，确保三者数据信息统一，若发现捐赠机构存在异常行为，视情节严重予以警告甚至撤销其合法身份。

4.7 安全性对比

本文方案与文献[5,25-28]的安全性对比如表 2 所示。文献[5,25-26]是目前慈善捐赠领域具有代表性的物资捐赠方案，文献[27-28]是基于群签名技术的隐私保护方案。

表 2 方案安全性对比

方案	身份认证	隐私保护	数据安全	用户匿名	不可伪造	可追踪性
文献[5]	√	×	√	×	×	×
文献[25]	×	√	×	×	×	×
文献[26]	√	√	√	√	×	×
文献[27]	√	√	√	√	√	×
文献[28]	√	√	√	√	×	√
本文方案	√	√	√	√	√	√

注：√表示方案具备某种功能，×表示方案不具备某种功能。

文献[5]提出了一种安全的可验证性捐赠系统 Astraea，保护捐赠隐私。但该方案缺乏用户匿名性，无法保证捐赠时捐赠者和受赠者的身份隐私。文献[25]提出基于区块链的慈善计划，将资金分配和计划数据视为区块链中的账本条目，以减少虚假筹款活动，从而保护众多用户的安全和隐私。然而，其系统内部缺乏身份认证机制，对用户访问捐赠数据的限制太弱，任何用户都可以访问关键数据，不利于信息安全保护。文献[26]通过简短群签名（BBS+）和零知识证明实现了用户匿名与信息的隐私保护，使匿名用户能够捐赠和接收物品，但该方案未被证明具有不可伪造性，无法防止用户消息被伪造。本文方案基于群签名技术和 Elgamal 加密实现了匿名捐赠和接收功能，使匿名用户能够捐赠和接收物品，并具有不可伪造性。

文献[27]是基于群签名的边缘计算数据的隐私保护方案，该方案在边缘设备与终端设备间建立了长期可信任联系以及从减轻计算开销的角度舍弃了群签名的可追踪性，但这不代表该方案不需要追责功能。从系统安全架构的完整性角度分析，追责机制作为隐私保护系统的重要安全属性以及群签名方案的独特优势，在实际场景中不可或缺。文献[28]提出了区块链下的动态设备管理的隐私保

护方案，虽然证明了该方案可实现数据安全和隐私保护以及匿名性等功能，但未证明其具有不可伪造性。

由表2可以看出，本文方案满足身份认证、隐私保护、数据安全、用户匿名、不可伪造和可追踪性，而其余对比方案只能满足上述功能中的部分特性。

5　实验分析

5.1　性能分析

表3给出了各种密码的运算名称及操作执行的平均时间。实验是在内存为16 GB、处理器为Intel® Core™ i7-8700 CPU @ 3.20 GHz的个人计算机上实现的。具体而言，实验在Ubuntu 24.04.2 LTS操作系统和MSVC编译器的环境下，在Visual Stdio 2022中编译调用函数库实现，该函数库是使用C++语言编写的miracl函数库。本文实验选定的椭圆曲线为 $y^2 = x^3 + 7 \bmod p$，素数域 p 大小取160 bit，并通过使用SHA-256哈希函数来确保数据的完整性。

表3　　相关操作执行时间

运算名称	缩写	平均执行时间/ms
椭圆曲线上的乘法	T_{ECM}	0.315 6
双线性运算	T_B	4.741 2
标量乘法	T_{SM}	0.761 1
通用散列函数	T_h	0.000 9
模乘	T_{MM}	0.012 1
模幂	T_{ME}	0.503 2

分析本文方案3个实体（捐赠者、捐赠机构和受捐者）的计算开销，并与文献[26]的实验结果进行比较，因为文献[26]的方案与文本方案类似，是慈善捐赠领域少数基于用户隐私保护的方案。在本文方案中，捐赠者请求由于预计算的存在，共需要执行模乘6次，模幂1次，椭圆曲线上的乘法3次，通用散列函数2次，即共需要 $6T_{MM} + T_{ME} + 3T_{ECM} + 2T_h \approx 1.524\,4$ ms；捐赠机构需要验证请求的签名解密信息，由于预计算的存在，共需要执行模乘1次，模幂2次，椭圆曲线上的乘法1次，通用散列函数2次，双线性运算4次，此外，在证书发放阶段，按照公开证书发放步骤，共需要执行模乘4次，模幂1次，椭圆曲线上的乘法2次，通用散列函数2次，即共需要 $5T_{MM} + 3T_{ME} + 3T_{ECM} + 4T_h + 4T_B \approx 21.485\,3$ ms；在受捐者请求物资时，共需要执行模乘6次，模幂1次，椭圆曲线上的乘法3次，通用散列函数2次，即共需要 $6T_{MM} + T_{ME} + 3T_{ECM} + 2T_h \approx 1.524\,4$ ms。文献[26]中捐赠者中认证需执行椭圆曲线上的乘法3次，通用散列函数1次，此外，零知识证明还需执行椭圆曲线上的乘法10次，通用散列函数1次，双线性运算3次，共需要 $13T_{ECM} + 2T_h + 3T_B \approx 18.328\,2$ ms；捐赠机构认证需执行椭圆曲线上的乘法12次，通用散列函数2次，需进行2次零知识证明验证，每次都需要椭圆曲线上的乘法3次，双线性运算3次，共需 $18T_{ECM} + 2T_h + 6T_B \approx 34.129\,8$ ms；受捐者类似捐赠者，需执行椭圆曲线上的乘法2次，通用散列函数1次，此外，零知识证明还需执行椭圆曲线上的乘法10次，通用散列函数1次，双线性运算3次，共需 $12T_{ECM} + 2T_h + 3T_B \approx 18.012\,6$ ms。此外，即使对于本文方案公开捐赠的捐赠者需要验证证书的签名，还需要额外执行椭圆曲线上乘法1次，模幂1次，双线性运算3次，$T_{ME} + T_{ECM} + 3T_B \approx 15.042\,4$ ms，本文方案捐赠者共需约16.566 8 ms，依然相较于文献[26]有优势。由表4可知，本文方案中捐赠者和受捐者的请求效率约为文献[26]的12.02倍，捐赠机构约为文献[26]的1.59倍。

表4　　慈善捐赠方案开销对比

方案	捐赠者/ms	捐赠机构/ms	受捐者/ms
文献[26]	18.328 2	34.129 8	18.012 6
本文方案	1.524 4	21.485 3	1.524 4

5.2　物资存储

本文基于Python编程语言生成了大量模拟捐赠数据，并按物资管理架构构建了数据结构。设置完成后，可以模拟捐赠机构响应物资查询的速度。本节分别在总物资数量为1 000、2 000、3 000、4 000、5 000的5种设置下各进行了100次物资匹配实验。如图3所示，总匹配时间小于2 ms。本文在哈希图谱中使用了二叉树，因此平均匹配时间和修改时间都是 $O(\mathrm{lbNum})$。本文在哈希节点之后的链表中插入新的物资节点，使平均插入时间为

O(lbNum)。其中一些具有较高时间的离群值意味着对应的存储节点位于树中极端位置。

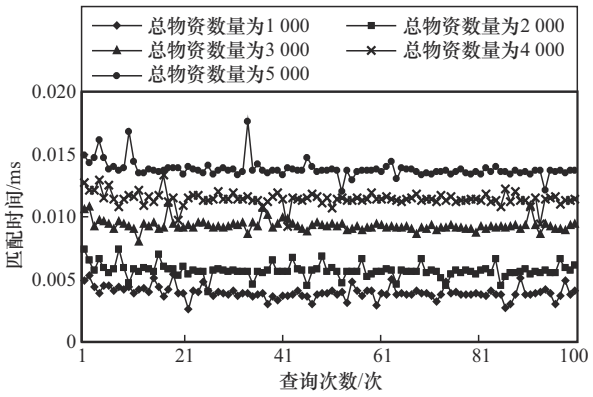

图3 物资匹配时间

6 结束语

本文针对慈善捐赠领域目前存在的隐私泄露、问责机制缺失等问题，提出了一种基于群签名的慈善捐赠身份隐私安全保护方案。通过融合基于身份的群签名技术与动态哈希图谱存储结构，构建了条件隐私保护框架，在确保用户匿名性的同时支持高效身份追溯，适配家庭级捐赠场景。在安全性证明中证明了本文方案能有效实现用户的隐私保护。最后通过实验评估，本文方案在同类方案中具有显著的效率提升。本文为慈善捐赠系统的用户隐私提供了关键技术支撑，同时本文方案具有高安全性与轻量级的优点，可以有效与现有区块链技术相结合，将所有关键操作在链上留痕且不可篡改，达到更高的监管与治理效果。未来将进一步探索对于捐赠物资和参与各方的审计与核查，增强慈善捐赠的公信力以应对复杂捐赠生态中的动态信任挑战，推动慈善事业在数字时代的可持续发展。

参考文献：

[1] 王丽辉. 我国慈善事业功能塑造与创新[J]. 合作经济与科技, 2025(5): 166-169.
WANG L H. The function shaping and innovation of charity in China[J]. Co-Operative Economy & Science, 2025(5): 166-169.

[2] 张吉鹏, 李禹燊, 陈希多. 慈善组织声誉与信息披露对捐赠意愿和风险态度的正向影响[J]. 经济学(季刊), 2025, 25(1): 206-223.
ZHANG J P, LI Y S, CHEN X D. The positive effects of charity reputation and information disclosure on the willingness to give and risk attitudes of donors in China[J]. China Economic Quarterly, 2025, 25(1): 206-223.

[3] PRASHAR A, GUPTA P. How to build trust in Gen Y in online donation crowdfunding: an experimental study[J]. Behaviour & Information Technology, 2024, 43(4): 677-694.

[4] KAUR M, KAUR P D, SOOD S K. Blockchain oriented effective charity process during pandemics and emergencies[J]. IEEE Transactions on Computational Social Systems, 2024, 11(1): 431-441.

[5] LI M, CHEN Y F, ZHU L H, et al. Astraea: anonymous and secure auditing based on private smart contracts for donation systems[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(4): 3002-3018.

[6] HAWASHIN D, JAYARAMAN R, SALAH K, et al. Blockchain-based management for organ donation and transplantation[J]. IEEE Access, 2022, 10: 59013-59025.

[7] BREUER M, MEYER U, WETZEL S, et al. A privacy-preserving protocol for the kidney exchange problem[C]//Proceedings of the 19th Workshop on Privacy in the Electronic Society. New York: ACM Press, 2020: 151-162.

[8] VANHOLDER R, DOMÍNGUEZ-GIL B, BUSIC M, et al. Organ donation and transplantation: a multi-stakeholder call to action[J]. Nature Reviews Nephrology, 2021, 17(8): 554-568.

[9] SINGH A, RAJAK R, MISTRY H, et al. Aid, charity and donation tracking system using blockchain[C]//Proceedings of the 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI) (48184). Piscataway: IEEE Press, 2020: 457-462.

[10] SHAHEEN E, HAMED M A, ZAGHLOUL W, et al. A track donation system using blockchain[C]//Proceedings of the 2021 International Conference on Electronic Engineering (ICEEM). Piscataway: IEEE Press, 2021: 1-7.

[11] WANG B Y, LUEKS W, SUKAITIS J, et al. Not yet another digital ID: privacy-preserving humanitarian aid distribution[C]//Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2023: 645-663.

[12] SONNINO A, AL-BASSAM M, BANO S, et al. Coconut: threshold issuance selective disclosure credentials with applications to distributed ledgers[J]. arXiv Preprint, arXiv: 1802.07344, 2018.

[13] LI M, SHEN Y Z, YE G X, et al. Anonymous, secure, traceable, and efficient decentralized digital forensics[J]. IEEE Transactions on Knowledge and Data Engineering, 2023, 36(5): 1874-1888.

[14] CHAUM D, HEYST E V. Group signatures[C]//Advances in Cryptology - EUROCRYPT'91, Workshop on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 1991: 257-265.

[15] CAO Y B, XU S Y, CHEN X, et al. A forward-secure and efficient authentication protocol through lattice-based group signature in VANETs scenarios[J]. Computer Networks, 2022, 214: 109149.

[16] SONI M, SINGH D K. Blockchain-based group authentication scheme for 6G communication network[J]. Physical Communication, 2023, 57: 102005.

[17] GU K, YANG L H, WANG Y, et al. Traceable identity-based group signature[J]. RAIRO - Theoretical Informatics and Applications, 2016, 50 (3): 193-226.

[18] ZHU X Y, JIANG S R, WANG L M, et al. Privacy-preserving authentication based on group signature for VANETs[C]//Proceedings of the 2013 IEEE Global Communications Conference (GLOBECOM). Piscataway: IEEE Press, 2013: 4609-4614.

[19] LIN C, HE D B, KUMAR N, et al. HomeChain: a blockchain-based secure mutual authentication system for smart homes[J]. IEEE Internet of Things Journal, 2020, 7(2): 818-829.

[20] 杨亚涛, 蔡居良, 张筱薇, 等. 基于SM9算法可证明安全的区块链隐私保护方案[J]. 软件学报, 2019, 30(6): 1692-1704.
YANG Y T, CAI J L, ZHANG X W, et al. Privacy preserving scheme in block chain with provably secure based on SM9 algorithm[J]. Journal of Software, 2019, 30(6): 1692-1704.
[21] CHEN L Q, CHENG Z H. Security proof of Sakai-kasahara's identity-based encryption scheme[C]//Proceedings of the 10th international conference on Cryptography and Coding. Berlin: Springer, 2005: 442-459.
[22] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[C]//Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology. Berlin: Springer, 2001: 514-532.
[23] POINTCHEVAL D, STERN J. Security proofs for signature scheme[C]//Proceedings of the 1996 Annual International Conference on Theory and Applications of Cryptographic Techniques. Berlin: Springer, 1996: 387-398.
[24] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985, 31(4): 469-472.
[25] SARASWAT D, PATEL F, BHATTACHARYA P, et al. UpHaaR: Blockchain-based charity donation scheme to handle financial irregularities[J]. Journal of Information Security and Applications, 2022, 68: 103245.
[26] ZHOU Y, LEI H, BAO Z J. Eisdspa: an efficient and secure blockchain-based donation scheme with privacy protection and auditability[J]. IEEE Open Journal of the Communications Society, 2024, 5: 7498-7510.
[27] WANG Z W. Blockchain-based edge computing data storage protocol under simplified group signature[J]. IEEE Transactions on Emerging Topics in Computing, 2022, 10(2): 1009-1019.
[28] ZHANG A Q, ZHANG P Y, WANG H Q, et al. Application-oriented block generation for consortium blockchain-based IoT systems with dynamic device management[J]. IEEE Internet of Things Journal, 2021, 8(10): 7874-7888.

[作者简介]

刘飚（1981– ），男，湖南邵阳人，博士，北京电子科技学院副教授、硕士生导师，主要研究方向为隐私保护、超晶格密码等。

王治中（2001– ），男，内蒙古锡林浩特人，北京电子科技学院硕士生，主要研究方向为身份隐私保护。

袁喜琴（1998– ），男，山西大同人，北京电子科技学院博士生，主要研究方向为隐私保护与零知识证明等。

封化民（1963–），男，陕西渭南人，博士，北京电子科技学院教授、博士生导师，主要研究方向为密码与信息安全。