d 维(t,n)门限量子同态加密算法的设计与仿真

宋秀丽[1,2],周道洋[2],文爱君[2]
(1. 重庆邮电大学网络空间安全与信息法学院,重庆 400065;2. 重庆邮电大学计算机科学与技术学院,重庆 400065)

摘 要: 量子同态加密对量子态密文直接进行同态评估计算,而不是将密文解密之后再进行计算. 基于相位和状态变换的 d 维通用酉算子,提出了一种 d 维(t,n)门限量子同态加密算法. 在该算法中,客户端将量子态密文传送给 n 个服务器中的 t 个,这 t 个服务器生成评估子密钥,运行评估算法对量子态密文执行同态计算. 客户端对解密之后的量子态执行 CNOT 门操作,$t+1$ 个粒子的聚合值就是评估算法对量子态明文计算之后的结果. 该算法使用 Shamir (t,n)门限机制隐藏了评估密钥,保护了客户端的隐私数据. 从理论上证明了算法的正确性,各个阶段操作过程的仿真实现进一步验证了算法的正确性.

关键词: 量子同态加密; d 维; (t, n) 门限; 通用酉算子; 评估计算
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2020)05-0846-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.05.003

Design and Simulation of d Dimensional (t,n) Threshold Quantum Homomorphic Encryption Algorithm

SONG Xiu-li[1,2], ZHOU Dao-yang[2], WEN Ai-jun[2]
(1. *Chongqing University of Posts and Telecommunications, School of Cyber Security and Information Law, Chongqing* 400065, *China*;
2. *Chongqing University of Posts and Telecommunications, College of Computer Science and Technology, Chongqing* 400065, *China*)

Abstract: Quantum homomorphic cryptography directly evaluates the quantum ciphertext, rather than decrypts the quantum ciphertext and then calculates it. Based on a general d-dimensional unitary operator of phase and state transformation, a d-dimensional (t,n) threshold quantum homomorphic encryption algorithm was proposed. In this algorithm, the client sent the quantum state ciphertext to t of n servers. Each of the t servers generated the evaluation sub-keys, and then run the evaluation algorithm on the quantum state ciphertext to complete the calculation of quantum homomorphism. The client performed CNOT gates on the quantum states after decryption, and the aggregate value of $t+1$ particles was the result after evaluation calculation on the quantum state plaintext. The algorithm uses Shamir's (t,n) threshold scheme to hide the evaluation keys, so that it protects the client's private data. The theorems prove the correctness of the algorithm theoretically, and the simulations of each stage of the algorithm further verify its correctness.

Key words: quantum homomorphic encryption; d-dimension; (t, n) threshold; general unitary operator; evaluation calculation

1 引言

经典密码学使用保密的通信方式隐蔽和保护通信双方发送的信息,使未授权者不能获取这些信息的任何内容. 1994 年,Shor[1] 提出了著名的大整数分解和离散对数计算的概率量子算法,使得依赖于求解数学问题复杂性的经典密码学的安全性受到了巨大的威胁. 量子密码学以量子物理原理为基础,利用量子相干叠加、量子纠缠效应等技术增强量子通信传输中的可证明安全性和对扰动的可检测性,能弥补经典密码学的安全脆弱性. 量子同态加密技术是量子密码学的一个重要的分支,它可实现在量子通信环境下对加密量子态数据的同态计算,即对量子态密文直接进行评估计算,而不是将密文解密之后再进行计算. 假设客户端拥

收稿日期:2019-05-23;修回日期:2019-12-04;责任编辑:马兰英
基金项目:国家自然科学基金(No. 61772098, No. 61772099, No. 61802039);重庆市科学技术委员会基础科学与前沿技术项目(No. cstc2018jcyjAX0510)

有大量的敏感数据,例如个人账务、网上交易记录等等,他需要对这些数据进行函数或集合计算,但他自身并没有这种计算能力,于是他将这些数据送交给第三方服务器,委托它来完成计算任务,同时,又不能让它知晓敏感数据的具体内容. 客户端和第三方服务器可使用量子同态加密技术来实现这种隐私计算任务.

早在 1978 年,文献[2]提出了经典同态加密算法的概念,自此之后,一些研究者提出了更多的经典同态加密算法[3~6]. 经典同态加密为分布式环境下的用户隐私提供强力保护,在安全云计算与委托计算、密文检索、远程文件检索等领域都有广泛的应用. 借鉴经典同态加密的思想,基于量子力学的基本原理,一些研究者将经典同态加密拓展到量子世界,提出了量子同态加密算法[7~15]. 文献[7]使用玻色子采样和多步量子行走模型实现有限的量子同态加密. 文献[8]提出了一种量子全同态加密算法. 该算法借助于通用量子线路的黑盒实现量子同态变换,由密钥迭代算法保证密钥的安全性. 文献[9]通过定义一种三维量子门提出了三值量子同态加密算法,扩展了量子同态加密的希尔伯特空间维度. 文献[10]在量子线路基础上构造一种量子同态加密算法. 文献[11]基于量子编码理论提出一种量子同态加密算法. 文献[12]通过二维基本量子门构造了量子同态加密算法,文献[13]基于量子 T 门构造两种量子同态加密算法. 文献[14]在二维量子旋转变换门基础之上提出一种量子同态加密算法. 文献[15]利用量子容错结构提出了量子同态加密算法,扩展了量子同态加密算法的类型.

在上述量子同态加密算法中,大多数算法的量子态希尔伯特空间的维度局限在二维,虽然文献[9]将空间维度从二维拓展为三维,但不能向更高维空间拓展. 有些算法的存在风险和脆弱性,安全性有待进一步增强. 例如,文献[12]提出的量子同态加密算法中的评估算法并不独立于密钥,增加了算法的安全风险. 有些算法中的量子同态变换存在局限性,不具有通用性. 例如文献[14]中的算法仅仅局限于量子门旋转变换,不能执行更多通用的同态变换.

本文突破上述量子同态加密算法的局限性,基于相位和状态变换的 d 维酉算子,利用此算子的部分可交换性构造了一种 d 维(t,n)门限量子同态加密算法. 在该算法中,客户端使用 Shamir(t,n)门限机制[16]将评估初始密钥分解成 n 个份额分发给 n 个服务器,将加密之后的量子态密文传送给信任的 t 个服务器. 这 t 个服务器生成评估子密钥,运行评估算法执行同态计算. 客户端通过控制 CNOT 门操作,将评估操作信息恢复.

2　预备知识

为了能够清晰描述(t,n) 门限量子同态加密算法,本节将给出基于相位和状态变换的 d 维通用酉算子定义.

定义 1　(d 维通用酉算子)在 d 维复内积空间中,一种基于相位和状态变换的 d 维通用酉算子定义如式(1)所示[17]:

$$G_{\alpha,\beta}=\sum_{u=0}^{d-1}\omega^{\beta u}\,|u+\alpha\rangle\langle u| \tag{1}$$

其中 $\alpha,\beta\in\{0,1,\cdots,d-1\}$,$\omega=e^{2\pi i/d}$,"+"代表模 d 加法运算. d 维通用酉算子 $G_{\alpha,\beta}$ 对于任意量子态 $|x\rangle$ ($x\in\{0,\cdots,d-1\}$)的变换结果如式(2)所示.

$$\begin{aligned}G_{\alpha,\beta}|x\rangle&=\Big(\sum_{u=0}^{d-1}\omega^{\beta u}\,|u+\alpha\rangle\langle u|\Big)|x\rangle\\&=(\omega^{\beta\cdot 0}\,|\alpha\rangle\langle 0|+\omega^{\beta\cdot 1}\,|1+\alpha\rangle\\&\quad\langle 1|+\cdots+\omega^{\beta\cdot x}\,|x+\alpha\rangle\langle x|+\cdots\\&\quad+\omega^{\beta\cdot(d-1)}\,|d-1+\alpha\rangle\langle d-1|)\,|x\rangle\\&=\omega^{\beta\cdot x}\,|x+\alpha\rangle\end{aligned} \tag{2}$$

特别地,在 d 维复内积空间中,当 $G_{\alpha,\beta}$ 中 $\alpha,\beta\in\{0,1\}$时,对应的基本门运算 X,Z 门定义如式(3)、式(4)所示:

$$X=G_{1,0}=\sum_{x=0}^{d-1}|x+1\rangle\langle x| \tag{3}$$

$$Z=G_{0,1}=\sum_{x=0}^{d-1}\omega^{x}\,|x\rangle\langle x| \tag{4}$$

3　d 维(t,n)门限量子同态加密算法

本节将具体描述 d 维(t,n)门限量子同态加密算法,并构建该算法的量子线路,最后对其在理论上进行正确性证明.

3.1　算法描述

在提出的(t,n)门限量子同态加密算法中,客户端有一量子态明文 $|\sigma\rangle$,他想对其执行评估计算 $G_{a_0,b_0}()$,但是他自身存储容量和计算能力有限,于是他委托存储能力和计算能力足够强大的 n 个第三方服务器协同来完成评估计算任务. 由于客户端对他委托的部分服务器不太信任,于是他将量子态明文首先进行加密运算,然后发送给他信任的 t 个服务器执行评估计算. 当 t 个服务器完成计算任务之后,他们返回计算结果给客户端,客户端对这些计算结果解密并重构出最终的评估计算结果. 该算法包括五个阶段:准备阶段、加密阶段、评估阶段、解密阶段和重构阶段.

3.1.1　准备阶段

(1)加解密密钥的生成

客户端运行密钥生成算法 $G(1^{\lambda})$随机生成两个密钥 $k,l\in\{0,1,\cdots,d-1\}$,其中,λ 是一个安全参数. 这两个密钥仅仅在客户端保存,既作为加密密钥又作为解

密密钥.

(2)评估初始密钥的生成

建立在 Shamir(t,n)门限机制的基础上,客户端随机生成两个 $t-1$ 次多项式,如式(5)、式(6)所示:

$$g_1(x)=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+\cdots+a_1x+a_0(\mathrm{mod}d) \quad (5)$$

$$g_2(x)=b_{t-1}x^{t-1}+b_{t-2}x^{t-2}+\cdots+b_1x+b_0(\mathrm{mod}d) \quad (6)$$

其中 $g_1(x),g_2(x)\in GF(d)$,且 a_0,b_0 为两个评估初始密钥.

客户端首先建立两个集合$\{x_{1i}\mid i=1,2,\cdots,n\}$和$\{x_{2i}\mid i=1,2,\cdots,n\}$,每个集合有 n 个非零且互不相等的整数. 然后他分别计算评估密钥 a_0 和 b_0 的份额$\{(x_{1i},y_{1i}=g_1(x_{1i}))\mid i=1,2,\cdots,n\}$和$\{(x_{2i},y_{2i}=g_2(x_{2i}))\mid i=1,2,\cdots,n\}$. 客户端将份额$\{(x_{1i},y_{1i}),(x_{2i},y_{2i})\}(i=1,2,\cdots,n)$发送到第 i 个服务器 W_i.

3.1.2 加密阶段

客户端首先将明文制备成 $t+1$ 个量子态$|(1-t)\sigma\rangle_0\otimes|\sigma\rangle_1\otimes\cdots\otimes|\sigma\rangle_t$,称之为量子态明文,以 k,l 作为加密密钥,Encrypt( )作为加密算法,客户端对量子态明文中的粒子$\{|\sigma\rangle_1,|\sigma\rangle_2,\cdots,|\sigma\rangle_t\}$执行加密运算,那么这 t 个粒子构成了一个复合量子态密文系统,如式(7)所示:

$$\begin{aligned}\Psi&=\otimes_{r=1}^{t}Encrypt(k,l,|\sigma\rangle_r)\\&=\otimes_{r=1}^{t}X^kZ^l|\sigma\rangle_r\\&=\otimes_{r=1}^{t}|\rho\rangle_r\end{aligned} \quad (7)$$

客户端从 n 个服务器$\{W_i\mid i=1,2,\cdots,n\}$中选择信任的 t 个服务器,假设这 t 个服务器为$\{W_r\mid r=1,2,\cdots,t\}$,客户端将量子态密文$|\rho\rangle_r(r=1,2,\cdots,t)$发送到第 r 个服务器 W_r.

3.1.3 评估阶段

在此阶段,t 个服务器$\{W_r\mid r=1,2,\cdots,t\}$中的每个服务器取出自己存储的份额$\{(x_{1r},y_{1r}),(x_{2r},y_{2r})\}$,计算该份额对应的评估子密钥,如式(8)、式(9)所示:

$$s_{1r}=y_{1r}\prod_{\substack{j=1\\j\neq r}}^{t}\frac{x_{1j}}{x_{1j}-x_{1r}}(\mathrm{mod}d) \quad (8)$$

$$s_{2r}=y_{2r}\prod_{\substack{j=1\\j\neq r}}^{t}\frac{x_{2j}}{x_{2j}-x_{2r}}(\mathrm{mod}d) \quad (9)$$

以(s_{1r},s_{2r})作为评估子密钥,Evaluate( )作为评估算法,每个服务器 $W_r(r=1,2,\cdots,t)$对客户端发送的加密量子态 $|\rho\rangle_r$ 执行评估计算,得到评估结果,如式(10)所示:

$$|\delta\rangle_r=\mathrm{Evaluate}(s_{1r},s_{2r},|\rho\rangle_r)=G_{s_{1r},s_{2r}}|\rho\rangle_r \quad (10)$$

每个服务器 $W_r(r=1,2,\cdots,t)$将评估操作计算后的量子态 $|\delta\rangle_r$ 通过安全可信量子信道发回客户端,等待客户端解密.

3.1.4 解密阶段

客户端对每个服务器 $W_r(r=1,2,\cdots,t)$发回的评估计算结果执行解密算法 Decrypt( ),得到直接计算结果.

$$\begin{aligned}|\varphi\rangle_r&=\mathrm{Decrypt}(k,l,s_{1r},s_{2r},|\delta\rangle_r)\\&=\omega^{s_{1r}l-s_{2r}k}Z^{-l}X^{-k}|\delta\rangle_r\\&=G_{s_{1r},s_{2r}}|\sigma\rangle_r=\omega^{s_{2r}\cdot\sigma}|\sigma+s_{1r}\rangle_r\end{aligned} \quad (11)$$

此量子态 $|\varphi\rangle_r$ 即为评估算法 Evaluate( )对量子态明文 $|\sigma\rangle_r$ 直接计算后的结果 $G_{s_{1r},s_{2r}}|\sigma\rangle_r$. 其中 $r=1,2,\cdots,t$.

3.1.5 重构阶段

当客户端对从 t 服务器接收到的 t 个量子态$\{|\delta_r\rangle\mid r=1,2,\cdots,t\}$解密完毕,此时他拥有的 $t+1$ 个量子态所构成的复合量子系统为 Γ_1:

$$\begin{aligned}\Gamma_1&=|(1-t)\sigma\rangle_0\otimes|\varphi\rangle_1\otimes|\varphi\rangle_2\otimes\cdots\otimes|\varphi\rangle_t\\&=\omega^{\sum_{r=1}^{t}s_{2r}\cdot\sigma}|(1-t)\sigma\rangle_0\otimes_{r=1}^{t}|\sigma+s_{1r}\rangle_r\end{aligned} \quad (12)$$

接着,客户端对此量子系统中的粒子$\{|\varphi\rangle_1,|\varphi\rangle_2,\cdots,|\varphi\rangle_t\}$执行 d 维 CNOT 门操作 $R_c(|\varphi\rangle_j,|\varphi\rangle_{j-1})(j=t,t-1,\cdots,1)$,其中 $|\varphi\rangle_j$ 是控制粒子,$|\varphi\rangle_{j-1}$是目标粒子. 当对 t 个粒子执行完毕,此时客户端拥有的 $t+1$ 个量子态所构成的复合量子系统为 Γ_2:

$$\begin{aligned}\Gamma_2&=\omega^{\sum_{r=1}^{t}s_{2r}\cdot\sigma}|(1-t)\sigma\rangle_0\otimes|t\sigma+\sum_{r=1}^{t}s_{1r}\rangle_1\otimes\cdots\\&\otimes|(t-j+1)\sigma+\sum_{r=j}^{t}s_{1r}\rangle_j\otimes\cdots\otimes|\sigma+s_{1t}\rangle_t\end{aligned} \quad (13)$$

最后,以$|t\sigma+\sum_{r=1}^{t}s_{1r}\rangle_1$作为控制粒子,以$|(1-t))\sigma\rangle_0$为目标粒子,对两粒子执行 d 维 CNOT 门 R_c( )操作,此时客户端拥有的 $t+1$ 个量子态所构成的复合量子系统为 Γ_3:

$$\begin{aligned}\Gamma_3&=\omega^{\sum_{r=1}^{t}s_{2r}\cdot\sigma}|\sigma+\sum_{r=1}^{t}s_{1r}\rangle_0\otimes|t\sigma+\sum_{r=1}^{t}s_{1r}\rangle_1\otimes\cdots\\&\otimes|(t-j+1)\sigma+\sum_{r=j}^{t}s_{1r}\rangle_j\otimes\cdots\otimes|\sigma+s_{1t}\rangle_t\end{aligned} \quad (14)$$

根据拉格朗日插值公式,由于存在以下等式:

$$a_0=\sum_{r=1}^{t}s_{1r}=\sum_{r=1}^{t}y_{1r}\prod_{\substack{j=1\\j\neq r}}^{t}\frac{x_{1j}}{x_{1j}-x_{1r}}(\mathrm{mod}d) \quad (15)$$

$$b_0=\sum_{r=1}^{t}s_{2r}=\sum_{r=1}^{t}y_{2r}\prod_{\substack{j=1\\j\neq r}}^{t}\frac{x_{2j}}{x_{2j}-x_{2r}}(\mathrm{mod}d) \quad (16)$$

因此,在等式(14)中,序号为0的粒子可写为:

$$\begin{aligned}\omega^{\sum_{r=1}^{t}s_{2r}\cdot\sigma}|\sigma+\sum_{r=1}^{t}s_{1r}\rangle_0&=\omega^{b_0\cdot\sigma}|\sigma+a_0\rangle_0\\&=G_{a_0,b_0}|\sigma\rangle_0\end{aligned} \quad (17)$$

从等式(17)可看出,等式(14)中序号为 0 的粒子就是评估算子 $G_{a_0,b_0}()$ 对明文量子态 $|\sigma\rangle_0$ 直接计算之后的结果.

3.2　算法的量子线路图

上一节详细描述了 d 维(t,n)门限量子同态加密算法的设计过程,本节给出了该算法的加密阶段、评估阶段、解密阶段和重构阶段的具体量子线路设计图,如图 1 所示.

在图 1 的加密阶段中,客户端对制备的初始量子态明文 $|\sigma\rangle_1\otimes\cdots\otimes|\sigma\rangle_t$ 中的每个明文执行加密算法,加密密钥为 l,k,加密算子为 X,Z;在评估阶段中,每个服务器 $W_r(r=1,2,\cdots,t)$ 使用评估子密钥(s_{1r},s_{2r})对量子态密文执行评估计算 $G_{s_{1r},s_{2r}}$,并将计算结果发回客户端;在解密阶段中,客户端对评估计算之后的每个量子态执行解密算法,解密密钥为 l,k,解密算子为 Z^{-1},X^{-1}. 重构阶段对相邻粒子执行 d 维控制非门 R_c 运算,最终序号为 0 的粒子就是评估算子 $G_{a_0,b_0}()$ 对明文量子态 $|\sigma\rangle_0$ 直接计算之后的结果.

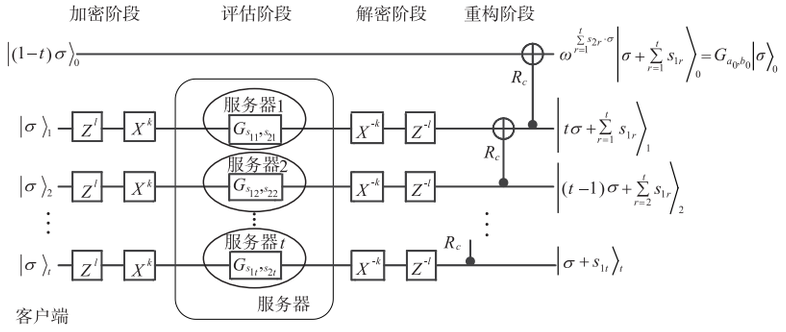

图1　算法量子线路图

3.3　算法的正确性证明

定理 1　基于相位和状态变换的 d 维通用算子 $G_{\alpha,\beta}$ 具有部分可交换性.

证明　假设 $G_{\alpha,\beta},G_{p,q}$ 是定义 1 中两个任意的通用酉算子,其中 $\alpha,\beta,p,q\in\{0,1,\cdots,d-1\}$,则 $G_{\alpha,\beta},G_{p,q}$ 的内积如下:

$$\begin{aligned}G_{\alpha,\beta}\cdot G_{p,q}&=\sum_{x=0}^{d-1}\omega^{\beta x}|x+\alpha\rangle\langle x|\cdot\sum_{y=0}^{d-1}\omega^{qy}|y+p\rangle\langle y|\\&=(\omega^{\beta\cdot0}|0+\alpha\rangle\langle0|+\cdots+\omega^{\beta\cdot p}|p+\alpha\rangle\langle p|\\&\quad+\omega^{\beta\cdot(p+1)}|p+1+\alpha\rangle\langle p+1|+\cdots\\&\quad+\omega^{\beta\cdot(d-1)}|d-1+\alpha\rangle\langle d-1|)\\&\quad\cdot(\omega^{q\cdot0}|0+p\rangle\langle0|+\omega^{q\cdot1}|1+p\rangle\langle1|\\&\quad+\omega^{q\cdot2}|2+p\rangle\langle2|+\cdots+\omega^{q\cdot(d-1)}|d-1+p\rangle\langle d-1|)\\&=\omega^{\beta\cdot p+q\cdot0}|p+\alpha\rangle\langle0|+\omega^{\beta\cdot(p+1)+q\cdot1}|1+p+\alpha\rangle\langle1|\\&\quad+\omega^{\beta\cdot(p+2)+q\cdot2}|2+p+\alpha\rangle\langle2|+\cdots\\&\quad+\omega^{\beta\cdot(p+d-1)+q\cdot(d-1)}|d-1+p+\alpha\rangle\langle d-1|\\&=\omega^{\beta\cdot p}\sum_{x=0}^{d-1}\omega^{(\beta+q)\cdot x}|x+p+\alpha\rangle\langle x|\\&=\omega^{\beta\cdot p}G_{\alpha+p,\beta+q}\end{aligned}\tag{18}$$

因此,由等式(18)可知,任意两个 d 维通用酉算子 $G_{\alpha,\beta},G_{p,q}$ 之间具有以下关系式:

$$\begin{aligned}G_{\alpha,\beta}\cdot G_{p,q}&=\omega^{\beta\cdot p}G_{\alpha+p,\beta+q}\\&=\omega^{\beta\cdot p-\alpha\cdot q}G_{p,q}\cdot G_{\alpha,\beta}\end{aligned}\tag{19}$$

由等式(19)得知,对于任意两个 d 维通用酉算子 $G_{\alpha,\beta},G_{p,q}$,在允许一定相位差 $\omega^{\beta\cdot p-\alpha\cdot q}$ 的情况下具有可交换性,定理 1 得证.

正确性 1　根据定理 1 基于相位和状态变换的 d 维通用算子的部分可交换性,在评估阶段对量子态密文 $|\rho\rangle_r(r=1,\cdots,t)$ 执行评估计算时,等式(20)正确:

$$\begin{aligned}|\delta\rangle_r&=\text{Evaluate}(s_{1r},s_{2r},|\rho\rangle_r)=G_{s_{1r},s_{2r}}|\rho\rangle_r\\&=\omega^{s_{2r}\cdot k-s_{1r}\cdot l}X^kZ^l\omega^{s_{2r}\cdot\sigma}|\sigma+s_{1r}\rangle_r\end{aligned}\tag{20}$$

其中 $r=1,2,\cdots,t$.

证明　根据等式(18)和(19),d 维通用算子具有部分可交换性,存在:

$$\begin{aligned}G_{s_{1r},s_{2r}}|\rho\rangle_r&=G_{s_{1r},s_{2r}}X^kZ^l|\sigma\rangle_r\\&=G_{s_{1r},s_{2r}}G_{k,l}|\sigma\rangle_r\\&=\omega^{s_{2r}\cdot k-s_{1r}\cdot l}G_{k,l}G_{s_{1r},s_{2r}}|\sigma\rangle_r\\&=\omega^{s_{2r}\cdot k-s_{1r}\cdot l}X^kZ^lG_{s_{1r},s_{2r}}|\sigma\rangle_r\\&=\omega^{s_{2r}\cdot k-s_{1r}\cdot l}X^kZ^l\omega^{s_{2r}\cdot\sigma}|\sigma+s_{1r}\rangle_r\end{aligned}\tag{21}$$

由于定理 1 中 d 维通用算子具有部分可交换性使得评估算子 $G_{s_{1r},s_{2r}}$ 可以在相位差为 $\omega^{s_{2r}\cdot k-s_{1r}\cdot l}$ 的情况下与加密算子 X^kZ^l 实现交换. 在解密阶段通过填补相应的相位差,使得评估算子能够实现对量子态明文 $|\sigma\rangle_r$ $(r=1,\cdots,t)$ 的同态计算.　　证毕.

正确性 2　正确性 1,当客户端对第 r 个服务器 W_r 返回的评估计算结果 $|\delta\rangle_r$ 执行解密算法 Decrypt() 时,等式(22)正确:

$$\begin{aligned}|\varphi\rangle_r&=Decrypt(k,l,s_{1r},s_{2r},|\delta\rangle_r)\\&=\omega^{s_{1r}\cdot l-s_{2r}\cdot k}Z^{-l}X^{-k}|\delta\rangle_r=G_{s_{1r},s_{2r}}|\sigma\rangle_r\end{aligned}\tag{22}$$

其中 $r=1,2,\cdots,t$.

证明 根据等式(20)和式(21)的计算结果,当对每个服务器发回的计算结果执行添加校正相位的解密操作 $\omega^{s_{1r}\cdot l-s_{2r}\cdot k}Z^{-l}X^{-k}$ 时,变换过程如下:

$$\begin{aligned}|\varphi\rangle_r &=\omega^{s_{1r}\cdot l-s_{2r}\cdot k}Z^{-l}X^{-k}|\delta\rangle_r\\ &=\omega^{s_{1r}\cdot l-s_{2r}\cdot k}Z^{-l}X^{-k}G_{s_{1r},s_{2r}}|\rho\rangle_r\\ &=\omega^{s_{1r}\cdot l-s_{2r}\cdot k}Z^{-l}X^{-k}\omega^{s_{2r}\cdot k-s_{1r}\cdot l}X^kZ^l\omega^{s_{2r}\cdot\sigma}|\sigma+s_{1r}\rangle_r\\ &=\omega^{s_{1r}\cdot l-s_{2r}\cdot k+s_{2r}\cdot k-s_{1r}\cdot l}Z^{-l}X^{-k}X^kZ^l\omega^{s_{2r}\cdot\sigma}|\sigma+s_{1r}\rangle_r\\ &=\omega^{s_{2r}\cdot\sigma}|\sigma+s_{1r}\rangle_r\\ &=G_{s_{1r},s_{2r}}|\sigma\rangle_r \end{aligned}\tag{23}$$

从等式(23)得知,解密之后的结果就是评估算子对量子态明文 $|\sigma\rangle_r$ 直接计算之后的结果,因此解密过程中的等式(22)正确。

既然评估阶段的评估算法对量子态的变换过程是正确性的,即正确性1,解密阶段的解密算法对量子态的变换过程也是正确性的,即正确性2,那么本文所提的 d 维 (t,n) 门限量子同态加密算法当然也是正确的.

4 安全性分析

本节将对提出的 d 维 (t,n) 门限量子同态加密算法进行安全性分析,分别从截获-测量攻击、纠缠-测量攻击和合谋攻击三方面具体展开.

4.1 截获-测量攻击

假设 Eve 是一个熟知算法的外部窃听者,他知道算法的所有执行过程和客户端公布的数据,但不知道客户端保密的数据. 当 Eve 截获加密阶段客户端发送给任意一个服务器 W_r 的量子态密文 $|\rho\rangle_r(r\in\{1,2,\cdots,t\})$ 之后,她使用 d 维测量基 $\{\omega^{\beta\cdot j}|j+\alpha\rangle\ |j=0,1,\cdots,d-1\}$ 测量截获的量子态密文 $|\rho\rangle_r$,其中 $\alpha,\beta\in\{0,1,\cdots,d-1\}$,她将以 $1/d^2$ 的概率得到 $\omega^{l\cdot\sigma}|\sigma+k\rangle$,以 $1-1/d^2$ 的概率得不到任何有价值的信息. 即使 Eve 以小概率事件获得了 $\omega^{l\cdot\sigma}|\sigma+k\rangle$,但加解密密钥 k,l 是由客户端秘密保存且不对外公开的,因此她并不能从 $\omega^{l\cdot\sigma}|\sigma+k\rangle$ 中能计算出量子态明文 $|\sigma\rangle$.

当 Eve 截获评估阶段中任一服务器 W_r 发送回客户端的评估计算结果 $|\delta\rangle_r(r\in\{1,2,\cdots,t\})$ 时,并使用 d 维测量基 $\{\omega^{\beta\cdot j}|j+\alpha\rangle\ |j=0,1,\cdots,d-1\}$ 测量截获的量子态 $|\delta\rangle_r$ 时,她将以 $1/d^2$ 的概率得到 $\omega^{(\sigma+k)s_{2r}+\sigma\cdot l}|\sigma+k+s_{1r}\rangle$,以 $1-1/d^2$ 概率得不到任何有价值的信息. 即使 Eve 以小概率事件获得了 $\omega^{(\sigma+k)s_{2r}+\sigma\cdot l}|\sigma+k+s_{1r}\rangle$,但加解密密钥 k,l 和评估子密钥 s_{1r},s_{2r} 是保密的,因此她并不能从 $\omega^{(\sigma+k)s_{2r}+\sigma\cdot l}|\sigma+k+s_{1r}\rangle$ 中能计算出量子态明文 $|\sigma\rangle$. 既然在加密阶段和评估阶段,Eve 都不能从她所截获的量子态获得有价值的信息,因此她的截获-测量攻击失败.

4.2 纠缠-测量攻击

假设 Eve 首先截获加密阶段客户端发送给任意一个服务器 W_r 的量子态密文 $|\rho\rangle_r(r\in\{1,2,\cdots,t\})$,并制备一个辅助粒子 $|e_1\rangle_a$. 然后,她以 $|\rho\rangle_r$ 为控制粒子,以 $|e_1\rangle_a$ 为目标粒子执行 d 维 R_c 门变换,可得到 $R_c(|\rho\rangle_r,|e_1\rangle_a)=\omega^{l\cdot\sigma}|\sigma+k\rangle_r\ |e_1+\sigma+k\rangle_a$. 其次,Eve 使用测量基 $\{|0\rangle,|1\rangle,\cdots,|d-1\rangle\}$ 对辅助粒子 $|\rangle_a$ 执行测量操作,那么他将以 $1/d$ 的概率得到 $|e_1+\sigma+k\rangle_a$,以 $1-1/d$ 概率得不到任何有价值的信息. 即使 Eve 以小概率事件获得了 $|e_1+\sigma+k\rangle_a$,但加密密钥 k 是由客户端生成且是保密的,因此 Eve 并不能从 $|e_1+\sigma+k\rangle_a$ 中计算出明文信息 $|\sigma\rangle$.

当 Eve 截获评估阶段任意一个服务器 W_r 发送回客户端的评估计算结果 $|\delta\rangle_r(r\in\{1,2,\cdots,t\})$ 之后,制备了一个辅助粒子 $|e_2\rangle_a$. 然后,她以 $|\delta\rangle_r$ 为控制粒子,以 $|e_2\rangle_a$ 为目标粒子执行 d 维 R_c 门变换,可得 $R_c(|\delta\rangle_r,|e_2\rangle_a)=\omega^{s_{2r}\cdot k-s_{1r}\cdot l}\cdot\omega^{(s_{2r}+l)\cdot\sigma}|\sigma+k+s_{1r}\rangle_r\ |e_2+\sigma+k+s_{1r}\rangle_a$. Eve 使用测量基 $\{|0\rangle,|1\rangle,\cdots,|d-1\rangle\}$ 对辅助粒子 $|\rangle_a$ 执行测量操作,那么他将以 $1/d$ 的概率得到 $|e_2+\sigma+k+s_{1r}\rangle_a$,以 $1-1/d$ 概率得不到任何有价值的信息. 即使 Eve 以小概率事件获得 $|e_2+\sigma+k+s_{1r}\rangle_a$,但加密密钥 k 和评估子密钥 s_{1r} 她都无从知晓,因此 Eve 并不能从 $|e_2+\sigma+k+s_{1r}\rangle_a$ 中计算出明文信息 $|\sigma\rangle$. 既然在加密阶段和评估阶段,Eve 都不能从她所制备的辅助量子态中获得有价值的信息,因此她的纠缠-测量攻击失败.

4.3 合谋攻击

在本 (t,n) 门限量子同态加密算法中,n 个服务器中的每个服务器分别拥有两个评估密钥的份额. 假设有若干个服务器不诚实,试图合谋通过拥有的份额重建出原始评估密钥 a_0,b_0. 根据 Shamir (t,n) 门限机制,必须至少有 t 个份额才能重建原始信息. 由于各个服务器之间互不透明,任何一个服务器并不知晓其他服务器拥有的份额,因此只要 t 个或大于 t 个服务器是诚实的,即使剩余的部分服务器被腐蚀,他们发起合谋攻击,使用拉格朗日插值多项式并不能重构出评估密钥 a_0,b_0,因此合谋攻击失败.

5 仿真实现

前面几节的正确性证明和举例验证都是从理论层面证明了提出的 (t,n) 门限量子同态加密算法的正确性,本节在经典计算机上使用 C++ 语言对该算法的运算逻辑进行仿真验证. 仿真过程列举了在不同门限、不同维度下,取不同加密密钥和评估密钥时加密阶段、评估阶段、解密阶段的输出结果,验证了算法的正确性.

仿真计算结果将显示在表 1 和表 2 中. 在两张表中,所　　有计算结果都精确到小数点后面的六位.

表 1　$t=2,n=3$ 时算法的仿真结果

初始参数	加解密密钥	评估初始密钥	评估子密钥	加密结果	评估结果	解密结果	重构结果
$d=5$, $\|\sigma\rangle=\|1\rangle$	$k=1$, $l=1$	$a_0=1$, $b_0=0$	$s_{11}=1$, $s_{21}=0$	$0.309017+i0.951057\|2\rangle$	$0.309017+i0.951057\|3\rangle$	$1.000000+i0.000001\|2\rangle$	$1.000000+i0.000001\|2\rangle$
			$s_{12}=0$, $s_{22}=0$	$0.309017+i0.951057\|2\rangle$	$0.309017+i0.951057\|2\rangle$	$1.000000+i0.000001\|1\rangle$	
$d=23$, $\|\sigma\rangle=\|1\rangle$	$k=5$, $l=18$	$a_0=0$, $b_0=3$	$s_{11}=13$, $s_{21}=11$	$0.203457-i0.979084\|7\rangle$	$-0.576679-i0.816971\|19\rangle$	$-0.990686-i0.136165\|14\rangle$	$0.682551+i0.730838\|1\rangle$
			$s_{12}=10$, $s_{22}=15$	$0.203457-i0.979084\|7\rangle$	$-0.334879-i0.942261\|16\rangle$	$-0.576679-i0.816971\|11\rangle$	
$d=103$, $\|\sigma\rangle=\|1\rangle$	$k=43$, $l=91$	$a_0=47$, $b_0=67$	$s_{11}=85$, $s_{21}=67$	$0.743825-i0.668374\|44\rangle$	$-0.999535-i0.030497\|26\rangle$	$-0.585314-i0.810807\|85\rangle$	$-0.585313-i0.810808\|48\rangle$
			$s_{12}=65$, $s_{22}=0$	$0.743825-i0.668374\|44\rangle$	$-0.743825-i0.668374\|6\rangle$	$1.000000+i0.000001\|65\rangle$	

表 2　$t=5,n=9$ 时算法的仿真结果

初始参数	加解密密钥	评估初始密钥	评估子密钥	加密结果	评估结果	解密结果	重构结果
$d=7$, $\|\sigma\rangle=\|1\rangle$	$k=3$, $l=4$	$a_0=2$, $b_0=2$	$s_{11}=3$, $s_{21}=4$	$-0.900969-i0.433884\|4\rangle$	$0.623490-i0.781831\|0\rangle$	$-0.900968-i0.433885\|4\rangle$	$-0.222528+i0.974926\|3\rangle$
			$s_{12}=5$, $s_{22}=1$	$-0.900969-i0.433884\|4\rangle$	$0.623489+i0.781832\|2\rangle$	$0.623489+i0.781832\|6\rangle$	
			$s_{13}=0$, $s_{23}=5$	$-0.900969-i0.433884\|4\rangle$	$-0.900969+i0.433883\|4\rangle$	$-0.222519-i0.974928\|1\rangle$	
			$s_{14}=1$, $s_{24}=0$	$-0.900969-i0.433884\|4\rangle$	$-0.900969-i0.433884\|5\rangle$	$1.000000+i0.000001\|2\rangle$	
			$s_{15}=0$, $s_{25}=6$	$-0.900969-i0.433884\|4\rangle$	$1.000000+i0.000001\|4\rangle$	$0.623491-i0.781831\|1\rangle$	
$d=43$, $\|\sigma\rangle=\|1\rangle$	$k=2$, $l=23$	$a_0=17$, $b_0=8$	$s_{11}=40$, $s_{21}=18$	$-0.976076-i0.217431\|3\rangle$	$0.252934-i0.967484\|0\rangle$	$-0.872050+i0.489417\|41\rangle$	$0.391098+i0.920349\|18\rangle$
			$s_{12}=6$, $s_{22}=33$	$-0.976076-i0.217431\|3\rangle$	$0.520941-i0.853593\|9\rangle$	$0.109372-i0.994001\|7\rangle$	
			$s_{13}=0$, $s_{23}=41$	$-0.976076-i0.217431\|3\rangle$	$-0.791497+i0.611173\|3\rangle$	$0.957601-i0.288098\|1\rangle$	
			$s_{14}=18$, $s_{24}=36$	$-0.976076-i0.217431\|3\rangle$	$0.957600+i0.288100\|21\rangle$	$0.520942-i0.853592\|19\rangle$	
			$s_{15}=39$, $s_{25}=9$	$-0.976076-i0.217431\|3\rangle$	$0.520940+i0.853594\|42\rangle$	$0.252932+i0.967484\|40\rangle$	

续表 2

初始参数	加解密密钥	评估初始密钥	评估子密钥	加密结果	评估结果	解密结果	重构结果
$d=101$, $\|\sigma\rangle=\|1\rangle$	$k=27$, $l=21$	$a_0=29$, $b_0=37$	$s_{11}=15$, $s_{21}=27$	$0.261322+i0.965252\|28\rangle$	$-0.350126-i0.936703\|43\rangle$	$-0.108654+i0.994080\|16\rangle$	$-0.667593+i0.744526\|30\rangle$
			$s_{12}=76$, $s_{22}=60$	$0.261322+i0.965252\|28\rangle$	$0.544205-i0.838952\|3\rangle$	$-0.830387-i0.557187\|77\rangle$	
			$s_{13}=41$, $s_{23}=19$	$0.261322+i0.965252\|28\rangle$	$-0.987930+i0.154898\|69\rangle$	$0.379088+i0.925361\|42\rangle$	
			$s_{14}=92$, $s_{24}=89$	$0.261322+i0.965252\|28\rangle$	$0.734059-i0.679086\|19\rangle$	$0.734059-i0.679085\|93\rangle$	
			$s_{15}=7$, $s_{25}=44$	$0.261322+i0.965252\|28\rangle$	$-0.830388+i0.557185\|35\rangle$	$-0.919353+i0.393433\|8\rangle$	

表 1 中列举了 $t=2,n=3$ 情况下,表 2 中列举了 $t=5,n=9$ 情况下 d 维 (t,n) 门限量子同态加密算法中的初始参数、加密密钥、评估初始密钥、评估子密钥、加密结果、评估结果、解密结果和重构结果. 其中初始参数包括量子空间维度 d、初始量子态明文 $|\sigma\rangle$;加解密密钥 k,l;评估密钥 a_0,b_0;评估子密钥 s_{1r},s_{2r};加密结果是以 k,l 为加密密钥,使用加密算法对量子态明文运算之后的结果;评估结果是以 s_{1r},s_{2r} 作为评估子密钥,使用评估算法对量子态密文运算之后的结果;解密结果是以 k,l 为解密密钥,使用解密算法对评估量子态运算之后的结果;重构结果是通过 d 维 CNOT 门对解密的量子态运算之后 0 号粒子的结果,此结果就是评估算法对量子态明文的直接计算结果.

6 总结

本文通过定义一个新的 d 维通用酉算子,构建了一种能够满足通用计算需求的量子同态加密算法. 虽然此算子具有不完全可交换性,但在算法的具体设计上通过调整量子态的相位使得算法恰好满足同态计算的特性. 同时在评估密钥的传输方式上,一改以往的完全共享方式,利用 Shamir(t,n) 门限思想计算其份额,并将份额在网络中传输,避免了评估密钥的泄露,保护了客户端的隐私数据. 从理论层面证明了提出的(t,n)门限量子同态加密算法的正确性,通过对该算法中各个阶段操作过程的仿真实现,进一步验证了算法的正确性.

参考文献

[1] Shor P. Algorithms for quantum computation: discrete logarithms and factoring[A]. 35th Annual Symposium on the Foundations of Computer Science[C]. Los Alamitos, CA: IEEE Press, 1994. 124 – 134.

[2] Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978: 169 – 179.

[3] Gentry C. A fully homomorphic encryption scheme[D]. Stanford: Stanford University, 2009. 1 – 34.

[4] Gentry C. Computing arbitrary functions of encrypted data[J]. Communications of the ACM, 2010, 53(3): 97 – 104.

[5] Castelluccia C, Chan C F, Mykletun E, et al. Efficient and provably secure aggregation of encrypted data in wireless sensor networks[J]. ACM Transactions on Sensor Networks, 2009, 5(3): 1 – 36.

[6] Hessler A, Kakumaru T, Perrey H, et al. Data obfuscation with network coding[J]. Computer Communications, 2012, 35(1): 48 – 61.

[7] Rohde P P, Fitzsimons J F, Gilchrist A. Quantum walks with encrypted data[J]. Physical Review Letters, 2012, 109(15): 150501.

[8] Liang M. Quantum fully homomorphic encryption scheme based on universal quantum circuit[J]. Quantum Information Processing, 2015, 14(8): 2749 – 2759.

[9] Wang Y, She K, Luo Q, et al. Symmetric weak ternary quantum homomorphic encryption schemes[J]. Modern Physics Letters B, 2016, 30(07): 1650076.

[10] Ouyang Y K, Tan S H, Fitzsimons J F. Quantum homomorphic encryption from quantum codes[J]. Physical Review A, 2015, 98: 042334.

[11] Armknecht F, Augot D, Perret L, et al. On constructing homomorphic encryption schemes from coding theory[A]. Cryptography and Coding, 13th IMA International Conference[C]. UK: Oxford, Springer, 2011. 23 – 40.

[12] Liang, M. Symmetric quantum fully homomorphic encryption with perfect security[J]. Quantum Information Processing, 2013, 12(12): 3675 – 3687.

[13] Broadbent A, Jeffery S. Quantum homomorphic encryption for circuits of low T-gate complexity[J]. Quantum Information Processing, 2015, 9216: 609 – 629.

[14] Sun X, Wang T, Sun Z, et al. An efficient quantum some-

what homomorphic symmetric searchable encryption[J]. International Journal of Theoretical Physics,2017,56(4):1335 – 1345.

[15] Min L, Li Y. Quantum fully homomorphic encryption scheme based on quantum fault-tolerant construction[J]. Quantum Information Processing,2016,25:749 – 759.

[16] Shamir A. How to share a secret[J]. Communications of the ACM,1979,22(11):612 – 613.

[17] Thas K. The geometry of generalized Pauli operators of N-qudit Hilbert space,and an application to MUBs[A]. IEEE International Conference on Systems,Man,and Cybernetics[C]. Japanese:IEEE Press,2009. 5:3816 – 3822.

作者简介

宋秀丽(通讯作者)　女,1972 年出生,博士,重庆邮电大学副教授,硕士生导师,计算机学会会员,IEEE 会员. 研究领域包括量子密码学、量子保密通信、云计算安全和车联网安全.
E-mail:songxl@ cqupt. edu. cn

周道洋　男,1992 年出生,在读硕士生. 研究方向为量子密码学,主要研究量子同态加密、量子秘密共享相关协议及其仿真实现.
E-mail:243486249@ qq. com

文爱君　女,1993 年出生,在读硕士生. 研究方向为量子密码学,主要研究量子计算、量子秘密共享相关协议.
E-mail:766705892@ qq. com