



一种新的满足隐私性的云存储公共审计方案^{*}

王少辉^{1,2,3}, 陈丹伟^{1,2}, 王志伟^{1,2}, 常素琴^{1,2}

(1. 南京邮电大学计算机学院 南京 210003; 2. 江苏省无线传感网高技术研究重点实验室 南京 210003;
3. 网络与数据安全四川省重点实验室 成都 610054)

摘要

在云存储网络环境中,数据的安全性、完整性和隐私性是用户最关心的问题之一。云存储服务中,用户将存储的数据和认证标识信息存储在云服务器中。为了保证存储数据的完整性,云存储服务提供者需要向用户或第三方审计者证明其正确地持有用户存储的数据。公共审计是指由用户以外的第三方代替用户完成审计工作,这对于计算资源比较有限的用户尤其重要。目前多数云存储审计方案没有考虑隐私性问题。本文提出了一种新的可聚合基于签名的广播加密(ASBB)方案,并在此基础上设计了新的满足隐私性的云存储公共审计方案。新方案在随机预言模型下是可证安全的,并且在计算开销方面更具有优势。

关键词 云计算;云存储;公共审计;隐私性;完整性

1 引言

近年来,云计算越来越受到学术界和产业界的关注。云计算利用互联网平台为用户提供分布式、可靠、高可用、低成本按需付费、强大的计算能力以及无限存储、数据、信息、知识和协作的可能,使人类信息技术达到无时无处不在的可用性和服务能力。作为云计算重要应用业务之一的云存储是从云计算概念衍生和发展起来的一种数据外包存储服务技术,其依靠低成本、易于使用的接口和高可扩展性的商业优势得到了业内的广泛关注。

云存储具备物美价廉的优点,企业通过使用云存储可以降低存储数据的成本,用户不必考虑存储管理、数据备份、容灾的问题,只要在需要的时候访问云存储即可,省去了管理维护的工作量和成本。然而,云存储的安全性、可靠

性及服务水平等还存在众多问题亟待解决,所以在使用便利的同时,也引起了用户对安全性的担忧,目前仍未得到广泛认可与使用。数据存放在云存储中,用户最关心的问题之一是数据的完整性。存储服务商可以有效地对用户提供的数据完整性验证,并不断提高服务水平,云存储将获得广泛的应用。

用户在物理上已经不再拥有这些外包存储的数据,所以传统的用于数据完整性检测的密码学方法并不能很好地解决云存储中的数据完整性检测问题。数据完整性检测最直接简单的方法是利用散列函数。用户可以保存外包数据 F 的散列值 $Hash(F)$,当需要验证数据的完整性时,云存储服务提供者将完整的数据 F' 发送给用户,用户验证散列值 $Hash(F')$ 是否和保存的散列值 $Hash(F)$ 相等。这个方法由于昂贵的网络 I/O 和传输的费用代价,在实际中并不可行。

为了解决云存储中远程数据的完整性检测问题,依据不同的应用场景和应用需求,提出了众多的研究方案^[1-16]。目前的研究工作主要集中在可证明数据持有(provable

^{*} 国家自然科学基金资助项目(No.60903181),南京邮电大学基金资助项目(No.NY208072)



data possession, PDP) 方案和可恢复证明 (proofs of retrievability, PoR) 方案。PDP 和 PoR 方案的主要区别是: PDP 方案可检测存储数据是否完整, 但无法确保数据的可恢复性; PoR 方案可以保证存储数据的可恢复性。

Ateniese 等^[2,3]基于 RSA 算法的同态性提出了 PDP 方案, 以审计存储数据的完整性。但是该方案必须预先设定好审计的次数并且不支持公共审计。所谓公共审计是指允许除数据拥有者之外的第三方来验证远程存储数据的完整性。Juels 利用“哨兵”, 并使用纠错码编码这一工具提出了 PoR 方案^[4]。PoR 方案是典型的挑战—应答式协议, 可以使云存储服务提供者向用户证明一个文件是可恢复的, 不会有任意的数据丢失和破坏。Erway 等^[5]基于跳跃表 (skip list) 研究了在存储数据动态变化的情况下云存储安全审计的问题, 其运行效率还存在一定的争议。同时, Wang 等^[6]提出了公共检测的一个动态模型框架。

到目前为止, 多数的审计方案^[2-4,7]并没有考虑审计过程中用户数据的隐私性问题。通常在审计过程中, 云服务提供者会将用户数据直接发送给审计者, 从而将存储的数据内容泄密。从保护用户数据隐私性的角度来看, 这很大程度上影响了这些审计方案在云计算平台的安全性^[8]。Wang 等^[9]基于 Shacham 和 Waters 的方案^[10]提出了一个满足隐私性的云存储公共审计方案。为了提高方案的隐私安全需求, 参考文献[9]中方案的效率要明显低于参考文献[10]中的方案。

本文对保持隐私性的云存储公共审计方案进行了研究, 给出了一个密码学原语的新设计——可聚合基于签名的广播加密 (aggregatable signature-based broadcast, ASBB) 方案^[17]。利用 ASBB 方案的同聚合性质, 提出了一个高效的、满足隐私性要求的云存储公共审计方案。新方案采用挑战—应答的方式, 属于 PDP 方案, 其计算开销要优于参考文献[9]中的方案。

2 基础知识

本节给出本文所用的基础知识的相关概念, 主要包括双线性映射、计算困难性问题和 ASBB 方案。

2.1 双线性映射和计算困难性问题

设 G 和 G_T 分别是阶为大素数 p 的乘法循环群, g 是 G 群的生成元。假设离散对数问题在群 G 和 G_T 中都是难解的。

定义 1 如果满足下列 3 个条件, 则称映射 $e: G \times G \rightarrow G_T$

为一个双线性对映射。

- 双线性: 对于任意 $u, v \in G$ 和 $a, b \in Z_p^*$, 满足 $e(u^a, v^b) = e(u, v)^{ab}$ 。
- 非退化性: $e(g, g) \neq 1$ 。
- 可计算性: 对于任意 $u, v \in G$, 存在有效的算法计算 $e(u, v)$ 。

新方案用到的困难性问题假设主要包括计算 Diffie-Hellman (CDH) 假设、判断双线性 Diffie-Hellman (DBDH) 假设、双线性对假设和双线性 Diffie-Hellman 假设。

- 计算 Diffie-Hellman 假设: 给定三元组 (g, g^a, g^b) , 其中 $a, b \in Z_p^*$ 未知, g^{ab} 在计算上是困难的。
- 判断双线性 Diffie-Hellman 假设: 给定四元组 (g, g^a, g^b, g^c) 和任意 $Z \in G_T$, 其中 $a, b, c \in Z_p^*$ 未知, 区分 $T = e(g, g)^{abc}$ 和 Z 在计算上是困难的。
- 双线性对假设: 给定群 G 和生成元 g , 由 $T = e(X, g) \in G_T$ 计算 $X \in G$ 是困难的。
- 双线性 Diffie-Hellman 假设: 给定三元组 (g, g^a, g^b) , 其中 $a, b \in Z_p^*$ 未知, 对于任意的 $h \neq g \in G$, $e(h, g^{ab})$ 在计算上困难的。

2.2 可聚合基于签名的广播加密方案

在 ASBB 方案^[17]中, 用户的公钥可同时用来验证签名的合法性和加密消息, 并且任意合法的签名可以用来解密该公钥加密的密文。一个 ASBB 方案通常包含如下 6 个多项式时间算法。

- ParaGen 算法(1^λ): 输入安全参数 1^λ , 输出系统的公共参数 π 。
- KeyGen 算法(π): 输入参数 π , 输出用户的公钥/私钥对 (pk, sk) 。
- Sign 算法(pk, sk, s): 对于消息 s , 利用公钥/私钥对 (pk, sk) , Sign 算法输出签名 σ 。
- Verify 算法(pk, s, σ): 对于公钥 pk 和消息 s 以及对应的签名 σ , Verify 算法输出 1 (如果 σ 是消息 s 的合法签名); 否则算法输出 0。
- Encrypt 算法(pk, m): 输入公钥 pk 和明文 m , Encrypt 算法输出相应的密文 c 。
- Decrypt 算法(pk, s, σ, c): 利用公钥 pk 和任意合法的签名对 (s, σ) , 对密文 c 解密得到相应的明文 m 。

参考文献[17]提出的 ASBB 方案的重要之处在于, 它具有密钥同态性, 这意味着给定同一消息在两个不同私钥下的签名, 可以有效地生成该消息在新的私钥下的签名,

而新的私钥由最初的两个私钥生成。在参考文献[17]中, Wu 等提出了一个高效的基于双线性映射的 ASBB 方案, 该方案简介如下。

- ParaGen 算法(1^A): 输入安全参数 1^A , G 和 G_T 是阶为大素数 p 的乘法循环群, g 是群 G 的生成元, $H: \{0,1\}^* \rightarrow G$ 是安全散列函数, $e: G \times G \rightarrow G_T$ 是双线性映射, 方案的公共参数为 (g, H, p, G, G_T, e) 。
- KeyGen 算法: 随机选择 $r \in Z_p^*$, $X \in G \setminus \{1\}$, 计算 $R = g^r$, $A = e(X, g)$ 。方案的公钥和私钥分别为 $pk = (R, A)$, $sk = (r, X)$ 。
- Sign 算法: 对于任意消息 $s \in \{0,1\}^*$, 其相应的签名为 $\sigma = XH(s)^r$ 。
- Verify 算法: 给定消息签名对 (s, σ) , 验证者验证方程 $e(\sigma, g)e(H(s), R) = A$ 是否成立。如果方程成立, 则输出 1, 说明 σ 是消息的合法签名; 否则输出 0 并拒绝签名。
- Encrypt 算法: 对于明文 $m \in G_T$, 随机选择 $t \in Z_p^*$, 并计算 $c_1 = g^t$, $c_2 = R^t$, $c_3 = mA^t$ 。密文为 (c_1, c_2, c_3) 。
- Decrypt 算法: 给定密文 (c_1, c_2, c_3) , 任何拥有合法消息/签名对的人都可利用 $m = c_3 / (e(\sigma, c_1)e(H(s), c_2))$ 解密得到明文。

ASBB 方案的安全性包括对 Sign 算法的选择、消息攻击下的不可伪造性和针对 Encrypt 算法的抗适应性选择密文攻击。

3 保持隐私性的云存储公共审计方案

本节给出了云存储公共审计方案和方案所要满足的安全需求(包括完备性、健壮性和隐私性)的定义。

本文采用与参考文献[9]一样的云存储系统架构, 如图1所示。云存储服务涉及3个不同的实体: 云用户将自身的数据文件远程存储在提供存储服务的云平台上; 云服务器 (cloud server, CS) 提供云存储服务, 并由云服务供应商进

行管理和维护; 第三方审计者 (third party auditor, TPA) 代表用户对云服务器存储服务的可靠性进行评估, 即检测用户存储的数据文件是否丢失或被破坏。

定义 2 (云存储公共审计方案) 保持隐私性的云存储公共审计方案通常由 Keygen、Gentag 和 Audit 3 个多项式时间算法构成。

- Keygen 算法: 输入安全参数 λ , 该算法生成方案的公共参数和云用户的公钥/私钥对 (pk, sk) 。
- Gentag 算法: 以用户私钥 sk 和数据文件 $F \in \{0,1\}^*$ 作为输入, 该算法生成文件的认证标识 t , 文件和认证标识将同时保存在 CS 中。标识中通常会包含存储数据的相关信息和利用私钥 sk 生成的额外的私有验证信息。
- Audit 算法: 公共审计算法通过 TPA 和 CS 之间的交互协议 ($TPA(pk) \leftrightarrow CS(pk, F, t)$) 来完成。协议执行时, TPA 作为验证方, 首先以公钥 pk 和 Gentag 算法输出的文件描述信息 t 作为输入, 生成审计挑战信息发送给 CS; 而 CS 作为证明方, 将存储的数据信息和保存的认证标识作为输入生成并回送 TPA 应答消息; 协议的最终, 如果 TPA 验证 CS 存储的文件保存完好没有变更, 则 TPA 输出 1, 否则将输出 0。

通常, 假设 TPA 被用户所信任, 其公共审计业务是可靠的, 而存储数据的完整性威胁主要来源于 CS 和恶意的外部敌手。CS 可能会由于自身或者外在的原因造成存储数据的破坏或丢失, 而其又会在审计中欺骗 TPA 存储数据保持完整。保持隐私性云存储公共审计方案应满足完备性、健壮性和隐私性等安全需求。简单地说, 完备性是指对于合法的 CS 和 TPA, 其审计结果应总是 1; 而健壮性指对于拥有更改数据的 CS, 其不可能通过 Audit 算法的交互获得 TPA 的验证确认; 而隐私性指攻击者不能采用被动或者主动的攻击方式从审计方案中获知用户存储的数据内容。

定义 3 (完备性) 云存储公共审计方案的完备性要求对任意由 Keygen 算法输出的公钥/私钥对 (pk, sk) 、任意数据文件 $F \in \{0,1\}^*$ 和由 Gentag 算法生成的认证标识 t , TPA 和 CS 通过审计算法交互后的输出总是 1, 即 $pr(Audit(TPA(pk) \leftrightarrow CS(pk, F, t)) = 1) = 1$ 。

定义 4 (健壮性) 下面利用参考文献[10]的方法给出健壮性定义, 该定义通过攻击者 A 与挑战者 B 所参与的如下 Game 定义。

挑战者 B 运行 Keygen(1^A) 算法生成公钥/私钥对 (pk, sk) ,

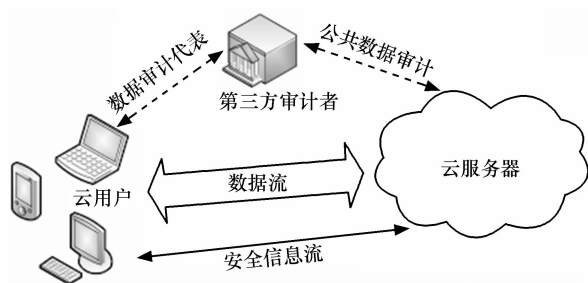


图1 云数据存储服务的架构



将公钥 pk 发送给敌手 A ; 敌手 A 可以与挑战者 B 进行交互,访问如下预言机: A 可以访问 G_{entag} 预言机,对于每一次访问,挑战者 B 选择数据信息 M ,并计算 $t \leftarrow G_{\text{entag}}(sk, M)$ 生成相应的认证标识,文件 M 和相应的标识 t 都将发送给敌手 A 。同时, A 也可以访问 A_{udit} 预言机与 B 进行交互,在交互过程中,敌手 A 扮演证明者 CS 的角色,而挑战者 B 扮演验证者 TPA 的角色。最终,敌手 A 输出消息 M_1 发送给挑战者,由挑战者生成认证标识 t ;然后敌手 A 将消息修改为 $M^* \neq M_1$,并与挑战者 B 进行 A_{udit} 算法的交互 $B(pk, sk) \leftrightarrow A(pk, M^*, t)$ 。

如果如下概率是可以忽略的,则称云存储公共审计方案是健壮的:

$$pr(A_{\text{udit}}(B(pk, sk) \leftrightarrow A(pk, M^*, t))=1) \quad (1)$$

定义 5 (隐私性)通过攻击者 A 和挑战者 B 参与的如下 Game 定义隐私性。

挑战者 B 运行 $Keygen(1^\lambda)$ 算法生成公钥/私钥对 (pk, sk) ,并将 pk 发送给敌手 A ; 敌手 A 可以向挑战者 B 询问 G_{entag} 预言机,对于每一次访问,挑战者 B 选择数据信息 M ,并计算 $t \leftarrow G_{\text{entag}}(sk, M)$ 生成相应的认证标识,文件 M 和相应的标识 t 都将发送给敌手 A 。最终,挑战者 B 选择数据 M_1 ,并计算相应的认证标识 $t \leftarrow G_{\text{entag}}(sk, M_1)$,攻击者 A 和挑战者 B 进行 A_{udit} 交互,在此交互中,敌手 A 扮演 TPA 的角色,而挑战者 B 则扮演 CS 的角色;最后敌手 A 输出数据文件 M^* 。

假设消息 M_1 具有大的信息熵,则称云存储公共审计方案满足隐私性,如果通过上述的 Game, 概率 $pr(M^* \leftarrow A(pk); M_1 = M^*)$ 是可以忽略的。

4 本文提出的方案

本节设计了一个新的高效 ASBB 方案,并基于该方案设计了满足隐私性的云存储公共审计方案。

4.1 新的 ASBB 方案设计

新提出的 ASBB 方案的效率和参考文献[17]中方案的效率相当,具体方案描述如下。

- **ParaGen 算法**(1^λ):输入安全参数 1^λ , G 和 G_T 是阶为大素数 p 的乘法循环群, g 是群 G 的生成元, $H: \{0,1\}^* \rightarrow G$ 是安全散列函数, $e: G \times G \rightarrow G_T$ 是双线性映射,方案的公共参数为 (g, H, p, G, G_T, e) 。
- **KeyGen 算法**:随机选择 $r \in Z_p^*$, $X \in G \setminus \{1\}$, 计算 $R = g^r$, $A = e(X, g)$ 。方案的公钥和私钥分别为 $pk = (R, A)$, $sk =$

(r, X) 。

- **Sign 算法**:对于任意消息 $m \in Z_p^*$, 首先随机选择 $s \in \{0,1\}^*$, 计算 $\sigma = X^m H(s)^r$, 消息 m 对应的签名为 (s, σ) 。
- **Verify 算法**:给定消息签名对 (m, s, σ) , 验证者验证方程 $e(\sigma, g) e(H(s), R) = A^m$ 是否成立。如果方程成立,则输出 1, 说明 (s, σ) 是消息的合法签名; 否则输出 0 并拒绝签名。
- **Encrypt 算法**:对于明文 $m \in G_T$, 随机选择 $t \in Z_p^*$, 并计算 $c_1 = g^t$, $c_2 = R^t$, $c_3 = mA^t$ 。密文为 (c_1, c_2, c_3) 。
- **Decrypt 算法**:给定密文 (c_1, c_2, c_3) , 任何拥有合法消息签名对 (m, s, σ) 的人都可使用式(2)解密得到明文:

$$M = c_3 / e(\sigma, c_1) e(H(s), c_2)^{m^{-1}} \quad (2)$$

方案的正确性显然成立,并且容易看出新的 ASBB 方案的安全性可以规约到参考文献[17]中方案的安全性上。以 Sign 算法为例,如果攻击者能够伪造公钥为 (R, A) 的合法签名 (m, s, σ) ,则在参考文献[17]的方案中,可以伪造公钥信息为 $(R^{m^{-1}}, A)$ 的合法签名 $(s, \sigma^{m^{-1}})$ 。

定理 1 新提出的 ASBB 方案满足如下两个条件:

- 假设 CDH 假设和 DBDH 假设成立, 新的 ASBB 方案的签名方案在随机预言模型下满足选择消息的不可伪造性,而加密方案满足选择明文攻击的不可区分性;
- 假设 BDHE 假设成立,新的 ASBB 方案在随机预言模型下满足非适应选择消息的可聚合性。

4.2 满足隐私性的云存储公共审计方案

下面利用 ASBB 方案的可聚合性,给出满足隐私性的云存储公共审计方案,具体描述如下。

(1) $Keygen(1^\lambda)$ 算法

令 G 和 G_T 是具有阶为大素数 p 的乘法循环群,而 $e: G \times G \rightarrow G_T$ 是双线性映射, g 是群 G 的生成元。 $H: \{0,1\}^* \rightarrow G$ 是安全的散列函数,将任意输入映射到群 G 上。系统的公共参数为 (g, H, p, G, G_T, e) 。随机选择 $r \in Z_p^*$, $X \in G \setminus \{1\}$, 计算 $R = g^r$, $A = e(X, g)$ 。则用户的公钥和私钥对分别为 $pk = (R, A)$, $sk = (r, X)$ 。

(2) $G_{\text{entag}}(sk, F)$

给定数据文件 $F = \{m_i\}_{i=1,2,\dots,n}$, 对于每一个消息块 $m_i \in Z_p^*$, 用户计算其认证标识为 $\sigma_i = X^{m_i} H(id \| i) \in G$, 其中 id 由用户在 Z_p^* 随机选择作为文件 F 的标识。用户将数据文件 F 和标识远程存储在 CS 中。

(3) A_{udit} 算法

该算法通过 TPA 和 CS 如下的交互过程完成。

步骤 1: 为了生成审计的挑战消息, TPA 首先随机选择 $t \in Z_p^*$, c 个取值于 $[1:n]$ 的随机数 $I=\{s_1, s_2, \dots, s_c\} \in [1:n]$ 。对每一个 $i \in I$, TPA 随机选择整数值 v_i (该值不需要太大), 计算 $c_1=g^t$ 、 $c_2=R^t$ 和 $c_3=A^t$ 。最终的挑战消息为 $(\{i, v_i\}_{i \in I})$ (c_1 和 c_2 作为秘密不发送给 CS)。

步骤 2: 接收到挑战信息后, CS 首先查找相应数据信息和认证标识 $\sigma_i, i \in I$, 并计算 $\sigma = \prod_{i \in I} \sigma_i^{v_i}$, 然后计算:

$$B = (c_3)^\mu = (A^t)^\mu = e(X, g^t)^{\sum_{i \in I} v_i m_i} \quad (3)$$

其中, $\mu = \prod_{i \in I} v_i m_i$, 则 CS 将 (σ, B) 发送给 TPA 作为应答消息。

步骤 3: 接收到应答消息 (σ, B) 后, TPA 利用 c_1 和 c_2 验证式(4)是否成立。如果成立, 则 TPA 判定 CS 通过了审计验证; 否则审计不成功, 存储的数据存在破坏:

$$B = e(\sigma, c_1) \cdot e(\prod_{i \in I} H(id \| i)^{v_i}, c_2) \quad (4)$$

下面说明验证方程的正确性, 简单起见, 用 H_i 代替 $H(id \| i)$:

$$\begin{aligned} & e(\sigma, c_1) \cdot e(\prod_{i \in I} H_i^{v_i}, c_2) \\ &= e(\prod_{i \in I} \sigma_i^{v_i}, g^t) \cdot e(\prod_{i \in I} H_i^{v_i}, g^{-rt}) \\ &= e(\prod_{i \in I} (X^{m_i} (H_i)^r)^{v_i}, g^t) \cdot e(\prod_{i \in I} H_i^{v_i}, g^{-rt}) \\ &= e(\prod_{i \in I} X^{m_i v_i}, g^t) = (e(X, g^t))^{\sum_{i \in I} m_i v_i} = B \end{aligned} \quad (5)$$

5 效率和安全性分析

首先与参考文献[9]中的方案在效率方面进行了比较, 然后证明新提出的公共审计方案满足健壮性和隐私性。

5.1 性能分析

分别从存储开销、通信开销和计算开销 3 个方面将新提出的方案与参考文献[9]中的方案进行了比较。假设在两个方案中, 存储的数据文件 F 是一样的, 而 TPA 提出的挑战信息 $I=\{s_1, s_2, \dots, s_c\} \in [1:n]$ 和 $\{v_i\}_{i \in I}$ 也是一样的。

(1) 存储开销

就系统参数而言, 参考文献[9]的公钥需要 3 个群元素, 而私钥需要 1 个取值为 Z_p 的整数; 而新方案的公钥需要 3 个群元素, 私钥包括 1 个整数和 1 个群元素。在两个方案中, 作为数据文件存储时产生的额外开销, 也就是生成的认证标识的数目是一样的。

(2) 通信开销

两个方案的审计交互中, 除了相同的挑战信息 $\{(i, v_i)\}_{i \in I}$ 外, 参考文献[9]中 CS 发送的应答消息包括 2 个群元素和

1 个整数; 而新方案中, TPA 需要额外多发送 1 个群元素, 而 CS 的应答消息包含 2 个群元素。

(3) 计算开销

在挑战生成阶段, 新方案中的 TPA 比参考文献[9]额外需要 3 个群模幂运算, 即 $(c_1=g^t, c_2=R^t, c_3=A^t)$, 但是由于这 3 个参数和应答无关, 所以可以在空闲的时间进行预计算完成, 并不多占用审计时的计算时间开销。而在验证阶段, 参考文献[9]比新方案多 3 个模幂运算、1 个群模乘运算和 1 个散列运算。就 CS 而言, 参考文献[9]比新方案额外多了 1 个双线性对运算、1 个散列运算和 1 个整数模乘运算。

从上面的比较可以看出, 因为私钥是不需要存储的, 所以两个方案的存储开销相当; 通信开销整体而言两个方案也是相当的。因为双线性对的运算效率明显低于模幂运算, 并且新方案的 3 个模幂运算可以预计算并不占用审计时间, 所以就计算开销而言, 新方案要明显优于参考文献[9]。

5.2 安全性分析

简要说明新方案满足健壮性和隐私性。通过定理 2 证明 CS 在数据被更改的情况下, 不可能产生合法的应答消息通过 TPA 的审计。而定理 3 说明方案满足隐私性, 新的方案并没有将数据泄露。

定理 2 如果计算 Diffie-Hellman 和 Bilinear Pairing 的假设成立, 则在新方案中 CS 在不具有完好无损的数据信息的情况下, 能生成合法应答通过审计过程的概率是可忽略的。

证明 如果 CS 能够用修改过后的数据产生合法的应答消息, 则其可以解决计算 Diffie-Hellman 和 Bilinear Pairing 的问题。

当接收到 TPA 的挑战消息 $\{(i, v_i)\}_{i \in I}, c_3$ 之后, 由离散对数问题和计算 Diffie-Hellman 的困难性, CS 不可能由 c_3 计算得到 c_2 和 c_1 。

为了能够通过审计的验证方程, CS 生成的合法应答消息 (σ, B) 一定满足:

$$B = e(X, g^t)^\mu = e(\sigma, c_1) \cdot e(\prod_{i \in I} H(id \| i)^{v_i}, c_2) \quad (6)$$

假设 CS 在存储的数据信息产生了错误破坏的情况下能够通过审计验证, 此时必定存在应答消息 $(\sigma^* \neq \sigma, B^*)$ 可以满足审计过程的验证方程:

$$B^* = e(X, g^t)^{\mu'} = e(\sigma^*, c_1) \cdot e(\prod_{i \in I} H(id \| i)^{v_i}, c_2) \quad (7)$$

在这里, 验证方程中 $\mu \neq \mu'$, 否则将与假设不相符。由方程(6)和(7)可以得到:



$$B/B^* = e(X, g')^{\mu-\mu'} = e(\sigma/\sigma^*, c_1) = e(\sigma/\sigma^*, g')(8)$$

这也就意味着, $X^{\mu-\mu'} = \sigma/\sigma^*$, i.e. $X = (\sigma/\sigma^*)^{(\mu-\mu')^{-1}}$, 从而CS可以解决双线性对的假设问题, 这与双线性对问题的困难性假设相违背。

定理 3 假设离散对数问题是困难的, 则攻击者从审计方案中提取出存储数据的概率是可忽略的。

证明 首先对于值 μ 和数据 $F = \{m_i\}_{i=1,2,\dots,n}$ 的获知是等价的。如果攻击者能够得到值 μ , 则通过求解方程组, 就可以获得存储的数据信息。直观上看, 因为涉及的数据消息 $F = \{m_i\}_{i=1,2,\dots,n}$ 的操作都在指数上。如果 TPA 或者攻击者能够通过新的审计方案获得存储的数据 $F = \{m_i\}_{i=1,2,\dots,n}$, 则相当于攻击者可以获得值 $\mu = \prod_{i \in I} m_i$, 从而推导出消息 B 关于 A 的离散对数为 μ , 这与离散对数问题的困难性假设相矛盾。

如果存在攻击者 Adv_1 能够破坏新方案的隐私性, 则假设攻击者 Adv_2 需要计算 $h = g^\alpha$ 的离散对数 α , 此时 Adv_2 随机选择 $\beta \in Z_p^*, r \in Z_p^*$, 并计算 $R = g^r, A = e(X^\beta, g)$ 。则公钥信息 $pk = (R, A)$ 交给攻击者 Adv_1 。对于给定的数据 $F = \{m_i\}_{i=1,2,\dots,n}$, 消息块 m_i 的认证标识 $\sigma^i = h^{\beta m_i} H(id||i)^r = (g\beta)^{\alpha m_i} H(id||i)^r$ 。从定理2的证明可以看出, 挑战信息包含 c_1 并不影响方案的健壮性, 从而对于攻击者 Adv_1 的挑战信息 $(\{i, v\}_{i \in I}, c_1, c_3)$, Adv_2 可以计算应答信息 $\sigma = \prod_{i \in I} \sigma_i^{v_i}, B = e(h^\beta, g)^{\sum_{i \in I} v_i m_i} = e(g^\beta, g)^{\alpha \sum_{i \in I} v_i m_i}$ 。从而对于攻击者 Adv_1 而言, 用户选择的数据信息为 $\alpha \cdot m_i$ 。如果 Adv_1 能够将消息恢复出来, 则 Adv_1 能计算得到 $h = g^\alpha$ 的离散对数 α 。

6 结束语

目前, 因为安全性、可靠性、隐私性等问题, 云存储服务还不为用户广泛接纳与采用。而一旦云存储的安全性、可靠性、隐私性得到保障, 它将具有广泛而巨大的应用前景。本文首先提出了一个新的可聚合基于签名的广播加密方案, 并在此基础上给出了一个新的保持隐私性的云存储公共审计方案。攻击者或者 TPA 无法从新审计方案中获知存储的数据内容。新方案与参考文献[9]中的方案具有相同的存储开销和传输开销, 而在计算开销上有明显的优势。

通常用户需要外包存储的数据并不是静态不变的, 用户会对数据进行诸如修改、插入、添加、删除等操作, 参考文献[9]对数据动态变化情况下的公共审计方案进行了初步研究, 但是方案并不能很好地支持插入和删除操作。如何设计高效的、满足隐私性并支持动态变化的审计方案是下一步要考虑的工作。

参考文献

- 1 Einar M, Maithili N, Gene T. Authentication and integrity in outsourced databases. *ACM Transactions on Storage*, 2006, 2(2): 107~138
- 2 Ateniese G, Burns R, Curtmola R, *et al.* Provable Data Possession at Untrusted Stores. *Cryptology ePrint Archive*, Report 2007/202, 2007
- 3 Ateniese G, Pietro R D, Mancini L V, *et al.* Scalable and efficient provable data possession. *Proceedings of the 4th International Conference on Security and Privacy in Communication Networks*, Istanbul, Turkey, ACM, 2008
- 4 Juels A, Kaliski B. Pors: proofs of retrievability for large files. *Proceedings of CCS 2007*, Alexandria, VA, USA, 2007: 584~597
- 5 Erway C, Kupcu A, Papamanthou C, *et al.* Dynamic Provable Data Possession. *Cryptology ePrint Archive*, Report 2008/432, 2008
- 6 Wang Q, Wang C, Li J, *et al.* Enabling public verifiability and data dynamics for storage security in cloud computing. *Lecture Notes in Computer Science*, 2009(5789): 355~370
- 7 Wang Q, Wang C, Ren K, *et al.* Enabling public auditability and data dynamics for storage security in cloud computing. *IEEE Transactions on Parallel and Distributed Systems*, 2011, 22(5): 847~859
- 8 Shah M A, Baker M, Mogul J C, *et al.* Auditing to keep online storage services honest. *Proceedings of HotOS'07*, Berkeley, CA, USENIX, 2007: 1~6
- 9 Cao N, Yang Z Y, Wang C, *et al.* Privacy-preserving public auditing for data storage security in cloud computing. *Proceedings of IEEE INFOCOM 2010*, San Diego, CA, 2010: 525~533
- 10 Shacham H, Waters B. Compact proofs of retrievability. *Proceedings of ASIACRYPT 2008*, Melbourne, Australia, 2008: 90~107
- 11 Sebe F, Domingo-Ferrer J, Balleste A M, *et al.* Efficient remote data possession checking in critical information infrastructures. *IEEE Transactions on Knowledge and Data Engineering*, 2008: 1034~1038
- 12 Wang C, Wang Q, Ren K, *et al.* Ensuring data storage security in cloud computing. *Proceedings of IW QoS 2009*, Charleston, South Carolina, USA, 2009
- 13 Bowers K D, Juels A, Oprea A. Proofs of retrievability: theory and implementation. *Proceedings of the 2009 ACM Workshop on Cloud Computing Security*, CCSW 2009, Co-located with the 16th ACM Computer and Communications Security Conference, New York, 2009: 43~54
- 14 Kamara S, Lauter K. Cryptographic cloud storage. *Lecture Notes in Computer Science, Financial Cryptography and Data Security*, Berlin, Springer, 2010: 136~149

- 15 Hao Z, Yu N. A multiple-replica remote data possession checking protocol with public verifiability. Proceedings of Second Int'l Data, Privacy and E-Commerce Symposium (ISDPE '10), New York, USA, 2010
- 16 Zheng Q, Xu S. Fair and dynamic proofs of retrievability. Proceedings of 1st ACMM Conference on Data and Application Security and Privacy (CODASPY), San Antonio, TX, USA, 2011
- 17 Wu Q, Mu Y, Susilo W, *et al.* Joux A (ed). Asymmetric group key agreement. EUROCRYPT 2009, Springer, Heidelberg, 2009: 153~170
- 18 Goldwasser S, Micali S, Rivest R. A digital signature scheme secure against adaptive chosen-message attacks. SIAM J Computing, 1988,17(2): 281~308
- 19 Chaum D, Pederson P T. E F Brichell (ed). Wallet databases with observers. Advances in Cryptology-CRYPTO'92, LNCS 740, 1993:89~105

A New Solution of Privacy-Preserving Public Auditing Scheme for Cloud Storage Security

Wang Shaohui^{1,2,3}, Chen Danwei^{1,2}, Wang Zhiwei^{1,2}, Chang Suqin^{1,2}

(1.College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;

2. Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China;

3. Network and Data Security Key Laboratory of Sichuan Province, Chengdu 610054, China)

Abstract When user stores their data in the cloud storage, they most concern about whether the data is complete, privacy and unchanged. To ensure the availability and integrity of users' stored data, cloud server must prove a verifier that it is actually storing all of a client's data unchanged. And, enabling public auditability for cloud storage is of critical importance to users with constrained computing resources, who can resort to a third party auditor to check the integrity of outsourced data. However, most of the existing auditing schemes do not consider data privacy problem. In this paper, after giving a new construction of a recently proposed primitive named aggregatable signature based broadcast encryption scheme, we present an efficient public auditing scheme with privacy property. The new scheme is secure in the random oracle model and has less computation cost than existing auditing scheme with privacy property.

Key words cloud computing, cloud storage, public auditing, privacy, integrity

(收稿日期:2012-07-28)

• 简讯 •

亿阳安全管理平台再添新份额

2012年7月,亿阳安全在安全管理平台解决方案方面再接再厉,成功中标“四川移动业务支撑系统安全管理平台”项目、“江苏移动业务支撑系统安全管理平台”项目。

亿阳信通安全管理平台是基于安全策略实现安全管理工作的常态化运行的技术支撑平台,重点实现集中化的安全策略管理、安全资产配置管理、安全风险管理和安全运维作业管理和安全法规符合性管理,以提升全网安全防护能力。

亿阳安全凭借专业的安全技术、丰富的安全运营经验和安全咨询服务能力,为中国移动用户量身打造了安全管理平

台解决方案。亿阳网警安全管理平台为安全管理的智能化分析、可管理、可控制、可运维和可测量提供综合的技术支撑手段,确保安全策略、过程、技术和机制在整个组织的信息基础设施的所有层面都能得以实施。同时,亿阳安全咨询和运营服务团队能为安全管理平台的成功落地、调整和优化提供持续动力,确保安全管理平台效用得到最大化的发挥。

亿阳安全管理平台的市场份额不断提升,不仅是产品解决方案领先的体现,更是用户对亿阳安全技术实力、产品、服务品质的进一步肯定。亿阳安全将始终坚持以用户需求为导向,专注于前沿领域的研究和创新,为用户提供具有国际竞争力的先进产品与服务。