基于代理重加密的云端多要素访问控制方案

苏铓[1]，史国振[2]，付安民[1]，俞研[1]，金伟[3]

（1. 南京理工大学计算机科学与工程学院，江苏 南京 210094；
2. 北京电子科技学院信息安全系，北京 100070；3. 中国科学院信息工程研究所，北京 100093）

摘 要：云服务是天地一体化信息网络的重要应用形式之一，用户可以通过云快捷、方便地获取信息和服务。云端数据的机密性、完整性直接关系到天地一体化信息网络的数据安全，所以云端数据多以密文形式进行流通。云端访问控制技术的研究则需要面向密文数据，同时兼顾复杂环境下的多要素描述需求。以此为背景，结合代理重加密技术，提出一种云端多要素访问控制（PRE-MFAC, proxy re-encryption based multi-factor access control）方案，首先，明确设计目标和前提假设；其次，构造具体方案，描述 PRE-MFAC 系统模型和相关算法；最后，对 PRE-MFAC 的安全性、特点进行比较分析。PRE-MFAC 通过将代理重加密技术和多要素访问控制融合，实现云端密文数据的多要素化授权管理，同时，充分发挥云端服务器的运算和存储能力，降低个人用户加解密运算量和密钥管理难度。

关键词：代理重加密；多要素；访问控制；云计算；天地一体化信息网络

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000-436x.2018028

Proxy re-encryption based multi-factor access control scheme in cloud

SU Mang[1], SHI Guozhen[2], FU Anmin[1], YU Yan[1], JIN Wei[3]

1. School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China
2. School of Information Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China
3. Institute of Information Engineering, CAS, Beijing 100093, China

Abstract: Cloud computing is one of the space-ground integration information network applications. Users can access data and retrieve service easily and quickly in cloud. The confidentiality and integrity of the data cloud have a direct correspondence to data security of the space-ground integration information network. Thus the data in cloud is transferred with encrypted form to protect the information. As an important technology of cloud security, access control should take account of multi-factor and cipher text to satisfy the complex requirement for cloud data protection. Based on this, a proxy re-encryption based multi-factor access control (PRE-MFAC) scheme was proposed. Firstly, the aims and assumptions of PRE-MFAC were given. Secondly, the system model and algorithm was defined. Finally, the security and properties of PRE-MFAC were analyzed. The proposed scheme has combined the PRE and multi-factor access control together and realized the multi-factor permission management of cipher text in cloud. Meanwhile, it can make the best possible use of cloud in computing and storing, then reduce the difficulty of personal user in cryptographic computing and key managing.

Key words: proxy re-encryption, multi-factor, access control, cloud computing, space-ground integration information network

收稿日期：2017-11-08；**修回日期**：2018-01-10

通信作者：史国振，sgz@besti.edu.cn

基金项目：国家重点研发计划基金资助项目（No.2016YFB0800303）；国家自然科学基金资助项目（No.61702266, No.61572255）；江苏省自然科学基金资助项目（No.BK20150787, No.BK20141404）；北京市自然科学基金资助项目（No.4152048）

Foundation Items: The National Key Research and Development Program of China (No.2016YFB0800303), The National Natural Science Foundation of China (No.61702266, No.61572255), The Natural Science Foundation of Jiangsu Province (No.BK20150787, No.BK20141404), The Natural Science Foundation of Beijing (No.4152048)

1　引言

天地一体化信息网络集成了天基骨干网、天基接入网、地基节点网和互联网、移动通信网等地面网络，全方位地扩展了人类信息的传播范围[1]。天地一体化信息网络的构建将提升现有信息系统的数据传播空间，使其由原有的地面互联互通转变为在陆、海、空、天等不同维度空间的多维联动。作为现有信息系统的主要应用形式之一，云具有海量的存储能力和超强的运算能力，天地一体化信息网络的建设将使云服务的领域和范畴更为丰富和多样化，用户则可以通过云进行随时随地的数据交互和个性化运算，真正实现云服务的“招之即来，挥之即去”。但是，天地一体化信息网络的异构、开放和高度融合性也为云端数据的保障带来了更为严峻的安全形势。首先，云用户接入网络的方式将更加多要素化和随机化，管理和控制的难度更大。云端数据管理需要考虑更加复杂的要素，仅通过用户名、口令的形式已经远不能满足云端主客体的特征描述需求，角色、时态、物理环境、网络属性、资源安全级别甚至陆、海、空、天的多维信息等均成为云端数据安全管理考虑的范畴。其次，云端数据量会随着网络的复杂化激增，随之而来的机密数据和隐私信息也将越来越多。存储和传输技术形态需要更加注重密文数据的特征，云计算环境下，用户将自身数据的运算、管理托管到云服务器，大大减轻了个人用户在数据处理过程中的资源消耗和时间损失，同时也带来隐私数据被泄露的风险。云端数据往往以密文的形态存在，因此，需要关注如何针对密文数据进行保护和处理。

访问控制通过对用户的资源访问活动进行有效监控，实现了对云数据安全性和云服务可靠性的保障，是云安全系统的基础核心服务，具有非常重要的地位和作用。同时，基于上述云环境的全新安全问题，访问控制技术的研究也面临多要素化和密文化的挑战。针对云计算环境的特点，以天地一体化信息网络为基础的云端访问控制方案设计主要应满足以下需求。

1) 能够描述天地一体化带来的多种复杂访问控制要素及其约束关系。如云计算环境下时间、物理环境、网络属性以及各个空间和维度带来的复杂要素及其约束关系。

2) 能够针对密文数据进行管理。访问控制机制应与密码技术结合，否则将导致访问控制描述策略与数据加解密相互脱节的问题。如用户定义了基于时态的访问控制，而数据的加密以身份信息为密钥。

3) 访问控制方案的部署和实施要考虑个人用户的加解密运算能力和密钥管理能力，充分发挥云服务器的运算和存储能力。

针对上述需求，出现了大量的模型和方案，例如，针对时间要素的重要性，出现了基于时态特性的 RBAC（TRBAC, temporal role-based access control）模型及其扩展模型[2]等，将为云计算环境下访问控制模型的构建提供参考。文献[3]提出了 CARBAC 模型，将角色属性划分为用户和数据所有者，细化了角色要素的描述，但是该模型要求数据所有者具有很强的计算能力，没有发挥云强大的计算优势。Luo 等[4]提出了 SAT-RBAC 模型，将用户、环境、系统状态之间的信任关系作为重要的访问控制要素，并将信任关系依据云环境的特征进行了划分。针对位置信息，Li 等[5]通过对云端存储位置的约束对其数据进行安全保护。上述文献均以云端访问控制多要素化为需求，以不同的侧重点阐述了相关模型和机制，但是并未提及如何针对密文数据进行管理。而针对密文数据的云端访问控制，通常以数据所有者在使用云服务前将数据进行加密处理为前提，出现了基于角色加密[6]、IBE、ABE 等机制。例如，文献[7]中数据所有者将数据加密存储到云服务器中，只有特定角色的用户才可以对数据进行解密从而获得明文。此类模型和方案完全依赖用户自身进行数据密文的产生、密钥的产生、数据的解密等运算，严重消耗个人用户的资源和时间。同时细粒度化的密文访问控制带来了大量的密钥，个人用户将耗费大量的精力进行各类密钥的管理，同时闲置云服务器的运算能力，导致云仅成为数据转存的中心，无法发挥其优势。

在天地一体化这一立体化、全方位的复杂环境下，用户的数据管理除了面临角色、时态、物理位置、网络状态等传统访问控制要素之外，还需要考虑不同网络边界、跨域等复杂要素。针对上述现状和需求，本文结合代理重加密技术，提出一种云端多要素访问控制方案（PRE-MFAC），从而实现在复杂云环境下密文数据的多要素访问控制管理，同时，将云服务器作为访问控制实施的主体，减轻终端用户的运算负担和密钥管理难度。首先，给出 PRE-MFAC 的设计目标和假设，明确研究的目的和

前提条件；其次，构造具体方案，描述系统模型和相关算法；最后，对 PRE-MFAC 的特征、优缺点进行分析。本文提出的 PRE-MFAC 将为云计算环境提供细粒度、多要素的数据保障，进而成为天地一体化信息网络数据安全研究的重要基础。

2 相关技术

代理重加密（PRE, proxy re-encryption）技术基于公钥密钥体制，首先，数据创建者 A 产生由其自身公钥加密产生的密文 C_A；其次，A 将 C_A 提交给代理服务器，重加密后产生可由用户 B 解密的重加密密文 $C_{A\to B}$，这个过程中 A 仅需要进行一次加密运算，产生密文 C_A，然后将加密的工作托管给代理，代理服务器仅具有 A 数据的密文 C_A，无法获取明文，确保了 A 的数据机密性，同时也减轻了 A 的运算量。这样的工作原理适用于云环境中密文访问控制充分发挥云服务器运算能力，同时确保数据安全性的需求，借助云计算平台强大的运算能力，减轻了用户在数据创建与访问时个人用户的运算量。PRE 技术并非独立存在和发展的，需要基于 IBE、ABE 等具体机制在云环境中实施，因此，出现了基于身份与属性的代理重加密机制[8,9]，提高了重加密机制的灵活性。访问控制相关属性的多样化增加了 ABE 加解密条件描述的难度，出现了与证书结合的代理重加密[10]，它基于证书集成部分属性描述，通过 CA 等权威机构签发，保证属性管理的可信性。时态要素也是代理重加密技术研究中的一个重要组成部分[11]。代理重加密与云端访问控制的结合逐步面向多样化的访问控制条件，产生了基于条件的代理重加密（CPRE, condition based PRE）[12]。但是上述代理重加密技术需要数据访问者针对不同的密文提供不同的私钥，这样，在面向云环境中复杂的访问控制属性时，访问者的密钥管理量和难度都会激增。同时，重加密密钥的生成与分发仍由数据所有者完成。为了进一步减轻数据所有者的计算难度，充分利用云服务端的计算能力，文献[13,14]提出一种多要素代理重加密机制，将代理重加密的解密密钥定义为用户私钥与条件要素两种，通过两者的数据运算产生最终的解密密钥；其中，条件要素被定义为无符号二进制串，可以由多个参数连接后的运算产生。上述文献主要针对主体访问控制要素如何实现代理重加密的密钥构造问题进行论述。文献[14]则将密文进行了细粒度划分，定义为不同的类型，用户依据不同的类型提供不同的密钥进行解密。本文进一步将代理重加密技术和多要素访问控制描述进行结合，借鉴文献[13,14]中多要素、细粒度的管理思路，进一步提出基于代理重加密的访问控制部署方案，设计基于重加密的数据加解密算法，实现云端快速、有效的数据授权管理。

3 设计目标与方案假设

3.1 设计目标

PRE-MFAC 方案的设计目标如下。

1) 实现密文数据的访问控制请求多要素化描述

PRE-MFAC 中针对密文数据的访问管理以现有多要素访问控制及相关研究为基础，在密钥和加密密钥的构造中引入多种访问控制要素。

2) 细化密文管理粒度，减轻用户密钥管理难度，兼顾访问控制客观性

PRE-MFAC 中重加密密文的解密基于用户的私钥和用户所具备的复杂访问控制要素，用户仅需保存其唯一的解密私钥，而访问数据的解密密钥由其私钥和访问控制条件运算产生，用户不需针对不同粒度的密文保管不同的密钥。

3) 充分发挥代理重加密服务器的运算能力，减轻用户密文创建和访问的运算消耗

数据的创建者仅需要计算初始密文，不需针对不同的数据共享需求计算大量密文，代理重加密服务器依据初始密文和数据共享需求，产生重加密密文，由密钥管理服务器进行重加密密钥的管理和运算，个人用户不需消耗珍贵的资源和时间。

4) 能够抵抗攻击

PRE-MFAC 方案要求能够抵抗传统的密码分析和蛮力攻击、抵抗针对 PRE 的合谋共计、抵抗云服务提供商的数据隐私窃取。

3.2 方案假设

为了实现 PRE-MFAC 方案，需要满足如下假设。

1) 网络连接。数据创建者 A 和访问用户 U 都可以连接到互联网，以便能够与密钥管理服务器（KM, key management server）、策略管理服务器（PM, police management server）、代理重加密服务器（PRE, proxy re-encryption server）、云数据服务器（DC, data center server）进行交互，实现密钥获取、策略发布、数据访问等。

2) 密钥生成中心（KGC, key generation center）、A 和 U 可信，KGC 负责公共参数和公私钥的

产生，数据所有者是初次密文的创建者；U 不会主动泄露相关密钥数据。PRE、KM、PM 半可信，是 PRE-MFAC 实施的核心，负责产生重加密密钥、重加密密文等，该部分进行数据密文重加密的实施，同时有泄露用户数据的可能。

3）DC 不可信。提供存储服务，具有开放性的特征。

4　方案构造

4.1　系统模型

PRE-MFAC 方案中涉及符号说明如表 1 所示。

表 1　PRE-MFAC 方案参数说明

名称	说明
pk_i	用户 i 的公钥
sk_i	用户 i 的私钥
$K(M)$	对称密钥 K 加密产生的消息 M 的密文
$E(K)_i$	用户 i 私钥可以解密的密文
$Cert_i$	用户 i 的公钥证书
con_i	用户 i 的访问控制条件
P_MFAC	访问控制策略
$rk_{i\to j}$	用户 i 到 j 的代理重加密密钥

PRE-MFAC 方案的系统模型如图 1 所示，包含数据创建者 A、访问用户 U、KCG、云端数据服务器、云端访问控制服务器 5 个实体。具体说明如下。

1）数据创建者 A。创建被访问数据 M，并对其进行加密等安全处理，最终通过云服务器进行数据的共享。

2）访问用户 U。对消息 M 提出访问申请，通过云服务器获取数据并进行解密，最终实现数据或服务的获取。

3）云数据服务器（DC）。存储对称加密后的密文数据。

4）云端访问控制服务器。包含 PM、KM 和 PRE，分别用于访问控制策略管理和描述、重加密密钥管理和对称密钥密文管理、代理重加密运算。

另外，系统面临着针对对称密文、重加密密文的暴力破解和密码分析，同时需要应对云服务商和攻击者针对重加密密文的合谋攻击。

4.2　PRE-MFAC 方案系统描述

PRE-MFAC 主要涉及 2 个主要流程，即数据创建流程和数据访问流程。

1) 数据创建流程

该流程中以数据创建者为发起方，将数据 M 进

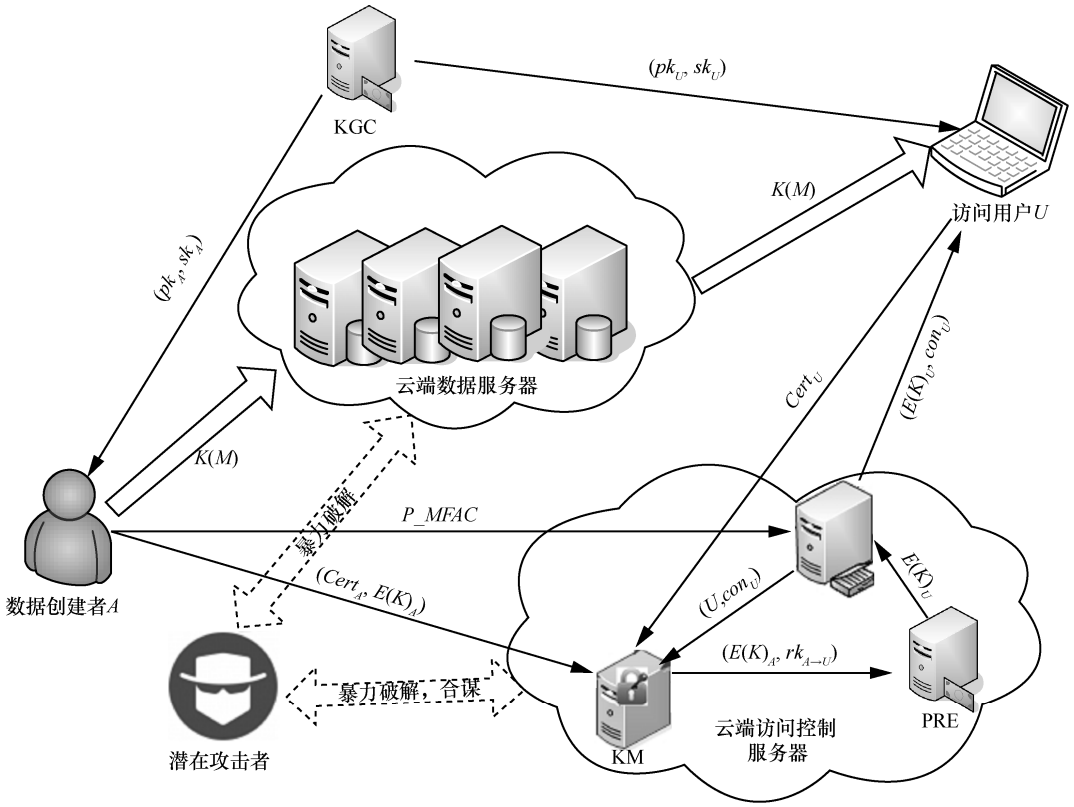

图 1　PRE-MFAC 方案的系统模型

行对称加密产生密文 $K(M)$，并将对称密钥 K 进行非对称加密产生 $E(K)_A$，向 PM 提交访问控制策略 P_MFAC，如图 2 所示，详细流程描述如下。

Step1 数据创建者 A 生成明文数据 M 的对称加密密文 $K(M)$，并将 $K(M)$上传至云端数据服务器。

Step2 数据创建者 A 调用函数 $Enc(K, pk_A)$ 加密 K，产生 $E(K)_A$，上传至密钥管理服务器。

① A 向 KCG 提交密钥对产生请求，同时提供参数 q。

② KCG 获取 q，进行调用函数 $Setup(q)$ 初始化，产生系统安全参数信息表 $param$。

③ KCG 调用函数 $KeyGen(param)$，生成 A 的公私钥对 (pk_A, sk_A)，并反馈给 A。

④ 数据创建者 A 产生 K 的第一次加密密文 $E(K)_A$，上传至 KM。

Step3 数据创建者 A 构造多要素访问控制策略 P_MFAC，上传至 PM。

2) 数据访问流程

该流程以访问用户 U 为发起方，U 向云端数据管理服务器请求数据密文 $K(M)$，同时向访问控制

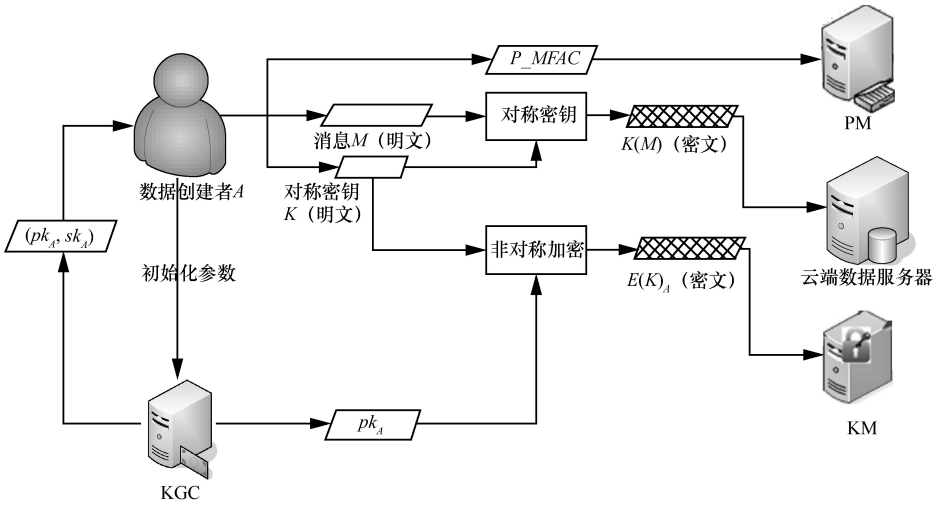

图 2 PRE-MFAC 数据创建流程

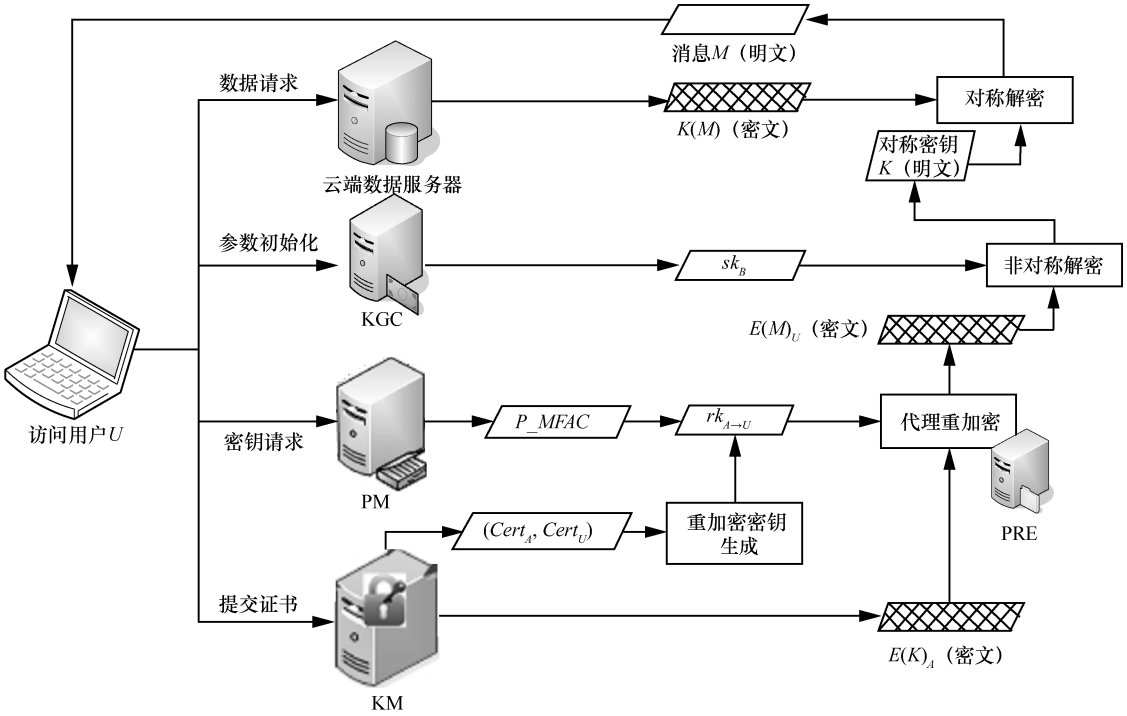

图 3 PRE-MFAC 数据访问流程

服务器请求对称密钥 K 的密文数据，最终通过自身密钥 sk_U 解密获取 K，实现 $K(M)$的解密，如图 3 所示，具体流程说明如下。

Step1　用户 U 向云端数据服务器请求 $K(M)$。

Step2　用户 U 向云端访问控制服务器请求 $E(K)_U$。

① 用户 U 将自身证书提交给 KM，用于重加密密钥生成。

② 用户 U 向 PM 提出密钥密文访问申请。

③ PM 获取用户的属性和环境参数，进行 P_MFAC 匹配，提取访问控制条件 con_U。

④ KM 提取数据创建者 A 和访问用户 U 的证书信息 $(Cert_A, Cert_U)$，基于 $(Cert_A, Cert_U)$ 与 con_U，通过函数 $ReKeyGen(sk_A, pk_U, con_U)$ 生成重加密密钥 $rk_{A\to U}$；KM 将 $(rk_{A\to U}, E(K)_A)$ 给 PRE。

⑤ PRE 获取 KM 提取的 $E(K)_A$，与 $rk_{A\to U}$ 通过代理重加密函数 $\mathrm{Re}Enc(E(K_A),\ rk_{A\to U})$，获得 $E(K)_U$，反馈 $(E(K)_U, con_U)$ 给用户 U。

Step3　用户 U 解密获得明文 M。

① 用户 U 使用 sk_U 解密调用函数 $Dec_2(sk_U, E(K)_U, con_U)$ 解密 $E(K)_U$，获取 K。

② 使用 K 对称解密 $K(M)$，获取明文 M。

4.3　PRE-MFAC 方案算法描述

PRE-MFAC 的实施过程中主要涉及以下 7 个算法函数。

1)参数建立：$Setup(q)\to param$

选取长度为 q 的素数 p，群 G_1、G_2 为乘法循环群，g 为 G_1 的生成元，散列函数组 H_1、H_2、H_3、H_4，其中，$H_1:\{0,1\}^*\to G_1$，$H_2:\{0,1\}^*\to Z_p^*$，$H_3:G_2\to\{0,1\}^l$，$H_4:\{0,1\}^*\to G_1$。公开参数 $param=\{p, G_1, G_2, g, H_i(i=1,\cdots,4)\}$。

定义双线性映射 $e:G_1\times G_2\to G_2$。

2)初始密钥生成：$KeyGen(param)\to(sk_i, pk_i)$

选取 $x_i\in Z_p^*$，则 $sk_i=x_i$，$pk_i=g^{x_i}$。

3) 加密：$Enc(k, pk_A)\to E(k)_A$

数据创建用户 A 使用自身公钥 pk_A 加密对称密钥 K，选取 $i\in G_2$，计算 $r=H_2(k\|i)$，则 $E(K)_A=\{c_1, c_2, c_3, c_4, c_5\}$。其中，$c_1=g^r$，$c_2=ie(pk_A, H_1(pk_A))^r$，$c_3=k\oplus H_3(i)$，$c_4=H_1(pk_A)$，$c_5=H_4(c_1\|c_2\|c_3\|c_4)$。

4) 代理重加密密钥生成：$ReKeyGen(sk_A, pk_U, con_U)\to rk_{A\to U}$

生成由 A 到 U 基于条件 con_U 的代理重加密密钥 $rk_{A\to U}=(pk_U, pk_U^r, H_1(pk_U\|con_U)H_1(pk_A)^{sk_A}, g^{-r})$。

5) 代理重加密：$ReEnc(E(K)_A, rk_{A\to U})\to E(K)_U$

加密代理对对称密钥的密文 $E(K)_A$ 进行重加密，生成可以被 sk_U 解密的对称密钥的密文 $E(K)_U=\{c_1', c_2', c_3', c_4', c_5'\}$。若 $e(c_1, H_4(c_1\|c_2\|c_3\|c_4))=e(g, c_5)$，则进行如下计算：$c_1'=c_1$；$c_2'=c_2e(pk_U^r g^{-r}, H_1(pk_A)^{-sk_A})\ e(pk_U^r, H_1(pk_U\|\ con_U)\ H_1(pk_A)^{-sk_A})=ie(pk_U^r, H_1(pk_U\|con_U))$；$c_3'=c_3$；$c_4'=H_1(pk_U)$。$c_5'=H_4(c_1'\|c_2'\|\ c_3'\|c_4')^r$。否则，反馈信息完整性错误。

6) 解密：$Dec_1(sk_A, E(K)_A)\to K$

数据创建用户 A 解密自身公钥加密的对称密钥密文，获取对称密钥 K。

若 $e(c_1, H_4(c_1\|c_2\|c_3\|c_4))=e(g, c_5)$，则进行如下计算，否则反馈信息完整性错误。

计算 $i=\dfrac{c_2}{e(c_1, c_4)^{sk_A}}$；

计算明文 $K=c_3\oplus H_3(i)$；

计算 $r=H_2(K\|i)$，若 $c_1=g^r$ 且 $c_2=ie(g, c_4)^{rsk_A}$，则输出 K。

7)基于条件解密：$Dec_2(sk_U, E(K)_U, con_U)\to K$

用户 U 解密重加密后对称密钥密文，获取对称密钥 K。若 $e(c'_1, H_4(c'_1\|c'_2\|c'_3\|c'_4))=e(g, c'_5)$，则进行如下计算，否则反馈信息完整性错误。

计算 $i=\dfrac{c_2'}{e(c_1', H_1(pk_U\|con_U))^{sk_U}}$；

计算明文 $K=c'_3\oplus H_3(i)$；

计算 $r=H_2(K\|i)$，若 $c'_1=g^r$ 且 $c'_2=ie(pk_U, H_1(pk_U\|con_U))^r$，则输出 K。

4.4　*P_MFAC* 描述及代理重加密参数提取

P_MFAC 是用户在创建数据时提交到策略管理服务器 PM 的访问控制策略，P_MFAC 定义为二元组(ID_O, $P\text{-}con_U$)，其中，ID_O 表示客体 ID，$P\text{-}con_U$ 表示访问客体需要的主体条件约束。P_MFAC 在 PM 中以列表的形式存在，该列表以 ID_O 区分不同的表项，ID_O 定义为无符号字符型数组，由数字和字母组成，命名规则依据不同的云服务器约定。用户在

创建数据并提交对称密文 $K(M)$到云数据服务器时便获得客体资源的 ID_O，并将 ID_O 和 $P\text{-}con_U$ 合并为 *P_MFAC* 提交到 PM。$P\text{-}con_U$ 主要针对访问用户在用户名、角色、时态、物理位置、网络属性等信息进行定义和描述。系统所依据的访问控制模型不同，则 $P\text{-}con_U$ 的定义和描述也不同。例如，以基于属性的访问控制为模型，则 $P\text{-}con_U$ 中将描述主体的属性，包含时间、环境等及不同属性之间的逻辑运算关系。

PM 在接收到数据创建者上传的 *P_MFAC* 表项后，将其追加到策略管理列表中。访问用户向 PM 提出请求后，首先，PM 分析用户的访问请求，提取 ID_O，进行策略表项的检索，提取对应的 $P\text{-}con_U$；其次，PM 获取访问用户的客观访问控制条件，如用户的角色、时态、物理环境等信息，并与 $P\text{-}con_U$ 进行比较，若提取的用户信息满足 $P\text{-}con_U$ 描述的访问控制需求，则将提取的用户信息统一化描述，进一步生成为指定长度的主体条件数据 con_U，提交给 KM 进行运算。

5 PRE-MFAC 方案

5.1 安全性

本文提出的 PRE-MFAC 以 PRE 为实现基础，因此，方案的安全性依托于所提出算法的安全性，基于文献[15]的算法构造方案和理论，PRE-MFAC 方案中的算法满足 CCA 安全要求。PER-MFAC 的系统中针对明文信息 M 的加密依托于对称加密算法，方案中采用现有成型的对称密码体制，能够抵抗针对性的密码分析和暴力破解；另外，在半可信的访问控制服务器中，用户敏感数据 K 采用密文的形式出现，依托于具备 CCA 安全性的 PRE 算法，能够抵御攻击者和云访问控制服务器的合谋攻击。

5.2 性能

为了进行算法的性能分析，假设 n 为访问控制要素的个数，t_1 为指数运算的时间开销，t_2 为线性对运算的时间开销，PRE-MFAC 主要函数的时间复杂度如表 2 所示。

表 2 PRE-MFAC 主要函数的时间复杂度

函数	开销
Enc	$3t_1+t_2$
ReEnc	$2t_1+3t_2$
Dec_1	$3t_1+3t_2$
Dec_2	$3t_1+4t_2$

空间复杂度主要关注用户密钥存储花费的开销，由于 PRE-MFAC 用户解密时提供其唯一私钥，同时由系统实时获取其所处的客观访问控制环境，因此，无论访问控制要素为多少，密钥存储的空间复杂度为 $O(1)$。

5.3 属性

PRE-MFAC 方案中将代理重加密技术和多要素访问控制进行融合，在系统部署和算法中设置代理重加密服务器、策略管理服务器、密钥管理服务器，能够解决目前多要素访问控制机制设计和密文访问控制相互脱节的问题，下面就是否针对复杂访问控制要素、是否支持密文访问控制、加解密运算执行方和多要素访问控制对用户密钥管理的空间复杂度造成的影响等方面将 PRE-MFAC 与现有研究进行对比，如表 3 所示。具体说明如下。

1) 支持密文数据访问控制

PRE-MFAC 中访问控制的属性通过 con_S 传递给重加密密钥函数进行数据的重加密和处理；TAAC[16]仅论述基于属性访问控制机制在云存储中的授权策略描述，并未论述如何针对云端数据密文进行处理，因此，并不支持密文访问控制。

2) 支持细粒度管理需求

PRE-MFAC 对于密文可以划分为满足需求的

表 3 本文方案与现有研究对比分析

属性模型	密文访问控制	细粒度	多要素	用户密钥管理量	加解密运算执行方
TAAC	×	×	√	—	—
JBE	√	×	×	较小	用户
CPRE	√	×	√	较大	用户
Type-PRE	√	√	×	较大	用户
ACC-PRE	√	×	×	较小	用户&云服务器
PRE-MFAC	√	√	√	较小	用户&云服务器

注：TAAC 并未针对密文进行访问控制，因此，不涉及密钥管理问题。

粒度，产生不同的密文数据及其对应的重加密密钥。其中，Type-PRE[15]对密文数据以类型进行划分，同样可以满足细粒度的要求，其他文献则并未针对密文的细粒度管理设计相关机制。

3) 支持多要素访问控制描述

PRE-MFAC 支持访问用户角色、时态、环境等多种要素信息的定义及其约束关系的描述；TAAC 以基于属性的访问控制为基础，重点突出了时间因素的作用，兼顾各类访问控制要素的描述；CPRE[8]则以条件作为重加密密钥生成的参数，也能够满足复杂访问控制条件的描述；JBE[7]以角色作为数据加密的参数，并不能够支持时态、环境等复杂访问控制要素的管理需求；ACC-PRE[14]提出访问控制条件为重加密密钥参数，但是并未实质论述如何将复杂的访问控制条件转化为重加密密钥参数。

4) 具有较低用户的密钥存储开销

PRE-MFAC 在支持细粒度访问控制的同时，减轻用户的运算量和密钥管理难度，用户针对不同密文可以解密，所需要提供的私钥不变，通过所处的访问控制条件进行区分；JBE 的密钥管理量与用户角色数量挂钩，但是缺乏多要素和细粒度的支持；CPRE 则要求用户针对不同的访问控制条件提供不同的解密密钥；Type-PRE 要求用户针对不同的密文类型提供不同的解密密钥，两者在多要素和细粒度的管理需求下都会造成用户密钥管理量的激增。此处假设用户的主体访问控制要素为 n 个，则 CPRE 中要求用户提供基于不同访问控制条件组合的密钥进行数据的加密和管理，密钥的管理量表示为 $O(n!)$，若密文的粒度划分为 m 个层级，则 Type-PRE 的密钥管理量则为 $O(m)$。与之对比，PRE-MFAC 无论主体属性和客体粒度的划分层次，用户解密均提供唯一私钥，多种访问控制条件和密文粒度则以重加密解密的第二个参数被系统获取，其密钥的管理量理论上为 $O(1)$。

5) 加解密的执行方

PRE-MFAC 一改其他文献加解密由用户自身执行的问题，提出了基于代理重加密的云服务实施方案，提升了云服务器在访问控制机制中的参与度。

此外，PRE-MFAC 提高访问控制判断客观性，用户针对细粒度密文的密钥不再是按需自行提供，而是由系统客观获取访问控制条件，进行重加密运算后进行管理，大大提高了访问控制判定的客观程度。

6　结束语

云计算技术的发展推动了人类社会信息化的进程，同时，天地一体化信息网络的发展也为云服务提供了更为坚实和宽阔的网络支撑。通过云端，人们实现了信息、服务甚至运算能力的共享，而天地一体化信息网络全方位地扩展了人类信息的传播范畴，这些在带给人们便捷的同时，也带来了全新的安全问题。访问控制这一传统的信息安全技术，通过控制用户的访问行为，实现对指定资源的保护，针对云计算环境，访问控制技术仍然至关重要，它需要满足多要素的描述需求，同时要能够以云端的数据密文为管理对象。如何将多要素描述与密文管理相结合成为云端访问控制技术研究的热点问题。现有的密文访问控制中要求用户针对自身安全需求进行数据密文的计算，为了应对细粒度的访问控制描述，用户需要管理大量的密钥。因此，本文将代理重加密技术与多要素访问控制技术相结合，以天地一体化信息网络中的云端数据安全为应用背景，提出了一种基于代理重加密的多要素访问控制（PRE-MFAC）实施方案。通过系统模型描述和算法定义，实现了云端的多要素密文访问控制，数据创建者仅需要提交访问控制策略和基于自身私钥加密的密文，不需针对不同的共享用户多次计算密文数据；由代理重加密系统依据用户的客观访问控制条件，产生代理重加密密文，访问用户仅需持有唯一私钥，即可进行解密。PRE-MFAC 将为云端密文数据高效、安全访问控制机制的发展奠定基础，并将进一步支持天地一体化信息网络中数据安全存储和传输相关技术的研究与发展。

参考文献：

[1] 李凤华, 殷丽华, 吴巍, 等. 天地一体化信息网络安全保障技术研究进展及发展趋势[J]. 通信学报, 2016, 37(11): 156-168.
LI F H, YIN L H, WU W, et al. Research status and development trends of security assurance for space-ground integration information network[J]. Journal on Communications, 2016, 37(11): 156-168.

[2] JHA S, SURAL S, VAIDYA J, et al. Security analysis of temporal RBAC under an administrative model[J]. Computers & Security, 2014(46): 154-172.

[3] 杨柳, 唐卓, 李仁发, 等. 云计算环境中基于用户访问需求的角色

查找算法[J]. 通信学报, 2011, 32(7): 169-175.
YANG L, TANG Z, LI R F, et al. Roles query algorithm in cloud computing environment based on user require[J]. Journal on Communications, 2011, 32(7): 169-175.

[4] LUO J, WANG H, GONG X, et al. A novel role-based access control model in cloud environments[J]. International Journal of Computational Intelligence Systems, 2016, 9(1): 1-9.

[5] LI J W, SQUICCIARINI A, LIN D J, et al. SecLoc: securing location-sensitive storage in the cloud[C]// The 20th ACM Symposium on Access Control Models and Technologies. 2015: 51-61.

[6] ZHOU L, VARADHARAJAN V, HITCHENS M. Trust enhanced cryptographic role-based access control for secure cloud data storage[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(11): 2381-2395.

[7] ZHOU L, VARADHARAJAN V, GOPINATH K. A secure role-based cloud storage system for encrypted patient-centric health records[J]. Computer Journal, 2016, 59(11): 1593-1611.

[8] XU P, JIAO T, WU Q, et al. Conditional identity-based broadcast proxy re-encryption and its application to cloud email[J]. IEEE Transactions on Computers, 2015, 65(1): 66-79.

[9] ZHANG Y, LI J, CHEN X, et al. Anonymous attribute based proxy re-encryption for access control in cloud computing[J]. Security and Communication Networks, 2016, 9(14): 2397-2411.

[10] LI J, ZHAO X, ZHANG Y, et al. Provably secure certificate-based conditional proxy re-encryption[J]. Journal of Information Science & Engineering, 2016, 32(4): 813-830.

[11] LIU Q, WANG G, WU J. Time-based proxy re-encryption scheme for secure data sharing in a cloud environment[J]. Information Sciences, 2014, 258(3): 355-370.

[12] YANG Y, LU H, WENG J, et al. Fine-grained conditional proxy re-encryption and application[C]//International Conference on Provable Security. 2014: 206-222.

[13] 苏铓, 史国振, 谢绒娜, 等. 面向移动云计算的多要素代理重加密方案[J]. 通信学报, 2015, 36(11): 73-79.
SU M, SHI G Z, XIE R N, et al. Multi-element based on proxy re-encryption scheme for mobile cloud computing[J]. Journal on Communications, 2015, 36(11): 73-79.

[14] SU M, LI F, SHI G, et al. A user-centric data secure creation scheme in cloud computing[J]. Chinese Journal of Electronics, 2016, 25(4): 753-760.

[15] TANG Q. Type-based proxy re-encryption and its construction[C]//International Conference on Cryptology in India: Progress in Cryptology. 2008: 130-144.

[16] YANG K, LIU Z, JIA X, et al. Time-domain attribute-based access control for cloud-based video content sharing: a cryptographic approach[J]. IEEE Transactions on Multimedia, 2016, 18(5): 940-950.

[作者简介]

苏铓（1987-），女，内蒙古赤峰人，博士，南京理工大学讲师，主要研究方向为云安全、访问控制、隐私保护等。

史国振（1974-），男，河南济源人，博士，北京电子科技学院副教授、硕士生导师，主要研究方向为嵌入式系统、网络安全、访问控制等。

付安民（1981-），男，湖北通城人，博士，南京理工大学副教授，主要研究方向为云安全、隐私保护等。

俞研（1972-），男，吉林长春人，博士，南京理工大学副教授，主要研究方向为无线网络、网络空间安全等。

金伟（1994-），女，北京人，中国科学院信息工程研究所博士生，主要研究方向为访问控制。