基于热带矩阵密钥交换协议的密码分析

黄华伟[1*],李春华[2]
(1. 贵州师范大学 数学科学学院,贵州 贵阳 550001;
2. 华东交通大学 理学院,江西 南昌 330013)

摘 要:量子计算机的发展对目前广泛使用的公钥密码体制构成了潜在的威胁,具有抗量子分析性质的密码体制受到了广泛关注。由于热带半环中的乘法实际上是普通加法,具有运算效率高的优势,且求解多变量热带非线性多项式方程组是 NP 问题,近年来一些基于热带半环的公钥密码被提出。该文分析了 Grigoriev 和 Shpilrain 基于热带矩阵半环半直积的密钥交换协议安全性。定义了一种矩阵的比较大小关系,并证明了半直积运算具有部分的保序性,元素的乘法幂关于第一个分量矩阵构成了单调递减序列。据此,针对该协议,提出了一种简单的二分查找攻击算法。该算法通过公开信息可以求用户私钥,从而破解了该协议。该攻击算法的比特位运算的计算复杂度为 $O(2\log 2r(2k^3+5k^2))$,其中 r 为指数上界,k 为矩阵的阶。实验结果表明,如果协议参数选取自 Grigoriev 和 Shpilrain 建议的范围,攻击算法在一分钟内就能求出私钥。而且即使增大协议的参数,该攻击仍然有效。

关键词:公钥密码;密钥交换协议;密码分析;热带半环;热带矩阵
中图分类号:TP309.2;TN918.1 **文献标识码**:A **文章编号**:1673-629X(2023)03-0093-05
doi:10.3969/j.issn.1673-629X.2023.03.014

Cryptanalysis of a Key Exchange Protocol Based on Tropical Matrices

HUANG Hua-wei[1*],LI Chun-hua[2]
(1. School of Mathematical Sciences,Guizhou Normal University,Guiyang 550001,China;
2. School of Science,East China Jiaotong University,Nanchang 330013,China)

Abstract:With the development of quantum computer,the classical public key cryptosystems widely used will encounter potential threat. So it is currently a research focus of cryptography to explore the cryptosystems which can resist quantum attack. Because the multiplication in tropical semiring is actually the ordinary addition,it has the advantage of high operation efficiency. And the problem of solving multivariable tropical nonlinear polynomial equations is NP hard. In recent years,some public key cryptography based on tropical semiring have been proposed. We analyze the security of a key exchange protocol based on the semidirect product of tropical matrix semiring. A matrix size comparison is defined,and it is proved that the semidirect product operation has partial order preservation,and the multiplicative power of the element constitutes a monotonically decreasing sequence with respect to the first component matrix. Therefore,a simple binary search attack algorithm is proposed for the protocol. The algorithm can find the user´s private key through public information,so as to crack the protocol. The computational complexity of the bit operation of the attack algorithm is $O(2\log 2r(2k^3+5k^2))$,where r is the upper bound of the index and k is the order of the matrix. The experimental results show that if the protocol parameters are selected in the range suggested by Grigoriev and Shpilrain,the attack algorithm can find the private key in one minute. Moreover,even if the parameters of the protocol are increased,the attack is still effective.

Key words:public-key cryptography;key exchange protocol;cryptanalysis;tropical semi-ring;tropical matrix

1 概 述

量子计算机的发展对目前广泛使用的公钥密码体制构成了潜在的威胁,具有抗量子分析的密码体制受到了广泛关注[1]。目前抗量子分析密码体制主要基于交换代数结构,如交换群和交换环[2]。许多学者都希望找到可用于密码学的新的非交换代数结构。例如,Maze 提出了基于半群作用问题的公钥加密方案[3]。Baumslag 等[4]把格密码研究领域中的带噪声的学习问题推广到一般的代数群上,进而构造出非交换密码方案。Bagheri 等[5]提出基于四元数代数的非交换

收稿日期:2022-03-30 **修回日期**:2022-08-03
基金项目:国家自然科学基金资助项目(61462016,61962011);贵州省科学技术基金资助项目(黔科合基础:[2019]1221 号;ZK[2021]一般 313 号)
作者简介:黄华伟(1978-),男,副教授,CCF 会员(K4081M),通讯作者,研究方向为密码学与信息安全。

NTRU 型密码体制。Climent 等[6]提出基于非交换 Bergman 环的密码体制,但被 Zhang 破解[7]。

近年来,随着热带代数(Tropical Algebra)的研究逐渐深入,热带代数理论和计算理论研究方面都有很大进展。Grigoriev[8]提出了求解整系数热带齐次线性方程组和整系数热带非齐次线性方程组的多项式时间算法,并证明了求解实系数热带齐次线性方程组是 NP-C 问题。无论是超定还是未定的实系数热带线性方程组求解都是 NP-C 问题。Maze 等[9]首先提出了基于一类六元单半环的半群作用问题的密码体制,但 Steinwandt 等[10]利用六元单半环的运算性质破解了该方案。Atani[11]提出了基于因子半环上的半模的密码系统。Durcheva[12]提出基于幂等半环的密码协议。Ahmed 等[13]详细分析了它们的缺点并破解了这两个方案。Grigoriev, Shpilrain[14]证明了求解多变量热带非线性多项式方程组是 NP 问题,并首次使用热带矩阵半环作为平台来构造密码系统,提出了基于热带矩阵的公钥密码体制。由于热带代数只涉及数的加法和比较大小两种运算,因此基于热带代数的密码体制一般效率都非常高。2018 年,Kotov 等[15]根据整数热带矩阵的代数性质破解了该方案。2019 年,Grigoreiv, Shpilrain[16]对原方案进行了改进,提出基于热带矩阵半环的半直积的公钥密码体制。

该文主要研究文献[16]基于热带矩阵半环半直积的密钥交换协议的安全性,提出了一种攻击方法。从协议的公开信息通过简单的二分查找就可获得用户的私钥。结果表明文中的热带代数结构并不适合构建公钥密码体制。

2 整数的热带半环

令 Z 为整数集合, Z 上的热带半环[14,16](tropical semi-ring)为 $(Z\cup\{\infty\},\oplus,\otimes)$,其运算为:

$(\forall x,y\in Z)\ x\oplus y=\min\{x,y\}, x\otimes y=x+y$

$(\forall x\in Z)\ \infty\oplus x=x\oplus\infty=x,\ \infty\otimes x=x\otimes\infty=\infty$

即 $(Z\cup\{\infty\},\oplus)$ 与 $(Z\cup\{\infty\},\otimes)$ 都是半群,且 $\otimes$ 对 $\oplus$ 满足分配律。

热带半环 $(Z\cup\{\infty\},\oplus,\otimes)$ 满足以下性质[14,16]:

(1) $(Z\cup\{\infty\},\oplus)$ 是交换半群, ∞ 为单位元;

(2) $(Z\cup\{\infty\},\otimes)$ 是交换半群,无单位元;

(3) $(\forall x\in Z\cup\{\infty\})\ x\oplus x=x$。

令 $\boldsymbol{U}_k$ 为 $Z\cup\{\infty\}$ 上所有的 $k\times k$ 矩阵,即:

$$\boldsymbol{U}_k=\{(a_{ij})_{k\times k}\mid a_{ij}\in Z\cup\{\infty\}\}$$

在 $\boldsymbol{U}_k$ 上定义的热带矩阵半环为 $(\boldsymbol{U}_k,\bar{\oplus},\bar{\otimes})$,其中 $\bar{\oplus}$、$\bar{\otimes}$ 的定义类似于通常的矩阵加法和乘法,只不过每个矩阵元素计算中所有加法都是 $\oplus$,所有乘法都是 $\otimes$。例如:

$$\begin{pmatrix}1&2\\5&-1\end{pmatrix}\bar{\oplus}\begin{pmatrix}0&3\\2&8\end{pmatrix}=\begin{pmatrix}0&2\\2&-1\end{pmatrix}$$

$$\begin{pmatrix}1&2\\5&-1\end{pmatrix}\bar{\otimes}\begin{pmatrix}0&3\\2&8\end{pmatrix}=\begin{pmatrix}1&4\\1&7\end{pmatrix}$$

热带矩阵半环 $(\boldsymbol{U}_k,\bar{\oplus},\bar{\otimes})$ 满足以下性质[16]:

(1) $(\boldsymbol{U}_k,\bar{\oplus})$ 是交换半群, ∞_k 为单位元(∞_k 表示所有元素都是 ∞ 的 $k\times k$ 矩阵);

(2) $(\boldsymbol{U}_k,\bar{\otimes})$ 是非交换半群, $\boldsymbol{I}_k$ 单位元($\boldsymbol{I}_k$ 表示对角线元素都是 0,其他所有元素都是 ∞ 的 $k\times k$ 矩阵);

(3) $(\forall \boldsymbol{A}\in U_k)\ \boldsymbol{A}\bar{\oplus}\boldsymbol{A}=\boldsymbol{A}$;

在 $\boldsymbol{U}$ 上定义运算。如下:

$$(\forall \boldsymbol{A},\boldsymbol{B}\in\boldsymbol{U}_k)\boldsymbol{A}\circ\boldsymbol{B}=\boldsymbol{A}\bar{\oplus}\boldsymbol{B}\bar{\oplus}(\boldsymbol{A}\bar{\otimes}\boldsymbol{B})$$

则 $(\boldsymbol{U},\bar{\oplus},\circ)$ 也是半环。

引理[16]:令 $\Omega=\{(\boldsymbol{M},\boldsymbol{H})\mid\boldsymbol{M},\boldsymbol{H}\in\boldsymbol{U}_k\}$,在 Ω 上定义运算 $\bullet$ 如下:

$$(\forall(\boldsymbol{M}_1,\boldsymbol{H}_1),(\boldsymbol{M}_2,\boldsymbol{H}_2)\in\Omega)$$

$$(\boldsymbol{M}_1,\boldsymbol{H}_1)\bullet(\boldsymbol{M}_2,\boldsymbol{H}_2)=((\boldsymbol{M}_1\circ\boldsymbol{H}_2)\bar{\oplus}\boldsymbol{M}_2,\boldsymbol{H}_1\circ\boldsymbol{H}_2)$$

则 Ω 的运算 $\bullet$ 满足结合律,即 $(\Omega,\bullet)$ 是半群。称 $(\Omega,\bullet)$ 为热带矩阵半环半直积。

下文中约定:$(\forall\boldsymbol{A}\in\boldsymbol{U})\ \boldsymbol{A}^n$ 表示 $\underbrace{\boldsymbol{A}\circ\boldsymbol{A}\circ\cdots\circ\boldsymbol{A}}_{n}$;

$(\forall\boldsymbol{M},\boldsymbol{H}\in\boldsymbol{U})\ (\boldsymbol{M},\boldsymbol{H})^n$ 表示

$$\underbrace{(\boldsymbol{M},\boldsymbol{H})\bullet(\boldsymbol{M},\boldsymbol{H})\bullet\cdots\bullet(\boldsymbol{M},\boldsymbol{H})}_{n}$$

为简便,在下文中约定:$\boldsymbol{A}+\boldsymbol{B}$ 表示 $\boldsymbol{A}\bar{\oplus}\boldsymbol{B}$, $\boldsymbol{AB}$ 表示 $\boldsymbol{A}\circ\boldsymbol{B}$。在该记法下有:

$$(\boldsymbol{M}_1,\boldsymbol{H}_1)\bullet(\boldsymbol{M}_2,\boldsymbol{H}_2)=(\boldsymbol{M}_1\boldsymbol{H}_2+\boldsymbol{M}_2,\boldsymbol{H}_1\boldsymbol{H}_2)$$

3 热带矩阵半环半直积的密钥交换协议

用户 Alice 与用户 Bob 希望通过协议交换共享密钥。首先,他们选取公开的 $\boldsymbol{M},\boldsymbol{H}\in\boldsymbol{U}_k$, Alice 选取保密的正整数 m, Bob 选取保密的正整数 n。

文献[16]的基于热带矩阵半环半直积的密钥交换协议如下:

(1) Alice 计算 $(\boldsymbol{M},\boldsymbol{H})^m=(\boldsymbol{A},\boldsymbol{H}^m)$,将 $\boldsymbol{A}$ 发送给 Bob;

(2) Bob 计算 $(\boldsymbol{M},\boldsymbol{H})^n=(\boldsymbol{B},\boldsymbol{H}^n)$,将 $\boldsymbol{B}$ 发送给 Alice;

(3) Alice 计算 $\boldsymbol{K}_A=\boldsymbol{B}\boldsymbol{H}^m+\boldsymbol{A}$;Bob 计算 $\boldsymbol{K}_B=\boldsymbol{A}\boldsymbol{H}^n+\boldsymbol{B}$。

因为,

$$(\boldsymbol{M},\boldsymbol{H})^{m+n}=(\boldsymbol{M},\boldsymbol{H})^{m}\bullet(\boldsymbol{M},\boldsymbol{H})^{n}=$$
$$(\boldsymbol{A},\boldsymbol{H}^{m})\bullet(\boldsymbol{B},\boldsymbol{H}^{n})=$$
$$(\boldsymbol{A}\boldsymbol{H}^{n}+\boldsymbol{B},\boldsymbol{H}^{m+n})$$
$$(\boldsymbol{M},\boldsymbol{H})^{m+n}=(\boldsymbol{M},\boldsymbol{H})^{n}\bullet(\boldsymbol{M},\boldsymbol{H})^{m}=$$
$$(\boldsymbol{B},\boldsymbol{H}^{n})\bullet(\boldsymbol{A},\boldsymbol{H}^{m})=$$
$$(\boldsymbol{B}\boldsymbol{H}^{m}+\boldsymbol{A},\boldsymbol{H}^{m+n})$$

所以,Alice 与 Bob 交换了共享密钥 $\boldsymbol{K}=\boldsymbol{K}_A=\boldsymbol{K}_B$。

例 1:Alice 和 Bob 选取公开的 $\boldsymbol{M}=\begin{pmatrix}1&-2\\-3&4\end{pmatrix}$, $\boldsymbol{H}=\begin{pmatrix}-5&6\\7&-8\end{pmatrix}$,Alice 选取保密的正整数 $m=13$,Bob 选取保密的正整数 $n=11$。Alice 与 Bob 执行密钥交换协议如下:

(1)Alice 计算

$$(\boldsymbol{M},\boldsymbol{H})^{13}=\left(\begin{pmatrix}1&-2\\-3&4\end{pmatrix},\begin{pmatrix}-5&6\\7&-8\end{pmatrix}\right)^{13}=$$
$$\left(\begin{pmatrix}-83&-98\\-81&-96\end{pmatrix},\begin{pmatrix}-75&-90\\-89&-104\end{pmatrix}\right)=(\boldsymbol{A},\boldsymbol{H}^{13})$$

将 $\boldsymbol{A}=\begin{pmatrix}-83&-98\\-81&-96\end{pmatrix}$ 发送给 Bob。

(2)Bob 计算

$$(\boldsymbol{M},\boldsymbol{H})^{11}=\left(\begin{pmatrix}1&-2\\-3&4\end{pmatrix},\begin{pmatrix}-5&6\\7&-8\end{pmatrix}\right)^{11}=$$
$$\left(\begin{pmatrix}-67&-82\\-65&-80\end{pmatrix},\begin{pmatrix}-59&-74\\-73&-88\end{pmatrix}\right)=(\boldsymbol{B},\boldsymbol{H}^{11})$$

将 $\boldsymbol{B}=\begin{pmatrix}-67&-82\\-65&-80\end{pmatrix}$ 发送给 Alice。

(3)Alice 计算

$$\boldsymbol{K}_A=\boldsymbol{B}\boldsymbol{H}^{13}+A=$$
$$\begin{pmatrix}-67&-82\\-65&-80\end{pmatrix}\circ\begin{pmatrix}-75&-90\\-89&-104\end{pmatrix}\bar{\oplus}$$
$$\begin{pmatrix}-83&-98\\-81&-96\end{pmatrix}=\begin{pmatrix}-171&-186\\-169&-184\end{pmatrix}$$

Bob 计算

$$\boldsymbol{K}_B=\boldsymbol{A}\boldsymbol{H}^{11}+B=$$
$$\begin{pmatrix}-83&-98\\-81&-96\end{pmatrix}\circ\begin{pmatrix}-59&-74\\-73&-88\end{pmatrix}\bar{\oplus}$$
$$\begin{pmatrix}-67&-82\\-65&-80\end{pmatrix}=\begin{pmatrix}-171&-186\\-169&-184\end{pmatrix}$$

该协议的优点是执行速度很快,因为所有的运算都只有整数的加法和比较大小。

4　基于热带矩阵半环半直积的密钥交换协议的密码分析

从协议可知矩阵 $\boldsymbol{M},\boldsymbol{H},\boldsymbol{A},\boldsymbol{B}$ 都是公开的,正整数 m,n 是保密的。如果能求出正整数 m 或 n,那么易求出共享密钥。

由整数热带半环的加法定义 $x\oplus y=\min\{x,y\}$,显然 $x\oplus y\leqslant x$,且 $x\oplus y\leqslant y$。下面定义一种矩阵的比较大小关系,易知热带矩阵加法也有类似的性质。

定义 1:令 $\boldsymbol{A}=(a_{ij}),\boldsymbol{B}=(b_{ij})\in\boldsymbol{U}_k$,若 $\forall i,j(1\leqslant i\leqslant k,1\leqslant j\leqslant k)$ 都有 $a_{ij}\leqslant b_{ij}$,则称矩阵 $\boldsymbol{A}$ 小于等于矩阵 $\boldsymbol{B}$,记为 $\boldsymbol{A}\leqslant\boldsymbol{B}$。

定义 2:令 $\boldsymbol{A}=(a_{ij}),\boldsymbol{B}=(b_{ij})\in\boldsymbol{U}_k$,若 $\forall i,j(1\leqslant i\leqslant k,1\leqslant j\leqslant k)$ 都有 $a_{ij}\leqslant b_{ij}$ 且存在 $i,j(1\leqslant i\leqslant k,1\leqslant j\leqslant k)$ 使 $a_{ij}<b_{ij}$,则称矩阵 $\boldsymbol{A}$ 小于矩阵 $\boldsymbol{B}$,记为 $\boldsymbol{A}<\boldsymbol{B}$。

定理 1:令 $\boldsymbol{A}=(a_{ij}),\boldsymbol{B}=(b_{ij})\in\boldsymbol{U}_k$,则 $\boldsymbol{A}+\boldsymbol{B}\leqslant\boldsymbol{A}$,且 $\boldsymbol{A}+\boldsymbol{B}\leqslant\boldsymbol{B}$。

证明:由于 $\boldsymbol{A}+\boldsymbol{B}=\boldsymbol{A}\bar{\oplus}\boldsymbol{B}=(a_{ij}\oplus b_{ij})_{k\times k}$,而 $\forall i,j(1\leqslant i\leqslant k,1\leqslant j\leqslant k)$ 都有 $a_{ij}\oplus b_{ij}\leqslant a_{ij}$,且 $a_{ij}\oplus b_{ij}\leqslant b_{ij}$。因此,$\boldsymbol{A}+\boldsymbol{B}\leqslant\boldsymbol{A}$,且 $\boldsymbol{A}+\boldsymbol{B}\leqslant\boldsymbol{B}$。

由运算定义:

$$(\boldsymbol{M}_1,\boldsymbol{H}_1)\bullet(\boldsymbol{M}_2,\boldsymbol{H}_2)=(\boldsymbol{M}_1\boldsymbol{H}_2+\boldsymbol{M}_2,\boldsymbol{H}_1\boldsymbol{H}_2)$$
$$(\boldsymbol{M}_1,\boldsymbol{H}_1)^2=(\boldsymbol{M}_1\boldsymbol{H}_1+\boldsymbol{M}_1,\boldsymbol{H}_1^2)$$

根据命题 1,$\boldsymbol{M}_1\boldsymbol{H}_1+\boldsymbol{M}_1\leqslant\boldsymbol{M}_1$,因此 $(\boldsymbol{M}_1,\boldsymbol{H}_1)^2$ 的第一个分量矩阵小于 $(\boldsymbol{M}_1,\boldsymbol{H}_1)$ 的第一个分量矩阵。类似地,$(\boldsymbol{M}_1,\boldsymbol{H}_1)^3$ 的第一个分量矩阵小于 $(\boldsymbol{M}_1,\boldsymbol{H}_1)^2$ 的第一个分量矩阵,……。因此 $(\boldsymbol{M}_1,\boldsymbol{H}_1)$,$(\boldsymbol{M}_1,\boldsymbol{H}_1)^2$,$(\boldsymbol{M}_1,\boldsymbol{H}_1)^3$,……。关于第一个分量矩阵是一个递减矩阵序列。

例 2:令 $\boldsymbol{M}=\begin{pmatrix}1&-2\\-3&4\end{pmatrix},H=\begin{pmatrix}-5&6\\7&-8\end{pmatrix}$,则 $\{(\boldsymbol{M}_1,\boldsymbol{H}_1)^n\}$ 如下:

$$(\boldsymbol{M},\boldsymbol{H})^1=\left(\begin{pmatrix}1&-2\\-3&4\end{pmatrix},\begin{pmatrix}-5&6\\7&-8\end{pmatrix}\right)$$
$$(\boldsymbol{M},\boldsymbol{H})^2=\left(\begin{pmatrix}-5&-10\\-8&-8\end{pmatrix},\begin{pmatrix}-10&-2\\-1&-16\end{pmatrix}\right)$$
$$(\boldsymbol{M},\boldsymbol{H})^3=\left(\begin{pmatrix}-10&-18\\-13&-16\end{pmatrix},\begin{pmatrix}-15&-10\\-9&-24\end{pmatrix}\right)$$
$$(\boldsymbol{M},\boldsymbol{H})^4=\left(\begin{pmatrix}-15&-26\\-18&-24\end{pmatrix},\begin{pmatrix}-20&-18\\-17&-32\end{pmatrix}\right)$$
……

由协议知,$(\boldsymbol{M},\boldsymbol{H})^m=(\boldsymbol{A},\boldsymbol{H}^m)$,容易看到,通过简单的二分查找就可以由 $\boldsymbol{A}$ 求出 m。

假设用户 $\boldsymbol{A}$ 的私钥整数 m 满足:$1\leqslant m\leqslant r$,则攻击算法如下:

基于热带矩阵半环半直积的密钥交换协议的攻击算法:

输入:矩阵 $\boldsymbol{M},\boldsymbol{H},\boldsymbol{A}$(满足 $(\boldsymbol{M},\boldsymbol{H})^m=(\boldsymbol{A},\boldsymbol{H}^m)$);

输出：m

(1)令 left=1,right=r;

(2)若 left ≤ right ,执行下面循环

(i) mid = left + (right - left)/2;

(ii)计算 $(\boldsymbol{M},\boldsymbol{H})^{\text{mid}} = (\boldsymbol{P},\boldsymbol{Q})$

若 $\boldsymbol{P} < \boldsymbol{A}$,则 right = mid - 1;

若 $\boldsymbol{A} < \boldsymbol{P}$,则 left = mid + 1;

若 $\boldsymbol{P} = \boldsymbol{A}$,则输出 m = mid 结束。

注：由于 $(\boldsymbol{M}_1,\boldsymbol{H}_1) \bullet (\boldsymbol{M}_2,\boldsymbol{H}_2) = ((\boldsymbol{M}_1 \bar{\oplus} \boldsymbol{H}_2 \bar{\oplus} (\boldsymbol{M}_1 \bar{\otimes} \boldsymbol{H}_2)) \bar{\oplus} \boldsymbol{M}_2, \boldsymbol{H}_1 \bar{\oplus} \boldsymbol{H}_2 \bar{\oplus} (\boldsymbol{H}_1 \bar{\otimes} \boldsymbol{H}_2))$。因此，两个半直积元素的乘法需 2 次热带矩阵乘法和 5 次热带矩阵加法。如果 $(\boldsymbol{M},\boldsymbol{H})^{\text{mid}}$ 的指数运算采用平方乘快速算法，则最多需要 $2\log_2 r$ 次半直积乘法。因此，该攻击算法的比特位运算的计算复杂度为 $O(2\log_2 r(2k^3 + 5k^2))$。因此，该攻击算法十分有效。

例 3：用上述算法破解例 1。

在 Intel(R) Core(TM) i7-5500 CPU @ 2.40 GHz 处理器的计算机上运行攻击算法的 C 程序。

输入 $\boldsymbol{M} = \begin{pmatrix} 1 & -2 \\ -3 & 4 \end{pmatrix}$，$\boldsymbol{H} = \begin{pmatrix} -5 & 6 \\ 7 & -8 \end{pmatrix}$，$\boldsymbol{A} = \begin{pmatrix} -83 & -98 \\ -81 & -96 \end{pmatrix}$。在 0.038 秒输出 m = 13，得到了 Alice 的私钥。

输入 $\boldsymbol{M} = \begin{pmatrix} 1 & -2 \\ -3 & 4 \end{pmatrix}$，$\boldsymbol{H} = \begin{pmatrix} -5 & 6 \\ 7 & -8 \end{pmatrix}$，$\boldsymbol{A} = \begin{pmatrix} -67 & -82 \\ -65 & -80 \end{pmatrix}$。在 0.013 秒输出 m = 11，得到了 Bob 的私钥。

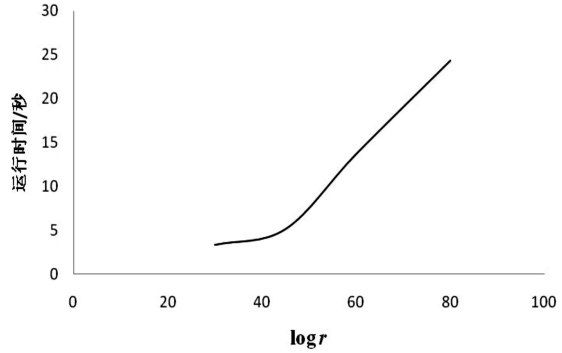
最后，采用平方乘快速算法计算 $(\boldsymbol{M},\boldsymbol{H})^{11+13} = \left(\begin{pmatrix} -171 & -186 \\ -169 & -184 \end{pmatrix}, \begin{pmatrix} -163 & -178 \\ -177 & -192 \end{pmatrix}\right)$，提取第一个分量矩阵即得共享 Alice 和 Bob 的共享密钥 $K = \begin{pmatrix} -171 & -186 \\ -169 & -184 \end{pmatrix}$。

实验一：

按照文献[16]的建议参数：矩阵的阶 k = 30，矩阵的元属于[-1 000,1 000]，在 Intel(R) Core(TM) i7-5500 CPU @ 2.40 GHz 处理器的计算机上运行攻击算法的 C 程序，结果见表 1 和图 1。

表 1 攻击算法运行时间随指数变化情况

指数 m 的上界 r	运行时间/s
2^{30}	3.328
2^{45}	5.133
2^{60}	13.694
2^{80}	24.345



(注：r 为指数的上界)

图 1 攻击算法运行时间随指数变化情况

实验二：

指数固定为 $m = 2^{50} - 1$，$r = 2^{62} - 1$，矩阵元素取自[-1 000,1 000]。在 Intel(R) Core(TM) i7-4700MQ CPU @ 2.40 GHz 处理器的计算机上运行攻击算法的 C 程序，结果见表 2 和图 2。

表 2 攻击算法运行时间随矩阵阶 k 变化情况

矩阵的阶 k	运行时间/s
5	0.175
10	0.876
15	2.296
20	4.918
25	8.772
30	14.461
32	16.764
34	19.760
36	23.170
38	26.503
40	31.271
42	35.292

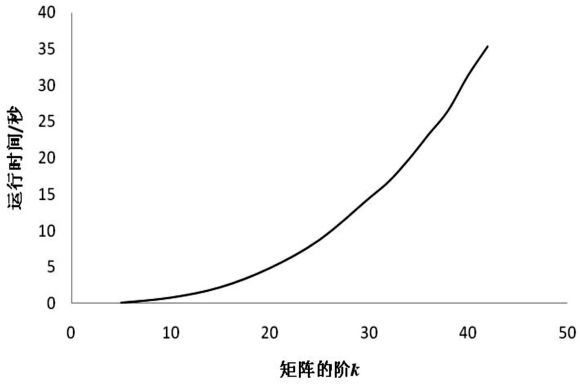
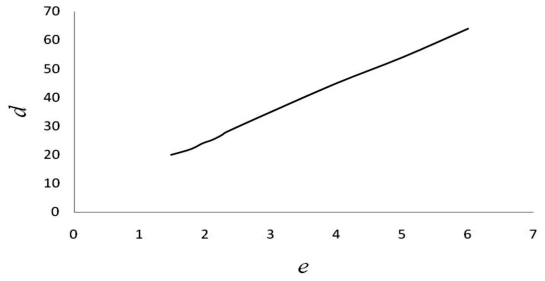


图 2 攻击算法运行时间随矩阵阶 k 变化情况

固定为 r = 80，攻击算法的时间复杂度随矩阵阶 k 增大的情况比较见表 3，攻击算法时间复杂度随矩阵阶变化情况见图 3。

表 3　攻击算法时间复杂度随矩阵阶 k 变化情况

矩阵的阶 k	时间复杂度
30	$O(2^{20})$
60	$O(2^{22})$
90	$O(2^{24})$
120	$O(2^{25})$
150	$O(2^{26})$
180	$O(2^{27})$
210	$O(2^{28})$
10^3	$O(2^{35})$
10^4	$O(2^{45})$
10^5	$O(2^{54})$
10^6	$O(2^{64})$



(注:矩阵的阶为 10^e,攻击算法时间复杂度 $O(2^d)$)

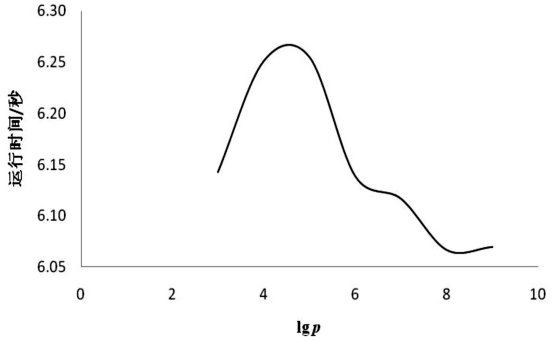
图 3　攻击算法时间复杂度随矩阵阶变化情况

实验三:

指数固定为 $m=2^{30}-1$,$r=2^{45}-1$,矩阵的阶固定为 $k=30$。在 Intel(R) Core(TM) i7-4700MQ CPU @ 2.40 GHz 处理器的计算机上运行攻击算法的 C 程序,结果见表 4 和图 4。

表 4　攻击算法运行时间随矩阵元素取值范围变化情况

矩阵元素取值范围	运行时间/s
$[-10^3,10^3]$	6.143
$[-10^4,10^4]$	6.251
$[-10^5,10^5]$	6.255
$[-10^6,10^6]$	6.139
$[-10^7,10^7]$	6.117
$[-10^8,10^8]$	6.067
$[-10^9,10^9]$	6.070



(注:矩阵元素取值范围为 $[-p,p]$)

图 4　攻击算法运行时间随矩阵元素取值范围变化情况

实验三表明,矩阵元素的取值范围对攻击算法的时间复杂度影响不大。

5　结束语

该文分析了 Grigoriev 和 Shpilrain[16] 提出的基于热带矩阵半环半直积密钥交换协议的安全性,在 $\Omega=\{(\boldsymbol{M},\boldsymbol{H})\mid \boldsymbol{M},\boldsymbol{H}\in \boldsymbol{U}_k\}$ 定义的半直积运算具有部分的保序性,由其乘法定义 $(\boldsymbol{M}_1,\boldsymbol{H}_1)\bullet(\boldsymbol{M}_2,\boldsymbol{H}_2)=(\boldsymbol{M}_1\boldsymbol{H}_2+\boldsymbol{M}_2,\boldsymbol{H}_1\boldsymbol{H}_2)$ 可知,其第一个矩阵分量小于等于 $\boldsymbol{M}_2$,这使得 $\{(\boldsymbol{M}_1,\boldsymbol{H}_1)^n\}$ 关于第一个分量矩阵构成了一个单调递减序列。据此,给出了一种二分查找的攻击算法。该算法通过公开信息可以求用户密钥,从而破解了该协议。该攻击算法的比特位运算的计算复杂度为 $O(2\log_2 r(2k^3+5k^2))$,其中 r 为指数上界,k 为矩阵的阶。实验结果表明,如果协议参数选取自 Grigoriev 和 Shpilrain 建议的范围,攻击算法在 1 分钟之内就能求出私钥。矩阵元素的取值范围对攻击算法的时间复杂度影响不大。对攻击算法有影响的参数是矩阵的阶 k 和指数取值的上界 r,而其中矩阵的阶 k 的影响又是最主要的。从表 3 可以看到,除非将矩阵的阶增大到 100 万阶以上,否则即使增大协议的参数,该攻击仍然有效。因此,热带半环代数结构 $(\Omega,\bullet)$ 并不适合构建安全的密码体制。

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

[3] 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. Lausanne:IEEE,2002:266-289.

[4] BAUMSLAG G,FAZIO N,NICOLOSI A R,et al. Generalized learning problems and applications to non-commutative cryptography[C]//Lecture notes in computer science. Berlin:Springer,2011:324-339.

[5] BAGHERI K,SADEGHI M R,PANARIO D. A non-commutative cryptosystem based on quaternion algebras[J]. Designs,Codes and Cryptography,2018,86:2345-2377.

[6] CLIMENT J,NAVARRO P,LEANDRO T. 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.

[7] ZHANG Y. Cryptanalysis of a key exchange protocol based on the ring Ep(m)[J]. Applicable Algebra in Engineering,

(下转第 104 页)