基于多离散对数问题的公钥密码的分析

苏盛辉[1,2,3], 孙国栋[2]
(1. 南京航空航天大学计算机学院,江苏南京 211106;2. 北京工业大学计算机学院, 北京 100124;
3. 南京理工大学公共安全科技创新中心,江苏南京 210094)

摘 要: 本文对一个特定群生成元系中元素的阶数的选取做了讨论,对多离散对数问题和基于它的公钥加密方案做了分析. 指出在原文所述情况下,多离散对数问题可转化为离散对数问题,从而,该问题存在亚指数时间解,并导致相关私钥在大多数情况下是亚指数时间不安全的. 本文进一步指出,在几乎任何情况下,密文还原问题都可转化为离散对数问题,从而,它也存在亚指数时间解. 所以,要把离散对数问题和 ElGamal 公钥密码改造成抗 Shor 量子算法攻击的,还需做更深入的、持久的探索.

关键词: 多离散对数问题; 公钥密码; 安全性; 量子算法; 亚指数时间解
中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112 (2018)01-0218-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.01.030

Analysis of a Public-Key Cryptograph Based on Multi-Discrete Logarithm Problems

SU Sheng-hui[1,2,3], SUN Guo-dong[2]
(1. *College of Computers, Nanjing University of Aeronautics & Astronautics, Nanjing, Jiangsu* 211106, *China*;
2. *College of Computers, Beijing University of Technology, Beijing* 100124, *China*;
3. *Public Security Innovation Center, Nanjing University of Science & Technology, Nanjing, Jiangsu* 210094, *China*)

Abstract: The paper discusses the selection of orders of elements in one generator set for a specified group, and analyzes multi-discrete logarithm problems (MDLP) and a public key encryption scheme based on the MDLP. The paper points out that under the circumstances described by the original paper, the MDLP may be transformed into a discrete logarithm problem, which manifests that there exists a sub-exponential time solution for the MDLP, and causes a related private key insecure in sub-exponential time in most cases. Further, in almost any case, a ciphertext inversion problem may be transformed into a discrete logorithm problem, which illustrates that there also exists a sub-exponential time solution to the ciphertext. Therefore, to convert a discrete logarithm and the ElGamal cryptosystem into those which are resistant to the Shor quantum alg. orithm attack, the people still need to make deeper and longer explorations.

Key words: multi-discrete logarithm problem; public key cryptograph; security; quantum algorithm; sub-exponential time solution

1 引言

两个著名的量子算法,尤其 Shor 量子算法,对现有公钥密码构成了极大威胁[1,2]. 一旦大型量子计算机被生产出来,那么,在有隐含子群的离散对数问题(Discrete Logarithm Problem, DLP)和因式分解问题(Integer Factorization Problem, IFP)的基础上构建的公钥密码体制,例如,ElGamal 和 RSA 等[3-5],都将陷入被破译的困境. 因此,如何设计抗量子计算的公钥密码是当前业界学者面临的一项紧迫任务[6].

2011 年中国学者在国际上提出了一个全新的公钥密码体制[7],它基于三个新的计算问题:多变量排列问题(Multivariate Permutation Problem, MPP)、非范子集积问题(Anomalous Subset Product Problem, ASPP)和超越对数问题(Transcendental Logarithm Problem, TLP). 该三个问题的计算复杂度被分别证明是至少等价于离散对

收稿日期:2014-12-19;修回日期:2017-01-22;责任编辑:郭游
基金项目:国家 863 高技术研究发展计划(No. 2009AA01Z441)

数问题的,且存在一些证据使人们倾向于相信 MPP、ASPP、TLP 是比离散对数问题更为困难的[8]. 目前,该三个问题不存在亚指数时间解[9],因而极有可能是抗量子计算攻击的.

近来,我国学者提出了一个基于多离散对数问题(Multi-Discrete Logarithm Problem,MDLP)的公钥加密方案[10],它被原作者认为在经典计算机上没有亚指数时间解、是抗量子计算攻击的,即抗 Shor 量子算法的(该量子算法使得 DLP、IFP 在量子计算机上存在多项式时间解[10]). 然而,令人遗憾的是,现时的分析表明,多离散对数问题在原文所述情况下存在亚指数时间解,而基于多离散对数问题的公钥加密方案在几乎任何情况下都存在亚指数时间解,与作者的设计初衷相背离.

2　多离散对数问题到离散对数问题的转化

对于离散对数问题[11],大家并不陌生. 例如,给定 $y \in \mathbb{Z}_p$,求 x 满足 $y = g^x \bmod p$,其中,p 为素数,$g \in \mathbb{Z}_p$ 为生成元.

2.1　多离散对数问题的定义

多离散对数问题被原作者定义如下:

定义 1　给定 $g_1, g_2, \cdots, g_t \in \mathbb{Z}_N$,$\gcd(g_i, N) = 1$,$g_i$ 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 $i, v_i (1 \leqslant i \leqslant t, \leqslant v_i \leqslant r_i - 1)$,有 $g_i^{vi} \notin \langle g_1, \cdots, g_{i-1}, g_{i+1}, \cdots, g_t \rangle$,给定 $\beta \in \langle g_1, g_2, \cdots, g_t \rangle$,求解整数 $k_1, k_2, \cdots, k_t$ $(0 \leqslant k_i \leqslant r_i - 1)$,使得 $\beta = g_1^{k1} g_2^{k2} \cdots g_t^{kt} \bmod N$[10].

不难理解,如果 $g_i^{vi} \in \langle g_1, \cdots, g_{i-1}, g_{i+1}, \cdots, g_t \rangle$,则 β 可表示为 $g_1^{k'1} \cdots g_{i-1}^{k'i-1} g_{i+1}^{k'i+1} \cdots g_t^{k't} \bmod N$,这样,多离散对数问题可逐渐退化为离散对数问题.

也容易看到,如果 N 为素数,则很可能 $g_i^{vi} \in \langle g_1, \cdots, g_{i-1}, g_{i+1}, \cdots, g_t \rangle$,因此,$N$ 不能为素数. 进一步,$\langle g_1, g_2, \cdots, g_t \rangle$ 不能为循环子群.

为了进一步避免多离散对数问题退化为离散对数问题,原作者给出了定理 1:

定理 1　给定 $g_1, g_2, \cdots, g_t \in \mathbb{Z}_N$,$gcd(g_i, N) = 1$,$g_i$ 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 $i, v_i \leqslant 1 \leqslant i \leqslant t, 1 \leqslant v_i \leqslant r_i - 1)$,有 $g_i^{vi} \in \langle g_1, \cdots, g_{i-1}, g_{i+1}, \cdots, g_t \rangle$,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 $\beta = g_1^{k1} g_2^{k2} \cdots g_t^{kt} \bmod N$,如果存在 $i, j \in \{1, 2, \cdots, t\}$ 且 $i \neq j$,满足 $\gcd(r_i, r_j) \nmid (k_i - k_j)$,则必不存在 k,使得 $\beta = (g_1 g_2 \cdots g_t)^k \bmod N$[10].

显然,如果存在 k,使得 $\beta = (g_1 g_2 \cdots g_t)^k \bmod N$,则可令 $g = g_1 g_2 \cdots g_t \bmod N$,进而,多离散对数问题退化为离散对数问题($N$ 可先分解为素数之幂积,分别列出同余式求出模各素数幂之 k,然后,再利用中国剩余定理求合成之 k[11]).

2.2　生成元系中元素阶数的选取

由 2.1 节知,生成元系中元素 $g_1, g_2, \cdots, g_t \in \mathbb{Z}_N$ 的阶分别为 $r_1, r_2, \cdots, r_t$. 原文没有对 $r_1, r_2, \cdots, r_t$ 的取值给出清晰的说明,但是,根据定义 1,对任意的 $i, v_i (1 \leqslant i \leqslant t, 1 \leqslant v_i \leqslant r_i - 1)$,须有 $g_i^{vi} \notin \langle g_1, \cdots, g_{i-1}, g_{i+1}, \cdots, g_t \rangle$. 因此,对 $r_1, r_2, \cdots, r_t$ 的选取需考虑下面几点:

(1)实际上,我们不可能对于每个 g_i^{vi} 是否属于 $\langle g_1, \cdots, g_{i-1}, g_{i+1}, \cdots, g_t \rangle$ 去试算、判断一次,因为这样的试算与判断在非确定情况下将需要指数时间.

(2)从 $\mathbb{Z}_N$ 是 Abel 群,可知 $\langle g_1, g_2, \cdots, g_t \rangle = \langle g_1 \rangle \langle g_2 \rangle \cdots \langle g_t \rangle = \{g_1^1, g_1^2, \cdots, g_1^{r1}\} \{g_2^1, g_2^2, \cdots, g_2^{r2}\} \cdots \{g^1, g^2, \cdots, g_t^{rt}\}$[12].

(3)若元素 g_i 的阶为 r_i,则对于每个正整数 k_i,$g_i^{ki} \bmod N$ 的阶是 $r_i / \gcd(r_i, k_i)$[12].

(4)由于 $\mathbb{Z}_N$ 是 Abel 群,因此,若元素 g_i 和 g_j 的阶为 r_i 和 r_j,且 $\gcd(r_i, r_j) = 1$,则 $g_i g_j$ 的阶为 $r_i r_j$;若 $\gcd(r_i, r_j) \neq 1$,则 $g_i g_j$ 的阶为 $\mathrm{lcm}(r_i, r_j)$ 或 $\mathrm{lcm}(r_i, r_j)$ 的一个真因子[13].

(5)根据(3)和(4),如果存在过多的 $\gcd(r_i, r_j) \neq 1$ $(i \neq j)$,则很可能导致 $g_i^{vi} \in \langle g_1, \cdots, g_{i-1}, g_{i+1}, \cdots, g_t \rangle$.

(6)同样,根据(3)和(4),如果存在 $r_i = r_j (i \neq j)$,则很可能存在 $g_i^{vi} \in \langle g_j \rangle$ 或 $\in \langle g_1, \cdots, g_{i-1}, g_{i+1}, \cdots, g_t \rangle$.

综合上述六点,$r_1, r_2, \cdots, r_t$ 应该两两不同,每个 r_i 应该含有不同的素因子,且 $\gcd(r_i, r_j) \neq 1 (i \neq j)$ 不应太多.

例如,$\{r_1, r_2, r_3, r_4, \cdots\} = \{34393, 140669, 38873, 65537, \cdots\}$ 无关 N 时是合理的.

2.3　多离散对数问题的亚指数时间解法

由于定理 1 表明只要存在一对 $(r_i, r_j) (i \neq j)$ 满足 $\gcd(r_i, r_j) \nmid (k_i - k_j)$,则不存在 k,使得 $\beta = (g_1 g_2 \cdots g_t)^k \bmod N$,以及原密钥生成算法明确规定 $\gcd(r_1, r_2) \nmid (k_1 - k_2)$,因此,在下面的算法中,我们假设 $\gcd(r_1, r_2) \neq 1 < 2^{76}$ 且 $\gcd(r_i, r_j) = 1 (i \neq j \neq 1, 2)$. 从定理 1、密钥生成和阶选六点来看,该假设是符合原文所述情况的. 在该情况下,即使 $r_1, r_2, \cdots, r_t$ 如原文所说的足够大也无济于事. 注意,$g_1, g_2, \cdots, g_t$ 的排列顺序是可以改变的.

我们给出原文所述情况下的多离散对数问题求解算法.

输入:$\beta (= g_1^{k1} g_2^{k2} \cdots g_t^{kt} \bmod N)$;$g_1, g_2, \cdots, g_t$;$N$.

S1:利用数域筛法[11],求出 N 的素因子.

S2:根据求阶算法[11],计算 $r_1, r_2, \cdots, r_t$.

S3:置 $s \leftarrow t, \beta_s \leftarrow \beta$.

S4:如果 $s > 1$,则令 $h \leftarrow \mathrm{lcm}(r_1, r_2, \cdots, r_{s-1})$;否则 $h \leftarrow 1$.

S5:计算 $\beta' \leftarrow \beta_s^h \bmod N$(注意,$\beta_s^h \equiv g_s^{kh} (\bmod N)$).

S6:根据指数算法[11],求 x 满足 $\beta' = g_s^x \bmod N$ 和 k_s 满足 $x = hk_s \bmod r_s$.

若 $s=2$,则 k_2 还需满足 $\beta_2 (g_2^{k2})^{-1} \bmod N \in \langle g_1 \rangle$.

S7:如果 $s=1$,则结束;

否则,做 $\beta_{s-1} \leftarrow \beta_s (g_s^{ks})^{-1} \bmod N$,令 $s \leftarrow s-1$,转至S4.

输出:$k_1, k_2, \cdots, k_t (0 \leqslant k_i \leqslant r_i - 1)$.

如果定义1中的条件满足,则解是唯一的;如果不满足,则存在多个解.

注意,在S4,可定义 $\mathrm{lcm}(r_1) = r_1$;在S6,是否 $\beta_2 (g_2^{k2})^{-1} \bmod N \in \langle g_1 \rangle$ 可结合元素的阶来判断(由于 $\langle g_1 \rangle$ 的阶所含素因子是相当有限的,因此,该方法(尽管不具充分性)在亚指数时间内是行之有效的).

不难分析,该算法的S1和S6调用了两个亚指数时间算法,因此,其时间复杂度也是亚指数相关的.

我们举一个小的例子来演示上述的算法.

令 $N = 7*7*11*19*23 = 235543$,则 $\phi(N) = 6*7*10*18*22 = 2^4*3^3*5*7*11 = 166320$.

又令 $g_1 = 3497$、$g_2 = 30430$、$g_3 = 33650$、$g_4 = 20483$,则有 $r_1 = 6$、$r_2 = 15$、$r_3 = 7$、$r_4 = 11$,$\langle 3497, 30430, 33650, 20483 \rangle = \langle 3497 \rangle \langle 30430 \rangle \langle 33650 \rangle \langle 20483 \rangle$,它满足定义1中的条件,并有 $\gcd(r_1, r_2) = 3 \neq 1$.

问题:

给定 $3497^{k_1} 30430^{k_2} 33650^{k_3} 20483^{k_4} \equiv 192880 \pmod{235543}$,求 k_1、k_2、k_3、k_4.

求解过程:

(1)由于 $\mathrm{lcm}(6, 15, 7) = 210$ 和 $3497^{k_1} 30430^{k_2} 33650^{k_3} 20483^{k_4} \equiv 192880 \pmod{235543}$,故有 $(3497^{k_1} 30430^{k_2} 33650^{k_3} 20483^{k_4})^{210} \equiv 20483^{k_4} \equiv (192880)^{210} \equiv 40965 \pmod{235543}$.

即 $20483^{k_4} \equiv 40965 \pmod{235543}$,从而 $k_4 \equiv 8 \pmod{11}$.

(2)从 $3497^{k_1} 30430^{k_2} 33650^{k_3} 20483^{8} \equiv 192880 \pmod{235543}$ 求出 $3497^{k_1} 30430^{k_2} 33650^{k_3} \equiv 192880 \cdot 215062 \equiv 151916 \pmod{235543}$,进而 $(3497^{k_1} 30430^{k_2} 33650^{k_3})^{30} \equiv (151916)^{30} \equiv 33650$.

即 $33650^{2k_3} \equiv 33650 \pmod{235543}$,从而 $2k_3 \equiv 1 \pmod 7$,$k_3 \equiv 1 \cdot 4 \equiv 4 \pmod 7$.

(3)从 $3497^{k_1} 30430^{k_2} 33650^{4} \equiv 151916 \pmod{235543}$ 求出 $3497^{k_1} 30430^{k_2} \equiv 151916 \cdot 100948 = 118267 \pmod{235543}$,进而 $(3497^{k_1} 30430^{k_2})^6 \equiv (118267)^6 \equiv 214131$.

即 $30430^{6k_2} \equiv 214131 \pmod{235543}$,从而 $6k_2 \equiv 12 \pmod{15}$,k_2(2,7 或 12 $\pmod{15}$).

由于 $118267 \cdot (30430^2)^{-1} \bmod 235543 = 196030 \notin \langle 3497 \rangle$ 和 $118267 \cdot (30430^{12})^{-1} \bmod 235543 = 96854 \notin \langle 3497 \rangle$,因此,选定 $k_2 \equiv 7 \pmod{15}$.

(4)从 $3497^{k_1} 30430^{7} \equiv 118267 \pmod{235543}$ 求出 $3497^{k_1} \equiv 118267 \cdot 43954 \equiv 109251 \pmod{235543}$.

即 $3497^{k_1} \equiv 109251 \pmod{235543}$,从而 $k_1 \equiv 5 \pmod 6$.

得到 $k_1 \equiv 5 \pmod 6$、$k_2 \equiv 7 \pmod{15}$、$k_3 \equiv 4 \pmod 7$、$k_4 \equiv 8 \pmod{11}$.

此时,我们还看到,$\langle g_1 = 3497 \rangle \cap \langle g_2 = 30430 \rangle = \{1\}$,$\gcd(r_1, r_2) = 3 \nmid (k_1 - k_2)$,这正是原密钥生成算法和定理1中规定的条件.

3 基于 MDLP 的公钥加密方案的不安全性

原文基于多离散对数问题提出了一个公钥加密方案,不难看出,它是对 ElGamal 公钥密码体制的改造.

根据原文抗量子计算的设计目标,我们这里所指的不安全性是指该方案在经典计算机上存在离散对数亚指数时间破解方法.

另外,根据公钥密码的"三公"原则:算法公开、公钥公开、密文公开,我们在破译过程中把算法、公钥、密文三个要素当作已知条件加以利用.

3.1 原公钥加密方案

它包括密钥生成、加密、解密三个算法[10].

原文加密算法中出现了私钥,这种表达方式是明显不规范的. 因此,在转述中,我们用公钥取代了相应的私钥.

3.1.1 密钥生成算法

S1:随机选取公共参数 $N, g_1, g_2 \in \mathbb{Z}_N$,$\gcd(g_i, N) = 1$,$\langle g_1 \rangle \cap \langle g_2 \rangle = \{1\}$,$g_i$ 的阶为 r_i 已知,其中 $i = 1, 2$.

S2:选取 k_1, k_2,且 $\gcd(r_1, r_2) \nmid (k_1 - k_2)$.

S3:选取 $g_3, g_4 \in \mathbb{Z}_N$,其阶分别为 r_3, r_4.

再选取 $k_1', k_2', k_3, k_4, (, d_1, d_2, x_1, x_2$ 使得

$\lambda(k_1 - k_1') = 0 \bmod r_1$,$\lambda(k_2 - k_2') = 0 \bmod r_2$ 和

$\lambda x_1 k_3 = d_1 \bmod r_3$,$\lambda x_2 k_4 = d_2 \bmod r_4 (r_3 \nmid \lambda, r_4 \nmid \lambda)$.

S4:计算 $y_1 \leftarrow g_1^{k1} g_2^{k2} g_3^{k3} \bmod N$,$y_2 \leftarrow g_1^{k1} g_2^{k2} g_4^{k4} \bmod N$,

$y_3 \leftarrow g_1^{-k'1} g_2^{-k'2} \bmod N$,$y_4 \leftarrow g_3^{-d1} g_4^{-d2} \bmod N$.

以 $k_1', k_2', k_1, k_2, k_3, k_4, \lambda, d_1, d_2, x_1, x_2, g_1, g_2, g_3, g_4$ 作为私钥,以 N, y_1, y_2, y_3, y_4 作为公钥.

注意,由于 g_3、g_4 的阶为 r_3 和 r_4,且有 $\lambda x_1 k_3 = d_1 \bmod r_3$、$\lambda x_2 k_4 = d_2 \bmod r_4$,这表明 r_3、r_4 不为0,因此,隐含有 $\gcd(g_3, N) = 1$ 和 $\gcd(g_4, N) = 1$.

3.1.2 加密算法

S1:用户A选择两个整数 $g_5, g_6 \in \mathbb{Z}_N$(阶 r_5, r_6)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 $\gcd(r_5, r_6) \nmid (k_5 - k_6)$.

S2:A 随机选择 $k(1\leqslant k\leqslant N-1)$,计算 $c_1\leftarrow y_1^k g_5^{k5} g_6^{k6} \bmod N$,

$c_2\leftarrow y_2^k g_5^{k5} g_6^{k6} \bmod N, c_3\leftarrow y_3^k g_5^{-k5} g_6^{-k6} \bmod N$.

S3:把秘密信息表示为$\{0,1,\cdots,N-1\}$中的某个整数 m.

S4:计算 $c_4\leftarrow y_4^k m \bmod N$.

用户 A 将密文 $c=(c_1,c_2,c_3,c_4)$传给用户 B.

3.1.3　解密算法

S1:用户 B 收到密文后,计算

$$A_1\leftarrow (c_1)^{\lambda} \bmod N,$$

$$A_2\leftarrow (c_2)^{\lambda} \bmod N,$$

$$A_3\leftarrow (c_3)^{\lambda} \bmod N.$$

S2:计算 $B_1\leftarrow A_1A_3 \bmod N, B_2\leftarrow A_2A_3 \bmod N$.

S3:计算 $m\leftarrow (B_1)^{x1}(B_2)^{x2}(c_4) \bmod N$.

最后,求出的 m 即为原来的明文.

3.2　私钥的亚指数时间提取

从原密钥生成算法知,公钥

$y_1=g_1^{k_1}g_2^{k_2}g_3^{k_3} \bmod N$、$y_2=g_1^{k_1}g_2^{k_2}g_4^{k_4} \bmod N$、

$y_3=g_1^{-k'_1}g_2^{-k'_2} \bmod N$、$y_4=g_3^{-d_1}g_4^{-d_2} \bmod N$.

按照多离散对数问题的定义,g_1,g_2,g_3,g_4 理应做为公钥公布,但原作者并没有公布它们. 这就使得 $y_1=g_1^{k_1}g_2^{k_2}g_3^{k_3} \bmod N$ 等 4 个方程不是多离散对数问题,而是有点超越对数问题的味道了. 这与原作者提出多离散对数问题在逻辑上似乎有点不一致.

从解密算法看,由于

$$\begin{aligned} m &\equiv (B_1)^{x_1}(B_2)^{x_2}(c_4)\\ &\equiv (A_1A_3)^{x_1}(A_2A_3)^{x_2}(y_4^k m)\\ &\equiv ((c_1)^{\lambda}(c_3)^{\lambda})^{x_1}((c_2)^{\lambda}(c_3)^{\lambda})^{x_2}(y_4^k m) \pmod N. \end{aligned}$$

即

$$\begin{aligned} m &\equiv (y_1^k g_5^{k_5} g_6^{k_6})^{\lambda x_1}(y_2^k g_5^{k_5} g_6^{k_6} y_3^k g_5^{-k_5} g_6^{-k_6})^{\lambda x_2}\\ &\quad\cdot (y_4^k m) \equiv (y_1y_3)^{k\lambda x_1}(y_2y_3)^{k\lambda x_2}(y_4^k m)\\ &\equiv (g_1^{k_1}g_2^{k_2}g_3^{k_3}g_1^{-k'_1}g_2^{-k'_2})^{k\lambda x_1}(g_1^{k_1}g_2^{k_2}g_4^{k_4}g_1^{-k'_1}g_2^{-k'_2})^{k\lambda x_2}\\ &\quad\cdot ((g_3^{-d_1}g_4^{-d_2})^k m)\\ &\equiv (g_1^{\lambda(k_1-k'_1)}g_2^{\lambda(k_2-k'_2)}g_3^{\lambda k_3})^{kx_1}(g_1^{\lambda(k_1-k'_1)}g_2^{\lambda(k_2-k'_2)}g_4^{\lambda k_4})^{kx_2}\\ &\quad\cdot ((g_3^{-\lambda x_1 k_3}g_4^{-\lambda x_2 k_4})^k m)\\ &\equiv (g_3^{(k_3)})^{kx_1}(g_4^{\lambda k_4})^{kx_2}((g_3^{-\lambda x_1 k_3}g_4^{-\lambda x_2 k_4})^k m)\\ &\equiv m. \end{aligned}$$

该推导过程显示,g_1,g_2,g_3,g_4 在解密时并没有发挥实质性作用,因此,依据 N 的素因子和元素可能的阶数,我们可以假设 g_1,g_2,g_3,g_4 的合理的值.

这样,在大部分情况下,根据 2.3 节求解算法,$k_1,k_2,k_3,k_4,k'_1,k'_2,d_1,d_2$ 可以在亚指数时间内被求出来,并要满足 $\gcd(r_1,r_2)\nmid(k_1-k_2)$.

进而,根据 $\lambda(k_1-k'_1)=0 \bmod r_1$、$\lambda(k_2-k'_2)=0 \bmod r_2$ 和 $\lambda x_1k_3=d_1 \bmod r_3$、$\lambda x_2k_4=d_2 \bmod r_4$($r_3\nmid\lambda, r_4\nmid\lambda$),可以求出 λ 以及 x_1、x_2 的值.

3.3　密文的亚指数时间还原

密文 c 由四部分(c_1,c_2,c_3,c_4)组成,它存在亚指数时间破译方法.

输入:密文(c_1,c_2,c_3,c_4)和公钥(N,y_1,y_2,y_3,y_4).

S1:计算 $u\leftarrow c_1c_3 \bmod N$,即 $u\leftarrow (y_1y_3)^k \bmod N$.

S2:根据指数算法[11],求 k 满足 $u=(y_1y_3)^k \bmod N$.

S3:计算 m 满足 $c_4=y_4^k m \bmod N$(注意,y_4^{-k} 存在).

输出:明文 m.

这样,在亚指数时间内恢复出了原来的明文 m. 因此,密文不是抗量子计算攻击的.

4　结论

即使多离散对数问题满足定义 1、定理 1 和密钥生成算法中的限制条件,但它在原文所述情况下($\gcd(r_1,r_2)\neq 1<2^{76}$且 $\gcd(r_i,r_j)=1$ 附带 $i\neq j\neq 1,2$)还是存在亚指数时间解. 如果该有解情况被有限破坏,那么,本文 2.3 节中的求解算法应该仍然是有效的. 不过,有一点要注意,当上述有解情况被严重破坏时,从阶选择六点来看,定义 1 中的限制条件也可能同时被破坏.

由于多离散对数问题在原文所述情况下可转化为离散对数问题,因此,原加密方案中的私钥在大多数情况下也是不安全的.

更为糟糕的是,在几乎任何情况下,密文 c 都可以转化为离散对数问题,因而它不能抵御 Shor 量子算法的攻击. 这使得对多离散对数问题的研究失去了主要的应用价值.

所以,要把现有的离散对数问题和 ElGamal 加密算法改造成抗量子计算攻击的,还需做更深入的、持久的探索.

参考文献

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

[2] Grover L K. Quantum mechanics helps in searching for a needle in a Haystack[J]. Physical Review Letters,1997,79(2):325 – 328.

[3] Rivest R L,Shamir A,Adleman L M. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM,1978,21(2):120 – 126.

[4] ElGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory,1985,31(4):469 – 472.

[5] 张文芳,王小敏,郭伟,等. 基于椭圆曲线密码体制的高效虚拟企业跨域认证方案[J]. 电子学报,2014,42(6):

1095 – 1102.
ZHANG Wen-fang, WANG Xiao-min, GUO Wei, et al. An efficient inter-enterprise authentication scheme for VE based on the elliptic curve cryptosystem[J]. Acta Electronica Sinica, 2014, 42(6): 1095 – 1102. (in Chinese)

[6] 古春生,景征骏,于志敏,等. 基于遍历矩阵的公钥加密方案的安全性分析[J]. 电子学报, 2014, 42(10): 2081 – 2085.
GU Chun-sheng, JING Zheng-jun, YU Zhi-min, et al. Security on public key encryption scheme based on ergodic matrice[J]. Acta Electronica Sinica, 2014, 42(10): 2081 – 2085. (in Chinese)

[7] Su S, Lü S. A public key cryptosystem based on three new provable problems [J]. Theoretical Computer Science, 2012, 426 – 427: 91 – 117.

[8] Su S, Lü S, Fan X. Asymptotic granularity reduction and its application[J]. Theoretical Computer Science, 2011, 412(39): 5374 – 5386.

[9] Su S, Lü S. REESSE1 + Reward Proof by Experiment A New Approach to Proof of P! = NP[DB/OL]. Cornell University Library (http://arxiv.org/pdf/0908.0482/), 2009-08-04(revised 2014-08-25).

[10] 付向群,鲍皖苏,史建红,等. 基于多离散对数问题的公钥密码[J]. 电子与信息学报, 2014, 36(6): 1423 – 1427.
Fu Xiang-qun, Bao Wan-su, Shi Jian-hong, et al. Public-key cryptograph based on the multi-discrete logarithm problem[J]. Journal of Electronics & Information Technology, 2014, 36(6): 1423 – 1427. (in Chinese)

[11] Menezes A, Oorschot van P C, Vanstone S. Handbook of Applied Cryptography[M]. London, UK: CRC Press, 1996.

[12] Hungerford W T. Algebra[M]. New York: Springer-Verlag, 1998.

[13] Snaith P V. Groups, Rings and Galois Theory[M]. Singapore: World Scientific Publishing, 1998.

作者简介

苏盛辉 博士,教授,博导,研究方向为计算复杂性理论、身份认证学、密码学和网络信息安全. REESSE1 + 非对称体制、JUNA 单向散列函数与轻量级数字签名体制、JUOAN 非对称密码体制首席发明人, MPP/ASPP/TLP 三个新计算难题、渐近粒度归约方法 AGR、身份认证学(Idology)主要提出者.
E-mail: reesse@126.com

孙国栋 博士生,研究方向为非对称密码体制、非对称身份认证体制和网络信息安全.