一个改进型云存储共享方案

伍 琦 万常选 李国林
(江西财经大学信息管理学院 南昌 330032)

摘 要 云存储安全一直是云安全研究的重点。Zhao等提出了一种云存储可信共享(TSCS)方案,但分析发现,该方案不能抵抗恶意CSP攻击。根据云存储安全需求,构建了云存储可信共享模型。随后,依据云存储可信共享模型构造了一个云存储可信共享方案。分析表明,新方案减弱了对随机数的依赖,不仅具有Zhao等的TSCS方案的安全性能,还能抵御服务器端的恶意篡改。新TSCS方案具有一定的应用前景。

关键词 云安全,云存储安全,可信共享
中图法分类号 TP309 **文献标识码** A

Improved Data Sharing Scheme over Cloud Storage

WU Qi WAN Chang-xuan LI Guo-lin
(School of Information Technology, Jiangxi University of Finance and Economics, Nanchang 330032, China)

Abstract Cloud storage security has always been emphasis in cloud security. Zhao et al. proposed a TSCS(Trusted Sharing over Cloud Storage) scheme, which is incapable of withstanding malicious CSP attacks, according to our analysis. This paper constructed the model of TSCS in terms of its requirements for security. Afterwards, a new TSCS scheme was proposed based on it. Analysis shows the new one relies less on random numbers, and not only retains the security properties of Zhao et al.'s scheme, but also resists tampering of the server, and could be put into application.

Keywords Cloud security, Cloud storage security, Trusted sharing

基于分布式计算、并行计算、网格计算、效用计算等概念,工业界推出了云计算。云计算将网上大量存储资源和计算资源整合起来,按需提供给用户。它将业务逻辑与计算资源分离,让用户从繁复的计算资源配置、维护和管理中解脱出来,使用户能专注于业务逻辑。目前Amazon、Google、Yahoo、Dell、Microsoft等企业[1]均在积极进行云计算的研发,学术界的研究成果也不断涌现[2-4]。

云计算在带来巨大市场前景的同时,也存在巨大的风险。Gartner公司[5]指出,安全问题是云计算发展的重大障碍。目前,云安全研究主要集中在计算安全和存储安全这两个方向。以下简单介绍云存储安全研究现状。

1 云存储安全概述

Ateniese等[6]提出PDP(Provable Data Possession,可证数据拥有)模型,并基于RSA和KEA1设计了两个方案,即S-PDP(Secure-PDP)和E-PDP(Efficient-PDP)。Ateniese等[7]随后基于对称密码学,提出了一个支持动态操作的新方案。C. Wang等[8]提出了一个方案,实现了数据错误定位。Juels等[9]提出POR(Proofs of Retrievability,可检索性证明)模型,其使用"哨兵"(sentinel)和纠错码来保证数据的可检索性。Q. Wang等[10]基于双线性映射和Merkle散列树,提出了一个新方案,首次同时支持公开验证和动态操作。C. Wang等[11]基于双线性映射,提出了一个方案,实现了公开批量审核,并且其计算和通信开销较小。Erway等[12]扩展了PDP模型,提出了支持可证更新的DPDP模型。Zhang等[13]基于RSA假设提出了一个方案,并讨论了其安全性。Hao等[14]基于双线性映射提出了一个支持公开验证的多备份数据审核方案。Wei等[15]基于双线性映射和Merkle散列树提出了一个同时实现存储安全和计算安全的方案。

以往方案中,绝大多数在云服务器端存储的是明文,即未考虑对云服务器端数据的被动攻击。在2010年云计算IEEE会议上,Zhao等[16]基于ECDLP(Elliptic Curve Discrete Logarithm Problem,椭圆曲线离散对数问题)提出了一个数据存储可信共享访问方案。该方案能强制执行数据拥有者的访问控制策略,阻止云服务器的未授权访问和制造非法授权来访问数据。该方案虽然考虑了服务器端的窃听,但过度依赖随机数,并忽略了服务器端的主动攻击:服务器可任意篡改数据,而不被数据拥有者和共享请求方发现。

为解决文献[16]中的问题,重新定义云存储可信共享的模型,并基于DLP(Discrete Logarithm Problem,离散对数问题)提出了一个改进方案。分析表明,该方案能检测出服务器端的恶意篡改,具有一定的实用价值。

2 预备知识

下面介绍本文用到的3个密码学假设,其详细定义见文

到稿日期:2011-09-19 返修日期:2011-11-02 本文受国家自然科学基金(10961013)和江西省教育厅科学技术研究项目(GJJ11730)资助。
伍 琦(1984—),男,博士生,主要研究方向为信息安全,E-mail:wuqiocjzd@126.com;万常选(1962—),男,博士,教授,博士生导师,CCF高级会员,主要研究方向为数据库;李国林(1985—),女,硕士生,主要研究方向为数据库。

献[17]。

定义 1(离散对数假设,DLP) 给定大质数 q 及 Z_q^* 中生成元 g,对任何概率多项式时间图灵机 T,对任意小正数 ε,有 $\Pr[T(g^x)=x]-\frac{1}{|q-1|}<\varepsilon$(离散对数问题在多项式时间内不可解)。

定义 2(计算性 DH 难假设,CDH,Computational Diffie-Hellman) 给定大质数 q 及 Z_q^* 中生成元 g,对任何概率多项式时间图灵机 T,对任意小正数 ε,有 $\Pr[T(g^a,g^b)=g^{ab}]-\frac{1}{|q-1|}<\varepsilon$(CDH 问题在多项式时间内不可解)。

定义 3(椭圆曲线离散对数假设,ECDLP) 给定一椭圆曲线及其加法群生成元 G,对任何概率多项式时间图灵机 T,椭圆曲线离散对数问题在多项式时间内不可解,即对任意小正数 ε,有 $\Pr[T(xG)=x]-\frac{1}{ord(G)}<\varepsilon$。

3 云存储可信共享

云计算旨在让用户从繁琐的存储资源和计算资源管理中解脱出来,尽可能让服务器端承担尽量多的计算机功能,以实现真正的"瘦客户机"模式。其中,云存储是重点,也是基础。服务器端数据的存储是云计算输入的必要条件,也是云计算输出的必备保障。

共享是通信协议中常要求实现的功能之一。虽然数据存储在云服务器端,但数据拥有权仍属于用户。用户可授权任何其他用户来访问自己的数据,同时不让服务器取得任何与数据有关的信息。

以下给出云存储可信共享模型的定义及其安全性质。

3.1 云存储可信共享 TSCS(Trusted Sharing over Cloud Storage)模型定义

该模型包含 3 个实体:数据拥有者 Alice、共享请求方 Bob、云存储提供商 CSP(Cloud Storage Provider)。

该模型包含 7 个算法:

(1)密钥生成算法

$\text{Setup}(1^k)\rightarrow(F,(sk_A,pk_A),(sk_B,pk_B),(sk_C,pk_C))$:KG(Key Generator,密钥发生器)由输入安全参数 k,生成有限域 F(以下算法均在 F 中操作)。KG 再分别为 Alice、Bob 和 CSP 生成公私密钥对 (sk_A,pk_A),(sk_B,pk_B),(sk_C,pk_C)。

(2)数据加密算法 $\text{Enc}(m,pk_A,pk_C)\rightarrow m_e$:Alice 由自己的公钥 pk_A、CSP 的公钥 pk_C 及明文 m,计算密文 m_e。

(3)验证算法 $\text{Ver}_A(m_e,sk_A)\rightarrow\{0,1\}$:Alice 由密文 m_e 及自己的私钥 sk_A,得到验证结果(0 表示不通过,1 表示通过)。

(4)授权算法 $\text{Auth}(sk_A,pk_B,pk_C)\rightarrow(msg_1,msg_2)$:Alice 由自己的私钥 sk_A、Bob 的公钥 pk_B 和 CSP 的公钥 pk_C,计算凭据 msg_1 和 msg_2。

(5)重加密 $\text{ReEnc}(m_e,msg_1,sk_C)\rightarrow m_c$:CSP 由密文 m_e、凭据 msg_1 和自己的私钥 sk_C,计算新密文 m_c。

(6)恢复算法 $\text{Rec}(m_c,msg_2,sk_B)\rightarrow m_b$:Bob 由新密文 m_c、凭据 msg_2 和自己的私钥 sk_B,计算 m_b。

(7)证实算法 $\text{Ver}_B(m_b,msg_2,sk_B)\rightarrow\{0,1\}$:Bob 由 m_b、凭据 msg_2 和自己的私钥 sk_B,得到验证结果(0 表示不通过,1 表示通过)。

3.2 TSCS 安全性质

一个 TSCS 方案应满足:

(1)完备性

· 正确性:

$\text{Rec}(\text{ReEnc}(\text{Enc}(m,pk_A,pk_C),msg_1,sk_C),msg_2,sk_B)=m$

· 可验证性:

给定 $m_e=\text{Enc}(m,pk_A,pk_C)$,有 $\text{Ver}_A(m_e,sk_A)=1$。

合法密文必可通过 Alice 验证。

给定 $m_b=m$,有 $\text{Ver}_B(m_b,msg_2,sk_B)=1$。

若正确恢复出原明文,必可通过 Bob 验证。

(2)数据机密性

· 对任意概率多项式时间敌手 T,对任意小正数 ε,有 $\Pr[T(m_e)=m]-\frac{1}{|F|}<\varepsilon$。$T$ 由密文求出明文的概率接近猜测攻击。

· 对任意概率多项式时间敌手 T,对任意小正数 ε,有 $\Pr[T(m_c)=m]-\frac{1}{|F|}<\varepsilon$。$T$ 由重加密密文求出明文的概率接近猜测攻击。

(3)不可移交性

对任意概率多项式时间敌手 T,若 T 不知道 sk_B,则对任意小正数 ε,有 $\Pr[T(m_c,msg_2)=m]-\frac{1}{|F|}<\varepsilon$。$T$ 由重加密密文 m_c 及凭据 msg_2 求出明文的概率接近猜测攻击。

(4)防篡改性

· 给定 $m_e'\neq Enc(m,pk_A,pk_C)$,对任意小正数 ε,有 $\Pr[\text{Ver}_A(m_e',sk_A)=1]<\varepsilon$。任意密文经篡改后,均难通过 Alice 验证。

· 给定 $m_b'\neq m$,对任意小正数 ε,有 $\Pr[\text{Ver}_B(m_b',msg_2,sk_B)=1]<\varepsilon$。Bob 恢复结果若非原明文,则难通过验证。

3.3 TSCS 方案一般框架

以下给出通常 TSCS 方案执行的步骤。

第一阶段:参数生成阶段

(1)KG 调用 Setup,为 Alice、Bob 和 CSP 生成密钥对;

第二阶段:存储阶段

(2)Alice 调用 Enc,将数据 m 加密后得 m_e,并传给 CSP;

第三阶段:共享阶段

(3)Bob 向 Alice 发出申请;

(4)Alice 调用 Auth,向 CSP 发送消息 msg_1,并向 Bob 发送消息 msg_2;

(5)CSP 调用 ReEnc,将 m_c 发送给 Bob;

(6)Bob 调用 Rec,得到 m_b,再调用 Ver_B,若得到 0,则拒绝。

步骤(2)之后,Alice 可随时调用 Ver_A,若得到 0,则拒绝。

4 Zhao 等的 TSCS 方案

下面简要回顾文献[16]中的方案。

(1)KG 调用 Setup,生成域 F(以下数及坐标,若未指定,均在 F 下)及椭圆曲线加法群生成元 G,生成 Alice 密钥对 $(sk_A=k_a,pk_A=k_aG)$、Bob 密钥对 $(sk_B=k_b,pk_B=k_bG)$、CSP 密钥对 $(sk_C=k_c,pk_C=k_cG)$;

(2)Alice 选随机数 r 和 t,调用 Enc,计算:

$m_e=\text{Enc}(m,pk_c)=m+rk_cG+tG$

Alice 在本地存储 r 和 t,在 CSP 处存储 m_e;

(3)Bob 向 Alice 发出请求;

(4)Alice 选随机数 r_c 和 r_b，调用 Auth，计算

$(msg_1, msg_2)=\text{Auth}(pk_B, pk_C)=((r_cG, t_cG), r_bG)$

其中，$t_cG=-r_bk_bG-r_ck_cG-rk_cG-tG$，Alice 发送 msg_1 给 CSP，并发送 msg_2 给 Bob；

(5)CSP 调用 ReEnc，计算

$m_c=\text{ReEnc}(m_e, msg_1, sk_C)=m_e+r_ck_cG+t_cG$，发送给 Bob；

(6)Bob 调用 Rec，计算

$m_b=\text{Rec}(m_c, msg_2, sk_B)=m_c+r_bk_bG$

该方案的正确性、数据机密性及不可移交性均已在文献[16]中讨论，在此不再赘述。

下面根据 3.1 节的模型，来讨论该方案存在的安全问题。我们发现 Zhao 等的 TSCS 方案存在以下两个问题：

• Alice 调用 Enc 时，未用到 pk_A；调用 Auth 时，未用到 sk_A。显然，该方案中，Alice 对密文及授权的保护仅仅在于随机数 r 和 t 的保密和性能。但通常来说，用户对随机数的保管力度远弱于私钥。此外，由于用户的计算能力有限，选择的随机数不一定能达到系统安全要求。

• 该方案未实现 Ver_A 和 Ver_B，未满足防篡改性要求。步骤(2)之后，CSP 可随时将 m_e 修改为任意值，而不被 Alice 查出。恶意 CSP 具体的攻击方法如下：

(1)KG 调用 Setup，生成域 F(以下数及坐标，若未指定，均在 F 下)及椭圆曲线加法群生成元 G，生成 Alice 密钥对 $(sk_A=k_a, pk_A=k_aG)$，Bob 密钥对 $(sk_B=k_b, pk_B=k_bG)$，CSP 密钥对 $(sk_C=k_c, pk_C=k_cG)$；

(2)Alice 选择随机数 r 和 t，调用 Enc，计算

$m_e=\text{Enc}(m, pk_c)=m+rk_cG+tG$

Alice 在本地存储 r 和 t，在 CSP 处存储 m_e；

(2)'CSP 将 m_e 改为 m_e'；

(3)Bob 向 Alice 发出请求；

(4)Alice 选择随机数 r_c 和 r_b，调用 Auth，计算

$(msg_1, msg_2)=Auth(pk_B, pk_C)=((r_cG, t_cG), r_bG)$

其中，$t_cG=-r_bk_bG-r_ck_cG-rk_cG-tG$，Alice 发送 msg_1 给 CSP，并发送 msg_2 给 Bob；

(5)CSP 调用 ReEnc，计算

$m_c=\text{ReEnc}(m_e', msg_1, sk_C)=m_e'+r_ck_cG+t_cG$，发送给 Bob；

(6)Bob 调用 Rec，计算

$m_b=\text{Rec}(m_c, msg_2, sk_B)=m_c+r_bk_bG$

此时有

$$\begin{aligned} m_b &= m_e'+r_ck_cG+t_cG+r_bk_bG \\ &= m_e'-rk_cG-tG \\ &\neq m_e-rk_cG-tG=m \end{aligned}$$

即 Bob 无法取到正确的明文。

同理，Alice 查询时，也无法求得原明文 m。Alice 将求得 $m'=m_e'-rk_cG-tG\neq m$。

步骤(5)中，CSP 可不调用 ReEnc，直接将任意值 m_c 发送给 Bob，而不被 Bob 查出。恶意 CSP 具体的攻击方法如下：

(1)KG 调用 Setup，生成域 F(以下数及坐标，若未指定，均在 F 下)及椭圆曲线加法群生成元 G，生成 Alice 密钥对 $(sk_A=k_a, pk_A=k_aG)$、Bob 密钥对 $(sk_B=k_b, pk_B=k_bG)$、CSP 密钥对 $(sk_C=k_c, pk_C=k_cG)$；

(2)Alice 选择随机数 r 和 t，调用 Enc，计算

$m_e=\text{Enc}(m, pk_c)=m+rk_cG+tG$

Alice 在本地存储 r 和 t，在 CSP 处存储 m_e；

(3)Bob 向 Alice 发请求；

(4)Alice 选择随机数 r_c 和 r_b，调用 Auth，计算

$(msg_1, msg_2)=\text{Auth}(pk_B, pk_C)=((r_cG, t_cG), r_bG)$

其中，$t_cG=-r_bk_bG-r_ck_cG-rk_cG-tG$，Alice 发送 msg_1 给 CSP，并发送 msg_2 给 Bob；

(5)'CSP 将任意值 m_c' 发给 Bob；

(6) Bob 调用 Rec，计算

$m_b=\text{Rec}(m_c', msg_2, sk_B)=m_c'+r_bk_bG$。

此时有 $m_b=m$，当且仅当 $m_c'=m-r_bk_bG$。由 m_c' 的任意性可知，Bob 取到正确的明文的概率仅为 $\frac{1}{ord(G)}$。

为此，我们提出改进 TSCS 方案。

5 新的 TSCS 方案

新方案的时序图(见图 1)及步骤说明如下：

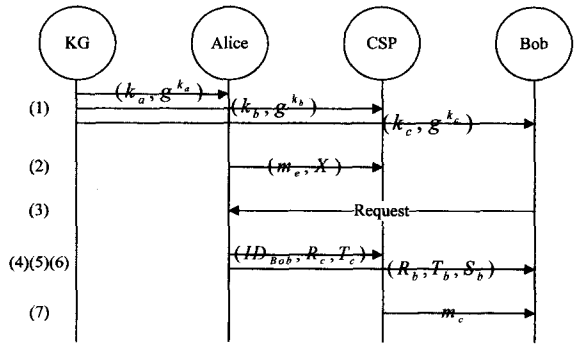

图 1 新方案时序图

新的 TSCS 方案可分为 3 个阶段。

第一阶段：生成阶段

(1)KG 调用 Setup，生成大质数 q，以及 $F=Z_q^*$ 中生成元 g(q 和 g 均公开)(以下计算，若未指定，均在 F 下；各方 ID 也在 F 下)。KG 生成 Alice 密钥对 $(sk_A=k_a, pk_A=g^{k_a})$，Bob 密钥对 $(sk_B=k_b, pk_B=g^{k_b})$，CSP 密钥对 $(sk_C=k_c, pk_C=g^{k_c})$；

第二阶段：存储阶段

(2)假设 $m\in F$。Alice 选择 $r, t, x\in_R F$，调用 Enc，计算

$$\begin{aligned} (m_e, X) &= \text{Enc}(m, pk_A, pk_C) \\ &= (m\cdot pk_C^r\cdot g^t\cdot pk_A^m, x\cdot g^m) \end{aligned}$$

Alice 在本地存储(r, t, x)，在 CSP 处存储(m_e, X)；

第三阶段：共享阶段

(3)Bob 向 Alice 发请求；

(4)Alice 选择 $r_c, r_b\in_R F$，从 CSP 处取 X，调用 Auth，计算

$$\begin{aligned} (msg_1, msg_2) &= \text{Auth}(sk_A, pk_B, pk_C) \\ &= ((ID_{Bob}, R_c, T_c), (R_b, T_b, S_b)) \end{aligned}$$

其中，$R_c=g^{r_c}$，$T_c=(pk_B^{r_b})^{-1}\cdot(pk_C^{r_c})^{-1}\cdot(pk_C^r)^{-1}\cdot(g^t)^{-1}$，$R_b=g^{r_b}$，$T_b=((X\cdot x^{-1})^{k_a})^{-1}$，$S_b=X\cdot x^{-1}\cdot pk_B$；

Alice 发送 msg_1 给 CSP，并发送 msg_2 给 Bob；

(5)CSP 调用 ReEnc，计算

$m_c=\text{ReEnc}(m_e, msg_1, sk_C)=m_e\cdot R_c^{k_c}\cdot T_c$，发送给 Bob；

(6)Bob 调用 Rec,计算

$m_b=\mathrm{Rec}(m_c,msg_2,sk_B)=m_c\cdot R_b^{k_b}\cdot T_b$

(7)Bob 调用 Ver_B,计算

$bool_b=\mathrm{Ver}_B(m_b,msg_2,sk_B)=(g^{m_b+k_b}==S_b)$

若 $bool_b$ 为 0,则 Bob 拒绝。

Alice 随时可取数据,调用 Ver_A,计算

$bool_a=\mathrm{Ver}_A((m_e,X),sk_A)$

$=(x\cdot g^{m_e\cdot(pk_C^r)^{-1}\cdot(g^t)^{-1}\cdot((X\cdot x^{-1})^{k_a})^{-1}}==X)$

若 $bool_a$ 为 0,则 Alice 拒绝。

通常,$m'=m_e\cdot(pk_C^r)^{-1}\cdot(g^t)^{-1}\cdot((X\cdot x^{-1})^{k_a})^{-1}$ 即为 Alice 所需的明文。可见验证过程并未影响 Alice 的正常读取需求。

简便起见,该方案基于 DLP。它的 ECDLP 形式也不难得到,例如将(2)改为:

$m_e=m+rk_cG+tG+(m_x+m_y)k_aG$

$X=x+(m_x+m_y)G$

式中,m_x 和 m_y 是 m 的横纵坐标,其后步骤作相应修改即可。

下面分析新方案的安全性能。

6 新的 TSCS 方案安全性分析

定理 1(完备性) 新的 TSCS 方案满足完备性。

证明:

·若各方遵循协议,则 Bob 应取到 Alice 最初存的明文 m:

$$\begin{aligned}m_b&=m_c\cdot R_b^{k_b}\cdot T_b\\&=m_e\cdot R_c^{k_c}\cdot T_c\cdot g^{r_bk_b}\cdot((X\cdot x^{-1})^{k_a})^{-1}\\&=m\cdot(g^{k_c})^r\cdot g^t\cdot(g^{k_a})^m\cdot g^{r_ck_c}\cdot((g^{k_b})^{r_b})^{-1}\cdot\\&\quad((g^{k_c})^{r_c})^{-1}\cdot((g^{k_c})^r)^{-1}\cdot(g^t)^{-1}\cdot g^{r_bk_b}\cdot g^{-k_am}\\&=m\end{aligned}$$

·Alice 验证时,若 m_e 未经改动,则:

$$\begin{aligned}m'&=m_e\cdot((g^{k_c})^r)^{-1}\cdot(g^t)^{-1}\cdot((X\cdot x^{-1})^{k_a})^{-1}\\&=m\cdot(g^{k_c})^r\cdot g^t\cdot(g^{k_a})^m\cdot((g^{k_c})^r)^{-1}\cdot(g^t)^{-1}\cdot\\&\quad g^{-k_am}\\&=m\end{aligned}$$

此时 $x\cdot g^{m'}=x\cdot g^m=X$,验证通过。

·Bob 验证时,若 m_c 未经改动,由前述,有 $m_b=m$,此时 $g^{m_b+k_b}=g^{m+k_b}=x\cdot g^m\cdot x^{-1}\cdot g^{k_b}=S_b$,验证通过。

综上,新方案满足完备性。

定理 2(数据机密性) 新的 TSCS 方案满足数据机密性。

证明:

·给定 X,因为 CSP 不知道 x,所以取得 g^m 的概率仅为 $\frac{1}{q-1}$;即使 CSP 取得了 g^m,由于 DLP 的困难性,此时 CSP 取得 m 的概率仅为 $\frac{1}{q-1}$。可见,CSP 以该途径成功取得 m 的概率仅为 $\frac{1}{(q-1)^2}$。

·给定 m_e,因为 CSP 不知道 r 和 t,所以 CSP 成功消去 $pk_C^r\cdot g^t$ 的概率仅为 $\frac{1}{(q-1)^2}$;即使 CSP 取得了 g^m,由于 CSP 不知道 k_a,因此 CSP 成功消去 $(g^{k_a})^m$ 的概率仅为 $\frac{1}{(q-1)^2}$。可见,CSP 以该途径成功取得 m 的概率仅为 $\frac{1}{(q-1)^4}$。

·给定 m_c,即使 CSP 截到了 R_b,也取到了 Bob 的公钥 g^{k_b},由于 CDH 问题的困难性,CSP 无法求得 $R_b^{k_b}$。此时 CSP 成功取得 m 的概率仅为 $\frac{1}{q-1}$。

综上,新方案满足数据机密性。

定理 3(不可移交性) 新的 TSCS 方案满足不可移交性。

证明:

·任何实体取得 $S_b=g^{m+k_b}$ 之后,即使可取得 Bob 的公钥 g^{k_b} 以求得 g^m,但由于 DLP 的困难性,成功取得 m 的概率仅为 $\frac{1}{q-1}$。同理,由 $T_b=g^{-k_am}$ 取得 m 的概率也仅为 $\frac{1}{q-1}$。

·任何实体取得 m_c,R_b,T_b 之后,恢复出 m 的唯一途径是使用 k_b。因此,任何非 Bob 方恢复出 m 的概率仅为 $\frac{1}{q-1}$。

综上,新方案满足不可移交性。

以下单独分析新方案相比原方案的改进。

7 防篡改性分析

由第 5 节显见,新方案的步骤中用到了 (sk_A,pk_A)。因此,无论是在 Alice 授权的独有性,还是 Alice 加密的安全性上,其均有显著改善。

以下分情况讨论并证明新方案的防篡改性。

定理 4(防篡改性) 新的 TSCS 方案满足防篡改性。

证明:

·Alice 检测篡改:

(1) 若 CSP 只将 m_e 改为 m_e',且 Alice 通过验证,则

$x\cdot g^{m'}=X=x\cdot g^m \bmod q$

$g^{m'}=g^m \bmod q$

$m'=m$

$$\begin{aligned}&m_e'\cdot((g^{k_c})^r)^{-1}\cdot(g^t)^{-1}\cdot((X\cdot x^{-1})^{k_a})^{-1}\\&\quad=m_e\cdot((g^{k_c})^r)^{-1}\cdot(g^t)^{-1}\cdot((g^{k_a})^m)^{-1} \bmod q\end{aligned}$$

$m_e'=m_e$

矛盾。所以此时 Alice 必拒绝。

(2) 设 $x=g^y(y\in Z_q^*)$,若 CSP 只将 $X=g^{m+y}$ 改为 $X'=g^z(z\in Z_q^*,g^z\neq g^{m+y})$,且 Alice 通过验证,则

$x\cdot g^{m'}=X' \bmod q$

$g^{m'+y}=g^z \bmod q$

$(q-1)\mid(m'+y-z)$

$z=m'+y$ 或 $z=m'+y-q+1$

若 $z=m'+y$,则

$$\begin{aligned}z&=y+m_e\cdot g^{-rk_c}\cdot g^{-t}\cdot((X'\cdot x^{-1})^{k_a})^{-1} \bmod q\\&=y+m\cdot(g^{k_a})^m\cdot((g^{z-y})^{k_a})^{-1} \bmod q\\&=y+m\cdot(g^{k_a})^{m+y-z} \bmod q\end{aligned}\quad(1)$$

该超越方程除了 $z=m+y$ 这一平凡解外(此时 $g^z=g^{m+y}$,矛盾),难以观察出其他解。显然,即使 CSP 知道 m 和 y,想求解式(1)也是不可行的,更何况 CSP 无法求出 m 和 y。

$z=m'+y-q+1$ 情况类似,不再赘述。

可见,CSP 无法构造出通过验证的 X',即 Alice 将拒绝。

(3) 若 CSP 同时修改 m_e 和 X,符号同上,且 Alice 通过验证,则

$x\cdot g^{m'}=X' \bmod q$

$g^{m'+y}=g^z \bmod q$

$(q-1)\mid(m'+y-z)$

$z=m'+y$ 或 $z=m'+y-q+1$

若 $z=m'+y$，则

$$z=y+m_e'\cdot g^{-rk_c}\cdot g^{-t}\cdot((X'\cdot x^{-1})^{k_a})^{-1} \bmod q$$

$$=y+m_e'\cdot g^{-rk_c}\cdot g^{-t}\cdot g^{k_a(y-z)} \bmod q \quad (2)$$

显然，CSP 不知道 y,r,t，无法求解 m_e' 和 z。

$z=m'+y-q+1$ 情况类似，不再赘述。

可见，CSP 无法构造出通过验证的 m_e' 和 X'，即 Alice 将拒绝。

· Bob 检测篡改：

若 CSP 将 m_c 改为 m_c'，且 Bob 通过验证，则

$g^{m_b+k_b}=g^{s_b} \bmod q$

$g^{m_b+k_b}=g^{m+k_b} \bmod q$

$g^{m_b}=g^m \bmod q$

$m_b=m$

$m_c'\cdot g^{r_bk_b}\cdot g^{t_b}=m_c\cdot g^{r_bk_b}\cdot g^{t_b} \bmod q$

$m_c'=m_c$

矛盾。所以此时 Bob 必拒绝。

综上所述，Alice 和 Bob 均可检测出 CSP 对数据的恶意篡改，新方案实现了防篡改性。

8 算法复杂度分析

KG 的密钥生成计算和 Alice 的随机数生成计算涉及质量，此处不作讨论。以下仅讨论各实体计算的时间复杂度，其通信时间复杂度及空间复杂度不作赘述。

· Alice 在存储数据时，进行 4 次模乘和 4 次模幂；在共享时，进行 1 次模加、4 次模乘、6 次模幂和 5 次模逆(第 5 节中的部分操作可简化)；在验证时，进行 5 次模乘、4 次模幂和 4 次模逆。

· Bob 在共享时，进行 2 次模乘和 1 次模幂；在验证时，进行 1 次模加和 1 次模幂。

· CSP 在共享时，进行 2 次模乘和 1 次模幂。

各实体计算量如表 1 所列。

表 1 各实体计算量表

计算量 / 月份 / 阶段	Alice	Bob	CSP
存储	4Mul+4Pow	\	\
共享	1Add+4Mul+6Pow+5Inv	2Mul+1Pow	2Mul+1Pow
验证	5Mul+4Pow+4Inv	1Add+1Pow	\

设 $k=\log_2 q$。众所周知，模 q 下的加法、乘法、幂和求逆的按位计算复杂度分别为 $O_B(k)$、$O_B(k^2)$、$O_B(k^3)$ 和 $O_B(k^2)$[17]。因此，各实体各阶段的计算复杂度均为 $O_B(k^3)$。

结束语 本文提出了云存储可信共享模型及其安全要求，并针对文献[16]中方案抵御篡改方面的不足，提出了改进方案。分析表明，新的 TSCS 方案不仅保持了原方案所有的安全性能，更实现了数据拥有者和共享请求者两方对服务器端恶意篡改的检测，并削弱了数据拥有者对随机数的依赖。新方案的计算复杂度适中，其具有良好的应用前景。

本文对于云存储可信共享的研究仅考虑了抵御服务器端方的篡改，而未考虑重放、中间人等各类主动攻击。这是未来工作的方向。

参 考 文 献

[1] 陈海波. 云计算平台可信性增强技术的研究[D]. 上海：复旦大学，2008

[2] 冯登国，张敏，张妍，等. 云计算安全研究[J]. 软件学报，2011，22(1)：71-83

[3] 张逢喆，陈进，陈海波，等. 云计算中的数据隐私性保护与自我销毁[J]. 计算机研究与发展，2011，48(7)：1155-1167

[4] 李乔，郑啸. 云计算研究现状综述[J]. 计算机科学，2011，38(4)：32-37

[5] Heiser J，Nicolett M. Assessing the Security risks of cloud computing[EB/OL]. http://www.gartner.com/DisplayDocument?id=685308，2008

[6] Ateniese G，Burns R，Curtmola R，et al. Provable data possession at untrusted stores[C]// Proceedings of the 14th ACM Conference on Computer and Communications Security. 2007：598-609

[7] Ateniese G，Di Pietro R，Mancini L，et al. Scalable and efficient provable data possession[C]// Proceedings of the 4th International Conference on Security and Privacy in Communication Networks. 2008

[8] Wang Cong，Wang Qian，Ren Kui，et al. Ensuring data storage security in cloud computing[C]// Proceedings of the 17th IEEE International Workshop on Quality of Service. 2009：1-9

[9] Juels A，Kaliski J B. PORs：Proofs of retrievability for large files[C]// Proceedings of the 14th ACM Conference on Computer and Communications Security. 2007：584-597

[10] Wang Qian，Wang Cong，Li Jin，et al. Enabling public verifiability and data dynamics for storage security in cloud computing[C]// Proceedings of the 14th European Symposium on Research in Computer Security. 2009

[11] Wang Cong，Wang Qian，Ren Kui，et al. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing[C]// Proceedings of the 29th IEEE Conference on Computer Communications. 2010：1-9

[12] Erway C，Kupcu A，Papamanthou C，et al. Dynamic provable data possession[C]// Proceedings of the 16th ACM Conference on Computer and Communications Security. 2009：213-222

[13] Zhang Jian-hong，Chen Hua. Security Storage in the Cloud Computing：A RSA-based Assumption Data Integrity Check without Original Data[C]// Proceedings of the IEEE Conference on Educational and Information Technology. 2010，2：143-147

[14] Hao Zhuo，Yu Neng-hai. A Multiple-Replica Remote Data Possession Checking Protocol with Public Verifiability[C]// Proceedings of the 2nd IEEE Symposium on Data，Privacy，and E-Commerce. 2010：84-89

[15] Wei Li-fei，Zhu Hao-jin，Cao Zhen-fue，et al. SecCloud：Bridging Secure Storage and Computation in Cloud[C]// Proceedings of the 30th IEEE Conference on Distributed Computing Systems Workshops. 2010：52-61

[16] Zhao Gan-sen，Rong Chun-ming，Jin Li，et al. Trusted Data Sharing over Untrusted Cloud Storage Providers[C]// Proceedings of the 2nd IEEE Conference on Cloud Computing Technology and Science. 2010：97-103

[17] Mao Wen-bo. Modern Cryptography：Theory and Practice [M]. Beijing：Publishing House of Electronics Industry，2004