基于可聚合PVSS和联盟链的密钥可公开验证MA-CP-ABE方案

景旭[1,2]，蒋炎[1,2]

（1. 西北农林科技大学信息工程学院，陕西 杨凌 712100；2. 陕西省农业信息智能感知与分析工程技术研究中心，陕西 杨凌 712100）

摘　要：针对基于门限的多机构密文策略属性基加密（MA-CP-ABE）存在属性颁发机构（AA）不可信、属性私钥正确性无法公开验证等问题，提出了一种基于可聚合PVSS和联盟链的密钥可公开验证MA-CP-ABE方案。基于ElGamal改进可聚合PVSS算法，实现系统主密钥分发的可公开验证；基于双线性映射和ElGamal加密，构造MA-CP-ABE属性私钥可公开验证方法，实现属性私钥及其子份额密文条件下的可公开验证；基于联盟链提出密钥可公开验证MA-CP-ABE方案，通过联盟链保证验证参数可信，通过智能合约实现自动化验证。正确性、机密性、鲁棒性和活性等分析表明，当总AA数量为n、门限值为t、恶意AA数量不超过t–1时，所提方案能够保证属性私钥的正确分发，且系统主密钥初始化的通信开销复杂度为$O(tn)$。

关键词：分布式密钥生成；多机构密文策略属性基加密；可公开验证秘密共享；联盟链

中图分类号：TP309；TP393

文献标志码：A

DOI：10.11959/j.issn.1000–436x.2024139

Key public verifiable MA-CP-ABE scheme based on aggregatable PVSS and consortium blockchain

JING Xu[1,2], JIANG Yan[1,2]

1. College of Information Engineering, Northwest A&F University, Yangling 712100, China
2. Shaanxi Engineering Research Center of Agricultural Information Intelligent Perception and Analysis, Yangling 712100, China

Abstract: To address challenges associated with threshold-based multi-authority ciphertext-policy attribute-based encryption (MA-CP-ABE), such as untrusted attribute authorities (AA) and the inability to verify the correctness of attribute private keys publicly, a key public verifiable MA-CP-ABE scheme based on aggregatable publicly verifiable secret sharing (PVSS) and consortium blockchain was proposed. An aggregatable PVSS algorithm was improved based on ElGamal, which enabled the public verifiability of the system master key distribution. A publicly verifiable method for MA-CP-ABE attribute private keys was constructed based on bilinear maps and ElGamal encryption, enabling the public verifiability of attribute private keys and their shares in ciphertext conditions. A key public verifiable MA-CP-ABE scheme was proposed based on a consortium blockchain, ensuring the trustworthiness of verification parameters through the consortium blockchain and achieving automated verification via smart contracts. The analysis of correctness, confidentiality, robustness, and liveness indicates that when the total number of AA is n, the threshold value is t, and the number of malicious AA is not more than t–1, the scheme can ensure the correct distribution of attribute private keys, and the communication overhead complexity of the system master key initialization is $O(tn)$.

Keywords: DKG, MA-CP-ABE, PVSS, consortium blockchain

收稿日期：2024–02–18；**修回日期：**2024–07–01

基金项目：国家自然科学基金资助项目（No.72271202）；国家重点研发计划基金资助项目（No.2020YFD1100601）；陕西省秦创原“科学家+工程师”队伍建设基金资助项目（No.2022KXJ-67）；西北农林科技大学研究生创新竞赛基金资助项目

Foundation Items: The National Natural Science Foundation of China (No.72271202), The National Key Research and Development Program of China (No.2020YFD1100601), The “Scientist+Engineer” Team Building Foundation of Shaanxi Qinchuangyuan (No.2022KXJ-67), Northwest A&F University Graduate Innovation Competition Project

0　引言

多机构密文策略属性基加密（MA-CP-ABE, multi-authority ciphertext-policy attribute-based encryption）能够实现一对多的数据加密，广泛应用于数据共享的隐私保护中[1]。MA-CP-ABE改善了单机构密文策略属性基加密证书颁发机构（CA, certificate authority）存在的密钥泄露、拒绝服务等问题[2]，但依旧存在属性颁发机构（AA, attribute authorities）不可信[3-4]、属性私钥正确性无法公开验证[5]等问题。因此，研究恶意模型下的MA-CP-ABE具有重要意义。

Chase[6]提出了一种MA-CP-ABE方案，颁发机构由一个可信CA和多个AA组成，AA由CA初始化。Huang等[7]、吴光强[8]、Xue等[9]和Wang等[10]依据Chase[6]的思路分别提出了具体应用中的MA-CP-ABE。上述研究的基本思想是由一个CA初始化多个AA，由AA分发属性私钥份额，均假设CA和AA均是诚实的，难以克服单点故障和满足存在恶意AA下的密钥分发要求。

在Yang等[1]、Lewko等[11]、闫玺玺等[12]和Datta等[13]的MA-CP-ABE方案中，将整个属性集划分成多个不相交的子集，各子集由一个或多个AA维护，攻击者只攻陷一个机构就可以获得特定属性私钥的颁发权限，因此依旧无法突破单点故障瓶颈，难以保证存在恶意AA时正确分发属性密钥。

基于门限的MA-CP-ABE安全性和鲁棒性更高，系统主密钥泄露风险更低，能够降低单点故障瓶颈风险。Lin等[14]提出了基于门限的MA-CP-ABE方案。Li等[15]和Gu等[16]实现了云存储中基于门限的MA-CP-ABE方案。Ramesh等[17]提高了Li等[15]的加密效率。唐飞等[18]优化了用户属性证明的验证计算开销。在上述方案中，当总AA数量为n，门限值为t时，仅当颁发属性私钥的AA数量超过$t-1$时，才能为用户颁发正确的属性私钥。但是若存在一个恶意AA不按照协议生成或分发系统主密钥和属性私钥时，会导致系统或用户陷入长时间等待状态，无法保证用户及时获取完整、正确的属性私钥，也不能及时定位到恶意AA。此外，在系统主密钥生成阶段，AA间通信的时间复杂度较高。

针对上述问题，本文提出了一种基于可聚合可公开验证秘密共享（PVSS, publicly verifiable secret sharing）[19]和联盟链的密钥可公开验证MA-CP-ABE方案，主要研究包括以下3个方面。

1) 基于ElGamal改进Gurkan等[19]提出的可聚合PVSS算法（简称Gurkan可聚合PVSS），用ElGamal加密方式替换Gurkan可聚合PVSS的加密方式，实现对群元加密的支持，使加密算法满足选择明文攻击下的不可区分（IND-CPA, indistinguishability under chosen plaintext attack）安全，提供系统主密钥子份额的ElGamal同态承诺。

2) 在研究1) 中基于ElGamal改进的可聚合PVSS产生的可公开参数、ElGamal同态承诺以及双线性映射的双线性，构造MA-CP-ABE属性私钥可公开验证方法，实现对属性私钥子份额ElGamal密文条件下的可公开验证。当出现恶意分发时，能够通过验证定位到作恶AA。

3) 在研究2) 的基础上，基于联盟链提出了密钥可公开验证MA-CP-ABE方案。通过基于ElGamal改进的可聚合PVSS，实现系统主密钥子份额的分发和可公开验证，利用PVSS的聚合性缩短MA-CP-ABE系统主密钥子份额分发的验证时间；通过联盟链记录系统中的公开验证参数，实现验证过程中数据难篡改和数据来源的可追溯；结合来自联盟链的可信数据，将MA-CP-ABE属性私钥可公开验证方法集成到智能合约中，保证链上用户的属性私钥密文都是诚实AA生成的。

1　相关知识

1.1　MA-CP-ABE方案

在Waters[20]的密文策略属性基加密（CP-ABE, ciphertext-policy attribute-based encryption）方案基础上，Li等[15]提出了一种MA-CP-ABE方案，其中属性私钥SK为$\{\mathrm{SK}_1=g^{d},\mathrm{SK}_2=g^{\alpha}g^{\beta d},\mathrm{SK}_{3,m}=h_m^{d}\}$，属性公钥PK为$\{\mathrm{PK}_1=g,\mathrm{PK}_2=g^{\beta},\mathrm{PK}_3=e(g,g)^{\alpha}\}$，$S$为属性私钥申请者拥有的属性映射到群$G$的集合，$m$为用户属性值$\mathrm{att}_m$在$S$中的索引值，$h_m$为将用户属性值$\mathrm{att}_m$映射到群$G$的值，且$\alpha,\beta,d\in Z_p$。

1.2　基于双线性映射的ElGamal加密

ElGamal加密具有乘法同态性[21]，实现方式多样。基于双线性映射的实现方式契合本文选择的基

础MA-CP-ABE方案，所以本文方案采用基于双线性映射的ElGamal加密方式。

引理1[22] ElGamal加密是一种基于离散对数难题（DLP, discrete logarithm problem）的加密体系，具有语义安全性，满足IND-CPA安全。

2 面向MA-CP-ABE的可聚合PVSS

在Cascudo等[23]提出的基于双线性映射的PVSS方案基础上，Gurkan等[19]利用承诺[24]的同态性，提出了一种支持聚合的PVSS方案，降低了秘密共享验证阶段的复杂度，但是恢复秘密时会直接生成原始的秘密值，无法对群元进行加密。MA-CP-ABE要求系统主密钥可复用[15]，用于加密的值（系统主密钥）应当是群元。此外，Gurkan可聚合PVSS采用的“加密”实际是Diffie-Hellman密钥交换协议，严格意义上来说不能称作加密，不满足IND-CPA安全。因此，Gurkan可聚合PVSS难以满足应用要求。

ElGamal加密基于Diffie-Hellman密钥交换协议，理论上有替换Gurkan可聚合PVSS加密方式的基础，并且基于双线性映射实现ElGamal加密的方式契合当前主流的MA-CP-ABE实现方式。

综上所述，本文方案采用具有乘法同态特性的ElGamal加密算法替换Gurkan可聚合PVSS的加密方式，实现对群元的加密，同时为后续用户属性私钥子份额的验证提供系统主密钥子份额的ElGamal同态承诺。

2.1 基于ElGamal的可聚合PVSS

1) 协商通用字符串。G为大素数p阶乘法循环群，g和h为G的2个不同的生成元，参与者P_j的编号为w_j，$\mathrm{pk}_j = g^{\mathrm{sk}_j}$，$\mathrm{sk}_j \in Z_p$。系统中的参与者个数为$n$，门限值为$t$，$u_1$是群$G$上的元素。

2) 秘密生成与共享。秘密分发者选择t−1阶多项式$f(x) = (a_0, a_1, \cdots, a_{t-1})$，其中$f(0) = a_0$，$g^{a_0}$为将要分发的实际秘密值，分别计算$f(x)$各系数的Fledman承诺$F_k = h^{a_k}$，$k \in [0, t-1]$。分发者用$f(x)$和参与者$\mathrm{P}_j$的编号$w_j$，计算对参与者$\mathrm{P}_j$共享的秘密子份额$f(w_j)$和承诺$A_j = h^{f(w_j)}$。此外，计算辅助参数$u_2 = u_1^{a_0}$。

F、A和u_2生成方式与Gurkan可聚合PVSS保持一致。秘密子份额$f(w_j)$的加密方式更改为基于双线性映射的ElGamal，加密结果如式(1)所示。

$$(Y_j^1 = g^{r_j};\ Y_j^2 = g^{f(w_j)}\mathrm{pk}_j^{r_j}) \tag{1}$$

其中，Y_j^1为ElGamal加密因子，Y_j^2为ElGamal消息密文，$r_j \in Z_p$，pk_j为P_j的ElGamal公钥。

$Y_j^3 = h^{r_j}$用于后续验证，由此得到秘密子份额的ElGamal密文$Y_j = \{Y_j^1, Y_j^2, Y_j^3\}$，$\mathrm{pvss}_j = \{F_*, Y_j, A_j, u_2\}$组成该分发者对参与者$\mathrm{P}_j$的一条PVSS记录。

3) 验证。任何一个参与者都能够验证任意一条PVSS记录的正确性，验证方式如式(2)~式(6)所示。由于F、A和u_2的生成方式不变，因此式(2)和式(3)与Gurkan可聚合PVSS保持一致，其中$\Delta w_j(w)$表示参与者P_j的拉格朗日基多项式在$x = w$处的取值。多项式的承诺没有改变，因此出错秘密子份额的定位方式也不变，如式(6)所示。

由于加密方式的改变，需要对密文的验证方式进行修改，修改后的验证如式(4)和式(5)所示。

$$\prod_{j=1}^{n} A_j^{\Delta w_j(w)} \stackrel{?}{=} \prod_{k=0}^{t-1} F_k^{w^k} \tag{2}$$

$$e(F_0, u_1) \stackrel{?}{=} e(h, u_2) \tag{3}$$

$$e(h, Y_j^1) \stackrel{?}{=} e(Y_j^3, g) \tag{4}$$

$$e(h, Y_j^2) \stackrel{?}{=} e(A_j, g)\, e(Y_j^3, \mathrm{pk}_j) \tag{5}$$

$$A_j \stackrel{?}{=} \prod_{k=0}^{t-1} F_k^{w_j^k} \tag{6}$$

4) 解密。如果上述验证都通过，则说明分发者进行了一次诚实的秘密共享，参与者P_j使用私钥解密获取秘密子份额$\mathrm{sub_sk}_j$，如式(7)所示。

$$\mathrm{sub\_sk}_j = \frac{Y_j^2}{(Y_j^1)^{\mathrm{sk}_j}} \tag{7}$$

5) 聚合。由于ElGamal具有乘法同态性质，所以聚合过程和Gurkan可聚合PVSS保持一致。假设分发者D_1和D_2分别选择t−1阶多项式f_1和f_2，对n个参与者P_j进行秘密共享。D_1的PVSS记录$\mathrm{pvss}_{1,j} = \{F_{1,*}, Y_{1,j}, A_{1,j}, u_{1,2}\}$，$\mathrm{D}_2$的PVSS记录$\mathrm{pvss}_{2,j} = \{F_{2,*}, Y_{2,j}, A_{2,j}, u_{2,2}\}$。聚合后可得$f_1 + f_2$的共享记录$\mathrm{pvss}_{1+2} = \{F_{1+2,*}, Y_{1+2,j}, A_{1+2,j}, u_{1,2+2,2}\}$，聚合过程如式(8)所示。

$$\begin{cases} F_{1+2,k} = F_{1,k}F_{2,k}, k \in [0, t-1] \\ A_{1+2,j} = A_{1,j}A_j, j \in [0, n-1] \\ Y_{1+2,j} = Y_{1,j}Y_{2,j}, j \in [0, n-1] \\ u_{1+2,2} = u_{1,2}u_{2,2} \end{cases} \tag{8}$$

由式(8)可见，对 D_1 和 D_2 的 PVSS 验证可以转化为对 pvss_{1+2} 的验证，减少了需要验证的 PVSS 记录数量，降低了验证时间。

6) 秘密重建。当有大于或等于 t 个诚实参与者参与重建时，可通过拉格朗日插值恢复 g^{a_0}，如式(9)所示。

$$\prod_{j=0}^{t} \text{sub\_sk}_j^{\Delta_{w_j}(0)} = g^{\sum_{j=0}^{t} f(w_j)\Delta_{w_j}(0)} = g^{f(0)} = g^{a_0} \tag{9}$$

2.2　正确性

定理 1　基于 ElGamal 的可聚合 PVSS 记录验证是正确的。

证明　在验证方法中，式(2)和式(3)与 Gurkan 可聚合 PVSS 的验证方式一致，验证所有秘密子份额是否来自同一个多项式；式(4)和式(5)分别验证 Y_j^3 和 Y_j^1 关于 ElGamal 加密的随机数是否相同以及加密后的秘密子份额是否正确。根据 2.1 节可知 $Y_j^1 = g^{r_j}$ 和 $Y_j^3 = h^{r_j}$，代入式(4)可得

$$e(h, Y_j^1) \stackrel{?}{=} e(Y_j^3, g) \Rightarrow e(h, g^{r_j}) \stackrel{?}{=} e(h^{r_j}, g) \tag{10}$$

当分发者诚实分发秘密时，式(10)显然成立。该式用来验证 ElGamal 加密因子 Y_j^1 使用的随机数和 Y_j^3 中承诺的加密随机数是否一致。

式(5)验证密文中的秘密子份额与式(2)和式(3)确定的秘密共享多项式相关，式(5)各部分代入参数可得

$$\begin{cases} e(h, Y_j^2) = e(h, g^{f(w_j)}\text{pk}_j^{r_j}) \\ e(A_j, g) = e(h^{f(w_j)}, g) \\ e(Y_j^3, \text{pk}_j) = e(h^{r_j}, \text{pk}_j) \end{cases} \tag{11}$$

式(5)代入式(11)的参数后可以得到式(12)。根据双线性映射中的双线性特点，当 PVSS 记录中通过 ElGamal 加密的秘密值满足承诺多项式，并且加密参数正确时，等式(12)成立，说明 Y_j^2 中使用的随机数和 Y_j^1 中的一致。根据式(4)可推出 Y_j^1 和 Y_j^3 中承诺的加密随机数一致。此外，说明 Y_j^2 密文对应的明文（秘密子份额）和 A_j 承诺的秘密值一致；若分发不正确，则等式(12)不成立。

$$e(h, g^{f(w_j)}\text{pk}_j^{r_j}) \stackrel{?}{=} e(h^{f(w_j)}, g)\, e(h^{r_j}, \text{pk}_j) \tag{12}$$

综上，基于 ElGamal 的可聚合 PVSS 记录验证是正确的。证毕。

定理 2　基于 ElGamal 的可聚合 PVSS 聚合过程是正确的。

证明　在式(8)中，F、A 和 u 都没有发生变化，所以只需证明聚合 Y 的正确性，如式(13)所示。

$$\begin{cases} Y_{1+2,j}^1 = Y_{1,j}^1 Y_{2,j}^1 = g^{r_{1,j}} g^{r_{2,j}} = g^{r_{1,j}+r_{2,j}} = g^{r_{1+2,j}} \\ Y_{1+2,j}^2 = Y_{1,j}^2 Y_{2,j}^2 = g^{r_{1,j}} \text{pk}_j^{r_{1,j}} g^{r_{2,j}} \text{pk}_j^{r_{2,j}} \\ \qquad = g^{r_{1,j}+r_{2,j}} \text{pk}_j^{r_{1,j}+r_{2,j}} = g^{r_{1+2,j}} \text{pk}_j^{r_{1+2,j}} \\ Y_{1+2,j}^3 = Y_{1,j}^3 Y_{2,j}^3 = h^{r_{1,j}} h^{r_{2,j}} = h^{r_{1,j}+r_{2,j}} = h^{r_{1+2,j}} \end{cases} \tag{13}$$

分发者 D_1 和 D_2 分别选择多项式对参与者 P_j 共享秘密值，再对秘密值求和，相当于一个分发者通过这 2 个多项式的和 $B(x) = f_1(x) + f_2(x)$ 对一个参与者 P_j 共享秘密值 $B(0)$。证毕。

2.3　安全性

定理 3　基于 ElGamal 改进的可聚合 PVSS 在决策 Diffie-Hellman（DDH, decisional Diffie- Hellman）假设下是安全的。

证明　本文方案对于 Gurkan 可聚合 PVSS 方案的改进采用了 ElGamal 加密，新增了一个辅助变量 $Y_j^3 = h^{r_j}$，从 Y_j^3 中求解 r_j，属于 DLP。因此，Y_j^3 不会泄露加密随机数 r_j，也不会影响 ElGamal 加密的安全性。此外，Y_j^3 只与 ElGamal 加密的随机数有关，不会影响 Gurkan 可聚合 PVSS 的安全性。

Y_j^2 和 Y_j^1 是对秘密子份额的 ElGamal 加密结果，F_*、A_j、u_2 和 Gurkan 可聚合 PVSS 相同，因此本文的 PVSS 安全性可以归结到 ElGamal 加密算法以及 Gurkan 可聚合 PVSS 的安全性。Gurkan 可聚合 PVSS 在随机预言模型中的 DDH 假设下被认为是安全的[19,23]。根据引理 1 可知，ElGamal 加密满足 IND-CPA 安全。证毕。

3　属性私钥可公开验证方法

MA-CP-ABE 方案[15]默认分发者在分发属性私钥子份额是诚实或半诚实的，没有考虑存在恶意分发者的情况。如何及时找到出错的属性私钥子份额并在公开场景中验证，是一个亟待解决的问题。基于双线性映射的双线性特点，本文提出了一种 MA-

CP-ABE 属性私钥可公开验证方法。

分析 MA-CP-ABE 属性私钥 SK 的构成{$SK_1 = g^d, SK_2 = g^{\alpha} g^{\beta d}, SK_{3,m} = h_m^d$}，推导出验证可以分为 SK_2 的生成是否使用了系统主密钥（g^{α}，对于属性私钥子份额则为是否使用系统主密钥子份额 $g^{\alpha_j} = g^{f(w_j)}$）和系统主公钥（$PK_2 = g^{\beta}$），以及 SK 的 3 个组成部分是否使用了同一个随机数 d。由于属性私钥子份额和属性私钥构成形式一致，故可以使用同一种方法进行验证。

通过 2.1 节基于 ElGamal 的可聚合 PVSS 分发系统主密钥子份额，公共环境中存在关于秘密值（$\alpha = a_0$）及其子份额（$\alpha_j = f(w_j)$）的承诺，为上述验证提供了理论基础。

3.1 模型

公告板能够产生不可伪造的证据，并证明该证据已发布。文献[23]和文献[25]使用公告板发布验证的信息，因此本文采用公告板提供公开的验证参数。

系统参数 G、g、h、u_1 以及各参与者的 ElGamal 公钥等已经存在公告板中。假设分发者利用 2.1 节基于 ElGamal 的可聚合 PVSS 对所有参与者实现秘密（MA-CP-ABE 系统主密钥）子份额的分发，并将 PVSS 记录上传到公告板。每个参与者 P_i 选择随机数 β_i，并将 g^{β_i} 上传到公告板。已知 $PK_1 = g$，可通过式(14)计算系统主公钥 PK_2；通过式(15)和式(16)计算 PK_3，其中的参数都来自公开的 PVSS 记录。

$$PK_2 = \prod g^{\beta_i} = g^{\sum \beta_i} = g^{\beta} \tag{14}$$

$$\frac{e(Y_i^2, g)}{e(pk_i, Y_i^1)} = \frac{e(g^{f(w_i)} pk_i^{r_i}, g)}{e(pk_i, g^{r_i})} = \frac{e(g^{f(w_i)}, g) e(pk_i^{r_i}, g)}{e(pk_i, g^{r_i})} = e(g,g)^{\alpha_i} \tag{15}$$

$$PK_3 = \prod e(g,g)^{\alpha_i \cdot \Delta w_i(0)} = e(g,g)^{\sum \alpha_i \Delta w_i(0)} = e(g,g)^{\alpha} \tag{16}$$

公告板中拥有系统参数、pk_i、PK、$pvss_i$ 等，各参与者通过解密 PVSS 中的 ElGamal 密文数据获取系统主密钥子份额 $sub\_sk_i = g^{\alpha_i}$。

3.2 各方颁发属性私钥子份额

属性私钥申请者的 ElGamal 公私钥对为(usk,upk = g^{usk})，将公钥 upk 上传到公告板。当密钥分发者 P_i 诚实时生成属性私钥 SK_i 为{$SK_{1,i} = PK_1^{d_i}, SK_{2,i} = sub\_sk_i \cdot PK_2^{d_i}, SK_{3,m,i} = h_m^{d_i}$}，其中 $SK_{1,i}$ 和 $SK_{2,i}$ 分别对应完整属性私钥 SK 中 SK_1 和 SK_2 的子份额，$SK_{3,m,i}$ 对应 $SK_{3,m}$ 的子份额。

P_i 使用 upk 加密 $SK_{2,i}$ 和 $SK_{3,m,i}$，然后将其发送到公告板上，加密后的属性私钥密文如式(17)所示。

$$\{CSK_{1,i}; CSK_{2,i}^1 = g^k, CSK_{2,i}^2 = SK_{2,i} upk^k; CSK_{3,m,i}^1 = g^{s_m}, CSK_{3,m,i}^2 = SK_{3,m,i} upk^{s_m}\} \tag{17}$$

其中，$(CSK_{2,i}^1, CSK_{2,i}^2)$ 和 $(CSK_{3,m,i}^1, CSK_{3,m,i}^2)$ 分别表示对 $SK_{2,i}$ 和 $SK_{3,m,i}$ 采用 ElGamal 加密的结果，且 $CSK_{1,i} = SK_{1,i}$。

3.3 属性私钥子份额公开验证方法

基于双线性映射构造的属性私钥子份额公开验证方法如式(18)和式(19)所示，其中所有的参数来自公告板。

$$e(CSK_{2,i}^2, PK_1) \stackrel{?}{=} \frac{e(PK_2, CSK_{1,i}) e(Y_i^2, PK_1) e(upk, CSK_{2,i}^1)}{e(pk_i, Y_i^1)} \tag{18}$$

$$e(PK_1, CSK_{3,m,i}^2) \stackrel{?}{=} e(CSK_{1,i}, h_m) e(CSK_{3,m,i}^1, upk) \tag{19}$$

当式(18)和式(19)同时成立时，表示密文 CSK_i 对应的明文 SK_i 是 P_i 颁发的正确属性私钥子份额。若存在一个验证等式不成立，则表示颁发的属性私钥子份额存在错误。

通过上述方法，能够在密文条件下验证 P_i 颁发的属性私钥子份额中 3 个组件是否使用了同一个随机数，同时验证是否使用了正确的系统主密钥子份额和系统主公钥，能够防止恶意分发者发送错误的属性私钥子份额给用户，造成用户无法获得属性私钥或陷入长时间等待的问题。

3.4 验证方法正确性与完备性

定理 4 若式(18)和式(19)同时成立，则表示 CSK_i 对应的 SK_i 是正确的。

证明 通过验证属性私钥子份额 $SK_{2,i}$ 是否为 $g^{\alpha_i + \beta d_i}$ 的形式，以及 $SK_{1,i}$、$SK_{3,m,i}$ 和 $SK_{2,i}$ 是否使用了同一个随机数，可判断属性私钥子份额的正确性。

若 P_i 颁发了正确的属性私钥子份额，则式(18)代入参数计算如式(20)所示，此时等式显然成立，说明 $SK_{2,i}$ 的生成使用了正确的系统参数 g^{α_i}、g^{β} 和 upk，并且和 $SK_{1,i}$ 使用了同一个随机数 d_i；若

其中存在一个参数不正确，则等式不成立，即说明该参与者颁发了错误的属性私钥子份额。式(19)代入参数计算如式(21)所示，若等式成立，说明 $\mathrm{SK}_{1,i}$ 和 $\mathrm{SK}_{3,m,i}$ 使用了同一个随机数 d_i；若等式不成立，则说明属性私钥子份额的颁发错误。证毕。

$$\begin{cases} e(\mathrm{sub\_sk}_i \mathrm{PK}_2^{d_i} \mathrm{upk}^k, g) \stackrel{?}{=} \\ \dfrac{e(g^{\beta}, g^{d_i}) e(g^{\alpha_i} \mathrm{pk}_i^{r_i}, g) e(\mathrm{upk}, g^k)}{e(\mathrm{pk}_i, g^{r_i})} \\ e(g^{\alpha_i} g^{\beta d_i} \mathrm{upk}^k, g) \stackrel{?}{=} \\ \dfrac{e(g^{\beta d_i}, g) e(g^{\alpha_i}, g) e(\mathrm{pk}_i^{r_i}, g) e(\mathrm{upk}, g^k)}{e(\mathrm{pk}_i, g^{r_i})} \\ e(g^{\alpha_i} g^{\beta d_i} \mathrm{upk}^k, g) \stackrel{?}{=} e(g^{\alpha_i}, g) e(g^{\beta d_i}, g) e(\mathrm{upk}^k, g) \end{cases} \tag{20}$$

$$\begin{cases} e(\mathrm{PK}_1, \mathrm{CSK}_{3,m,i}^2) \stackrel{?}{=} e(\mathrm{CSK}_{1,i}, h_m) e(\mathrm{CSK}_{3,m,i}^1, \mathrm{upk}) \\ e(g, h_m^{d_i} \mathrm{upk}^{s_m}) \stackrel{?}{=} e(g^{d_i}, h_m) e(g^{s_m}, \mathrm{upk}) \\ e(g, h_m^{d_i} \mathrm{upk}^{s_m}) \stackrel{?}{=} e(g, h_m^{d_i}) e(g, \mathrm{upk}^{s_m}) \end{cases} \tag{21}$$

定理5　式(18)和式(19)的验证是完备的。

证明　若 P_i 诚实生成并加密用户属性私钥，根据正确性分析，式(18)和式(19)一定能够被诚实的验证者验证通过。

$e(\mathrm{CSK}_{2,i}^2, \mathrm{PK}_1)$ 代入参数后可表示为 $e(g^{\alpha_i+\beta d_i} \mathrm{upk}^k, g)$，又有 $\mathrm{upk}^k = g^{\mathrm{usk}k}$，进一步计算得到 $e(\mathrm{CSK}_{2,i}^2, \mathrm{PK}_1) = e(g^{\alpha_i + \beta \cdot d_i + \mathrm{usk}k}, g)$。$\mathrm{CSK}_{2,i}^2$ 与 $\mathrm{CSK}_{1,i} = g^{d_i}$ 和 $\mathrm{CSK}_{2,i}^1 = g^k$ 相关，$\mathrm{CSK}_{1,i}$ 和 $\mathrm{CSK}_{2,i}^1$ 之间相互独立，且 d_i、k 为随机预言机模型下生成的随机数，对 $\mathrm{CSK}_{1,i}$，$\mathrm{CSK}_{2,i}^1$，$\mathrm{CSK}_{2,i}^2$ 的恶意篡改可以视为对 $\mathrm{CSK}_{2,i}^2$ 的篡改，即 $\mathrm{CSK}_{1,i}$，$\mathrm{CSK}_{2,i}^1$ 可以视为正确的。由于 β、usk、α_i 都有相应的承诺 $\mathrm{PK}_2 = g^{\beta}$、$\mathrm{upk} = g^{\mathrm{usk}}$、$e(g,g)^{\alpha_i}$，证明者需要构造 $\mathrm{fakeCSK}_{2,i}^2 = g^v$，$e(g^v, g) = e(g^{\alpha_i + \beta d_i + \mathrm{usk}k}, g)$ 才能欺骗验证者。已知双线性映射 e 是非退化的，所以一定有 $v = \alpha_i + \beta d_i + \mathrm{usk}k \pmod p$ 成立。有限域中的乘法和加法满足封闭性，所以 v 一定能拆解为 $\alpha_i + \beta d_i + \mathrm{usk}k \pmod p$ 形式，此时仍然是正确属性私钥子份额的ElGamal消息密文，因此恶意AA无法构造错误的属性私钥子份额欺骗诚实的验证者。同理，可证明式(19)的完备性。证毕。

3.5　验证方法安全性

定理6　验证参数的零知识性，即 CSK_i 不会造成信息泄露。

证明　由于 $\mathrm{CSK}_{1,i} = g^{d_i}$，根据DLP，目前难以在多项式时间内求解 d_i，所以 $\mathrm{CSK}_{1,i}$ 不会泄露有关属性私钥随机数 d_i 的信息。$(\mathrm{CSK}_{2,i}^1, \mathrm{CSK}_{2,i}^2)$ 和 $(\mathrm{CSK}_{3,m,i}^1, \mathrm{CSK}_{3,m,i}^2)$ 是对属性私钥 $\mathrm{SK}_{2,i}$ 和 $\mathrm{SK}_{3,m,i}$ 分别采用ElGamal加密后的结果，由引理1可知，ElGamal加密满足IND-CPA安全，所以在DLP下，CSK_i 是IND-CPA安全的。证毕。

定理7　验证的加密参数满足DLP下的IND-CPA安全。

证明　由于验证过程使用的参数都来自可聚合PVSS和ElGamal加密后的数据，所以安全性归结到基于ElGamal的可聚合PVSS的安全性。根据定理3得出，验证加密参数满足DLP下的IND-CPA安全。证毕。

4　密钥可公开验证MA-CP-ABE方案

在实际应用中，应当有一个可信的第三方提供公告板服务。联盟链通过多方维护账本，利用智能合约机制在链下实现数据上链前的校验，符合当前应用场景。MA-CP-ABE中的多个AA天然就是一个联盟，因此，本文方案以全部AA构成联盟链维护账本的形式来提供可信的公告板服务。

4.1　系统架构

密钥可公开验证MA-CP-ABE模型如图1所示。由图1可知，密钥可公开验证MA-CP-ABE模型由3类实体组成，分别为全局证书颁发机构（CA）、多个属性颁发机构（AA）和属性私钥申请者。属性私钥申请者又可分为数据拥有者（DO, data owner）和数据使用者（DU, data user）。CA和AA都单独作为组织，在CA的初始协调下加入同一条联盟链，AA和CA之间、AA和AA之间以及AA和用户之间均通过联盟链进行交互。DO和DU处于同一个用户属性私钥使用域中，其他主体的主要功能和文献[15]一致。

4.2　安全假设与安全模型

4.2.1　安全假设

假设AA中存在恶意者，且恶意AA数不超过 $t-1$。恶意AA可能在系统主密钥生成阶段进行错误的秘密共享，或者在属性私钥生成阶段分发错误的

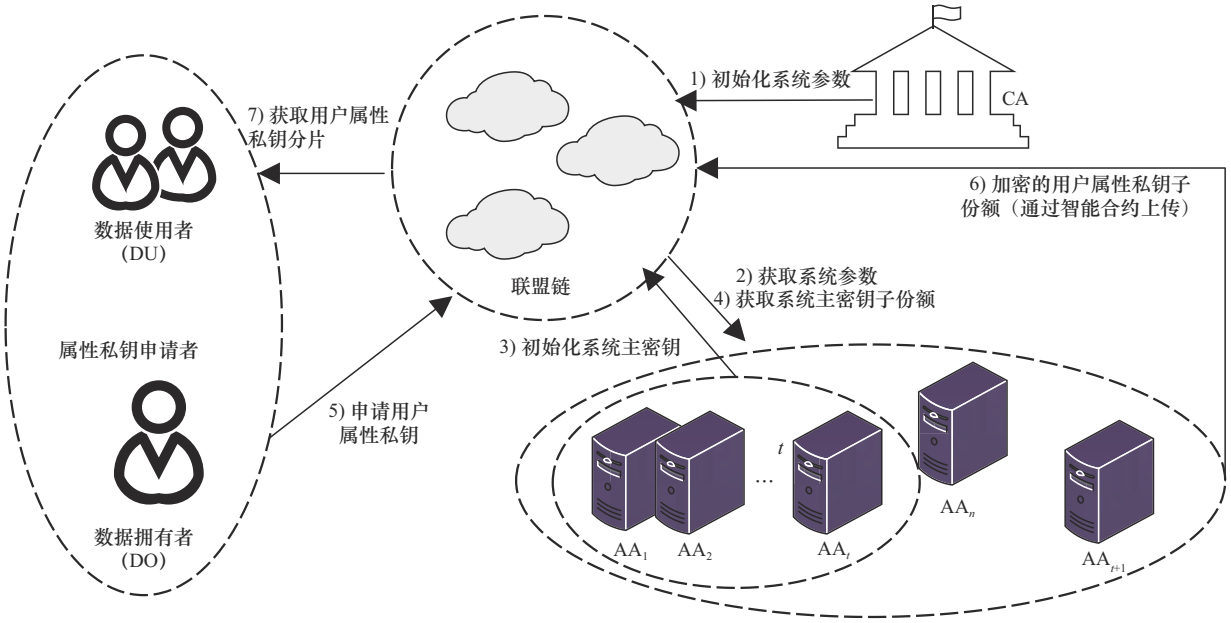


图1　密钥可公开验证MA-CP-ABE模型

属性私钥子份额，影响其他AA获取系统主密钥子份额或影响用户获取正确属性私钥。其他实体的安全假设与文献[15]和文献[17]一致。

4.2.2　安全模型

多个AA联合初始化系统主密钥和颁发属性私钥，属于分布式密钥生成（DKG, distributed key generation）协议，需要满足正确性、机密性、鲁棒性和活性[26]。假设系统中最多有f（f<t）个恶意AA，最坏的情况是他们私下串通。上述假设可以简化为一个敌手$\mathcal{A}$控制了f个AA。为了更为直观地描述敌手$\mathcal{A}$，考虑以下3种情形。

情形1　系统主密钥生成阶段。$\mathcal{A}$选择f（f<t）个AA进行腐败攻击，使它们遵守$\mathcal{A}$选择的任何协议，其他AA遵守原有协议。$\mathcal{A}$试图阻止系统主密钥生成阶段的秘密共享，影响系统主密钥MSK和系统主公钥PK的生成。

情形2　属性私钥生成阶段前。$\mathcal{A}$继续控制f（f<t）个AA，并且掌握PK；$\mathcal{A}$尝试获取有关系统主密钥MSK的信息。

情形3　属性私钥生成阶段。$\mathcal{A}$控制另外f（f<t）个AA，且失去对前阶段AA的控制，同样掌握PK，其他AA遵守属性私钥生成协议，$\mathcal{A}$试图阻止用户获得属性私钥子份额，或分发错误属性私钥子份额影响属性私钥计算。

4.3　方案流程

本节介绍基于可聚合PVSS和联盟链的密钥可公开验证MA-CP-ABE方案的执行流程，从系统初始化阶段到属性私钥分发完毕如图2所示。

4.3.1　系统初始化阶段

1) CA初始化系统公开参数。CA生成系统参数$\mathrm{GP}=\{p,G,G_T,g,h,u_1\}$，其中$p$为一个大素数，$G$是阶为$p$的乘法循环群，$e$:$G\times G\rightarrow G_T$为非退化的

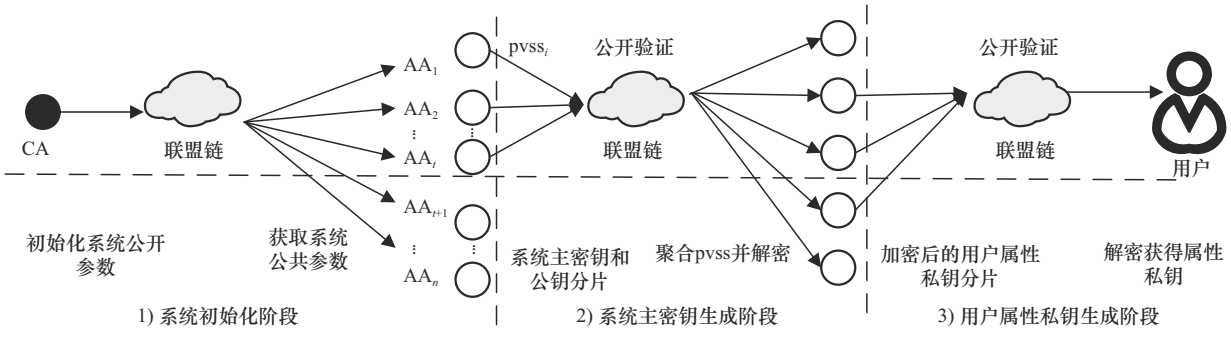


图2　方案流程

双线性映射，$u_1 \in G$；将GP打包上链。

2) AA初始化。每个AA从联盟链上获取GP；AA_i生成ElGamal加密的公私钥对(sk_i，pk_i)，将公钥发送给CA注册；CA验证通过后，生成一个全局唯一的aid_i，作为AA_i的ID；CA将AA_i对应的aid_i和pk_i上链。

3) 门限值选择。所有AA的集合用AASet表示，排序规则为加入联盟链的次序；CA根据注册AA的个数n，选择合适的门限值t后上链。

4) 选择初始化系统主密钥的AA集合。CA选择初始化系统主密钥的t个AA，记为SAASet。

4.3.2 系统主密钥生成阶段

1) 系统主密钥的初始化与公钥子份额分发

SAASet中所有AA_i各自选择一个多项式如式(22)所示，然后对AASet中所有的AA基于ElGamal的可聚合PVSS进行共享。AA_i对应AA_j的PVSS记录为$pvss_{i,j} = \{ F_{i,*},A_{i,j},Y_{i,j},u_{i,2}\}$，$i \in$ SAASet，$j \in$ AASet，并上链。

$$f_i(x) = a_{i,0} + a_{i,1}x^1 + \cdots + a_{i,t-1}x^{t-1} \bmod p \quad (22)$$

AA_i生成系统主公钥PK的相关参数$g^{\beta_i},\beta_i \in Z_p$后上链。通过式(14)计算$PK_2$，令$\beta = \prod \beta_i$，则$PK_2 = g^{\beta}$，且$\beta$保持机密。

2) PVSS记录的聚合与验证

AA_j对所有PVSS记录$pvss_{i,j}$进行聚合与验证，保证AA获取的系统主密钥子份额来自同一个聚合后的多项式。为了降低计算复杂度，AA_j先将所有$pvss_{i,j}$聚合为一个$pvss_{\sum,j}$，然后进行验证。聚合后相当于多个AA生成了一个如式(23)所示的多项式，其中$B(x) = \sum f_i(x)$。令$\alpha = b_0$，$\alpha_j = B(aid_j)$，通过该过程t个AA隐式生成了MA-CP-ABE系统主密钥$MSK = g^{\alpha}$。

$$B(x) = b_0 + b_1x^1 + \cdots + b_{t-1}x^{t-1}, b_x = \sum a_{i,x} \quad (23)$$

AA_j从联盟链中获取PVSS记录，聚合后的PVSS记录表示为$pvss_{\sum,j} = \{ F_{\sum,*},Y_{\sum,j},A_{\sum,j},u_{\sum,2}\}$，其中$j \in$ AASet。各部分的聚合过程如下。

$$F_{\sum,k} = \prod_{i \in \mathrm{SAASet}} F_{i,k} = h^{\sum_{i \in \mathrm{SAASet}} a_{i,k}} = h^{b_k}, k \in [0, t-1]$$

$$A_{\sum,j} = \prod_{i \in \mathrm{SAASet}} A_{i,j} = h^{\sum_{i \in \mathrm{SAASet}} f_i(\mathrm{aid}_j)} = h^{B(\mathrm{aid}_j)}$$

$$u_{\sum,2} = \prod_{i \in \mathrm{SAASet}} u_{i,2} = u_1^{\sum_{i \in \mathrm{SAASet}} a_{i,0}} = u_1^{b_0}$$

$Y_{\sum,j} = \prod_{i \in \mathrm{SAASet}} Y_{i,j}$的聚合过程如下。

$$\begin{cases} Y^1_{\sum,j} = g^{\sum_{i \in \mathrm{SAASet}} r_{i,j}} = g^{r_{\sum,j}} \\ Y^2_{\sum,j} = g^{\sum_{i \in \mathrm{SAASet}} f_i(\mathrm{aid}_j)} \mathrm{pk}_j^{\sum_{i \in \mathrm{SAASet}} r_{i,j}} = g^{\alpha_j} \mathrm{pk}_j^{r_{\sum,j}} \\ Y^3_{\sum,j} = h^{\sum_{i \in \mathrm{SAASet}} r_{i,j}} = h^{r_{\sum,j}} \end{cases}$$

此时，等价于一个AA对n个AA针对多项式$B(x)$利用基于ElGamal的可聚合PVSS共享系统主密钥。AA_j根据式(2)~式(6)验证聚合后的PVSS记录，如果等式都成立，则验证通过；否则验证失败，并向联盟链发送验证失败的信息，进而根据式(6)分别验证$pvss_{i,j}$定位到错误的PVSS记录，再依据联盟链记录追踪到对应的作恶AA。

3) 各AA获取系统主密钥子份额

聚合验证后，AA_j计算自身的系统主密钥子份额sub_sk_j，解密过程参考式(7)得到式(24)。

$$\mathrm{sub\_sk}_j = \frac{Y^2_{\sum,j}}{(Y^1_{\sum,j})^{\mathrm{sk}_j}} \quad (24)$$

4) 系统主公钥PK的生成

PK_3的生成参考式(16)，只需要选择达到门限值个数的AA公开参数进行计算，统一选择SAASet中的AA，得到式(25)。综合式(14)，各方得到系统主公钥PK: $\{ PK_1 = g, PK_2, PK_3\}$。

$$\mathrm{PK}_3 = \prod_{j \in \mathrm{SAASet}} \{ \frac{e(Y^2_{\sum,j}, g)}{e(\mathrm{pk}_j, Y^1_{\sum,j})} \}^{\Delta w_j(0)} \quad (25)$$

最后，SAASet中的AA将销毁多项式相关参数。

4.3.3 用户属性私钥生成阶段

1) 用户注册。用户u向CA注册全局唯一的ID表示为uid_u，ElGamal公私钥对为(usk_u,$upk_u = g^{\mathrm{usk}_u}$)，用户ID和公钥由CA上链。

2) 用户申请属性私钥。用户选择至少t个AA，发送自己签名的属性证明申请属性私钥。

3) AA颁发属性私钥子份额。AA_j收到用户申请属性私钥的信息后，验证该用户的属性是否属实。若通过，则生成属性私钥子份额SK_j；否则，不响应，详细流程如下。

AA_j计算$SK_{1,j}$、$SK_{2,j}$和$SK_{3,m,j}$，对应的值分别为$PK_1^{d_j}$、$sub_sk_j PK_3^{d_j}$和$h_m^{d_j}$。然后，加密$SK_{2,j}$和所有的$SK_{3,m,j}$，得到CSK_j如下。

$$\mathrm{CSK}_{1,j}=\mathrm{PK}_1^{d_j}$$

$$\begin{cases}\mathrm{CSK}_{2,j}^1=g^{k_j}\\ \mathrm{CSK}_{2,j}^2=\mathrm{SK}_{2,j}\mathrm{upk}_u^{k_j}\end{cases}$$

$$\begin{cases}\mathrm{CSK}_{3,m,j}^1=g^{s_{m,j}}\\ \mathrm{CSK}_{3,m,j}^2=h_m^{d_j}\mathrm{upk}^{s_{m,j}}\end{cases}$$

最后，将CSK_j与用户uid_u和AA_j绑定后上链。

4) 公开验证属性私钥子份额。参考式(18)和式(19)所示的属性私钥公开验证方法，应用到该方案后如式(26)和式(27)所示。

$$e(\mathrm{CSK}_{2,j}^2,\mathrm{PK}_1)\stackrel{?}{=}\frac{e(\mathrm{PK}_2,\mathrm{CSK}_{1,j})e(Y_{\sum,j}^2,g)e(\mathrm{upk}_u,\mathrm{CSK}_{2,j}^1)}{e(\mathrm{pk}_j,Y_{\sum,j}^1)}\tag{26}$$

$$e(\mathrm{PK}_1,\mathrm{CSK}_{3,m,j}^2)\stackrel{?}{=}e(\mathrm{CSK}_{1,j},h_m)e(\mathrm{CSK}_{3,m,j}^1,\mathrm{upk}_u)\tag{27}$$

当式(26)和式(27)同时成立时，可视为一个对uid_u正确的属性私钥子份额。若不通过，则表示AA_i在属性私钥颁发过程中存在恶意行为，任何用户都可以在密文条件下验证AA_j颁发给uid_u的属性私钥子份额的正确性，因此能够将该过程写入智能合约中。只有通过验证的密文数据才能执行上链操作，保证链上的属性私钥子份额密文都是正确的、有效的属性私钥子份额。

用户uid_u选择t个AA在联盟链上查询有关自身的属性私钥子份额，实现可信的查询，获取足够的属性私钥子份额计算生成完整的属性私钥。因为链上属性私钥子份额密文都是通过验证的，保证了正确性。因此，若用户提供的证明无误，而恶意AA不响应，也可以直接定位到该恶意AA，这里不对该情形进行叙述。

5) 用户解密获取属性私钥。用户uid_u在接收到选择的t个经过验证的属性私钥子份额后，计算自己的属性私钥（用AAs表示参与属性私钥生成的t个AA集合）。用$\mathrm{CSK}_\sum$表示CSK_j聚合后的结果如式(28)所示，解密过程如式(29)所示。

$$\mathrm{CSK}_\sum=\prod^{j\in\mathrm{AAs}}(\mathrm{CSK}_j)^{\Delta w_j(0)}\tag{28}$$

$$\left\{\mathrm{CSK}_{1,\sum};\frac{\mathrm{CSK}_{2,\sum}^2}{(\mathrm{CSK}_{2,\sum}^1)^{\mathrm{usk}_u}};\frac{\mathrm{CSK}_{3,m,\sum}^2}{(\mathrm{CSK}_{3,m,\sum}^1)^{\mathrm{usk}_u}}\right\}\tag{29}$$

4.3.4 加解密过程

本文没有对基础的MA-CP-ABE加解密过程进行改动，具体加解密过程参考文献[15]。

4.4 正确性与安全性证明

定理 8 t个诚实AA颁发的属性私钥子份额能够生成正确的属性私钥。

证明 若t个$\mathrm{AA}_j,j\in[0,t-1]$为用户$\mathrm{uid}_u$颁发了正确的属性私钥子份额，计算属性私钥如下。

$$\mathrm{CSK}_{1,\sum}=\prod^{j\in\mathrm{AAs}}(\mathrm{CSK}_{1,j})^{\Delta w_j(0)}=g^{\sum^{j\in\mathrm{AAs}}d_j\Delta_j(0)}=g^d,d=\sum^{j\in\mathrm{AAs}}\Delta w_j(0)d_j$$

$$\mathrm{CSK}_{2,\sum}^1=\prod^{j\in\mathrm{AAs}}(\mathrm{CSK}_{2,\sum}^1)^{\Delta w_j(0)}=\prod^{j\in\mathrm{AAs}}(g^{k_j})^{\Delta w_j(0)}=g^{\sum^{j\in\mathrm{AAs}}\Delta w_j(0)k_j}=g^k,k=\sum^{j\in\mathrm{AAs}}\Delta w_j(0)k_j$$

$$\mathrm{CSK}_{2,\sum}^2=\prod^{j\in\mathrm{AAs}}(\mathrm{CSK}_{2,\sum}^2)^{\Delta w_j(0)}=\prod^{j\in\mathrm{AAs}}(\mathrm{SK}_{2,j}\mathrm{upk}_u^{k_j})^{\Delta w_j(0)}=\prod^{j\in\mathrm{AAs}}(\mathrm{sub\_sk}_j\mathrm{PK}_3{}^{d_j}\mathrm{upk}_u^{k_j})^{\Delta w_j(0)}=g^{\sum^{j\in\mathrm{AAs}}\Delta w_j(0)\alpha_j}g^{\sum^{j\in\mathrm{AAs}}\Delta w_j(0)\beta d_j}\mathrm{upk}_u^{\sum^{j\in\mathrm{AAs}}\Delta w_j(0)k_j}g^{\alpha}g^{\beta d}\mathrm{upk}^k$$

$$\mathrm{CSK}_{3,m,\sum}^1=\prod^{j\in\mathrm{AAs}}(\mathrm{CSK}_{3,m,\sum}^1)^{\Delta w_j(0)}=\prod^{j\in\mathrm{AAs}}(g^{s_{m,j}})^{\Delta w_j(0)}=g^{\sum^{j\in\mathrm{AAs}}\Delta w_j(0)s_{m,j}}=g^{s_m},s_m=\sum^{j\in\mathrm{AAs}}\Delta w_j(0)s_{m,j}$$

$$\mathrm{CSK}_{3,m,\sum}^2=\prod^{j\in\mathrm{AAs}}(\mathrm{CSK}_{3,m,\sum}^2)^{\Delta w_j(0)}=h_m^{\sum^{j\in\mathrm{AAs}}s_{m,j}\Delta w_j(0)}=h_m^d\mathrm{upk}_u^{s_m}$$

通过式(29)解密得到属性私钥如式(30)所示，解密结果符合MA-CP-ABE[15]中属性私钥的定义。只要AA_j按照既定方式为用户颁发属性私钥子份额，则该属性私钥子份额有效，能够作为有效子份额恢复出完整、正确的属性私钥。证毕。

$$\{\mathrm{SK}_1=g^d;\mathrm{SK}_2=g^{\alpha}g^{\beta d};\mathrm{SK}_{3,m}=h_m^d\}\tag{30}$$

引理2　在系统主密钥生成阶段，任意f（$f<t$）个恶意AA无法阻碍系统的构建。

证明　f（$f<t$）个恶意AA可以生成任意的PVSS记录从而影响系统主密钥生成。该行为能够通过基于ElGamal的可聚合PVSS的验证发现，并定位到作恶AA，随后可重新选择另外一个AA替代该AA参与系统主密钥生成。证毕。

引理3　（正确性C1）当恶意节点数量$f<t$时，SAASet中所有AA定义了唯一的MSK和PK。

证明　根据引理2可知，最终完成系统主密钥分发的SAASet中AA的行为一定都符合预定协议。通过多项式系数隐式相加，定义了唯一的MSK和PK。证毕。

引理4　（正确性C1'）诚实的t个AA能够重构出系统主密钥MSK。

证明　经过验证PVSS记录，每个AA都获得了以自身ID为输入的多项式$B(x)$值。如果收集到$s\geq t$个诚实用户的秘密子份额，则能够通过拉格朗日插值恢复出系统主密钥g^{α}。对于β，只需要用到公开值g^{β}，任何用户都可以获取。综上，诚实的t个AA能够重构出系统主密钥MSK。证毕。

引理5　（正确性C2）系统主密钥生成阶段完成后，所有联盟链参与者能够获得唯一系统主公钥PK。

证明　系统主公钥为PK: $\{PK_1,PK_2,PK_3\}$，其中，PK_1由初始CA生成并上传到联盟链中，所有用户能够获得一致的PK_1；PK_2和PK_3通过公开的PVSS记录计算，由引理3可知，PK_1、PK_2和PK_3是唯一的，所以系统中所有用户能够获得唯一的PK。证毕。

引理6　（正确性C3）α和β均匀分布在Z_p中，g^{α}均匀分布在G中，$PK_3=e(g,g)^{\alpha}$均匀分布在G_T中，$PK_2=g^{\beta}$均匀分布在G中。

证明　$PK_3=e(g,g)^{\alpha}$，$PK_2=g^{\beta}$，其中，α和β是由SAASet中的t个AA隐式生成的。当存在f（$f<t$）个恶意节点时，根据鸽巢原理，SAASet中至少有一个诚实节点会随机生成α_i和β_i，所以α和β可以视为均匀分布在Z_p中的随机数。因此，α和β均匀分布在Z_p中，进而推出g^{α}均匀分布在G中，$PK_3=e(g,g)^{\alpha}$均匀分布在G_T中，$PK_2=g^{\beta}$均匀分布在G中。证毕。

引理7　（机密性）任意$f<t$个AA都无法重构出系统主密钥MSK，即MSK对任何少于t的AA集合都是保密的。

证明　系统隐式生成的主密钥为$MSK=g^{\alpha}$，系统主公钥的重要参数为β，α和β是由SAASet中t个AA合作生成的，且由引理6可知，α和β随机分布在Z_p中，只有2种方式可获取α和β的值，分别为SAASet中的t个AA合谋直接以原始秘密值恢复α和β，或者t个及以上的AA合谋通过拉格朗日插值恢复g^{α}。

安全假设中恶意节点$f<t$，系统主密钥生成阶段存在$t-f$（大于或等于1）个诚实的AA，诚实AA在完成系统主密钥生成后，将有关系统主密钥的参数销毁了，因此无法从SAASet中获取α和β。

通过拉格朗日插值恢复MSK需要有至少t个AA共同参与；因此，任意$f<t$个AA都无法获取系统主密钥MSK。证毕。

引理8　（鲁棒性）即使有f（$f<t$)个恶意AA，任何$s\geq t$个诚实方都可以为合法用户生成正确的属性私钥。

证明　用户可以自由选择属性私钥生成的t个AA。在密文条件下，通过智能合约公开验证属性私钥子份额的正确性，AA恶意生成的属性私钥子份额无法上链，且能够及时定位作恶AA。当用户在一定时间内收不到对应AA属性私钥子份额时，会选择另外一个AA替代该AA加入属性私钥生成的集合，其余没有作恶的AA不需要重新生成属性私钥。因此，恶意AA不会影响属性私钥生成。证毕。

引理9　（活性）任何f个恶意AA无法阻止$s\geq t$个诚实AA为用户生成正确的属性私钥。

证明　根据引理8，恶意AA在颁发属性私钥子份额时的恶意行为能够被MA-CP-ABE属性私钥可公开验证方法及时发现，进而替换处理，所以恶意AA无法影响诚实AA的属性私钥分发。证毕。

定理9　（主定理）对于给定的密钥可公开验证MA-CP-ABE方案，在存在自适应攻击者$\mathcal{A}$的情况下，存在安全的分布式密钥生成协议。

证明　由引理3可知，控制f个AA的攻击者$\mathcal{A}$无法阻止系统主密钥生成阶段的完成。因此，在情形1中，$\mathcal{A}$无法破坏系统主密钥生成。通过引理6和引理7，证明了即使$\mathcal{A}$控制了f（$f<t$）个

AA，MSK都是保持机密的。因此，$\mathcal{A}$在情形2中没有优势；通过引理4和引理5，证明了可以在没有f（$f<t$）个恶意AA的参与下有效地为用户生成属性私钥，并获取正确的系统主公钥；通过引理8和引理9，可以证明即使f个AA发布无效的属性私钥子份额，也可以通过公开验证发现，并重新选择AA生成。因此，$\mathcal{A}$在情形3中没有优势。证毕。

4.5 方案对比与分析

本文方案引入Hyperledger Fabric（简称Fabric）联盟链作为可信备份，生成系统主密钥时总共有t个PVSS记录，Raft共识的通信复杂度为$O(n)$，所以系统主密钥初始化通信开销为$O(tn)$。本文方案与现有基于门限的MA-CP-ABE方案比较如表1所示。

由表1可以看出，本文在考虑系统主密钥生成阶段和用户属性私钥生成阶段恶意AA的基础上，优化了基于门限的MA-CP-ABE系统主密钥初始化阶段的通信开销；所有的信息加密存储在联盟链上，对与之无关的用户保密，形成了AA行为的公开记录，能够追溯到作恶AA并提供不可否认的证据；保证了较低的系统主密钥子份额验证时间，能够公开验证系统主密钥生成阶段各AA的秘密子份额颁发的正确性；能够在属性私钥颁发阶段公开验证AA颁发的私钥子份额是否正确，可以防止恶意AA的时延攻击，能够限制恶意AA的行为。

4.6 测试分析

测试环境为Ubuntu 20.10操作系统，内存为6 GB，使用JPBC库的TypeA型双线性映射。Fabric默认提供Raft共识机制，智能合约可以实现数据上链前的验证，因此，测试方案中的联盟链采用Fabric。由于Fabric链上存储数据为String类型，上链群元数据需要进行Base64编码并转为String类型后方可上链存储；获取链上群元数据则执行上述逆过程，然后映射到群G或G_T上即可。

功能测试采用10个AA，门限值设置为5，链下仿真测试结果如图3所示。

初始5个AA选择多项式如图3(a)所示，5个多项式逐项相加即为隐式生成的多项式。这5个AA分别利用生成的多项式采取基于ElGamal的可聚合PVSS进行系统主密钥相关秘密值的共享，各PVSS记录的聚合如图3(b)所示，聚合验证获取系统主密钥子份额如图3(c)所示。

系统主密钥子份额分发完成后，下一步是为属性私钥申请者颁发相应的属性私钥。为了确保属性私钥的完整性和正确性，需对每个属性私钥子份额的正确性进行验证。设置属性私钥申请者的属性个数为5，生成用户属性私钥后的验证如图3(d)所示。验证通过后，属性私钥申请者解密用户属性私钥子份额如图3(e)所示。

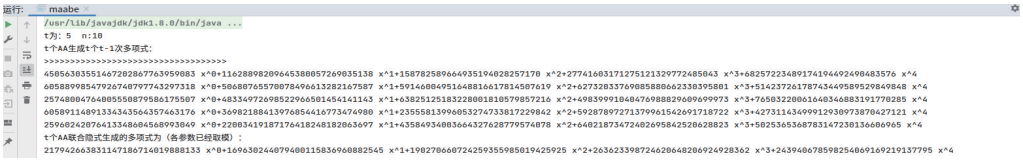
利用Fabric联盟链的智能合约，在用户属性私钥上链前验证正确性；修改正确子份额，则验证失败，无法执行后续上链，如图3(f)所示。

5 结束语

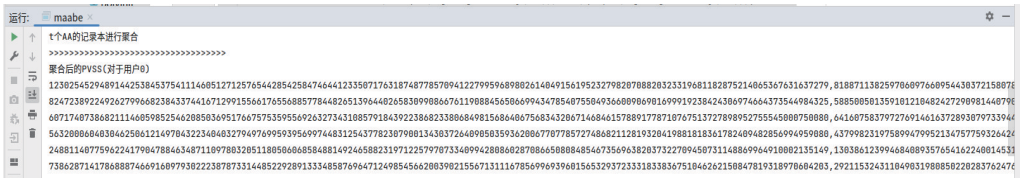
本文提出了一种基于可聚合PVSS和联盟链的密钥可公开验证MA-CP-ABE方案。基于可聚合PVSS分发系统主密钥，实现了系统主密钥子份额密文条件下的公开可验证，利用其聚合性质缩短了系统主密钥子份额的验证时间；初始AA数量降到门限阈值t，降低了MA-CP-ABE系统主密钥初始化阶段的通信量，进一步缩短了验证时间。基于双线性映射的双线性构造了MA-CP-ABE属性私钥可公开验证方法，实现了AA行为的可公开验证，预防AA恶意行为威胁系统。通过联盟链进行通信交互和可信备份，实现了公开验证参数的难以篡改和可追溯。

表1 方案对比分析

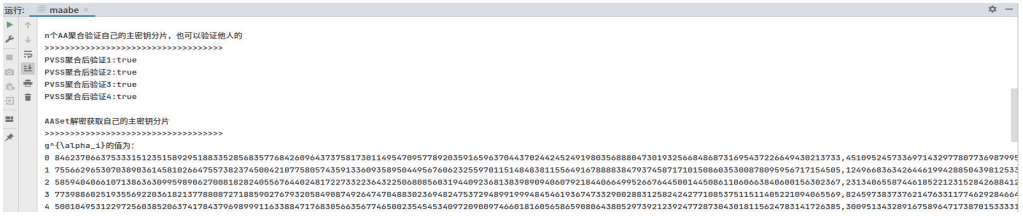
方案	系统主密钥初始化通信开销	AA行为的难以篡改和可追溯	系统主密钥子份额		属性私钥子份额公开验证
			不可公开验证	可公开验证	
文献[15]	$O(n^2)$	×	√	×	×
文献[17]	$O(n^2)$	×	×	×	×
文献[16]	$O(n^2)$	×	×	×	×
文献[18]	$O(n^2)$	×	√	×	×
本文方案	$O(tn)$	√	√	√	√



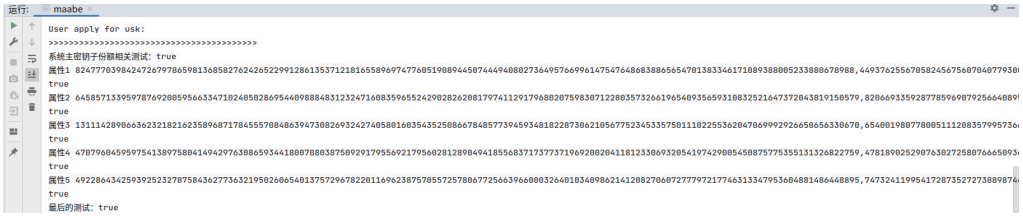
(a) 多项式



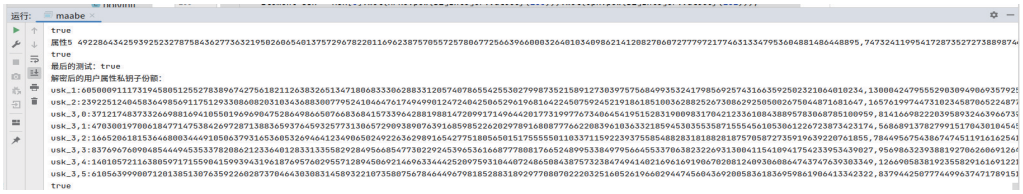
(b) PVSS记录的聚合



(c) 聚合验证获取系统主密钥子份额



(d) 用户属性私钥验证



(e) 解密用户属性私钥子份额

(f) 智能合约验证

图3　功能测试

参考文献:

[1] YANG K, JIA X H. Expressive, efficient, and revocable data access control for multi-authority cloud storage[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(7): 1735-1744.

[2] OBERKO P S K, OBENG V H K S, XIONG H. A survey on multi-authority and decentralized attribute-based encryption[J]. Journal of Ambient Intelligence and Humanized Computing, 2022, 13(1): 515-533.

[3] 崔皓宇, 马利民, 王佳慧, 等. 基于区块链的属性加密多授权机构安全模型研究[J]. 信息网络安全, 2022(5): 84-93.
CUI H Y, MA L M, WANG J H, et al. Research on the security model of multi-authority for attribute encryption based on blockchain[J]. Netinfo

Security, 2022(5): 84-93.

[4] 李学俊, 吕茂旭. 移动云环境下的多授权机构属性基加密方案[J]. 计算机应用研究, 2018, 35(5): 1519-1525, 1544.
LI X J, LYU M X. Multi-authority attribute-based encryption scheme in mobile cloud environment[J]. Application Research of Computers, 2018, 35(5): 1519-1525, 1544.

[5] GUO Z Z, WANG G L, LI Y X, et al. Accountable attribute-based data-sharing scheme based on blockchain for vehicular ad hoc network[J]. IEEE Internet of Things Journal, 2023, 10(8): 7011-7026.

[6] CHASE M. Multi-authority attribute based encryption[C]//Theory of Cryptography Conference. Berlin: Springer, 2007: 515-534.

[7] HUANG X F, TAO Q, QIN B D, et al. Multi-authority attribute based encryption scheme with revocation[C]//Proceedings of the 2015 24th International Conference on Computer Communication and Networks (ICCCN). Piscataway: IEEE Press, 2015: 1-5.

[8] 吴光强. 适合云存储的访问策略可更新多中心CP-ABE方案[J]. 计算机研究与发展, 2016, 53(10): 2392-2398.
WU G Q. Multi-authority CP-ABE with policy update in cloud storage[J]. Journal of Computer Research and Development, 2016, 53(10): 2392-2398.

[9] XUE K P, XUE Y J, HONG J N, et al. RAAC: robust and auditable access control with multiple attribute authorities for public cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(4): 953-967.

[10] WANG C, JIN H, WEI R L, et al. Revocable, dynamic and decentralized data access control in cloud storage[J]. The Journal of Supercomputing, 2022, 78(7): 10063-10087.

[11] LEWKO A, WATERS B. Decentralizing attribute-based encryption[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2011: 568-588.

[12] 闫玺玺, 刘媛, 李子臣, 等. 支持隐私保护的多机构属性基加密方案[J]. 计算机研究与发展, 2018, 55(4): 846-853.
YAN X X, LIU Y, LI Z C, et al. Multi-authority attribute-based encryption scheme with privacy protection[J]. Journal of Computer Research and Development, 2018, 55(4): 846-853.

[13] DATTA P, KOMARGODSKI I, WATERS B. Fully adaptive decentralized multi-authority ABE[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2023: 447-478.

[14] LIN H, CAO Z F, LIANG X H, et al. Secure threshold multi authority attribute based encryption without a central authority[J]. Information Sciences, 2010, 180(13): 2618-2632.

[15] LI W, XUE K P, XUE Y J, et al. TMACS: a robust and verifiable threshold multi-authority access control system in public cloud storage[J]. IEEE Transactions on Parallel and Distributed Systems, 2016, 27(5): 1484-1496.

[16] GU J, SHEN J Q, WANG B Y. A robust and secure multi-authority access control system for cloud storage[J]. Peer-to-Peer Networking and Applications, 2021, 14(3): 1488-1499.

[17] RAMESH D, MISHRA R, TRIVEDI M C. PCS-ABE (t, n): a secure threshold multi authority CP-ABE scheme based efficient access control systems for cloud environment[J]. Journal of Ambient Intelligence and Humanized Computing, 2021, 12(10): 9303-9322.

[18] 唐飞, 包佳立, 黄永洪, 等. 基于属性的多授权中心身份认证方案[J]. 通信学报, 2021, 42(3): 220-228.
TANG F, BAO J L, HUANG Y H, et al. Multi-authority attribute-based identification scheme[J]. Journal on Communications, 2021, 42(3): 220-228.

[19] GURKAN K, JOVANOVIC P, MALLER M, et al. Aggregatable distributed key generation[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2021: 147-176.

[20] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[C]//International Workshop on Public Key Cryptography. Berlin: Springer, 2011: 53-70.

[21] 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.

[22] 刘明达, 陈左宁, 拾以娟, 等. 区块链在数据安全领域的研究进展[J]. 计算机学报, 2021, 44(1): 1-27.
LIU M D, CHEN Z N, SHI Y J, et al. Research progress of blockchain in data security[J]. Chinese Journal of Computers, 2021, 44(1): 1-27.

[23] CASCUDO I, DAVID B. SCRAPE: scalable randomness attested by public entities[C]//International Conference on Applied Cryptography and Network Security. Berlin: Springer, 2017: 537-556.

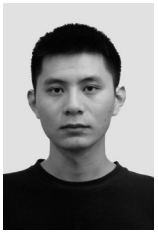
[24] FELDMAN P. A practical scheme for non-interactive verifiable secret sharing[C]//Proceedings of the 28th Annual Symposium on Foundations of Computer Science (sfcs 1987). Piscataway: IEEE Press, 1987: 427-438.

[25] 柯唯阳, 石润华. 基于测量设备无关的可认证身份量子投票方案[J]. 软件学报, 2023, 34(11): 5376-5391.
KE W Y, SHI R H. Measurement-device-independent quantum voting scheme with identity authentication[J]. Journal of Software, 2023, 34(11): 5376-5391.

[26] ZHANG L, QIU F Y, HAO F, et al. 1-round distributed key generation with efficient reconstruction using decentralized CP-ABE[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 894-907.

[作者简介]

景旭（1971– ），男，陕西咸阳人，博士，西北农林科技大学副教授、硕士生导师，主要研究方向为区块链技术、隐私保护、访问控制、信息系统安全等。



蒋炎（1999– ），男，湖南长沙人，西北农林科技大学硕士生，主要研究方向为区块链技术、访问控制等。