面向电力调度指令的区块链隐私可追踪存证方案

王栋[1,2]，王合建[1,2]，玄佳兴[1,2]，郑尚卓[1,2]，陈炳聪[3]

（1. 国网区块链科技（北京）有限公司，北京 100053；2. 国网数字科技控股有限公司，北京 100053；
3. 西安电子科技大学广州研究院，广东 广州 510555）

摘　要：在区块链上对电力调度指令进行可信存证是解决异议调度追责困难的有效手段。电力调度包含指令发起者、接收者、调度指令等高度敏感内容，调度指令存证需在保证敏感内容隐私性的同时验证接收者身份及调度指令的合规性，并在异议调度发生时追踪发起者身份。现有的区块链隐私存证方案大多采用中心化管理方式，这与区块链分布式设置相违背。针对电力调度指令存证的特定需求，设计一个支持调度发起者身份隐私且可追踪、接收者身份以及调度指令隐私且合规的区块链存证方案。将接收者身份及调度指令进行编码，经承诺加密并提供相应的零知识证明保证承诺密文合规后存储至区块链上。采用秘密共享方案对传统的群签名算法进行改进，在不影响签名与验证效率的前提下，将群管理员数量由单方拓展至多方。当异议调度发生时，多名群管理员共同追踪异议调度发起者身份，揭示接收者身份及调度指令信息。理论分析与实验结果表明，该方案具有较高的安全性，执行效率满足实施需求。

关键词：隐私保护；区块链；可追踪；群签名；电力调度

中图分类号：TP309　　**文献标志码**：A　　**DOI**：10.19678/j.issn.1000-3428.0066876

Blockchain Privacy-Traceable Deposit Scheme for Power-Dispatch Instructions

WANG Dong[1,2], WANG Hejian[1,2], XUAN Jiaxing[1,2], ZHENG Shangzhuo[1,2], CHEN Bingcong[3]

(1. State Grid Blockchain Technology(Beijing) Co., Ltd., Beijing 100053, China;
2. State Grid Digital Technology Holding Co., Ltd., Beijing 100053, China;
3. Guangzhou Institute of Technology, Xidian University, Guangzhou 510555, Guangdong, China)

【Abstract】 Solving the challenge of accountability for objection scheduling is an effective method to realize the reliable storage of power-dispatch instructions on blockchain. Power dispatching involves highly sensitive content such as command initiators, receivers, and dispatching commands. The dispatching-command storage must verify the compliance of the recipients and dispatch commands while ensuring the privacy of sensitive content, as well as track the initiator when an objection to dispatch occurs. Most existing blockchain storage and certificate schemes adopt a centralized management method, which is contrary to the blockchain-distributed setting. Based on the specific requirements of power-dispatching storage, a blockchain certificate-storage scheme is designed to support the privacy and traceability of the dispatcher's identity, the privacy and compliance of the receiver's identity, and the dispatching instructions. The recipient identity and scheduling instruction are encoded and stored on the blockchain after being encrypted by the commitment and providing the corresponding zero-knowledge proof to ensure compliance with the commitment ciphertext. The classical group-signature algorithm is improved using a secret-sharing scheme, and the number of group administrators is expanded from one party to multiple parties without affecting the efficiency of the signature and verification. When objection scheduling occurs, multiple group administrators jointly track the identity of the objection-scheduling initiator as well as reveal the receiver identity and scheduling-instruction information. Theoretical analysis and experimental results show that the scheme demonstrates high safety and execution efficiency, thus satisfying the implementation requirements.

【Key words】 privacy protection; blockchain; traceable; group signature; power dispatching

0　引言

传统的电子存证面临丢失风险高、自动化程度低、易被篡改破坏等问题，司法机关难以采信，阻碍了电子存证的广泛应用。区块链因其数据分布式存储带来的难以篡改、可追溯的天然特性，极适合与电子存证相结合，能够有效克服传统电子存证的缺陷。目前，区块链存证技术在图书侵权记录[1]、水质信息存证[2]、农产品溯源[3]等领域已经有了初步应用。

电力调度是确保电力系统安全、经济运行和提

收稿日期：2023-02-06　　**修回日期**：2023-03-29

基金项目：国家电网有限公司总部管理科技项目（5108-202114038A-0-0-00）。

通信作者 E-mail：wanghejian@sgdt.sgcc.com.cn

高电能质量所必需的重要手段[4]。具体来说,系统调度员按照规定的权限对其调度范围内的下一级调度机构调度员和发电厂以及变电所值班人员下达调度任务。电力调度具有高度严肃性,要求指令发布者发布正确的指令,接收者在收到指令之后必须严格执行[5]。为避免调度指令下达或执行有误后产生的纠纷,需要设计一种有效指令存证机制以确保错误调度任务的准确追责。

与版权、水质信息、农产品等存证不同,典型的电力调度包括发起者、接收者、调度指令、辅助信息(如指令执行期限)等 4 个部分的内容,具有高度信息敏感特性。区块链数据分布式存储意味着链上存储的数据对所有共识节点公开可见,这就要求链上存证的电力调度满足以下需求与挑战:

1)在分布式环境下调度发起者身份隐私与可追踪的挑战。通常存证发起者对存证内容执行数字签名然后上传到区块链上,以满足存证内容的不可否认性。然而,在基于区块链环境的电力调度存证应用中:一方面,不存在一个可信中心来为整个系统生成相关成员密钥材料;另一方面,发起者身份需要条件隐私保护,即在确保调度发起者身份隐私保护的同时,在异议调度发生时能够有效揭露发起者真正身份。

2)接收者身份以及调度指令隐私且合规的挑战。在版权等存证应用中,对存证内容采用哈希函数计算,然后将计算出的数据指纹记录在区块链,这一朴素式的存证方案不能直接应用于电力调度存证。主要原因在于:以调度指令为例,调度指令通常包括有限个种类,如开关、刀闸、巡线等相关操作。指令接收者身份数量也是受限的。因而,在确保接收者身份以及调度指令隐私的同时,还需要能够验证接收者以及调度指令内容的合规性,即调度指令确实为开关、刀闸、巡线中的某一个操作,接收者为系统中的有效成员。

现有区块链存证研究[1-3]大多将公开可见的数据或数据指纹存入区块链,无法保证存证发起者身份隐私与存证内容的隐私与合规。文献[6-7]使用环签名以及隐蔽地址技术实现了区块链交易的完全匿名性,但并不适用于监管需求的可追踪存证方案。文献[8-11]使用群签名技术实现身份隐私保护与身份可监管之间的平衡,设置单一管理员对身份信息进行监管,保证了身份信息对其他用户不可见。其中心化管理方式与区块链分布式相违背,完全依赖于中心管理的可信性,一定程度上增加了用户隐私泄露的风险。文献[12]通过多群管理员设置分散管理员权限,但其计算开销较高且缺少形式化安全定义及严谨的安全证明。此外,针对存证内容隐私且合规这一特定场景应用,还未见相关的研究工作。

本文针对电力调度存证特定需求,基于分布式区块链环境设计一个支持调度发起者身份隐私且可追踪、接收者身份以及调度指令隐私且合规的安全协议。首先对传统群签名进行改进,设计分布式密钥生成的群签名协议,多群管理员共同完成身份隐私及追踪,调度发起者身份对单一管理员不可见。然后对调度接收者身份以及调度指令进行全局编号,经承诺后上链存储保证其隐私性,并构造零知识证明协议确保上链数据合规性。在异议调度查验时,通过挑战-应答的方式完成隐私数据揭示。最后对所设计的群签名协议进行形式化安全定义及严谨的安全证明。

1 相关工作

目前,已经有许多学者针对区块链存证[13-14]、区块链隐私保护以及追踪与监管技术问题进行了研究,主要包括:群签名与区块链的结合,零知识证明、同态加密与区块链的结合,以及对密文状态下的隐私数据分发和存证的效率研究等。

在区块链存证技术方面,文献[1-3]在不同应用场景下对区块链与电子存证相结合进行探索,验证区块链应用于数据存证领域的可行性,表明区块链存证技术可提高电子证据的司法采信度,降低独立审计成本和难度。但是以上技术均未考虑区块链公开透明的特性,将未经处理的数据存入区块链会带来用户隐私泄露风险。2021 年 11 月 1 日起施行的《中华人民共和国个人信息保护法》对个人敏感数据的公开制度进行了严格的规定,这要求区块链存证方案需考虑用户隐私泄露风险。

在区块链隐私保护技术方面,文献[6]提出了一种基于轻量级同态加密和零知识证明的版权区块链隐私保护方案,弥补了区块链网络中全部数据公开的不足,同时使效率问题得到了改善。门罗币(Monero)[15]使用环签名技术解决了比特币中的可追溯性问题,使得实际输入在一组签名中被隐藏,无法确定具体用户信息。文献[7]提出了一种基于椭圆曲线密码学的环签名方案,相比于传统的基于双线性配对的环签名方案,提高了安全性和身份隐藏性。但在有监管需求的场景下,这些方案并不适用且会带来安全隐患,如门罗币匿名性犯罪问题。

在区块链追踪与监管技术方面,文献[8]提出了一种基于 SM9 算法的群签名方案,实现在节点间进

行身份验证的同时保护节点的隐私。文献[9]提出了一种基于环签名、同态承诺、隐私地址技术的可追踪区块链账本方案,监管人可对交易双方地址和交易数据进行追踪。文献[10]基于群签名、Groth-Sahai 证明系统提出可同时保证发送方、接收方匿名可追踪的方案,达到隐私保护和监管平衡的目标。文献[11]利用群签名和知识证明技术对门罗币的底层技术 CryptoNote 进行改进,实现对门罗币的监管。然而上述隐私可追踪方案均只设置了一名监管者且将其视为可信第三方,未解决恶意监管者窃取用户隐私的问题。

文献[12]提出了一种基于群签名、隐私地址协议、零知识证明、属性加密技术的分布式可监管隐私保护方案。该方案在平衡区块链隐私与可追踪性的同时,针对单一监管者权限过于集中而造成的隐私泄露问题,通过对群签名进行改进,将多群管理员的群签名运用在区块链系统中,解决了以往的区块链隐私可追踪方案监管权限集中的不足。但其多群管理员设置并不完善,签名与验证阶段的计算开销较高,且缺少形式化的安全定义及证明。

综上所述,现有相关工作大多未能在监管能力与隐私泄露间达到良好的平衡,且在多群管理员构造方面还有所欠缺。

2 预备知识

2.1 联盟链与智能合约

最早的区块链定义是一种用于存储比特币交易历史数据的数据结构[16]。区块链以互联网为基础,依托于算法、软件等技术,为彼此不信任的交易参与方间搭建了一个可信平台。区块链按照开放程度可以分为公有链、联盟链[17]和私有链。公有链是开放的与可自由加入的,账本公开范围和应用范围都是所有人,满足完全去中心化。联盟链由联盟成员作为共识节点,区块链账本在联盟成员间公开可见。私有链只对单独的个体或实体开放。相比于公有链,联盟链具有监管性强、共识效率高等特点。在实际应用中需要根据不同的需求和应用场景来选择所使用的区块链类型。由于联盟链的共识过程由预先选好的节点控制,交易的确认时间较短,每秒的交易数较多,在安全与性能上的要求较高,因此在隐私保护的区块链存证场景中使用联盟链最为适合。

智能合约是运行在区块链上的程序,通过 API 接口与区块链进行交互。智能合约具有自动执行、公开透明、不可篡改等特性,即开发者通过编写智能合约来规定事件的执行,智能合约一旦写好被上传至区块链网络就无法改变。当设定的条件被触发时,智能合约就会自动执行,他方无法进行干涉。

2.2 Shamir 门限秘密共享方案

秘密共享方案是指把主秘密 S 分成 n 个子秘密 $S_1,S_2,\cdots,S_n$,将子秘密 S_i 分发给参与方 P_i,被授权的参与方子集能够利用其拥有的子秘密恢复主秘密 S。

1979 年,文献[18]提出了基于 Lagrange 插值公式的(t,n)门限秘密共享方案,具体步骤主要包括秘密分发阶段和秘密恢复阶段。

1)秘密分发阶段。秘密分发者随机地从有限域 $F_q(q\geqslant n,q>s)$ 中选取 n 个不同的非零元素 x_1,$x_2,\cdots,x_n$,构造 $t-1$ 阶多项式:

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}\bmod q$$

其中:q 是个大素数,要分发的秘密 $s=f(0)=a_0$。然后计算子秘密 $s_i=f(x_i)$,将 (x_i,s_i)分发给参与者 P_i。

2)秘密恢复阶段。根据多项式插值的存在唯一性定理,任意 t 个点 (x_i,s_i)可以唯一确定一个 $t-1$ 阶多项式。利用 Lagrange 插值公式进行秘密恢复:

$$f(x)=\sum_{i=1}^{t}s_i\sum_{1\leqslant j\leqslant t,j\neq i}\frac{x-x_j}{x_i-x_j}\bmod q$$

最终得到秘密 $s=f(0)$。

2.3 短群签名算法

群签名是一种特殊的数字签名。一般来讲,群签名要满足以下 4 个性质:

1) 不可伪造性,即只有群成员才能生成有效可被验证的群签名。

2) 匿名性,即验证者只能验证签名的有效性,并得到签名者所属群组,无法获得签名者身份。

3) 不可链接性,即无法判断 2 个签名是否来自同一个签名者。

4) 可追溯性,即群管理员可以通过群签名追溯到其群成员。

目前已知的签名长度最短的群签名算法是文献[19]提出的短群签名算法。该算法基于强 Diffie-Hellman 假设和双线性映射构造了小于 200 Byte 的签名,在应用于区块链时,可以在实现用户匿名和签名追溯的同时节约链上空间。

2.4 Pedersen 承诺

密码学中的承诺方案是关于承诺方和接收方的两方交互协议,Pedersen 承诺[20]是其中一种具有完美隐藏性和强绑定性同时满足同态性质的承诺。

本文利用 Pedersen 承诺的完美隐藏性保证接收者身份及调度指令不会被泄露,利用绑定性保证

接收者身份及调度指令不会被恶意篡改，通过承诺的同态性结合范围证明实现接收者身份及调度指令的合规性验证。

2.5 范围证明

范围证明保证接收者身份及调度指令的合规性。为提高方案实现的效率，本文使用一种快速的范围证明方案 Bulletproofs[21]，可以将生成证明的时间降低为毫秒级。同时，可以使用 Fiat-Shamir 启发式构造一个非交互式的范围证明，这将会减少证明方与验证方的交互次数，便于方案的简洁执行。

在本文方案中，范围证明用于保证区块链存储的接收者身份及调度指令编码值处于事先制定好的编码表内，而非无效值。

3 分布式密钥生成的群签名协议

群签名协议保证群成员无法获取签名者身份，但群管理员可使用追踪密钥揭示签名者身份。然而传统的群签名方案[19]的单一管理员设置导致管理权限过于集中，使用秘密共享方案结合文献[22-23]中指数逆计算的思想改进传统的群签名方案，使管理权限由多名群管理员共同掌握。

本节采用文献[19]中的符号系统描述群签名协议，G_1、G_2 是两个循环群，公钥 $\mathrm{gpk}=(g_1,g_2,h,u,v,\omega)$，其中，$g_1,u,v,h\in G_1$，$g_2,\omega\in G_2$ 且 $g_1=\psi(g_2)$。随机选取 $\xi_1,\xi_2,\gamma\in\mathbb{Z}_p$，$u^{\xi_1}=v^{\xi_2}=h$，$\omega=g_2{}^{\gamma}$。私钥 $\mathrm{gsk}[m]=(A_m,x_m)$，其中，$A_m\in G_1,x\in\mathbb{Z}_p$ 且满足 $A_m^{x+\gamma}=g_1$，使得 $e(A_m,\omega g_2^{x})=e(g_1,g_2)$。与文献[19]不同的是为满足分布式追踪需求，追踪密钥不再为 $\mathrm{gmsk}=(\xi_1,\xi_2)$，而是 $\mathrm{tpk}[m]=A_m^{r}$。

在分布式密钥生成的群签名协议中，协议 1、4、5、6 为主要协议，协议 2、3 为辅助协议。算法 1、2 用于签名与验证。本文分布式密钥生成的群签名协议用于保护调度指令发起者身份隐私。

3.1 密钥生成阶段

协议 1 初始化协议。

初始化协议用于生成联合公钥生成协议、分布式成员私钥生成协议所需的参数碎片 r_i、ξ_{1i}、ξ_{2i}、γ_i，具体过程如下：

1）每个群管理员选择 $R_i,x_{1i},x_{2i},y_i\xleftarrow{R}\mathbb{Z}_p^*(i=0,1,\cdots,n-1)$，用 Shamir 秘密共享的形式将 R_i、x_{1i}、x_{2i}、y_i 的秘密分片共享给其他群管理员。

2）每个群管理员将所收到的秘密分片相加得到 R'_i、x'_{1i}、x'_{2i}、$y'_i(i=0,1,\cdots,n-1)$，其分别为 r、ξ_1、ξ_2、γ 的 (t,n) 共享形式。

3）选取出 t 个群管理员，计算：

$$r_i=\lambda_i R'_i$$
$$\xi_{1i}=\lambda_i x'_{1i}$$
$$\xi_{2i}=\lambda_i x'_{2i}$$
$$\gamma_i=\lambda_i y'_i$$

其中：$\lambda_i=\prod_{j=0,j\neq i}^{t-1}\frac{-j-1}{(i-j)}$，$i=0,1,\cdots,t-1$。$r_i$、$\xi_{1i}$、$\xi_{2i}$、$\gamma_i$ 满足如下等式：

$$r=\sum_{i=0}^{t-1}r_i=\sum_{i=0}^{n-1}R_i$$
$$\xi_1=\sum_{i=0}^{t-1}\xi_{1i}=\sum_{i=0}^{n-1}x_{1i}$$
$$\xi_2=\sum_{i=0}^{t-1}\xi_{2i}=\sum_{i=0}^{n-1}x_{2i}$$
$$\gamma=\sum_{i=0}^{t-1}\gamma_i=\sum_{i=0}^{n-1}y_i$$

协议 2 乘法共享转换求和协议。

指数逆计算过程中面临 P_i 方持有 b_i，P_j 方持有 θ_j，但需求解 $b\theta=\sum_{i=0}^{t-1}b_i\sum_{j=0}^{t-1}\theta_j$ 的问题，其中 P_i、$P_j(i,j=0,1,\cdots,t-1,i\neq j)$ 为不同的群管理员。此处利用 Paillier 公钥加密体制[24]的加法同态性质，将乘法共享转换为加法共享，使得 $b_i\theta_j=\alpha_{ij}+\beta_{ij}$，具体过程如下：

1）每个 P_i 生成 Paillier 公钥加密密钥对，公开公钥 pk_i。

2）每个 P_i 计算 $E_{\mathrm{pk}_i}(\theta_i)$、$b_i\theta_i$，并将结果公开。

3）每个 P_i 为收到的 $E_{\mathrm{pk}_j}(\theta_j)$ 随机选择 β'_{ij} 后计算 $E_{\mathrm{pk}_j}(b_i\theta_j+\beta'_{ij})$ 发送至 P_j，令 $\beta_{ij}=-\beta'_{ij}$，并公开结果。

4）每个 P_i 解密收到 $E_{\mathrm{pk}_i}(b_i\theta_j+\beta'_{ij})$，计算 $\alpha_{ij}=b_i\theta_j+\beta'_{ij}$，并将结果公开。

5）每个 P_i 计算 $\lambda=b\theta=\sum_{i=0}^{t-1}b_i\sum_{j=0}^{t-1}\theta_j=\sum_{k=0}^{t-1}b_k\theta_k+\sum_{0\leqslant i,j\leqslant t-1,i\neq j}(\alpha_{ij}+\beta_{ij})$。

协议 3 指数逆计算协议。

密钥生成协议执行过程中面临多方联合求指数逆 $a^{\left(\sum_{i=0}^{t-1}b_i\right)^{-1}}$ 的问题，其中 b_i 由每个群管理员持有。在此处先引入掩码 θ 再明文进行求逆，具体过程如下：

1）每个群管理员随机选择一个 $\theta_i\xleftarrow{R}\mathbb{Z}_p^*$，计算 a^{θ_i}，并将结果公开。

2）每个群管理员在收到其他成员的结果之后计算 $a^{\theta}=\prod_{i=0}^{t-1}a^{\theta_i}$。

3)t 个群管理员利用协议 2 计算 $\lambda=b\theta$，并公开 λ^{-1}。

4)每个群管理员计算 $a^{\left(\sum_{i=0}^{t-1}b_i\right)^{-1}}=(a^{\theta})^{\lambda^{-1}}$。

协议 4 联合公钥生成协议。

选取出的 t 个群管理员协同生成公钥 $\mathrm{gpk}=(g_1,g_2,h,u,v,\omega)$，具体过程如下：

1)随机选取 G 的生成元 g_2，g_1 由同构映射 $\psi(g_2)$ 产生，联合选择 $h\xleftarrow{R}G_1\backslash\{1_{G_1}\}$。

2)每个群管理员分别求 $g_2^{\gamma_i}$，并将结果公开，每个群管理员计算 $\omega=\prod_{i=0}^{t-1}g_2^{\gamma_i}$。

3)t 个群管理员使用协议 3 联合求 $u=h^{\xi_1^{-1}}$、$v=h^{\xi_2^{-1}}$。

协议 5 分布式成员私钥生成协议。

选取出的 t 个群管理员可以为成员 m 颁发成员私钥 $\mathrm{gsk}[m]=(A_m,x_m)$，公开追踪密钥 $\mathrm{tpk}[m]=A_m^r$，成员私钥由成员 m 掌握，追踪密钥用于追踪成员身份，具体过程如下：

1)每个群管理员选择 $x_i\xleftarrow{R}\mathbb{Z}_p^*$，并将其发送给成员 m，成员 m 根据收到的 x_i 计算 $x_m=\sum_{i=0}^{t-1}x_i$。

2)t 个群管理员使用协议 3 联合求解 $A_m=g_1^{(\gamma+x_m)^{-1}}$，但在步骤 3 中不同步计算 λ，而是所有群管理员将合成 λ 的碎片信息发送给成员 m，由成员 m 计算 λ，并最终获得 A_m。

3)每个群管理员计算 $g_1^{r_i}$ 并将结果公开，每个群管理员在收到其他成员的结果之后计算 $g_1^r=\prod_{i=0}^{t-1}g_1^{r_i}$。$t$ 个群管理员使用协议 3 联合求追踪密钥 $\mathrm{tpk}[m]=g_1^{r\sum_{i=0}^{t-1}(\gamma_i+x_i)^{-1}}=g_1^{r(\gamma+x_m)^{-1}}=A_m^r$，并公开结果。

3.2 签名与验证阶段

算法 1 签名算法

输入 公钥 gpk，成员私钥 $\mathrm{gsk}[m]$，消息 $M\in\{0,1\}^*$

输出 签名 σ

1. 选择 $\alpha,\beta\xleftarrow{R}\mathbb{Z}_p$，计算 $T_1=u^{\alpha}$，$T_2=v^{\beta}$，$T_3=A_m h^{\alpha+\beta}$，$\delta_1=x_m\alpha$，$\delta_2=x_m\beta$。

2. 选择 $r_\alpha,r_\beta,r_x,r_{\delta_1},r_{\delta_2}\xleftarrow{R}\mathbb{Z}_p$，计算：$R_1=u^{r_\alpha}$，$R_2=v^{r_\beta}$，$R_4=T_1^{r_x}\cdot u^{-r_{\delta_1}}$，$R_5=T_2^{r_x}\cdot v^{-r_{\delta_2}}$，$R_3=e(T_3,g_2)^{r_x}\cdot e(h,w)^{-r_\alpha-r_\beta}\cdot e(h,g_2)^{-r_{\delta_1}-r_{\delta_2}}$。

3. 计算挑战 $c=H(M,T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5)$，其中 H 为哈希函数。

4. 计算响应 $s_\alpha=r_\alpha+c\alpha$，$s_\beta=r_\beta+c\beta$，$s_x=r_x+cx_m$，$s_{\delta_1}=r_{\delta_1}+c\delta_1$，$s_{\delta_2}=r_{\delta_2}+c\delta_2$。

5. 签名 $\sigma=(T_1,T_2,T_3,c,s_\alpha,s_\beta,s_x,s_{\delta_1},s_{\delta_2})$。

算法 2 验证算法

输入 公钥 gpk，消息 $M\in\{0,1\}^*$，签名 σ

输出 验证是否通过

1. 计算：$\widetilde{R}_1=u^{s_\alpha}/T_1^c$，$\widetilde{R}_2=v^{s_\beta}/T_2^c$，$\widetilde{R}_4=T_1^{s_x}/u^{s_{\delta_1}}$，$\widetilde{R}_3=e(T_3,g_2)^{s_x}\cdot e(h,w)^{-s_\alpha-s_\beta}\cdot e(h,g_2)^{-s_{\delta_1}-s_{\delta_2}}\cdot((e(T_3,w)/e(g_1,g_2))^c$，$\widetilde{R}_5=T_2^{s_x}/v^{s_{\delta_2}}$。

2. 验证 $c\stackrel{?}{=}H(M,T_1,T_2,T_3,\widetilde{R}_1,\widetilde{R}_2,\widetilde{R}_3,\widetilde{R}_4,\widetilde{R}_5)$，通过则输出 res 值为 1，否则输出 res 值为 0(其中，res 表示 1 bit 的验证结果，1 表示验证正确，0 表示验证错误)。

3.3 分布式联合追踪阶段

协议 6 联合追踪协议。

选取出的 t 个群管理员可以联合追踪一个签名 σ 的签名者身份，具体过程如下：

1)每个群管理员计算 $T_1^{r_i}$、$T_2^{r_i}$、$T_3^{r_i}$ 并公开结果，每个成员计算 $T_1^r=\prod_{i=0}^{t-1}T_1^{r_i}$、$T_2^r=\prod_{i=0}^{t-1}T_2^{r_i}$、$T_3^r=\prod_{i=0}^{t-1}T_3^{r_i}$。

2)每个群管理员计算 $T_1^{r\xi_{1i}}$、$T_2^{r\xi_{2i}}$ 并公开结果，每个成员计算 $T_1^{r\xi_1}\cdot T_2^{r\xi_2}=\prod_{i=0}^{t-1}T_1^{r\xi_{1i}}\cdot T_2^{r\xi_{2i}}$。

3)每个群管理员计算 $A_x^r=T_3^r/(T_1^{r\xi_1}\cdot T_2^{r\xi_2})$，与 $\mathrm{tpk}[m]$ 对比确定签名成员的索引，确定签名者的身份。

4 本文方案

本文方案将分布式密钥生成的群签名协议与联盟链相结合，一个联盟链与群签名中一个群的概念对等[25]，在后续方案表述中，调度数据委员会委员与上文群管理员对等，方案中共识节点分为管理节点和存证节点，行使功能如下：

1) 管理节点：调度数据链委员会委员(群管理员)接入管理节点，联合执行密钥生成协议为调度指令发起者派发成员私钥。当调度数据出现争议时，追踪调度指令发起者身份，揭示调度指令内容，同时作为联盟链中的全节点，验证交易合法性、维护全网账本。

2) 存证节点：调度指令发起者接入存证节点，通过执行智能合约的方式在联盟链上存储隐私保护的调度数据信息，同时作为联盟链中的全节点，验证交易合法性、生成区块并且维护全网账本。

本文方案围绕调度者身份的隐私可追踪性、调度指令及调度对象的合法性、调度指令的准确性进行设计，方案包括系统初始化、生成存证数据、调度数据隐私存证、异议调度审查 4 个部分。本文方案框架如图 1 所示。

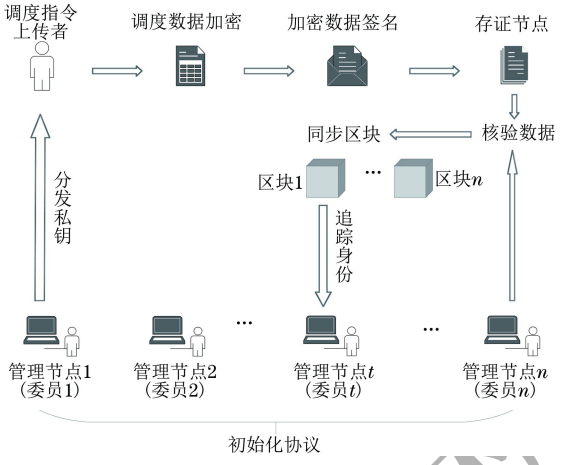

图 1 本文方案框架

Fig. 1 Framework of this paper scheme

4.1 系统初始化

调度数据链委员会确认门限值(t,n)，选取出 t 个委员执行后续协议，委员会委员联合执行协议 1 生成分布式群签名公私钥碎片信息 r_i、ξ_{2i}、ξ_{2i}、γ_i。委员会委员联合执行协议 4 生成分布式群签名公钥 gpk 并公开，由所有共识节点持有。符合条件的调度指令发起者 m 可申请参与存证业务，委员会委员联合执行协议 5 生成分布式成员私钥 $\mathrm{gsk}[m]$ 由调度指令发起者 m 持有及追踪密钥 $\mathrm{tpk}[m]$ 由管理节点持有。

调度指令包含调度指令内容与调度指令接收者身份两部分信息。调度数据链委员会对调度指令内容以及调度指令接收者进行编码，构造调度指令信息编码表，其中，调度指令内容编码为 $\mathrm{Msg}_i=\{\mathrm{Msg}_0,\mathrm{Msg}_1,\cdots,\mathrm{Msg}_{n_1}\}$，$n_1$ 为调度指令内容的总数量，调度指令接收者编码为 $\mathrm{ID}_j=\{\mathrm{ID}_0,\mathrm{ID}_1,\cdots,\mathrm{ID}_{n_2}\}$，$n_2$ 为调度指令接收者的总数量，调度数据链委员会协商安全参数 λ，委员会选取一个委员执行 Pedersen 承诺初始化算法 $\mathrm{Setup}(1^\lambda)$ 得到参数 g、h、p、q 并公开，选择 $\boldsymbol{g},\boldsymbol{h}\in G^n$ 并公开，$\boldsymbol{g}$、$\boldsymbol{h}$ 表示生成元的一个 n 维向量，该委员随机选择 $r_{n1},r_{n2}\in\mathbb{Z}_q$ 并公开，计算 $C_{n_1}=g^{n_1}h^{r_{n1}}$、$C_{n_2}=g^{n_2}h^{r_{n2}}$ 并公开，其他委员验证承诺值计算是否正确。

4.2 存证数据生成

调度指令发起者 m 根据调度指令信息编码表，将调度指令内容及调度指令接收者信息映射为编码值 Msg_i、ID_j，随机选择 $r_i,r_j\in\mathbb{Z}_q$，计算 $C_i=g^{\mathrm{Msg}_i}h^{r_i}$，$C_j=g^{\mathrm{ID}_j}h^{r_j}$，同时计算 $C_{n_1-i}=C_{n_1}/C_i$，$C_{n_2-j}=C_{n_2}/C_j$。

对于承诺值 C_i，调度指令发起者使用公开元组 g、h、$\boldsymbol{g}$、$\boldsymbol{h}$，其中 $\boldsymbol{g}$、$\boldsymbol{h}$ 表示生成元的一个 n 维向量，数值 i 执行算法 3 得到 P_i 证明 $\mathrm{Msg}_i\geqslant 0$，使用公开元组 g、h、$\boldsymbol{g}$、$\boldsymbol{h}$，数值 n_1-i 执行算法 3 得到 P_{n_1-i} 证明 $\mathrm{Msg}_i\leqslant n_1$。

对于承诺值 C_j，调度指令发起者使用公开元组 g、h、$\boldsymbol{g}$、$\boldsymbol{h}$，数值 j 执行算法 3 得到 P_j 证明 $\mathrm{ID}_j\geqslant 0$，使用公开元组 g、h、$\boldsymbol{g}$、$\boldsymbol{h}$，数值 n_2-j 执行算法 3 得到 P_{n_2-j} 证明 $\mathrm{ID}_j\leqslant n_2$。

算法 3 生成算法

输入 公开元组 g、h、$\boldsymbol{g}$、$\boldsymbol{h}$，数值 v

输出 范围证明 P_v

1. 选择 $a_L=\{a_1,a_2,\cdots,a_n\}\in\{0,1\}^n$ 令$\langle a_L,2^n\rangle=v$，$a_R=a_L-1^n$，从 $\mathbb{Z}_p$ 中随机挑选元素 α，对 a_L 和 a_R 进行承诺 $A=h^\alpha g^{a_L}h^{a_R}$，从 $\mathbb{Z}_p^n$ 中随机挑选盲因子 S_L、S_R 以及从 $\mathbb{Z}_p$ 中随机挑选元素 ρ，对 S_L 和 S_R 进行承诺 $S=h^\rho g^{S_L}h^{S_R}$；计算 $y=H(A,S)$，$z=H(A,S,y)$，输出 A、S、y、z。

2. 构造零知识体系 $l(X)=a_L-z\cdot 1^n+S_L\cdot X$，$r(X)=y^n\circ(a_R+z\cdot 1^n+S_R\cdot X)+z^2\cdot 2^n$，$t(X)=\langle l(X),r(X)\rangle=t_0+t_1\cdot X+t_2\cdot X^2$，从 $\mathbb{Z}_p$ 中随机挑选元素 τ_1、τ_2，对系数 t_i 进行承诺得到 $T_i=g^{t_i}h^{\tau_i}$，$i=\{1,2\}$，计算 $x=H(T_1,T_2,z)$，输出 T_1、T_2、x。

3. 计算 $l(x)=l(X)$，$r(x)=r(X)$，$t(x)=\langle l(x),r(x)\rangle$，随机选取 γ，计算 $\tau_x=\tau_1\cdot x+\tau_2\cdot x^2+z^2\cdot\gamma$，$\mu=\alpha+\rho\cdot x$，输出 $l(x)$、$r(x)$、$t(x)$、τ_x、μ，构造范围证明 $P_v=(A,S,y,z,T_1,T_2,x,l(x),r(x),t(x),\tau_x,\mu)$。

调度指令发起者 m 对消息 $M=(C_i,C_j,C_{n_1-i},C_{n_2-j},P_i,P_j,P_{n_1-i},P_{n_2-j})$ 使用成员私钥 $\mathrm{gsk}[m]$，公钥 gpk 执行算法 1 得到签名 σ 并向存证节点申请将上述调度信息上链存储。

4.3 调度数据隐私存证

存证节点将上述信息打包为区块并广播至所有共识节点，各共识节点使用消息 M 和公开信息 C_{n_1}、C_{n_2} 验证等式 $C_i\cdot C_{n_1-i}=C_{n_1}$，$C_j\cdot C_{n_2-j}=C_{n_2}$ 是否正确，利用算法 4 以及消息 M 验证范围证明是否通过，使用公钥 gpk，签名 σ 以及消息 M 执行算法 2 验证签名是否正确，上诉验证均通过则所有共识节点执行共识算法，将消息 M 上链存储。

算法 4 验证算法

输入 公开元组 g、h、$\boldsymbol{g}$、$\boldsymbol{h}$，承诺 Com，范围证明 P_v

输出 验证是否通过

1. 验证等式 $y=H(A,S)$，$z=H(A,S,y)$，$x=H(T_1,T_2,z)$是否均正确。

2. 令 $h_i'=h_i^{y^{-i+1}}$，$\forall i\in[1,n]$，验证 t,τ_x 的有效性，当且仅当其格式正确，等式 $g^t h^{\tau_x}=g^{\delta}\cdot Com^{z^2}\cdot T_1^x\cdot T_2^{x^2}$ 成立。

3. 令 $P=AS^x\cdot g^{-z}\cdot h'^{z\cdot y^n+z^2\cdot 2^n}$，验证 l、r 的有效性，当且仅当其格式正确，等式 $P=h^{\mu}\cdot g^{l}\cdot h'^{r}$ 成立。最终验证多项式等式 $t(x)=\langle l(x),r(x)\rangle$是否成立并输出 res 值，若成立则明文范围验证通过，res 值为 1，否则验证失败，res 值为 0。

4.4 异议调度审查

在调度数据出现纠纷时，委员会委员联合执行协议 6，追踪异议调度指令发起者身份信息。调度数据链委员会从区块链上获取其存储的承诺值 C_i、C_j，向异议调度指令发起者 m 请求调度指令信息 Msg_i、ID_j 及盲因子 r_i、r_j。调度数据链委员会核验 $C_i \stackrel{?}{=} g^{Msg_i}h^{r_i}$ 和 $C_j \stackrel{?}{=} g^{ID_j}h^{r_j}$，通过则将 Msg_i、ID_j 根据此前建立的调度指令信息编码表映射为调度内容、调度指令接收者信息，对该信息的正确性及合理性进行审查，惩罚相应责任人。

5 实验

5.1 方案对比

本文分别从群管理员数量、追踪方、是否有严格的安全定义与证明 3 个方面将本文方案与其他方案进行对比，如表 1 所示。

表 1 不同方案群管理员数量、追踪方、严格安全定义与证明的对比

Table 1 Comparison of the number of group administrators, tracking parties, strict security definitions and proofs for different schemes

方案	群管理员数量	追踪方	严格的安全定义与证明
本文方案	动态	双方	是
文献[12]方案	动态	双方	否
文献[10]方案	1	双方	否
文献[11]方案	1	单方	否

通过对比可以看出，本文方案在实现多群管理员监管的同时，实现对调度双方身份进行追踪，并且提供了严格的安全定义与证明。

表 2 对比了本文方案与文献[12]方案所需的计算成本。其中，模幂运算计算成本表示为$|M|$，线性对运算计算成本表示为$|P|$，哈希运算计算成本表示为$|H|$。

从表 2 可以看出，本文方案在公钥生成、成员私钥生成、身份追踪步骤需要更高的计算成本，且此部分计算成本与群管理员数量呈线性正相关。相比文献[12]方案，本文方案在公钥生成、成员私钥生成步骤需要额外增加 $18t|M|$ 的计算成本，在身份追踪步骤需要额外增加$(5t-1)|M|$的计算成本。本文方案在签名与签名验证步骤的计算成本与群管理员数量无关，并且与文献[12]方案在 $t=1$ 时的计算成本相同，极大地减少了在群管理员人数较多时的计算成本。在实际应用中，每次存证均需执行签名与验证步骤，而公私钥生成步骤只需在群成员加入或群管理员变更时执行，身份追踪步骤只需在异议调度发生时执行，相比文献[12]方案，本文方案在实际应用中效率更高，更具有实际意义。

表 2 不同方案的计算成本对比

Table 2 Calculation cost comparison of different schemes

步骤	本文方案	文献[12]方案
公钥生成	$19t\|M\|$	$t\|M\|$
成员私钥生成	$19t\|M\|$	$t\|M\|$
签名	$12\|M\|+3\|P\|+\|H\|$	$(11+t)\|M\|+(2+t)\|P\|+\|H\|$
签名验证	$12\|M\|+5\|P\|+\|H\|$	$(9+3t)\|M\|+(1+4t)\|P\|+\|H\|$
身份追踪	$5t\|M\|$	$\|M\|$
数据查验	$4\|M\|$	$\|M\|+\|P\|$

5.2 实验验证

为测试本文方案的实际时间开销，使用 Go 语言编写测试程序，所有测试均在 Inter Core i5-8500 3.00 GHz 的 6 核 CPU 与 8 GB RAM 的设备上进行，操作系统配置为 Ubuntu-20.04.3。

首先测试文中群签名协议的表现情况。在不计算网络开销的情况下，本地测试了初始化协议(协议 1)、联合公钥生成协议(协议 4)、分布式用户密钥生成协议(协议 5)、联合追踪协议(协议 6)在不同群管理员数量下的执行时间。由于协议所需时间开销主要取决于门限值 t 的大小而不是 n，因此在测试中将 n 的值固定设置为 21。

不同群管理员数量下各协议执行时间如图 2 所示。

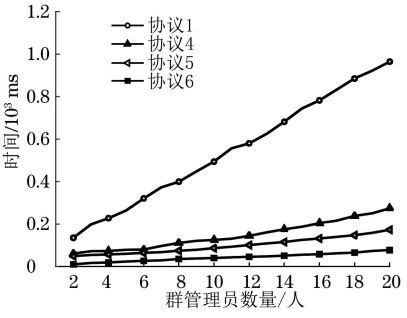

图 2 不同群管理员数量下的协议执行时间

Fig. 2 Protocol execution time of different group administrators

从图 2 可以看出，由于涉及多方共同生成多个初始化参数，协议 1 初始化协议耗时最多，但在群管理员为 20 人的情况下仍可以在 1 000 ms 内完成运算，且该协议可预先多次执行生成本地数据用于后续协议。协议 4、5、6 在群为 20 人的情况下执行时间分别为 274.16、173.36、77.31 ms，即使在参与协议的群管理员人数较多的情况仍然可以以毫秒级的延时完成群签名公私钥的生成，且调度指令生成者身份追踪时间仅需 70 ms，保证了在出现异议调度时追踪的高效性。

其次测试文中方案在群管理人数为 10 人时各步骤执行情况，其中范围证明区间为 $[0,2^{32}-1]$。不同方案性能对比如表 3 所示。

表 3 不同方案性能对比

Table 3 Performance comparison of different schemes

单位：ms

步骤	算法	计算开销
系统初始化	初始化协议	494.05
	公钥生成	124.92
	成员私钥生成	87.18
生成存证数据	承诺计算	4.31
	范围证明	62.22
	签名	51.92
身份隐私存证	范围证明验证	1.28
	签名验证	69.24
异议调度审查	身份追踪	40.05
	数据查验	0.66

从表 3 可以看出，在系统初始化步骤共需 706.15 ms，生成存证数据步骤共需 118.45 ms，身份隐私存证步骤共需 70.52 ms，异议调度审查步骤共需 40.71 ms，在不计算共识算法开销下每条调度指令链上存储所需总时间为 188.97 ms。

6 结束语

本文针对电力调度指令存证场景中面临的身份隐私保护及数据隐私保护需求，使用群签名技术结合多方安全计算，设计分布式密钥管理的群签名协议。该协议中的密钥分发及身份追踪阶段均需达到门限数量的多个调度数据链委员会委员联合执行，解决传统群签名中管理员的权力集中、身份隐私无法保障的问题，同时对调度数据进行全局编号，构造零知识证明协议确保链上调度指令内容隐私及合法性。此外，针对异议调度指令查验需求，采用安全计算技术揭示调度发起者真实身份，同时通过挑战-响应的方式完成调度指令以及调度指令接收者身份的揭示。由于当前群签名密钥生成时间随群管理员数量的增多而增加，因此优化密钥生成时间，提高方案执行效率是下一步的研究方向。

参考文献

[1] 张逸飞，曹少中，祁德力，等. 基于区块链的图书侵权记录存证平台[J]. 应用科学学报，2020，38(1)：184-196.
ZHANG Y F，CAO S Z，QI D L，et al. Book infringement record depositing platform based on blockchain[J]. Journal of Applied Sciences，2020，38(1)：184-196.(in Chinese)

[2] 邹秀清，罗得寸，林平，等. 基于区块链的河长制水质信息存证系统[J]. 应用科学学报，2020，38(1)：65-80.
ZOU X Q，LUO D C，LIN P，et al. System of river chief-oriented water quality information certification based on blockchain[J]. Journal of Applied Sciences，2020，38(1)：65-80.(in Chinese)

[3] 吴晓彤，柳平增，王志铧. 基于区块链的农产品溯源系统研究[J]. 计算机应用与软件，2021，38(5)：42-48.
WU X T，LIU P Z，WANG Z H. Traceability system of agricultural products based on blockchain[J]. Computer Applications and Software，2021，38(5)：42-48.(in Chinese)

[4] 刘路登，贾伟，陈天宇，等. 智能化电力调度指令操作系统研究与应用[J]. 电子器件，2021，44(5)：1204-1209.
LIU L D，JIA W，CHEN T Y，et al. Research and application of intelligent power dispatching order operating system[J]. Chinese Journal of Electron Devices，2021，44(5)：1204-1209.(in Chinese)

[5] 林志贤，刘雪飞，郑炜楠，等. 电力调度操作网络发令系统的研究与应用[J]. 自动化技术与应用，2021，40(3)：180-182，186.
LIN Z X，LIU X F，ZHENG W N，et al. Research and application on power dispatching operation network order system[J]. Techniques of Automation and Applications，2021，40(3)：180-182，186.(in Chinese)

[6] 王瑞锦，唐榆程，裴锡凯，等. 基于轻量级同态加密和零知识证明的区块链隐私保护方案[J]. 计算机科学，2021，48(S2)：547-551.
WANG R J，TANG Y C，PEI X K，et al. Blockchain privacy protection scheme based on lightweight homomorphic encryption and zero-knowledge proof[J]. Computer Science，2021，48(S2)：547-551.(in Chinese)

[7] LI X F，MEI Y R，GONG J，et al. A blockchain privacy protection scheme based on ring signature[J]. IEEE Access，2020，8：76765-76772.

[8] 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.(in Chinese)

[9] 张思亮，凌捷，陈家辉. 可追踪的区块链账本隐私保护方案[J]. 计算机工程与应用，2020，56(23)：31-37.
ZHANG S L，LING J，CHEN J H. Traceable blockchain ledger privacy protection scheme[J]. Computer Engineering and Applications，2020，56(23)：31-37.(in Chinese)

[10] 李佩丽，徐海霞. 区块链用户匿名与可追踪技术[J]. 电子与信息学报，2020，42(5)：1061-1067.
LI P L，XU H X. Blockchain user anonymity and traceability technology[J]. Journal of Electronics & Information Technology，2020，42(5)：1061-1067.(in Chinese)

[11] 田海博，林会智，罗裴然，等. 一种用户隐私保护数字货币的可监管方案[J]. 西安电子科技大学学报，2020，47(5)：40-47.
TIAN H B，LIN H Z，LUO P R，et al. Scheme for being able to regulate a digital currency with user privacy protection

[J]. Journal of Xidian University, 2020, 47(5): 40-47. (in Chinese)
[12] 李莉,杜慧娜, 李涛. 基于群签名与属性加密的区块链可监管隐私保护方案[J]. 计算机工程, 2022, 48(6): 132-138.
LI L, DU H N, LI T. Blockchain supervisable privacy protection scheme based on group signature and attribute encryption[J]. Computer Engineering, 2022, 48(6): 132-138. (in Chinese)
[13] NAMASUDRA S, SHARMA P, CRESPO R G, et al. Blockchain-based medical certificate generation and verification for IoT-based healthcare systems [J]. IEEE Consumer Electronics Magazine, 2023, 12(2): 83-93.
[14] XI P, ZHANG X L, WANG L, et al. A review of blockchain-based secure sharing of healthcare data [J]. Applied Sciences, 2022, 12(15): 7912.
[15] HINTEREGGER A, HASLHOFER B. An empirical analysis of Monero cross-chain traceability[EB/OL]. [2023-01-03]. https://arxiv.org/pdf/1812.02808.
[16] SU S, WANG K, KIM H S. Smartsupply: smart contract based validation for supply chain blockchain[C]//Proceedings of IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data. Washington D. C., USA: IEEE Press, 2018: 988-993.
[17] 邹均,张海宁, 唐屹, 等. 区块链技术指南[M]. 北京: 机械工业出版社, 2016.
ZOU J, ZHANG H N, TANG Y, et al. Blockchain technical guide[M]. Beijing: China Machine Press, 2016. (in Chinese)
[18] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.
[19] BONEH D, BOYEN X, SHACHAM H. Short group signatures[M]. Berlin, Germany: Springer, 2004.
[20] PEDERSEN T P. Non-interactive and information-theoretic secure verifiable secret sharing [M]. Berlin, Germany: Springer, 2007.
[21] BUNZ B, BOOTLE J, BONEH D, et al. Bulletproofs: short proofs for confidential transactions and more[C]//Proceedings of IEEE Symposium on Security and Privacy. San Francisco, USA: IEEE Press, 2018: 315-334.
[22] GENNARO R, GOLDFEDER S. Fast multiparty threshold ECDSA with fast trustless setup[C]// Proceedings of 2018 ACM SIGSAC Conference on Computer and Communications Security. New York, USA: ACM Press, 2018: 1179-1194.
[23] GENNARO R, GOLDFEDER S. One round threshold ECDSA with identifiable abort [EB/OL]. [2023-01-03]. https://eprint.iacr.org/2020/540.pdf.
[24] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[M]. Berlin, Germany: Springer, 2007.
[25] DEVIDAS S, SUBBA RAO Y V, REKHA N R. A decentralized group signature scheme for privacy protection in a blockchain [J]. International Journal of Applied Mathematics and Computer Science, 2021, 31(2): 353-364.

编辑 索书志