基于矩阵作用问题的公钥密码体制抗量子攻击安全性分析

黄华伟
（贵州师范大学数学科学学院，贵州 贵阳 550025）

摘 要：半群作用问题作为离散对数问题的推广，在公钥密码的设计中有着重要应用。通过分析基于整数矩阵乘法半群在交换群直积上的作用问题的公钥密码体制，将矩阵看作直积元素的指数，这类矩阵作用具有类似群的指数运算法则。首先证明了若矩阵作用是单射或隐藏子群的生成元个数小于或等于矩阵阶的平方，则这类矩阵作用问题可在多项式时间归约为矩阵加法群直和的隐藏子群问题。其次证明了交换矩阵作用问题一定可在多项式时间归约为矩阵加法群直和的隐藏子群问题。因此基于这类矩阵作用问题的公钥密码体制无法抵抗量子攻击，该结论对抗量子攻击的公钥密码设计有理论指导意义。

关键词：Shor 算法；隐藏子群问题；半群作用问题；公钥密码；抗量子攻击
中图分类号：TN918.1
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2023064

Security analysis of public-key cryptosystems based on matrix action problem against quantum attack

HUANG Huawei
School of Mathematical Sciences, Guizhou Normal University, Guiyang 550025, China

Abstract: As a generalization of the discrete logarithm problem, semigroup action problem has important applications in the design of public-key cryptography. Public-key cryptosystems based on action problem of integer matrix semigroups on the direct product of commutative groups were analyzed. The matrix was regarded as the exponent of direct product elements, and this class of matrix action had the exponential rules similar to group. It was proved that if the matrix action was injective or the number of generators of the hidden subgroup was less than or equal to the square of the order of the matrix, the matrix action problem could be reduced in polynomial time to the hidden subgroup problem of the direct sum of the additive group of the matrices. And it was proved that commutative matrix action problem could also be reduced to hidden subgroup problem of the direct sum of the additive group of the matrices in polynomial time. The cryptosystems based on this class of matrix action problem cannot against quantum attacks. This conclusion has theoretical significance in the design of public-key cryptography against quantum attacks.

Keywords: Shor’s algorithm, hidden subgroup problem, semigroup action problem, public-key cryptography, against quantum attack

0 引言

大多数公钥密码体制都是基于数学难题建立的，如整数因子分解问题和离散对数问题等，分析这些数学问题的计算复杂度十分重要。在量子计算环境下，Shor 算法[1]相比经典算法达到了指数级加速，能够在多项式时间求解大整数因子分解问题和离散对数问题。除 Shor 算法外，近年来，研究者提出的其他近似优化量子算法，如变分量子算法等在预处理步骤简化布尔变量方程，极大地减少 Shor

收稿日期：2022−10−24；**修回日期：**2023−01−20
基金项目：国家自然科学基金资助项目（No.61462016）；贵州省科学技术基金资助项目（黔科合基础 ZK[2021]一般 313 号）
Foundation Items: The National Natural Science Foundation of China (No.61462016), The Science and Technology Foundation of Guizhou Province (No.ZK[2021]313)

算法所需的量子比特数[2-5]。这些量子算法对目前广泛使用的公钥密码体制构成了潜在威胁，因此具有抗量子攻击的密码体制受到了广泛关注。

目前，抗量子攻击密码体制主要有基于纠错码的密码体制、基于格的密码体制、多变量密码体制、基于 Hash 函数的密码体制、基于椭圆曲线同源问题的密码体制[6-10]。这些密码体制所依赖的数学难题包括伴随式译码问题（校验子译码问题）、最短向量问题、有限域上多元二次多项式方程组求解问题等。其中，大部分数学难题被证明是 NP 困难的，因此这些密码体制被普遍认为具有抗量子攻击的特性。

也有一些学者利用其他数学问题来设计公钥密码体制。例如，文献[11-14]提出了基于半群作用问题的公钥加密方案。文献[15]提出了基于辫群上的共轭链接问题的数字签名方案。文献[16]提出了基于 Bergman 矩阵环分解问题的密钥交换协议。文献[17-18]采用热带半环矩阵分解问题来构造公钥密码体制。那么基于这些数学问题的密码体制是否能抵抗量子攻击？

文献[19-20]将整数因子分解问题和离散对数问题归约为一类更广泛的代数问题，即交换群的隐藏子群问题，并提出推广的 Shor 算法可以在多项式时间求解这类问题。如果一个数学问题能够在多项式时间归约为交换群隐藏子群问题，那么基于此数学问题设计的密码体制就不能抵抗量子攻击。除了因子分解问题和离散对数问题外，还可以有效归约为交换群隐藏子群问题，包括隐藏线性函数问题[21]、解 Pell 方程和主理想问题等[22-23]。此外，Goncalves 等[24]证明了存在有效量子算法求解非交换半直积群 $Z_N \otimes Z_{q^s}$ 的隐藏子群问题。Horan 等[25]回顾了隐藏子群问题量子复杂性的已知结果并讨论了一些基于群结构的后量子密码体制。Suo 等[26]从密码分析的角度讨论了典型密码系统所依赖的数学难题的量子算法，包括整数分解问题、离散对数问题及其变体、格问题、二面体隐藏子群问题等的量子算法设计、算法框架和最新进展。

本文主要分析了文献[11-14]提出的一类公钥密码体制，该体制基于整数矩阵乘法半群在交换群直积上的作用问题，通过研究这种半群作用问题的特点，得出 2 个结论。首先，本文证明了如果矩阵作用是单射或隐藏子群的生成元个数小于或等于矩阵阶的平方，那么这种半群作用问题可以在多项式时间归约为矩阵加法群直和的隐藏子群问题。其次，证明了交换群直积的交换矩阵作用问题一定可以在多项式时间归约为矩阵加法群直和的隐藏子群问题。由于隐藏子群问题存在有效的广义 Shor 算法，本文结果表明，在量子计算机上采用广义 Shor 算法可有效破解这类公钥密码体制。最后，讨论了采用交换半群直积上的矩阵作用问题设计新型抗量子攻击公钥密码体制的可能性。本文研究结果对设计安全的新型后量子密码体制具有一定的理论指导意义。

1　预备知识

设 $G_1,\cdots,G_n$ 是群，在 $G_1,\cdots,G_n$ 的直积

$$G_1\times\cdots\times G_n=\{(g_1,\cdots,g_n)\,|\,g_i\in G_i,1\leqslant i\leqslant n\} \quad (1)$$

上定义运算

$$(g_1,\cdots,g_n)(h_1,\cdots,h_n)=(g_1h_1,\cdots,g_nh_n) \quad (2)$$

则 $G_1\times\cdots\times G_n$ 对此运算构成群，称为 $G_1,\cdots,G_n$ 的直积。若 $G_1=G_2=\cdots=G_n=G$，则 $G_1\times\cdots\times G_n$ 为 G^n。若 $G_1,\cdots,G_n$ 是加法交换群，则 $G_1\times\cdots\times G_n$ 也是交换群，并将其记为 $G_1\oplus\cdots\oplus G_n$，称为 $G_1,\cdots,G_n$ 的直和。

定义 1　半群作用[11-12]。设 T 为半群，X 为非空集合，如果对任意 $t\in T,x\in X$，存在唯一的元素 $t\circ x\in X$ 且满足条件 $\forall t_1,t_2\in T,x\in X$，有 $(t_1t_2)\circ x=t_1\circ(t_2\circ x)$，那么称映射 $T\times X\to X;(t,x)\to t\circ x$ 为半群 T 在集合 X 上的作用。

定义 2　整数矩阵作用[11-12]。令 $\boldsymbol{M}_n(\mathbb{Z})$ 为整数环 $\mathbb{Z}$ 上所有 n 阶方阵，G^n 为交换群 G 的 n 重直积，$\boldsymbol{A}=(a_{ij})_{n\times n}\in\boldsymbol{M}_n(\mathbb{Z})$，$\boldsymbol{g}=(g_1,g_2,\cdots,g_n)\in G^n$，则映射

$$\boldsymbol{M}_n(\mathbb{Z})\times G^n\to G^n$$

$$(\boldsymbol{A},\boldsymbol{g})\to\boldsymbol{A}\circ\boldsymbol{g}=\left(\prod_{j=1}^{n}g_j^{a_{1j}},\prod_{j=1}^{n}g_j^{a_{2j}},\cdots,\prod_{j=1}^{n}g_j^{a_{nj}}\right) \quad (3)$$

是矩阵乘法半群 $\boldsymbol{M}_n(\mathbb{Z})$ 在交换群直积 G^n 上的作用，简称为整数矩阵作用。为表示方便，下文将 $\boldsymbol{A}\circ\boldsymbol{g}$ 记为 $\boldsymbol{g}^{\boldsymbol{A}}$。

定义 3　整数矩阵作用问题[11-12]。令 $\boldsymbol{A}\in\boldsymbol{M}_n(\mathbb{Z})$，$G^n$ 为交换群 G 的 n 重直积，$\boldsymbol{g}\in G^n$，$\boldsymbol{b}=\boldsymbol{g}^{\boldsymbol{A}}$，已知 $\boldsymbol{g},\boldsymbol{b}\in G^n$，求 $\boldsymbol{A}\in\boldsymbol{M}_n(\mathbb{Z})$。

当 n=1 时，整数矩阵作用问题为群上的离散对数问题。因此离散对数问题是整数矩阵作用问题的

一个特例。

引理 1 对任意 $\boldsymbol{A},\boldsymbol{B}\in\boldsymbol{M}_n(\mathbb{Z})$，$\boldsymbol{g}\in G^n$，有

① $(\boldsymbol{g}^{\boldsymbol{A}})^{\boldsymbol{B}}=\boldsymbol{g}^{\boldsymbol{BA}}$；

② $\boldsymbol{g}^{\boldsymbol{A}}\boldsymbol{g}^{\boldsymbol{B}}=\boldsymbol{g}^{\boldsymbol{A}+\boldsymbol{B}}$；

③ $\boldsymbol{g}^{\boldsymbol{A}}\boldsymbol{g}^{-\boldsymbol{B}}=\boldsymbol{g}^{\boldsymbol{A}-\boldsymbol{B}}$。

证明

① 因为 $\boldsymbol{g}^{\boldsymbol{A}}=\boldsymbol{A}\circ\boldsymbol{g}$，且映射

$$\begin{aligned}&\boldsymbol{M}_n(\mathbb{Z})\times G^n\to G^n\\&(\boldsymbol{A},\boldsymbol{g})\to\boldsymbol{A}\circ\boldsymbol{g}\end{aligned}\tag{4}$$

是 $\boldsymbol{M}_n(\mathbb{Z})$ 在 G^n 上的半群作用，根据定义 1 可知 $(\boldsymbol{g}^{\boldsymbol{A}})^{\boldsymbol{B}}=\boldsymbol{g}^{\boldsymbol{BA}}$ 成立。

② 设 $\boldsymbol{A}=(a_{ij})_{n\times n}$，$\boldsymbol{B}=(b_{ij})_{n\times n}$，则

$$\boldsymbol{g}^{\boldsymbol{A}}=\left(\prod_{j=1}^{n}g_j^{a_{1j}},\prod_{j=1}^{n}g_j^{a_{2j}},\cdots,\prod_{j=1}^{n}g_j^{a_{nj}}\right)\tag{5}$$

$$\boldsymbol{g}^{\boldsymbol{B}}=\left(\prod_{j=1}^{n}g_j^{b_{1j}},\prod_{j=1}^{n}g_j^{b_{2j}},\cdots,\prod_{j=1}^{n}g_j^{b_{nj}}\right)\tag{6}$$

因 G 是交换群，从而有

$$\boldsymbol{g}^{\boldsymbol{A}}\boldsymbol{g}^{\boldsymbol{B}}=\left(\prod_{j=1}^{n}g_j^{a_{1j}}\prod_{j=1}^{n}g_j^{b_{1j}},\prod_{j=1}^{n}g_j^{a_{2j}}\prod_{j=1}^{n}g_j^{b_{2j}},\cdots,\prod_{j=1}^{n}g_j^{a_{nj}}\prod_{j=1}^{n}g_j^{b_{nj}}\right)=$$

$$\left(\prod_{j=1}^{n}g_j^{a_{1j}+b_{1j}},\prod_{j=1}^{n}g_j^{a_{2j}+b_{2j}},\cdots,\prod_{j=1}^{n}g_j^{a_{nj}+b_{nj}}\right)=\boldsymbol{g}^{\boldsymbol{A}+\boldsymbol{B}}\tag{7}$$

③ 令 $\boldsymbol{E}$ 为 $\boldsymbol{M}_n(\mathbb{Z})$ 的单位矩阵，由定义 2 可知 $\boldsymbol{g}^{-\boldsymbol{E}}=\left(g_1^{-1},g_2^{-1},\cdots,g_n^{-1}\right)$。由引理 1 中的①可得 $\boldsymbol{g}^{-\boldsymbol{B}}=(\boldsymbol{g}^{-\boldsymbol{E}})^{\boldsymbol{B}}$，再由引理 1 中的由②可得 $\boldsymbol{g}^{\boldsymbol{A}}\boldsymbol{g}^{-\boldsymbol{B}}=\boldsymbol{g}^{\boldsymbol{A}-\boldsymbol{B}}$。证毕。

令 $\boldsymbol{B}\in\boldsymbol{M}_n(\mathbb{Z})$，$\mathbb{Z}[\boldsymbol{B}]=\{p(\boldsymbol{B})\mid p(x)\in\mathbb{Z}[x]\}$，则 $\mathbb{Z}[\boldsymbol{B}]$ 是 $\boldsymbol{M}_n(\mathbb{Z})$ 的交换子环。

定义 4 整数交换矩阵作用问题[12]。令 $\boldsymbol{B}\in\boldsymbol{M}_n(\mathbb{Z})$，$\boldsymbol{A}\in\mathbb{Z}[\boldsymbol{B}]$，$G^n$ 为交换群 G 的 n 重直积，$\boldsymbol{g}\in G^n$，$\boldsymbol{b}=\boldsymbol{g}^{\boldsymbol{A}}$。已知 $\boldsymbol{g},\boldsymbol{b}\in G^n$，求 $\boldsymbol{A}\in\mathbb{Z}[\boldsymbol{B}]$。

定义 5 有限域矩阵作用[13-14]。令 p 为素数，$\boldsymbol{M}_n(\mathbb{Z}_p)$ 为有限域 $\mathbb{Z}_p$ 上所有 n 阶方阵，G^n 为 p 阶交换群 G 的 n 重直积，$\boldsymbol{A}=(a_{ij})_{n\times n}\in\boldsymbol{M}_n(\mathbb{Z}_p)$，$\boldsymbol{g}=(g_1,g_2,\cdots,g_n)\in G^n$，则映射

$$\begin{aligned}&\boldsymbol{M}_n(\mathbb{Z}_p)\times G^n\to G^n(\boldsymbol{A},\boldsymbol{g})\to\boldsymbol{A}*\boldsymbol{g}=\\&\left(\prod_{j=1}^{n}g_j^{a_{1j}},\prod_{j=1}^{n}g_j^{a_{2j}},\cdots,\prod_{j=1}^{n}g_j^{a_{nj}}\right)\end{aligned}\tag{8}$$

是有限域矩阵乘法半群 $\boldsymbol{M}_n(\mathbb{Z}_p)$ 在交换群直积 G^n 上的作用，简称为有限域矩阵作用。为表示方便，在不产生混淆的情况下将 $\boldsymbol{A}*\boldsymbol{g}$ 记为 $\boldsymbol{g}^{\boldsymbol{A}}$。

定义 6 有限域矩阵作用问题[13-14]。令 p 为素数，$\boldsymbol{A}\in\boldsymbol{M}_n(\mathbb{Z}_p)$，$G^n$ 为 p 阶交换群 G 的 n 重直积，$\boldsymbol{g}\in G^n$，$\boldsymbol{b}=\boldsymbol{g}^{\boldsymbol{A}}$。已知 $\boldsymbol{g},\boldsymbol{b}\in G^n$，求 $\boldsymbol{A}\in\boldsymbol{M}_n(\mathbb{Z}_p)$。

引理 2 对任意 $\boldsymbol{A},\boldsymbol{B}\in\boldsymbol{M}_n(\mathbb{Z}_p)$，$\boldsymbol{g}\in G^n$，有

① $(\boldsymbol{g}^{\boldsymbol{A}})^{\boldsymbol{B}}=\boldsymbol{g}^{\boldsymbol{AB}}$；

② $\boldsymbol{g}^{\boldsymbol{A}}\boldsymbol{g}^{\boldsymbol{B}}=\boldsymbol{g}^{\boldsymbol{A}+\boldsymbol{B}}$；

③ $\boldsymbol{g}^{\boldsymbol{A}}\boldsymbol{g}^{-\boldsymbol{B}}=\boldsymbol{g}^{\boldsymbol{A}-\boldsymbol{B}}$。

证明过程与引理 1 的证明类似，此处省略。

令 $\boldsymbol{B}\in\boldsymbol{M}_n(\mathbb{Z}_p)$，$\mathbb{Z}_p[\boldsymbol{B}]=\{p(\boldsymbol{B})\mid p(x)\in\mathbb{Z}_p[x]\}$，同样 $\mathbb{Z}_p[\boldsymbol{B}]$ 是 $\boldsymbol{M}_n(\mathbb{Z}_p)$ 的交换子环。

定义 7 有限域交换矩阵作用问题[13-14]。令 $\boldsymbol{B}\in\boldsymbol{M}_n(\mathbb{Z}_p)$，$\boldsymbol{A}\in\mathbb{Z}_p[\boldsymbol{B}]$，$G^n$ 为 p 阶交换群 G 的 n 重直积，$\boldsymbol{g}\in G^n$，$\boldsymbol{b}=\boldsymbol{g}^{\boldsymbol{A}}$。已知 $\boldsymbol{g},\boldsymbol{b}\in G^n$，求 $\boldsymbol{A}\in\mathbb{Z}_p[\boldsymbol{B}]$。

令 $f:G\to X$ 为加法交换群 $(G,+)$ 到非空集合 X 的映射，$K=\{k\in G\mid f(k+g)=f(g)\forall g\in G\}$，则 K 是 G 的子群，称为映射 f 的对称群（或称为交换群 G 对映射 f 的隐藏子群）。由定义 7 可知，K 刻画了 f 对 G 的群运算的周期。

定义 8 隐藏子群问题[20]。令 G 是交换群，X 是非空集合，$f:G\to X$ 是 G 到 X 的映射。给定 G,X 且存在计算映射 $f:G\to X$ 的有效算法，求群 G 对映射 f 的隐藏子群 K（或求 K 的最小生成子集）。

引理 3[20] 存在推广的 Shor 量子算法可在多项式时间求解交换群的隐藏子群问题。

2 矩阵作用公钥密码

2.1 基于整数交换矩阵作用问题的密钥交换协议

文献[11-12]采用 $\boldsymbol{M}_n(\mathbb{Z})$ 的交换子环 $\mathbb{Z}[\boldsymbol{B}]$，设计了基于整数交换矩阵作用问题的密钥交换协议，具体介绍如下。

公开参数：n 为正整数，$\boldsymbol{B}\in\boldsymbol{M}_n(\mathbb{Z})$，$G^n$ 为交换群 G 的 n 重直积，$\boldsymbol{g}\in G^n$。

1) Alice 随机选取 $\boldsymbol{P}\in\mathbb{Z}[\boldsymbol{B}]$，计算 $\boldsymbol{k}_1=\boldsymbol{g}^{\boldsymbol{P}}$ 并将其发送给 Bob。

2) Bob 随机选取 $\boldsymbol{Q}\in\mathbb{Z}[\boldsymbol{B}]$，计算 $\boldsymbol{k}_2=\boldsymbol{g}^{\boldsymbol{Q}}$ 并将其发送给 Alice。

3) Alice 计算 $\boldsymbol{k}_2^{\boldsymbol{P}}$，Bob 计算 $\boldsymbol{k}_1^{\boldsymbol{Q}}$，并得到共享密钥 $\boldsymbol{k}=\boldsymbol{k}_1^{\boldsymbol{Q}}=\boldsymbol{g}^{\boldsymbol{PQ}}=\boldsymbol{g}^{\boldsymbol{QP}}=\boldsymbol{k}_2^{\boldsymbol{P}}$。

2.2　基于有限域交换矩阵作用问题的广义 ElGamal 公钥加密方案

基于有限域 Z_p 上的交换矩阵作用问题，文献[13-14]设计了广义 ElGamal 公钥加密方案、广义 Cramer-Shoup 公钥加密方案、广义 Naor-Reingold 伪随机函数和广义 BHHO 加密方案等标准模型下可证明安全的公钥密码体制。下面仅以广义 ElGamal 公钥加密方案为例进行介绍，其他方案详见文献[13-14]。

密钥生成。n 为正整数，$\boldsymbol{B}\in\boldsymbol{M}_n(\mathbb{Z}_p)$，$G^n$ 为 p 阶交换群 G 的 n 重直积，$\boldsymbol{g}\in G^n$。随机选取 $\boldsymbol{A}\in\mathbb{Z}_p[\boldsymbol{B}]$，计算 $\boldsymbol{b}=\boldsymbol{g}^{\boldsymbol{A}}$，则 Alice 的公钥为 $\boldsymbol{b}=\boldsymbol{g}^{\boldsymbol{A}}$，Alice 的私钥为 $\boldsymbol{A}$。

加密。假设 Bob 要发送明文消息 $\boldsymbol{m}\in G^n$ 给 Alice，则随机选取 $\boldsymbol{R}\in\mathbb{Z}_p[\boldsymbol{B}]$，计算 $\boldsymbol{e}=\boldsymbol{g}^{\boldsymbol{R}}$，$\boldsymbol{c}=\boldsymbol{b}^{\boldsymbol{R}}\boldsymbol{m}$，然后将密文 $\mathrm{CT}=(\boldsymbol{e},\boldsymbol{c})$ 发送给 Alice。

解密。Alice 收到密文 $\mathrm{CT}=(\boldsymbol{e},\boldsymbol{c})\in G^n\times G^n$，计算 $\boldsymbol{c}(\boldsymbol{e}^{\boldsymbol{A}})^{-1}$ 即得到明文消息 $\boldsymbol{m}$。

3　整数矩阵作用问题归约隐藏子群问题

定理 1　令 $\boldsymbol{g}\in G^n$，若映射 $\sigma:\boldsymbol{M}_n(\mathbb{Z})\to G^n,\ \boldsymbol{A}\to\boldsymbol{g}^{\boldsymbol{A}}$ 是单射，则其对应的整数矩阵作用问题可在多项式时间归约为交换群 $\boldsymbol{M}_n(\mathbb{Z})\oplus\boldsymbol{M}_n(\mathbb{Z})$ 的隐藏子群问题，其中，$\boldsymbol{M}_n(\mathbb{Z})\oplus\boldsymbol{M}_n(\mathbb{Z})$ 为整数矩阵加法群 $(\boldsymbol{M}_n(\mathbb{Z}),+)$ 的二重直和。

证明　假设存在有效求解隐藏子群问题的算法 $\mathcal{A}$，已知 $\boldsymbol{g},\boldsymbol{b}=\boldsymbol{g}^{\boldsymbol{A}}\in G^n$，下面调用 $\mathcal{A}$ 求 $\boldsymbol{A}\in\boldsymbol{M}_n(\mathbb{Z})$。

构造函数

$$f:\boldsymbol{M}_n(\mathbb{Z})\oplus\boldsymbol{M}_n(\mathbb{Z})\to G^n$$
$$f(\boldsymbol{X},\boldsymbol{Y})=\boldsymbol{g}^{\boldsymbol{X}}\boldsymbol{b}^{-\boldsymbol{Y}}\tag{9}$$

由引理 2 可知，$f(\boldsymbol{X},\boldsymbol{Y})=\boldsymbol{g}^{\boldsymbol{X}-\boldsymbol{AY}}$，因此

$$f(\boldsymbol{X}_1,\boldsymbol{Y}_1)=f(\boldsymbol{X}_2,\boldsymbol{Y}_2)\Leftrightarrow\boldsymbol{g}^{\boldsymbol{X}_1-\boldsymbol{AY}_1}=\boldsymbol{g}^{\boldsymbol{X}_2-\boldsymbol{AY}_2}\Leftrightarrow$$
$$\boldsymbol{X}_1-\boldsymbol{AY}_1=\boldsymbol{X}_2-\boldsymbol{AY}_2\quad(\text{因}\sigma\text{是单射})\Leftrightarrow$$
$$\boldsymbol{X}_2=\boldsymbol{X}_1+\boldsymbol{A}(\boldsymbol{Y}_2-\boldsymbol{Y}_1)\Leftrightarrow(\exists\boldsymbol{B}\in\boldsymbol{M}_n(\mathbb{Z}))$$
$$\begin{cases}\boldsymbol{X}_2=\boldsymbol{X}_1+\boldsymbol{AB}\\ \boldsymbol{Y}_2=\boldsymbol{Y}_1+\boldsymbol{B}\end{cases}\Leftrightarrow$$
$$\exists\boldsymbol{B}\in\boldsymbol{M}_n(\mathbb{Z}),\text{使}(\boldsymbol{X}_2,\boldsymbol{Y}_2)=(\boldsymbol{X}_1,\boldsymbol{Y}_1)+(\boldsymbol{A},\boldsymbol{E})\boldsymbol{B}\tag{10}$$

设 K 为交换群 $\boldsymbol{M}_n(\mathbb{Z})\oplus\boldsymbol{M}_n(\mathbb{Z})$ 对映射 f 的隐藏子群，由 K 的定义及式(10)可知

$$K=\{(\boldsymbol{A},\boldsymbol{E})\boldsymbol{B}\mid\boldsymbol{B}\in\boldsymbol{M}_n(\mathbb{Z})\}\tag{11}$$

易见，$(\boldsymbol{A},\boldsymbol{E})\in K$ 但不一定是 K 的生成元。

对函数 $f(\boldsymbol{X},\boldsymbol{Y})=\boldsymbol{g}^{\boldsymbol{X}}\boldsymbol{b}^{-\boldsymbol{Y}}$ 调用算法 $\mathcal{A}$，求 $\boldsymbol{M}_n(\mathbb{Z})\oplus\boldsymbol{M}_n(\mathbb{Z})$ 隐藏子群 K 的最小生成集

$$\{(\boldsymbol{AB}_1,\boldsymbol{B}_1),(\boldsymbol{AB}_2,\boldsymbol{B}_2),\cdots,(\boldsymbol{AB}_t,\boldsymbol{B}_t)\}\tag{12}$$

由于 $(\boldsymbol{A},\boldsymbol{E})\in K$ 是固定的，因此有 $(K,+)\cong(\boldsymbol{M}_n(\mathbb{Z}),+)$。而矩阵加法群 $(\boldsymbol{M}_n(\mathbb{Z}),+)$ 同构于整数加法群的 n^2 重直和 $(\mathbb{Z}^{n^2},+)$。因此 $(K,+)\cong(\mathbb{Z}^{n^2},+)$，且 K 的生成元个数 $t=n^2$。$\{(\boldsymbol{AB}_1,\boldsymbol{B}_1),(\boldsymbol{AB}_2,\boldsymbol{B}_2),\cdots,(\boldsymbol{AB}_t,\boldsymbol{B}_t)\}$ 是 K 的生成集且 $(\boldsymbol{A},\boldsymbol{E})\in K$，那么存在 $\lambda_1,\lambda_2,\cdots,\lambda_{n^2}\in\mathbb{Z}$

$$(\boldsymbol{A},\boldsymbol{E})=\lambda_1(\boldsymbol{AB}_1,\boldsymbol{B}_1)+$$
$$\lambda_2(\boldsymbol{AB}_2,\boldsymbol{B}_2)+\cdots+\lambda_{n^2}(\boldsymbol{AB}_{n^2},\boldsymbol{B}_{n^2})\tag{13}$$

可得

$$\begin{cases}\lambda_1\boldsymbol{AB}_1+\lambda_2\boldsymbol{AB}_2+\cdots+\lambda_{n^2}\boldsymbol{AB}_{n^2}=\boldsymbol{A}\\ \lambda_1\boldsymbol{B}_1+\lambda_2\boldsymbol{B}_2+\cdots+\lambda_{n^2}\boldsymbol{B}_{n^2}=\boldsymbol{E}\end{cases}\tag{14}$$

$\{(\boldsymbol{AB}_1,\boldsymbol{B}_1),(\boldsymbol{AB}_2,\boldsymbol{B}_2),\cdots,(\boldsymbol{AB}_{n^2},\boldsymbol{B}_{n^2})\}$ 是 K 的最小生成集，$\boldsymbol{B}_1,\boldsymbol{B}_2,\cdots,\boldsymbol{B}_{n^2}$ 是线性无关的，而 $\boldsymbol{B}_1,\boldsymbol{B}_2,\cdots,\boldsymbol{B}_{n^2},\boldsymbol{E}$ 是线性相关的。因此以矩阵 $\boldsymbol{B}_1,\boldsymbol{B}_2,\cdots,\boldsymbol{B}_{n^2},\boldsymbol{E}$ 作为列向量的矩阵 $(\boldsymbol{B}_1,\boldsymbol{B}_2,\cdots,\boldsymbol{B}_{n^2})$ 和 $(\boldsymbol{B}_1,\boldsymbol{B}_2,\cdots,\boldsymbol{B}_{n^2},\boldsymbol{E})$ 具有相同的秩。根据 $\lambda_1\boldsymbol{B}_1+\lambda_2\boldsymbol{B}_2+\cdots+\lambda_{n^2}\boldsymbol{B}_{n^2}=\boldsymbol{E}$，求解线性方程组（$n^2$ 个未知数，n^2 个方程且系数矩阵与增广矩阵有相同的秩），解得 $\lambda_1,\lambda_2,\cdots,\lambda_{n^2}$，再代入 $\lambda_1\boldsymbol{AB}_1+\lambda_2\boldsymbol{AB}_2+\cdots+\lambda_{n^2}\boldsymbol{AB}_{n^2}=\boldsymbol{A}$ 可求得 $\boldsymbol{A}$，即解决了整数矩阵作用问题。

采用高斯消元法，由 $\lambda_1\boldsymbol{B}_1+\lambda_2\boldsymbol{B}_2+\cdots+\lambda_{n^2}\boldsymbol{B}_{n^2}=\boldsymbol{E}$ 求解 $\lambda_1,\lambda_2,\cdots,\lambda_{n^2}$ 的计算复杂度为 $O(n^6)$，代入 $\lambda_1\boldsymbol{AB}_1+\lambda_2\boldsymbol{AB}_2+\cdots+\lambda_{n^2}\boldsymbol{AB}_{n^2}=\boldsymbol{A}$ 求 $\boldsymbol{A}$ 只需 n^2 次矩阵数乘运算和 n^2 次矩阵加法。证毕。

推论 1　无限循环群上的离散对数问题可在多项式时间归约为交换群 $\mathbb{Z}\oplus\mathbb{Z}$ 的隐藏子群问题。

证明　令 g 为无限循环群 G 的生成元，$h\in G$。已知 g 和 h，对应的离散对数问题即求 $k\in\mathbb{Z}$ 使 $h=g^k$。

该问题为整数矩阵作用问题在 n=1 时的一个特例。因 g 为 G 的生成元，此时映射 $\sigma:\mathbb{Z}\to G,k\to g^k$ 是单射。由定理 1 可知，该问题可在多项式时间归

约为交换群 $\mathbb{Z}\oplus\mathbb{Z}$ 的隐藏子群问题。证毕。

定理 2 若交换群 $\boldsymbol{M}_n(\mathbb{Z})\oplus\boldsymbol{M}_n(\mathbb{Z})$ 对函数 $f(\boldsymbol{X},\boldsymbol{Y})=\boldsymbol{g}^{\boldsymbol{X}}\boldsymbol{b}^{-\boldsymbol{Y}}$ 的隐藏子群的最小生成子集元素个数小于或等于 n^2，则整数矩阵作用问题可在多项式时间归约为交换群 $\boldsymbol{M}_n(\mathbb{Z})\oplus\boldsymbol{M}_n(\mathbb{Z})$ 的隐藏子群问题。

证明 假设存在有效求解隐藏子群问题的算法 $\mathcal{A}$，已知 $\boldsymbol{g}$，$\boldsymbol{b}=\boldsymbol{g}^{\boldsymbol{A}}\in G^n$，下面调用 $\mathcal{A}$ 求 $\boldsymbol{A}\in\boldsymbol{M}_n(\mathbb{Z})$。

与定理 1 类似，有 $f(\boldsymbol{X},\boldsymbol{Y})=\boldsymbol{g}^{\boldsymbol{X}-\boldsymbol{AY}}$。设 $\lambda\in\mathbb{Z}$，$\boldsymbol{X}_1,\boldsymbol{Y}_1,\boldsymbol{X}_2,\boldsymbol{Y}_2\in\boldsymbol{M}_n(\mathbb{Z})$，则

$$(\boldsymbol{X}_2,\boldsymbol{Y}_2)=(\boldsymbol{X}_1,\boldsymbol{Y}_1)+\lambda(\boldsymbol{A},\boldsymbol{E})\Rightarrow\begin{cases}\boldsymbol{X}_2=\boldsymbol{X}_1+\lambda\boldsymbol{A}\\ \boldsymbol{Y}_2=\boldsymbol{Y}_1+\lambda\boldsymbol{E}\end{cases}\Rightarrow$$
$$\boldsymbol{X}_2=\boldsymbol{X}_1+\boldsymbol{A}(\boldsymbol{Y}_2-\boldsymbol{Y}_1)\Rightarrow\boldsymbol{X}_1-\boldsymbol{AY}_1=\boldsymbol{X}_2-\boldsymbol{AY}_2\Rightarrow$$
$$\boldsymbol{g}^{\boldsymbol{X}_1-\boldsymbol{AY}_1}=\boldsymbol{g}^{\boldsymbol{X}_2-\boldsymbol{AY}_2}\Rightarrow f(\boldsymbol{X}_1,\boldsymbol{Y}_1)=f(\boldsymbol{X}_2,\boldsymbol{Y}_2)\tag{15}$$

设 K 为交换群 $\boldsymbol{M}_n(\mathbb{Z})\oplus\boldsymbol{M}_n(\mathbb{Z})$ 对映射 f 的隐藏子群，由 K 的定义及式(15)可知

$$\{\lambda(\boldsymbol{A},\boldsymbol{E})\mid\lambda\in\mathbb{Z}\}=\langle(\boldsymbol{A},\boldsymbol{E})\rangle\subseteq K\tag{16}$$

同样 $(\boldsymbol{A},\boldsymbol{E})\in K$，但不一定是 K 的生成元。

对函数 $f(\boldsymbol{X},\boldsymbol{Y})=\boldsymbol{g}^{\boldsymbol{X}}\boldsymbol{b}^{-\boldsymbol{Y}}$ 调用算法 $\mathcal{A}$，求 $\boldsymbol{M}_n(\mathbb{Z})\oplus\boldsymbol{M}_n(\mathbb{Z})$ 隐藏子群 K 的最小生成集

$$\{(\boldsymbol{A}_1,\boldsymbol{B}_1),(\boldsymbol{A}_2,\boldsymbol{B}_2),\cdots,(\boldsymbol{A}_t,\boldsymbol{B}_t)\}\tag{17}$$

根据定理条件 $t\leqslant n^2$，如果 $(\boldsymbol{A},\boldsymbol{E})\in K$，那么存在 $\lambda_1,\lambda_2,\cdots,\lambda_t\in\mathbb{Z}$，满足

$$(\boldsymbol{A},\boldsymbol{E})=\lambda_1(\boldsymbol{A}_1,\boldsymbol{B}_1)+\lambda_2(\boldsymbol{A}_2,\boldsymbol{B}_2)+\cdots+\lambda_t(\boldsymbol{A}_t,\boldsymbol{B}_t)\tag{18}$$

因此，有

$$\begin{cases}\lambda_1\boldsymbol{A}_1+\lambda_2\boldsymbol{A}_2+\cdots+\lambda_t\boldsymbol{A}_t=\boldsymbol{A}\\ \lambda_1\boldsymbol{B}_1+\lambda_2\boldsymbol{B}_2+\cdots+\lambda_t\boldsymbol{B}_t=\boldsymbol{E}\end{cases}\tag{19}$$

由于 $\{(\boldsymbol{A}_1,\boldsymbol{B}_1),(\boldsymbol{A}_2,\boldsymbol{B}_2),\cdots,(\boldsymbol{A}_t,\boldsymbol{B}_t)\}$ 是 K 的最小生成集，$\boldsymbol{B}_1,\boldsymbol{B}_2,\cdots,\boldsymbol{B}_t$ 是线性无关的，而 $\boldsymbol{B}_1,\boldsymbol{B}_2,\cdots,\boldsymbol{B}_t,\boldsymbol{E}$ 是线性相关的。因此以矩阵 $\boldsymbol{B}_1,\boldsymbol{B}_2,\cdots,\boldsymbol{B}_t,\boldsymbol{E}$ 作为列向量的矩阵 $(\boldsymbol{B}_1,\boldsymbol{B}_2,\cdots,\boldsymbol{B}_t)$ 和 $(\boldsymbol{B}_1,\boldsymbol{B}_2,\cdots,\boldsymbol{B}_t,\boldsymbol{E})$ 具有相同的秩。根据 $\lambda_1\boldsymbol{A}_1+\lambda_2\boldsymbol{A}_2+\cdots+\lambda_t\boldsymbol{A}_t=\boldsymbol{A}$，求解线性方程组（$t$ 个未知数，n^2 个方程且系数矩阵与增广矩阵有相同的秩），可求得 $\lambda_1,\lambda_2,\cdots,\lambda_t$，代入 $\lambda_1\boldsymbol{B}_1+\lambda_2\boldsymbol{B}_2+\cdots+\lambda_t\boldsymbol{B}_t=\boldsymbol{E}$ 即得 $\boldsymbol{A}$，即解决了整数矩阵作用问题。

采用高斯消元法，由 $\lambda_1\boldsymbol{A}_1+\lambda_2\boldsymbol{A}_2+\cdots+\lambda_t\boldsymbol{A}_t=\boldsymbol{A}$ 求解 $\lambda_1,\lambda_2,\cdots,\lambda_t$ 的计算复杂度为 $O(n^6)$，代入 $\lambda_1\boldsymbol{B}_1+\lambda_2\boldsymbol{B}_2+\cdots+\lambda_t\boldsymbol{B}_t=\boldsymbol{E}$ 求 $\boldsymbol{A}$ 只需 t 次矩阵数乘运算和 t 次矩阵加法。证毕。

推论 2 令 $\boldsymbol{B}\in\boldsymbol{M}_n(\mathbb{Z})$，$\boldsymbol{A}\in\mathbb{Z}[\boldsymbol{B}]$，$G^n$ 为交换群 G 的 n 重直积，$\boldsymbol{g}\in G^n$，$\boldsymbol{b}=\boldsymbol{g}^{\boldsymbol{A}}$。则当 $n\geqslant 2$ 时，其对应的整数交换矩阵作用问题可在多项式时间归约为交换群 $\mathbb{Z}[\boldsymbol{B}]\oplus\mathbb{Z}[\boldsymbol{B}]$ 的隐藏子群问题，其中，$\mathbb{Z}[\boldsymbol{B}]\oplus\mathbb{Z}[\boldsymbol{B}]$ 为矩阵加法群 $\mathbb{Z}[\boldsymbol{B}]$ 的二重直和。

证明 与定理 2 类似，只需证明定理 2 的条件此时一定成立。考虑交换群 $\mathbb{Z}[\boldsymbol{B}]\oplus\mathbb{Z}[\boldsymbol{B}]$ 对函数 $f(\boldsymbol{X},\boldsymbol{Y})=\boldsymbol{g}^{\boldsymbol{X}}\boldsymbol{b}^{-\boldsymbol{Y}}$ 的隐藏子群 K 的最小生成子集元素个数。根据凯莱–哈密顿定理，有

$$\mathbb{Z}[\boldsymbol{B}]=\{a_0\boldsymbol{E}+a_1\boldsymbol{B}+\cdots+a_{n-1}\boldsymbol{B}^{n-1}\mid a_i\in\mathbb{Z}\}\tag{20}$$

可知 $(\mathbb{Z}[\boldsymbol{B}],+)$ 的生成元个数小于或等于 n，从而 $\mathbb{Z}[\boldsymbol{B}]\oplus\mathbb{Z}[\boldsymbol{B}]$ 的生成元个数小于或等于 $2n$。由于隐藏子群 K 是 $\mathbb{Z}[\boldsymbol{B}]\oplus\mathbb{Z}[\boldsymbol{B}]$ 的子群，其生成元的个数也必然小于或等于 $2n$。注意到，当 $n\geqslant 2$ 时，$2n\leqslant n^2$。因此由定理 2 可知，结论成立。证毕。

推论 3 基于整数交换矩阵作用问题的密码体制不能抵抗量子攻击。

证明 由推论 2 和引理 3 可得。证毕。

根据推论 3，文献[11-12]提出的基于整数交换矩阵作用问题的公钥密码体制不能抵抗量子攻击。

4 有限域矩阵作用问题归约隐藏子群问题

定理 3 令 $\boldsymbol{g}\in G^n$，若映射 $\sigma:\boldsymbol{M}_n(\mathbb{Z}_p)\to G^n$，$A\to\boldsymbol{g}^A$ 是单射，则其对应的有限域矩阵作用问题可在多项式时间归约为交换群 $\boldsymbol{M}_n(\mathbb{Z}_p)\oplus\boldsymbol{M}_n(\mathbb{Z}_p)$ 的隐藏子群问题，其中，$\boldsymbol{M}_n(\mathbb{Z}_p)\oplus\boldsymbol{M}_n(\mathbb{Z}_p)$ 为有限域矩阵加法群 $\boldsymbol{M}_n(\mathbb{Z}_p)$ 的二重直和。

证明 证明过程与定理 1 类似，只需将定理 1 证明中的 $\boldsymbol{M}_n(\mathbb{Z})$ 换成 $\boldsymbol{M}_n(\mathbb{Z}_p)$，$\mathbb{Z}$ 换成 $\mathbb{Z}_p$。证毕。

推论 4 令 p 为素数，则 p 阶循环群上的离散对数问题可在多项式时间归约为交换群 $\mathbb{Z}_p\oplus\mathbb{Z}_p$ 的隐藏子群问题。

证明 令 g 为 p 阶循环群 G 的生成元，$h\in G$。已知 g 和 h，对应的离散对数问题即求 $k\in\mathbb{Z}_p$ 使 $h=g^k$。

该问题为有限域矩阵作用问题在 n=1 时的特例。因 g 为 G 的生成元，映射 $\sigma:\mathbb{Z}_p\to G,k\to g^k$ 是单射。由定理 3 可知，该问题可在多项式时间归约为交换群 $\mathbb{Z}_p\oplus\mathbb{Z}_p$ 的隐藏子群问题。证毕。

定理 4　若交换群 $\boldsymbol{M}_n(\mathbb{Z}_p)\oplus\boldsymbol{M}_n(\mathbb{Z}_p)$ 对函数 $f(\boldsymbol{X},\boldsymbol{Y})=\boldsymbol{g}^{\boldsymbol{X}}\boldsymbol{b}^{-\boldsymbol{Y}}$ 的隐藏子群的最小生成子集的元素个数小于或等于 n^2，则有限域矩阵作用问题可在多项式时间归约为交换群 $\boldsymbol{M}_n(\mathbb{Z}_p)\oplus\boldsymbol{M}_n(\mathbb{Z}_p)$ 的隐藏子群问题。

证明　证明过程与定理 2 类似，只需将定理 2 证明中的 $\boldsymbol{M}_n(\mathbb{Z})$ 换成 $\boldsymbol{M}_n(\mathbb{Z}_p)$，$\mathbb{Z}$ 换成 $\mathbb{Z}_p$。证毕。

推论 5　令 $\boldsymbol{B}\in\boldsymbol{M}_n(\mathbb{Z}_p)$，$\boldsymbol{A}\in\mathbb{Z}_p[\boldsymbol{B}]$，$G^n$ 为 p 阶交换群 G 的 n 重直积，$\boldsymbol{g}\in G^n$，$\boldsymbol{b}=\boldsymbol{g}^{\boldsymbol{A}}$。则当 $n\geqslant 2$ 时，其对应的有限域交换矩阵作用问题可在多项式时间归约为交换群 $\mathbb{Z}_p[\boldsymbol{B}]\oplus\mathbb{Z}_p[\boldsymbol{B}]$ 的隐藏子群问题，其中，$\mathbb{Z}_p[\boldsymbol{B}]\oplus\mathbb{Z}_p[\boldsymbol{B}]$ 为矩阵加法群 $\mathbb{Z}_p[\boldsymbol{B}]$ 的二重直和。

证明　证明过程与定理 4 类似，只需证明定理 4 的条件此时一定成立。考虑交换群 $\mathbb{Z}_p[\boldsymbol{B}]\oplus\mathbb{Z}_p[\boldsymbol{B}]$ 对函数 $f(\boldsymbol{X},\boldsymbol{Y})=\boldsymbol{g}^{\boldsymbol{X}}\boldsymbol{b}^{-\boldsymbol{Y}}$ 的隐藏子群 K 的最小生成子集元素个数。根据凯莱–哈密顿定理，有

$$\mathbb{Z}_p[\boldsymbol{B}]=\left\{a_0\boldsymbol{E}+a_1\boldsymbol{B}+\cdots+a_{n-1}\boldsymbol{B}^{n-1}\mid a_i\in\mathbb{Z}_p\right\}\tag{21}$$

可知 $\left(\mathbb{Z}_p[\boldsymbol{B}],+\right)$ 的生成元个数小于或等于 n，从而 $\mathbb{Z}_p[\boldsymbol{B}]\oplus\mathbb{Z}_p[\boldsymbol{B}]$ 的生成元个数小于或等于 $2n$。由于隐藏子群 K 是 $\mathbb{Z}_p[\boldsymbol{B}]\oplus\mathbb{Z}_p[\boldsymbol{B}]$ 的子群，其生成元的个数也必然小于或等于 $2n$。注意到，当 $n\geqslant 2$ 时，$2n\leqslant n^2$。因此由定理 4 可知，结论成立。证毕。

推论 6　基于有限域交换矩阵作用问题的密码体制不能抵抗量子攻击。

证明　由推论 5 和引理 3 可得。证毕。

根据推论 6，文献[13-14]提出的基于有限域交换矩阵作用问题的广义 Diffie-Hellman 密钥交换协议、广义 ElGamal 公钥加密方案、广义 Cramer-Shoup 公钥加密方案、广义 Naor-Reingold 伪随机函数和广义 BHHO 加密方案等公钥密码体制都不能抵抗量子攻击。

采用离散对数问题或矩阵作用问题设计的密码主要用到了性质 $(\boldsymbol{g}^{\boldsymbol{x}})^{\boldsymbol{y}}=\boldsymbol{g}^{\boldsymbol{xy}}$（矩阵作用中 $\boldsymbol{g}$ 是向量，$\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是矩阵），其中指数是乘积形式，指数所在的代数结构关于乘法都是半群（分别是 $(\mathbb{Z}_{p-1},\times),(\mathbb{Z}[\boldsymbol{B}],\times),(\mathbb{Z}_p[\boldsymbol{B}],\times)$）。但是归约到隐藏子群问题的证明是利用性质 $\boldsymbol{g}^{\boldsymbol{x}}\boldsymbol{g}^{\boldsymbol{y}}=\boldsymbol{g}^{\boldsymbol{x}+\boldsymbol{y}}$，即幂的乘积转化为指数的加法，将问题归约为指数所在加法群（分别是 $(\mathbb{Z}_{p-1},+),(\mathbb{Z}[\boldsymbol{B}],+),(\mathbb{Z}_p[\boldsymbol{B}],+)$）直和的隐藏子群问题。

如果将交换群 G 换成交换半群 S，那么 S^n 上的矩阵作用问题能否归约为隐藏子群问题？由于在半群中不是所有元素都有逆元，此时 $\boldsymbol{g}^{-\boldsymbol{E}}=\left(g_1^{-1},g_2^{-1},\cdots,g_n^{-1}\right)$ 没有意义，引理 1 的③和引理 2 的③不再成立，因此无法再采用类似方法研究该问题（$f(\boldsymbol{X},\boldsymbol{Y})=\boldsymbol{g}^{\boldsymbol{X}}\boldsymbol{b}^{-\boldsymbol{Y}}$ 没有意义）。交换半群直积上的整数矩阵作用问题的计算复杂度有待进一步研究。

文献[27]证明了半群的离散对数问题可以归约为群的离散对数问题，但该归约不是多项式时间的。文献[28-29]研究了半群上离散对数问题求解算法的计算复杂度，目前求解半群上的非平凡离散对数问题的算法都是指数时间的，对该问题没有发现存在有效量子计算机算法（或传统计算机算法）。半群上的离散对数问题是半群直积上的矩阵作用问题的一个特例，因此基于半群直积上的矩阵作用问题有可能设计具有抗量子攻击的新型公钥密码体制。

5　结束语

在量子计算机上，Shor 量子算法可以在多项式时间内求解整数因子分解问题和离散对数问题，推广的 Shor 量子算法可以在多项式时间内求解更一般的交换群隐藏子群问题。本文分析了整数（有限域）矩阵半群在交换群直积的作用问题，证明了如果矩阵作用是单射或隐藏子群的生成元个数小于或等于 n^2，那么这类数学问题可以在多项式时间归约为整数（有限域）矩阵加法群直和的隐藏子群问题，从而存在量子算法可以在多项式时间求解该问题。由于文献[11-14]中用到的矩阵作用问题的隐藏子群生成元个数都小于或等于 n^2，因此文献[11-14]提出的基于整数（有限域）矩阵半群的密码体制都无法抵抗量子攻击。

参考文献：

[1] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Journal on Computing, 1997, 26(5): 1484-1509.

[2] MONTANARO A. Quantum algorithms: an overview[J]. NPJ Quantum Information, 2016, 2(1): 1-8.

[3] ANSCHUETZ E, OLSON J, ASPURU-GUZIK A, et al. Variational quantum factoring[C]//Quantum Technology and Optimization Prob-

lems. Berlin: Springer, 2019: 74-85.

[4] GYONGYOSI L, IMRE S. A survey on quantum computing technology[J]. Computer Science Review, 2019, 31: 51-71.

[5] DALEY A J, BLOCH I, KOKAIL C, et al. Practical quantum advantage in quantum simulation[J]. Nature, 2022, 607(7920): 667-676.

[6] 王丽萍, 戚艳红. 基于编码的后量子公钥密码研究进展[J]. 信息安全学报, 2019, 4(2): 20-28.
WANG L P, QI Y H. Recent progress of code-based post-quantum public key cryptography[J]. Journal of Cyber Security, 2019, 4(2): 20-28.

[7] 王小云, 刘明洁. 格密码学研究[J]. 密码学报, 2014, 1(1): 13-27.
WANG X Y, LIU M J. Survey of lattice-based cryptography[J]. Journal of Cryptologic Research, 2014, 1(1): 13-27.

[8] ASIF R. Post-quantum cryptosystems for Internet-of-things: a survey on lattice-based algorithms[J]. IoT, 2021, 2(1): 71-91.

[9] 郁昱. 后量子密码专栏序言[J]. 密码学报, 2017, 4(5): 472-473.
YU Y. Preface to post-quantum cryptography column[J]. Journal of Cryptologic Research, 2017, 4(5): 472-473.

[10] BERNSTEIN D J, BUCHMANN J, DAHMEN E. Post-quantum cryptography[M]. Berlin: Springer, 2009.

[11] MAZE G, MONICO C, ROSENTHAL J. A public key cryptosystem based on actions by semigroups[C]//Proceedings of the IEEE International Symposium on Information Theory. Piscataway: IEEE Press, 2004: 266.

[12] MAZE G, MONICO C, ROSENTHAL J, et al. Public key cryptography based on semigroup actions[J]. Advances in Mathematics of Communications, 2007, 1(4): 489-507.

[13] HUANG H W, YANG B, ZHU S L, et al. Generalized ElGamal public key cryptosystem based on a new Diffie-Hellman problem[C]//International Conference on Provable Security. Berlin: Springer, 2008: 1-21.

[14] CRAMER R, DAMGARD I, KILTZ E, et al. DDH-like assumptions based on extension rings[C]//International Workshop on Public Key Cryptography. Berlin: Springer, 2012: 644-661.

[15] WANG L C, WANG L H, CAO Z F, et al. Conjugate adjoining problem in braid groups and new design of braid-based signatures[J]. Science China Information Sciences, 2010, 53(3): 524-536.

[16] CLIMENT J J, NAVARRO P R, TORTOSA L. An extension of the noncommutative Bergman's ring with a large number of noninvertible elements[J]. Applicable Algebra in Engineering, Communication and Computing, 2014, 25(5): 347-361.

[17] GRIGORIEV D, SHPILRAIN V. Tropical cryptography[J]. Communications in Algebra, 2014, 42(6): 2624-2632.

[18] GRIGORIEV D, SHPILRAIN V. Tropical cryptography II: extensions by homomorphisms[J]. Communications in Algebra, 2019, 47(10): 4224-4229.

[19] EKERT A, JOZSA R. Quantum computation and Shor's factoring algorithm[J]. Reviews of Modern Physics, 1996, 68(3): 733-753.

[20] JOZSA R. Quantum factoring, discrete logarithms, and the hidden subgroup problem[J]. Computing in Science & Engineering, 2001, 3(2): 34-43.

[21] BONEH D, LIPTON R J. Quantum cryptanalysis of hidden linear functions[C]//Advances in Cryptology — CRYPT0' 95. Berlin: Springer, 1995: 424-437.

[22] HALLGREN S. Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem[J]. Journal of the ACM, 2007, 54(1): 1-19.

[23] AMBAINIS A. New developments in quantum algorithms[C]//International Symposium on Mathematical Foundations of Computer Science. Berlin: Springer, 2010: 1-11.

[24] GONCALVES D N, FERNANDES T, COSME C. An efficient quantum algorithm for the hidden subgroup problem over some non-abelian groups[J]. Tema, 2017, 18(2): 215-223.

[25] HORAN K, KAHROBAEI D. The hidden subgroup problem and post-quantum group-based cryptography[C]//International Congress on Mathematical Software. Berlin: Springer, 2018: 218-226.

[26] SUO J W, WANG L C, YANG S J, et al. Quantum algorithms for typical hard problems: a perspective of cryptanalysis[J]. Quantum Information Processing, 2020, 19(6): 178.

[27] BANIN M T, TSABAN B. A reduction of Semigroup DLP to classic DLP[J]. Designs, Codes and Cryptography, 2016, 81(1): 75-82.

[28] HAN J, ZHUANG J C. DLP in semigroups: algorithms and lower bounds[J]. Journal of Mathematical Cryptology, 2022, 16(1): 278-288.

[29] TINANI S, ROSENTHAL J. A deterministic algorithm for the discrete logarithm problem in a semigroup[J]. Journal of Mathematical Cryptology, 2022, 16(1): 141-155.

[作者简介]

黄华伟（1978– ），男，江西樟树人，博士，贵州师范大学副教授、硕士生导师，主要研究方向为密码学与信息安全。