doi:10.11959/j.issn.1000-436x.2017109

格上可重新拆分的门限多代理者的代理重加密方案

李菊雁[1]，马春光[1,2]，赵乾[1]
(1. 哈尔滨工程大学计算机科学与技术学院，黑龙江 哈尔滨 150001；2. 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 100093)

摘 要：在格上利用 2 个不同的加密方案及拉格朗日插值多项构造了一个可重新拆分的门限多代理者的代理重加密方案，即在密文输入输出面与重加密面的加密方案是不同的，这使噪音的界有更宽的选择范围。另外，门限多代理者不仅保证了重加密密钥的安全性，而且当个别代理不能提供正常服务时，重加密方案仍能正确工作。该方案证明是 IND-UniRTPRE-CPA 安全的。

关键词：代理重加密；门限多代理者；容错学习问题；IND-UniRTPRE-CPA 安全
中图分类号：TP309 **文献标识码**：A

Resplittable threshold multi-broker proxy re-encryption scheme from lattices

LI Ju-yan[1], MA Chun-guang[1,2], ZHAO Qian[1]
(1. College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China;
2. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

Abstract: Two different encryption schemes and Lagrange polynomial were used to construct a resplittable threshold multi-broker proxy re-encryption scheme on the lattice, namely the encryption in the ciphertext input and output side was different from the encryption in the re-encryption side which make the bound of noise was more relaxed. Threshold multi proxy not only ensure the safety of re-encryption key, but also ensure re-encryption scheme can still work even if the individual proxy could not provide normal services. The scheme is proven IND-UniRTPRE-CPA secure.

Key words: proxy re-encryption, threshold multi-proxy, learning with error, IND-UniRTPRE-CPA secure

1 引言

随着云计算的发展，越来越多的用户选择将数据加密后存储在云中，因此，如何灵活地共享存储在云中加密的数据成为一个挑战。代理重加密为云数据加密共享提供了一种有效的解决方案。门限密码技术可以用于密钥托管，并且能有效地增强数字签名服务器及认证服务器的安全性和可靠性，在数字签名、认证及秘密恢复系统中也有着重要的应用。当用户将云中的数据共享时，并不能保证代理的诚实（计算），而门限密码可以允许个别代理的不诚实或不正常工作，因此，研究门限多代理者的代理重加密方案具有重要的现实意义。

代理重加密（PRE）是公钥加密的一个扩展。在一个 PRE 方案中，代理者（一般为半诚实的）获得一个从授权者 Alice 到受理者 Bob 的代理重加密密钥 $rk_{A\to B}$ 和 Alice 的一个密文 ct，在不对 ct 解密的情况下输出一个 Bob 的输出密文 $\widehat{ct}$，使 Bob 对 $\widehat{ct}$ 解密得到的明文和 Alice 对 ct 解密得到的明文相同，而代理者不能获得任何明文信息[1]。PRE 最近

收稿日期：2016-08-23；**修回日期**：2017-04-13
通信作者：马春光,machunguang@hrbeu.edu.cn
基金项目：国家自然科学基金资助项目（No.61472097）；高等学校博士学科点专项科研基金资助项目（No.20132304110017）；信息安全国家重点实验室开放课题基金资助项目（No.2016-MS-10）
Foundation Items: The National Natural Science Foundation of China (No.61472097), The Special Research Found for the Doctoral Program of Higher Education of China (No.20132304110017), The Open Fund of the State Key Lab of Information Security (No.2016-MS-10)

引起了广泛的研究[2~10]。格密码是一种抗量子计算攻击的公钥密码体制。自从 Regev[11]在量子归约下证明了容错学习（LWE, learning with error）问题至少与最坏情况的近似因子为 $\widetilde{O}\left(\frac{n}{\alpha}\right)$ 的求格最短向量(SVP)问题、最短线性无关向量(SIVP)问题的变体一样困难，其中，α 是 LWE 实例中与扰动分布的方差有关的参数。基于 LWE 的格上代理重加密方案引起了广泛的关注。

Xagawa[2]在格上构造了第一个双向的 PRE 方案，并证明方案是 CPA 安全的，但是该方案不能抵抗合谋攻击。Aono 等[3]利用 Lindner[12]的加密方案在格上构造了一个密钥隐私的 PRE 方案（KP-PRE）。Singh 等[4]指出 Aono 等[3]的方案在主密钥安全模型下是不安全的，即当代理者和受理者共谋时可以攻击授权者的密钥。Nishimak 等[5]分别利用 Lindner 等[12]的加密方案和 Regev[11]的加密方案构造了 2 个密钥隐私的 PRE 方案，即 Reg-to-Reg 方案和 LP-to-LP 方案。Jiang 等[6]利用 Gentry 等[13]的加密方案构造了一个抗共谋攻击的 PRE 方案，并且证明该方案在标准模型下是 CPA 安全的。周潭平等[8]构造了一个全同态代理加密方案。Singh 等[9]构造了一个基于身份的单向 PRE。苏等[10]构造了一个面向移动云计算的多要素代理重加密方案。但是这些 PRE 方案的构造，都只是利用一个加密方案，即在密文输入输出面的加密方案与重加密面的加密方案是相同的。本文将利用 2 个不同的加密方案构造一个代理重加密方案，即加密算法与重加密算法是不同的。

门限密码的思想是由 Desmedt 等[14]在 1989 年首次提出的。一个（t, u）门限公钥加密方案（TPKE）指的是在一个公钥加密方案中，密钥被分给 u 个不同的用户，只有当至少 t 个用户共同解密时，才能正确对密文进行解密。可重新拆分的门限公钥加密方案指的是在门限公钥加密方案中引入了一个新的算法——Tsplit。可重新拆分的门限公钥加密方案（RTPKE）由 Hanaoka 等[15]在 2012 年首次提出，在 RTPKE 中，如果随机算法 Tsplit 输出的共享腐败私钥的个数小于 t，则私钥的拆分能做任意多项式次。但是在 TPKE 中，私钥的拆分只能在密钥生成算法中执行一次。

Singh 等[16]在格上构造了一个 RTPKE，并证明其是在 LWE 假设下是 CPA 安全的。楼圣铭等[17]首次将代理重加密与门限密码和基于身份密码相结合，提出第一个基于身份的门限多代理者的代理重加密方案。但是其安全性是基于 q 增加双线性 Diffie-Hellman 指数的。

本文的主要贡献是，首先在格上利用 2 个不同的加密方案构造一个门限多代理者的代理重加密方案，即利用 Regev[11]的加密方案和 Lindner[12]的加密方案构造一个重加密方案，在密文输入输出时的加密方案是 Lindner[12]的加密方案，而在重加密时利用的是 Regev[11]的加密方案，这使噪音的界有更宽的选择范围。其次是在格上将 PRE 与门限密码结合。最后证明该方案是选择明文攻击下不可区分（IND-UniRTPRE-CPA）安全的。

2 预备知识

本文中的数、列向量、矩阵分别记为 x、$\boldsymbol{x}$、$\boldsymbol{X}$。$\lfloor x\rfloor$、$\lceil x\rceil$、$\lfloor x\rceil$（$x\geqslant 0$）表示对数 x 向下、向上和四舍五入取整。$\boldsymbol{x}^{\mathrm{T}}$、$\boldsymbol{A}^{\mathrm{T}}$ 分别表示向量 $\boldsymbol{x}$、矩阵 $\boldsymbol{A}$ 的转置，向量的内积记为 $<\boldsymbol{v},\boldsymbol{u}>$，$\boldsymbol{I}_k$ 表示 k 阶单位矩阵。$\eta=\lceil \mathrm{lb}q\rceil$，$\mathbb{Z}_q=\left(-\frac{q}{2},\frac{q}{2}\right]\cap\mathbb{Z}$，$[k]$表示集合 $\{1,2,\cdots,k\}$，$\|\boldsymbol{V}\|_p$ 表示向量 $\boldsymbol{V}$ 的 l_p 模，当 p=2 时，$\boldsymbol{V}$ 的 l_2 模$\|\boldsymbol{V}\|_2$ 指的是 $\boldsymbol{V}$ 的欧几里得模，$\|\boldsymbol{V}\|_2$ 简记为 $\|\boldsymbol{V}\|$，当 p=∞时，$\boldsymbol{V}$ 的 l_∞模$\|\boldsymbol{V}\|_\infty$指的是 $\boldsymbol{V}$ 中元素的最大量级。对于概率分布 χ 而言，$x\leftarrow\chi$ 表示 x 依概率分布 χ 选取，对于集合 S，$x\leftarrow S$ 表示 x 在集合 S 上均匀随机选取。

对于 2 个矩阵 $\boldsymbol{X}\in\mathbb{Z}_q^{m\times n},\boldsymbol{Y}\in\mathbb{Z}_q^{m\times l}$，规定 $[\boldsymbol{X}\,|\,\boldsymbol{Y}]\in\mathbb{Z}_q^{m(n+l)}$ 是 $\boldsymbol{X}$ 与 $\boldsymbol{Y}$ 的按列连接。对于 2 个矩阵 $\boldsymbol{X}\in\mathbb{Z}_q^{nm},\boldsymbol{Y}\in\mathbb{Z}_q^{lm}$，规定$[\boldsymbol{X};\boldsymbol{Y}]\in\mathbb{Z}_q^{(n+l)m}$ 是 $\boldsymbol{X}$ 与 $\boldsymbol{Y}$ 的按行连接。对于任意的向量 $\boldsymbol{x}^{\mathrm{T}}=(x_1,\cdots x_n)\in\mathbb{Z}_q^n$，记 $g^{\boldsymbol{x}^{\mathrm{T}}}=\left(g^{x_1},\cdots,g^{x_n}\right)$。

对于向量 $\boldsymbol{x}\in\mathbb{Z}_q^n$，规定

$$\begin{aligned}P_2(\boldsymbol{x})&=\left(1,2,\cdots,2^{\eta-1}\right)^{\mathrm{T}}\otimes\boldsymbol{x}\\&=\left(1\boldsymbol{x};2\boldsymbol{x};\cdots;2^{\eta-1}\boldsymbol{x}\right)^{\mathrm{T}}\in\mathbb{Z}_q^{n\eta}\\BD\left(\boldsymbol{x}^{\mathrm{T}}\right)&=\left(\boldsymbol{u}_1^{\mathrm{T}}\,|\cdots|\,\boldsymbol{u}_\eta^{\mathrm{T}}\right)\in\{0,1\}^{n\eta}\end{aligned}$$

其中，$\boldsymbol{x}^{\mathrm{T}}=\sum_{k=1}^{\eta}2^{k-1}\boldsymbol{u}_k^{\mathrm{T}}$。对于矩阵 $\boldsymbol{A}$，$P_2(\boldsymbol{A})$ 表示用函数 $P_2(\bullet)$ 依次作用于 $\boldsymbol{A}$ 的列。

引理 1[5]（leftover hash 引理）设 q 为素数，假

设 D 为 $\mathbb{Z}_q^m$ 上最小熵为 $(n+l)\eta+g(n)$ 的分布，那么 $(\boldsymbol{A},\boldsymbol{e}^{\mathrm{T}}\boldsymbol{A})$ 和 $(\boldsymbol{A},\boldsymbol{u})$ 的统计距离

$$\Delta\left((\boldsymbol{A},\boldsymbol{e}^{\mathrm{T}}\boldsymbol{A}),(\boldsymbol{A},\boldsymbol{u})\right)\leqslant 2^{-\frac{g(n)}{2}}$$

其中，$\boldsymbol{A}\leftarrow\mathbb{Z}_q^{m\times(n+l)}$，$\boldsymbol{e}\leftarrow D$，$\boldsymbol{u}\leftarrow\mathbb{Z}_q^{n+l}$。

定义 1[11]　对于整数 $q=q(n)$，向量 $\boldsymbol{s}\in\mathbb{Z}_q^n$ 及一个 $\mathbb{Z}_q$ 上的误差分布 $\chi=\chi(n)$，选取 $\boldsymbol{a}\leftarrow\mathbb{Z}_q^n$ 及 $x\leftarrow\chi$，输出 $(\boldsymbol{a},<\boldsymbol{a},\boldsymbol{s}>+x)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$，该分布为 $A_{s,\chi}$。$\mathrm{LWE}_{n,m,q,\chi}$ 的判定问题为，以不可忽略的优势区分 m 个来自 $A_{s,\chi}$ 的取样和 m 个 $\mathbb{Z}_q^n\times\mathbb{Z}_q$ 上的均匀随机取样是困难的。

定义 2[18]　对于一个给定在整数上的分布全体 $\{\chi_n\}_{n\in N}$，如果 $\underset{e\leftarrow\chi_n}{Pr}[|e|>B]$ 是可忽略的，则 $\{\chi_n\}_{n\in N}$ 称为 B 界的。

定义 3[16]　拉格朗日插值多项是 $L(x)=\sum_{i=0}^{k-1}y_i l_i(x)$，其中，$l_i(x_i)=\prod_{0\leqslant m\leqslant k-1,m\neq i}\frac{x-x_m}{x_i-x_m}$，$(x_0,y_0)$，$(x_1,y_1),\cdots,(x_n,y_n)$ 为给定的 n+1 对数，其中 $x_i\neq x_j,i\neq j$。

定理 1[16]　在二维平面中，对于给定的 t 个不同的点 $(x_1,y_1),\cdots,(x_t,y_t)$，其中，$x_i\neq x_j,i,j\in[t]$，存在且仅存在一个 $t-1$ 次多项式 $f(x)$，使 $f(x_i)=y_i$，$i\in[t]$。

Nishimak 等[5]指出在一个单跳的单向代理重加密方案中，存在 2 种类型的密文，一种是输入密文，记作 ct，另一种是输出密文，记作 $\widehat{ct}$。代理可以把输入密文转换成输出密文，而不可以把输出密文转换成另外的密文，Nishimak 等[5]构造的方案包括 2 个公钥加密方案和一个重加密方案（将一个方案的输入密文转化为另一个方案的密文）。本文类似于 Nishimak 等[5]构造的代理重加密方案，也研究一种称为 2 种格式的重加密方案，并借鉴了 Singh 等[16]构造的 RTPKE，楼等[17]构造的基于身份的门限多代理者的代理重加密方案。可重新拆分的门限多代理者的代理重加密方案为定义 4。

定义 4　一个单向的可重新拆分的门限多代理者的代理重加密方案(UniRTPRE)由以下 10 个算法组成。

1) 初始化阶段 Setup(1^k)：对给定的安全参数 k，输出公共参数 pp。

2) 加/解密密钥生成算法 Gen(pp)：对于给定的 pp, 输出一对加密/解密密钥 $\left(\left(ek,\widehat{ek}\right),\left(dk,\widehat{dk}\right)\right)$。

3) 输出面的加密算法 $\widehat{\mathrm{Enc}}(pp,\widehat{ek},\mu)$：对于给定的 pp、$\widehat{ek}$ 和明文 μ，输出一个输出面的密文 $\widehat{ct}$。

4) 输出面的解密算法 $\widehat{\mathrm{Dec}}\left(pp,\widehat{dk},\widehat{ct}\right)$：对于给定输出面的 $\widehat{dk}$ 和 $\widehat{ct}$，输出明文 μ 或错误符号 $\perp$。

5) 输入面的加密算法 $\mathrm{Enc}(pp,ek,\mu)$：对于给定的 pp、ek 及明文 μ，输出一个输入面的密文 ct。

6) 输入面的解密算法 $\mathrm{Dec}\left(pp,dk,ct\right)$：对于给定的输入面的 dk 和 ct，输出明文 μ 或错误符号 $\perp$。

7) 门限代理重加密密钥生成算法 Tsplit(pp, $dk_{\mathrm{A}},ek_{\mathrm{A}},\widehat{ek_{\mathrm{B}}},t,u$)：对于给定的 pp、授权者的私钥为 dk_{A}、公钥为 ek_{A}、受理者的公钥为 $\widehat{ek_{\mathrm{B}}}$ 以及门限参数(t, u)，输出代理重加密私钥 $trk_{\mathrm{A}\to\mathrm{B}}=\{trk^1_{\mathrm{A}\to\mathrm{B}},trk^2_{\mathrm{A}\to\mathrm{B}},\cdots,trk^u_{\mathrm{A}\to\mathrm{B}}\}$ 和代理验证钥 $vk_{\mathrm{A}\to\mathrm{B}}=\{vk^1_{\mathrm{A}\to\mathrm{B}},vk^2_{\mathrm{A}\to\mathrm{B}},\cdots,vk^u_{\mathrm{A}\to\mathrm{B}}\}$，其中，$trk^i_{\mathrm{A}\to\mathrm{B}}$、$vk^i_{\mathrm{A}\to\mathrm{B}}$ 分别为第 i 个代理者的代理重加密密钥和代理验证钥，前者是秘密分发给代理者，而后者是公开的。

8) 重加密密文碎片生成算法 $\mathrm{PreEnc}\left(trk^k_{\mathrm{A}\to\mathrm{B}},ct_{\mathrm{A}}\right)$：对于给定的密文 ct_{A} 及第 k 个代理者的代理重加密私钥 $trk^k_{\mathrm{A}\to\mathrm{B}}$，输出重加密密文碎片 $\widehat{pct^k_{\mathrm{A}\to\mathrm{B}}}$。

9) 重加密密文碎片验证算法 VpreEnc(vk, $\widehat{pct^k_{\mathrm{A}\to\mathrm{B}}}$)：对于给定的重加密密文碎片 $\widehat{pct^k_{\mathrm{A}\to\mathrm{B}}}$ 及代理验证钥 vk。如果 $\widehat{pct^k_{\mathrm{A}\to\mathrm{B}}}$ 确实是用 $trk^k_{\mathrm{A}\to\mathrm{B}}$ 转化 ct_{A} 得来的，则输出 1，否则输出 0。

10) 重加密密文碎片合成算法 CReEnc ($\left\{\widehat{pct^k_{\mathrm{A}\to\mathrm{B}}}\right\}_{k=1,\cdots,t}$，$ct_i$)：对于给定的 t 个有效的从 ct_{A} 转化而来的重加密密文碎片 $\widehat{pct^k_{\mathrm{A}\to\mathrm{B}}}$，输出重加密密文 $\widehat{ct_{\mathrm{B}}}$。

Nishimak 等[5]指出，如果在一个代理重加密方案中，敌手在输入面获得了重加密私钥和重加密密文（该密文不包括目标用户到腐败用户的重加密密文），而不能区分真实的密文和随机的密文。在输出面，敌手获得了重加密私钥和重加密密文（该密文无任何限制），也不能区分真实的密文和随机的密文，则称该代理重加密方案是 IND-UniPRE-CPA 安全的。本文定义的安全模型借鉴了 Nishimak 等[5]、Singh 等[16]和楼等[17]的安全模型。形式化的定义见定义 5 和定义 6。

定义 5 (输出面的 IND-UniRTPRE-CPA 安全) 设 UniRTPRE=(Setup, Gen, $\widehat{\text{Enc}}$, Enc, $\widehat{\text{Dec}}$, Dec, Tsplit, PreEnc, VpreEnc, CReEnc) 是一个单向的、单跳的门限多代理者的代理重加密方案，k 为安全参数。假设在输出面存在一个以 pp 为输入，随机密文为输出的 PPT 算法 $\widehat{\text{RandEnc}}$。关于 k 的多项式 $H=H(k)$ 和 $C=C(k)$ 分别记作诚实用户和腐败用户的个数。考虑如下挑战者和敌手之间的游戏，记作 $Expt_{\text{A,UniRTPRE}}^{\text{IND-UniRTPRE-CPA,O}}(k)$。

初始化：对于给定的安全参数 k 和随机数 $b\in\{0,1\}$，挑战者运行 $pp\leftarrow\text{Setup}(1^k)$，得到钥匙对 $\left(\left(ek_i,\widehat{ek_i}\right),\left(dk_i,\widehat{dk_i}\right)\right)\leftarrow\text{Gen}(pp,i)$，$i=0,\cdots,H+C$。敌手获得 pp，诚实用户的公钥 $\left\{\left(ek_i,\widehat{ek_i}\right)\right\}_{i=0,\cdots,H}$，腐败用户的钥匙对 $\left\{\left(\left(ek_i,\widehat{ek_i}\right),\left(dk_i,\widehat{dk_i}\right)\right)\right\}_{i=H+1,\cdots,H+C}$。

学习阶段：敌手能以任意多次访问挑战者 $O_{\text{CHALLENGE}}$。

挑战者 $O_{\text{CHALLENGE}}$：输入 μ，如果 $b=0$，返回 $\widehat{ct}\leftarrow\widehat{\text{RandEnc}}(pp)$；如果 $b=1$，返回 $\widehat{ct}\leftarrow\widehat{\text{Enc}}(pp,\widehat{ek_0},\mu)$。

最后，敌手输出 $b'\in\{0,1\}$，停止访问。

结束：如果 $b'=b$，则输出 1，否则输出 0。

定义敌手的优势为

$$\begin{aligned}&Adv_{\text{A,UniRTPRE}}^{\text{IND-UniRTPRE-CPA,O}}(k)\\&=\left|Pr\left[Expt_{\text{A,UniRTPRE}}^{\text{IND-UniRTPRE-CPA,O}}(k)\to1\middle|b=1\right]-\right.\\&\left.Pr\left[Expt_{\text{A,UniRTPRE}}^{\text{IND-UniRTPRE-CPA,O}}(k)\to1\middle|b=0\right]\right|\end{aligned}$$

如果对于每一个 PPT 的敌手而言，$Adv_{\text{A,UniRTPRE}}^{\text{IND-UniRTPRE-CPA,O}}(\bullet)$ 是可忽略的，则称 UniRTPRE 在输出面是 IND-UniRTPRE-CPA 安全的。

定义 6 (输入面的 IND-UniRTPRE-CPA 安全) 设 UniRTPRE=(Setup, Gen, $\widehat{\text{Enc}}$, Enc, $\widehat{\text{Dec}}$, Dec, Tsplit, PreEnc, VpreEnc, CReEnc) 是一个单向的、单跳的门限多代理者的代理重加密方案，k 为安全参数。假设在输出面存在一个以 pp 为输入，随机密文为输出的 PPT 算法 RandEnc。关于 k 的多项式 $H=H(k)$ 和 $C=C(k)$ 分别记作诚实用户和腐败用户的个数。考虑如下挑战者和敌手之间的游戏，记作 $Expt_{\text{A,UniRTPRE}}^{\text{IND-UniRTPRE-CPA,I}}(k)$。

初始化：对于给定的安全参数 k 和随机数 $b\in\{0,1\}$，挑战者运行 $pp\leftarrow\text{Setup}(1^k)$，获得钥匙对 $\left(\left(ek_i,\widehat{ek_i}\right),\left(dk_i,\widehat{dk_i}\right)\right)\leftarrow\text{Gen}(pp,i)$，$i=0,\cdots,H+C$。敌手获得 pp，诚实用户的公钥 $\left\{\left(ek_i,\widehat{ek_i}\right)\right\}_{i=0,\cdots,H}$，腐败用户的钥匙对 $\left\{\left(\left(ek_i,\widehat{ek_i}\right),\left(dk_i,\widehat{dk_i}\right)\right)\right\}_{i=H+1,\cdots,H+C}$。令 $CU\leftarrow\{H+1,\cdots,H+C\}$。

学习阶段：敌手能以任意顺序访问下列预言机。

重加密私钥碎片预言机 O_{REKEY}：输入 2 个用户 $i,j\in[0,H+C]$。如果 $i=j$ 或 $(i=0)\cap(j\in CU)$ 则返回 $\perp$；否则，返回 $t-1$ 个不同的代理重加密私钥碎片 $trk_{i\to j}^k$，$k\in[u]$ 和代理验证钥 $vk_{i\to j}=\{vk_{i\to j}^1,vk_{i\to j}^2,\cdots,vk_{i\to j}^u\}$。

重加密密文碎片预言机 O_{REENC}：输入 2 个用户 $i,j\in[0,H+C]$ 及密文 ct_i。如果 $i=j$ 或 $(i=0)\cap(j\in CU)$，则返回 $\perp$；否则，用 (i,j) 访问 O_{REKEY} 得到 $t-1$ 个不同的代理重加密私钥碎片 $trk_{i\to j}^k$，$k\in[u]$，返回相应的重加密密文碎片 $\widehat{pct_{i\to j}^k}$，$k\in[u]$。

挑战者 $O_{\text{CHALLENGE}}$：输入 μ，如果 $b=0$，返回 $ct\leftarrow\text{RandEnc}(pp)$；如果 $b=1$，返回 $ct\leftarrow\text{Enc}(pp,ek_0,\mu)$。

最后，敌手输出 $b'\in\{0,1\}$ 停止访问。

结束：如果 $b'=b$，则输出 1，否则输出 0。

定义敌手的优势为

$$\begin{aligned}&Adv_{\text{A,UniRTPRE}}^{\text{IND-UniRTPRE-CPA,I}}(k)\\&=\left|Pr\left[Expt_{\text{A,UniRTPRE}}^{\text{IND-UniRTPRE-CPA,I}}(k)\to1\middle|b=1\right]-\right.\\&\left.Pr\left[Expt_{\text{A,UniRTPRE}}^{\text{IND-UniRTPRE-CPA,I}}(k)\to1\middle|b=0\right]\right|\end{aligned}$$

如果对于每一个 PPT 的敌手而言，$Adv_{\text{A,UniRTPRE}}^{\text{IND-UniRTPRE-CPA,I}}(\bullet)$ 是可忽略的，则称 UniRTPRE 在输入面是 IND-UniRTPRE-CPA 安全的。

3 单向单跳的可重新拆分的代理重加密方案

为了叙述简洁，本文只考虑明文是一个比特的情况。本节将 Nishimak 等[5]构造的 2 个代理重加密方案，Singh 等[16]构造的门限加密方案，楼圣铭等[17]的基于身份的门限多代理者的代理重加密方案相结合得到了单向门限多代理者的代理重加密方案。

1) Setup(1^k)

① $m\geqslant(n+1)\eta+\omega(\text{lb}k)$，$\boldsymbol{A}\leftarrow\mathbb{Z}_q^{m\times n}$，素数 p

使离散对数问题在循环群 $Z_p=\langle g\rangle$ 中是困难的。

② 输出 $pp=\left(1^k,1^n,1^m,p,q,\chi,\boldsymbol{A}\right)$。

2) $\mathrm{Gen}(pp)$

① $\boldsymbol{b}\leftarrow\boldsymbol{A}\boldsymbol{s}+\boldsymbol{x}$，$\boldsymbol{c}\leftarrow\boldsymbol{A}\boldsymbol{t}+\boldsymbol{y}$，其中，$\boldsymbol{s}\leftarrow\chi^n$，$\boldsymbol{x}\leftarrow\chi^m$，$\boldsymbol{t}\leftarrow\chi^n,\boldsymbol{y}\leftarrow\chi^m$。

②输出 $\left(\left(ek,\widehat{ek}\right),\left(dk,\widehat{dk}\right)\right)=\left((\boldsymbol{b},\boldsymbol{c}),(\boldsymbol{s},\boldsymbol{t})\right)$。

3) $\widehat{\mathrm{Enc}}(pp,\widehat{ek}=\boldsymbol{c},\mu\in\{0,1\})$

① $\left(\boldsymbol{u}^{\mathrm{T}},\boldsymbol{c}\right)\leftarrow\left(\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{A}+\boldsymbol{e}_2,\langle\boldsymbol{e}_1,\boldsymbol{c}\rangle+e_3+\left\lfloor\frac{q}{2}\right\rfloor\mu\right)$，其中 $\boldsymbol{e}_1\leftarrow\chi^m,\boldsymbol{e}_2\leftarrow\chi^n,e_3\leftarrow\chi$

② 输出 $\widehat{ct}=\left(\boldsymbol{u}^{\mathrm{T}},c\right)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$。

4) $\widehat{\mathrm{Dec}}\left(pp,\widehat{dk}=\boldsymbol{t},\widehat{ct}=\left(\boldsymbol{u}^{\mathrm{T}},c\right)\right)$

① $d\leftarrow c-\left\langle\boldsymbol{u}^{\mathrm{T}},\boldsymbol{t}\right\rangle$。

② $\mu\leftarrow\lfloor\frac{2}{q}d\rceil\bmod 2$。

③输出 μ。

5) $\mathrm{Enc}(pp,ek=\boldsymbol{b},\mu\in\{0,1\})$

① $\left(\boldsymbol{u}^{\mathrm{T}},c\right)\leftarrow\left(\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{A}+\boldsymbol{e}_2,\langle\boldsymbol{e}_1,\boldsymbol{b}\rangle+e_3+\left\lfloor\frac{q}{2}\right\rfloor\mu\right)$，其中，$\boldsymbol{e}_1\leftarrow\chi^m,\boldsymbol{e}_2\leftarrow\chi^n,e_3\leftarrow\chi$。

②输出 $ct=\left(\boldsymbol{u}^{\mathrm{T}},c\right)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$。

6) $Dec\left(pp,dk=\boldsymbol{s},ct=\left(\boldsymbol{u}^{\mathrm{T}},c\right)\right)$

① $d\leftarrow c-\left\langle\boldsymbol{u}^{\mathrm{T}},\boldsymbol{s}\right\rangle$。

② $\mu\leftarrow\lfloor\frac{2}{q}d\rceil\bmod 2$。

③输出 μ。

7) $\mathrm{Tsplit}\left(pp,dk=\boldsymbol{s}_{\mathrm{A}},ek=\boldsymbol{b}_{\mathrm{A}},\widehat{ek}=\boldsymbol{c}_{\mathrm{B}},t,n\right)$

①设 $\boldsymbol{M}_{\mathrm{A}\to\mathrm{B}}=(m_{i,j})\in\mathbb{Z}_q^{(n\eta+1)(n+1)}$

$$=\left(\boldsymbol{R}_{\mathrm{A}\to\mathrm{B}}\left[\boldsymbol{A}\,|\,\boldsymbol{c}_{\mathrm{B}}\right]+P_2\left[\boldsymbol{0}_n\,|\,-\boldsymbol{s}_{\mathrm{A}}\right];\left[\boldsymbol{0}\,|\,1\right]\right)$$

$$=\begin{pmatrix}\boldsymbol{R}_{\mathrm{A}\to\mathrm{B}}\boldsymbol{A} & \boldsymbol{R}_{\mathrm{A}\to\mathrm{B}}\boldsymbol{c}_{\mathrm{B}}-P_2\left(\boldsymbol{s}_{\mathrm{A}}\right)\\ \boldsymbol{0}_{1\times n} & 1\end{pmatrix}$$

其中，$\boldsymbol{R}_{\mathrm{A}\to\mathrm{B}}\leftarrow\{0,1\}^{n\eta\times m}$。随机生成 $n\eta(n+1)+1$ 个 $t-1$ 多项式，$f_{i,j}\leftarrow Z_q[x]$ 且 $f_{i,j}(0)=m_{i,j}$，$i\in[n\eta]$，$j\in[n+1]$，$(i,j)=(n\eta+1,n+1)$。假设共有 u 个代理，对任意的 $i\in[u]$，第 i 个代理的陷门私钥为

$$tsk_{\mathrm{A}\to\mathrm{B}}^i=\begin{pmatrix}f_{1,1} & \cdots & f_{1,n} & f_{1,n+1}\\ \vdots & & \vdots & \vdots\\ f_{n\eta,1} & \cdots & f_{n\eta,n} & f_{n\eta,n+1}\\ 0 & \cdots & 0 & f_{n\eta+1,n+1}\end{pmatrix}$$

相对应的代理验证钥为

$$vk_{\mathrm{A}\to\mathrm{B}}^i=\begin{pmatrix}g^{f_{1,1}} & \cdots & g^{f_{1,n}} & g^{f_{1,n+1}}\\ \vdots & & \vdots & \vdots\\ g^{f_{n\eta,1}} & \cdots & g^{f_{n\eta,n}} & g^{f_{n\eta,n+1}}\\ 0 & \cdots & 0 & g^{f_{n\eta+1,n+1}}\end{pmatrix}$$

②在 u 个代理中任取 t 个代理作为一个小组，有 $\binom{u}{t}$ 种可能。对于任意的 $\alpha=1,\cdots,\binom{u}{t}$，任取随机数 k_α，并把 k_α 发送给不在第 α 个小组的 $u-t$ 个代理，即每个代理都将收到 $\binom{u-1}{t}$ 个随机数。

③输出第 i 个代理的重加密密钥碎片 $trk_{\mathrm{A}\to\mathrm{B}}^i=\left(tsk_{\mathrm{A}\to\mathrm{B}}^i,\binom{u-1}{t}\text{个随机数}\right)$ 及代理验证钥 $vk_{\mathrm{A}\to\mathrm{B}}=\left(vk_{\mathrm{A}\to\mathrm{B}}^1,\cdots,vk_{\mathrm{A}\to\mathrm{B}}^u\right)$。

8) $\mathrm{PreEnc}\left(trk_{\mathrm{A}\to\mathrm{B}}^i,ct_{\mathrm{A}}=\left(\boldsymbol{u}^{\mathrm{T}},c\right)\right)$

① $sd_i\leftarrow\left(BD\left(\boldsymbol{u}^T\right),c\right)tsk_i$。

②假设存在一个以密文 ct_{A} 及 k_α 为输入的伪随机函数 ϕ，其输出 $\phi_{k_\alpha}\left(ct_{\mathrm{A}}\right)$ 在某个已知区间内。第 i 个代理对属于自己的所有 k_α 所对应的伪随机函数值求和，即 $x_i=\sum\phi_{k_\alpha}\left(ct_{\mathrm{A}}\right)$。

③ $pe_i=\left(BD\left(\boldsymbol{u}^{\mathrm{T}}\right),c\right)tsk_i+\left(\boldsymbol{0}_{1\times n},x_i\right)$。

④输出重加密密文碎片 $\widehat{pct_{\mathrm{A}\to\mathrm{B}}^i}=\left(pe_i,g^{x_i}\right)$。

9) $\mathrm{VpreEnc}(vk,\ \widehat{pct_{\mathrm{A}\to\mathrm{B}}^i})$

设 $\left(BD\left(\boldsymbol{u}^{\mathrm{T}}\right),c\right)=\left(u_1,\cdots u_{n\eta},c\right)$，其中，$u_i\in\{0,1\}$。对 $i\in[u]$，如果

$$g^{pe_i}=\left(\prod_{j=1}^{n\eta}\left(g^{f_{j,1}}\right)^{u_j},\cdots,\prod_{j=1}^{n\eta}\left(g^{f_{j,n}}\right)^{u_j},\prod_{j=1}^{n\eta}\left(g^{f_{j,n+1}}\right)^{u_j}\left(g^{f_{n\eta+1,n+1}}\right)^{c}g^{x_i}\right)$$

则输出 1，否则输出 0。

10) $\mathrm{CReEnc}\left(\left\{\widehat{pct_{\mathrm{A}\to\mathrm{B}}^i}\right\}_{i=1,\cdots,t},\ ct_{\mathrm{A}}\right)$

①如果 $\mathrm{VpreEnc}(vk,\widehat{pct_{A\to B}^i})=0$，则退出。否则进行步骤②。

②不失一般性，不妨设分别从标号为 $1,\cdots,t$ 的

代理接收到 t 个有效的重加密密文碎片。以代理的标号作为 x 的值，pe_i 的第 i 个分量作为 y 的值，应用拉格朗日插值，则得到拉格朗日多项式 $f_i(x)$ 及 $f_i(0), i\in[n+1]$。

③输出重加密密文 $\widehat{ct_{\mathrm{B}}}=\left(f_1(0),\cdots,f_{n+1}(0)\right)$。

下面，本文证明方案的正确性。为了叙述简洁，不妨假设 χ 为 δ 界分布。

命题 1 如果 $\delta+(m+n)\delta^2<\frac{q}{4}$，则方案在输入面解密正确。

证明 设 $\boldsymbol{b}\leftarrow\boldsymbol{A}\boldsymbol{s}+\boldsymbol{x}$，其中，$\boldsymbol{A}\leftarrow\mathbb{Z}_q^{m\times n}$，$\boldsymbol{s}\leftarrow\chi^n,\boldsymbol{x}\leftarrow\chi^m$。明文 μ 所对应的密文为 $\left(\boldsymbol{u}^{\mathrm{T}},c\right)\leftarrow\left(\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{A}+\boldsymbol{e}_2,\langle\boldsymbol{e}_1,\boldsymbol{b}\rangle+e_3+\left\lfloor\frac{q}{2}\right\rfloor\mu\right)$，其中，$\boldsymbol{e}_1\leftarrow\chi^m$，$\boldsymbol{e}_2\leftarrow\chi^n,e_3\leftarrow\chi$。用私钥 $\boldsymbol{s}$ 对密文 $\left(\boldsymbol{u}^{\mathrm{T}},c\right)$ 解密，有

$$\begin{aligned}d&=c-\left\langle\boldsymbol{u}^{\mathrm{T}},\boldsymbol{s}\right\rangle\\&=\langle\boldsymbol{e}_1,\boldsymbol{b}\rangle+e_3+\left\lfloor\frac{q}{2}\right\rfloor\mu-\left\langle\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{A}+\boldsymbol{e}_2,\boldsymbol{s}\right\rangle\\&=\left\lfloor\frac{q}{2}\right\rfloor\mu+e_3+\langle\boldsymbol{e}_1,\boldsymbol{x}\rangle-\langle\boldsymbol{e}_2,\boldsymbol{s}\rangle\end{aligned}$$

如果 $\left\|e_3+\langle\boldsymbol{e}_1,\boldsymbol{x}\rangle-\langle\boldsymbol{e}_2,\boldsymbol{s}\rangle\right\|_\infty<\frac{q}{4}$，则 $\mu=\lfloor\frac{2}{q}d\rceil\bmod 2$。事实上

$$\begin{aligned}&\left\|e_3+\langle\boldsymbol{e}_1,\boldsymbol{x}\rangle-\langle\boldsymbol{e}_2,\boldsymbol{s}\rangle\right\|_\infty\\&\leqslant\|e_3\|_\infty+\left\|\langle\boldsymbol{e}_1,\boldsymbol{x}\rangle\right\|_\infty+\left\|\langle\boldsymbol{e}_2,\boldsymbol{s}\rangle\right\|_\infty\\&\leqslant\delta+m\delta^2+n\delta^2\\&=\delta+(m+n)\delta^2\end{aligned}$$

因此由假设 $\delta+(m+n)\delta^2<\frac{q}{4}$，可知解密正确。

命题 2 如果 $\delta+(m+n)\delta^2<\frac{q}{4}$，则方案在输出面解密正确。

证明 证明类似于命题 1。

命题 3 如果 $m\delta^2+\delta+n\delta^2+\|h(0)\|_\infty+mn\eta\delta<\frac{q}{4}$，其中，$h(0)$ 为已知范围的数，则方案对重加密密文解密正确。

证明 假设第 i 个代理的有效重加密密文碎片为 $\widehat{pct_{\mathrm{A}\to\mathrm{B}}^i}=\left(pe_i,g^{x_i}\right)$，其中，$pe_i=\left(\delta D\left(\boldsymbol{u}^{\mathrm{T}}\right),c\right)tsk_i+\left(\boldsymbol{0}_{1\times n},x_i\right)$，$ct_A=\left(\boldsymbol{u}^{\mathrm{T}},c\right)\leftarrow\left(\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{A}+\boldsymbol{e}_2,\langle\boldsymbol{e}_1,\boldsymbol{b}\rangle+e_3+\left\lfloor\frac{q}{2}\right\rfloor\mu\right)$，$\boldsymbol{b}\leftarrow\boldsymbol{A}\boldsymbol{s}_{\mathrm{A}}+\boldsymbol{x}$，$\boldsymbol{s}_{\mathrm{A}}\leftarrow\chi^n,\boldsymbol{x}\leftarrow\chi^m$，$\boldsymbol{e}_1\leftarrow\chi^m$，$\boldsymbol{e}_2\leftarrow\chi^n$，$e_3\leftarrow\chi$，$x_i=\sum\phi_{k_\alpha}(ct)$，$tsk_i=\begin{pmatrix}f_{1,1}&\cdots&f_{1,n}&f_{1,n+1}\\\vdots&&\vdots&\vdots\\f_{n\eta,1}&\cdots&f_{n\eta,n}&f_{n\eta,n+1}\\0&\cdots&0&f_{n\eta+1,n+1}\end{pmatrix}$，$\boldsymbol{M}_{\mathrm{A}\to\mathrm{B}}=(m_{i,j})\in\mathbb{Z}_q^{(n\eta+1)(n+1)}=(\boldsymbol{R}_{\mathrm{A}\to\mathrm{B}}[\boldsymbol{A}|\boldsymbol{c}_{\mathrm{B}}]+P_2[\boldsymbol{0}_{n\times1}|-\boldsymbol{s}_{\mathrm{A}}];[\boldsymbol{0}_{n\times1}|1])$，$\boldsymbol{c}_{\mathrm{B}}\leftarrow\boldsymbol{A}\boldsymbol{t}_{\mathrm{B}}+\boldsymbol{y}$，$\boldsymbol{t}_{\mathrm{B}}\leftarrow\chi^n,\boldsymbol{y}\leftarrow\chi^m$，$\boldsymbol{R}_{\mathrm{A}\to\mathrm{B}}\leftarrow\{0,1\}^{n\eta\times m}$。不妨设分别从代理标号为 $1,\cdots,t$ 接收到 t 个有效的重加密密文碎片。以代理的标号作为 x 的值，pe_i 的第 i 个分量作为 y 的值，应用拉格朗日插值，得到拉格朗日多项式 $f_i(x)$，且当 $i\in[n]$ 时，有

$$\begin{aligned}f_i(0)&=\left(\delta D\left(\boldsymbol{u}^{\mathrm{T}}\right),c\right)\begin{pmatrix}f_{1,i}(0)\\\vdots\\f_{n\eta,i}(0)\\0\end{pmatrix}\\&=\left(\delta D\left(\boldsymbol{u}^{\mathrm{T}}\right),c\right)\begin{pmatrix}m_{1,i}\\\vdots\\m_{n\eta,i}\\0\end{pmatrix}\end{aligned}$$

当 $i=n+1$ 时，有

$$\begin{aligned}f_{n+1}(0)&=\left(\delta D\left(\boldsymbol{u}^{\mathrm{T}}\right),c\right)\begin{pmatrix}f_{1,n+1}(0)\\\vdots\\f_{n\eta,n+1}(0)\\f_{n\eta+1,n+1}(0)\end{pmatrix}+x_i\\&=\left(\delta D\left(\boldsymbol{u}^{\mathrm{T}}\right),c\right)\begin{pmatrix}m_{1,n+1}\\\vdots\\m_{n\eta,n+1}\\m_{n\eta+1,n+1}\end{pmatrix}+h(0)\end{aligned}$$

其中，$h(0)$ 是以代理的标号作为 x 的值，x_i 作为 y 的值，应用拉格朗日插值得到另外一个拉格朗日函数 $h(x)$ 在 $x=0$ 的值，且 $h(0)\leqslant\sum_{i=1}^{t}x_i$。需要注意的是，因为 $\phi_{k_\alpha}(ct_{\mathrm{A}})$ 在某个已知区间内，所以本文可以通过限制 x_i，得到 $h(0)$ 的界，可以把 $h(0)$ 看作一个已知范围的数。因此，重加密密文

$$\begin{aligned}\widehat{ct_\delta}&=\left(f_1(0),\cdots,f_{n+1}(0)\right)\\&=\left(\delta D\left(\boldsymbol{u}^{\mathrm{T}}\right),c\right)\begin{pmatrix}\boldsymbol{R}_{\mathrm{A}\to\mathrm{B}}\boldsymbol{A}&\boldsymbol{R}_{\mathrm{A}\to\mathrm{B}}\boldsymbol{c}_{\mathrm{B}}-P_2\left(\boldsymbol{s}_{\mathrm{A}}\right)\\\boldsymbol{0}_{1\times n}&1\end{pmatrix}+\\&\quad(\boldsymbol{0}_{1\times n},h(0))\end{aligned}$$

$$=\left(\delta D\left(\boldsymbol{u}^{\mathrm{T}}\right)\boldsymbol{R}_{\mathrm{A}\to\mathrm{B}}\boldsymbol{A},\delta D\left(\boldsymbol{u}^{\mathrm{T}}\right)\boldsymbol{R}_{\mathrm{A}\to\mathrm{B}}\boldsymbol{c}_{\mathrm{B}}-\right.$$
$$\left.\delta D\left(\boldsymbol{u}^{\mathrm{T}}\right)P_2\left(\boldsymbol{s}_{\mathrm{A}}\right)+c+h(0)\right)$$

用私钥 $\boldsymbol{t}_{\mathrm{B}}$ 对重加密密文 $\widehat{ct_{\mathrm{B}}}$ 解密，有

$$d=\delta D\left(\boldsymbol{u}^{\mathrm{T}}\right)\boldsymbol{R}_{\mathrm{A}\to\mathrm{B}}\boldsymbol{c}_{\mathrm{B}}-\delta D\left(\boldsymbol{u}^{\mathrm{T}}\right)P_2\left(\boldsymbol{s}_{\mathrm{A}}\right)+$$
$$c+h(0)-\left\langle\delta D\left(\boldsymbol{u}^{\mathrm{T}}\right)\boldsymbol{R}_{\mathrm{A}\to\mathrm{B}}\boldsymbol{A},\boldsymbol{t}_{\mathrm{B}}\right\rangle$$
$$=c-\boldsymbol{u}^{\mathrm{T}}\boldsymbol{s}_{\mathrm{A}}+h(0)+\delta D\left(\boldsymbol{u}^{\mathrm{T}}\right)\boldsymbol{R}_{\mathrm{A}\to\mathrm{B}}\boldsymbol{y}$$
$$=\left\langle\boldsymbol{e}_1,\boldsymbol{b}\right\rangle+e_3+\left\lfloor\frac{q}{2}\right\rfloor\mu-\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{A}\boldsymbol{s}_{\mathrm{A}}+\boldsymbol{e}_2^{\mathrm{T}}\boldsymbol{s}_{\mathrm{A}}+$$
$$h(0)+\delta D\left(\boldsymbol{u}^{\mathrm{T}}\right)\boldsymbol{R}_{\mathrm{A}\to\mathrm{B}}\boldsymbol{y}$$
$$=\left\lfloor\frac{q}{2}\right\rfloor\mu+\boldsymbol{e}_1\boldsymbol{x}+e_3+\boldsymbol{e}_2^{\mathrm{T}}\boldsymbol{s}_{\mathrm{A}}+h(0)+$$
$$\delta D\left(\boldsymbol{u}^{\mathrm{T}}\right)\boldsymbol{R}_{\mathrm{A}\to\mathrm{B}}\boldsymbol{y}$$

如果 $\left\|\boldsymbol{e}_1\boldsymbol{x}+\boldsymbol{e}_3+\boldsymbol{e}_2^{\mathrm{T}}\boldsymbol{s}_{\mathrm{A}}+h(0)+\delta D\left(\boldsymbol{u}^{\mathrm{T}}\right)\boldsymbol{R}_{\mathrm{A}\to\mathrm{B}}\boldsymbol{y}\right\|_\infty<\frac{q}{4}$，则 $\mu=\left\lfloor\frac{2}{q}d\right\rceil\bmod 2$。事实上

$$\left\|\boldsymbol{e}_1\boldsymbol{x}+e_3+\boldsymbol{e}_2^{\mathrm{T}}\boldsymbol{s}_{\mathrm{A}}+h(0)+\delta D\left(\boldsymbol{u}^{\mathrm{T}}\right)\boldsymbol{R}_{\mathrm{A}\to\mathrm{B}}\boldsymbol{y}\right\|_\infty$$
$$\leqslant\left\|\boldsymbol{e}_1\boldsymbol{x}\right\|_\infty+\left\|e_3\right\|_\infty+\left\|\boldsymbol{e}_2^{\mathrm{T}}\boldsymbol{s}_{\mathrm{A}}\right\|_\infty+$$
$$\left\|h(0)\right\|_\infty+\left\|\delta D\left(\boldsymbol{u}^{\mathrm{T}}\right)\boldsymbol{R}_{\mathrm{A}\to\mathrm{B}}\boldsymbol{y}\right\|_\infty$$
$$\leqslant m\delta^2+\delta+n\delta^2+\left|h(0)\right|+mn\eta\delta$$

因此，由假设 $m\delta^2+\delta+n\delta^2+\left|h(0)\right|+mn\eta\delta<\frac{q}{4}$，可知解密正确。

定理 2　如果 $m\delta^2+\delta+n\delta^2+\left\|h(0)\right\|_\infty+mn\eta\delta<\frac{q}{4}$，其中，$h(0)$ 为已知范围的数，则方案解密正确。

证明　由命题 1~3 可知结论正确。

注：本文方案的加密算法与重加密算法是不同的。如果重加密算法也采用与加密算法相同的算法，则在重加密的过程中噪音的增长会变得更大。这是因为加密算法的安全性是基于 LWE 困难问题的，在解密的时候噪音的级别为 δ^2。而重加密算法的安全性利用了 leftover hash 引理，在解密的时候噪音的级别也是 δ^2。如果在重加密算法的时候也采用与加密算法相同的算法，即基于 LWE 安全性，则解密后噪音的级别为 δ^3。因此，本文方案在参数的选取上有更宽的选择范围。

4　安全性

本节讨论构造的门限多代理者的代理重加密方的安全性。即证明方案在输出面、输入面是 IND-UniRTPRE-CPA 安全的。

命题 4　在 $\mathrm{LWE}_{n,q,\chi}$ 困难假设下，上述门限多代理者的代理重加密方案在输出面是 IND- UniRTPRE-CPA 安全的。

证明　考虑如下游戏，其中，$b\in\{0,1\}$。

RealPK_b：这个游戏与 $Expt_{\mathrm{A,UniPRE}}^{\mathrm{Ind\text{-}UniPRE\text{-}CPA,O}}(k)$ 相同。假设目标公钥是 $\left(ek_0,\widehat{ek_0}\right)=\left(\boldsymbol{b}_0,\boldsymbol{c}_0\right)$，其中，$\boldsymbol{b}_0=\boldsymbol{A}\boldsymbol{s}_0+\boldsymbol{x}_0$，$\boldsymbol{c}_0=\boldsymbol{A}\boldsymbol{t}_0+\boldsymbol{y}_0,\boldsymbol{s}_0,\boldsymbol{t}_0\leftarrow\chi^n,\boldsymbol{x}_0,\boldsymbol{y}_0\leftarrow\chi^m$。挑战者回答敌手对 $\mu\in\{0,1\}$ 的密文询问如下。

1) 如果 $b=0$，返回 $\widehat{ct}\leftarrow\mathbb{Z}_q^{n+1}$。

2) 如果 $b=1$，返回 $\widehat{ct}\leftarrow(\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{A}+\boldsymbol{e}_2,\left\langle\boldsymbol{e}_1,\boldsymbol{c}_0\right\rangle+e_3+\left\lfloor\frac{q}{2}\right\rfloor\mu)$，其中，$\boldsymbol{e}_1\leftarrow\chi^m,\boldsymbol{e}_2\leftarrow\chi^n,e_3\leftarrow\chi$。

敌手输出 $b'\in\{0,1\}$ 后停止询问。

FakePK_b：修改目标用户的公钥，用 $\boldsymbol{c}_0^+\leftarrow\mathbb{Z}_q^m$ 来代替 $\boldsymbol{c}_0$，挑战者利用 $\boldsymbol{c}_0^+$，如同 RealPK_b 计算目标密文，其余与 RealPK_b 相同。

因为在这 2 个游戏中，挑战者不需要私钥 $\boldsymbol{t}_0$，所以在 $\mathrm{LWE}_{n,q,\chi}$ 假设下，有 $\boldsymbol{c}_0\approx_c\boldsymbol{c}_0^+$。进而 $\mathrm{RealPK}_b\approx_c\mathrm{FakePK}_b$。再由 leftover hash 引理可知 $\mathrm{FakePK}_0\approx_s\mathrm{FakePK}_1$。综上，在 $\mathrm{LWE}_{n,q,\chi}$ 假设下，$\mathrm{RealPK}_0\approx_c\mathrm{RealPK}_1$。

命题 5　在 $\mathrm{LWE}_{n,q,\chi}$ 困难假设下，上述门限多代理者的代理重加密方案在输入面是 IND-UniRTPRE-CPA 安全的。

证明　考虑如下游戏，其中，$b\in\{0,1\}$。

Game_0^b：这个游戏与 $Expt_{\mathrm{A,UniPRE}}^{\mathrm{IND\text{-}UniPRE\text{-}CPA,I}}(k)$ 相同。假设目标公钥是 $\left(ek_0,\widehat{ek_0}\right)=\left(\boldsymbol{b}_0,\boldsymbol{c}_0\right)$，其中，$\boldsymbol{b}_0=\boldsymbol{A}\boldsymbol{s}_0+\boldsymbol{x}_0,\boldsymbol{c}_0=\boldsymbol{A}\boldsymbol{t}_0+\boldsymbol{y}_0,\boldsymbol{s}_0,\boldsymbol{t}_0\leftarrow\chi^n$，$\boldsymbol{x}_0,\boldsymbol{y}_0\leftarrow\chi^m$。诚实用户的公钥为 $\left\{\left(ek_i,\widehat{ek_i}\right)\right\}_{i=1,\cdots,H}=\left\{\left(\boldsymbol{b}_i,\boldsymbol{c}_i\right)\right\}_{i=1,\cdots,H}$，$\boldsymbol{b}_i=\boldsymbol{A}\boldsymbol{s}_i+\boldsymbol{x}_i$，$\boldsymbol{c}_i=\boldsymbol{A}\boldsymbol{t}_i+\boldsymbol{y}_i$。挑战者计算从用户 0 到用户 $i\in[H]$ 的 $t-1$ 个不同的代理重加密私钥碎片 $trk_{0\to i}^k$，$k\in[u]$，及相应的 $t-1$ 个重加密密文碎片 $\widehat{pct_{i\to j}^k}$，$k\in[u]$。挑战者回答敌手对 $\mu\in\{0,1\}$ 的密文询问如下。

1) 如果 $b=0$，返回 $ct\leftarrow\mathbb{Z}_q^{n+1}$。

2) 如果 $b=1$，返回 $ct\leftarrow(\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{A}+\boldsymbol{e}_2,\left\langle\boldsymbol{e}_1,\boldsymbol{b}_0\right\rangle+$

$e_3+\left\lfloor\frac{q}{2}\right\rfloor\mu)$，其中，$\boldsymbol{e}_1\leftarrow\chi^m,\boldsymbol{e}_2\leftarrow\chi^n,e_3\leftarrow\chi$。

敌手输出 $b'\in\{0,1\}$ 后停止询问。

Game_1^b：挑战者分别用一组随机数来代替 $t-1$ 个不同的代理重加密私钥碎片 $trk_{0\to i}^k$，$k\in[u]$，并用这组随机数如同 Game_0^b 计算相应的重加密密文碎片 $\widehat{pct_{i\to j}^k}$。其余与 Game_0^b 相同。

因为 $trk_{0\to i}^k$ 是随机的，再由 leftover hash 引理可知 $\text{Game}_0^b\approx_c\text{Game}_1^b$。

Game_2^b：用 $\boldsymbol{b}_0^+\leftarrow\mathbb{Z}_q^m$ 代替 $\boldsymbol{b}_0$，其余与 Game_1^b 相同。

因为挑战者不需要私钥 $\boldsymbol{s}_0$，所以在 $\text{LWE}_{n,q,\chi}$ 假设下，有 $\boldsymbol{b}_0\approx_c\boldsymbol{b}_0^+$。在 $\text{LWE}_{n,q,\chi}$ 假设下，$\text{Game}_1^b\approx_c\text{Game}_2^b$。

最后，因为在 $\text{LWE}_{n,q,\chi}$ 假设下，可知 $\text{Game}_2^0\approx_c\text{Game}_2^1$。综上，可知 $\text{Game}_0^0\approx_c\text{Game}_0^1$。

定理 3 在 $\text{LWE}_{n,q,\chi}$ 困难假设下，上述门限多代理者的代理重加密方案在输入/出面是 IND- UniRTPRE-CPA 安全的。

证明 由命题 4 和命题 5 可知结论正确。

5 结束语

代理重加密在云数据的共享中有着重要的作用。门限多代理者的代理重加密方案在个别代理不诚实或是瘫痪不能提供服务时，保证了云数据共享的安全性和正确性。本文在格上将代理重加密与可重新拆分的门限密码结合，构造一个可重新拆分的门限多代理者的代理重加密方案，并证明该方案在 LWE 假设下是 IND-UniRTPRE-CPA 安全的。

参考文献：

[1] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography[C]//Advances in Cryptology — EUROCRYPT. 1998: 127-144.

[2] XAGAWA K. Cryptography with lattices[D]. Tokyo: Tokyo Institute of Technology, 2010.

[3] AONO Y, BOYEN X, PHONG T L, et al. Key-private proxy re-encryption under LWE[C]//Progress in Cryptology -INDOCRYPT. 2013:1-18.

[4] SINGH K, PANDU R C, BANERJEE A K. Cryptanalysis of unidirectional proxy re-encryption scheme[C]//Information and Communication Technology. 2014:564-575.

[5] NISHIMAK R, XAGAWA K. Key-private proxy re-encryption from lattices, revisited[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2015, E98-A(1): 100-116.

[6] JIANG M M, HU Y P, WANG B C, et al. Lattice-based multi-use unidirectional proxy re-encryption[J]. Security and Communication Networks, 2015, 8(18): 3796-3803.

[7] KIRSHANOVA E. Proxy re-encryption from lattices[C]//Public-Key Cryptography – PKC. 2014: 77-94.

[8] 周潭平, 杨海滨, 杨晓元, 等. 一个全同态代理加密方案[J]. 四川大学学报(工程科学版), 2016,48(1):99-105.
ZHOU T P, YANG H B, YANG X Y, et al. A fully homomorphic proxy re-encryption scheme based on LWE[J]. Journal of Sichuan University (Engineering Science Edition), 2016,48(1): 99-105.

[9] SINGH K C, RANGAN P, BANERJEE A K. Lattice based identity based unidirectional proxy re-encryption scheme[C]//Security, Privacy, and Applied Cryptography Engineering. 2014: 76-91.

[10] 苏铓, 历国振, 谢荣娜, 等. 面向移动云计算的多要素代理重加密方案[J]. 通信学报, 2015, 36(11): 73-79.
SU M, LI G Z, XIE R N, et al. Multi-element based on proxy re-encryption scheme for mobile cloud computing[J]. Journal on Communications, 2015，36(11):73-79.

[11] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[C]//The 37th annual ACM Symposium on Theory of Computing. 2005: 84- 93.

[12] LINDNER R, PEIKERT C. Better key sizes (and attacks) for LWE-based encryption[C]//Topics in Cryptology–CT-RSA. 2011: 319-339.

[13] GENTRY C, HALEVI S, VAIKUNTANATHAN V. A simple BGN-type cryptosystem from LWE[C]//Advances in Cryptology–Eurocrypt. 2010:506-522.

[14] DESMEDT Y, YAIR F Y. Threshold cryptosystems[C]//Proceedings of Advances in Cryptology-CRYPTO. 1989: 307-315.

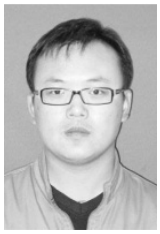
[15] HANAOKA G, KAWAI Y, KUNIHIRO N, et al. Generic construction of chosen ciphertext secure proxy re-encryption[C]//Cryptographers' Track at the RSA Conference. 2012: 349-364.

[16] SINGH K C, RANGAN P, BANERJEE A K. Lattice-based identity-based resplittable threshold public key encryption scheme[J]. International Journal of Computer Mathematics, 2016, 93(2): 289-307.

[17] 楼圣铭, 曹珍富. 基于身份的门限多代理者的代理重加密方案[J]. 黑龙江大学自然科学学报, 2010, 27(2): 151-156.
LOU S M, CAO Z F. Identity-based proxy re-encryption with threshold multi-proxy[J]. Journal of Natural Science of Heilongjiang University, 2010, 27(2): 151-156.

[18] GENTRY C, SAHAIY A, WATERS B. Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, Attribute-based[C]//Advances in Cryptology-Crypto. 2013:75-92.

作者简介：



李菊雁（1983-），男，黑龙江虎林人，哈尔滨工程大学博士生，主要研究方向为密码学、网络与信息安全。

马春光（1974-），男，黑龙江双鸭山人，哈尔滨工程大学教授、博士生导师，主要研究方向为密码学、网络与信息安全。

赵乾（1993-），女，黑龙江双鸭山人，哈尔滨工程大学硕士生，主要研究方向为密码学、网络与信息安全。