基于多离散对数问题的公钥密码

付向群 鲍皖苏* 史建红 李发达
(信息工程大学 郑州 450004)

摘 要：该文首先定义了多离散对数问题，给出了现有隐含子群问题量子计算算法不适用于求解该问题的必要条件，且该问题在经典计算模式下，其困难性比离散对数问题难，用于求解有限域上离散对数问题的数域筛法不适用于求解多离散对数问题。然后设计了基于多离散对数问题的公钥密码，其安全性依赖于多离散对数问题，且公私钥的数据量小，分析了算法参数的选取原则，证明了算法脱密原理的正确性，算法在每次加密时需要随机选取一个数，使得算法对同一个明文加密所得的密文不一定相同。

关键词：密码学；离散对数问题；公钥密码；量子计算
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2014)06-1423-05
DOI: 10.3724/SP.J.1146.2013.01324

Public-key Cryptograph Based on the Multi-discrete Logarithm Problem

Fu Xiang-qun Bao Wan-su Shi Jian-hong Li Fa-da
(*Information Engineering University*, *Zhengzhou* 450004, *China*)

Abstract: In this paper, the multi-discrete logarithm problem is formally defined, and the necessary conditions of resistance to the quantum algorithm for the hidden subgroup problem are given. It is more difficult than the discrete logarithm problem. And the number field sieve for the discrete logarithm problem is not suitable for addressing it. Furthermore, the public-key cryptograph is designed against the problem, of which the key amount is small. This paper analyses the principles of parameter selection and proves the correctness of the decryption works. It is critical that different random integers are received to the encrypt different messages.

Key words: Cryptography; Discrete logarithm problem; Public-key cryptograph; Quantum computation

1 引言

信息安全主要依赖于密码算法，为了达到该目的，密码算法应当满足：密码体制能够抵抗现有的各种可能攻击方法；算法的安全性依赖于密钥且易于实现。因此，密钥在密码算法中起到重要的作用。文献[1]提出公钥密码思想，有效解决了密钥分配问题。

随着计算机技术的不断发展，密码算法的设计方法也层出不穷。同时，密码学者也在不停地寻求新的密码分析方法。自量子计算概念提出以后，因其强大的并行计算能力引起了学者的广泛关注[2−4]，不断地探寻量子计算是否可以用来攻击密码算法。文献[5]提出大整数分解和离散对数问题的多项式时间量子计算算法。文献[6]提出未加整理数据库的量子搜索算法，与经典搜索算法相比，该算法可以提供二次平方根的加速。这两个算法提出后，对现代密码算法带来了严重的威胁，特别是公钥密码。因此，如何设计抗量子计算攻击的公钥密码成为研究的热点[7−11]。

公钥密码能否抵抗量子计算攻击，在于安全性依赖的数学难题能否抵抗量子计算攻击。目前，学者普遍认为，基于 NPC 问题的公钥密码体制可以抵抗现有条件下量子计算攻击，一般指的是抵抗现有隐含子群问题量子计算算法，主要有基于纠错编码的公钥密码体制、基于辫群的公钥密码体制、基于多变量方程组的公钥密码体制、基于格的公钥密码体制。基于纠错编码的公钥密码体制的密钥量大，不具有实用性；基于辫群、多变量方程组的安全性受到质疑，不能达到理想的安全强度；如果基于格的公钥密码体制所使用的格是一些具有特殊性质的格，其安全强度不够，易于受到攻击，比如 Ajtai 设计的 AD 公钥密码体制[12]。由此可以看出，抵抗现有条件下量子计算攻击的公钥密码都存在一些缺陷，要么存在密钥量大，不实用的缺陷，要么安全性受到学者们的质疑，因此，给出一个密钥量小、安全性高且能抵抗现有条件下量子计算攻击的公钥密码，值得进一步研究与探索。

本文首先定义了多离散对数问题，给出了该问

2013-08-28 收到，2013-12-13 改回
国家 973 计划项目(2013CB338002)资助课题
*通信作者：鲍皖苏 2010thzz@sina.com

题存在多项式时间量子计算算法的条件，进一步给出了该问题可以抵抗现有隐含子群问题量子计算算法攻击的条件，且该问题在经典计算机上的难度至少相当于离散对数问题，因此，只要该问题选择合适的参数，就可以抵抗现有隐含子群问题量子计算算法攻击以及现有的经典攻击方法。然后设计了基于多离散对数问题的公钥密码，其安全性建立在多离散对数问题的基础上，可以抵抗现有的攻击方法，并分析了该算法选取的参数的存在性与选取原则，该公钥密码可以抵抗现有隐含子群问题量子计算算法的攻击以及求解有限域上离散对数问题的数域筛法，而且其公私钥的数据量小，该算法在每次加密时，均要选择一个随机数，以此来达到对同一个明文加密所得密文不一定相同的目的，并证明了算法脱密原理的正确性。

2 多离散对数问题的经典计算复杂性

定义 1(离散对数问题)[13] 给定一个阶为 n 的有限循环群 G , G 的一个生成元 α 和一个元素 $\beta\in G$，求解整数 x , $0\le x\le n-1$，使得 $\alpha^x=\beta$。

定义 2(多离散对数问题) 给定 $g_1,g_2,\cdots,g_t\in Z_N$, $\gcd(g_i,N)=1$, g_i 的阶为 r_i 且已知，$\langle g_1,g_2,\cdots,g_t\rangle$ 是由 $g_1,g_2,\cdots,g_t$ 生成的群，该群上的运算是模数为 N 的模乘运算，对任意的 i , v_i , $1\le i\le t$, $1\le v_i\le r_i-1$, $g_i^{v_i}\notin\langle g_1,\cdots,g_{i-1},g_{i+1},\cdots,g_t\rangle$ ，给定 $\beta\in\langle g_1,g_2,\cdots,g_t\rangle$ ，求解整数 $k_1,k_2,\cdots,k_t$ ，$0\le k_i\le r_i-1$，使得 $\beta=g_1^{k_1}g_2^{k_2}\cdots g_t^{k_t}\bmod N$。

多离散对数问题实质上是通过多个离散对数问题复合在一起，以此来增加问题的困难性，因此，在经典计算机上，多离散对数问题的求解难度至少等价于离散对数问题，亦即该问题是一个困难问题。下面分析多离散对数问题的经典计算复杂性。

2.1 穷尽攻击

采用穷尽搜索定义 2 中多离散对数问题的解 $k_1,k_2,\cdots,k_t$，由于选择的 $g_i^{v_i}\notin\langle g_1,\cdots,g_{i-1},g_{i+1},\cdots,g_t\rangle$，因此，$k_i$ 不能依据 $k_1,\cdots,k_{i-1},k_{i+1},\cdots,k_t$ 和 $g_1,\cdots,g_{i-1},g_{i+1},\cdots,g_t$ 求解出来，亦即只能遍历所有的 $k_1,k_2,\cdots,k_t$，才能得到正确解，其中 $i=1,2,\cdots,t$。又由于每个 k_i 的可能取值有 r_i 个，因此，只要保证 $r_1r_2\cdots r_t$ 的值足够大，就能抵抗穷尽攻击。

2.2 离散对数问题的数域筛法

目前，解决有限域 $\mathrm{GF}(p)$ 上的离散对数问题的最优算法是数域筛法[14]，其计算复杂性是亚指数时间 $e^{O(\log p)^{1/3}(\log\log p)^{2/3}}$。用数域筛法求解定义 1 中的离散对数问题，其具体步骤如下：

步骤 1 对 β 进行标准整数分解，即 $\beta=p_1^{s_1}p_2^{s_2}\cdots p_n^{s_n}$；

步骤 2 建立关于因子基 $\log_\alpha p_1,\log_\alpha p_2,\cdots,\log_\alpha p_n$ 的线性关系式；

步骤 3 用构造的多个线性关系式组成线性方程组，进而通过解方程组求出因子基；

步骤 4 依据 $\log_\alpha\beta=\sum_{i=1}^n s_i\log_\alpha p_i$ 求出离散对数 x。

将该算法用于求解多离散对数问题，可以分别求出 $\log_\alpha\beta,\log_\alpha g_1,\log_\alpha g_2,\cdots,\log_\alpha g_t$，则必有关系式 $\log_\alpha\beta=\sum_{i=1}^t k_i\log_\alpha g_i$，此时可以选择另外一个 α'，得到 $\log_{\alpha'}\beta=\sum_{i=1}^t k_i\log_{\alpha'}g_i$，由 $\log_{\alpha'}x=\dfrac{\log_\alpha x}{\log_\alpha\alpha'}$，易知 $\dfrac{\log_{\alpha'}\beta}{\log_\alpha\alpha'}=\dfrac{1}{\log_\alpha\alpha'}\sum_{i=1}^t k_i\log_\alpha g_i$，因此，无法通过建立方程组求出 $k_1,k_2,\cdots,k_t$，亦即数域筛法不适用于求解多离散对数问题，在经典计算机上不存在多离散对数问题的亚指数时间求解算法。

3 多离散对数问题的量子计算复杂性

在现有公开文献中，大部分多项式时间量子计算算法都能归约为隐含子群问题量子计算算法，是一个通用的量子计算算法，而其它多项式时间量子计算算法均需要依据所求问题具有特殊的性质，才能使得算法以很大的概率求出问题的解，例如 Pell 方程量子计算算法[15]，该算法是依据 Pell 方程的所有解可由其中一个解全部生成。因此，本文主要分析隐含子群问题量子计算算法是否适用于求解多离散对数问题。

在定义 2 中，选取 $g_i^{v_i}\notin\langle g_1,\cdots,g_{i-1},g_{i+1},\cdots,g_t\rangle$ 是为了不降低算法穷尽搜索的计算复杂度，如果 $g_i\in\langle g_1,\cdots,g_{i-1},g_{i+1},\cdots,g_t\rangle$，则问题退化成求解整数 $k_1',\cdots,k_{i-1}',k_{i+1}',\cdots,k_t'$，使得 $\beta=g_1^{k_1'}\cdots g_{i-1}^{k_{i-1}'}g_{i+1}^{k_{i+1}'}\cdots g_t^{k_t'}\bmod N$。进一步，如果多离散对数问题退化成求解整数 k_j''，使得 $\beta=g_j^{k_j''}\bmod N$，此时与离散对数问题的定义一样，存在多项式时间的量子计算算法。

同样在选取 $k_1,k_2,\cdots,k_t$ 时，也要考虑是否会退化成离散对数问题，如果存在 k，使得 $k_i=k\bmod r_i$，其中 $i=1,2,\cdots,t$，则有 $\beta=(g_1g_2\cdots g_t)^k\bmod N$，此时多离散对数问题退化成离散对数问题，因此，利用 Shor 量子计算算法可以在多项式时间内求出 $k_1,k_2,\cdots,k_t$，而且由下面的推论 1 可知，k 对模 $\mathrm{lcm}(r_1,r_2,\cdots,r_t)$ 有唯一解。

在多离散对数问题中，只有选取合适的参数，才能避免其退化成离散对数问题，那么如何选取参数 $k_1,k_2,\cdots,k_t$ 才能达到该目的呢？

引理 1[16] 一次同余式组

$$\left.\begin{aligned} x &= b_1 \bmod m_1 \\ x &= b_2 \bmod m_2 \end{aligned}\right\}$$

有解的充分必要条件是 $\gcd(m_1,m_2)\mid(b_1-b_2)$，且当同余式组有解时对模 $\mathrm{lcm}(m_1,m_2)$ 有唯一解。

定理 1　给定 $g_1,g_2,\cdots,g_t\in Z_N$，$\gcd(g_i,N)=1$，$g_i$ 的阶为 r_i 且已知，$\langle g_1,g_2,\cdots,g_t\rangle$ 是由 $g_1,g_2,\cdots,g_t$ 生成的群，且对任意的 i，v_i，$1\le i\le t$，$1\le v_i\le r_i-1$，$g_i^{v_i}\notin\langle g_1,\cdots,g_{i-1},g_{i+1},\cdots,g_t\rangle$，给定 $\beta\in\langle g_1,g_2,\cdots,g_t\rangle$，即存在 $k_1,k_2,\cdots,k_t$，使得 $\beta=g_1^{k_1}g_2^{k_2}\cdots g_t^{k_t}\bmod N$，如果存在 $j_1,j_2\in\{1,2,\cdots,t\}$ 且 $j_1\ne j_2$，满足 $\gcd(r_{j_1},r_{j_2})\nmid(k_{j_1}-k_{j_2})$，则必不存在 k，使得 $\beta=(g_1g_2\cdots g_t)^k\bmod N$。

证明　要证明定理成立，只需证明一次同余式组

$$\left.\begin{aligned} x &= k_1 \bmod r_1 \\ x &= k_2 \bmod r_2 \\ &\vdots \\ x &= k_t \bmod r_t \end{aligned}\right\} \tag{1}$$

无解。

如果一次同余式组式(1)有解，那么对任意的一次同余式组

$$\left.\begin{aligned} x &= k_i \bmod r_i \\ x &= k_j \bmod r_j \end{aligned}\right\}$$

都有解，其中 $i,j\in\{1,2,\cdots,t\}$。

由于存在 $j_1,j_2\in\{1,2,\cdots,t\}$ 且 $j_1\ne j_2$，满足 $\gcd(r_{j_1},r_{j_2})\nmid(k_{j_1}-k_{j_2})$，因此，一次同余式组

$$\left.\begin{aligned} x &= k_{j_1} \bmod r_{j_1} \\ x &= k_{j_2} \bmod r_{j_2} \end{aligned}\right\}$$

无解，矛盾，亦即式(1)无解。　　证毕

推论 1　在定理 1 中，如果存在 k，使得 $\beta=(g_1g_2\cdots g_t)^k\bmod N$，那么 k 对模 $\mathrm{lcm}(r_1,r_2,\cdots,r_t)$ 有唯一解。

证明　由引理 1 易得推论 1。　　证毕

由定理 1 可知，定义 2 中多离散对数问题只要存在 $j_1,j_2\in\{1,2,\cdots,t\}$ 且 $j_1\ne j_2$，满足 $\gcd(r_{j_1},r_{j_2})\nmid(k_{j_1}-k_{j_2})$，就可以保证多离散对数问题不会退化成离散对数问题。

离散对数问题存在多项式时间量子计算算法，在于其能归约为隐含子群问题，通过隐含子群问题量子计算算法可以建立关于待求量的关系式，进而求出待求量，然而该算法只能建立一个关系式，又由于多离散对数问题有多个待求量 $k_1,k_2,\cdots,k_t$，而且 $k_1,k_2,\cdots,k_t$ 同时蕴含在 β 中，因此，即使多离散对数问题可以归约为隐含子群问题，也无法通过隐含子群问题量子计算算法建立关于 $k_1,k_2,\cdots,k_t$ 的关系式，亦即在多离散对数问题不可以退化成离散对数问题的情况下，现有隐含子群问题量子计算算法不适用于求解多离散对数问题。

综上分析，定义 2 中多离散对数问题只要存在 $j_1,j_2\in\{1,2,\cdots,t\}$ 且 $j_1\ne j_2$，满足 $\gcd(r_{j_1},r_{j_2})\nmid(k_{j_1}-k_{j_2})$，现有隐含子群问题量子计算算法就不适用于求解该问题，也就是说该条件是多离散对数问题抗现有隐含子群问题量子计算算法攻击的必要条件。下面举例说明此类多离散对数问题的存在性。

取 $N=15$，$t=2$，$g_1=2$，$g_2=11$，则 $r_1=4$，$r_2=2$，因此，可得 $g_1^{k_1}g_2^{k_2}\bmod N$ 的值如表 1 所示。

表 1　$g_1^{k_1}g_2^{k_2}\bmod N$ 值

	k_1=1	k_1=2	k_1=3	k_1=4
k_2=1	7	**14**	13	**11**
k_2=2	**2**	4	**8**	1

由表 1 可知，(k_1,k_2) 取值为 $(1,2),(2,1),(3,2),(4,1)$ 时，满足 $\gcd(r_1,r_2)\nmid(k_1-k_2)$，因此，由定理 1 可知，用户选择的 (k_1,k_2) 为这些值时，攻击者无法通过量子计算算法求出 (k_1,k_2)。

4　基于多离散对数问题的公钥密码

量子计算算法的出现，对现代密码产生了重要的影响，设计抗量子计算攻击的密码算法成为研究的热点，为此本文设计了基于多离散对数问题的公钥密码算法。

4.1 基于多离散对数问题的公钥密码算法

4.1.1 用户 B 选取参数并生成密钥

步骤 1　随机选取公共参数 Z_N，$g_1,g_2\in Z_N$，$\gcd(g_i,N)=1$，$\langle g_1\rangle\cap\langle g_2\rangle=\{1\}$，$g_i$ 的阶为 r_i 且已知，其中 $i=1,2$；

步骤 2　选取 k_1,k_2，且 $\gcd(r_1,r_2)\nmid(k_1-k_2)$；

步骤 3　选取 $g_3,g_4\in Z_N$，g_3,g_4 的阶分别为 r_3，r_4，再选取 k_1'，k_2'，k_3，k_4，λ，d_1，d_2，x_1，x_2 使得 $\begin{cases}\lambda(k_1-k_1')=0\bmod r_1\\ \lambda(k_2-k_2')=0\bmod r_2\end{cases}$，$\begin{cases}\lambda x_1k_3=d_1\bmod r_3\\ \lambda x_2k_4=d_2\bmod r_4\end{cases}$，$r_3\nmid\lambda$，$r_4\nmid\lambda$；

步骤 4　$k_1',k_2',k_1,k_2,k_3,k_4,\lambda,d_1,d_2,x_1,x_2,g_1,g_2,g_3,g_4$ 作为私钥，N，$g_1^{k_1}g_2^{k_2}g_3^{k_3}\bmod N$，$g_1^{k_1}g_2^{k_2}g_4^{k_4}\bmod N$，$g_1^{-k_1'}g_2^{-k_2'}\bmod N$，$g_3^{-d_1}g_4^{-d_2}\bmod N$ 作为公钥。

4.1.2 用户 A 加密

步骤 1　用户 A 选择两个整数 $g_5,g_6\in Z_N$ 与 k_5，k_6，满足 $\gcd(g_5,N)=\gcd(g_6,N)=1$，$\langle g_5\rangle\cap\langle g_6\rangle$

$=\{1\}$ 且 $\gcd(r_5,r_6)\nmid(k_5-k_6)$，其中 r_5,r_6 分别为 g_5,g_6 的阶；

步骤 2 A 随机选择 k，其中 $1\le k\le N-1$，计算 $c_1=g_1^{kk_1}g_2^{kk_2}g_3^{kk_3}g_5^{k_5}g_6^{k_6}\bmod N$，$c_2=g_1^{kk_1}g_2^{kk_2}g_4^{kk_4}g_5^{k_5}g_6^{k_6}\bmod N$，$c_3=g_1^{-kk_1'}g_2^{-kk_2'}g_5^{-k_5}g_6^{-k_6}\bmod N$；

步骤 3 把秘密信息表示成 $\{0,1,\cdots,N-1\}$ 中的某个整数 m，计算密文 $c_4=mg_3^{-kd_1}g_4^{-kd_2}\bmod N$；

步骤 4 将密文 $c=(c_1,c_2,c_3,c_4)$ 传给用户 B。

4.1.3 用户 B 脱密

步骤 1 用户 B 收到密文后，计算 $A_1=(c_1)^\lambda\bmod N$，$A_2=(c_2)^\lambda\bmod N$，$A_3=(c_3)^\lambda\bmod N$；

步骤 2 计算 $B_1=A_1A_3\bmod N$，$B_2=A_2A_3\bmod N$；

步骤 3 计算 $m=B_1^{x_1}B_2^{x_2}c_4\bmod N$。

4.2 正确性分析

用户 B 收到密文后，能否正确得到明文 m，其脱密原理的正确性分析如下：

$$A_1=(c_1)^\lambda\bmod N=g_1^{\lambda kk_1}g_2^{\lambda kk_2}g_3^{\lambda kk_3}g_5^{\lambda k_5}g_6^{\lambda k_6}\bmod N \quad (2)$$

$$A_2=(c_2)^\lambda\bmod N=g_1^{\lambda kk_1}g_2^{\lambda kk_2}g_4^{\lambda kk_4}g_5^{\lambda k_5}g_6^{\lambda k_6}\bmod N \quad (3)$$

$$A_3=(c_3)^\lambda\bmod N=g_1^{-\lambda kk_1'}g_2^{-\lambda kk_2'}g_5^{-\lambda k_5}g_6^{-\lambda k_6}\bmod N \quad (4)$$

由于 $\begin{cases}\lambda(k_1-k_1')=0\bmod r_1\\ \lambda(k_2-k_2')=0\bmod r_2\end{cases}$，因此，结合式(2)，式(3)，式(4)可得

$$\left.\begin{aligned}B_1&=g_3^{\lambda kk_3}\bmod N\\ B_2&=g_4^{\lambda kk_4}\bmod N\end{aligned}\right\} \quad (5)$$

又由于 $\begin{cases}\lambda x_1k_3=d_1\bmod r_3\\ \lambda x_2k_4=d_2\bmod r_4\end{cases}$，则有

$$B_1^{x_1}B_2^{x_2}=g_3^{kd_1}g_4^{kd_2}\bmod N \quad (6)$$

亦即

$$B_1^{x_1}B_2^{x_2}c_4\bmod N=m \quad (7)$$

因此，基于多离散对数问题的公钥密码的脱密原理是正确的。

4.3 安全性分析

下面分析必存在参数 $k_1',k_2',k_3,k_4,\lambda,d_1,d_2,x_1,x_2$。

选取参数 λ 满足 $r_3\nmid\lambda$ 且 $r_4\nmid\lambda$，则对任意的 k_1,k_2，存在 k_1',k_2' 使得 $\begin{cases}\lambda(k_1-k_1')=0\bmod r_1\\ \lambda(k_2-k_2')=0\bmod r_2\end{cases}$，对任意的 x_1,x_2，只要选择的 d_1,d_2 满足 $\gcd(\lambda x_1,r_3)\mid d_1$，$\gcd(\lambda x_2,r_4)\mid d_2$，则一定存在 k_3，k_4 使得 $\begin{cases}\lambda x_1k_3=d_1\bmod r_3\\ \lambda x_2k_4=d_2\bmod r_4\end{cases}$。因此，必定能找到参数 $k_1',k_2',k_3,k_4,\lambda,d_1,d_2,x_1,x_2$ 使得 $\begin{cases}\lambda(k_1-k_1')=0\bmod r_1\\ \lambda(k_2-k_2')=0\bmod r_2\end{cases}$，$\begin{cases}\lambda x_1k_3=d_1\bmod r_3\\ \lambda x_2k_4=d_2\bmod r_4\end{cases}$，$r_3\nmid\lambda$，$r_4\nmid\lambda$。

选取的参数 λ 满足 $r_3\nmid\lambda$ 且 $r_4\nmid\lambda$，是为了能够找到不为 0 的 d_1,d_2，否则算法将存在安全隐患。

由于 g_3,g_4,d_1,d_2 是用户 B 的私钥，因此，即使选择的 d_1,d_2 满足 $\gcd(r_3,r_4)\mid(d_1-d_2)$，攻击者无法由 $g_3^{-d_1}g_4^{-d_2}\bmod N$ 得到 $g_3^{d_1}$，$g_4^{d_2}$，亦即无法通过 $\begin{cases}\lambda(k_1-k_1')=0\bmod r_1\\ \lambda(k_2-k_2')=0\bmod r_2\end{cases}$，$\begin{cases}\lambda x_1k_3=d_1\bmod r_3\\ \lambda x_2k_4=d_2\bmod r_4\end{cases}$ 求出 r,x_1,x_2。

在算法中，由于选取 k_1',k_2' 不一定满足 $\gcd(r_1,r_2)\nmid(k_1'-k_2')$，也就是说攻击者可能依据 $g_1^{-k_1'}g_2^{-k_2'}\bmod N$ 求出 k_1',k_2'。然而在该公钥密码中，由于 g_3,g_4,k_3,k_4,d_1,d_2 是未知的，因此，即使攻击者知道了 k_1',k_2'，也无法得到 r,x_1,x_2，亦即 k_1',k_2' 对该公钥密码的安全性没有影响，只是一个用于辅助脱密的参数。

如果攻击者能够由 $g_1^{k_1}g_2^{k_2}g_3^{k_3}\bmod N$，$g_1^{k_1}g_2^{k_2}g_4^{k_4}\bmod N$ 求出密钥 k_1,k_2,k_3,k_4，进而得到 $g_3^{k_3}$，$g_4^{k_4}$，或者通过密文 $c=(c_1,c_2,c_3,c_4)$ 求出 k_5,k_6，进而得到 k，那么攻击者可以得到明文 m。因此，为了保证 $g_3^{k_3},g_4^{k_4}$ 的安全性，用户 B 需要选择合适的参数 g_1,g_2,k_1,k_2，而且至少要选择两个 g_1,g_2，否则不能抵抗现有隐含子群问题量子计算算法攻击，同样为了保证密文 $c=(c_1,c_2,c_3,c_4)$ 的安全性，需要选择合适的参数 g_5,g_6,k_5,k_6，且至少要有两个 g_5,g_6。用户 A 至少需要选取两个 g_3,g_4，如果只选择一个 g_3，那么攻击者通过求 $g_1^{k_1}g_2^{k_2}g_3^{k_3}g_3^{-d_1}\bmod N$ 的阶，即可得到明文 m。

由于选取的 k_1，k_2，k_5，k_6 满足 $\gcd(r_1,r_2)\nmid(k_1-k_2)$，$\gcd(r_5,r_6)\nmid(k_5-k_6)$，但此时并不会因该性质而降低算法的穷尽搜索的计算复杂性，原因在于 r_1,r_2,r_5,r_6 是未知的，攻击者并不知道满足 $\gcd(r_1,r_2)\mid(k_1-k_2)$，$\gcd(r_5,r_6)\mid(k_5-k_6)$ 的 k_1，k_2，k_5，k_6，从而降低穷尽搜索的计算复杂性，因此，只要 r_1r_2,r_5r_6 足够大，就能抵抗穷尽攻击。

4.4 数据量分析

由用户的脱密过程可以看出，用户 B 在脱密时只要用到 r,x_1,x_2，因此，用户的私钥的数据量很小，而且用户 B 只需提供 5 个不超过 N 的公钥，亦即公钥的数据量也很小。

由用户的加密过程可以看出，密文长度是明文长度的 4 倍。

综上分析可知，基于多离散对数问题的公钥密码算法可以抵抗现有隐含子群问题量子计算算法攻

击，公私钥的数据量小，而且与基于离散对数问题的公钥密码算法相比，其被攻破的难度更难。在算法的加脱密过程中，算法只需要用到乘法运算，因此，算法易于实现。

5 结束语

本文给出了多离散对数问题的定义，给出了其抵抗现有隐含子群问题量子计算算法攻击的必要条件，并基于该问题设计了公钥密码，该算法可以抵抗现有的经典攻击方法，且可以抵抗现有隐含子群问题量子计算算法攻击。然而本文没有给出多离散对数问题抵抗现有隐含子群问题量子计算算法攻击的充分条件，如何给出该充分条件有待进一步研究与探索。

参 考 文 献

[1] Diffie W and Hellman M E. New directions on cryptography [J]. *IEEE Transactions on Information Theory*, 1976, IT-22(6): 644–654.

[2] 李凯, 黄晓英, 滕吉红, 等. 一种基于 Einstein-Podolsky-Rosen(EPR)序列的量子安全通信协议[J]. 电子与信息学报, 2012, 34(8): 1917–1922.
Li Kai, Huang Xiao-ying, Teng Ji-hong, *et al*.. A quantum secure direct communication scheme based on Einstein-Podolsky-Rosen (EPR) sequence[J]. *Journal of Electronics & Information Technology*, 2012, 34(8): 1917–1922.

[3] 易运晖, 朱畅华, 裴昌幸, 等. 偏振旋转的量子私有信息检索方案[J]. 电子与信息学报, 2012, 34(10): 2353–2357.
Yi Yun-hui, Zhu Chang-hua, Pei Chang-xing, *et al*.. Quantum private information retrieval based on polarization rotation[J]. *Journal of Electronics & Information Technology*, 2012, 34(10): 2353–2357.

[4] Fu Xiang-qun, Bao Wan-su, Zhou Chun, *et al*.. *t*-bit semiclassical quantum Fourier transform[J]. *Chinese Science Bulletin*, 2012, 57(1): 119–124.

[5] 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.

[6] Grover L K. A fast quantum mechanics algorithm for database search[C]. Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of computing, Philadelphia, 1996: 212–219.

[7] 王保仓, 韦永壮, 胡予濮. 基于随机背包的公钥密码[J]. 电子与信息学报, 2010, 32(7): 1580–1584.
Wang Bao-cang, Wei Yong-zhuang, and Hu Yu-pu. Public key cryptosystem using random knapsacks[J]. *Journal of Electronics & Information Technology*, 2010, 32(7): 1580–1584.

[8] 韩立东, 刘明洁, 毕经国. 两种背包型的公钥密码算法的安全性分析[J]. 电子与信息学报, 2010, 32(6): 1485–1488.
Han Li-dong, Liu Ming-jie, and Bi Jing-guo. Security analysis of two knapsack-type public key cryptosystems[J]. *Journal of Electronics & Information Technology*, 2010, 32(6): 1485–1488.

[9] 鲁晓彬, 鲍皖苏, 李发达, 等. 基于 MI 和 TPM 混合的多变量数字签名方案[J]. 电子学报, 2012, 40(10): 2021–2025.
Lu Xiao-bin, Bao Wan-su, Li Fa-da, *et al*.. A MPKC signature scheme based on mixing of MI and TPM[J]. *Acta Electronica Sinica*, 2012, 40(10): 2021–2025.

[10] 叶茂, 胡学先, 刘文芬. 基于格的三方口令认证密钥交换协议[J]. 电子与信息学报, 2013, 35(6): 1376–1381.
Ye Mao, Hu Xue-xian, and Liu Wen-fen. Password authenticated key exchange protocol in the three party setting based on lattices[J]. *Journal of Electronics & Information Technology*, 2013, 35(6): 1376–1381.

[11] 光焱, 顾纯祥, 祝跃飞, 等. 一种基于 LWE 问题的无证书全同态加密体制[J]. 电子与信息学报, 2013, 35(4): 988–993.
Guang Yan, Gu Chun-xiang, Zhu Yue-fei, *et al*.. Certificateless fully homomorphic encryption based on LWE problem[J]. *Journal of Electronics & Information Technology*, 2013, 35(4): 988–993.

[12] Ajtai M. Generating hard instances of lattice problems[C]. Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, 1996: 1–32.

[13] Menezes A J, Oorschot P C V, and Vanstone S A. Handbook of Applied Cryptography[M]. Canda: CRC Press LLC, 1997: 103–104.

[14] Gordon D M. Discrete Logarithms in GF(P) using the number field sieve[J]. *SIAM Journal on Discrete Mathematics*, 1993, 6(1): 124–138.

[15] Hallgren S. Polynomial-time Quantum algorithm for Pell's equation and the principal Ideal problem[C]. Proceedings of the 34th Annual ACM Symposium on Theory of Computation, New York, 2002: 653–658.

[16] 潘承洞, 潘承彪. 初等数论[M]. 第 2 版, 北京: 北京大学出版社, 2003: 155–190.
Pan Cheng-dong and Pan Cheng-biao. Elementary Number Theory[M]. Second Edition, Beijing: Peking University Press, 2003: 155–190.

付向群： 男，1985 年生，博士生，研究方向为量子密码与量子计算.

鲍皖苏： 男，1966 年生，博士生导师，教授，研究方向为量子密码、序列密码、公钥密码.

史建红： 男，1975 年生，硕士生导师，副教授，研究方向为量子密码、量子协议、公钥密码.

李发达： 男，1989 年生，硕士生，研究方向为量子计算.