doi:10.11959/j.issn.1000-436x.2017100

抗隐蔽敌手的云外包秘密共享方案

张恩[1,2]，耿魁[1]，金伟[1,3]，李勇俊[1,3]，孙韵清[4]，李凤华[1,3]

(1. 中国科学院信息工程研究所信息安全国家重点实验室，北京 100195；2. 河南师范大学计算机与信息工程学院，河南 新乡 453007；
3. 中国科学院大学网络空间安全学院，北京 100049；4. 西安电子科技大学通信工程学院，陕西 西安 710071)

摘 要：为了促使计算能力薄弱的云租户有效及公平地重构秘密，结合云外包计算和秘密共享特性，提出一种云外包秘密共享方案。在云外包秘密共享过程中，云租户间无需交互，只需进行少量解密和验证操作，而将复杂耗时的秘密重构计算外包给云服务提供商。该方案无需复杂的交互论证或零知识证明，能够及时发现云租户和云服务提供商的恶意行为，达到抵抗隐蔽敌手攻击的目的，最终每位云租户都能够公平和正确地得到秘密。安全分析和性能比较表明方案是安全和有效的。

关键词：秘密共享；外包计算；隐蔽敌手；公平性

中图分类号：TP309.2 **文献标识码**：A

Cloud outsourcing secret sharing scheme against covert adversaries

ZHANG En[1,2], GENG Kui[1], JIN Wei[1,3], LI Yong-jun[1,3], SUN Yun-qing[4], LI Feng-hua[1,3]

(1. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100195, China;
2. College of Computer and Information Engineering, Henan Normal University, Xinxiang 453007, China;
3. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China;
4. School of Telecommunications Engineering, Xidian University, Xi'an 710071, China)

Abstract: In order to make computationally weak cloud tenants can reconstruct a secret with efficiency and fairness, a cloud outsourcing secret sharing scheme was proposed, which combined cloud outsourcing computation with secret sharing scheme. In the process of outsourcing secret sharing, cloud tenants just need a small amount of decryption and validation operations, while outsource expensive cryptographic operations to cloud service provider (CSP). The scheme, without complex interactive augment or zero-knowledge proof, could detect malicious behaviors of cloud tenants or cloud service providers. And the scheme was secure against covert adversaries. Finally, every cloud tenant was able to obtain the secret fairly and correctly. Security analysis and performance comparison show that scheme is safe and effective.

Key words: secret sharing, outsourcing computation, covert adversaries, fairness

1 引言

秘密共享是密码学领域的重要研究内容，也是许多密码协议的基石，在密钥管理、电子商务、安全协议、数据安全存储、银行保险门开启、导弹发射控制等多方面有广泛的应用。秘密共享的思想是将秘密以某种方式拆分，拆分后的每个子份额由不同的参与者拥有，只有若干个参与者协同合作才能恢复秘密，这样达到防止秘密过于集中和容忍入侵的目的。经典的 (m,n) 门限秘密共享方案由 Shamir[1] 和 Blakeley[2]于 1979 年分别基于多项式插值法和多维空间点的特性提出。方案要求大于或等于 m 人才

收稿日期：2016-12-15；**修回日期**：2017-03-21
通信作者：耿魁，gengkui@iie.ac.cn
基金项目：国家高技术研究发展计划（"863"计划）基金资助项目（No.2015AA016007）；国家自然科学基金资助项目（No.U1401251, No.U1604156）；中国科学院大学生创新实践训练计划基金资助项目（No.1188005088）；河南省科技攻关基金资助项目（No.172102210045）

Foundation Items: The National High Technology Research and Development Program of China (863 Program) (No.2015AA016007), The National Natural Science Foundation of China (No.U1401251, No.U1604156), Innovative Practice Project of College Students in Chinese Academy of Sciences (No.1188005088), Science and Technology Research Project of Henan Province (No.172102210045)

可以重构出秘密，少于 m 人合作得不到秘密。然而，文献[1,2]不能防止分发者和参与者欺诈。此后，Chor 等[3]提出可验证秘密共享（VSS, verifiable secret sharing）方案，Feldman[4]和 Pedersen[5]基于同态性质分别提出一种可验证的秘密共享方案。张福泰等[6]提出一种有效的信息论安全的可验证秘密共享方案。Mahabir 等[7]提出一种公开可验证的秘密共享方案，每个参与者都可以公开验证秘密的正确性。刘木兰等[8]通过图上的随机游动，提出一种基于图的秘密共享方案，该重构算法的空间复杂度由一般多项式降低至对数级别。Hou 等[9]提出一种可视秘密共享方案，依靠人类的视觉进行解密，改进了秘密共享体制中重构秘密的复杂性。另外，在现实生活中，参与者之间常常需要共享多个秘密，当然可以简单重复利用单秘密共享体制来实现多个秘密共享，然而这种方法的缺陷是参与者管理的秘密子份额多，数量大，秘密重构的效率低下。针对此类问题，Dehkordi 等[10]、Fatemi 等[11]、Mashhadi 等[12]分别对多秘密共享方案进行了研究。Liu 等[13]对几个可验证多秘密共享方案进行了攻击，进而提出 2 个改进的多秘密共享方案。Cramer 等[14]基于线性纠错码和线性散列函数提出一种线性秘密共享方案。Mohammad 等[15]基于 Hermit 插值法和双线性映射提出一种动态可验证多秘密共享方案。Komargodski 等[16]基于多线性对提出一种分布式秘密共享方案。

以上经典的秘密共享方案在重构阶段有 2 种方案，一种需要可信用户参与，另一种不需要可信用户参与，但这 2 种方案都有相应的问题。如果重构阶段有可信用户参与，当然可以避免参与者的欺骗问题，最终每个参与者可以公平地得到秘密。但是要找到大家都可信的人则是非常困难的。如果没有可信用户参与，参与者的子份额依靠同时广播的方式发送，大家同时发送并且同时得到其他人的子份额，而在这种情况下，存在参与者欺诈问题，只能起到事后验证而不能起到事先预防的作用。例如，在秘密重构过程中，一个参与者 A 广播一个错误的子份额，而其他 $m-1$ 个人广播了正确的子份额。这样，欺骗者 A 就能独自得到秘密，尽管其欺骗行为在事后能被可验证的方法发现（但为时已晚），同样也会出现 2 个或多个人合谋欺骗或不发送子秘密份额的情形，这样合谋集团将独得秘密。而在异步通信网络中，参与者先后将子份额发给其他参与者，最后发送子份额者存在发送错误或不发送子份额的欺骗行为，这样欺骗者可以独自得到秘密，而其他诚实的参与者不能得到秘密或得到错误的秘密。

为了达到计算的公平性，Tompa 等[17]提出一种公平的秘密重构方法，方案将真实的秘密 D，放在一系列伪秘密中间 $\{D^1,\cdots,D^k\}$，其中，$D^i=D$，$1\leqslant i\leqslant k$，$D^j=pse$，$j\neq i$，pse 为伪秘密，然后将这一系列秘密拆分成子份额并分发给参与者。而秘密重构阶段需要运行多轮，参与者在每轮需要同时发送子份额，从而重构出一个秘密，当重构的秘密不是 pse 时，即为真实的秘密。因此，恶意参与者欺骗成功的概率为 $\frac{1}{k}$。Harn 等[18]提出一种公平的秘密共享方法，分发者选 k 个值 $\{s_1,\cdots,s_k\}$ 满足 $s_1>s_2>\cdots>s_{q-1}>s_q<s_{q+1}$，其中，$s_q$ 是秘密，$s_j\ (j\neq q)$ 是随机整数。将这 k 个值拆分后发给参与者。在重构阶段第 j 轮，$j=1,2,\cdots,k$，参与者合作重构出 s_j，然后和 s_{j-1} 进行比较，如果 $s_j>s_{j-1}$，则秘密是 s_{j-1}，否则，进行下一轮的比较。但在该方案中，如果协议运行至最后一轮，那么恶意的参与者通过欺骗将独自得到秘密，这样用逆向归纳法来分析，所有的参与者从开始就会保持沉默。

为了预防参与者欺诈及达到计算公平性，一系列文献[19~25]对理性秘密共享协议进行了研究，Halpern 和 Teague[19]首次将博弈论引入秘密共享和安全多方计算，不像传统方案，Halpern 和 Teague 认为所有的参与者都是自私的，都想使自己的效益最大化，参与者通过对自身利益得失的判断来决定是否遵守或背离协议，所设计的理性密码协议必须是多轮的，并且参与者不知道协议在哪一轮结束，从而才能使他们有合作的动机。但他们设计的理性秘密共享方案需要参与者人数大于或等于 3，并且协议在一定条件下需要重启，这样分发者需要重新分发秘密份额，相当于需要分发者一直在线。另外，他们的方案在 3 个成员参与的情况下，不能防止 2 个成员合谋；在多于 3 个成员参与的情况下，不能防止组长之间的合谋攻击。此后，田有亮等[20]基于贝叶斯博弈提出一种秘密共享方案。张志芳等[21]提出一种秘密共享扩展博弈方案。Maleka 等[22]提出一种基于重复博弈的秘密共享方案，通过考虑所有阶段博弈得益的贴现值之和（加权平均值）来对秘密共享建

立模型，使参与者考虑当前行为对后续博弈的影响，最终选择对自己最有利的策略，他们的方案要求构造子秘密的任意 2 个多项式的次数最多相差为 1，参与者不知道其他参与者多项式的次数，但参与者在自己最后一轮可以通过欺骗，以较高的概率获得秘密，所以他们的方案对逆向归纳来说是敏感的。另外，他们的方案需要利用拉格朗日插值法对分割后的子秘密进一步分割，所以协议的效率是非常低的，而且，这些方案也不能防止参与者合谋攻击，例如，如果有 2 个合谋者拥有的多项式的次数相差为 1 的话，那么合谋者能合谋得到秘密，同时阻止其他参与者获得秘密。Kol 等[23]利用二次剩余难题设计了有意义/无意义的加密算法，同时利用了安全多方计算等工具，构造了一种理性秘密共享方案。张恩等[24]提出一种点对点通信网络下多秘密共享方案。William 等[25]在异步信道下提出了一种秘密共享方案，方案需要有诚实的参与者，然而在分布式网络环境中，保证参与者始终诚实是非常困难的。

为了达到计算公平性，以上经典秘密共享和理性秘密共享方案均采用了多轮协议，期望的运行轮数越多，敌手欺骗的概率相对越小。因此，协议在秘密分发和重构阶段需要大量耗时的运算，并且需要客户间多次交互，协议效率低下、实现困难，更不能适用于计算能力薄弱的智能手机、平板电脑、PDA 等设备中。近年，为了进一步提高计算效率，云外包计算应运而生并很快成为学术界研究的热点，在云外包计算环境中，计算能力薄弱的云租户利用移动设备收集信息，当需要对收集的信息进行大量复杂耗时的计算时，将计算外包给具有强大计算能力的云服务提供商（CSP）来完成相关任务，这样租户可以享受无限制的计算资源，CSP 则根据租户计算任务按需收取相应报酬。Gennaro 等[26]在标准模型下，基于混淆电路和全同态提出一种适合于单个租户的可验证外包计算协议。方案增加了离线的预处理阶段，构造了具有全同态解密功能的混淆电路，租户能够验证 CSP 返回结果的正确性和完整性。Parno 等[27]提出一种公开代理和验证的方案，方案基于属性加密，但该方案不能保证属性的隐私。Glodwasser 等[28]提出一种基于 RLWE 问题的单密钥功能加密，并在功能加密基础上设计了公开可验证方案。Lopez 等[29]在 RLWE 困难问题基础上，提出一种 on-the-fly 安全多方计算协议，用户将密文存储在云中，CSP 可以动态选择计算功能，但其方案在解密阶段需要租户交互执行 MPC 协议。Gordon 等[30]结合具有 2 个输出结果的属性加密、混淆和代理不经意传输等加密方法，提出一种具有强安全保证的多租户验证外包计算。为了进一步提高外包计算效率以利于实际应用推广，文献[31~35]对具体的外包科学计算问题进行了研究。然而，目前尚没有针对秘密共享特性的云外包方案。

为了促使用户有效和公平地重构秘密，本文在结合云外包和秘密共享各自特性基础上，提出一种抗隐蔽敌手的云外包秘密共享方案。在本文设计的方案中，计算能力薄弱的云租户只需进行少量解密和验证操作，而将复杂耗时的计算外包给 CSP，能够有效提高云租户计算效率。另外，协议在解密阶段无需云租户间交互，所设计的验证算法无需复杂的非交互论证或零知识证明，从而更加实用。CSP 从自身声誉考虑，不会和云租户合谋，最终云租户能公平得到计算结果。方案具有以下性质：1) 隐私性，即在外包计算的同时能够保护云租户秘密子份额和最终重构秘密的隐私，CSP 不能获取云租户的子份额及最后重构的秘密任何有用信息；2) 抗合谋性，协议可抵抗至多 $m-1$ 个云租户合谋攻击，同时 CSP 从自身声誉考虑，不会选择和云租户合谋；3) 可验证性，即云租户可以有效验证 CSP 计算结果的正确性，同时云租户验证计算结果的时间不会超过云租户自身计算该结果所需时间；4) 公平性，即参与协议的所有云租户都能够公平地得到最终重构的秘密。

2　基础知识

2.1　攻击模型

根据攻击者的计算能力和行为，将敌手模型进行以下分类。

1) 根据计算能力将攻击者分为计算能力有限的敌手（概率多项式时间敌手）和具有无限计算能力的敌手。

2) 根据攻击者的行为分为半诚实敌手、恶意敌手和隐蔽敌手。

半诚实敌手模型也称被动攻击者，他们诚实地执行协议，但事后会将所得数据和其他不诚实者分享，用来分析其他参与者的输入和输出数据。

恶意敌手模型也称积极攻击者，在攻击参与者

后完全控制被攻击者并根据自身意愿任意背离协议如拒绝参加协议、更改输入、中断协议等。

隐蔽敌手模型处于半诚实模型和恶意模型之间，首先由 Aumann 和 Lindell[36]提出，主要思想是参与者为了自身利益可任意背离协议，但前提条件是希望自己的欺骗行为不易被别人发现，因为在商业、金融、政治和社交领域里，人们都不愿意冒失去信誉的风险，进而对今后的金融交易和社交造成负面影响。相比较其他 2 种模型，该模型更加符合实际。

3) 根据攻击者选择腐败对象的自适应性，将攻击者分为自适应性（即根据所得到的信息，在协议执行阶段能够任意腐败某些参与者）和非自适应性（即在协议执行前腐败的参与者已经确定）攻击者。

2.2 秘密共享

秘密共享系统由秘密空间、分发者、参与者、访问结构、秘密分发算法和秘密重构算法等组成。为了刻画哪些群体可以恢复秘密，即哪些参与者的集合是被授权恢复秘密的，本文将所有授权集的集合称为存取结构。设 $P=\{P_1,\cdots,P_n\}$ 是参与者集合，$AS\subseteq 2^P$ 是一个非空集，称 AS 是 P 上的存取结构，如果 AS 满足单调性，即如果 $A\in AS$，那么对任意 $A'\in 2^P$ 和 $A\subseteq A'$，有 $A'\in AS$。如果 AS 是 P 上的存取结构，那么 AS 中的任何集合称为 P 上的授权集。授权集有至少 m 个参与者构成，通常称这个存取结构为 (m,n) 门限存取结构。而秘密共享的信息率是为了研究秘密共享体制数据扩散程度，在秘密信息一定的条件下，透露给参与者的信息越少越利于体制的安全。

设 S 是 P_i（$1\leqslant i\leqslant n$）主秘密空间，S_i 是 P_i 的子秘密空间。将 $s\in S$ 表示为长度为 $\mathrm{lb}|S|$ 的比特串，同样，将 S_i 表示为长度为 $\mathrm{lb}|S_i|$ 的比特串，相对于 P_i 的信息率为

$$\rho_i=\frac{\mathrm{lb}|S|}{\mathrm{lb}|S_i|}$$

Shamir 于 1979 年基于 Lagrange 插值公式构造一种经典的门限秘密共享算法[1]。

1) 协议初始化阶段：分发者从 $GF(q)$ 中选取 n 个不同的非零元素 $x_1,\cdots,x_n$，然后将 x_i 分配给参与者 P_i，其中，q 为素数且 $q>n$。

2) 秘密分发阶段：从 $GF(q)$ 随机选择 $m-1$ 个元素 $a_1,\cdots,a_{m-1}$，构造 $m-1$ 次多项式 $f(x)=s+\sum_{i=1}^{m-1}a_ix^i$，计算 $y_i=f(x_i),1\leqslant i\leqslant n$，然后将 y_i 秘密发送给 P_i。

3) 秘密重构阶段：n 个参与者中的任意 m 个可重构多项式为

$$\begin{aligned}f(x)=&y_1\frac{(x-x_2)(x-x_3)\cdots(x-x_m)}{(x_1-x_2)(x_1-x_3)\cdots(x_1-x_m)}+\\&y_2\frac{(x-x_1)(x-x_3)\cdots(x-x_m)}{(x_2-x_1)(x_2-x_3)\cdots(x_2-x_m)}+\cdots+\\&y_m\frac{(x-x_1)(x-x_2)\cdots(x-x_{m-1})}{(x_t-x_1)(x_t-x_2)\cdots(x_m-x_{m-1})}\\=&\sum_{i=1}^{m}y_i\prod_{1\leqslant j\leqslant m,j\neq i}\frac{x-x_j}{x_i-x_j}\end{aligned}$$

其中，秘密 $s=f(0)$。

2.3 基于同态的可验证秘密共享方案

定义 1 同态加密。假设一个加密系统的加密函数与解密函数分别为 $E:\mathcal{M}\to\mathcal{C}$ 与 $D:\mathcal{C}\to\mathcal{M}$，其中，$\mathcal{M}$ 与 $\mathcal{C}$ 分别为明文空间与密文空间；令 $\otimes$ 和 $\oplus$ 分别为定义在明文空间和密文空间上的代数运算和算数运算，则加密方案的同态性定义为：给定任意 $m_1,m_2\in\mathcal{M}$，如果一个加密系统的加密函数与解密函数满足代数关系 $m_1\otimes m_2=D(E(m_1)\oplus E(m_2))$，则称该加密系统具有同态性。

同态加密又分为半同态加密和全同态加密，仅满足加法或乘法同态的叫半同态加密，既满足加法同态同时又满足乘法同态的叫全同态加密。

可验证秘密共享分为非交互式和交互式 2 种。若参与者在验证子份额时需要相互交换信息，称这种可验证秘密共享为交互式可验证秘密共享；若不需相互交换信息，则称之为非交互式可验证秘密共享。由于非交互式可验证秘密共享，减少了通信开销，所以更为常用。

Feldman[4]基于同态性质提出的非交互可验证秘密共享方法如下。

1) 方案参数 p 为大素数，q 为 $p-1$ 的大素数因子。$g\in Z_p^*$ 且为 q 阶生成元，三元组 (p,q,g) 公开。

2) 分发者在 Z_q 上构建一个 $t-1$ 次随机多项式 $f(x)$，$f(x)=a_0+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}$，其中，$a_0$ 是要共享的秘密。计算密钥子份额 $y_i=f(i)$ $(i=1,2,\cdots,n)$。

3) 分发者将 y_i 发送给参与者 P_i，并广播验证信息 $\alpha_j=g^{a_j}\bmod p$ $(j=0,\cdots,t-1)$。

4) 各参与者在收到密钥份额后，可以验证子份

额的正确性。参与者检查等式 $g^{y_i}=\prod_{j=0}^{t-1}(\alpha_j)^{i^j} \bmod p$ 是否成立，若成立，则说明参与者 P_i 收到的份额是正确的，否则是错误的。

Pedersen[5]基于同态性质的非交互可验证秘密共享方案如下。

1) 方案参数 p 为大素数，q 为 $p-1$ 的大素数因子，$g\in Z_p^*$ 且为 q 阶生成元。另取 $h\in Z_p^*$ 且 $h\in\langle g\rangle$，其中，$\log_g h$ 未知，四元组(p, q, g, h)公开。

2) 分发者在 Z_q 上任意选取 $2t-1$ 个随机数 $a_1,a_2,\cdots,a_{t-1},b_0,b_1,\cdots,b_{t-1}$ 构造以下 2 个多项式：$f(x)=a_0+\sum_{i=1}^{m-1}a_i x^i$ 和 $f(x)'=b_0+\sum_{i=1}^{m-1}b_i x^i$，其中，$f(0)=a_0$ 是要共享的秘密。计算相应的密钥子份额 $y_i=f(i), y_i'=f(i)'(1\leqslant i\leqslant n)$。

3) 分发者将子份额(y_i, y_i')发送给参与者 P_i，并广播验证信息 $\alpha_j=g^{a_j}h^{b_j} \bmod p(j=0,\cdots,m-1)$。

4) 各参与者在收到密钥份额后，可以验证子份额的正确性。参与者检查等式 $g^{y_i}h^{y_i'}=\prod_{j=0}^{m-1}(\alpha_j)^{i^j} \bmod p$ 是否成立，若成立，则说明参与者 P_i 收到的份额是正确的，否则是错误的。

2.4　多密钥全同态

多密钥全同态能够将具有单密钥性质的全同态方案扩展至多个参与者，每个参与者拥有各自的公私钥对，参与者使用不同的公钥加密各自的隐私输入，然后将密文上传给云服务提供者，云服务器对密文进行同态计算后得到密文 c 并将其发给每个参与者，最后，参与者使用各自的密钥共同解密得到最终的计算结果。

定义 2　多密钥 C-同态加密[29]。令 C 是电路簇，算法 $\{\Im^{(N)}=(Keygen,Enc,Dec,Eval)\}_{N>0}$ 如果满足以下性质，则称该算法是多密钥 C-同态的。

1) 密钥产生算法 $Keygen(1^k)\rightarrow(pk,sk,ek)$：输入安全参数 k，输出公钥 pk，私钥 sk，计算密钥 ek。

2) 加密算法 $Enc(pk,m_i)\rightarrow c_i$：给定公钥 pk 和信息 m_i，输出密文 c_i，其中，$i\in N$。

3) 计算算法 $c:=Eval(C,(c_1,pk_1,ek_1),\cdots,(c_N,pk_N,ek_N))$：给定布尔电路 C 和 N 元组 (c_i,pk_i,ek_i)，输出密文 c。

4) 解密算法 $C(m_1,\cdots,m_N):=Dec(sk_1,\cdots,sk_N,c)$：给定 N 个私钥 sk_i 和密文 c，输出 $C(m_1,\cdots,m_N)$。

定义 3　多密钥全同态[29]。对于所有电路簇 C，如果方案 $\{\Im^{(N)}=(Keygen,Enc,\ Dec,Eval)\}_{N>0}$ 满足多密钥 C-同态，则称该方案是多密钥全同态加密方案。

2.5　RLWE 问题

RLWE(ring learning with errors) 问题由 Lyubaskevsky 等[37]提出。此后一系列全同态加密方案基于该问题提出。

定义 4　RLWE 问题。对于安全参数 k，令 $f(x)=x^d+1$，其中，$d=d(k)$ 是 2 的幂次。令 $q=q(k)\in Z$ 是一个奇素数，$R=\frac{Z[X]}{f(x)}$，$R_q=\frac{R}{qR}$。令 $\chi=\chi(k)$ 是 R 上的分布。$RLWE_{f,q,\chi}$ 判定问题是指对于任意 $\ell=poly(k)$ 满足

$$\{(a_i,a_i s+e_i)\}_{i\in[\ell]}\overset{c}{\approx}\{(a_i,u_i)\}_{i\in[\ell]}$$

其中，s 是从噪音分布 χ 中的采样，a_i 在 R_q 中均匀分布，e_i 是从噪音分布 χ 中的采样，环元素 u_i 是 R_q 中均匀随机的元素。

2.6　Lopez 等的方案

该方案在 NTRU[38]基础上设计了多密钥全同态算法，步骤如下。

步骤 1　参与者 P_i 通过 $Keygen(1^k)$ 产生密钥元组 (pk_i,sk_i,ek_i)，然后通过算法 $Enc(pk,m_i)$ 加密输入信息 x_i 得到 c_i，将 (pk_i,ek_i,c_i) 发给云服务提供商。

步骤 2　云服务提供商计算密文 $c:=Eval(C,(c_1,pk_1,ek_1),\cdots,(c_N,pk_N,ek_N))$，然后广播密文 c。

步骤 3　参与者 $P_1,\cdots,P_N$ 运行安全多方计算协议得到 $Dec(sk_1,\cdots,sk_N,c)$。

为了抵抗恶意的参与者，方案采取了投币协议、零知识证明和承诺方案，为了验证云服务提供商的计算结果，方案采取了非交互论证等方法。

3　云外包秘密共享方案

为了高效及公平地重构秘密，本文方案结合云外包和秘密共享各自特性，在文献[29]设计的多密钥全同态基础上，提出一种抗隐蔽敌手的云外包秘密共享方案。

3.1　系统模型

方案包含分发者、云租户和云服务提供商 3 种实体，并分为 3 个阶段：秘密分发阶段、云外包计

算阶段和秘密解密验证阶段，其体系架构如图 1 所示。在秘密分发阶段，分发者将秘密子份额加密并进行数字签名后分发给云租户，以保证秘密的安全传输和验证。在云外包计算阶段（秘密重构），云服务提供商首先对云租户的信息进行验证，若验证成功则进行云外包密文计算，并将密文计算结果返回云租户；若验证失败则拒绝执行计算，并将参与者的欺骗行为进行广播。在秘密解密验证阶段，云租户对云服务提供商的密文计算结果解密并进行验证，以达到正确接收计算结果的目的。具体方案如下。

3.2 秘密分发阶段

步骤 1 由可信的秘密分发者运行数字签名的密钥产生算法得到密钥对 (pk_d, sk_d)，进而通过 Lopez[29] 设计的密钥产生算法 $Keygen(1^k)$ 得到 (pk_u, sk_u, ek_u)，其中，k 为安全参数，不同于文献[29]，本方案依据秘密共享的特性，云租户使用相同的公私钥对 (pk_u, sk_u)，这样在解密阶段，云租户无需交互，能够进一步提高云租户端计算和认证效率。为了降低客户端认证和计算开销，本文方案采用轻量级无需 CA 认证的 PKI[28]。

步骤 2 分发者从 $GF(q)$ 中随机选择 $m-1$ 个元素 $a_1,\cdots,a_{m-1}$，构造 $m-1$ 次多项式 $f(x)=s+\sum_{i=1}^{m-1}a_i x^i\ (1\leqslant i\leqslant n)$，其中，$s$ 为秘密。

步骤 3 分发者选择 n 个不同整数 $x_1,\cdots,x_n$，其中，x_i 作为参与者 P_i 的公开身份信息。计算 $y_i=f(x_i)$，然后通过多密钥全同态加密算法 $Enc(pk_u, y_i)$ 得到密文 c_i，并进行数字签名 $Sign_{sk_d}(c_i)\rightarrow\sigma_i$。

步骤 4 分发者用 CSP 的公钥 pk_{CSP} 加密 c_i，得到 $c_i'=Enc(pk_{CSP}, c_i)$。

步骤 5 分发者将元组 $(c_i', \sigma_i, h(s), sk_u)$ 发送给 P_i，其中，$h(\cdot)$ 为单向抗碰撞散列函数，并公开 (pk_u, ek_u)。

3.3 云外包计算阶段

步骤 1 由 m 个云租户分别将 $(c_i', \sigma_i)_{i\in m}$ 发给云服务提供商。

步骤 2 云服务提供商解密得到 c_i，运行签名验证算法 $Verify_{pk_d}(c_i, \sigma_i)$，如果验证成功，则执行步骤 3，如果验证失败，则拒绝执行计算，并将 P_i 的欺骗行为进行广播。

步骤 3 云服务提供商对密文进行计算 $c:=Eval(C,(c_1,pk_1,ek_1),\cdots,(c_m,pk_m,ek_m))$，其中，参与者公钥和计算密钥相同分别为 (pk_u, ek_u)，然后广播密文 c。

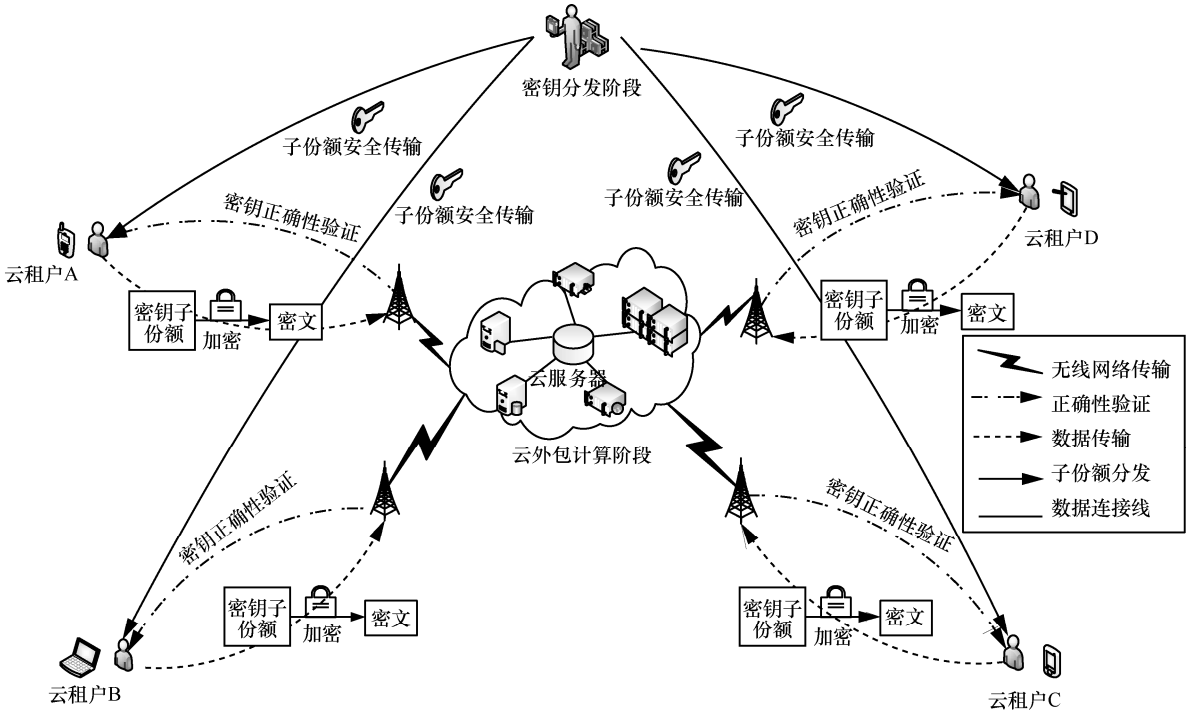

图 1 抗隐蔽敌手的云外包秘密共享方案体系架构

3.4 秘密解密验证阶段

步骤 1 云租户运行解密算法 $Dec(sk_1,\cdots,sk_m,c)$ 得到 $f(0)=\sum_{i=1}^{m} y_i \prod_{1\leqslant j\leqslant m,j\neq i}\frac{0-x_j}{x_i-x_j}$，这里，云租户私钥相同均为 sk_u。

解密算法 $Dec(sk_1,\cdots,sk_m,c)$ 如下。首先在密钥产生阶段产生 NTRU 公私钥对 $h:=[2gf^{-1}]$，$f\equiv 1(\mathrm{mod}\,2)$。令 (h_1,f_1) 和 (h_2,f_2) 是 2 个不同的 NTRU 公私钥对。密文 $c_1=[h_1s_1+2e_1+m_1]_q$ 和 $c_2=[h_2s_2+2e_2+m_2]_q$。利用 2 个私钥 f_1、f_2 能够分别将密文的乘积和密文的和解密得到相应明文的乘积和明文的和，计算过程如下

$$\begin{aligned}&[f_1f_2(c_1+c_2)]_q(\mathrm{mod}\,2)\\&=[2f_1f_2e_1+2f_1f_2e_2+2f_2g_1s_1+\\&\quad 2f_1g_2s_2+f_1f_2(m_1+m_2)]_q(\mathrm{mod}\,2)\\&=m_1+m_2(\mathrm{mod}\,2)\\&[f_1f_2(c_1c_2)]_q(\mathrm{mod}\,2)\\&=[4g_1g_2s_1s_2+2g_1s_1f_2(2e_2+m_2)+\\&\quad 2g_2s_2f_1(2e_1+m_1)+2f_1f_2(e_1m_2+\\&\quad e_2m_1+2e_1e_2)+f_1f_2(m_1m_2)]_q(\mathrm{mod}\,2)\\&=m_1m_2(\mathrm{mod}\,2)\end{aligned}$$

通过以上加法和乘法的组合，可以构造出任意电路计算功能。

步骤 2 云租户检验 $h(s)$ 和 $h(f(0))$ 是否相等，从而验证 CSP 计算结果的正确性。

4 方案分析与比较

4.1 安全分析

定理 1 如果 RLWE 问题是困难的，则本文方案中恶意的CSP获取云租户有用信息的优势 ε 是可忽略的。

证明 本文方案中，CSP 所采用的多密钥同态加密方案基于 RLWE 问题，设 A 为 CPA 攻击算法，其成功优势为 ε，则可以构造一个算法 B，该算法将算法 A 作为子程序调用，试图求解 RLWE 问题。首先算法 B 访问预言机得到一个采样 (h',C')。B 将 $h=ph'$ 发给 A 作为公钥。A 输出明文 m_0、m_1。B 选择一个随机比特 b，并计算挑战密文 $C=pC'+M_b$，然后将密文 C 发给 A。算法 A 输出一位 b'，如果 $b'=b$ 则算法 B 输出 1，否则输出 0。分析 B 的行为，有 2 种情况，一种是预言机从 RLWE 分布采样，另一种是从均匀分布采样。若从 RLWE 分布采样，又 $C'=hs+e$，则密文 $C=pC'+M_b$ 和 A 攻击方案的分布一样，其成功概率为 $\frac{1}{2}+\varepsilon$。若从均匀分布采样，则密文 C 是均匀分布的，A 输出 $b'=b$ 的概率为 $\frac{1}{2}$。又依据 RLWE 定义知 $\{(a_i,a_is+e_i)\}_{i\in[\ell]}\overset{c}{\approx}\{(a_i,u_i)\}_{i\in[\ell]}$，因此，可得 ε 是可忽略的。

定理 2 恶意的云租户不能用错误的输入信息欺骗 CSP。

证明 本文采用 CPA 安全的数字签名方案 $\prod=(Gen,Sign,Verify)$ 对云租户信息签名并验证。秘密分发者利用私钥 sk_d 对秘密子份额进行数字签名 $Sign_{sk_d}(c_i)\to\sigma_i$，云租户和 CSP 利用分发者的公钥 pk_d 对数字签名进行验证 $Verify_{pk_d}(c_i,\sigma_i)$，因此敌手 A 伪造子份额成功的优势 ε 是可忽略的。

定理 3 云租户可以有效验证 CSP 计算结果，最终所有云租户能够公平获得秘密。

证明 云租户运行解密算法 $Dec(sk_1,\cdots,sk_m,c)$ 得到 $f(0)=\sum_{i=1}^{m} y_i \prod_{1\leqslant j\leqslant m,j\neq i}\frac{0-x_j}{x_i-x_j}$。当 $h(s)$ 和 $h(f(0))$ 相等时，云租户能够确认 CSP 计算结果是正确的，否则认为 CSP 计算结果是错误的。假设敌手 $\mathcal{A}$ 能够找到一个 s'，使当 $s\neq s'$ 时 $h(s)=h(s')$，则敌手能够成功找到了一个散列碰撞，但由抗碰撞散列函数的性质可知，敌手成功的优势 ε 是可忽略的。

另外，在本文方案中假设 CSP 和云租户之间不能合谋，在现实社会中，一些大的 CSP 如 Google 云、百度云或阿里云等都是有社会声誉和地位的，失去信誉将会对其今后从事的金融交易和社交行为造成负面影响，因此，CSP 有正确执行协议的动机，最终所有云租户都能公平和正确地重构秘密。

4.2 性能比较

近年来，随着智能手机和平板电脑的日益普及，移动互联网在许多领域已对传统的 PC 互联网形成了替代。智能手机已改变了人们日常的工作、生活和学习方式。传统的秘密共享方案目前有 2 个缺陷：1) 无法有效应用于移动互联网；2) 很难保证计算公平性。而本文提出的基于云外包计算的秘密共享方案则可以有效解决以上 2 个问题。

首先，由分发者执行数字签名密钥产生算法、加密算法并进行数字签名，将加密信息、签名信息

和最终秘密的散列值发给参与者；然后参与者将加密子份额及分发者签名信息发给 CSP；接着，CSP 运行签名验证算法和同态计算并将结果返还给参与者；最后参与者解密并进行验证。在整个计算过程中，参与者仅需要进行少量解密和验证操作，而将大量的签名验证和同态计算外包给 CSP 进行计算。而分发者可以在空闲时间或预处理阶段对数据进行签名和加密操作。另外，通过引入 CSP，能够消除参与者后发子份额的优势，可以确保参与者及时正确地发送子份额，从而可以保证计算的公平性。

接下来，分别和近些年的经典秘密共享、公平的秘密共享协议和理性秘密共享 3 类相关方案进行比较，如表 1 所示。文献[13,14]为经典秘密共享协议，方案可以通过一轮协议重构秘密，文献[13,14]的通信开销为 $O(t)$，但受经典秘密共享束缚，该方案不能预防成员欺诈，不能达到计算公平目的。文献[18]提出一种公平的秘密共享协议，文献[20]提出一种理性秘密共享协议，两者可以预防成员欺诈、达到计算公平，但协议期望迭代轮数为多轮，用户间需要进行多次交互获得多个子份额并多次重构秘密，由于需要运行多轮（假设为 k 轮），因此，通信开销为 $O(tk)$，另外每一轮协议在实际运行中，还需要复杂的验证计算以检验参与者的诚实度，可知协议需要用户间大量交互计算，通信开销大，难以实现，不适合计算能力薄弱的设备。

表 1 方案比较

方案	期望迭代轮数	是否需要成员交互	计算是否公平	通信开销	秘密重构算法
文献[13]	一轮	是	否	$O(t)$	用户
文献[14]	一轮	是	否	$O(t)$	用户
文献[18]	多轮	是	是	$O(tk)$	用户
文献[20]	多轮	是	是	$O(tk)$	用户
本文方案	一轮	否	是	$O(1)$	云端

从表 1 中可知，文献[13,14,18,20]中每个用户通信开销会随着秘密共享门限 t 的增加而线性增大。相比而言，本文方案通过执行一轮云外包计算协议即可重构出秘密，且用户通信开销不随秘密共享门限 t 的增加而增加。随着方案运行轮数和门限的增加，本文方案通信开销优势会更加明显。另外，在本方案中，计算能力薄弱的租户设备只需一次解密操作和一次验证操作，而将大量耗时的运算外包给 CSP，云租户之间无需交互。同时，方案可以及时验证租户和 CSP 的恶意行为，并且无需零知识证明和非交互论证等复杂耗时的计算。最终每位云租户能够公平和正确地获得重构的秘密。

5 结束语

本文在结合云外包计算和秘密共享各自特性基础上提出了一种抗隐蔽敌手的云外包秘密共享方案，计算能力薄弱的云租户可以将大量耗时的秘密重构算法外包给 CSP，云租户仅需少量的解密和验证运算，在验证过程中，本文方案无需零知识证明和非交互论证等复杂的验证方法，能够及时发现云租户和 CSP 的恶意行为。在云外包计算过程中，CSP 不能获取有关云租户秘密子份额及最终重构秘密的任何有用信息，从自身声誉着想，云租户和 CSP 都不会冒失去信誉的风险而从事恶意行为，最终每位云租户都能够公平地得到重构的秘密。

参考文献：

[1] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(1): 612-613.

[2] BLAKELEY G R. Safeguarding cryptographic keys[C] // The National Computer Conference. 1979. 313-317.

[3] CHOR B, GOLDWASSER S, MICALI S, et al. Verifiable secret sharing and achieving simultaneity in the presence of faults[C]//26th IEEE Annual Symposium on Foundations of Computer Science. 1985: 383-395.

[4] FELDMAN P. A practical scheme for non-interactive verifiable secret sharing[C] // 28th IEEE Annual Symposium Foundations of Computer Science. 1987: 427-438.

[5] PEDERSEN T P. Distributed provers with applications to undeniable signatures[C] //Advances in Cryptology—EUROCRYPT'91. 1991: 221-242.

[6] ZHANG F T, ZHANG J. Efficient and information-theoretical secure verifiable secret sharing over bilinear groups[J]. Chinese Journal of Electronics, 2014, 23(1): 13-17.

[7] MAHABIR P J, AYINEEDI V, REIHANEH S N. Paillier-based publicly verifiable (non-interactive) secret sharing[J]. Designs Codes and Cryptography, 2014, 73(2): 529-540.

[8] 刘木兰，肖亮亮，张志芳．一类基于图上随机游动的密钥共享体制[J]. 中国科学 E 辑：信息科学, 2007, 37(2): 199-208.
LIU M L, XIAO L L, ZHANG Z F. Secret sharing schemes based on random walks on graphs[J]. Science in China (Series E), 2007, 37(2): 199-208.

[9] HOU Y C, QUAN Z Y, TSAI C F, et al. Block-based progressive visual secret sharing[J]. Information Sciences, 2013, 233(1): 290-304.

[10] DEHKORDI M H, FARZANEH Y. A new verifiable multi-secret sharing scheme realizing adversary structure[J]. Wireless Personal Communications, 2015, 82(3): 1749-1758.

[11] FATEMI M, GHASEMI R, EGHLIDOS T, et al. Efficient multistage secret sharing scheme using bilinear map[J]. Information Security, IET, 2014, 8(4): 224-229.

[12] MASHHADI S, DEHKORDI M H. Two verifiable multi secret sharing schemes based on nonhomogeneous linear recursion and LFSR

public-key cryptosystem[J]. Information Sciences, 2015, 294(2): 31-40.
[13] LIU Y H, ZHANG F T, ZHANG J. Attacks to some verifiable multi-secret sharing schemes and two improved schemes[J]. Information Sciences, 2016, 329(1): 524-539.
[14] CRAMER R, DAMGÅRD I B, DÖTTLING N, et al. Linear secret sharing schemes from error correcting codes and universal hash functions[C] //Advances in Cryptology-EUROCRYPT 2015. Springer Berlin Heidelberg, 2015: 313-336.
[15] MOHAMMA H T, HADI K, MOHAMMAD S H. Dynamic and verifiable multi-secret sharing scheme based on hermite interpolation and bilinear maps[J]. Information security, IET, 2015, 9(4): 234-239.
[16] KOMARGODSKI I, ZHANDRY M. Cutting-edge cryptography through the lens of secret sharing[C]//Theory of Cryptography. 2016: 449-479.
[17] TOMPA M, WOLL H. How to share a secret with cheaters[J]. Journal of Cryptology, 1989, 1(3): 133-138.
[18] HARN L, LIN C, LI Y. Fair secret reconstruction in (*t*, *n*) secret sharing[J]. Journal of Information Security & Applications, 2015, 23(C): 1-7.
[19] HALPERN J, TEAGUE V. Rational secret sharing and multiparty computation[C]//The 6th Annual ACM Symposium on Theory of Computing. ACM, 2004: 623-632.
[20] TIAN Y L, PENG C G, LIN D D, et al. Bayesian mechanism for rational secret sharing scheme[J]. Science China Information Sciences, 2015, 58(5): 1-13.
[21] ZHANG Z F, LIU M L. Rational secret sharing as extensive games[J]. Science China Information Sciences, 2013, 56(3): 1-13.
[22] MALEKA S, SHAREEF A, RANGAN C P. Rational secret sharing with repeated games[C]//Information Security Practice and Experience. 2008: 334-346.
[23] KOL G, NAOR M. Cryptography and game theory: designing protocols for exchanging information[M] //Theory of Cryptography. Springer Berlin Heidelberg, 2008: 320-339.
[24] ZHANG E, CAI Y Q. Rational multi-secret sharing scheme in standard point-to-point communication networks[J]. International Journal of Foundations of Computer Science, 2013,24(6): 879-897.
[25] WILLIAM K. MOSES J, C. RANGAN P. Rational secret sharing over an asynchronous broadcast channel with information theoretic security[J]. International Journal of Network Security & Its Applications, 2011, 3(6): 1-18.
[26] GENNARO R, GENTRY C, PARNO B. Non-interactive verifiable computing: outsourcing computation to untrusted workers[C]//Advances in Cryptology–CRYPTO 2010. 2010: 465-482.
[27] PARNO B, RAYKOVA M, VAIKUNTANATHAN V. How to delegate and verify in public: verifiable computation from attribute-based encryption[C]//Theory of Cryptography. 2012: 422-439.
[28] GOLDWASSER S, KALAI Y, POPA R A, et al. Reusable garbled circuits and succinct functional encryption[C]//The 44th Annual ACM Symposium on Theory of Computing. 2013: 555-564.
[29] LÓPEZ-ALT A, TROMER E, VAIKUNTANATHAN V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption[C]//The 44th Annual ACM Symposium on Theory of Computing. 2012: 1219-1234.
[30] GORDON S D, KATZ J, LIU F H, et al. Multi-client verifiable computation with stronger security guarantees[C]//Theory of Cryptography. 2015: 144-168.
[31] ZHANG E, LI F H, NIU B, et al. Server-aided private set intersection based on reputation[J]. Information Sciences, 2016, doi:10.1016/j.ins.2016.09.056.
[32] ZHANG F G, MA X, LIU S L. Efficient computation outsourcing for inverting a class of homomorphic functions[J]. Information Sciences, 2014, 286(1): 19-28.
[33] CHEN X F, HUANG X Y, LI J, et al. New algorithms for secure outsourcing of large-scale systems of linear equations[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(1): 69-78.
[34] WANG C, REN K, WANG J. Secure optimization computation outsourcing in cloud computing: a case study of linear programming[J]. IEEE Transactions on Computers, 2016, 65(1): 216-229.
[35] REN Y L, DING N, ZHANG X P, et al. Verifiable outsourcing algorithms for modular exponentiations with improved checkability[C] // The 11th ACM on Asia Conference on Computer and Communications Security. ACM, 2016: 293-303.
[36] AUMANN Y, LINDELL Y. Security against covert adversaries: efficient protocols for realistic adversaries[J]. Journal of Cryptology, 2010, 23(2): 281-343.
[37] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over ring[J]. Journal of the ACM, 2013, 60(6): 1-35.
[38] STEHLÉ D, STEINFELD R. Making NTRU as secure as worst-case problems over ideal lattices[C]//Advances in Cryptology– EUROCRYPT 2011. 2011: 27-47.

作者简介：

张恩（1974-），男，河南新乡人，博士，中国科学院信息工程研究所副教授、硕士生导师，主要研究方向为密码协议、隐私保护。

耿魁（1989- ），男，湖北红安人，博士，中国科学院信息工程研究所助理研究员，主要研究方向为网络安全。

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。

李勇俊（1992-），男，浙江丽水人，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。

孙韵清（1997-），女，陕西西安人，主要研究方向为网络安全防护。

李凤华（1966-），男，湖北浠水人，博士，中国科学院信息工程研究所副总工程师、研究员、博士生导师，主要研究方向为网络与系统安全、隐私计算、信息保护。