基于区块链与CP-ABE的可验证分布式密钥生成协议

彭长根[1),2)] 龙洋洋[1)] 陈玉玲[1)]

[1)](贵州大学省部共建公共大数据国家重点实验室 贵阳 550025)

[2)](贵州大学贵州省大数据产业发展应用研究院 贵阳 550025)

摘 要 分布式密钥生成(DKG)协议作为一种重要的密码学工具,它允许多个参与者共同协作生成一对额外的公私钥,而无需任何一方完全了解密钥的完整信息。由于DKG协议中的每个参与者仅持有其自身密钥份额,完整的密钥只有通过多个参与者协作时才能被重构出来,DKG协议能有效降低密钥泄露的风险。然而,现有分布式密钥生成(DKG)协议大多基于公开可验证秘密共享(PVSS)方案进行设计,协议的共享阶段和重构阶段至少各需要两轮交互,DKG协议的计算复杂度和通信复杂度较高,通常为$O(n^2)$,这在大规模分布式系统中可能成为性能瓶颈。密文策略属性加密(CP-ABE)因其支持密文从外部解密的特性备受关注,且区块链技术的兴起为DKG协议的安全性和透明性提供了新的解决方案。本文利用区块链作为公开信道、CP-ABE作为密码原语,提出基于区块链的一轮可验证DKG协议,旨在通过结合区块链技术和CP-ABE来优化传统DKG协议的性能和安全性。该协议仅需一轮交互即可完成密钥共享和重构。具体来说,该协议利用区块链作为公开信道,确保密钥生成过程的透明性和可追溯性,同时借助CP-ABE的特性,确保外部用户能对重构的密钥进行验证。在密文共享阶段,协议引入了通用哈希承诺机制,通过将承诺种子作为输入对CP-ABE的加密算法进行改进。同时,协议利用智能合约对DKG协议的子公钥进行有效性检查,验证复杂度为$O(1)$。在重构阶段,外部用户可通过智能合约获取参与节点提交的密钥份额密文和DKG协议子公钥,仅需$O(n)$的计算复杂度和通信复杂度,就能重构协议主私钥。安全性分析及实验分析表明,所提DKG协议需较低的计算、通信开销,且满足可验证性、有效性、保密性及鲁棒性等安全属性。

关键词 分布式密钥生成;属性加密;区块链;密钥管理;承诺

中图法分类号 TP309 **DOI号** 10.11897/SP.J.1016.2025.01342

Verifiable Distributed Key Generation Using Blockchain and CP-ABE

PENG Chang-Gen[1),2)] LONG Yang-Yang[1)] CHEN Yu-Ling[1)]

[1)](State Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025)

[2)](Guizhou Big Data Academy, Guizhou University, Guiyang 550025)

Abstract Distributed Key Generation (DKG) protocol, as an important cryptographic tool that allows multiple participants to collaborate together to generate a pair of additional public and private keys without the need for any party to have full knowledge of the complete information of the keys, has been widely used in the fields of multi-party computation, distributed systems, and privacy protection. Since each participant in the DKG protocol holds only its own key share, and the complete key can only be reconstructed through the collaboration of multiple participants, the DKG protocol effectively reduces the risk of key leakage and enhances system reliability and

收稿日期:2024-10-15;在线发布日期:2025-03-14。本课题得到国家重点研发计划(2022YFB2701400)和国家自然科学基金(62272124)资助。**彭长根**,博士,教授,中国计算机学会(CCF)杰出会员,主要研究领域为信息安全与密码学、区块链、安全计算。E-mail:cgpeng@gzu.edu.cn。**龙洋洋**(通信作者),博士研究生,中国计算机学会(CCF)学生会员,主要研究领域为区块链、大数据安全与隐私保护。E-mail:yylong2020@yeah.net。**陈玉玲**,博士,教授,中国计算机学会(CCF)专业会员,教育部青年长江学者,主要研究领域为大数据、安全系统和信息安全。

security. However, most existing DKG protocols are designed based on the Publicly Verifiable Secret Sharing (PVSS) scheme. The sharing and reconstruction phases each require at least two rounds of interaction, resulting in high computational and communication complexity for the DKG protocol, that is, $O(n^2)$. This can become a performance bottleneck in large-scale distributed systems. Therefore, exploring new methods to optimize the performance of DKG protocols and enhance their security remains an urgent issue to be addressed. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has garnered widespread attention as an emerging cryptographic technology due to its ability to support decryption of ciphertext from external sources. Meanwhile, the rise of blockchain technology has provided decentralized, immutable, and traceable characteristics for distributed systems, offering new solutions for the security and transparency of DKG protocols. This paper proposes a blockchain-based one-round verifiable DKG protocol, utilizing blockchain as a public channel and CP-ABE as a cryptographic primitive. The goal is to optimize the performance and security of traditional DKG protocols by combining blockchain technology and CP-ABE. This protocol completes key sharing and reconstruction in just one round of interaction. Specifically, the protocol leverages blockchain as a public channel to ensure the transparency and traceability of the key generation process. At the same time, it relies on the characteristics of CP-ABE to enable external users to verify the reconstructed key. In the ciphertext-sharing phase, the protocol introduces a universal hash commitment mechanism, which improves the CP-ABE encryption algorithm by using the commitment seed as input. The protocol also utilizes smart contracts to verify the validity of the sub-public keys of the DKG protocol, with a verification complexity of $O(1)$. In the reconstruction phase, external users can obtain the ciphertext of the key shares submitted by participating nodes and the sub-public keys of the DKG protocol through smart contracts. They can then reconstruct the main private key of the protocol with only $O(n)$ computational and communication complexity. Security and experimental analyses demonstrate that the proposed DKG protocol requires lower computational and communication overhead and satisfies security attributes such as verifiability, validity, confidentiality, and robustness. This provides a more efficient and secure solution for key management in multi-party computation. The proposed one-round verifiable DKG protocol based on blockchain and CP-ABE offers a novel approach to overcoming the challenges faced by existing DKG protocols. Its innovative use of blockchain as a public channel and CP-ABE as a cryptographic primitive sets a new standard for secure and efficient key generation in distributed systems.

Keywords distribute key generation; attribute-based encryption; blockchain; key management; commitment

1 引 言

分布式密钥生成(Distributed Key Generation，DKG)协议作为众多密钥管理系统[1]的核心组件，它允许一组节点在无可信第三方的环境下，协作生成一个共享密钥。在共享密钥生成的过程中，由于参与节点都独立生成其自身的密钥份额，攻击者无法在未持有其他参与者的份额的情况下单独推导出共享密钥，能有效避免各种阈值密码系统(如阈值加密[2]、阈值签名[3]、通用阈值硬币[4]等)中的可信设置，可作为构建区块链、共识协议的基本模块。考虑到DKG协议在实际应用(如海上运输系统[5]、工业物联网[6]等)中的广泛性，迫切需要开发更高效的DKG协议。

可验证秘密共享(Verifiable Secret Sharing，VSS)[7]和公开可验证秘密共享(Public Verifiable secret Sharing，PVSS)[8]被广泛用于实现DKG协议。VSS通过为份额附加非交互式零知识证明来确保参与节点能够验证其收到的份额[9]。然而，由

于份额均通过私有信道传输，节点可能会在共享阶段发送不正确的份额以发起DoS攻击。PVSS整合了额外的公开密钥加密方案，使份额可以加密和公开验证，即通过PVSS能在公开信道构建DKG协议。然而，在基于PVSS的DKG协议中，加密份额仅能由持有对应份额的用户解密，当外部用户发起重构时，会带来严重的计算成本和通信开销。因此，寻求更有效的方法以减少通信轮数以及降低参与者在验证和处理共享密钥时的计算负担和通信开销，仍然是一项挑战。

密文策略属性加密（Cipher-Policy Attribute-Based Encryption，CP-ABE）[10]允许用户根据特定的属性来加密数据，能实现对密文的外部解密，被广泛应用于需要对数据进行细粒度访问控制的环境，如云计算[11-12]、医疗健康[13]、金融服务[14]等。尽管PVSS和CP-ABE都能让每个参与节点在与多个参与者交互的过程隐藏其秘密份额，并进行公开验证和阈值恢复。但由于CP-ABE具有外部解密的特性（即外部用户可以解密密文），这为设计具有高效重构阶段的DKG协议提供了创新的解决策略。然而，在传统的CP-ABE中，由于解密权限由具有相同属性的多个用户共享，因此在给定公开的密钥时，很难识别原始密钥所有者。这使得恶意用户有机会泄露他们的数据以谋取收益，严重损害了数据安全性。此外，现有的CP-ABE访问控制方案大多存在信任建立成本高、单点故障等问题。因此，如何结合CP-ABE设计高效的DKG协议仍然是亟待解决的挑战。

区块链[15]是一种分布式账本技术，它以去中心化的方式存储数据，每个区块中均包含一系列的交易记录，并通过哈希与前一个区块相连。区块链网络中的节点通过共识算法（如工作量证明[16]、权益证明[17]等）达成一致，使得交易记录具有不可篡改性和透明性，可作为公开信道的具体实现，为分布式系统提供安全、去中心化的密钥管理。在区块链网络中，节点可通过DKG协议分布式地生成和管理用于数据保护和访问控制的共享密钥，克服了单点故障以及单个节点不可信任的问题。此外，凭借其不可篡改性和透明性，区块链能为DKG协议提供可验证环境以确保共享密钥生成过程的透明和可追溯。然而，在区块链上实现DKG协议，需要节点独立生成自身加密份额对应的公共验证参数，并通过智能合约广播给其他节点，其他节点仍需通过公共验证参数对加密份额进行验证，验证复杂度为$O(n)$，验证开销较大。因此，寻求更有效的方法降低参与者在验证加密份额时的计算负担和通信开销，仍然是一项挑战。

针对上述问题，本文聚焦于分布式共享密钥的生成，提出基于区块链和CP-ABE的一轮可验证DKG协议，即共享阶段和重构阶段仅需一轮就可以生成共享密钥。具体贡献包括：

（1）在共享阶段，引入通用的哈希承诺算法，将承诺种子作为输入对原始CP-ABE加密算法进行改进，并通过智能合约对DKG协议子公钥进行有效性检查，验证复杂度为$O(1)$。

（2）在重构阶段，外部用户可通过智能合约获取诚实的参与节点调用改进的CP-ABE加密算法生成的密钥份额密文和DKG协议子公钥，并基于本地的份额计算DKG协议的共享密钥，仅需$O(n)$的通信和计算复杂度。

（3）安全性分析表明所提DKG协议满足可验证性、有效性、保密性及鲁棒性等安全属性。性能分析表明所提DKG协议与现有方案对比，在加解密和存储方面均有更高的效率，为可验证解密提供防篡改性。

本文的其余部分组织如下：第2节讨论相关研究；第3节介绍本研究的相关概念；第4节给出协议模型和定义；第5节给出具体构建；第6节讨论协议正确性和安全性；第7节评估性能；第8部分对本文总结。

2 相关研究

VSS是确保DKG协议的完整性和保密性的解决方案之一。自Pedersen等人[18]首次提出DKG原型（Joint-Feldman DKG）以来，Tomescu等人[19]将可验证秘密共享和DKG协议整合至阈值签名方案。该方案在聚合阈值特征时，采用高效的多点多项式求值算法，加快拉格朗日系数的计算速度，可支持大规模参与者进行签名。然而，该方案依赖于可信中心的设置，仅专注于同步VSS和DKG协议，没有解决DKG中最坏情况下的投诉开销，并且在参与者不诚实的情况下，仍然有较高的开销。Kokoris-Kogias等人[20]基于异步可验证秘密共享，提出了首个异步分布式密钥生成协议。该协议能够生成具有双阈值$(f,f+1)$的分布式密钥，需要$O(f)$，其中f是错误方的数量。Gao等人[21]设计了复杂度为$O(n^3)$的常

数轮A-DKG协议，并将其应用于高效验证异步拜占庭协议。该协议构建了一个高效的领导者选举机制，且整个过程中仅依赖于公钥基础设施的配置。Fouque等人[22]在公共信道上构建了首个基于PVSS的一轮DKG协议，该协议在同步网络模型下，使用Paillier密码系统[23]作为底层公钥加密方案以确保密钥份额的可验证性，并确保共享阶段的安全性。其基本思想是，组中的每一方都运行一个PVSS协议，以便任意参与节点在达到阈值条件时能够恢复所有秘密，即使存在恶意的秘密份额，对这些秘密份额进行求和，也能构造主密钥。Gennaro等人[24]针对Joint-Feldman DKG协议容易受到恶意攻击，会导致创建的DKG主公钥在密钥空间上产生偏差这一问题，将共享阶段分为两部分来防止偏差，诚实参与节点在第一部分被定义合格的参与节点，DKG主公钥在第二部分进行计算。Neji等人[25]使用对称密钥加密份额，对Joint-Feldman DKG协议进行扩展，该协议使用以太坊平台作为公开信道、智能合约来处理争议。具体来说，该协议使用对称密钥对份额进行加密，对称密钥由发送者自己的私钥和每个接收者的公钥计算，这实际上是一个Diffie-Hellman密钥交换协议。Schindler等人[26]利用智能合约作为通信媒介来动态定义参与实体的集合，激励参与并惩罚恶意攻击行为，提出了基于区块链的分布式密钥生成协议。然而，Neji等人[25]和Schindler等人[26]协议都只是基于离散对数加密系统的实现，仅提供了一个可公开验证的投诉管理，并没有消除争议，因为加密的份额不可公开验证。

为确保各参与节点在解密份额密文后可对份额的有效性进行验证，Lai等人[27]通过将消息承诺与密文绑定，提出了第一个可验证的CP-ABE方案。在该方案中，为了生成这样的消息承诺，需要通过添加一些冗余组件将密文的大小增加到原始密文的两倍。为了减小文献[27]中密文的大小，提高消息承诺的生成效率，Mao等人[28]基于哈希的消息承诺，提出了不向密文中添加冗余成分的可验证CP-ABE方案。然而，在该方案中，只有拥有可信权威机构颁发的密钥的参与者才能生成对密文的消息承诺，不适用于DKG协议的构造。Zhang等人[29]基于非交互式零知识证明技术，提出了首个基于去中心化CP-ABE的DKG协议，该协议使用复杂度为$O(1)$的解密密钥来解密密文，在共享阶段的计算复杂度为$O(n)$、通信复杂度为$O(n)$、验证复杂度为$O(n^2)$，在重构阶段的计算复杂度为$O(n^2)$、通信复杂度为$O(n)$。然而，在该协议中，由于智能合约需要采用复杂的椭圆曲线和双线性配对加密技术对CP-ABE密文进行验证，存在通信和计算成本高的问题。因此，基于区块链和CP-ABE技术，构建具有低通信复杂度、低延迟、高重构能力的一轮可验证DKG协议仍是亟待解决的挑战。

3　基础知识

3.1　双线性映射及复杂性假设

3.1.1　双线性映射

设G_1、G_2和G_T是三个素数阶的循环群，设g_1，g_2分别是G_1和G_2的生成元，并且$e: G_1 \times G_2 \to G_T$是一个双线性映射，具有以下性质：

(1)双线性：对$\forall \mu \in G_1, \upsilon \in G_2$以及$a, b \in Z_p$有$e(\mu^a, \upsilon^b) = e(\mu, \upsilon)^{ab}$；

(2)非退化性：$e(g_1, g_2) \neq 1$；

(3)可计算性：G_T中的群运算和双线性映射e是可有效计算的。

3.1.2　复杂性假设

双线性映射的安全性是通过$\mathbb{G}$，$\mathbb{H}$和$\mathbb{G}_T$中离散对数问题(Discrete logarithm problem，DLP)的难度来评估的。令$y=(\mathbb{G}, \mathbb{H}, g, h, q, e: \mathbb{G} \times \mathbb{H} \to \mathbb{G}_T)$，没有多项式时间(Probabilistic polynomial-time，PPT)的敌手$\mathcal{A}$能通过给定的$g, g^x \in \mathbb{G}$和h，$h^x \in \mathbb{H}$以不可忽略的概率μ计算出$x \in \mathbb{Z}_p$，即$\Pr[A(g, g^x, h, h^x) = x | x \in \mathbb{Z}_p, g \in \mathbb{G}, h \in \mathbb{H}] \leqslant \mu$.

3.2　承诺机制

作为密码学中基本原语之一，承诺机制[30]通常由发送方和存储方之间的一对多项式时间算法(承诺、揭露)组成的两阶段加密协议：

(1)承诺阶段，发送方发送一个封闭的信封$\hat{c} = commit(m, r)$，其中包含消息m和随机值r；

(2)揭露阶段，发送方向接收方揭示(m, r)，接收方可以调用算法$verify(m, r, \hat{c}) \stackrel{?}{=} m$验证$m$和$r$。

3.3　密文策略属性加密

传统CP-ABE[10]包括4个多项式时间算法：

(1)$(TK, mk) \leftarrow Setup(\lambda)$：输入安全参数$\lambda$并输出全局参数$TK$和主密钥$mk$。

(2)$SK \leftarrow AttrKeyGen(mk, S)$：该算法输入属性集$S$和主密钥$mk$，并为属性集$S$生成对应的属性私钥$SK$。

(3)$C \leftarrow Encrypt(M, \mathbb{A}, TK)$:该算法输入消息$M$,访问结构$\mathbb{A}$,公共参数$TK$,输出密文$C$。

(4)$M \leftarrow Decrypt(TK, C, SK)$:该算法输入公共参数$TK$、密文$C$和一组属性$S$对应的私钥$SK$。若属性集$S$满足访问结构$\mathbb{A}$,则解密$C$并返回消息$M$。

3.4 区块链与智能合约

区块链平台,如以太坊,集成了智能合约执行引擎,允许开发者编写和部署自动执行的合约,这些合约一旦部署,就可以在满足预设条件时自动执行。以太坊作为一个无需许可的区块链平台,它不仅支持加密货币交易,还允许通过身份验证的用户存储数据,执行智能合约和去中心化应用,数据一旦上链,就具有防篡改的特性。以太坊虚拟机提供了图灵完备的执行环境,确保智能合约的有效运行。智能合约通常使用Solidity编程语言编写,合约一旦部署到区块链,就可以执行复杂的逻辑和操作,且所有操作均可公开验证。为防止恶意用户滥用资源,以太坊虚拟机通过Gas机制来限制计算和存储的开销,即交易调用者必须支付一定的费用。

4 系统模型及安全模型

4.1 符号说明

本文所涉及的符号说明如表1所示。

4.2 系统模型

所提DKG协议的系统模型由可信授权中心(TA)、参与节点和智能合约组成:

表1 系统参数

参数	含义
γ	将$\mathbb{G}_T$中的元素映射为$\mathbb{Z}_p$上的元素
e	从$\mathbb{G}\times\mathbb{H}\rightarrow\mathbb{G}_T$的双线性映射
h	$\mathbb{G}$上的生成元
$H_{\mathbb{H}}$	将属性通过哈希函数映射到密钥
S_r	随机值
P_θ	参与节点
$PK_{\Gamma,\theta}$	协议子公钥
$SK_{\Gamma,\theta}$	协议子公钥对应的私钥
MPK	协议主公钥
MSK	协议主公钥对应的主私钥
C_θ	CP-ABE密文
Com_θ	参与节点的承诺
(pk_i, sk_i)	参与节点P_i的公私钥对
TK	全局参数
mk	主密钥
S	属性集
Q	诚实的参与节点集合

(1) TA:负责初始化系统参数,为参与节点生成公私钥,并在以太坊区块链网络部署合约,不参与DKG协议密钥的生成过程。

(2) 参与节点:DKG协议的参与者,可以通过智能合约上传解密密钥和密文。

(3) 智能合约:全局函数,负责提供密文和协议子公钥的有效性验证和其他操作逻辑。

4.3 安全模型

如文献[30]所示,CP-ABE的可验证安全模型可被定义为挑战者$\mathcal{B}$和敌手$\mathcal{A}$之间的安全游戏,具体如下:

初始化:$\mathcal{B}$执行$Setup$算法生成密钥对(TK, mk),然后将TK发送给$\mathcal{A}$。

查询:敌手$\mathcal{A}$可做如下查询:

(1) 公钥查询:$\mathcal{A}$从$\mathcal{B}$处查询参与节点P_i的公钥pk_i。$\mathcal{B}$在查询列表中添加pk_i。

(2) 私钥查询:$\mathcal{A}$从$\mathcal{B}$处查询参与节点P_i的私钥sk_i。如果公钥pk_i在查询列表中,则$\mathcal{B}$向$\mathcal{A}$返回对应的私钥sk_i,并将sk_i添加在查询列表中。如果相应的pk_i不在查询列表中,则$\mathcal{B}$生成并返回公私钥对(pk_i, sk_i)给$\mathcal{A}$并将(pk_i, sk_i)添加到查询列表。

(3) 解密密钥查询:$\mathcal{A}$将属性集S_i发送给$\mathcal{B}$用于该查询。$\mathcal{B}$运行$AttrKeyGen(mk, S_i)\rightarrow K_i$提取参与节点的属性私钥,并将其发送给敌手$\mathcal{A}$。

(4) 辅助参数查询:$\mathcal{A}$可以向$\mathcal{B}$查询CT_{fp}及其对应的秘密参数s_i。

(5) 密文查询:在该查询中,敌手$\mathcal{A}$向B提交$\left((M_{l\times n}, \rho)_i, m_i \in G_T, pk_i, CT_{fpi}\right)$,$\mathcal{B}$模拟并返回密文$CT_i$。

输出:敌手$\mathcal{A}$向挑战者$\mathcal{B}$输出元组$\left(CT^*_{fp}, K^*\right)$,如果以下条件满足,则敌手$\mathcal{A}$赢得游戏:

$$\begin{aligned}\mathcal{A}\quad &\text{wins} = Decrypt(C^*, K^*) = m^* \\ &\wedge m^* \notin \{m_i\}_{i\in ql} \\ &\wedge CT^*_{fp} \in \{CT_{fpi}\}_{i\in ql}\end{aligned} \tag{1}$$

其中,ql为查询列表。

定义1. 如果对于所有多项式时间(PPT)的敌手$\mathcal{A}$,其在上述可验证性游戏中获胜的优势可忽略不计,则该CP-ABE方案满足可验证性。

在共享阶段,诚实的参与节点集合定义为Q,攻击者可通过向公共信道提交任意消息来计算MPK,

也可能会发起DoS攻击，偏离或中止协议。假设在协议中至多存在f个恶意的参与节点，即最坏的情况是f个恶意的参与节点私下相互勾结。也就是说，若攻击者控制了f个参与节点，则攻击者可以根据诚实的行为做出适应性的行为，包括发起快速攻击。为了保证可用性，诚实的参与节点应该多于腐败的一方，即$f<n/2$。在重构阶段，阈值设置为$t=n/2+1$，即只要有t个诚实的参与节点，则可重构出DKG协议的私钥。共享阶段和重构阶段的对手可以是不同的集合，这意味着所提DKG协议除CP-ABE的可验证性之外，还应该满足有效性、保密性及鲁棒性安全属性。具体如下：

（1）有效性：如果满足以下条件，DKG协议是有效的：①所有诚实的参与节点能重构DKG协议的私钥MSK；②所有诚实的参与节点都持有相同的协议公钥$MPK=h^{MSK}$，其中h是群$\mathbb{H}$的生成元。

（2）保密性：协议私钥MSK对任何人或任何共谋团体都是保密的。

（3）鲁棒性：即使有f个恶意方，任何n个诚实的参与节点也能有效地计算出协议主私钥MSK。

定义2.　所提DKG协议由n个参与节点组成，定义为$\mathbb{P}=\{P_1,P_2,\cdots,P_n\}$，以及一个智能合约，应满足有效性、保密性及鲁棒性安全属性。各参与节点共同生成公私钥对(MPK,MSK)，MPK在共享阶段产生，MSK由诚实的参与者在重构阶段恢复。

5　具体构造

5.1　概　述

如图1所示，所提DKG协议由初始化阶段、密文共享阶段和重构阶段组成。各阶段交互流程概述如下：

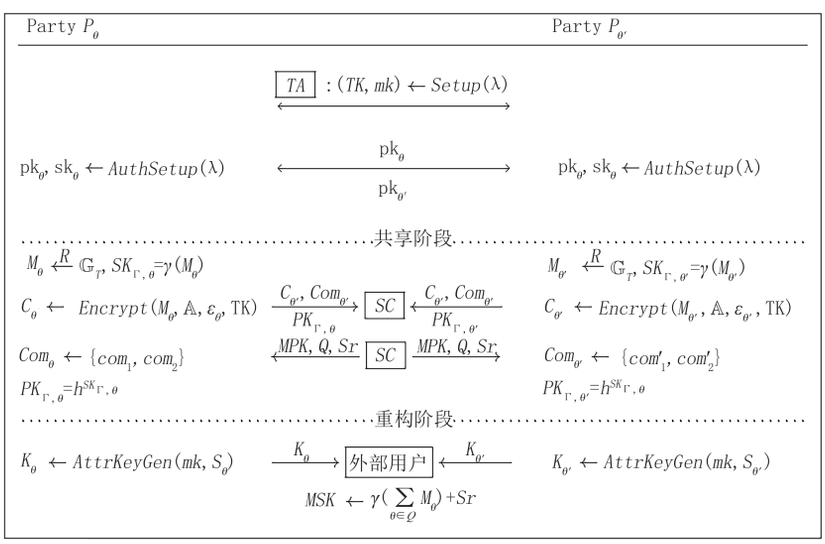

图1　概述示意图

（1）初始化阶段：①TA调用$Setup$算法输出全局参数TK和mk；②参与节点P_θ调用$AuthSetup$算法生成其长期私钥$sk_\theta=d_\theta$和公钥$pk_\theta=h^{d_\theta}$。

（2）密文共享阶段：①P_θ随机选择一个秘密M_θ，使用改进的CP-ABE加密算法对其进行加密，得到密文C_θ；②P_θ计算协议子公钥$PK_{\Gamma,\theta}=h^{SK_{\Gamma,\theta}}$，其中$SK_{\Gamma,\theta}=\gamma(M_\theta)$和$\gamma$是函数$\gamma: G_T\rightarrow Z_p$；③$P_\theta$计算承诺$Com_\theta$，并向合约发送元组$(PK_{\Gamma,\theta}, C_\theta, Com_\theta)$；④当合约收到元组$(PK_{\Gamma,\theta}, C_\theta, Com_\theta)$时，自动检查元组是否有效，若有效，$P_\theta$则被认为是诚实的参与节点。一旦超时事件触发或收到所有参与节点提交的元组，合约自动计算协议主公钥$MPK=\prod_{\theta\in Q} PK_{\Gamma,\theta}\cdot h^{S_r}$，任意外部用户均可发起重构。其中，$S_r$用于避免恶意攻击的一个随机值。注意：智能合约初始化时设定了全局时间参数Δ_τ，在有效时间内，参与节点可向合约多次提交元组，但在计算过程中只使用最后一次提交的内容。

（3）重构阶段：一旦任意外部用户发起重构请求，①合约返回元组集合$\{(PK_{\Gamma,\theta}, C_\theta)\}_{\theta\in Q}$，并向所有参与节点广播外部用户的地址；②$P_\theta$向TA提交属性信息，由TA调用$AttrKeyGen$算法生成$C_\theta$对应的解密密钥$K_\theta$，并将其离线发送给外部用户；③若外

部用户收到至少t个解密密钥，就可以解密对应的密文，并基于其份额计算DKG协议主私钥$MSK=\sum_{\theta\in Q}(SK_\theta+S_r)$。

5.2 智能合约设计

如图2所示，在所提DKG协议中，合约涉及5个算法，包括*Constructor*算法、*Join*算法、*Check*算法，*GenMPK*算法和*getCredentials*算法。其中，*Constructor*算法是部署合约时自动执行的构造函数，*Join*算法由P_θ调用提交密文组件和承诺信息，*Check*算法由合约自动执行来验证P_θ提交的密文组件和承诺，*GenMPK*算法由合约在有效时间到达后自动执行以计算协议主公钥*MPK*，*getCredentials*算法由外部用户调用以获取*MPK*和其他必要的凭据来计算协议主私钥*MSK*。

```
Algorithm 1: 合约算法
  //合约初始化.
1 Function CONSTRUCTOR()
2 |  struct Party { addr; C; PK_r; proof; }
3 |  S_r = ξ_r; Party[]ps, Q; Party p;
4 end
  //参与节点P_θ提交C_θ, PK_r,θ, Com_θ.
5 Function JOIN(C_θ, PK_r,θ, Com_θ)
6 |  p.C=C_θ; p.PK_r=PK_r,θ; p.proof = Com_θ;
7 |  if Check(PK_r,θ, Com_θ) = true then
8 |  |  Q.push(p);
9 |  end
10 end
  // 验证 PK_r,θ.
11 Function CHECK(PK_r,θ, Com_θ)
12 |  if com_1 = hash(CT_fp, pk_θ, h^com2 · (CT_fp·pk_θ)^-com1, PK_r,θ) then
13 |  |  return true;
14 |  end
15 end
  // 计算并返回 MPK.
16 Function GENMPK(Q, S_r)
17 |  return MPK = Π_θ∈Q PK_θ · h^Sr;
18 end
  // 凭证提取.
19 Function GETCREDENTIALS()
20 |  MPK = GenMPK(Q, S_r)
21 |  return {MPK, S_r, Q};
22 end
```

图2 智能合约设计

5.3 CP-ABE算法构建

不同于传统CP-ABE机制[10]，本文将可验证哈希承诺引入CP-ABE加密算法，以确保参与节点能验证解密数据的准确性。改进的方案包括以下4个多项式时间算法：

(1) $(TK,mk)\leftarrow Setup(\lambda)$：TA输入安全参数$\lambda$，调用该算法输出全局参数$TK$和$mk$。

(2) $K_\theta\leftarrow AttrKeyGen(mk,S_\theta)$：该算法输入一组属性$S_\theta$和主密钥$mk$，并为属性集$S_\theta$生成对应的属性私钥$K_\theta$。

(3) $C_\theta\leftarrow Encrypt(M_\theta,\mathbb{A},\varepsilon_\theta,TK)$：该算法输入消息$M_\theta$、访问结构$\mathbb{A}$、公共参数$TK$和辅助参数$\varepsilon_\theta$，输出密文$C_\theta$。

(4) $M_\theta\leftarrow Decrypt(TK,C_\theta,K_\theta)$：该算法输入全局参数$TK$、密文$C$和一组属性$S_\theta$的私钥$K_\theta$。如果属性集合$S_\theta$满足访问结构$\mathbb{A}$，则解密密文$C_\theta$并返回消息$M_\theta$。

5.4 DKG协议构造

所提DKG协议包含一个参与节点为n集合，记为$\mathbb{P}=\{P_1,P_2,\cdots,P_n\}$。

5.4.1 初始化阶段

TA调用*Setup*算法输出全局参数TK和mk。具体来说，首先选取阶为q的循环群$\mathbb{G}$和$\mathbb{H}$；其次选取g为$\mathbb{G}$的生成元、h为$\mathbb{H}$的生成元、双线性映射e：$\mathbb{G}\times\mathbb{H}\rightarrow\mathbb{G}_T$和抗碰撞哈希函数：$hash:\{0,1\}^*\times\mathbb{H}\times\mathbb{H}\times\mathbb{H}\rightarrow\mathbb{Z}_p$，$H:\{0,1\}^*\times\mathbb{H}\times\mathbb{H}\rightarrow\mathbb{Z}_p$，$H_{\mathbb{H}}:\{0,1\}^*\rightarrow\mathbb{H}$；最后，选择随机值$\alpha,b\in\mathbb{Z}_p$，计算主密钥$mk=g^\alpha$，并向所有参与节点发布全局参数$TK=\left(e(g,h)^\alpha,h^b,H,H_{\mathbb{H}},e,\mathbb{G},\mathbb{H},g,h\right)$。

参与节点P_θ调用*AuthSetup*算法生成其长期私钥$sk_\theta=d_\theta$和公钥$pk_\theta=h^{d_\theta}$。

5.4.2 密文共享阶段

在共享阶段，参与节点P_θ首先选择随机值$s\leftarrow Z_p$，使用其私钥计算辅助参数$\varepsilon_\theta=s+sk_\theta$和$CT_{fp}=h^s$。然后，$P_\theta$调用*Encrypt*算法计算密文组件。不同于Waters协议的加密算法，本文将承诺引入加密算法以确保外部用户也可以检查CP-ABE密文的有效性，该算法输入消息M_θ，访问控制策略$\mathbb{A}$，公共参数TK，并输出一个密文C_θ，具体如下：

$$\begin{aligned}M_\theta &\leftarrow\mathbb{G}_T\\ C_\theta &\leftarrow Encrypt(M_\theta,\mathbb{A},\varepsilon_\theta,TK)\end{aligned}\tag{2}$$

即P_θ从$\mathbb{G}_T$中随机选择一个值M_θ，并对M_θ进行加密，生成密文组件C_θ。对于任意$\mathbb{A}=(\boldsymbol{A}_{l\times n},\rho)$，$\boldsymbol{A}_{l\times n}$中的每一行$i$对应一个属性$\rho(i)$，$P_\theta$随机选择$\vec{v}=(\varepsilon_\theta,\zeta_1,\zeta_2,\cdots,\zeta_{n-1})\in\mathbb{Z}_p$并计算共享向量$\lambda_i=\vec{v}\cdot\boldsymbol{A}_i$，

其中$\boldsymbol{A}_i$是$\boldsymbol{A}$的第i行。然后，P_θ随机选择$\{r_1, r_2, \cdots, r_l\}\in\mathbb{Z}_p$并计算密文$C_\theta$：

$$C_\theta=\begin{cases}C_0=M_\theta\cdot e(g,h)^{\alpha\cdot\varepsilon_\theta}\\ \{C_{i,1}=h^{b\lambda_i}H(\rho(i))^{-r_i},\\ C_{i,2}=g^{r_i}\}_{i\in[l]}\end{cases}\tag{3}$$

随后，P_θ计算DKG协议子公钥$PK_{\Gamma,\theta}$：

$$PK_{\Gamma,\theta}=h^{\gamma(M_\theta)}\tag{4}$$

此外，为了验证$PK_{\Gamma,\theta}$的有效性，参与节点P_θ选择随机值$\varphi\leftarrow Z_p$，使用其公钥pk_θ、辅助参数ε_θ和CT_{fp}作为输入提取并导出对协议子公钥$PK_{\Gamma,\theta}$的哈希承诺Com_θ，如下所示：

$$\begin{aligned}&Com_\theta\leftarrow ComGen(CT_{fp}, pk_\theta, \varepsilon_\theta, PK_{\Gamma,\theta})\\ &Com_\theta=\{com_1=hash(CT_{fp}, pk_\theta, h^\varphi, PK_{\Gamma,\theta}),\\ &\qquad com_2=\varphi+\varepsilon_\theta\cdot com_1\}\end{aligned}\tag{5}$$

最后，P_θ将元组$(C_\theta, PK_{\Gamma,\theta}, Com_\theta)$发送给合约$SC$，这表明$P_\theta$向合约承诺$PK_{\Gamma,\theta}$有效。

当合约SC收到元组$(C_\theta, PK_{\Gamma,\theta}, Com_\theta)$后，自动调用$Check$算法检查$Com_\theta$的正确性和有效性，如下所示：

$$\begin{aligned}&True/False\leftarrow Check(CT_{fp}, pk_\theta, Com_\theta, PK_{\Gamma,\theta})\\ &com_1=hash(CT_{fp}, pk_\theta, h^{com_2}\cdot(CT_{fp}\cdot pk_\theta)^{-com_1}, PK_{\Gamma,\theta})\end{aligned}\tag{6}$$

通过验证的节点将被追加到集合Q中。

一旦各参与节点在时限Δ_τ内都提交了各自的密文和承诺或超时事件发生，外部用户可以调用合约SC中的$getCredentials$算法来获得DKG协议的主公钥MPK，其计算公式如下：

$$MPK\leftarrow\prod_{\theta\in Q}PK_{\Gamma,\theta}\cdot h^{S_r}=\prod_{\theta\in Q}h^{\gamma(M_\theta)}h^{S_r}\tag{7}$$

5.4.3　MSK重构阶段

在重构阶段，协议主私钥MSK定义如下：

$$MSK:=\sum_{\theta\in Q}\gamma(M_\theta)+S_r\tag{8}$$

由于集合Q中的每一个参与节点均为合法节点，若集合Q中的任何一个用户P_u想要恢复$\{M_\theta\}_{\theta\in Q}$，$P_u$首先向合约$SC$发起重构请求。合约收到请求后，返回密文及DKG协议子公钥元组集合$\{(PK_{\Gamma,\theta}, C_\theta)\}_{\theta\in Q}$，并向所有参与节点广播外部用户的地址。然后，$P_\theta$向TA提交密文对应的属性信息，TA调用计算复杂度为$O(1)$的$AttrKeyGen$算法生成C_θ对应的解密密钥K_θ，并将其离线发送给外部用户，具体如下：

$$\begin{aligned}&t\leftarrow\mathbb{Z}_p\\ &K_\theta\leftarrow AttrKeyGen(mk, S_\theta)\\ &\quad=\{K_1=g^\alpha g^{bt}, K_2=g^t, K_{attr_\theta}=H_{\mathbb{H}}(attr_\theta)^t{}_{attr_\theta\in S_u}\}\end{aligned}\tag{9}$$

其中$H_{\mathbb{H}}$可将属性映射到唯一的密钥中。

最后，当用户收到至少$t=[n/2]+1$个有效的解密密钥和密文时，就可以调用解密算法$M_\theta\leftarrow Decrypt(C_\theta, K_\theta)$以获得秘密值$\{M_\theta\}_{\theta\in Q}$。具体来说，针对秘密值$M_\theta$，该算法首先选择一组常数$w_i\in\mathbb{Z}_p$，使得$\sum_i w_i\boldsymbol{A}_i=(1,0,\cdots,0)$，其中$\boldsymbol{A}_i$表示$\boldsymbol{A}_{l\times n}$的第$i$行，这意味着$P_\theta$的属性满足策略$\mathbb{A}=(A_{l\times n}, \rho)$，且满足下式：

$$\sum_{i\in Q}w_i\lambda_i=\varepsilon_\theta\tag{10}$$

然后，计算F为：

$$\begin{aligned}F&=\frac{e(K_1, CT_{fp}\cdot pk_\theta)}{\prod_{i\in Q}(e(K_2, C_{i,1})e(C_{i,2}, K_{attr_i}))^{w_i}}\\ &=e(g,h)^{\alpha\varepsilon_\theta}\end{aligned}\tag{11}$$

最后，计算M_θ：

$$M_\theta=C_0/F=\frac{M_\theta\cdot e(g,h)^{\alpha\cdot\varepsilon_\theta}}{e(g,h)^{\alpha\varepsilon_\theta}}\tag{12}$$

P_u也可使用秘密值M_θ计算DKG协议子公钥$PK_{\Gamma,\theta}$，并通过合约与承诺值做进一步的对比。当P_u收到至少t个有效解密密钥$\{K_\theta\}_{\theta\in Q}$，就可以重构协议主私钥$MSK$。

$$MSK:=\gamma(\sum_{\theta\in Q}M_\theta)+S_r=\sum_{\theta\in Q}\gamma(M_\theta)+S_r\tag{13}$$

6　正确性与安全性分析

6.1　正确性分析

合约对协议子公钥$PK_{\Gamma,\theta}$进行验证主要通过式(6)完成，其正确性如下：

$$\begin{aligned}&com_1=hash(CT_{fp}, pk_\theta, h^{com_2}\cdot(CT_{fp}\cdot pk_\theta)^{-com_1},\\ &PK_{\Gamma,\theta})=hash(CT_{fp}, pk_\theta, h^{(s+sk_\theta)\cdot com_1+\varphi}\cdot h^{-(s+sk_\theta)\cdot com_1},\\ &PK_{\Gamma,\theta})=hash(CT_{fp}, pk_\theta, h^\varphi, PK_{\Gamma,\theta})\end{aligned}\tag{14}$$

CP-ABE密文C_θ的正确性主要由式(11)和式(12)决定，其正确性如下：

$$
\begin{aligned}
F &= \frac{e(K_1, CT_{fp} \cdot pk_\theta)}{\prod_{i\in Q}(e(K_2, C_{i,1})e(C_{i,2}, K_{attr_i}))^{w_i}} \\
&= \frac{e(g^\alpha g^{bt}, h^{\varepsilon_\theta})}{\prod_{i\in Q}(e(g^t, h^{b\lambda_i}H(\rho(i))^{-r_i})e(g^{r_i}, H(\rho(i))^t))^{w_i}} \\
&= \frac{e(g^\alpha g^{bt}, h^{\varepsilon_\theta})}{e(g,h)^{tb\sum_{i\in Q}\lambda_i w_i}} = \frac{e(g^\alpha g^{bt}, h^{\varepsilon_\theta})}{e(g,h)^{tb\varepsilon_\theta}} \\
&= e(g,h)^{\alpha\varepsilon_\theta}
\end{aligned} \tag{15}
$$

6.2 安全性分析

定理1. 改进的CP-ABE方案和文献[30]均基于DLP假设，若文献[30]满足CP-ABE的可验证属性，那么在改进的CP-ABE方案中，任何PPT对手在3.2节定义的可验证安全游戏中都具有可忽略的优势。

证明. 假设存在敌手$\mathcal{A}$，其拥有在多项式时间内以不可忽略的优势赢得3.2节定义的安全游戏，那么一定可以构建一个PPT算法来破解群$\mathbb{H}$中的DLP困难问题。

初始化：给定一个实例$y=(\mathbb{G}, \mathbb{H}, g, h, q, e: \mathbb{G}\times\mathbb{H}\to\mathbb{G}_T, g^d, h^d)$，挑战者$\mathcal{B}$运行*Setup*算法，将挑战参与节点$P_i$的公钥设置为$pk^*=h^d$，并将其发送给$\mathcal{A}$。

查询阶段：敌手$\mathcal{A}$可以进行以下查询：

(1) *hash*查询：$\mathcal{B}$保存*Hash*的查询列表L_H。使用$m_i\in\{0,1\}^*, R_i, F_i, PK_i\in H$作为输入。如果在哈希列表$L_H$中存在之前的响应记录，$\mathcal{B}$将该记录$\{(m_i, R_i, F_i, PK_i): h_i\}$返回给$\mathcal{A}$。否则，$\mathcal{B}$选择并返回随机值$h_i\in\mathbb{Z}_p$。然后，$\mathcal{B}$将元组$\{(m_i, R_i, F_i, PK_i): h_i\}$添加到$L_H$。

(2) 公私钥查询：$\mathcal{A}$从$\mathcal{B}$处查询参与节点P_i的公私钥。

(3) 解密密钥查询：$\mathcal{A}$将属性集S_i发送给$\mathcal{B}$用于该查询。由于$\mathcal{B}$持有主私钥，它可以运行$AttrKeyGen(mk, S_i)\to K_i$提取参与节点的属性私钥，并将其发送给敌手$\mathcal{A}$。

(4) 辅助参数查询：$\mathcal{A}$可以向$\mathcal{B}$查询CT_{fp}及其对应的秘密参数s_i。$\mathcal{B}$随机选择随机值$s_i\in\mathbb{Z}_p$，计算$CT_{fp}=h^{s_i}$，将CT_{fp}及秘密s_i返回给$\mathcal{A}$，并在查询列表中添加记录(s_i, CT_{fp})。

(5) 密文查询：在该查询中，攻击者$\mathcal{A}$向$\mathcal{B}$提交$\left((\boldsymbol{M}_{l\times n}, \rho)_i, m_i\in\mathbb{G}_T, CT_{fpi}\right)$。$\mathcal{B}$随机选择$n+1$个元素$\xi_2, \cdots, \xi_n, r_1, \cdots, r_l\in\mathbb{Z}_p$，然后构造密文为

$$
\begin{cases}
(C_0)_i = m_i \cdot e\left(g^\alpha, h^d \cdot CT_{fpi}\right), \\
\left\{(C_{k,1})_i = \left(h^d \cdot CT_{fpi}\right)^{M_{k,1}b} \cdot h^{b\sum_{j=2}^n \xi_j M_{k,1}} H(\rho(k))^{-r_k}, \right. \\
\left.(C_{k,2})_i = g^{r_k}\right\}_{k=1}^{l}
\end{cases} \tag{16}
$$

其中，

$$
\begin{aligned}
&\boldsymbol{\lambda}_k = (d+s_i)\boldsymbol{M}_{k,1} + \sum_{j=2}^n \xi_j \boldsymbol{M}_{k,1}, \\
&\begin{pmatrix}\lambda_1\\ \lambda_2\\ \vdots\\ \lambda_l\end{pmatrix} = \begin{pmatrix}M_{1,1} & \cdots & M_{1,n}\\ \vdots & \ddots & \vdots\\ M_{l,1} & \cdots & M_{l,n}\end{pmatrix} \cdot \begin{pmatrix}(d+s)\delta_i\\ \xi_2\\ \vdots\\ \xi_n\end{pmatrix} = \\
&\begin{pmatrix}M_{1,1}(d+s_i)\delta_i + \sum_{j=2}^n \xi_j M_{1,j}\\ M_{2,1}(d+s_i)\delta_i + \sum_{j=2}^n \xi_j M_{2,j}\\ \vdots\\ M_{l,1}(d+s_i)\delta_i + \sum_{j=2}^n \xi_j M_{l,j}\end{pmatrix}
\end{aligned} \tag{17}
$$

最后，$\mathcal{B}$在查询列表中记录元组(m_i, CT_{fpi}, s_i)

输出：完成这些查询后，$\mathcal{A}$向$\mathcal{B}$输出元组(CT_{fp}^*, K^*)。$\mathcal{B}$可获取$m^*=C_0^*/F^*$。因此，$\mathcal{A}$在上述游戏获胜的优势为

$$
\begin{aligned}
\Pr[\mathcal{A}\ \text{wins}] &= Decrypt(C^*, K^*) = m^* \\
&\wedge m^* \notin \{m_i\}_{i\in ql} \\
&\wedge CT_{fp}^* \in \{CT_{fpi}\}_{i\in ql}
\end{aligned} \tag{18}
$$

故改进的CP-ABE方案满足“可验证性”。

给定一个智能合约*SC*，在快速自适应对手$\mathcal{A}$下存在一个安全的DKG协议，即满足“有效性”、“保密性”、“鲁棒性”。

定理2. 如果满足以下条件，则所提DKG协议是有效的：

(1) 所有诚实的参与节点集合能计算出唯一的协议主秘钥*MSK*。

(2) 对于诚实的参与节点来说，存在一个有效的过程来计算协议主密钥*MSK*。

(3) 所有诚实的参与节点能计算出公钥$MPK=h^{MSK}$。

证明. 在密文共享阶段，$\mathcal{A}$可以通过控制f个参与节点，向合约*SC*提交无效的子公钥$PK_{\Gamma,\theta}=h^{\gamma(M_\theta)}$来偏离协议。但由于所提DKG协议使用哈希承诺

来检查参与节点所提交的元组$(C_\theta, PK_{\Gamma,\theta}, Com_\theta)$，通过验证式(7)，不诚实的参与节点将被合约$SC$检测出来，且元组$(C_\theta, PK_{\Gamma,\theta}, Com_\theta)$一旦提交至合约$SC$，任何攻击者无法篡改其内容。尽管在所提DKG协议中使用区块链作为公开信道，其存储的元组$(C_\theta, PK_{\Gamma,\theta}, Com_\theta)$以及协议主公钥$MPK$对所有节点均是公开透明的，由于离散对数假设，$\mathcal{A}$无法通过密文$C_\theta$和$PK_{\Gamma,\theta}$获取到秘密份额$M_\theta$，进一步重构协议主私钥$MSK$，这与区块链本身是开放的网络结构，不能提供安全信道并不冲突。因此，协议主密钥MSK具有唯一性，由$\sum_{\theta\in Q}\gamma(M_\theta)+S_r$所定义。当超时事件触发或收集到$n$个有效的子公钥$PK_\theta=h^{\gamma(M_\theta)}$时，合约$SC$能有效计算协议主公钥$MPK=h^{\sum_{\theta\in Q}\gamma(M_\theta)+S_r}=\prod_{\theta\in Q}h^{\gamma(M_\theta)+S_r}$。其中，$PK_\theta=h^{\gamma(M_\theta)}$和随机值$h^{S_r}$是公开的。在重构阶段，由于所有有效的密文$C_\theta$在加密算法中具有相同的阈值访问树。若收集$t=n/2+1$个诚实解密密钥$K_\theta$，外部用户可以解密$Q$中的所有密文$C_\theta$，进而重构出主私钥$MSK$。即使$Q$中的某一个参与节点在重构阶段表现不诚实，$\{M_\theta\}_{\theta\in Q}$可以被至少$t$个诚实的参与节点恢复。因此，所提DKG协议满足“有效性”。

定理3.　协议主密钥MSK对任何参与节点或任何共谋成员都是保密的。

证明. 协议主密钥MSK为随机秘密值M_θ的和。$\mathcal{A}$必须通过解密集合Q中所有的密文来获取所有的秘密值$\{M_\theta\}_{\theta\in Q}$。为了达到这一目的，$\mathcal{A}$需要解决离散对数问题以获取秘密值$\{M_\theta\}_{\theta\in Q}$。因此，协议主密钥$MSK$在重构前对任何参与节点或任何共谋成员$f(<n/2)$都是保密的。因此，所提DKG协议满足“保密性”。

定理4.　即使有f个恶意的参与节点，任何$t>n/2$个诚实的参与节点都可以有效地计算出主私钥MSK。

证明. 假设在重构阶段存在$f<n/2$恶意的参与节点，即诚实的参与节点数量大于阈值t，即$n-f\geqslant t$。将阈值t设置为$n/2+1(>f)$。每个参与节点都可以用关联的密文承诺其解密密钥的有效性。只要组合t个诚实解密密钥，就可以对诚实方Q的密文进行解密，保证获得MSK。各参与节点在构造MPK时调用$Encrypt$算法作为加密器，在恢复MSK时调用$AttrKeyGen$算法作为属性权威。这两种算法是独立调用的，保证可用性的诚实方在每种算法中可能不同。因此，通过调用密钥生成和解密算法，各参与节点可以有效地计算MSK，即协议对$f(<n/2)$个恶意的参与节点保持“鲁棒性”。

7　性能分析

所提DKG协议由线下和线上部分组成。实验设置$t=n/2+1$，在配备英特尔酷睿2.9 GHz i7-7500U CPU和8 GB RAM的计算机上进行性能评估，其中t是CP-ABE使用的阈值。针对线下开销，基于py_ecc库实现椭圆曲线“bn_128”，并在Python语言中实现改进的CP-ABE算法。此外，针对线上开销的评估，由于在共享阶段和重构阶段，参与节点只需要与智能合约进行交互，不需要实现P2P网络，因此，使用Solidity v0.5.17编写智能合约，并将其部署到以太坊平台以评估所提DKG协议的线上开销。

7.1　复杂度分析

表2给出了$Encrypt$算法、$AttrKeyGen$算法和$Decrypt$算法的运算次数。其中，$Add_{\mathbb{G}_i}$、$Mul_{\mathbb{G}_i}$、$Add_{\mathbb{H}}$和$Mul_{\mathbb{H}}$表示在群$\mathbb{G}_i$和$\mathbb{H}$上的加法运算和乘法运算操作，$ModPow$表示大素数的乘数除法操作，$Pairing$表示双线性映射$\mathbb{G}\times\mathbb{H}\rightarrow\mathbb{G}_T$。如表2所示，针对$Encrypt$算法，为了加密秘密值$M_\theta$，参与节点$P_\theta$需要在群$\mathbb{G}$上进行$n+1$次乘法操作，在群$\mathbb{H}$上进行$n$次加法操作和$3n$次乘法操作，在群$\mathbb{G}_T$上进行$n+1$次加法操作和$3n$次乘法操作；针对$AttrKeyGen$算法，为了生成解密密钥$K_\theta$，$P_\theta$需要在群$\mathbb{G}$上执行2次加法操作和3次乘法操作，在群$\mathbb{H}$上执行1次乘法操作；针对$Decrypt$算法，为了解密密文$C_\theta$，$P_\theta$需要在群$\mathbb{G}_T$上进行$3n$次加法操作、$4n$次乘法操作和1次双线性映射操作。

表3给出了密文C_θ和协议子公钥$PK_{\Gamma,\theta}$的创建成本。如表3所示，为了生成密文组件C_0，P_θ需执行

表2　CP-ABE中各算法的运算次数

操作/算法	$Encrypt$	$AttrKeyGen$	$Decrypt$
$Add_{\mathbb{G}}$	-	2	-
$Mul_{\mathbb{G}}$	$n+1$	3	-
$Add_{\mathbb{H}}$	n	-	-
$Mul_{\mathbb{H}}$	$3n$	1	-
$Add_{\mathbb{G}_T}$	$n+1$	-	$3n$
$Mul_{\mathbb{G}_T}$	$3n$	-	$4n$
$Pairing$	-	-	1

1次$Pairing$操作和1次$Mul_{\mathbb{H}}$操作；为了生成密文组件C_1，P_θ需执行n次$Add_{\mathbb{G}}$操作、$2n$次$Mul_{\mathbb{H}}$操作和$3n$次$ModPow$操作；为了生成密文组件C_2，P_θ需执行n次$Add_{\mathbb{G}}$操作和$2n$次$Mul_{\mathbb{H}}$操作；为了生成$PK_{\Gamma,\theta}$，P_θ需执行1次$Add_{\mathbb{G}}$操作和2次$Mul_{\mathbb{H}}$操作。

表3 密文及协议子公钥的创建成本

密文组件	$Add_{\mathbb{G}}$	$Mul_{\mathbb{H}}$	$ModPow$	$Pairing$
C_0	-	1	-	1
C_1	n	$2n$	$3n$	-
C_2	n	$2n$	-	-
$PK_{\Gamma,\theta}$	1	2	-	-

表4从密码原语、验证复杂度、计算复杂度和通信复杂度等方面给出了所提DKG协议与文献[22]和文献[29]的比较结果。如表4所示，在共享阶段协议的复杂度与文献[22]和文献[29]一致，在重构阶段低于文献[22]，和文献[29]一致。但在密文共享阶段，每次参与节点P_θ提交元组$(C_\theta, PK_{\Gamma,\theta}, Com_\theta)$，合约会对$PK_{\Gamma,\theta}$进行验证，验证复杂度为$O(1)$，低于文献[22]和文献[29]。在共享阶段，$P_\theta$运行$Encrypt$算法生成加密份额$C_\theta$和$PK_{\Gamma,\theta}$，并将其上传到合约。因此，共享阶段的通信和计算复杂度均为$O(n)$。在重构阶段，外部参与节点需调用$Decrypt$算法得到M_θ，且每个解密密钥的大小为$O(1)$，计算复杂度为$O(n)$，通信复杂度为$O(n)$。

表4 协议复杂度比较

协议	密码原语	验证	参与节点		外部参与节点	
			计算	通信	计算	通信
文献[22]	PVSS	$O(n^2)$	$O(n)$	$O(n)$	$O(n)$	$O(n^2)$
文献[29]	D-ABE	$O(n^2)$	$O(n)$	$O(n)$	$O(n)$	$O(n)$
所提协议	CP-ABE	$O(1)$	$O(n)$	$O(n)$	$O(n)$	$O(n)$

7.2 实验结果

7.2.1 链上开销

在密文共享阶段，无论有多少恶意参与节点，智能合约SC都会对协议子公钥$PK_{\Gamma,\theta}$进行有效性验证，且任意外部参与节点均能对CP-ABE密文的正确性进行验证。因此，在以太坊中使用智能合约来估算密钥份额验证的成本，以验证所提DKG协议的实用性。

如图3所示，部署合约SC所消耗的Gas值为909 713 Gas，使用$Check$算法验证DKG子公钥$PK_{\Gamma,\theta}$和使用$GenMPK$算法生成DKG公钥MPK的Gas消耗较小，参与节点使用$Join$算法提交承诺和使用$getCredentials$函数获取凭证的Gas消耗也不大。

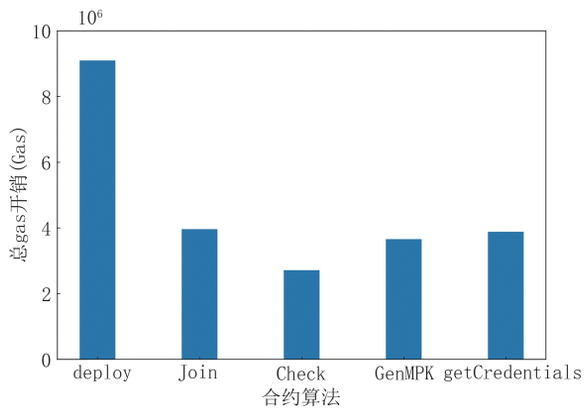

图3 合约Gas消耗

图4给出了参与节点数量从20到1000时不同DKG协议的总Gas消耗。如图4所示，总Gas开销随着参与节点数量的增加呈线性增长，所提DKG协议的总Gas开销小于文献[22]和文献[29]。这是由于文献[22]在共享阶段不是1轮的，需要向每个参与节点发送秘密份额，其加密份额是不可公开验证。此外，文献[29]在共享阶段需要生成更多的加密密钥份额。

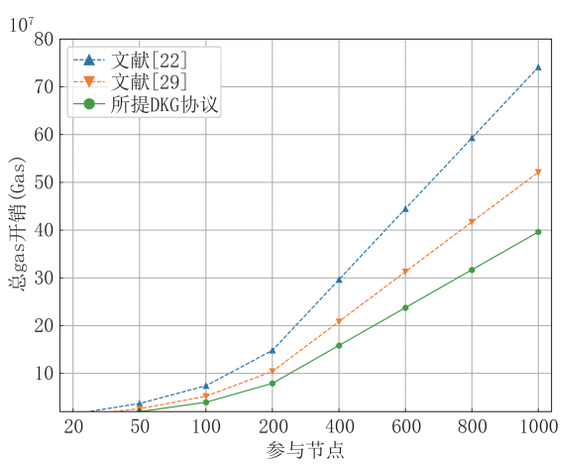

图4 参与节点增加时Gas消耗

7.2.2 线下开销

在所提DKG协议中，线下开销主要由密文共享阶段的密文C_θ和协议子公钥$PK_{\Gamma,\theta}$的创建成本以及重构阶段的解密开销所决定，故只针对协议子公钥$PK_{\Gamma,\theta}$和密文C_θ的创建成本、解密开销进行仿真评估。为了更好地评估参与节点的线下开销，在仿真过程中，实验设置属性个数为10，并评估了参与节点数量从20到1000变化时协议子公钥$PK_{\Gamma,\theta}$和密文C_θ的创建成本、解密开销。

图5给出了参与节点数量从20到1000变化时

协议子公钥$PK_{\Gamma,\theta}$和密文C_θ的创建成本。图6给出了参与节点数量从20到1000变化时外部用户运行解密算法解密密文C_θ以获取秘密值M_θ的开销。

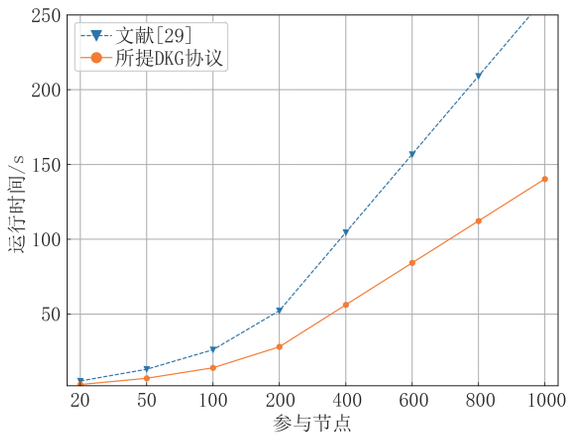

图5　协议子公钥$PK_{\Gamma,\theta}$和密文C_θ的创建开销

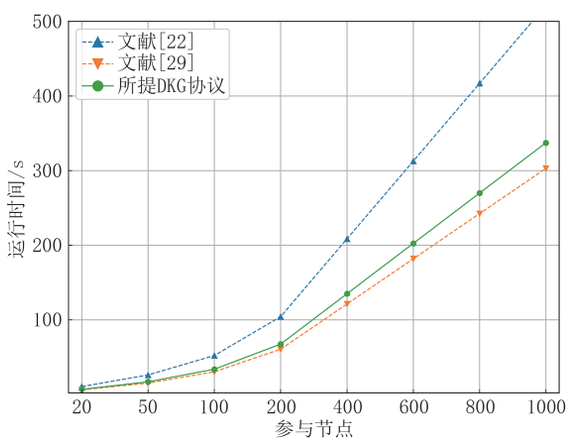

图6　不同协议的解密开销

如图5所示，随着参与节点数量的增加，在文献[29]和所提DKG协议中，协议子公钥$PK_{\Gamma,\theta}$保持一致，但密文C_θ的创建时间都会增加。这是因为文献[29]所需要生成的份额密文多于所提协议，故其密文创建开销较高于所提DKG协议。

如图6所示，随着参与节点数量的增加，文献[22]、文献[29]和所提DKG协议的密文解密时间都会增加。但由于文献[22]的DKG协议是基于PVSS设计的，所以其密文解密时间受拉格朗日插值法的限制，高于文献[29]和所提DKG协议。文献[29]所需的密文解密时间略低于所提DKG协议，这是因为所提DKG协议在密文生成的过程中引入了承诺种子，需要额外的计算开销。然而，文献[29]不支持外部用户对加密份额进行有效性验证，故所提DKG协议的整体性能优于献[22]和文献[29]。

8　结束语

本文提出了基于区块链与CP-ABE的一轮可验证DKG协议，仅需$O(n)$的通信计算复杂度即可恢复共享密钥。在共享阶段，首先设计了基于哈希的通用承诺，并将承诺种子整合至CP-ABE的加密算法，确保了外部用户可以对CP-ABE密文进行有效性验证。同时，在该阶段通过合约验证DKG协议子公钥，以筛选出合法的参与节点集合，验证复杂度为$O(1)$。最后，外部用户可通过合约获取诚实的节点集合提交的密钥份额密文和DKG协议子公钥，并基于本地的份额重构出共享密钥，仅需$O(n)$的通信和计算复杂度。实验结果表明，所提DKG协议在共享阶段需要更少的验证开销，且在协议主私钥重构阶段提供了可验证解密的能力，同时很少降低效率。然而，由于CP-ABE依赖于TA生成属性密钥，未来将进一步研究去中心化的CP-ABE算法，消除协议对TA的依赖。

参　考　文　献

[1] Long Y Y, Peng C G, Tan W J, et al. Blockchain-based anonymous authentication and key management for internet of things with Chebyshev chaotic maps. IEEE Transactions on Industrial Informatics, 2024, 20(5): 7883-7893

[2] Desmedt Y, Frankel Y. Threshold cryptosystems//Proceedings of the 9th Annual International Cryptology Conference. California, USA, 1989:307-315

[3] Li M, Ding H N, Wang Q, et al. Decentralized threshold signatures with dynamically private accountability. IEEE Transactions on Information Forensics and Security, 2024, 19: 2217-2230

[4] Cachin C, Kursawe K, Shoup V. Random oracles in constant inople: Practical asynchronous byzantine agreement using cryptography. Journal of Cryptology, 2005, 18(3): 219-246

[5] Wang C, Shen J, Vijayakumar P, et al. Attribute based secure data aggregation for isolated IoT-enabled maritime transportation systems. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(2): 2608-2617

[6] Wang C, Zhou T Q, Shen J, et al. Searchable and secure edge pre-cache scheme for intelligent 6G wireless systems. Future Generation Computer Systems, 2023, 140: 129-137

[7] Feldman P. A practical scheme for non-interactive verifiable secret sharing//Proceedings of the 28th Annual Symposium on Foundations of Computer Science. Los Angeles, USA, 1987: 427-438

[8] Stadler M. Publicly verifiable secret sharing. Advances in Cryptology Eurocrypt, 1985:190-199

[9] Chen X, Zhang L F. Publicly verifiable homomorphic secret sharing for polynomial evaluation. IEEE Transactions on Information Forensics and Security, 2023, 18: 4609-4624

[10] Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization// Proceedings of the International Workshop on Public Key Cryptography. Berlin, Germany, 2011:53-70

[11] Ning J, Cao Z F, Dong X L, et al. White-box traceable cp-abe for cloud storage service: how to catch people leaking the iraccess credentials effectively. IEEE Transactions on Dependable and Secure Computing, 2018, 15(5): 883-897

[12] Shen J, Zhou T Q, He D B, et al. Block design-based key agreement for group data sharing in cloud computing. IEEE Transactions on Dependable and Secure Computing, 2019, 16(6): 996-1010

[13] Su Y, Sun J M, Qin J, et al. Publicly verifiable shared dynamic electronic health record data bases with functional commitment supporting privacy-preserving integrity auditing. IEEE Transactions on Cloud Computing, 2022, 10(3): 2050-2065

[14] Wang T, Ma H, Zhou Y B, et al. Fully accountable data sharing for pay-as-you-go cloud scenes. IEEE Transactions on Dependable and Secure Computing, 2021, 18(4): 2005-2016

[15] Djenouri Y, Yazidi A, Srivastava G, et al. Blockchain: Applications, challenges, and opportunities in consumer electronics. IEEE Consumer Electronics Magazine, 2024, 13(2): 36-41

[16] Asanuma T, Isobe T. A proof of work based on key recovery problem of cascade block ciphers with ASIC resistance. Ieice Transactions on Information & Systems, 2022, 105-D(2): 248-255

[17] Misic J V, Misic V B, Chang X L. Design of proof-of-stake pbft algorithm for iot environments. IEEE Transactions on Vehicular Technology, 2023, 72(2): 2497-2510

[18] Pedersen T P. A threshold cryptosystem without a trusted party//Proceedings of the International Conference on the Cryptology-EUROCRYPT. Brighton, UK, 1991.221-242

[19] Tomescu A, Chen R, Zheng Y M, et al. Towards scalable threshold cryptosystems//Proceedings of the IEEE Symposium on Security and Privacy (SP), San Francisco, USA, 2020: 877-893

[20] Kogias E K, Malkhi D, Spiegelman A. Asynchronous distributed key generation for computationally-secure randomness, consensus, and threshold signatures//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. Virtual, 2020: 1751-1767

[21] Gao Y Z, LuY, Lu Z L, et al. Efficient asynchronous byzantine agreement without private setups//Proceedings of the IEEE 42nd International Conference on Distributed Computing Systems. Bologna, Italy, 2022: 246-257

[22] Fouque P A, Stern J. One round threshold discrete-log key generation without private channels//Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptosystems. Cheju Island, Republic of Korea, 2001: 300-316

[23] Paillier P. Public-key cryptosystems based on composite degree residuosity classes//Proceedings of the International Conference on the theory and applications of cryptographic techniques. Singapore, 1999:223-238

[24] Gennaro R, Jarecki S, Krawczyk H, et al. Secure distributed key generation for discrete-log based cryptosystems// Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany, 1999:295-310

[25] Neji W, Blibech K, BenRajeb N. Distributed key generation protocol with a new complaint management strategy. Security and communication networks, 2016, 9(17): 4585-4595

[26] Schindler P, Judmayer A, Stifter N, et al. ETHDKG: Distributed key generation with Ethereum smart contracts. arXivPreprintarXiv:2019/985

[27] Lai J Z, Deng R H, Guan C W, et al. Attribute-based encryption with verifiable outsourced decryption. IEEE Transactions on Information Forensics and Security, 2013, 8(8): 1343-1354

[28] Mao X P, Lai J Z, Mei Q X, et al. Generic and efficient constructions of attribute-based encryption with verifiable outsourced decryption. IEEE Transactions on Dependable and Secure Computing, 2016, 13(5): 533-546

[29] Zhang L, Qiu F Y, Hao F, et al. 1-round distributed key generation with efficient reconstruction using decentralized CP-ABE. IEEE Transactions on Information Forensics and Security, 2022, 17: 894-907

[30] Zhang Z, Huang W, Yang L, et. al. A stronger secure ciphertext fingerprint-Based commitment scheme for robuster verifiable OD-CP-ABE in IMCC. IEEE Internet of Things Journal, 2023, 10(18): 16531-16547

PENG Chang-Gen, Ph. D., professor. His research interests include information security and cryptography, blockchain, secure computing.

LONG Yang-Yang, Ph. D. candidate. His research interests include blockchain, big data security and privacy-preserving.

CHEN Yu-Ling, Ph. D., professor. Her research interests include big data, security system and information security.

Background

As a core issue in the field of cyberspace security, distributed key generation (DKG) protocols typically include two phases: sharing and key reconstruction. The crux of the matter is how to compute shared public and private keys through the multi-party participation, to address the issues of single-point failures and key escrow, while ensuring the security and correctness of the shared keys. Traditional DKG protocols are mostly constructed based on publicly verifiable secret sharing (PVSS), with the sharing phase and the reconstruction phase each requiring at least two rounds, the computational complexity and communication complexity are both $O(n^2)$, which is insufficient to be adapt to large-scale industrial application in complex network environments under the premise of security. Thus, seeking more efficient algorithms and methods to reduce the number of communication rounds and the computational burden on participants in verifying and processing key shares remain challenges.

Blockchain, as a distributed system with embedded trust, provides a new approach to implement key management under the conditions of multi-party cooperation in cyber scenarios. Besides, ciphertext policy attribute-based encryption (CP-ABE), as an encryption technique providing fine-grained access control, which allows users to encrypt data based on specific attributes or combinations of attributes with external decryption property (i. e., an external user can decrypt the ciphertexts), provides a more effective solution strategy for designing DKG protocols with an efficient key reconstruction phase than PVSS. Therefore, by utilizing blockchain as open channel and CP-ABE as cryptographic primitive, this paper proposes innovative one round verifiable DKG protocol to solve the above-mentioned limitations of distributed key generation.

We provide a more efficient DKG protocol with a combination of CP-ABE and the blockchain. The participating nodes collaborate in the sharing phase to generate the public key of DKG protocol and the verification complexity is $O(1)$. Moreover, the honest nodes collaborate to compute the corresponding private key of DKG protocol in the key reconstruction phase, and the external user only needs the communication and computation complexity of $O(n)$. To be specific, we first designed a generic hash commitment scheme, and with this commitment scheme, the smart contract can check the sub-public key of the participating node. After that, we improved the original CP-ABE encryption algorithm to ensure verifiability of secret shares of the participating node in DKG protocol by introducing an auxiliary parameter. The proposed DKG protocol is proved theoretically for verifiability, validity, confidentiality and robustness, as well as evaluated and benchmarked with algorithm complexity analysis and experimental measures.

The presented work is partially supported by the funds from the National Key Technologies R&D Programs of China under Grant No. 2022YFB2701400, the National Natural Science Foundation of China under Grant No. 61972032.