基于理想格的鲁棒门限代理重加密方案

吴立强,韩益亮,杨晓元,张敏情,杨 凯
(武警工程大学武警部队网络与信息安全保密重点实验室,陕西西安 710086)

摘 要: 代理重加密能够实现解密权限的转换,而鲁棒门限代理重加密(Threshold Proxy Re-Encryption,TPRE)不仅支持安全灵活的转化控制,而且支持转化密文的合法性验证. 本文利用理想格上工具构造了一种 TPRE 方案,采用 Shamir 秘密共享实现门限控制,采用格上同态签名技术实现鲁棒性,可完全抗量子攻击. 新方案与标准格上方案相比,密文尺寸小、密钥份额短、计算速度快;基于 PRE 和 TPRE 安全模型的差异,证明对 TPRE 的攻击多项式时间内可转化为对基础 PRE 方案的攻击,安全性可规约为 R-LWE(Learning With Errors over Ring)困难假设;新方案适用于在去中心化环境中实现密文访问控制,可用于基于区块链网络的文件共享和多域网络快速互联等场景.

关键词: 代理重加密; 理想格; 鲁棒性; 同态签名; 访问控制; 量子攻击
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2020)09-1786-09
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.09.017

Robust Threshold Proxy Re-encryption Scheme from Ideal Lattices

WU Li-qiang,HAN Yi-liang,YANG Xiao-yuan,ZHANG Min-qing,YANG Kai
(*Key Laboratory of Network and Information Security,Engineering University of Chinese Armed Police Force,Xi'an,Shaanxi* 710086,*China*)

Abstract: Proxy re-encryption can achieve decryption permission conversion,while robust threshold proxy re-encryption (TPRE) supports not only secure and flexible conversion control,but also the validity verification of converted ciphertext. An ideal lattices based TPRE was proposed achieving threshold control by Shamir secret sharing and robustness by homomorphic signature technique,which could resist to quantum analysis completely. The new scheme enjoys small ciphertext size,short key share and high calculation speed compared with the similar schemes from standard lattices. Based on the differences between PRE and TPRE security models,attacks on our TPRE can be transformed into corresponding attacks on potential PRE scheme in polynomial time,therefore its security can be reduced to R-LWE (Learning With Errors over Ring) difficult assumption. It provides encryption and cryptographic access control in a decentralized environment,and widely used in scenarios such as file sharing based on blockchain networks and rapid interconnection of multi-domain networks.

Key words: proxy re-encryption;ideal lattices;robustness;homomorphic signature;access control;quantum attack

1 引言

代理重加密(Proxy Re-Encryption,PRE)在公钥加密的基础上支持解密权限的转移,其最早由 Blaze 等[1]提出,并由 Atenise 等[2]进行了形式化定义. 近年来,面对量子计算的威胁,基于格上困难假设的 PRE 成果丰硕,主要集中在 3 个方面:(1)基于 LWE 的优化 PRE 方案[3~9];(2)基于 NTRU 的 PRE 方案[9,10];(3)PRE 安全模型的加强[11,12].

在上述代理重加密中,单一代理完全掌握转换密钥,因此存在权限滥用、密钥丢失、代理掉线等风险,而门限代理重加密方案(TPRE)能够将转化权限进行分割,很好地解决了这一问题. 楼等[13]首次将 PRE 与门限密码相结合. Boneh 等[14]利用同态加密和同态签名技术,构造了一个基于格的通用门限构造器. 李等[15]将门限作用于代理密钥上,基于 LWE 构造了一个可重新拆分的 TPRE 方案,方案具有鲁棒性,即可以识别出伪造或者错误的密文份额. 然而,实现鲁棒性的方法是采用基于离散对数困难问题的 DDH(Decisional Diffie-Hellman)假设,这种方法一是无法抵抗量子攻击;二是涉及

收稿日期:2019-09-27;修回日期:2019-12-03;责任编辑:覃怀银
基金项目:国家自然科学基金(No. U1636114, No. 61572521, No. 61772550);国家社会科学基金项目(No. 18XXW015); 武警工程大学创新团队科学基金资助(No. KYTD201805);陕西省自然科学基金(No. 2018JM6078)

大量指数运算,影响了方案整体效率. 对此,本文构造了一种基于理想格的鲁棒门限代理重加密方案. 采用格上同态签名技术来实现鲁棒性,签名的不可伪造性有效保证了代理转化的诚实性,最终方案可完全抗量子攻击;利用了理想格基循环紧凑的特性,与标准格上方案[15]相比,新方案在效率上具有密文尺寸短、计算速度快等优势.

2　符号定义

设 $Z[x]$ 是系数为整数的多项式集合. $R=Z[x]/<f(x)>$ 是模 $f(x)$ 的多项式环,长度为 m 维多项式向量记作 $\boldsymbol{x}=(x_1,x_2,\cdots,x_m)\in R^m$,定义:

(1) $\boldsymbol{x}\cdot y=(x_1\cdot y,x_2\cdot y,\cdots,x_m\cdot y)\in R^m,\boldsymbol{x}\in R^m,y\in R$.

(2) $\boldsymbol{x},\boldsymbol{y}=\sum_{i=1}^{m}(x_i,y_i)\in R,\boldsymbol{x}\in R^m,\boldsymbol{y}\in R^m$.

设多项式 $x\in R_q,m=\lceil\log_2 q\rceil,y\in R_q$,多项式 $x_i\in R_2$ $(i=1,2,\cdots,m)$ 满足 $x=\sum_{i=1}^{m}2^{i-1}x_i\in R_q$. 定义

(1) $\mathrm{Bits}(x)=[x_1,x_2,\cdots,x_m]\in R_2^m$;

(2) $\mathrm{Power2}(y)=[y,2y(\mathrm{mod}q),\cdots,2^{m-1}y(\mathrm{mod}q)]\in R_q^m$.

可以验证 $\mathrm{Bits}(x)\cdot\mathrm{Power2}(y)=x\cdot y\in R_q$.

定义在整数 Z 上的离散噪声分布为 $\chi_\delta=D_{Z,\delta}$,其中 δ 表示 n 维高斯分布的高斯偏差. 用 $\bar{S}$ 表示 Shamir 秘密共享方案中秘密值 S 的某个份额.

3　基于理想格的鲁棒门限代理重加密方案

新方案中安全参数 $n\geqslant 256$,素数 $q\geqslant n^3$ 满足 $2n\mid(q-1)$,$m=\lceil\log_2 q\rceil$,$f(x)=x^n+1$,其运算定义在环 $R_q=Z_q[x]/<f(x)>$ 上,明文空间为 $\{0,1,\cdots,p-1\}$,其中 $p\geqslant 2$ 为消息模数. 定义在 R_q 上的离散均匀分布 U_q,在 R_q 上的高斯噪声分布 χ_e,选择一个伪随机函数 $F_{K_{prk}}:R_q^2\to R_r^2$,输出多项式系数范围为 $[-r,r]$,$r\in Z$,代理数量为 N,门限值为 k,设 $\eta=(N!)^2$. 以 $\Pi_{\mathrm{HS}}=(\mathrm{HS.KeyGen},\mathrm{HS.Sign},\mathrm{HS.SignEval},\mathrm{HS.Verify})$ 抽象表示同态签名方案.

3.1　密钥产生算法

(1) $\mathrm{TPRE.KeyGen}(n)$:输入安全参数 n,随机选择 $a\leftarrow U_q,s\leftarrow\chi_e$ 和 $e\leftarrow\chi_e$,计算 $b=a\cdot s+pe\in R_q$,输出公私钥对 $(K_{\mathrm{pk}}=(a,b),K_{\mathrm{sk}}=(s))$.

(2) $\mathrm{TPRE.ReKeyGen}(K_{\mathrm{sk},A},K_{\mathrm{pk},B},N,k)$:输入用户 A 的私钥 $K_{\mathrm{sk},A}$、B 的公钥 $K_{\mathrm{pk},B}$、密钥份额总数 N、门限值 k,计算代理密钥份额 $\{K_{\mathrm{kFrag},i}\}(1\leqslant i\leqslant N)$.

①对于 $i=\{1,2,\cdots,m\}$,用户 B 随机选择多项式 $\beta_i\leftarrow\chi_e$ 和 $e_i\leftarrow\chi_e$,使用私钥 $K_{\mathrm{sk},B}$,计算 $\theta_i=\beta_i\cdot K_{\mathrm{sk},B}+pe_i\in R_q$,将 $(\boldsymbol{\beta},\boldsymbol{\theta})=(\beta_i,\theta_i)$ $(1\leqslant i\leqslant m)\in R_q^{2m}$ 作为 B 的公钥发送给 A.

②用户 A 得到 $(\boldsymbol{\beta},\boldsymbol{\theta})\in R_q^{2m}$,计算 $\boldsymbol{\gamma}=\boldsymbol{\theta}-\mathrm{Power2}(K_{\mathrm{sk},A})\in R_q^m$,得到部分代理密钥 $(\boldsymbol{\beta},\boldsymbol{\gamma})\in R_q^{2m}$.

③将 $(\boldsymbol{\beta},\boldsymbol{\gamma})=(\beta_i,\gamma_i)(1\leqslant i\leqslant m)\in R_q^{2m}$ 逐系数进行 Shamir 秘密分割.

具体方法是:对于 $i=\{1,2,\cdots,mn\}$,随机选择多项式函数 $l_i(x)=Z_q[x](1\leqslant i\leqslant mn)$ 满足次数等于 $k-1$ 且 $l_i(0)=\beta_i$. 再随机选择 $w_i(x)=Z_q[x](1\leqslant i\leqslant mn)$ 满足次数等于 $k-1$ 且 $w_i(0)=\gamma_i$. 对于 $1\leqslant j\leqslant N$,第 j 个解密服务器的部分份额为

$$\bar{\boldsymbol{u}}=(\bar{\boldsymbol{\beta}}_i,\bar{\boldsymbol{\gamma}}_i)=(l_1(j),l_2(j),\cdots,l_{mn}(j);w_1(j),w_2(j),\cdots,w_{mn}(j))\in R_q^{2m}$$

④调用同态签名算法 $\mathrm{HS.KeyGen}(n,N)$ 生成验证和签名密钥 $(K_{\mathrm{hsvk}},K_{\mathrm{hssk}})$. 选择 N 个互相独立的密钥 $K_{\mathrm{prfk},1},K_{\mathrm{prfk},2}\cdots K_{\mathrm{prfk},N}$. 对于 $i=\{1,2,\cdots,N\}$,设 $\boldsymbol{x}_i=(\bar{\boldsymbol{u}}_i,K_{\mathrm{prfk},i})$,使用 K_{hssk} 对 $\boldsymbol{x}_i$ 进行签名,得到 $\bar{\sigma}_i=\mathrm{HS.Sign}(K_{\mathrm{hssk}},\boldsymbol{x}_i)$.

⑤公开 K_{hsvk},用来验证签名. 将份额 $\boldsymbol{K}_{\mathrm{kFrag},i}=\{\bar{\boldsymbol{u}}_i,K_{\mathrm{prfk},i},\bar{\sigma}_i\}(1\leqslant i\leqslant N)$ 通过安全信道发送给各个代理服务器. 因为 $\boldsymbol{K}_{\mathrm{kFrag},i}$ 能够将密文部分重加密,任何攻击者获得后就具有相应的转化能力,因此需要一个安全信道保证不被第三方窃取. 例如,使用代理服务器公钥加密后传输,从而保证机密性.

在上述过程中,用户 B 提供的 $(\boldsymbol{\beta},\boldsymbol{\theta})$ 可以看作是 B 的公钥,用户 A 可独立完成代理密钥生成,因此方案满足非交互性.

3.2　加解密算法

(1) $\mathrm{TPRE.Enc}(K_{\mathrm{pk},A},M)$:输入 $K_{\mathrm{pk},A}=(a,b)$ 和待加密的消息 $M\in R_p$,随机选择 $v、e_0、e_1\leftarrow\chi_e$,计算 $c_0=b\cdot v+pe_0+M\in R_q$,$c_1=a\cdot v+pe_1\in R_q$,输出密文 $\boldsymbol{C}_A=(c_0,c_1)\in R_q^2$.

(2) $\mathrm{TPRE.Dec}(\boldsymbol{C}_A,K_{\mathrm{sk},A})$:输入 A 的私钥 $K_{\mathrm{sk},A}$ 和密文 $\boldsymbol{C}_A=(c_0,c_1)$,计算 $t=c_0-K_{\mathrm{sk},A}\cdot c_1\in R_q$,以及 $M'=t(\mathrm{mod}p)$. 输出解密消息 M' 或者 $\perp$.

3.3　密文份额处理算法

(1) $\mathrm{TPRE.PreEnc}(\boldsymbol{C}_A,\{\boldsymbol{K}_{\mathrm{kFrag},i}\})$:输入密文 $\boldsymbol{C}_A=(c_0,c_1)$ 和代理密钥份额 $\boldsymbol{K}_{\mathrm{kFrag},i}=\{\bar{\boldsymbol{u}}_i=(\bar{\boldsymbol{\beta}}_i,\bar{\boldsymbol{\gamma}}_i),K_{\mathrm{prfk},i},\bar{\sigma}_i\}$.

①计算 $c_0'=c_0+\bar{\boldsymbol{\gamma}}_i\cdot\mathrm{Bits}(c_1)\in R_q$,$c_1'=\bar{\boldsymbol{\beta}}_i\cdot\mathrm{Bits}(c_1)\in R_q$;

②计算 $(e_0',e_1')=F_{K_{prfk,i}}(c_0,c_1)\in R_q^2$;

③计算 $\bar{c}_0'=c_0'+\eta\cdot p\cdot e_0'$,$\bar{c}_1'=c_1'+\eta\cdot p\cdot e_1'$,则 $\bar{\boldsymbol{C}}_B=(\bar{c}_0',\bar{c}_1')\in R_q^2$;

④利用同态签名算法进行估值,估值电路为

$$g_{C_A}(\bar{\boldsymbol{u}}_i,K_{\mathrm{prfk},i})=(c_0+\bar{\boldsymbol{\gamma}}_i\cdot\mathrm{Bits}(c_1),\bar{\boldsymbol{\beta}}_i\cdot\mathrm{Bits}(c_1))+$$

$$\boldsymbol{\eta}\cdot p\cdot F_{K_{\text{prfk},i}}(c_0,c_1)\in R_q^2$$

计算 HS.SignEval$(g_{C_A},\bar{\sigma}_i)=\bar{\sigma}_i'$.

输出 B 对应的密文份额 $\boldsymbol{C}_{\text{cFrag},i}=\{\bar{\boldsymbol{C}}_B,\bar{\sigma}_i'\}$.

(2)TPRE.Verify$(\{\boldsymbol{C}_{\text{cFrag},i}\})$:输入密文份额 $\boldsymbol{C}_{\text{cFrag,i}}=\{\bar{\boldsymbol{C}}_B,\bar{\sigma}_i'\}$,计算 HS.Verify$(K_{\text{hsvk}},\bar{\boldsymbol{C}}_B,g_{C_A},\bar{\sigma}_i')$,输出 1 表示密文份额合法,否则 0 表示份额非法.

(3)TPRE.Comb$(\{\boldsymbol{C}_{\text{cFrag},i}\}_{i\in S})$:假设参与者集合为 S,$|S|=k'$表示元素数量. 如果 $k'<k$,输出 $\perp$;否则计算一个完整密文.

①对于 $i\in S$ 中每一个解密份额$\{\boldsymbol{C}_{\text{cFrag},i}\}$,计算 TPRE.Verify$(\{\boldsymbol{C}_{\text{cFrag,i}}\})$,若验证失败,输出 $\perp$ 并退出.

②使用$\{\boldsymbol{C}_{\text{cFrag,i}}\}(i\in S)$进行 Shamir 秘密重构. 方法是遍历 $\boldsymbol{C}_{\text{cFrag},i}=\{(\bar{c}_0',\bar{c}_1')_i,\bar{\sigma}_i'\}(i\in S)$,以参与者编号为 x 值,以$(\bar{c}_0',\bar{c}_1')_i$ 为 y 值. 计算 Lagrange 系数

$$\lambda_i=\prod_{j\in S,i\neq j}\frac{-i}{i-j}$$

计算完整密文

$$(c_0',c_1')=\sum_{i\in S}\lambda_i(\bar{c}_0',\bar{c}_1')_i+\sum_{i\in S}\lambda_i(1-c_0,0).$$

新方案的工作流程如图 1 所示. 系统包含 N 个代理服务器. 密文及密文份额的存储、密文重构都由存储服务器完成.

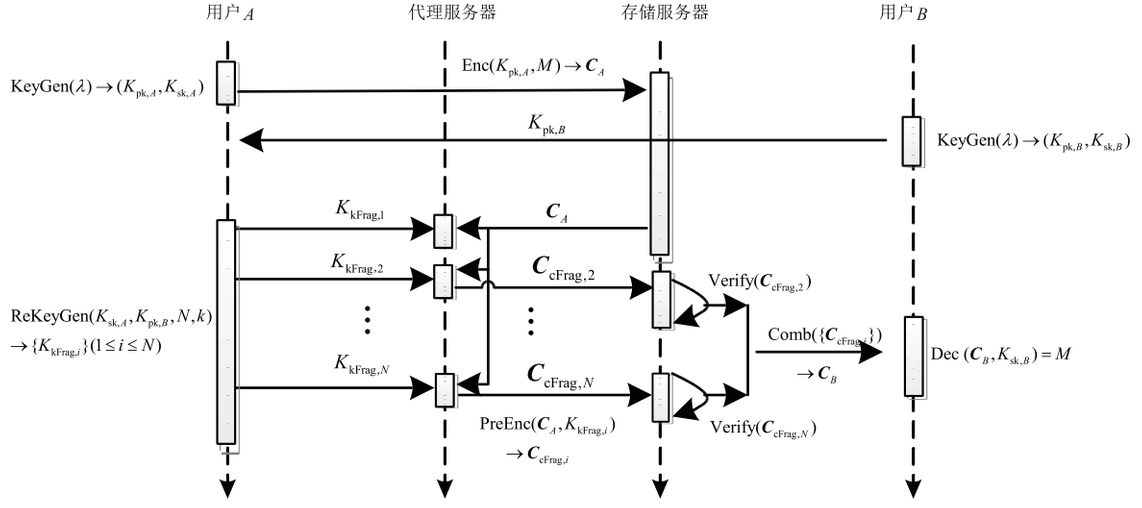


图1 TPRE方案工作流程

4 方案分析

4.1 正确性

定理 1(正确性) 安全参数 $n\in Z$,$m=\lceil\log_2 q\rceil$,$p\in Z$ 是消息空间,B_e 为离散高斯分布 χ_e 的长度上界,$F_{K_{\text{prfk}}}$的输出为均匀分布,上界为 B_r,设 $q>2p[3\sqrt{n}B_e^2+mnB_e+(N!)^3k(B_r+\sqrt{n}B_eB_r)]$. 在单跳情况下,新方案可正确解密.

证明

(1)未转换密文的解密正确性

使用 $c_0-c_1\cdot K_{\text{sk}}$解密.

$$\begin{aligned}c_0-c_1\cdot K_{\text{sk}}&=b\cdot v+pe_0+M-K_{\text{sk}}\cdot(a\cdot v+pe_1)\\&=(a\cdot s+pe)\cdot v+pe_0+M-K_{\text{sk}}\cdot(a\cdot v+pe_1)\\&=M+\underbrace{p(e\cdot v+e_0-K_{\text{sk}}\cdot e_1)}_{\text{noise}}\end{aligned}$$

只要噪声 $p(e\cdot v+e_0-K_{\text{sk}}\cdot e_1)$不超过 $q/2$,其值 mod p 后仍然能够恢复出 M. 事实上,参数 $K_{\text{sk}},v,e_0,e_1,e$ 都不会超过 B_e,即 $p(e\cdot v+e_0-s\cdot e_1)\leqslant 3\sqrt{n}pB_e^2$,因此 $q\geqslant 6\sqrt{n}pB_e^2$.

(2)转换密文的解密正确性

通过一次转换之后,B 对应的密文为:

$$\begin{aligned}\boldsymbol{C}_B&=(c_0',c_1')\\&=\sum_{i\in S}\lambda_i[c_0+\bar{\boldsymbol{\gamma}}_i\cdot\text{Bits}(c_1)+\boldsymbol{\eta}\cdot p\cdot(e_0')_i,\\&\bar{\boldsymbol{\beta}}_i\cdot\text{Bits}(c_1)+\boldsymbol{\eta}\cdot p\cdot(e_1')_i]+\sum_{i\in S}[(1-\lambda_i)c_0,0]\\&=(c_0+\sum_{i\in S}(\lambda_i\cdot\bar{\boldsymbol{\gamma}}_i)\cdot\text{Bits}(c_1)+\sum_{i\in S}(\boldsymbol{\eta}\cdot\lambda_i\cdot p\cdot(e_0')_i),\\&\sum_{i\in S}(\lambda_i\cdot\bar{\boldsymbol{\beta}}_i)\cdot\text{Bits}(c_1)+\sum_{i\in S}(\boldsymbol{\eta}\cdot\lambda_i\cdot p\cdot(e_1')_i))\end{aligned}$$

因为 $\sum_{i\in S}(\lambda_i\cdot\bar{\boldsymbol{\gamma}}_i)=\boldsymbol{\gamma}$,$\sum_{i\in S}(\lambda_i\cdot\bar{\boldsymbol{\beta}}_i)=\boldsymbol{\beta}$,则

$$\begin{aligned}&=(c_0+\boldsymbol{\gamma}\cdot\text{Bits}(c_1)+p\cdot\sum_{i\in S}\boldsymbol{\eta}\cdot\lambda_i\cdot(e_0')_i,\\&\boldsymbol{\beta}\cdot\text{Bits}(c_1)+p\cdot\sum_{i\in S}\boldsymbol{\eta}\cdot\lambda_i\cdot(e_1')_i)\end{aligned}$$

使用 B 的私钥 $K_{\text{sk},B}$解密密文.

$$\begin{aligned}&c_0'-c_1'\cdot K_{\text{sk},B}\\&=c_0+\boldsymbol{\gamma}\cdot\text{Bits}(c_1)+p\cdot\sum_{i\in S}(\boldsymbol{\eta}\cdot\lambda_i\cdot(e_0')_i)-\\&\quad(\boldsymbol{\beta}\cdot\text{Bits}(c_1)+p\cdot\sum_{i\in S}(\boldsymbol{\eta}\cdot\lambda_i\cdot(e_0')_i))\cdot K_{\text{sk},B}\\&=c_0+(p\boldsymbol{E}-\text{Power2}(K_{\text{sk},A}))\cdot\text{Bits}(c_1)+\end{aligned}$$

$$p\cdot\sum_{i\in S}(\eta\cdot\lambda_i\cdot(e_0')_i)-p\cdot K_{\mathrm{sk},B}\cdot\sum_{i\in S}(\eta\cdot\lambda_i\cdot(e_1')_i)$$
$$=M+\underbrace{p(e\cdot v+e_0-K_{\mathrm{sk},A}\cdot e_1)}_{\text{noise}}+p(\boldsymbol{E}\cdot\mathrm{Bits}(c_1)+$$
$$\underbrace{\sum_{i\in S}(\eta\cdot\lambda_i\cdot(e_0')_i)-K_{\mathrm{sk},B}\cdot\sum_{i\in S}(\eta\cdot\lambda_i\cdot(e_1')_i))}_{\text{noise}}$$

其中 $\boldsymbol{E}\in(\chi_e)^{2m}$. 可以验证,转化后密文可正确解密. 原因如下:相比于初始的噪声,转化的噪声更大. 具体分析,伪随机函数 $F_{K_{\mathrm{prfk}}}:R_q^2\to R_r^2$,其输出多项式系数范围为 $[-r,r]$,上界为 B_r,$\boldsymbol{E}\cdot\mathrm{Bits}(c_1)\leqslant mn\tilde{e}_0$,其中 $\tilde{e}_0$ 服从 χ_e 分布,其上界为 B_e.

定理 2[14]　设 Shamir 秘密共享中数量为 k 的有效用户集合为 $S\in[N]\cup\{0\}$,则 $(N!)^2\cdot\lambda_i$ 是一个整数,且 $|(N!)^2\cdot\lambda_i|\leqslant(N!)^3$,其中 λ_i 表示 Lagrange 系数.

根据定理 2,则

$$\sum_{i\in S}(\eta\cdot\lambda_i\cdot(e_0')_i)-K_{\mathrm{sk},B}\cdot\sum_{i\in S}(\eta\cdot\lambda_i\cdot(e_0')_i)$$
$$\leqslant(N!)^3k(\tilde{e}_1+\tilde{e}_2\cdot\tilde{e}_3)$$

其中 $\tilde{e}_2$ 服从 χ_e 分布,其上界为 B_e,$\tilde{e}_1$,$\tilde{e}_3$ 服从均匀分布,其上界为 B_r. 即所有噪声的上界为 $\|\mathrm{noise}\|\leqslant 3\sqrt{n}pB_e^2+pmnB_e+p(N!)^3k(B_r+\sqrt{n}B_eB_r)$,当 $q>2p[3\sqrt{n}B_e^2+mnB_e+(N!)^3k(B_r+\sqrt{n}B_eB_r)]$,解密正确.

(3)密文份额验证的正确性

密文份额验证的正确性是通过同态签名方案中验证算法 HS. Verify 来保证的. 在 TPRE. PreEnc($\boldsymbol{C}_A$,$\{\boldsymbol{K}_{\mathrm{kFrag},i}\}$)中,以 $\boldsymbol{C}_A=(c_0,c_1)\in R_q^2$ 定义的 g_{C_A} 作为估值电路,以 $\bar{\boldsymbol{u}}_j=(\bar{\boldsymbol{\beta}}_i,\bar{\boldsymbol{\gamma}}_i)$ 以及 $K_{\mathrm{prfk},i}$ 作为电路输入. 一方面,$\bar{\boldsymbol{C}}_B=(\bar{c}_0',\bar{c}_1')$ 的计算过程(TPRE. PreEnc 中的步骤①、②、③)可以看成是消息层面的计算;另一方面,HS. SignEval(g_{C_A},$\bar{\sigma}_i$)$=\bar{\sigma}_i'$ 可以看成签名层面的计算(TPRE. PreEnc 中的步骤④),根据同态签名方案的正确性定义,如果 $\bar{\sigma}_i'$ 的确是代理根据 HS. SignEval(g_{C_A},$\bar{\sigma}_i$)$=\bar{\sigma}_i'$ 诚实计算得到的结果,那么 HS. Verify(K_{hsvk},$\bar{\boldsymbol{C}}_B$,g_{C_A},$\bar{\sigma}_i'$)能够通过验证,验证算法的正确性得到证明.

4.2　安全性

定理 3(安全性)　如果 R-LWE 假设是困难的,那么基于理想格的 TPRE 方案是 CPA 安全的.

证明　TPRE 可以理解为 PRE 的一种扩展,TPRE 和 PRE 安全模型[2]的差异主要体现在当攻击者进行代理密钥和重加密询问时,挑战者根据询问参数,决定相应的回答内容,具体如图 2 所示.

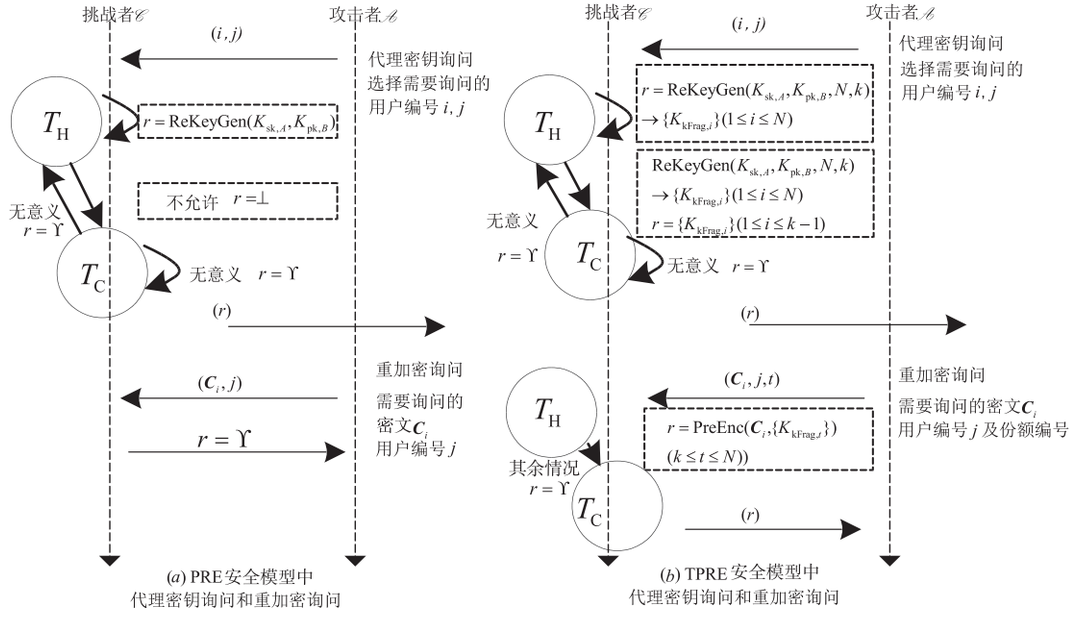


图2　PRE和TPRE安全模型比较

共有两处不同,一是在 $i\in T_{\mathrm{H}}$,$j\in T_{\mathrm{H}}$ 情况下,如果进行代理密钥询问,PRE 中返回的是完整代理密钥,而 TPRE 返回的是对完整代理密钥进行分割后的 N 个密钥份额. 二是在 $i\in T_{\mathrm{H}}$,$j\in T_{\mathrm{C}}$ 情况下,如果进行代理密钥询问,PRE 方案是不允许的,但 TPRE 可以返回腐化代理服务器相对应的 $k-1$ 个密钥份额;另外如果进行重加密询问,PRE 方案中挑战者返回的是 Υ,TPRE 方案中挑战者需要返回非腐化代理服务器相对应的密文份额.

基于上述分析,证明过程分为两个阶段,第一阶段证明上述两种挑战者返回信息的差异从信息量上是等

价的,因此可以将对 TPRE 方案的攻击转化为对潜在 PRE 方案的攻击;第二个阶段证明相应的 PRE 方案满足 CPA 安全.

Game T1:对于 TPRE 方案真实的 CPA 攻击游戏.

Game T2-1:对 Game T1 做如下改进:在代理密钥询问阶段,如果 $\mathscr{A}$ 询问的参数满足 $i\in T_{\mathrm{H}}, j\in T_{\mathrm{H}}$,那么挑战者 $\mathscr{C}$ 使用 $(K_{\mathrm{sk},i},K_{\mathrm{pk},j})$ 计算出完整的代理密钥 $\boldsymbol{K}_{\mathrm{rk},i\to j}$,之后将 $\boldsymbol{K}_{\mathrm{rk},i\to j}$ 以及 N、k 等参数交给自己的助手—模拟器 $\mathscr{S}$,$\mathscr{S}$ 完成 $\boldsymbol{K}_{\mathrm{rk},i\to j}$ 的分割,生成签名密钥对,对密钥份额签名,最后将 N 个密钥份额 $\{\boldsymbol{K}_{\mathrm{kFrag},i}\}$ $(1\leqslant i\leqslant N)$ 全部发送给攻击者 $\mathscr{A}$.

Game T1 与 Game T2-1 等价. 实际上,$\mathscr{C}$ 和模拟器 $\mathscr{S}$ 的工作共同组成了游戏 T1 中的 TPRE. ReKeyGen 步骤,因为 Shamir 秘密分割和重构过程,都能在多项式时间内完成计算,所以提供完整密钥 $\boldsymbol{K}_{\mathrm{rk},i\to j}$ 和提供 N 个密钥份额在信息量上是相等的,Game T1 与 GameT2-1 等价. PRE 和 TPRE 安全模型中第一点差异多项式时间可消除.

Game T2-2:对 GameT2-1 做如下改进:在重加密询问阶段,如果 $i\in T_{\mathrm{H}}, j\in T_{\mathrm{C}}$,挑战者 $\mathscr{C}$ 如实计算 $\overline{\boldsymbol{C}}_B=(\bar{c}_0',\bar{c}_1')$,但在计算同态签名过程中,不再使用 HS. SignEval$(g_{C_i},\bar{\sigma}_i)=\bar{\sigma}_i'$ 进行诚实计算,而是直接使用签名私钥 K_{hssk} 对转换后的密文份额 $\overline{\boldsymbol{C}}_B$ 进行签名,得到同态签名 $\bar{\sigma}_i'$.

Game T2-2 与 GameT2-1 等价,如果同态签名具备内容隐藏属性,从攻击者 $\mathscr{A}$ 的视角看来,由最终估值结果 $\boldsymbol{C}_{\mathrm{cFrag},i}=\{\overline{\boldsymbol{C}}_B,\bar{\sigma}_i'\}$ 得不到原始消息、原始签名的任何信息;而无论那种方法得到的签名 $\bar{\sigma}_i'$ 都能够通过 K_{hssk} 的验证.

Game T2-3:对 GameT2-2 做如下改进:在重加密询问阶段,如果 $i\in T_{\mathrm{H}}, j\in T_{\mathrm{C}}$,挑战者 $\mathscr{C}$ 计算 $\overline{\boldsymbol{C}}_B$ 的过程中,不再诚实地计算 $(e_0',e_1')=F_{K_{\mathrm{prf}}}(c_0,c_1)\in R_q^2$,而是随机选取系数在 $[-r,r]$ 的多项式 $(e_0',e_1')\xleftarrow{\$}\mathrm{R}_{\mathrm{r}}^2$.

Game T2-2 与 GameT2-3 等价. 根据伪随机函数 $F_{K_{\mathrm{prf}}}$ 的定义,多项式 (e_0',e_1') 无论是随机选取还是通过 $F_{K_{\mathrm{prf}}}$ 真实计算,最终结果都是 $[-r,r]$ 上的均匀分布,在攻击者 $\mathscr{A}$ 看来是完全一致的,因此 Game T2-2 与 GameT2-3 等价.

Game T2-4:在之前的攻击游戏中,挑战者 $\mathscr{C}$ 诚实地使用了代理密钥 $\boldsymbol{K}_{\mathrm{rk},i\to j}$ 进行 Shamir 秘密分割并得到密钥份额. 在 GameT2-4 中,当代理密钥询问满足 $i\in T_{\mathrm{H}}, j\in T_{\mathrm{C}}$ 时,挑战者随机选择均匀分布的 $\boldsymbol{u}=(\boldsymbol{\beta},\boldsymbol{\gamma})\in R_q^{2m}$ 作为 $\boldsymbol{K}_{\mathrm{rk},i\to j}$,秘密分割后将腐化服务器对应的 $k-1$ 个密钥份额发送给攻击者 $\mathscr{A}$(腐化服务器编号构成集合 S^*,$|S^*|=k-1$). 之后,当攻击者 $\mathscr{A}$ 询问 (C_i,j,t) 时,如果 $i\in T_{\mathrm{H}}, j\in T_{\mathrm{C}}$ 且 $t\in[N]\backslash S^*$,$\mathscr{C}$ 如下回答询问:

(1)计算 Lagrange 系数 $\lambda_w^{\tilde{S}^*}, w\in\tilde{S}^*$,其中 $\tilde{S}^*=S^*\cup\{0\}$.

(2)随机选择 $\boldsymbol{v}_j\leftarrow R_r^2$.

(3)计算

$$\begin{aligned}(\bar{c}_0',\bar{c}_1')=&\lambda_0^{\tilde{S}^*}(c_0+\boldsymbol{\gamma}\cdot\mathrm{Bits}(c_1),\boldsymbol{\beta}\cdot\mathrm{Bits}(c_1))\\&+\sum_{i\in S^*}\lambda_i^{S^*}(c_0+\bar{\boldsymbol{\gamma}}_i\cdot\mathrm{Bits}(c_1),\bar{\boldsymbol{\beta}}_i\cdot\mathrm{Bits}(c_1))\\&+\eta\cdot p\cdot\boldsymbol{v}_j\in R_q^2\end{aligned}$$

将结果返回给攻击者 $\mathscr{A}$.

Game T2-3 与 GameT2-4 等价. 首先分析密文份额,第一部分 $\lambda_0^{\tilde{S}^*}(c_0+\boldsymbol{\gamma}\cdot\mathrm{Bits}(c_1),\boldsymbol{\beta}\cdot\mathrm{Bits}(c_1))$ 是编号为 0,份额为 $\boldsymbol{u}=(\boldsymbol{\beta},\boldsymbol{\gamma})$ 的参与者提供的 1 个密文份额,第二部分是 $k-1$ 个参与者(来自 S^*)提供的 $k-1$ 个密文份额. 两者刚好到达了门限值 k. 因此

$$\begin{aligned}(\bar{c}_0',\bar{c}_1')=&\sum_{i\in S^*}\lambda_i^{S^*}(c_0+\bar{\boldsymbol{\gamma}}_i\cdot\mathrm{Bits}(c_1),\bar{\boldsymbol{\beta}}_i\cdot\mathrm{Bits}(c_1))\\&+\eta\cdot p\cdot\boldsymbol{v}_j\\=&(c_0+\boldsymbol{\gamma}\cdot\mathrm{Bits}(c_1),\boldsymbol{\beta}\cdot\mathrm{Bits}(c_1))\\&+\eta\cdot p\cdot\boldsymbol{v}_j\in R_q^2\end{aligned}$$

可以看到,在 $(\bar{c}_0',\bar{c}_1')$ 的计算过程中,提供的输入分布 $\boldsymbol{u}=(\boldsymbol{\beta},\boldsymbol{\gamma})$ 和 $\boldsymbol{v}_j$ 都和 Game T2-3 中相同,而且最终表达式 $(c_0+\boldsymbol{\gamma}\cdot\mathrm{Bits}(c_1),\boldsymbol{\beta}\cdot\mathrm{Bits}(c_1))+\eta\cdot p\cdot\boldsymbol{v}_j$ 和 TPRE. PreEnc 算法中密文份额表达式也是相同的. 因此从攻击者 $\mathscr{A}$ 角度来看,Game T2-3 与 Game T2-4 中接收到的密文份额在分布上是不可区分的,而在 Game T2-4 中,实际上挑战者 $\mathscr{C}$ 是不知道真实代理密钥的,不会泄露代理密钥 $\boldsymbol{K}_{\mathrm{rk},i\to j}$ 的任何信息. 所以 PRE 和 TPRE 安全模型中第二点差异在多项式时间可消除.

至此,对 TPRE 方案的攻击,在多项式时间内可以完全转化为对 PRE 方案的相应攻击. 实际上,新 TPRE 方案是基于 BV-PRE 方案构造的,BV-PRE 方案已经被证明在 R-LWE 困难假设[16]下是 CPA 安全的[9].

因此,TPRE 方案的安全性规约为 R-LWE 困难假设.

定理 4(鲁棒性) 如果同态签名 Π_{HS} 满足不可伪造性,那么新 TPRE 方案满足鲁棒性.

证明 利用同态签名的不可伪造性,可以证明新方案的鲁棒性. 如果一个攻击者 $\mathscr{A}$ 能够攻破鲁棒性游戏,那么就可以构造一个模拟器 $\mathscr{S}$,通过和同态签名安全模型中的挑战者 $\mathscr{C}$ 交互,攻破同态签名的不可伪造性. 其过程如下:

模拟器 $\mathscr{S}$ 首先从挑战者 $\mathscr{C}$ 那里获得验证公钥 $\boldsymbol{K}_{\mathrm{hsvk}}$,攻击者 $\mathscr{A}$ 选择想要攻击的代理密钥 $\boldsymbol{K}_{\mathrm{rk},i\to j}^*$,模拟器 $\mathscr{S}$ 运行 TPRE. ReKeyGen 算法对 $\boldsymbol{K}_{\mathrm{rk},i\to j}^*$ 逐系数进行 Shamir 秘密分割,得到部分代理密钥份额 $\bar{\boldsymbol{u}}_i^*$,同时选择

N 个互相独立的密钥 $K^*_{\text{prfk},1}, K^*_{\text{prfk},2}, \cdots, K^*_{\text{prfk},N}$,设 $i=\{1,2,\cdots,N\}$, $\boldsymbol{x}_i^* = (\bar{\boldsymbol{u}}_i^*, K^*_{\text{prfk},i})$,将 $\boldsymbol{x}_i^*$ 发送给同态签名挑战者 $\mathscr{C}$ 进行签名,得到 $\bar{\sigma}_i'^*$. 当攻击者 $\mathscr{A}$ 将一个伪造的重加密密文份额 $\boldsymbol{C}^*_{\text{cFrag},i} = \{\bar{\boldsymbol{C}}_B^* = (\bar{c}_0'^*, \bar{c}_1'^*), \bar{\sigma}_i'^*\}$ 提交给模拟器 $\mathscr{S}$ 时,$\mathscr{S}$ 进行加工得到 $(K_{\text{hsvk}}, \bar{\boldsymbol{C}}_B^*, g^*_{C_A}, \bar{\sigma}_i'^*)$,并作为一个伪造的同态签名提交给挑战者 $\mathscr{C}$.

如果攻击者 $\mathscr{A}$ 能够赢得鲁棒性游戏,那么 $\boldsymbol{C}^*_{\text{cFrag},i} \neq \text{TPRE.PreEnc}(\boldsymbol{C}_A, \{\boldsymbol{K}^*_{\text{kFrag},i}\})$,但是 $\text{TPRE.Verify}(\boldsymbol{C}^*_{\text{cFrag},i}) = 1$,这也说明 $\text{HS.Verify}(K_{\text{hsvk}}, \bar{\boldsymbol{C}}_B^*, g^*_{C_A}, \bar{\sigma}_i'^*)$ 能够通过验证,那么模拟器 $\mathscr{S}$ 成功伪造出了一个非法签名,即攻破了同态签名算法的不可伪造性.

因此,如果同态签名算法 Π_{HS} 满足不可伪造性,那么新 TPRE 能够实现鲁棒性.

4.3　方案比较

在现存的 TPRE 方案构造中,有两个典型 TPRE 方案值得关注. 一是 Umbral[17],它是 NuCypher 密钥管理系统的核心方案,另一个是标准格上 TPRE 方案[15].

新方案使用目前高效的 BV-PRE 来构造,每次处理的消息是 1 个长度为 n 的多项式,加解密都是在多项式环上进行,通过快速傅里叶变换 FFT(Fast Fourier Transform)可以提高加解密速度. 与标准格上方案[15]相比,新方案在密钥尺寸、密文尺寸上更为紧凑,在计算效率上也更为高效.

密文份额的合法性验证使用同态签名来进行,可以通过目前格上高效的同态签名方案[18,19]进行实例化,使得最终方案能够完全抵抗量子攻击. 另外,对原始签名进行估值时,定义估值函数 g_{C_A} 中 $\text{Bits}(c_1)$ 是布尔向量,同态签名计算实际上是布尔类型的运算,不涉及复杂的高次运算,因此较离散对数计算效率要高.

表 1 将 3 种方案在性质和效率方面进行比较. $|\mathbb{Z}_q|$ 表示 1 个模 q 集整数的长度,|Ploy| 表示 1 个维数为 n 的多项式的长度,Exp 表示 1 次群上指数运算,Hash 表示 1 次哈希运算,zMult 表示 1 次整数乘法运算,pMult 表示 1 次两个 n 维多项式的乘法运算,HS.Veriy 表示 1 次同态签名验证算法,忽略加法运算量. 密文份额和密钥份额尺寸不包含用作验证的信息负载,密文转换计算量不包含生成鲁棒性验证信息的计算.

表 1　类似 TPRE 方案比较

方案		文献[17]方案	文献[15]方案	本文方案
性质	基础 PRE 方案	BBS98[1]	Aono[4]	BV-PRE[9]
	构造工具	离散对数	整数格	理想格
	实现鲁棒性方法	零知识证明	零知识证明	同态签名
	实现鲁棒性工具	判定性离散对数	判定性离散对数	格
	是否抗量子攻击	加密和份额验证 都无法抵抗	加密可抵抗, 份额验证无法抵抗	加密和份额验证 都可抵抗
效率	1 次加密消息长度	$\{0,1\}^l$	$\{0,1\}$	$\{0,1,\cdots,p\}^n$
	密钥份额尺寸	$6\|\mathbb{Z}_q\|$	$(n\eta+1)(n+1)\|\mathbb{Z}_q\|$	$2m\|\text{Ploy}\|$
	密文份额尺寸	$4\|\mathbb{Z}_q\|$	$(n+1)\|\mathbb{Z}_q\|$	$2\|\text{Ploy}\|$
	密文转换计算量	2Exp	$(n\eta+1)(n+1)$ zMult	2 pMult
	鲁棒性验证计算量	2Exp + Hash	$(n\eta+1)(n+1)(\text{Exp}+\text{zMult})$	HS.Veriy
	运算方法	群运算	矩阵运算	FFT

5　应用

新 TPRE 具有“高可用、低信任、强安全”等优势,可成为密态信息安全分享的关键技术,在外包数据安全、多方安全计算、去中心化网络等方面有广泛应用.

5.1　基于区块链网络的文件共享系统

在传统代理重加密构造的文件共享系统中,代理通常由一个独立服务器担任,但是一旦中心化的代理不再保持中立并拒绝提供重加密服务,或故意提供错误的重加密服务,这将直接导致信息共享过程失效. 因此,可以考虑利用 TPRE 和区块链两项技术构造分布式文件共享系统,将密文转化的任务委托给一个去中心化的区块链网络来完成,如图 3 所示.

第一步,用户 A 选择存储位置,比如 Amazon S3、IPFS 等,用自己公钥加密文件,也可以采用混合加密模式.

第二步,当用户 A 需要与用户 B 共享某个密态文件 File_A 时,将区块链网络中每个节点作为一个代理服务器,为其生成密钥份额 $\{\boldsymbol{K}_{\text{kFrag},i}\}$ $(1 \leqslant i \leqslant N)$. 并向全网提供待共享文件地址、共享用户等信息,发布一个重加密任务.

第三步,当网络节点收到重新加密请求时,每个节点自主提供重加密服务以换取代币,比如,最早为用户 B 提供 k 个正确密文份额的节点将会获得系统给予的若干个代币奖励,方案的鲁棒性为鉴别转换结果是否正确提供了验证方法.

第四步,用户 B 对应的存储服务器将合法密文份额组合,得到完整密态文件 File_B 并保存,用户 B 进行下载、解密.

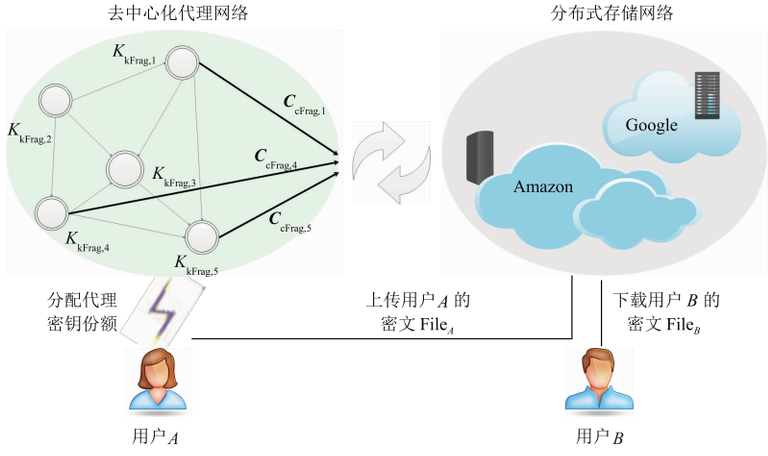


图3 基于区块链网络的文件共享系统

区块链网络中节点总数 N 一定程度上反映了系统的可用性. 假设网络中每个节点诚实工作的概率为 p (比如 $p=1/2$),只要 N 个代理节点中有 k 个在线并诚实提供重加密服务,文件共享就有效,因此成功转换的概率为

$$\Pr[\text{Succ}] = \sum_{i=k}^{N} C_N^i p^i (1-p)^{N-i}$$

当 N 和 k 的差值较大时,成功转化的概率较高. 从系统效率角度来分析,如果 N 值增大,一方面会增加系统的复杂性,因为密钥分割和密文合并的成本都和 N 有线性关系;另一方面,从正确性证明过程可以看出,其积累的噪声和 $(N!)^3$ 正向相关,过高噪声容易造成解密失败.

从安全性角度来讲,如果多个节点合谋,就有可能获取完整代理密钥,根据 Shamir 秘密恢复原理,攻击者至少需要腐化 k 个代理节点,其概率为

$$\Pr[\text{ProxyKey}] = \sum_{i=k}^{N} C_N^i (1-p)^i p^{N-i}$$

在 N 确定的情况下,k 值越大,其得到完整代理密钥的概率越小,其因此系统具有天然抗合谋攻击的性质. 另外,即使上述过程中攻击者掌握了代理密钥,其能够掌控密文转换的主动性,但文件始终以密态形式出现,明文仍然不会暴露.

5.2 多域网络快速互联

在一些灾难救援、互动会议等需要多域协同的场合,通常需要两个原本独立的网络临时连通并进行信息转发,而任务结束后,这种信任关系将会立刻撤销. 在需要协同工作时,在两个网络之间架设 N 个服务器作为代理节点,如图 4 所示. 当网络 1 中主机 A 要给网络 2 中主机 B、C 传输信息时,生成相应 $A\rightarrow B$、$A\rightarrow C$ 的代理密钥份额并分发给 N 个代理节点,A 只需要将文件使用自己的公钥加密,并转发到节点服务器上,当至少 k 个节点诚实转化密文时,B 和 C 就能够读取信息. 在功能上,这样的网络能够实现“一对多”的快速信息传输,而且方便实现群组用户的动态加入和退出;在性能上,即使某个节点由于自身故障或者被攻击停止服务,也不影响系统的正常运行,具有良好的健壮性.

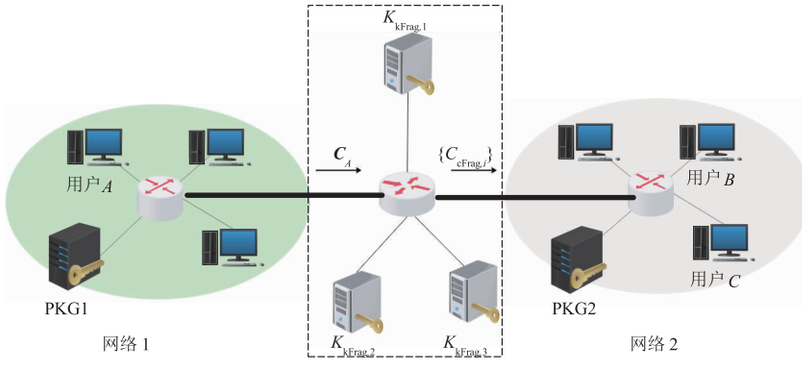


图4 多域环境下网络快速互联

6 总结及展望

结合 R-LWE、秘密共享和同态签名等技术,提出一种理想格上门限代理重加密方案. 该方案可以缩短密文尺寸、提高加解密效率. 使用格上同态签名方案对 TPRE 进行实例化后,可使最终方案具备鲁棒性,可完全抵抗量子攻击,因此具有广阔的应用前景. 下一步可对方案进行软件实现,更为精确地分析其效率,以及在保证效率的前提下,尝试构造 CCA 安全的 TPRE 方案.

参考文献

[1] M Blaze, G Bleumer, M Strauss. Divertible protocols and atomic proxy cryptography[A]. International Conference on the Theory and Applications of Cryptographic Techniques [C]. Berlin: Springer, 1998. 127 – 144.

[2] G Ateniese, K Fu, M Green, et al. Improved proxy reencryption schemes with applications to secure distributed storage [J]. ACM Transactions on Information and System Security (TISSEC), 2006, 9(1): 1 – 30.

[3] Xagawa K. Cryptography with Lattices[D]. Tokyo: Tokyo Institute of Technology, 2010.

[4] Aono Y, Boyen X, Wang L. Key-private proxy re-encryption under LWE[A]. International Conference on Cryptology[C]. Berlin: Springer, 2013. 1 – 18.

[5] Singh K, Rangan C P, et al. Cryptanalysis of unidirectional proxy re-encryption scheme[A]. Information and Communication Technology—EurAsia Conference [C]. Berlin: Springer, 2014. 564 – 575.

[6] Kirshanova, E. Proxy Re-encryption from lattices[A]. International Workshop on Public Key Cryptography [C]. Berlin: Springer, 2014. 77 – 94.

[7] Jiang M M, Hu Y P, et al. Lattice based multi-use unidirectional proxy re-encryption[J]. Security & Communication Networks, 2016, 8(18): 3796 – 3803.

[8] Fan X, Liu F H. Various Proxy Re-encryption Schemes from Lattices [EB/OL]. https://eprint. iacr. org/2016/278. pdf, 2017-05-11/2019-09-04.

[9] Polyakov Y, Rohloff K, et al. Fast proxy re-encryption for publish/subscribe systems[J]. ACM Transactions on Privacy and Security, 2017, 20(4): 1 – 31.

[10] Nu†ez D, Agudo I, Lopez J. NTRUReEncrypt: An efficient proxy re-encryption scheme based on NTRU[A]. Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security[C]. Singapore: ACM, 2015. 179 – 189.

[11] Cohen A. What about Bob? The inadequacy of CPA security for proxy reencryption[A]. IACR International Workshop on Public Key Cryptography[C]. Berlin: Springer, 2019. 287 – 316.

[12] Fuchsbauer G., Kamath C, et al. Adaptively secure proxy re-encryption[A]. IACR International Workshop on Public Key Cryptography [C]. Berlin: Springer, 2019. 317 – 346.

[13] 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.

[14] D Boneh, R Gennaro, et al. A Lattice-Based Universal Thresholdizer for Cryptographic Systems [EB/OL]. https://eprint. iacr. org/2017/251. pdf, 2017-03-19/2019-09-04.

[15] 李菊雁,马春光,赵乾. 格上可重新拆分的门限多代理者的代理重加密方案[J]. 通信学报,2017,38(5):157 – 164.
Ju-yan LI, Chun-guang MA, Qian ZHAO. Resplittable threshold multi-broker proxy re-encryption scheme from lattices[J]. Journal on Communications, 2017, 38(5): 157 – 164. (in Chinese)

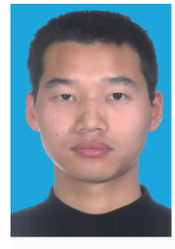
[16] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings[A]. Annual International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin: Springer, 2010. 1 – 23.

[17] David N. UMBRAL: A Threshold Proxy Re-Encryption Scheme [EB/OL]. https://github. com/nucypher/umbral-doc/ blob/master/mbral-doc. pdf, 2018-05-06/2019-09-04.

[18] Boneh D, Freeman D M. Homomorphic signatures for polynomial functions [A]. Annual International Conference on the Theory and Applications of Cryptographic Techniques[C]. Berlin: Springer, 2011. 149 – 168.

[19] Gorbunov S, Vaikuntanathan V, et al. Leveled fully homomorphic signatures from standard lattices [A]. Proceedings of the forty-seventh annual ACM symposium on Theory of computing[C]. USA: ACM, 2015. 469 – 477.

作者简介



吴立强　男,1986 年 7 月出生于陕西蓝田. 现为武警工程大学密码工程学院讲师. 主要研究方向为基于格的密码学和可证明安全理论. E-mail: latticewj@163. com

韩益亮(通信作者) 男,1977 年 10 月出生于甘肃会宁. 教授、博士生导师,主要研究方向为信息安全与密码学.
E-mail:hanyil@163.com

杨晓元 男,1959 年 11 月生于湖南湘潭,教授、博士生导师,主要研究领域为网络安全与密码学.
E-mail:yxyangyxyang@163.com

张敏情 女,1967 年 3 月出生于陕西西安,教授、博士生导师,主要研究领域为信息隐藏、密码学.
E-mail:api_zmq@126.com

杨 凯 男,1983 年 10 月出生于山东莱芜,讲师,博士,主要研究方向为网络安全.
E-mail:sydeny-001@163.com