软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2020,31(5):1563−1572 [doi: 10.13328/j.cnki.jos.005676]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于代理重加密的云数据访问授权确定性更新方案*

苏 铓[1], 吴 槟[2,3], 付安民[1], 俞 研[1], 张功萱[1]

[1](南京理工大学 计算机科学与工程学院,江苏 南京 210094)

[2](信息安全国家重点实验室(中国科学院 信息工程研究所),北京 100093)

[3](中国科学院大学 网络空间安全学院,北京 100049)

通讯作者: 苏铓, E-mail: sumang@njust.edu.cn

摘 要: 有越来越多的用户选择云为其进行存储、运算、共享等数据处理工作,因此云端数据量与日俱增,其中不乏敏感数据和隐私信息.如何对用户托管于云端的数据进行授权管理,保证数据机密性、访问授权有效性等至关重要.为此,提出一种基于代理重加密(proxy re-encryption,简称 PRE)的云端数据访问授权的确定性更新方案(proxy re-encryption based assured update scheme of authorization,简称 PAUA).首先将提出 PAUA 方案的前提假设和目标,其次论述系统模型和算法,最后对 PAUA 进行讨论和分析.PAUA 方案将减轻用户在数据共享时的计算量,同时将重加密密钥进行分割管理,实现授权变更时,密钥的确定性更新.

关键词: 代理重加密;确定性更新;密文访问控制;授权管理;云计算

中图法分类号: TP309

中文引用格式: 苏铓,吴槟,付安民,俞研,张功萱.基于代理重加密的云数据访问授权确定性更新方案.软件学报,2020,31(5):1563−1572. http://www.jos.org.cn/1000-9825/5676.htm

英文引用格式: Su M, Wu B, Fu AM, Yu Y, Zhang GX. Assured update scheme of authorization for cloud data access based on proxy re-encryption. Ruan Jian Xue Bao/Journal of Software, 2020,31(5):1563−1572 (in Chinese). http://www.jos.org.cn/1000-9825/5676.htm

Assured Update Scheme of Authorization for Cloud Data Access Based on Proxy Re-encryption

SU Mang[1], WU Bin[2,3], FU An-Min[1], YU Yan[1], ZHANG Gong-Xuan[1]

[1](School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China)

[2](State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences), Beijing 100093, China)

[3](School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: More and more people select cloud as an important tool for data storing, processing and sharing, as a result, the data in cloud increases rapidly, including some sensitive and privacy information. It is a vital problem to manage the authorizations of hosted data in cloud for confidentiality and effectiveness of access control. This study proposes a proxy re-encryption based assured update scheme of authorization for cloud data (PAUA) in light to solve the above mentioned problem. Firstly, the aims and assumptions of PAUA are given. Secondly, the system model and algorithm are shown. Finally, the comparisons with PAUA and the current status are carried out. The

* 基金项目: 国家自然科学基金(61702266, 61572255,); 江苏省自然科学基金(BK20150787, BK20141404); 赛尔网络下一代互联网技术创新项目(NGII20170404)

Foundation item: National Natural Science Foundation of China (61702266, 61572255); Natural Science Foundation of Jiangsu Province (BK20150787, BK20141404); CERNET Innovation Program for Next Generation of Internet (NGII20170404)

收稿时间: 2018-01-05; 修改时间: 2018-04-06; 采用时间: 2018-09-14; jos 在线出版时间: 2019-01-21

CNKI 网络优先出版: 2019-01-22 13:48:13, http://kns.cnki.net/kcms/detail/11.2560.TP.20190122.1348.002.html

PAUA reduces the encryption and decryption work of personal users. Meanwhile, it ensures the permission updating by dividing the parameters of re-encryption key generation.

Key words: proxy re-encryption, assured update, cipher text access control, authorization management, cloud computing

云计算为人们的生产生活提供了丰富的资源和信息,通过云端获取服务称为了一种全新的服务模式,内容包含了软件、平台和硬件设置等.用户通过购买云服务对数据进行存储、处理和共享,但是云端流通的数据量与日俱增,其中也包含了大量敏感数据和隐私信息,云为用户提供便捷的数据使用方式的同时,对用户数据的安全带来多方面的威胁.云用户通过网络进行数据的交互,数据所有者不再对数据具有控制权,而是托管到云端进行进一步的运算和处理.如何保障托管数据的机密性、完整性,如何保障用户数据访问控制和授权管理的有效性和可靠性,便成为了云端数据安全面临这全新的挑战.

针对数据的机密性和完整性问题,出现了云端密文访问控制技术,通过指定密码算法和密钥对数据进行加密处理,加密后的数据以密文的形式保存在云服务器中,保证云数据的机密性.通常情况下,数据所有者在使用云服务前将数据进行加密处理,将角色[1]、身份信息属性信息等作为密钥生成的参数,实现对用户权限的控制.如:基于角色的加密、基于身份的加密、属性基加密等机制(attribute based encryption,简称 ABE)等;ABE 等机制通过与访问控制模型相结合[2,3],能够在一定程度上保证授权策略的有效性;密钥策略属性基加密系统(key policy attribute based encryption,简称 KP-ABE)和密文策略属性基加密系统(ciphertext policy attribute based encryption,简称 CP-ABE)机制能够支持复杂策略,在细粒度的数据共享[4]和管理方面具有十分广阔的应用前景,适用于解密方不固定的情况,加密方无需关注解密方具体的身份,仅定义解密方需要具备的属性即可,免除了数据共享中因解密方变化导致频繁分发密钥的问题,从而推动了 ABE 等技术在云计算等相关领域的广泛运用.文献[5]提出了一种针对云存储的灵活的 ABE 机制,文献[6]则进一步阐述了 CP-ABE 在云计算环境下的应用策略.但是上述机制中,针对数据授权的变更问题,需要用户进数据的重复加密;同时,由于数据在云端托管,无法确定在数据授权更新后,原授权数据的彻底删除,因此缺乏授权变更的确定性.针对权限更新问题,文献[7]定义了全新的用户密钥形式,包含分为欺骗密钥和私钥,用户解密需要提供有两个参数产生的密钥,密钥通过欺骗密钥进行变化,但是,在怎样的应用场景和需求下管理密钥以及如何实现分发没有进行阐述和设计.若由数据所有者管理欺骗密钥,虽然可以进行权限的确定性更新,但是将会给用户带来巨大的运算和密钥管理负担.上述解决方案在一定程度上满足了云端数据机密性、完整性的安全管理需求,但是多要求创建者针对不同数据共享者进行多次数据加密,产生不同的共享密文,这样对于个人用户来讲将是性能和时间的巨大考验.同时,如何在发挥云服务器计算能力和存储能力的前提下实现托管数据授权的确定性更新这一关键问题鲜有论述.

本文针对上述问题,将代理重加密的思想引入到云端密文数据授权更新和管理中,提出一种基于代理重加密的云端数据权限确定性更新方案,数据所有者在共享数据时,无需重复数据的加密工作,仅需产生初始密文,也就是自身私钥加密的密文,其后的重加密工作则依托于云平台,完成数据的贡献.减轻用户的云端负担;同时,将重加密密钥的参数进行分割管理,一部分包含共享用户的公私钥等参数托管到云端,另一部分则定义为解密参数,由所有者管理;数据解密则需要同时提供用户自身私钥和解密参数,当发生权限变更时,仅需要所有者更改解密参数,即可实现确定性权限更新.本文将从系统模型和相关算法两个层面进行论述,并对 PAUA 方案的优缺点进行分析,为云端数据的授权管理提供重要的理论和实践基础.

1 基础知识

1.1 代理重加密技术

代理重加密能够将数据共享中的加解密工作进行拆分,大量的运算借助云计算平台完成,降低了用户创建、使用数据的运算量.基具体来说,用户在创建数据时数据加密的任务分成了首次加密和重加密,首次加密由用户完成,重加密则由云服务完成,服务器基于用户首次加密的数据,针对不同分享需求产生密文.通过将身份、属性等信息的引入,PRE 为云数据的密文访问控制提供了重要的支撑.身份[8]、属性[9]PRE 的算法构造中重要的

参数,此外,结合身份信息或属性信息的证书[10]、访问控制条件[11,12]以及用于细粒度管理的密钥类型[13]也称为了 PRE 密钥的重要参数,为云端密文数据的高效访问控制管理提供了重要理论和实践基础.

PRE 将密文共享的任务过渡到云服务器,减轻了用户在数据共享中的产生密文数据的计算量,重加密密钥的生成与分发仍然需要数据所有者完成.在共享用户海量的云环境,个人终端用户的计算量仍然是十分巨大的,需要用户具备很高运算性能和存储空间.为了将重加密密文产生和存储进一步托管于云端文献,文献[14]将代理重加密与懒惰加密技术相结合,提出了一种面向 KP-ABE 的 PRE 方案,其中,密钥的分发、更新和管理均有由云负责,初步解决了所有者在密钥生成上存在的计算量问题.但是云一般为半可信或不可信实体,将其作为重加密密钥的分发方与撤销方,可能会威胁到数据的隐私与安全,针对由权限撤销、数据变更等带来的密钥更新问题仍然亟待解决.

本文以上述文献的研究为基础,将代理重加密运用到云端数据密文的授权确定性更新方案中.

1.2 基于乘法循环群的双线性对映射

双线对映射在公钥密码尤其是身份、属性基加密等算法的构造和设计中广泛应用,令群 G_1,G_2,G_3 分别为乘法循环群,阶数为 p.

先存在映射 $e:G_1\times G_2\to G_3$,如果该映射符合以下条件,则称其为双线性映射.

(1) 双线性:对于任意元素 $a,b\in Z_p^*$,$g\in G_1,h\in G_2$,有 $e(g^a,h^b)=e(g^b,h^a)=e(g,h)^{ab}$ 成立.

(2) 非退化性:若元素 $g\in G_1,h\in G_2$,且 g,h 是非单位元素,有 $e(g,h)\neq 1$.

(3) 可计算性:对于任意 $g\in G_1$ 和 $h\in G_2$,存在有效的算法能够在多项式时间内运算出 $e(g,h)$.

2 PAUA 设计目标与系统假设

PAUA 方案的设计目标如下.

1) 动态更新密文数据访问授权,确保变更的有效、可靠:数据解密要求用户具备私钥以及基于授权的解密参数,数据创建者通过解密参数的管理,共享数据在创建用户的授权范围内可以被访问,授权失效后,权限将进行确定性更新.

2) 数据的授权和管理权由数据创建者管理:PAUA 将代理重加密密钥的生成参数进行拆分,一部分由数据创建者进行管理,并以解密参数的形式提供给授权用户,数据的权限由数据创建者进行管理,不受其他服务提供商的干涉.

3) 基于现有的网络设备、终端设备以及安全设备:PAUA 机制实现对数据的安全管理与控制,不需要用户和服务平台单独购买额外的专用平台和设备.

4) 充分利用服务器强大的运算能力,降低了用户生成与使用密文是的资源消耗,服务器包含了可信与半可信两个类型:数据创建用户不在需要依据共享需求和用户,分别多次产生不同的密文,仅产生初始密文即可,代理重加密服务器将以初始密文和共享用户的信息,生成针对性的密文,重加密密钥的管理则由密钥管理服务器负责,节约个人终端用户的时间和空间资源.

5) 抗攻击性:PAUA 方案要求具有抵抗传统密码分析、暴力破解以及针对 PRE 的合谋攻击等,同时防止云服务提供商对用户数据隐私的挖掘和窃取.

2.1 方案假设

PAUA 方案的实现需要基于如下假设.

1) 数据的创建和访问依托于网络.

数据所有者 A 和共享用户 B 均具有连接网络进行数据访问的能力,能够实现与重加密密钥生成服务器(re-encryption key generator,简称 RKG)、代理重加密服务器(re-encryption server,简称 Re-Enc)、密钥生成中心(key generation centre,简称 KGC)和重加密参数管理服务器(re-encryption key management,简称 RKM)等服务器的交互,实现数据创建和访问等.

2) 数据共享者不转存和私自存储已经授权的数据.

共享者进行数据访问时,通过网络进行参数的获取并进行解密,其后并不进行数据的本地保存、转授权.

KGC、RKM、数据所有者和数据共享用户为可信,KGC 负责公共参数和公私钥的产生,RKM 则协助数据创建用户进行重加密密钥参数的管理,数据所有者是完成数据的第 1 次加密;访问用户不会主动泄露密钥及其相关数据.RKG、Re-Enc 半可信服务器生成重加密密钥、重加密密文等,该部分对于数据密文重加密的实施工作忠心完成,但是,对用户数据和隐私可能进行挖掘和分析.

3 方案构造

3.1 系统模型

PAUA 方案中涉及的符号说明见表 1.

Table 1 Definitions for Notations of PAUA

表 1 PAUA 符号定义

名称	说明
pk_A	用户 A 的公钥
sk_A	用户 A 的私钥
$rk_{A\to B}$	用户 A 到 B 的代理重加密密钥
α	重加密密钥参数/重加密解密参数
β	重加密密钥参数
C_A	可以被 A 的私钥进行解密的密文
$C_{A\to B}$	由 C_A 重加密后产生的可以被 B 的私钥进行解密的密文,与 C_A 的区别在于需要 B 提供解密参数

PAUA 方案的系统模型如图 1 所示,包含实体及其功能说明如下.

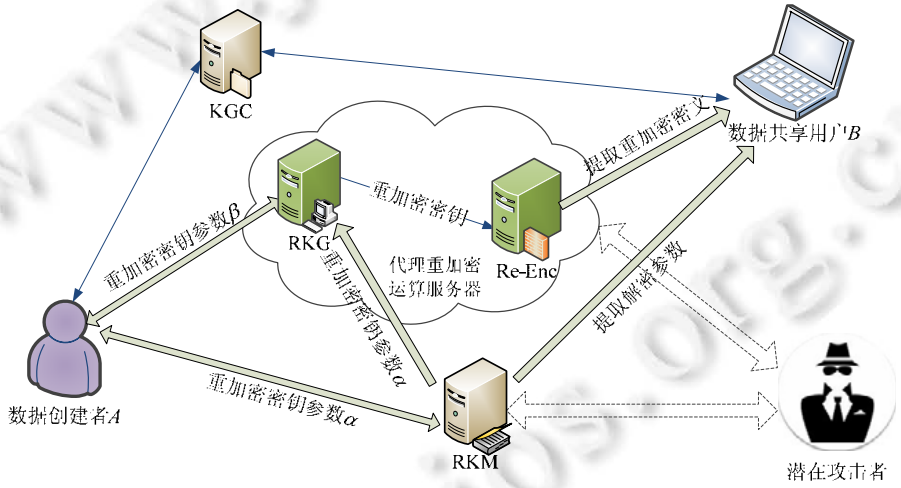

Fig.1 System model PAUA

图 1 PAUA 系统模型

1) 数据创建者 A:访问数据 m 的创造者,产生初始数据,并进行加密等安全处理,以云服务器为依托实现数据的共享,A 还规定了数据的使用权限.
2) 数据共享用户 B:具有对 M 使用的需求,数据或服务将通过云服务器获取并解密.
3) KGC:为用户进行重加密参数初始化,并产生公私钥对.
4) RKM:用于存储代理重加密密钥参数α,同时也是解密密钥参数,该服务器与数据创建者进行交互,通过参数α的管理实现授权的确定性变更.

5) RKG:用于代理重加密密钥的产生,需要用户的初始化参数β和 RKM 中存储的参数α共同产生代理重加密密钥.

6) Re-Enc:用于代理重加密的运算.

7) 潜在攻击者:存在针对系统中密文的分析攻击,针对 RKM、RKG、Re-Enc 等数据库的破解以及来自 RKG、Re-Enc 和攻击者的合谋攻击.

3.2 方案概述

PAUA 方案主要涉及两个阶段,工作原理如图 2 所示.

1) 阶段 1:该阶段完成数据的封装以及权限设置工作(图 2 左边部分),以数据创建者 A 为发起方,A 将数据 m 的进行代理重加密的第 1 次加密产生密文 C_A 并传输给 Re-Enc 服务器,用于分享过程中的代理重加密.同时,A 向 RKG 提交代理重加密密钥参数β,向 RKM 中提交重加密密钥参数α.

2) 阶段 2:该阶段完成数据的解密工作(图 2 右边部分),以数据共享用户 B 为发起方.B 在 Re-Enc 服务器获取密文数据 $C_{A\to B}$,在 RKM 获取解密参量α,以α和 sk_B 为参数构造解密密钥,实现 $C_{A\to B}$ 的解密,获取明文 m.

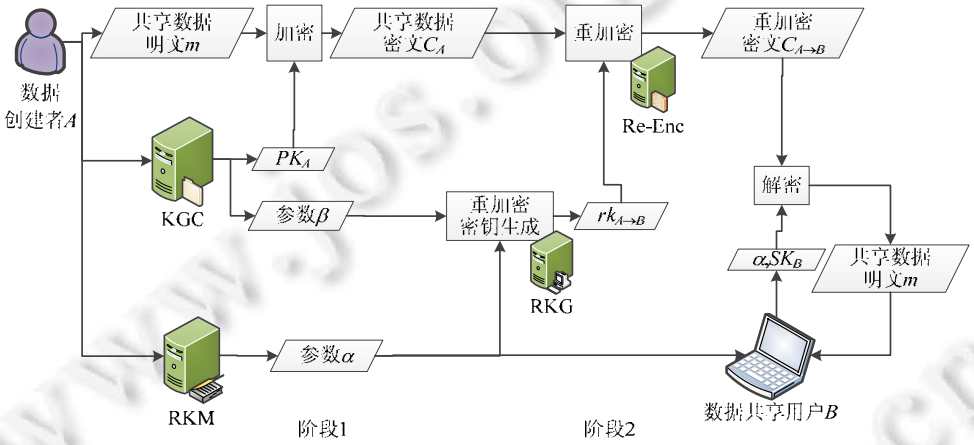

Fig.2 Working principles of PAUA

图 2 PAUA 方案工作原理

3.3 方案系统描述

PAUA 方案主要包含了如下 8 个系统流程.

1) 初始化:系统建立的第 1 步,整个过程中通过算法 *Setup* 的调用实现,产生公共参数、公/私钥等参数.

2) 数据创建:A 向 KCG 提交密钥对产生请求,同时提供参数 q 进行系统建立,KCG 调用算法层面函数 *KeyGeneration* 为 A 产生公私钥对(pk_A,sk_A),A 对数据 m 进行第 1 次加密,调用算法层面函数 *Encrpytion* 产生密文 C_A 并传输给 Re-Enc 服务器.而后,A 分别向 RKG 和 RKM 提交重加密密钥参数β,α,完成数据创建.

3) 代理重加密密钥参量生成:用户 A 在创建数据密文的同时,依据自身授权需求,产生代理重加密密钥参量,调用算法层面函数 *RkPara* 产生$\beta.\alpha$则为指定长度无符号字符串.

4) 密文数据获取:假设用户 B 数据共享者,B 向 Re-Enc 提交重加密密文数据获取请求,Re-Enc 获取 B 的请求后,向 B 提供代理重加密后的密文 $C_{A\to B}$.

5) 合法授权用户的重加密密文解密:假设 B 为合法访问用户,欲解密 $C_{A\to B}$,首先,B 在 RKM 获取解密参量α;其次,B 以α和 sk_B 为密钥解密,调用算法层面函数 *Decryption* 解密 $C_{A\to B}$ 获取 m.

6) 产生具有授权信息的密文数据:RKG 提取 A 提交的参量β,并向 RKM 提取参量α,调用算法层面函数

ReKeyGen 产生代理重加密密钥 $rk_{A\to B}$;Re-Enc 获取 $rk_{A\to B}$,调用算法层面函数 *ReEncrpytion*,运算 $C_{A\to B}$.

7) 授权确定性更新:*A* 更新 RKM 中的α参数列表,查找待撤销的授权对应参数α,并进行删除.

8) 授权撤销的用户进行数据解密:假设 *C* 为被撤销权限的访问用户,欲解密 $C_{A\to C}$,*C* 向 RKM 请求获取解密参数.由于 *C* 解密的参数已经被删除,故无法解密 $C_{A\to C}$.

3.4 算法描述

PAUA 的实施过程中包含 7 个函数,具体说明如下.

(1) 系统参数初始化:*Setup*(q)→*param*

选择一个素数 p,素数为 q 长度,定义乘法循环群 G_1,G_2,两个群的阶为 p,选取 G_1 的生成元 g,定义哈希函数组 $Hi(i=1,2,3,4)$,函数组具体定义如下:$H_1:\{0,1\}^*\to G_1$, $H_2:\{0,1\}^*\to Z_p^*$,$H_3:G_2\to\{0,1\}^l$,$H_4:\{0,1\}^*\to G_1$.公开参数 *param*=$\{p,G_1,G_2,g,H_1,H_2,H_3,H_4,\}$,定义 $e:G_1\times G_1\to G_2$ 作为双线性对.

(2) 初始密钥生成:*KeyGen*(*param*)→(sk_A,pk_A)

选取 $x_A\in Z_p^*$,则 $sk_A=x_A$, $pk_A=g^{x_A}$.

(3) 第 1 次加密:*Encrpytion*(m,pk_A)→C_A

用户 *A* 使用自身公钥 pk_A 加密明文信息 m,选取 $k\in G_2$,计算 $r=H_2(m||k)$,则 $C_A=(c_1,c_2,c_3,c_4,c_5)$.

- $c_1=g^r$;
- $c_2=k\cdot e(pk_A,H_1(pk_A))^r$;
- $c_3=m\oplus H_3(k)$;
- $c_4=H_1(pk_A)$;
- $c_5=H_4(c_1||c_2||c_3||c_4)^r$.

(4) 重加密参量β生成:*RkPara*(pk_B,pk_A,sk_A,r)→β

产生上传到 RKG 的代理重加密密钥参数,则 $\beta=\{pk_B,H_1(pk_A)^{sk_A},r\}$.

(5) 代理重加密密钥生成:*ReKeyGen*(α,β)→$rk_{A\to B}$

生成有 *A* 到 *B* 代理重加密密钥 $rk_{A\to B}$,则 $rk_{A\to B}=(pk_B,pk_B^r,H_1(pk_B\|\alpha)\cdot H_1(pk_A)^{sk_A},g^{-r})$.

(6) 代理重加密:*ReEncrpytion*(C_A,$rk_{A\to B}$)→$C_{A\to B}$

加密代理对密文 C_A 进行重加密,生成可以被 sk_B 所解密的密文 $C_B=(c_1',c_2',c_3',c_4',c_5')$.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;否则,反馈信息完整性错误.

- $c_1'=c_1$;
- $c_2'=c_2\cdot e(pk_B^r g^{-r},H_1(pk_A)^{-sk_A})\cdot e(pk_B^r,H_1(pk_B\|\alpha)\cdot H_1(pk_A)^{-sk_A})=k\cdot e(pk_B^r,H_1(pk_B\|\alpha))$;
- $c_3'=c_3$;
- $c_4'=H_1(pk_B)$;
- $c_5'=H_4(c_1',c_2',c_3',c_4')^r$.

(7) 解密 *Decryption*(sk_B,$C_{A\to B}$,α)

用户 *B* 重加密密文进行解密,获取明文 m.

若 $e(c_1',H_4(c_1'\|c_2'\|c_3'\|c_4'))=e(g,c_5')$,则进行解密运算;否则,提示完整性错误.

- 计算 $k=c_2'/e(c_1',H_1(pk_B\|\alpha))^{sk_A}$;
- 计算明文 $m=c_3'\oplus H_3(k)$;
- 计算 $r=H_2(m||k)$,若 $c_1'=g^r$ 且 $c_2'=k\cdot e(pk_B,H_1(pk_B\|\alpha))^r$,则输出明文 m.

4 综合分析

4.1 安全性证明与分析

PAUA 机制的核心是 PRE 算法,因此 PAUA 的安全性依托于 PRE 的安全性,为安全性证明构造安全模型.参照文献[15]进行证明.

DBDH(决策双线性 diffie-Hellman 问题(decisional bilinear diffie-Hellman))困难问题:给定形如$\langle g,g^a,g^b,g^c,g^{abc}\rangle$的结构,令算法$\mathcal{A}$进行 $z=abc \bmod p$ 的运算,当且仅当$|\Pr[A(g,g^a,g^b,g^c,e(g,g)^{abc})=0]-\Pr[A(g,g^a,g^b,g^c,e(g,g)^z)=0]|\leqslant\varepsilon$,$\mathcal{A}$具有$\varepsilon$的优势解决 DBDH 问题.

(1) 复杂性假设

DBDH 假设:不存在算法$\mathcal{A}$,使其在概率多项式时间内具有ε优势解决 DBDH 问题,则称 DBDH 假设成立.

(2) PAUA 的代理重加密安全模型

攻击者$\mathcal{A}$可以对 *KeyGeneration*、*RkPara*、*ReKeyGen*、*ReEncrpytion*、*Decryption* 等过程进行询问和挑战.

初始化:由挑战者选择参数,生成初始系统初始系数 *param*.

阶段 1:攻击者$\mathcal{A}$询问以下的过程完成阶段 1 的工作.

KeyGeneration、*RkPara*、*ReKeyGen*、*ReEncrpytion*、*Decryption*,使用 *KeyGeneration* 产生的密钥.

挑战:$\mathcal{A}$在阶段 1 后,将输出两个长度相同的明文$m_0,m_1\in M$,解密参数α^*,由 *RkPara* 生成的重加密参数β^*及被攻击目标的公钥pk^*,此处的pk^*由 *KeyGeneration* 产生,私钥未被泄露.当$\mathcal{A}$以$(\beta^*,\beta',\alpha^*)$询问 *ReKeyGen* 函数时,$\beta'$对应的私钥是保密的.挑战者选取$b\in\{0,1\}$作为随机比特,计算用于挑战询问的密文$C_b=Encrpytion(m_b,pk^*)$.

阶段 2:$\mathcal{A}$继续阶段 1 中的询问,同时满足以下条件.

(1) 当$\mathcal{A}$以$(\beta^*,\beta',\alpha^*)$对 *ReKeyGen* 进行询问时,$\beta'$的私钥保密;

(2) 当以$(C_b,\beta^*,\beta',\alpha^*)$对 *ReEncrpytion* 进行询问时,$pk'$的私钥保密;

(3) 当$\mathcal{A}$以$(\beta^*,\beta',\alpha^*)$对 *ReKeyGen* 进行询问时,则不可使用$C_b'$询问 *Decryption*,其中,$C_b'$为 *ReEncryption*$(C_b,\beta^*,\beta',\alpha^*)$的有效输出.

猜测:$\mathcal{A}$提出$b'\in\{0,1\}$的猜测,若$b'=b$,则说明挑战成功.

将$\mathcal{A}$在上述挑战中获胜的优势定义为ε,且$\varepsilon=\left|\Pr[b'=b]-\frac{1}{2}\right|$可忽略不计,则称$\mathcal{A}$挑战失败,也可以推出方案是选择密文安全的.

定理. 假设有群(G_1,G_2),如果 DBDH 在这个群组上成立,则说明 PAUA 方案的算法在随机语言模型下是选择密文安全的.

证明:上述定理的证明相当于证明$\mathcal{A}$以优势ε进行挑战,若ε可以忽略则说明定理成立.

首先定义挑战游戏$\mathcal{G}_i(i=0,\ldots,5)$,挑战者$\mathcal{C}$.$T_i$表示游戏中事件$b'=b$的发生.

(1) $\mathcal{G}_0$:挑战者$\mathcal{C}$对$\mathcal{A}$随机的问询诚实回答,同时对$H_i^{list}(i=1,...,4)$进行初始化,分别取$\pi_1,\pi_4\in G_1,\pi_2\in Z_p^*,\pi_3\in\{0,1\}^l$,分别将$(pk_i,\pi_1),(m,k,\pi_2),(k,\pi_3),(c_1,c_2,c_3,c_4,\pi_4)$存放到$H_i^{list}(i=1,...,4)$中.令$\delta_0=\Pr[b'=b]$,则$\left|\delta_0-\frac{1}{2}\right|=\varepsilon$.

(2) $\mathcal{G}_1$:挑战者$\mathcal{C}$采用$\mathcal{G}_0$中通的流程进行游戏,除了以下差异:$\mathcal{C}$随机选取$\tau\in\{1,2,\ldots,p+1\}$,问询$H_1$$\tau$次,当$\mathcal{C}$受到$\mathcal{A}$的挑战时,如果$\mathcal{A}$问询$H_1$,则$\mathcal{C}$停止游戏,$\mathcal{C}$成功的概率至少为$\frac{1}{p+1}$.在游戏$\mathcal{G}_1$中$\delta_1=\Pr[b'=b]$,则$\Pr[T_1]=\frac{\delta_1}{p+1}$.

(3) $\mathcal{G}_2$:挑战者$\mathcal{C}$采用$\mathcal{G}_1$中流程进行游戏.因为哈希函数H_i定义为标准的随机过程,故$|\Pr[T_1]-\Pr[T_2]|$可忽略.

(4) $\mathcal{G}_3$:挑战者$\mathcal{C}$采用$\mathcal{G}_2$中通的流程进行游戏,除了以下差异:调用 *Decryption* 时如果输入(C,β^*,α^*),$\mathcal{A}$没有对H_1使用$(\beta^*||\alpha^*)$询问,则$\mathcal{C}$停止游戏;否则,$\mathcal{C}$将解密结果反馈给$\mathcal{A}$.因为加解密算法确定,哈希函数标准随机,故

$|\Pr[T_2]-\Pr[T_3]|$可忽略.

(5) $\mathcal{G}_4$:挑战者$\mathcal{C}$采用$\mathcal{G}_3$中通的流程进行游戏,除了以下差异:调用 *ReKeyGen* 中$\mathcal{C}$使用$\mathcal{A}$提出的(β,α)对重加密密钥列表进行查询,若有结果,$\mathcal{C}$为$\mathcal{A}$反馈 $rk_{A\to B}=(pk_B, pk_B^r, H_1(pk_B \| \alpha)\cdot H_1(pk_A)^{sk_A}, g^{-r})$;否则,$\mathcal{C}$依据$\beta,\alpha$进行查询.

- 如果用户 A 的私钥泄露,即 $sk_A=x_A$;
- 如果 A 的密钥未泄露,则首先计算 A 的密钥,令 $a\in G_1$,则 $sk_A=ax_A$;
- 若 B 的私钥泄露,则$\mathcal{C}$反馈终止.

调用 *ReEncrpytion* 时$\mathcal{C}$采用来自$\mathcal{A}$的(β,α,C_i)产生 *ReEncrpytion* 中参数,如果失败,则$\mathcal{C}$终止游戏;否则,$\mathcal{C}$通过密钥和重加密密钥列表查询,为$\mathcal{A}$反馈密文数据.$\mathcal{A}$在 *ReKeyGen* 挑战必须通过 *KeyGeneration* 获取的 pk_B.$|\Pr[T_3]-\Pr[T_4]|$可忽略.

(6) $\mathcal{G}_5$:挑战者$\mathcal{C}$采用$\mathcal{G}_4$中通的流程进行游戏,在接到$\mathcal{A}$的挑战(m_0,m_1,α)后,$\mathcal{C}$计算首次解密密文.$\mathcal{G}_5$和$\mathcal{G}_4$的差别就在于是否问询了 H_3,但是由于 H_3 问询难度等同于 DBDH 问题,因此$|\Pr[T_4]-\Pr[T_5]|$可忽略.因此 $\Pr[T_5]=\frac{1}{2(p+1)}$.

基于步骤(1)~步骤(6)的分析,结合文献[15],攻击者$\mathcal{A}$获胜的概率可以忽略,说定理成立.证毕. □

其次,方案具备了抵抗密码分析和合谋攻击的能力.数据创建者 A 将重加密密钥对应的参量进行划分,其中,β中包含了创建者 A 和共享用户 B 的公钥信息以及 $pk_A^{sk_A}$,RKG 通过与共享用户 B 合谋,基于 $pk_A^{sk_A}$ 获取 A 的私钥 $sk_A=\log_{pk_A} pk_A^{sk_A}$ 属于计算离散对数问题,因此无法获取 A 的私钥.

4.2 性能分析

为了描述算法的性能,此处假设 t_e,t_l 分别表示指数和线性对运算的时间开销.本文中主要函数时间开销见表 2.

Table 2 Time complexity of main functions for PAUA

表 2 PAUA 主要函数时间复杂度

函数 时间开销	*Encryption* $3t_e+t_l$	*Decryption* $3t_e+2t_l$	*ReEncryption* $2t_e+2t_l$

下面分析空间复杂度,本方案中的空间复杂度主要在于用户端密钥存储的开销,该机制中,用户无需提供私钥之外的数据存储,因此,空间复杂度为 $O(1)$.

4.3 属性分析

PAUA 方案中综合了代理重加密技术和权限的确定性更新,通过可信第三方服务器 RKM、云端重加密密钥生成服务器 RKG、重加密服务器 Re-Enc 用于系统不背书,能够在未增加用户计算量和密钥管理量的前提下,实现用户数据授权变更时,重加密密钥的确定性更新.下面针对是否支持密文数据访问管理、是否支持授权变更、授权更新是否具有确定性以及加密运算和密钥管理参与方等方面,将 PAUA 与研究现状进行对比,见表 3.本节选择有代表性的 5 个方案与 PAUA 进行比较,其中,ABAC[16]针对权限变更进行了详细的描述,但是并未论述密文访问控制和管理的方案;EABDS[17]支持密文访问控制能够进行权限的更新,但是就确定更新的方面缺乏支持,同时,用户需要复杂自身数据的加解密运算,并进行大量密钥管理工作;文献[7]在密文访问控制和权限确定性更新方面提供了支持,但是用户的运算量和密钥管理量较大;文献[14]和 ACC-PRE[18]将云服务器引入到密文数据的处理和密钥管理中,减轻了用户的负担,但是缺乏对权限确定性更新的论述.

通过分析,PAUA 具有如下属性.

1) 支持密文数据访问控制.PAUA 方案基于代理重加密技术,对数据进行加密、重加密处理后以密文的形式进行存储、访问和流通.

2) 支持权限的撤销、变更.PAUA 中将通过重加密密钥的管理实现对密文数据访问的管理,当用户需要变更权限时,通过控制重加密密钥和密文的产生即可实现.

3) 权限的更新具有确定性.重加密密钥的产生参数划分为两部分,其中,一部分存储到重加密密钥生成服务器,由云端进行运维;另一部分则存储到可信服务器 RKM 中,由用户进行管理,当需要授权更新时,用户撤销 RKM 中的密钥参数分量,与之对应的密文数据将无法解密,实现确定性权限更新.

4) 适用于个人用户,对于系统的性能、运算能力和存储能力没有过高的要求.

Table 3 Comparison between PAUA and current schemes

表 3 PAUA 与现有机制对比分析

模型	属性				
	密文访问控制	授权变更	授权变更确定性	加密数据运算执行方	密钥管理参与方
ABAC[16]	×	√	√	–	–
EABDS[17]	√	√	×	用户	用户
文献[7]	√	√	√	用户	用户
文献[14]	√	√	×	用户+云服务器	用户+云服务器
ACC-PRE[18]	√	×	×	用户+云服务器	用户+云服务器
PAUA	√	√	√	用户+云服务器	用户+云服务器

注:ABAC 并未针对密文进行访问控制,因此不涉及加解密和密钥管理问题

5 结 论

本文提出了一种提出一种基于代理重加密的云端数据权限确定性更新方案(PAUA).首先,给出了 PAUA 机制成立的系统假设和前提条件;其次,论述了 PAUA 的系统模型、基本系统流程和算法;最后,将 PAUA 与现有研究成果进行对比,提出 PAUA 的优缺点.通过 PAUA 方案,一方面,用户在托管数据前仅进行一次数据初始加密,其后则交付重加密服务器进行再处理,减轻了用户的计算和存储负担;另一方面,用户创建数据的同时,进行代理重加密密钥的约束,将重加密密钥生成的参数进行分割,一部分交由云端代理重加密服务器管理,另一部分则为创建者控制,实现确定性的授权更新.PAUA 方案的提出,将为云端数据访问控制的可信实施奠定基础.

References:

[1] Zhou L, Varadharajan V, Hitchens M. Trust enhanced cryptographic role-based access control for secure cloud data storage. IEEE Trans. on Information Forensics and Security, 2015,10(11):2381−2395.

[2] Zhu Y, Huang D, Hu CJ, Wang X. From RBAC to ABAC: Constructing flexible data access control for cloud storage services. IEEE Trans. on Services Computing, 2015,8(4):601−616.

[3] Rezaeibagha FY, Mu Y. Distributed clinical data sharing via dynamic access-control policy transformation. Int'l Journal of Medical Informatics, 2016,89:25−31.

[4] Wang J, Huang CH, Wang JH. An access control mechanism with dynamic privilege for cloud storage. Journal of Computer Research and Development, 2016,53(4):904−920 (in Chinese with English abstract).

[5] Li J, Yao W, Zhang Y, Qian H, Han J, Flexible and fine-grained attribute-based data storage in cloud computing. IEEE Trans. on Service Computer, 2017,10(5):785−796.

[6] Li J, Yao W, Han J, Zhang Y, Shen J. User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage. IEEE Systems Journal, 2017,12(2):1767−1777. [doi: 10.1109/JSYST.2017.2667679]

[7] Ye J, Zhang W, Wu S, Gao Y, Qiu J Attribute-based fine-grained access control with user revocation. In: Proc. of the ICT-EurAsia 2014. 586−595.

[8] Xu P, Jiao T, Wu Q, Wang W, Jin H. Conditional identity-based broadcast proxy re-encryption and its application to cloud email. IEEE Trans. on Computers, 2015,65(1):66−79.

[9] Zhang Y, Li J, Chen X, Li H. Anonymous attribute based proxy re-encryption for access control in cloud computing. Security and Communication Networks, 2016,9(14):2397−2411.

[10] Li J, Zhao X, Zhang Y, Yao W. Provably secure certificate-based conditional proxy re-encryption. Journal of Information Science and Engineering, 2016,32(4):813−830.

[11] Yang Y, Lu H, Weng J, Zhang Y, Sakurai K. Fine-grained conditional proxy re-encryption and application. In: Proc. of the ProvSec. 2014. 206−222.

[12] Su M, Shi GZ, Xie RN, Fu AM. Multi element based on proxy re-encryption scheme for mobile cloud computing. Journal on Communications, 2016,36(11):73−79 (in Chinese with English abstract).

[13] Tang Q. Type-based proxy re-encryption and its construction. In: Proc. of the INDOCRYPT 2008. Berlin, Heidelberg: Springer-Verlag, 2008. 130−144.

[14] Yu S, Wang C, Ren K, Lou W. Achieving secure, scalable, and fine-grained data access control in cloud computing. In: Proc. of the IEEE INFOCOM. 2010. 1−9.

[15] Su M, Cao MY, Xie RN, Fu AM. PRE-TUAN: Proxy re-encryption based trusted update scheme of authorization for nodes on IoT cloud. Journal of Computer Research and Development, 2018,55(7):125−133 (in Chinese with English abstract).

[16] Servos D, Osborn S. Current research and open problems in attribute-based access control. ACM Computing Surveys (CSUR), 2017,49(4):65.1−65.45.

[17] Huang Q, Ma Z, Yang Y, Fu J, Niu X. EABDS: Attribute-based secure data sharing with efficient revocation in cloud computing. Chinese Journal of Electronics, 2015,24(4):862−868.

[18] Su M, Li F, Shi G, Geng K, Xiong J. A user-centric data secure creation scheme in cloud computing. Chinese Journal of Electronics, 2016,25(4):753−760.

附中文参考文献:

[4] 王晶,黄传河,王金海.一种面向云存储的动态授权访问控制机制.计算机研究与发展,2016,53(4):904−920.

[12] 苏铓,史国振,谢绒娜,付安民.面向移动云计算的多要素代理重加密方案.通信学报,2016,36(11):73−79.

[15] 苏铓,曹梦元,谢绒娜,付安民.基于代理重加密的物联网云节点授权可信更新机制.计算机研究与发展,2018,55(7):125−133.

苏铓(1987－),女,内蒙古赤峰人,博士,副教授,CCF 专业会员,主要研究领域为云计算安全,访问控制,代理重加密.

俞研(1972－),男,博士,副教授,CCF 专业会员,主要研究领域为网络安全.

吴槟(1980－),男,博士,副研究员,CCF 高级会员,主要研究领域为网络与信息系统安全,信息对抗理论与技术.

张功萱(1961－),男,博士,教授,博士生导师,CCF 杰出会员,主要研究领域为可信计算与网络安全, Web 服务与分布式系统.

付安民(1981－),男,博士,副教授,CCF 高级会员,主要研究领域为云计算安全,物联网安全.