计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2017.20170902
54(12): 2818-2824, 2017

采用扩展公钥的云存储广播加密优化方法

李春花 王 桦 张彦哲 周 可
(武汉光电国家实验室(华中科技大学) 武汉 430074)
(li.chunhua@hust.edu.cn)

Optimization for Broadcast Encryption in Cloud Using Extended Public Key

Li Chunhua, Wang Hua, Zhang Yanzhe, and Zhou Ke
(*Wuhan National Laboratory for Optoelectronics* (*Huazhong University of Science and Technology*), *Wuhan* 430074)

Abstract Security issues have been a major hurdle for the application of cloud storage. As data encryption is the mainstream method to ensure confidentiality, users always share their data by means of key's management and distribution. However, how to manage massive keys and distribute them securely and efficiently is a challenge in cloud storage. In recent years, broadcast encryption scheme has been paid more attention by researchers to mitigate above problems for cloud data sharing. Since current schemes take insufficient account of changes of users and users's privilege, they do not perform well in cloud. To reduce the overhead of key distribution, an optimization method is proposed for public-key based broadcast encryption in this paper. First, the scope of public keys is expanded to two or more times and the initial related parameters used for generating public keys are kept simultaneously. These parameters can ensure private keys distributed previously still available when they are employed to generate the new public keys for new valid users, thus greatly decreases the cost of redistributing private keys. Second, lazy revocation is adopted to reduce the cost of updating keys. Experimental results show that our optimized method outperforms the existing schemes while adding new users and revoking users' privilege in cloud.

Key words cloud storage; broadcast encryption; extended public key; key management; optimization

摘 要 基于广播加密的云存储系统受到研究者的关注.然而,基本的广播加密方案不能适应云存储环境中用户和权限的动态变更情况.针对广播加密中密钥管理分发开销大的问题,提出一种扩展公钥的广播加密优化方法,通过保留初始产生公钥时使用的部分私有参数,当用户加入或撤离系统时,使用保留的私有参数产生新的公钥来加密数据.这样,合法用户仍可以使用之前已分发的私钥解密新公钥加密的数据,从而避免了用户动态变化时公钥的频繁变化和密钥的重复分发.通过引入懒惰回收机制,降低了权限变更和密钥定期更新带来的开销.测试结果表明:采用优化方案后,增加用户数量和权限撤销时,系统性能得到较大提高.

关键词 云存储;广播加密;扩展公钥;密钥管理;优化

中图法分类号 TP391

收稿日期:2015-10-12;**修回日期**:2017-04-14

基金项目:国家重点研发计划项目(2016YFB0800402);中央高校基本科研业务费专项资金项目(2016YXMS020)
This work was supported by the National Key Research and Development Program of China (2016YFB0800402) and the Fundamental Research Funds for the Central Universities(2016YXMS020).

通信作者:王桦(birch_wh@163.com)

万方数据

近年来,云存储因其价格低廉、部署方便、随时随地可用等优点而成为信息领域的一大研究热点.然而,用户将数据存放到云端之后便失去了对数据的直接控制,存放在云端的数据能否得到安全的管理和有效的访问控制一直是用户担忧的问题,尤其是近年来屡次出现的一些隐私泄露、数据丢失等安全事件,给云存储系统的进一步推广应用带来了很大的阻碍[1-2].

数据加密技术是提高存储系统安全和数据安全的一种基本方法,将数据在上传到云端之前进行加密可以有效地保护数据的机密性.云存储系统中由于用户群体广泛、文件数量巨大,因此管理数据密钥和会话密钥非常复杂,加上云用户时不时地加入和撤离系统,导致密钥更新频繁,极大地影响了系统的性能.如何提高云存储系统中密钥管理的安全性、如何降低密钥重分发的性能开销是云存储安全研究的重要内容之一.

已有的安全云存储系统中针对密钥的管理和分发提出了很多方法.Adya 等人[3]提出一种无密钥服务器的分布式文件系统 FARSITE,他们采用对称密钥加密文件,并用被授权用户的公钥加密对称密钥后存储在云端,这种方式在权限变更时计算开销较大.文献[4]提出的 Plutus 系统中文件和目录都进行了加密,通过 file-groups 实现文件之间权限的共享,减少了分发密钥的次数;但是 Plutus 系统中用户是直接向数据拥有者请求密钥的,这样不仅增加了数据拥有者的负载,更重要的是在数据拥有者离线时无法获取文件访问权限,这种设计模式也使得权限的撤销变得更加复杂.Goh 等人[5]提出一种中间件形式的安全存储系统 SiRiUS,每个文件采用对称密钥进行加密,并用非对称密钥进行文件签名,以确保文件的完整性.同时每个用户拥有 2 个对应的非对称密钥用于加密文件密钥和签名密钥,并存储在元数据中以方便分发.这种方法虽然结合了 FARSITE 和 Plutus 的优点,但并没有克服密钥重分发和带宽开销较大问题,其扩展性不足以适应云存储环境.

文献[6]提出的 Cloudproof 系统使用广播加密机制进行密钥分发,密钥的管理比 SiRiUS 更加简单.同 Plutus 系统类似,Cloudproof 系统中也使用了群组的方式减少密钥数量,采用 block-group 将权限相同的块使用相同的密钥加密,虽比 Plutus 访问控制粒度更细,但并没有解决撤销权限时的开销问题.而且,Cloudproof 系统采用的是固定公钥广播加密方案,密文和私钥的大小固定,但要求接收用户集合在系统建立时就能唯一确定,此后若有用户加入或离开,则计算开销会很大,因此无法适应用户变化频繁的云存储环境.文献[7-8]提出了动态广播加密的概念,用户可以在广播系统建立之后再加入到系统中,但由于加解密时间开销较大,无法满足云存储系统的性能要求.文献[9]提出一种使用多重线性映射方法解决公钥广播加密中长期存在的性能开销问题,但不能保证重新生成的随机数是有效的,从而增加了系统的不稳定性.

本文将在 Cloudproof 基础上,对其使用的广播加密方案进行优化,通过扩展公钥和保留系统初始阶段产生公钥时所使用的部分私有参数来提高密钥管理的效率和权限变更时的性能.当用户加入或撤离系统时使用保留的私有参数产生新的公钥来加密数据,这样已授权用户仍可以使用之前分发的私钥来解密采用新公钥加密的数据,从而避免了因用户和权限的动态变化而导致频繁的公钥变化和密钥重分发等问题.

1 背景知识

广播加密用于在广播信道上传输加密的消息[10],通过广播加密进行加密的内容只有加密时选定的授权用户集合中的用户才能正确解密.密钥由数据拥有者管理,无需在系统中引入第三方,且数据拥有者不需要长期在线,大大简化了密钥管理的复杂性.本文采用文献[11]提出的公开密钥广播加密方案(BGW 方案),针对该方案应用在云存储环境中产生的问题进行优化.

1.1 双线性映射

设 G 和 G_1 是阶为 p 的乘法循环群,g 是群 G 的生成元,称映射 $e:G\times G\to G_1$ 为一个双线性映射,如果 e 满足 3 个性质:

1) 可计算性(computable).存在有效算法对 $\forall R,S\in G$,计算 $e(R,S)$ 的值.

2) 双线性(bilinear).对于 $\forall R,S\in G$ 和 $a,b\in Z_p$,都有换算关系:

$$e(R^a,S^b)=e(R,S)^{ab}. \tag{1}$$

3) 非退化性(non-degelerate).

$$e(g,g)\neq 1. \tag{2}$$

映射过程中用到的一些数学符号定义如下:

Z_p——模 p 的加法群$\{0,1,\cdots,p\}$;

G——包括 G 和 G_1,均是阶为 p 的乘法循环群;

万方数据

g——群 G 的生成元；

$e(\ ,\ )$——双线性映射.

1.2 BGW 方案

在 BGW 方案中，一个广播加密系统由 3 部分组成.

1) Setup(n). 输入接收者的数量 n，输出 n 个私钥 $d_1, d_2, \cdots, d_n$ 和公钥 PK. 具体过程如下：

选取 G 的任意生成元 $g \in G$ 和任意 $a \in Z_p$，对于 $i = 1, 2, \cdots, 2n$，计算 $g^{(a^i)} \in G$，将 $g^{(a^i)}$ 视作 g_i. 选取任意 $\gamma \in Z_p$，计算 $v = g^{\gamma} \in G$，最终得到：

$$PK = (g, g_1, \cdots, g_n, g_{n+2}, \cdots, g_{2n}, v). \tag{3}$$

计算用户私钥：

$$d_i = g_i^{\gamma} \in G. \tag{4}$$

2) Encrypt(S, PK). 输入一个接收者的子集 $S \subseteq \{1, 2, \cdots, n\}$ 和公钥 PK，输出 (Hdr, K). 其中 K 作为对称密钥用于加密，Hdr 则是本次加密产生的公开信息. 具体过程为：

在 Z_p 中选取随机的 t，使用 t 计算 $K = e(g_n, g_1)^t \in G_1$，$Hdr = (g^t, (v \times \prod_{j \in S} g_{n+1-j})^t)$，之后将 Hdr 记作 (C_0, C_1).

3) Decrypt(S, id, d_i, Hdr, PK). 输入公钥 PK、步骤 2 中输入的 S 和产生的 Hdr 以及用户的 id 和私钥 d_i，输出 K，用 K 解密数据：

$$K = e(g_i, C_1) / e(d_i \times \prod_{\substack{j \in S \\ j \neq i}} g_{n+1-j+i}, C_0). \tag{5}$$

BGW 方案中用户需要存储的私钥 d_i 大小固定，加解密时都需要使用公钥 PK，公钥大小为 $O(n)$，解密时还需要广播头 Hdr，Hdr 的大小固定，加解密的运算量均为 $O(t)$(与授权用户数相关).

2 基本方案及优化方法

本节分析了基于广播加密的密钥分发基本方案，指出了其中的不足，在此基础上提出了适用于云环境的广播加密优化方法.

2.1 基于广播加密的密钥分发基本方案分析

在云存储环境中使用广播加密管理密钥时，系统由 3 部分构成：云端、数据拥有者和普通用户. 每个用户都可以同时是数据拥有者和普通用户.

图 1 描述了用户与云端的交互过程。其中，用户 1 对于其上传到云端的文件来说是数据拥有者，用户 2 和用户 3 可以向用户 1 请求这些文件的访问权限，同时当用户 1 请求用户 2 和用户 3 的文件权限时又是普通用户. 所有文件的权限都由对应的文件上传者管理，云端只负责接收文件的读写请求，无法对没有权限的用户授权，也无法获取文件内容.

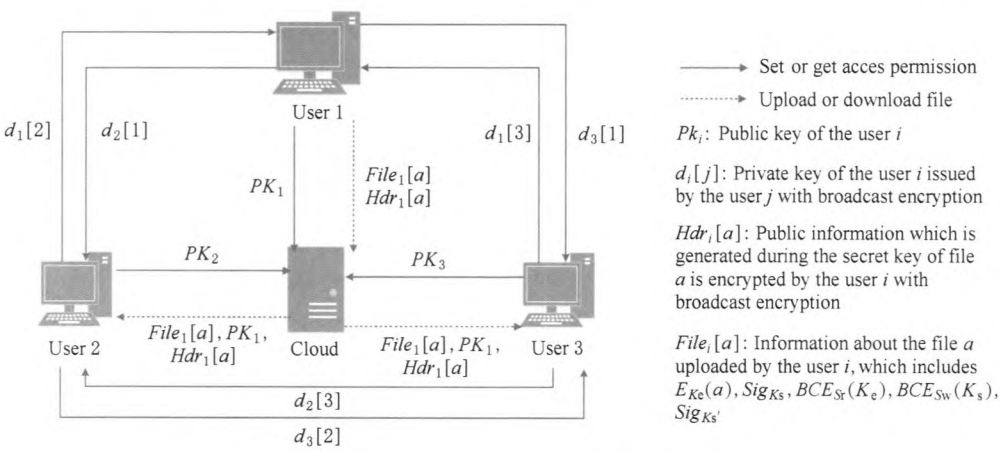

Fig. 1 Interactive processes between the user and the cloud

图 1 用户和云端的交互过程

1) 区分文件读写权限

数据拥有者上传文件之前首先使用对称加密算法加密文件，加密文件使用的密钥记作 K_e；之后选取一对非对称加密体制中的公私钥 K_v 和 K_s，使用私钥 K_s 对加密后的文件生成一个签名 Sig，并将签名和 K_v 与文件一起上传到云端. 这样数据拥有者就可以通过分发 K_e 和 K_s 的方式向用户授予读写权限. 得到 K_e 的用户可以解密出文件内容，即拥有读权限. 用户在每次修改文件内容时需要使用 K_e 将文件重新加密，然后使用 K_s 重新生成签名，云端需要在用户每次提交读请求时使用 K_v 检查签名是否正确，所以只有持有 K_s 的用户拥有写权限.

2) 授予用户权限

数据拥有者通过广播加密将读写密钥分发给其

万方数据

他用户,选取拥有读权限的用户集合 S_r 和拥有写权限的用户集合 S_w,分别用 2 个集合为参数使用广播加密将 K_e 和 K_s 加密,将加密后的 K_e 和 K_s 与文件一起上传到云端,这样有权限的用户就可以通过自己事先从数据拥有者获取到的广播加密私钥 d_i 解密出对应的 K_e 或 K_s,从而获取文件的权限.撤销用户权限时需要先生成新的读写密钥,将对应的密钥重新使用广播加密方案加密后上传.如果更新了读密钥还需要重新加密文件.

在系统初始化之后,数据拥有者保存了公钥 PK 和用户数 n,云端保存了公钥 PK,其他用户只保存自己对应的私钥 d_i.

在上传某个文件之后,数据拥有者和其他用户保存的内容不变,而云端则需要额外存储对应的用户集合 S_r,S_w 和广播加密生成的公开信息 Hdr.

如图 2 所示,存储在云端的文件信息包括 2 部分:数据内容(data block)和密钥内容(key block).其中,$E_{K_e}(data)$ 表示使用密钥 K_e 加密的数据,Sig_{K_s} 表示使用 K_s 生成的签名.$BCE_{S_r}(K_e)$ 表示对有读权限的用户集合 S_r 做广播加密之后的 K_e,$BCE_{S_w}(K_s)$ 表示对有写权限的用户集合 S_w 做广播加密之后的 K_s,修改 key block 这部分内容意味着将会改变对文件有操作权限的用户集合,所以只有数据拥有者才有权限修改 key block 信息,数据拥有者在上传文件时产生一对公私钥 K'_v 和 K'_s,并将 K'_v 上传到云端,每次修改 key block 时使用 K'_s 对 key block 中的内容生成签名 $Sig_{K'_s}$,这样云端就可以通过 K'_v 验证是否是数据拥有者进行的修改.

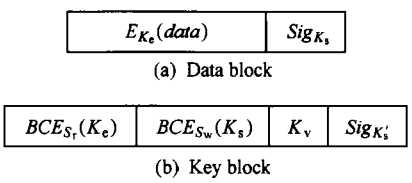

Fig. 2 Data format stored in the cloud

图 2 存储在云端的数据格式

从上述数据交互和密钥分发的过程可以看出:用户加入系统时需要获取其他所有用户分发的广播加密私钥,也需要向其他所有用户分发广播加密私钥,导致空间开销和带宽开销都很大.由于广播加密的初始阶段是根据当前指定的用户数进行初始化的,新用户加入系统必然引起所有用户的重新初始化,此时产生的新私钥和原有的私钥不同,文件也需要重新加密,因此导致时间开销和带宽开销都很大.针对以上问题本文提出一种针对广播加密的扩展公钥方法,以降低用户数量变化时密钥重分发引起的时间开销和带宽开销.

2.2 扩展公钥优化方法

广播加密系统中,用户之间交互时由于相互存储了对方提供的广播加密私钥,造成存储空间的浪费,同时也增加了用户分发私钥的时间开销.实际情况中用户不会向所有其他用户请求文件,因此,在用户加入系统时可以不获取所有私钥,而是在第 1 次请求文件时数据拥有者才向他分发广播加密私钥,这样不仅减少了用户存储的私钥数量,也减少了分发私钥的次数,从而减少了网络开销.然而当系统用户数增加时仍然会产生重新初始化的问题,针对此问题本文提出一种扩展公钥的方法,在撤销用户权限时使用懒惰回收策略以减少文件重加密引起的开销.

由 2.1 节可知,广播加密公钥 PK 和用户私钥 d_i 都是在系统初始化阶段生成:

$$PK=(g,g_1,\cdots,g_n,g_{n+2},\cdots,g_{2n},v),$$

$$d_i=g_i^{\gamma}.$$

其中,$g_i=g^{(\alpha^i)}$,$v=g^{\gamma}$.由生成方法可知,若数据拥有者保留初始化阶段选择的参数 α 和 γ,则对于新生成的一个公钥 PK':

$$PK'=(g,g_1,\cdots,g_n,g_{n+1},g_{n+3},\cdots,g_{2n},g_{2n+1},g_{2n+2},v),$$

增加一个私钥 $d_{n+1}=g_{n+1}^{\gamma}$ 时,使用新的公钥加密的文件,已授权用户使用原有的私钥仍然可以解密.

在新公钥中增加的 g_{n+1} 会破坏原有公钥的安全性,原有公钥中的 g_{n+2} 也会影响新公钥的安全性,因此如果按这种方式扩展公钥就需要将公钥扩展为原本的 2 倍大小以确保安全.用户请求私钥时先检查当前的公钥是否还可以产生新私钥,如果不可以再进行扩展.由于更新了广播加密公钥,之前的 key block 需要重新加密,这部分开销与文件数相关.

用户进行广播加密和解密时都需要下载公钥,实际加解密时使用的并不是公钥中的全部参数,而是有权限的用户对应的那一部分,若改变公钥的存储方式,让用户可以选择性地下载公钥中的某些参数,则可以将用户进行广播加解密时的带宽开销从 $O(n)$ 降低到 $O(t)$,其中 n 表示公钥能产生的私钥数,t 表示本次加密有权限的用户数.

2.3 懒惰权限回收的优化策略

本方案中,数据拥有者在撤销用户读权限之后生成新的对称密钥,并对新的有读权限的用户集合

万方数据

广播加密,使用版本号区分新旧密钥并且将版本号附在文件后上传到云端,用户在读文件时根据文件当前加密使用的版本号选取对应的密钥解密文件.用户提交写操作时使用最新的密钥加密,当文件密钥版本更新到最新之后,下次数据拥有者修改 key block 内容时将旧版本密钥丢弃.撤销用户写权限时生成新的公私钥对并立刻更新 key block 中的内容和文件签名即可.

之所以保留当前版本到最新版本的密钥,是因为如果数据拥有者在更新密钥时删除当前版本和最新版本之间的密钥,有可能在更新权限时有其他用户在进行写操作,那么其他用户加密使用的密钥会被丢弃,从而使得文件无法解密.而更新写密钥时进行写操作只会导致云端验证不通过,用户可以重新获取写密钥生成签名或重新提交写请求.

图 3 显示了引入懒惰回收机制后云端数据的格式变化.其中,VER_{K_c} 表示当前 K_c 的版本,保存从版本号 m 到版本号 n 的加密密钥,并且 $m \leqslant VER_{K_c} \leqslant n$,若数据拥有者此时修改 key block,则会删除 key block 中 VER_{K_c} 之前的 $BCE_{S_r}(K_c)$.相比每次撤销权限时立刻重新加密文件,懒惰回收降低了重新下载/上传文件的带宽开销和重新加密文件的时间开销,本方案中采用懒惰回收机制还可以将开销集中在重加密体积较小的 key block 上,从而进一步降低了回收性能开销.

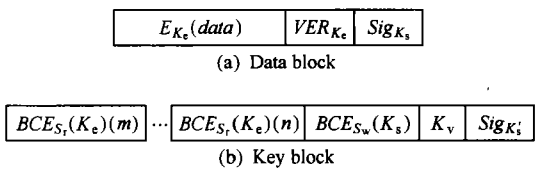

Fig. 3 The cloud data format when lazy revocation is introduced

图 3 引入懒惰回收后云端数据的格式

2.4 安全性分析

BGW 方案的安全性是基于 BDHE 假设的,可以抵抗完全同谋攻击,即所有无权限用户联合起来也不能获得广播加密明文,适合在云环境中保护密钥所需要的安全性,因此数据拥有者可以使用基本方案安全地分发密钥.

采用扩展公钥方法后,新产生的公钥中 g_{n-1} 会破坏原有公钥的安全性,因此在扩展公钥之后需要将 key block 使用新的公钥重加密.重新加密避免了增加用户带来的安全风险,但是也产生了额外计算开销,这部分开销会使得扩展公钥时用户加入所需的时间较长.原有公钥中的内容均包含在新公钥中,不会影响新公钥的安全性.由于数据拥有者需要保留 α 和 γ 以生成新公钥,而公开 α 会使得 BDHE 假设不成立,公开 γ 使得用户可以计算其他用户的私钥,因此数据拥有者需要避免 α 和 γ 的泄露.

引入懒惰回收机制,使得用户在被撤销读权限之后、文件读密钥更新之前仍可以使用之前的读密钥解密文件,即:若用户缓存了文件读密钥,则在文件密钥更新之前仍可以读取文件,这在一定程度上降低了安全性,但是用户被撤销权限之后只能获得修改之前的文件内容,无法获取文件最新内容,从而保护了修改后文件的安全访问.这样的权衡自然一定程度上降低了安全性,但是考虑到一旦用户可以读文件内容即可以保留一份文件的副本,本方法认为延长用户对文件历史版本的读权限的有效时间,虽然增加了信息泄露风险但提高了系统的整体性能,这种平衡策略是可以接受的.

3 性能评估

在开源云存储项目 OpenStack 的 Swift 平台上对本文方案进行了测试.密钥管理分发方案的额外开销主要产生在用户数量变化和密钥变化时,本文将从这 2 方面进行对比测试.

由 BGW 方案的介绍可知,方案中私钥 d_i 大小固定,加解密时都需要使用公钥 PK,公钥大小为 $O(n)$,初始化产生一个公钥的时间也是 $O(n)$,解密时还需要广播头 Hdr,Hdr 的大小固定,加解密的运算量均为 $O(t)$.对于扩展公钥的方法来说,加解密的运算量不变,扩展公钥到可以支持 n 个用户时的时间开销为 $O(n)$.

在实际使用中,当前对算法的实现中单个私钥大小为 276 B,Hdr 大小为 216 B,而公钥的大小则和用户数量相关,在用户数为 8 192 时约 7 MB.根据所使用的加密算法不同,key block 的大小也会不同,这部分开销与系统的具体实现相关.

3.1 扩展公钥方法的对比测试

在使用广播加密前需要针对对应的用户数量进行初始化.对于基本方案,有新用户加入系统时,系统中的其他用户都需要更新用户数并进行初始化,该用户也需要针对系统中其他用户做初始化.采用扩展公钥方法之后,用户第 1 次初始化产生一定大小的公钥,之后通过扩展公钥的方式适应用户数或角色数的变化.

万方数据

图 4 可以看出,系统采用扩展公钥优化方法之后,增加新用户时时间开销大大降低.基本方案中,每次加入新用户产生的重新初始化时间开销很大,增加 300 个用户的时间超过 770 s.对于扩展公钥方法,在当前公钥可以分配的私钥用完之前增加用户的开销非常低,增加 300 个用户的时间小于 10 s,增加 10 000 个用户的时间是 284.37 s(由于横坐标的关系,未在图上表示出来),而且之前已经加入的用户也不需要更换私钥.由于本文采用了公钥扩展方案后统一使用新公钥加密的方式,在公钥扩展时有可能需要对 key block 进行修改.

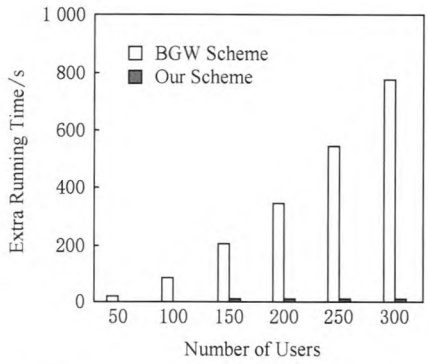

Fig. 4 Time cost vs the number of users between BGW and our scheme

图 4 系统增加用户时的时间开销

3.2 懒惰回收对密钥更新的优化

撤销权限的时间开销主要取决于对对应密钥进行广播加解密消耗的时间,在没有采用懒惰回收机制的方案中,用户撤销读权限需要下载文件重新加密,在采用了懒惰回收机制之后省去了这部分开销,撤销写权限不需要重加密,两者的开销是相同的.

图 5 表示基本方案和结合懒惰回收之后撤销读权限的开销,用户数为 1 000,授权用户数为 100.由于实验室测试环境处于同一局域网内,上传下载的速度可以达到 10 MBps 左右,但是在文件较大时,基本方案撤销读权限耗时仍较高.相比基本方案,采用懒惰回收之后的开销和文件大小没有关系,只有下载、修改和上传 key block 的开销,这部分时间开销在总用户数 1 000、授权用户数 100 时为 0.02 s,相比基本方案,时间开销降低很多,也节省了下载上传文件消耗的带宽.

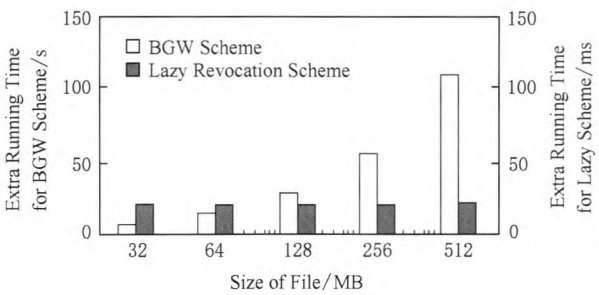

Fig. 5 Time cost when lazy revocation scheme is adopted

图 5 结合懒惰回收策略的时间开销

4 结束语

为了解决使用广播加密在云存储系统中重新分发密钥存在的性能开销大的问题,本文提出了一种对公钥进行扩展的方法,并且结合懒惰回收机制进一步优化了权限撤销时的性能.测试表明优化方法降低了基本方案在增加用户和更新密钥时的时间开销和带宽开销,可以更好地适应云存储系统中用户的动态变化.

参 考 文 献

[1] Liu Yahui, Zhang Tieying, Jin Xiaolong, et al. Personal privacy protection in the era of bid data [J]. Journal of Computer Research and Development, 2015, 52(1): 221-228 (in Chinese)
(刘雅辉,张铁赢,靳小龙,等.大数据时代的隐私保护[J].计算机研究与发展,2015,52(1):221-228)

[2] Kan Yang, Jia Xiaohua. Expressive, efficient, and revocable data access control for multi-authority cloud storage [J]. IEEE Trans on Parallel and Distributed Systems, 2014, 25(7): 1735-1744

[3] Adya A, Bolosky W J, Castro M, et al. Farsite: Federated, available, and reliable storage for an incompletely trusted environment [C] //Proc of the 5th Symp on OSDI. New York: ACM, 2002: 1-14

[4] Kallahalla M, Riedel E, Swaminathan R, et al. Plutus: Scalable secure file sharing on untrusted storage [C] //Proc of the 2nd USENIX Conf on File and Storage Technologies. Berkeley, CA: USENIX Association, 2003: 29-42

[5] Goh E, Shacham H, Modadugu M, et al. SiRiUS: Securing remote untrusted storage [C] //Proc of the Network and Distributed System Security Symp (NDSS 2003). Reston, VA: Internet Society, 2003: 131-145

[6] Popa R A, Lorch J, Molnar D, et al. Enabling security in cloud storage SLAs with CloudProof [C] //Proc of the 2011 USENIX Annual Technical Conf. Berkeley, CA: USENIX Association, 2011

[7] Cecile D, Pascal P, David P. Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys [C] //Proc of the 2007 Int Conf on Pairing-Based Cryptography. Berlin: Springer, 2007: 39-59

万方数据

[8] Cecile D. Identity-based broadcast encryption with constant size ciphertexts and private keys [C] //Proc of CRYPTO 2007. Berlin: Springer, 2007: 200-215

[9] Boneh D, Waters B, Zhandry M. Low overhead broadcast encryption from multilinear maps [C] //Proc of CRYPTO 2014. Berlin: Springer, 2014: 206-223

[10] Koyama K, Ohta K. Identity-based conference key distribution systems [C] //Proc of CRYPTO 1987. Berlin: Springer, 1987: 175-194

[11] Boneh D, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys [C] //Proc of CRYPTO 2005. Berlin: Springer, 2005: 258-275

Li Chunhua, born in 1971. PhD, associate professor. Her main research interests include storage security, privacy protection, and big data.

Wang Hua, born in 1975. PhD, associate professor. Her main research interests include cloud storage system, data backup and caching.

Zhang Yanzhe, born in 1991. Master. His main research interests include storage system and information security (465096070@qq.com).

Zhou Ke, born in 1974. Professor, PhD supervisor. Senior member of CCF. His main research interests include distributed system, cloud computing, storage security and big data (k.zhou@hust.edu.cn).

2018年《计算机研究与发展》专题(正刊)征文通知

——物联网安全研究进展

目前,随着物联网应用的广泛普及以及支撑技术的不断发展,其安全问题也愈发严重.物联网带来新的安全问题不仅会给广大用户和企业带来严重的损失,还会威胁国家安全与社会稳定.由于物联网设备的异构性,通信的复杂性等问题给广大科技工作者提出了大量的挑战性研究课题.现阶段物联网安全问题已经引起了学术界越来越多的重视,国内外相关学者开展了大量研究,也取得了许多不错的研究成果.

为了进一步推动我国物联网安全的科学研究和工程应用,及时报道物联网安全领域国内外科技工作者所取得的最新研究成果,同时展望物联网络空间安全的研究方向,《计算机研究与发展》将于2018年7月出版物联网安全专辑,欢迎相关领域的专家学者和科研人员踊跃投稿.现将专题论文征集的有关事项通知如下.

征文范围(但不限于)

1) **物联网网络安全问题**:物联网安全通信协议;物联网网络态势感知与网络威胁评估;物联网入侵检测与防御技术.

2) **物联网系统安全问题**:物联网操作系统安全;物联网恶意代码防御技术;物联网系统与固件安全更新技术;物联网设备漏洞挖掘技术.

3) **物联网应用与服务安全问题**:物联网应用隐私保护方案;物联网匿名与认证方案;物联网Web与云服务安全保护技术;物联网授权管理与访问控制技术.

4) **其他**:物联网设备信任问题;物联网设备测试框架;物联网设备物理安全;物联网设备软硬件攻击方法;适用于轻量级物联网设备的密码学(密钥协商、加解密、认证等)算法;跨层次的物联网安全问题;物联网在具体应用场景(智能家居、工业与公共基础设施、医疗健康等)中的安全问题.

征文要求

1) 论文应属于作者的科研成果,数据真实可靠,具有重要的学术价值与推广应用价值,未在国内外公开发行的刊物或会议上发表或宣读过,不存在一稿多投问题.作者在投稿时,需向编辑部提交签字版版权转让协议.

2) 论文一律用Word格式排版,论文格式体例参考近期出版的《计算机研究与发展》的要求(http://crad.ict.ac.cn/).论文需附通信作者的联系地址、电话或手机及E-mail地址.

3) 论文请通过期刊网站(http://crad.ict.ac.cn)进行投稿,作者留言中务必注明"物联网安全2018专题"(否则按自由来稿处理).

重要日期

征文截止日期:2018年1月31日　　录用通知日期:2018年3月31日

作者修改稿提交日期:2018年4月15日　　出版日期:2018年7月

特邀编委

张玉清　教　授　中国科学院大学、国家计算机网络入侵防范中心　zhangyq@ucas.ac.cn

Peng LIU　教　授　美国宾州州立大学　pliu@ist.psu.edu

李　晖　教　授　西安电子科技大学　lihui@mail.xidian.edu.cn

孙利民　研究员　中国科学院信息工程研究所　sunlimin@iie.ac.cn

联系方式

编　辑　部:crad@ict.ac.cn,010-62620696,010-62600350

通信地址:北京2704信箱《计算机研究与发展》编辑部　　邮政编码:100190

万方数据