热带 Linde-de-la Puente 矩阵的密码应用

潘戈洋，黄华伟，姜　鑫
（贵州师范大学 数学科学学院，贵州 贵阳 550025）

摘要：近年来，一些密码学研究者提出了基于热带代数半环的公钥密码，例如 Grigoriev 和 Shpilrain 提出了几个有关热带半环密码方案，但他们设计的方案都存在安全缺陷。为了解决有关他们设计方案中存在的缺陷，将采用一种新的热带 Linde-de-la Puente 矩阵的形式，设计一类新的热带半环密钥交换协议和公钥加密系统。该协议的安全性可归约为求解热带非线性整数方程组的 NP 困难问题。由于私钥矩阵不能用已知矩阵线性表示，因此可以抵抗 KU 攻击，该密码系统没有使用热带矩阵加法运算，因此同样也可以抵抗 RM 攻击，在抵御敌手攻击方面要优于 Grigoriev 和 Shpilrain 的方案。

关键词：公钥密码；密钥交换协议；公钥加密方案；热带代数半环；热带 Linde-de-la Puente 矩阵
中图分类号：TP309　　**文献标识码：**A　　**文章编号：**2096-9759(2023)06-0024-05

Cryptographic applications of the tropical Linde-de-la Puente matrix

PAN Ge yang, HUANG Hua wei, JIANG Xin
（College of Mathematical Sciences,Guizhou Normal University,Guiyang, 550025,China）

Abstract: In recent years, some cryptographic researchers have proposed public key cryptography based on tropical algebraic semirings.For example,Grigoriev and Shpilrain have proposed several schemes concerning tropical semirings, but the schemes they designed have security flaws. In order to address the shortcomings concerning their design scheme, a new class of tropical semiring key exchange protocols and public key cryptosystems will be designed in the form of a new tropical Linde-de-la Puente matrix.The security of this protocol can be reduced to the NP-hard problem of solving tropical nonlinear systems of integer equ ations. Since the private key matrix cannot be represented linearly by a known matrix and is therefore resistant to KU attacks, the cryptosystem does not use tropical matrix addition operations and is therefore similarly resistant to RM attacks, outperforming Grigoriev and Shpilrain's scheme in terms of resistance to adversary attacks.

Key words: Public Key Passwords; Key Exchange Protocol; Public key encryption schemes; Tropical algebraic semi-ring; Tropical Linde-de-la Puente Matrix

1 引言

密钥交换协议最初由 Diffie 和 Hellman[1]提出的。他们首次提出基于离散对数问题的密钥交换协议。随着计算机技术的发展，特别是在研究最新的量子计算机的进展中，目前基于 RSA 公钥方案以及基于 ElGamal 的公钥方案将会被未来的量子计算机攻破。特别是在 1996 年 Shor 在他的论文中[2]提出了一种量子算法可以在多项式时间内解决大数分解问题以及离散对数问题。因此，现如今迫切需要一些新的密钥交换协议。Maze 和 Monico 在 2002 年首次提出了基于半群作用问题的扩展 DH 密钥交换协议[3]，在 2007 年他们对半群作用于公钥密码学上进行了更加完善的补充[4]。2005 年，Stickel 根据 Diffie 和 Hellman 的思想，构建了一种密钥交换的方法[5]，其设计是建立在非交换群上的，但后来被人证实难以抵抗线性代数的攻击。许多学者希望能在其他代数结构设计类似的密钥交换协议。

Vandiver 首次提出了半环概念[6]。除了元素不存在加法逆这个性质以外，半环基本上拥有和环相同的性质。上世纪 80 年代巴西数学家 Imre Simon[7-8]首次提出了热带半环的结构。与一般的代数结构相比，热带半环的优势在于它的运算只涉及到比较大小以及加法运算，运算结构简洁，没有涉及数的乘法和除法。Grigoriev 和 Shpilrain 首次采用热带代数半环结构构造密钥交换协议[9]。在该协议中，密钥交换的双方都选取了随机的热带多项式，并将随机的热带多项式作用于热带矩阵，从而达到交换密钥的结果。但 Kotov 和 Ushakov 对 Grigoriev 和 Shpilrain 提出的密钥交换协议进行密码分析，提供了一些启发式的攻击方案[10]。针对热带矩阵元素范围包含负数的情况，对热带矩阵多次求幂发现热带矩阵的每一项很快就会变成负数，并且随着幂的次数增加而变小。根据这一规律可以制定相应的有效攻击方案。对热带矩阵不包含负数的情况，该启发式攻击的成功率骤降。因此 Kotov 和 Ushakov 也提出了一种更为广泛的一般式攻击。由于 Grigoriev 和 Shpilrain 提出的密钥交换协议中的热带矩阵是公开的，因而可以将保密的热带矩阵多项式用公开矩阵线性表示，通过求解热带非线性方程组将未知数求出，从而破解了保密的热带多项式。虽然该方法并不是多项式时间的，但对于次数较低的多项式和阶数较小的矩阵，该方法能够在可接受的时间内求出共享密钥。

针对 Kotov 和 Ushakov 提出的这种启发式攻击，Grigoriev 和 Shpilrain 对该密钥交换协议提出了一种新的改进，在 2019 年，他们提出基于热带矩阵半直积的密钥交换协议 [11]。然而 Rudy 和 Monico 发现由于热带矩阵半直积的密钥交换协议中采用的热带矩阵加法运算使得半直积的幂呈现部分保序性，可以采用二分法搜索的方法有效攻击该方案[12]。2020 年，Isaac 和 Kahrobaei 两人提出了一种比 Rudy 和 Monico 的二分法攻击方案还要更快一些的攻击方案[13]，他们发现在 Grigoriev 和 Shpilrain 所使用的参数下的热带矩阵具有周期性的特性，因此他们利用这一特性只要找出周期，便能快速攻破方案。

近年来，由于热带代数计算的高效性与便捷性，也诞生出

收稿日期：2023-03-13
基金项目：国家自然科学基金资助项目（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）。
作者简介：潘戈洋（1998-），男，广东韶关人，研究生，硕士，主要研究方向：密码学和代数学；黄华伟（1978-），男，江西樟树人，博士，副教授，硕士生导师，主要研究方向：密码学和代数学；姜鑫（1997-），男，贵州遵义人，研究生，硕士，主要研究方向：密码学和代数学。

许多基于热带代数以及相应的衍生设计的密钥交换协议，例如在 2022 年中 Huawei Huang 和 Chunhua Li 和 Lunzhi Deng 设计了一种在热带半环下通过定义一种新的热带循环矩阵来构造的密钥交换协议[14]，以及 Ahmed 和 Mohan 在 2022 年中通过修改热带代数结构而设计一种新的密钥交换协议[15]。

本文设计了一类新的基于热带 Linde-de-la Puente 矩阵的密钥交换协议和公钥加密方案，方案所使用的公钥与私钥都是采用极小加热带整数半环矩阵，设计密钥交换协议的安全性可归约为求解热带非线性方程组的 NP 困难问题。

本文的其余部分安排如下，第 2 节介绍了一些和本文有关的预备知识，第 3 节给出了基于热带 Linde-de-la Puente 矩阵的密钥交换协议和公钥加密方案，第 4 节对提出的密码系统进行安全性分析，第 5 节是给出了结论以及可能研究的问题。

2 预备知识

半环是类似于环的特殊代数结构，但是半环不同于环的在于它不要求每个元素都存在加法逆。

定义 1（半环）非空集合 R 中包含两个二元运算：分别是加法（+）和乘法（.）如果这个非空集合满足以下四个条件：

（1）$(R,+)$ 是交换幺半群，且有单位元 0；

（2）$(R,+,\cdot)$ 是幺半群，有单位元 1，并且 $1\neq 0$；

（3）乘法对加法满足左右分配律，即：

$$\forall a,b,c\in R,\ a\cdot(b+c)=(a\cdot b)+(a\cdot c),\quad (a+b)\cdot c=(a\cdot c)+(b\cdot c) \tag{1}$$

（4）$\forall a\in R$，有 $a\cdot 0=0\cdot a=0$

如果满足以上四个条件，那么非空集合 R 与这两个二元运算共同构成了一个半环。

定义 2（热带整数半环）：定义两种结构类似的热带整数半环，分别是极小加热带整数半环 $(\mathbb{Z}\cup\{\infty\},\underset{\min}{\oplus},\underset{\min}{\otimes})$ 以及极大加热带整数半环 $(\mathbb{Z}\cup\{-\infty\},\underset{\max}{\oplus},\underset{\max}{\otimes})$，其中的加法和乘法定义如 S 下：

极小加热带整数半环：

$$\forall x,y\in\mathbb{Z},x\underset{\min}{\oplus}y=\min(x,y),x\underset{\min}{\otimes}y=x+y \tag{2}$$

极大加热带整数半环：

$$\forall x,y\in\mathbb{Z},x\underset{\max}{\oplus}y=\max(x,y),x\underset{\max}{\otimes}y=x+y \tag{3}$$

这两种热带整数半环分别都有对应的加法与乘法单位元，在极小加热带整数半环中，有 $x\underset{\min}{\oplus}\infty=x,x\underset{\min}{\otimes}0=x$，因此它的加法单位元是 ∞，它的乘法单位元是 0。

在极大加热带整数半环中，有 $x\underset{\max}{\oplus}-\infty=x,x\underset{\max}{\otimes}0=x$，因此它的加法单位元是 $-\infty$，它的乘法单位元是 0。这两类半环分别记为 Z_{min} 和 Z_{max}。

很容易验证得出极小加热带整数半环 Z_{min} 以及极大加热带整数半环 Z_{max} 都是交换半环。热带矩阵的加法和乘法以及热带多项式同样也可以类比于普通代数的矩阵加法和乘法，以及多项式，只是其中的运算按照热带代数的定义实行，示例如下所示。我们将所有 Z_{min} 和 Z_{max} 上的 n 阶方阵构成的矩阵半环记为 $\mathbf{Z}_{\min}^{n\times n}$ 和 $\mathbf{Z}_{\max}^{n\times n}$。

例 1. 在热带二阶矩阵 A 和 B 中，令 $A=\begin{pmatrix}8&3\\1&7\end{pmatrix}$，$B=\begin{pmatrix}6&5\\1&4\end{pmatrix}$，则有：

$$\begin{aligned}&A\underset{\min}{\oplus}B=\begin{pmatrix}8&3\\1&7\end{pmatrix}\underset{\min}{\oplus}\begin{pmatrix}6&5\\1&4\end{pmatrix}=\begin{pmatrix}6&3\\1&4\end{pmatrix},\quad A\underset{\max}{\oplus}B=\begin{pmatrix}8&3\\1&7\end{pmatrix}\underset{\max}{\oplus}\begin{pmatrix}6&5\\1&4\end{pmatrix}=\begin{pmatrix}8&5\\1&7\end{pmatrix}\\&A\underset{\min}{\otimes}B=\begin{pmatrix}8&3\\1&7\end{pmatrix}\underset{\min}{\otimes}\begin{pmatrix}6&5\\1&4\end{pmatrix}=\begin{pmatrix}4&7\\7&6\end{pmatrix},\quad A\underset{\max}{\otimes}B=\begin{pmatrix}8&3\\1&7\end{pmatrix}\underset{\max}{\otimes}\begin{pmatrix}6&5\\1&4\end{pmatrix}=\begin{pmatrix}14&13\\8&11\end{pmatrix}\end{aligned} \tag{4}$$

下面给出一些符号的解释说明，$[n]$ 表示的是从 1 到 n 之间的整数，$[2r,r]$ 表示的是取值范围从 2r 到 r 之间的整数，其中 r 是一个负数。

定义 3　整数 $r\leq 0,k_1\geq 0$，在 $\mathbf{Z}_{\max}^{n\times n}$ 上满足下列条件的所有矩阵记为 $[2r,r]_n^{k_1}$，

（1）$\forall i\in[n]$，$a_{ii}=k_1\geq 0$

（2）$\forall i,j\in[n],i\neq j$，有 $a_{ij}\in[2r,r]$。这类矩阵最早由 J. Linde，M. J. de la Puente 提出[16]，在文献[17]中被称为 Linde-de-la Puente 矩阵，并证明了任意两个 $\mathbf{Z}_{\max}^{n\times n}$ 中的 Linde-de-la Puente 矩阵满足交换律。本文考察了 $\mathbf{Z}_{\min}^{n\times n}$ 中的 Linde-de-la Puente 型矩阵，我们发现它们同样满足交换律，这类矩阵我们简称为热带 Linde-de-la Puente 矩阵（或热带 LP 矩阵）。

定义 4　整数 $c\geq 0,k_1\leq 0$，在 $\mathbf{Z}_{\min}^{n\times n}$ 上满足下列条件的所有矩阵记为 $[c,2c]_n^{k_3}$，

（1）$\forall i\in[n]$，$a_{ii}=k_1\leq 0$

（2）$\forall i,j\in[n],i\neq j$，有 $a_{ij}\in[2r,r]$。将这种矩阵统称为热带 Linde-de-la Puente 矩阵，简称为热带 LP 矩阵。

后文内容并没有涉及到极大加热带整数半环，为方便，本文后续内容中的 $\mathbf{Z}_{\min}$ 和 $\mathbf{Z}_{\min}^{n\times n}$ 的运算简记为 $\oplus$ 和 $\otimes$。

定理 1　令 $A\in[c,2c]_n^{k_1}$，$B\in[d,2d]_n^{k_2}$。$\forall c,d\geq 0$ 和 $a_{ii}=k_1\leq 0$，$b_{ii}=k_2\leq 0$，则下列等式成立，$A\otimes B=B\otimes A=k_2\otimes A\oplus k_1\otimes B$。

证明：证明：对于 $\forall i,j$，我们有：

$$\begin{aligned}(A\otimes B)_{ij}&=a_{ii}\otimes b_{ij}\oplus a_{ij}\otimes b_{jj}\oplus\sum_{p\notin\{i,j\}}a_{ip}\otimes b_{pj}\\&=k_1\otimes b_{ij}\oplus k_2\otimes a_{ij}\oplus\sum_{p\notin\{i,j\}}a_{ip}\otimes b_{pj}\end{aligned} \tag{5}$$

若我们假定 $k_1\otimes b_{ij}\oplus k_2\otimes a_{ij}\leq a_{ip}\otimes b_{pj}$，实际上用普通的代数表示为：

$$\min(k_1+b_{ij},k_2+a_{ij})\leq\min(a_{ij},b_{ij})\leq c+d\leq a_{ip}+b_{pj} \tag{6}$$

根据 c,d 之间的关系，可以得到下列不等式：

$$\min(c,d)\leq\frac{c+d}{2} \tag{7}$$

综合上述式子可以得到：

$$\begin{aligned}&(A\otimes B)_{ij}=k_1\otimes b_{ij}\oplus a_{ij}\otimes k_2\oplus\sum_{p\notin\{i,j\}}a_{ip}\otimes b_{pj}\\&=k_1\otimes b_{ij}\oplus a_{ij}\otimes k_2=(k_2\otimes A\oplus k_1\otimes B)_{ij}=(B\otimes A)_{ij}\end{aligned} \tag{8}$$

因此，证明了任意两个热带 LP 矩阵满足交换律。

例 2：设在 $M_1\in[10,20]_3^{-9}$，$M_2\in[15,30]_3^{-6}$ 中分别有热带 LP 矩阵 M_1 和 M_2，其中：

$$\begin{aligned}&M_1=\begin{pmatrix}-9&16&11\\19&-9&20\\15&10&-9\end{pmatrix},\quad M_2=\begin{pmatrix}-6&17&22\\24&-6&21\\27&30&-6\end{pmatrix},\\&M_1\otimes M_2=\begin{pmatrix}-15&8&5\\13&-15&12\\9&4&-15\end{pmatrix},\quad M_2\otimes M_1=\begin{pmatrix}-15&8&5\\13&-15&12\\9&4&-15\end{pmatrix}\end{aligned} \tag{9}$$

因此 $M_1\otimes M_2$=$M_2\otimes M_1$，即热带 LP 矩阵交换律成立。

3 基于热带 LP 矩阵的公钥密码

3.1 基于热带 LP 矩阵的密钥交换协议

本节中符号 T_1 表示所有整数热带 LP 矩阵的集合，符号 T_2 表示 $\mathbf{Z}_{\min}^{n\times n}$ 上的一般矩阵集合。下面给出热带 LP 矩阵作用问题。

定义 5　设 $M_1\in T_1$，$N_1\in T_1$，$X\in T_2$，$U=M_1\otimes X\otimes N_1$。热带 LP 矩阵作用问题是在已知 U 和 X 的情况下，求两个保密的热带 LP 矩阵 $M_1\in T_1$，$N_1\in T_1$ 使得 $U=M_1\otimes X\otimes N_1$。

协议 1

令k_1,k_2,k_3,k_4是保密的非正整数，r,s,c,d是保密的非负整数，n是一个公开的正整数，同时公开一个$Z_{\min}^{n\times n}$上n阶一般矩阵X。

（1）Alice 随机选择两个保密的热带矩阵$M_1\in[c,2c]_n^{k_1}$，$N_1\in[r,2r]_n^{k_2}$，计算$U=M_1\otimes X\otimes N_1$，然后将 U 发送给 Bob。

（2）Bob 随机选择两个保密的热带矩阵，$M_2\in[d,2d]_n^{k_3}$，$N_2\in[s,2s]_n^{k_4}$，计算$V=M_2\otimes X\otimes N_2$，然后将 V 发送给 Alice。

（3）Alice 根据 Bob 发送的 V 计算：

$$K_a=M_1\otimes V\otimes N_1=M_1\otimes M_2\otimes X\otimes N_2\otimes N_1 \tag{10}$$

Bob 根据 Alice 发送的计算：

$$K_b=M_2\otimes U\otimes N_2=M_2\otimes M_1\otimes X\otimes N_1\otimes N_2 \tag{11}$$

因为热带 LP 矩阵$M_1,M2,N_1,N_2$满足交换律，$M_1\otimes M_2=M_2\otimes M_1$，$N_1\otimes N_2=N_2\otimes N_1$。最终 Alice 和 Bob 将会共享一个相同的密钥 K 。（文末附有小参数的例子。）

定义 6 设$M_1,M_2\in T_1$，$N_1,N_2\in T_1$ $X\in T_2$，假定$U=M_1\otimes X\otimes N_1$，$V=M_2\otimes X\otimes N_2$。计算热带 LP 矩阵作用问题是在已知 U,V和 X 的情况下，找到一个矩阵 K，使得$K=M_1\otimes M_2\otimes X\otimes N_2\otimes N_1$。

命题 1 如果存在有效算法可以解决热带 LP 矩阵作用问题，那么存在有效算法可以解决计算热带 LP 矩阵作用问题。

证明：如果存在一个热带 LP 矩阵作用问题的算法，那么利用这个算法可以求解保密的矩阵$M_1\in T_1$，$N_1\in T_1$。再利用该算法重新求出保密的矩阵$M_2\in T_1$，$N_2\in T_1$，将两次求出的保密矩阵 K 项代入的表达式中，即可求出所要的矩阵 K，从而解决计算热带 LP 矩阵作用问题。

3.2 基于热带 LP 矩阵的公钥加密方案

加密方案

密钥生成：

令 k_1,k_2,k_3,k_4 是保密的非正整数，r,s,c,d 是保密的非负整数，n 是一个公开的正整数。 $M_1\in[c,2c]_n^{k_1}$， $N_1\in[r,2r]_n^{k_2}$，X 是 上的一般矩阵，$U=M_1\otimes X\otimes N_1$。公开参数：矩阵的阶 n 和矩阵 X。Alice 的公钥是 U，Alice 的私钥是 M_1,N_1。

加密：

令 M_K 是 $n\times n$ 阶的非负整数矩阵的集合，且 M_K 代表的明文空间。假设 Bob 想把明文消息 $Y\in M_K$ 发送给 Alice。

（1）Bob 根据密钥生成中 d,s,k_3,k_4 的取值范围随机选取两个矩阵，分别是$M_2\in[d,2d]_n^{k_3}$，$N_2\in[s,2s]_n^{k_4}$。

（2）Bob 计算$V=M_2\otimes X\otimes N_2$，并将其作为密文中的一部分，然后再计算$W=Y+M_2\otimes U\otimes N_2$，注意，这里的加法是指普通的矩阵加法运算。

（3）Bob 最终的密文是(V,W)，并将密文发送给 Alice。

解密：

Alice 接收到密文后，使用私钥和对密文进行解密。

（1）Alice 首先计算 $K_v=M_1\otimes V\otimes N_1$。

（2）Alice 再计算 W-K_V，即可得到 Bob

原本的明文消息。注意，这里的减法是指普通的矩阵减法运算。

验证：

$$\begin{aligned}W-K_v&=Y+M_2\otimes U\otimes N_2-M_1\otimes V\otimes N_1\\&=Y+M_2\otimes M_1\otimes X\otimes N_1\otimes N_2-M_1\otimes M_2\otimes X\otimes N_2\otimes N_1\\&=Y+M_1\otimes M_2\otimes X\otimes N_1\otimes N_2-M_1\otimes M_2\otimes X\otimes N_1\otimes N_2\\&=Y\end{aligned} \tag{12}$$

定义 7 设$M_1,M_2,N_1,N_2\in T_1$，$X\in T_2$，$U=M_1\otimes X\otimes N_1$，$V=M_2\otimes X\otimes N_2$。判断热带 LP 矩阵作用问题就是给定一个已知的矩阵 E ，在已知 U,V,X 的情况下，判断 $E=M_1\otimes M_2\otimes X\otimes N_2\otimes N_1$ 是否成立。

命题 2 如果有效的解决判断热带 LP 矩阵作用问题的算法，那么存在有效算法可以判断出加密方案 1 密文的有效性，反之，若存在一有效判断密文有效性的算法，那么存在有效算法可解决判断热带 LP 矩阵作用问题。

证明：若存在有效算法σ_1可以解决判断热带LP矩阵作用问题，也就是说，对于给定已知的 U,V,X,E，可以判断出下列这个等式是否成立：

$$E=M_1\otimes M_2\otimes X\otimes N_2\otimes N_1 \tag{13}$$

若要验证密文是否有效，我们要对加密方案中的（V, W）密文进行验证，即：

$Y=W-M_2\otimes U\otimes N_2$，由定理 1 可知，热带LP矩阵满足交换律。因此：

$$M_2\otimes U\otimes N_2=M_2\otimes M_1\otimes X\otimes N_1\otimes N_2=M_1\otimes M_2\otimes X\otimes N_2\otimes N_1=E \tag{14}$$

故：$Y=W-M_2\otimes U\otimes N_2$=$W-E$，从而证明了判断热带 LP 矩阵作用问题的算法可以判断出密文的有效性。

若存在一种算法σ_2可以判断密文是否有效，给定X,U,V,W,Y，且下列等式成立：

$$W-Y=M_2\otimes U\otimes N_2 \tag{15}$$

同样是根据定理 1，可得：

$$M_2\otimes U\otimes N_2=M_2\otimes M_1\otimes X\otimes N_1\otimes N_2=M_1\otimes M_2\otimes X\otimes N_2\otimes N_1=E \tag{16}$$

故：W-Y=E，从而证明了判断密文有效性的算法可以判断热带 LP 矩阵作用问题。

综上所述，命题 2 成立。

4 安全性和效率分析

上一节所设计的密钥交换协议和公钥加密方案的安全性是基于计算热带 LP 矩阵作用问题来设计的。而此问题可以归约为求解热带非线性方程组的问题。2014 年 Grigoriev 和 Shpilrain 已经证明了热带半环的多项式方程是 NP 困难的。

攻击本文所设计的密码系统可归约为求解热带半环的非线性多项式方程。

例 3：设 $M_1=\begin{pmatrix}k_3&m_{12}&m_{13}\\m_{21}&k_3&m_{23}\\m_{31}&m_{32}&k_3\end{pmatrix}$，$N_1=\begin{pmatrix}k_1&n_{12}&n_{13}\\n_{21}&k_1&n_{23}\\n_{31}&n_{32}&k_1\end{pmatrix}$，

$$X=\begin{pmatrix}-53&65&75\\-16&-23&0\\19&33&-4\end{pmatrix}\quad U=\begin{pmatrix}-84&-41&-36\\-65&-54&-31\\-56&-34&-35\end{pmatrix} \tag{17}$$

要破解协议 1 需要求出保密的热带 LP 矩阵 M_1 和 N_1，求解 M_1 和 N_1 也可以转化为求解热带非线性方程组。根据已知条件可以列出下列方程，如下：

$$\begin{pmatrix}k_3&m_{12}&m_{13}\\m_{21}&k_3&m_{23}\\m_{31}&m_{32}&k_3\end{pmatrix}\otimes\begin{pmatrix}-53&65&75\\-16&-23&0\\19&33&-4\end{pmatrix}\otimes\begin{pmatrix}k_1&n_{12}&n_{13}\\n_{21}&k_1&n_{23}\\n_{31}&n_{32}&k_1\end{pmatrix}=\begin{pmatrix}-84&-41&-36\\-65&-54&-31\\-56&-34&-35\end{pmatrix} \tag{18}$$

首先化简前面一部分可得：

$$\begin{pmatrix} k_3\otimes(-53)\oplus m_{12}\otimes(-16)\oplus m_{13}\otimes 19 & k_3\otimes 65\oplus m_{12}\otimes(-23)\oplus m_{13}\otimes 33 & k_3\otimes 75\oplus m_{12}\otimes 0\oplus m_{13}\otimes(-4)\\ m_{21}\otimes(-53)\oplus k_3\otimes(-16)\oplus m_{23}\otimes 19 & m_{21}\otimes 65\oplus k_3\otimes(-23)\oplus m_{23}\otimes 33 & m_{21}\otimes 75\oplus k_3\otimes 0\oplus m_{23}\otimes(-4)\\ m_{31}\otimes(-53)\oplus m_{32}\otimes(-16)\oplus k_3\otimes 19 & m_{31}\otimes 65\oplus m_{32}\otimes(-23)\oplus k_3\otimes 33 & m_{31}\otimes 75\oplus m_{32}\otimes 0\oplus k_3\otimes(-4) \end{pmatrix} \tag{19}$$

再将上述式子和后面的矩阵作用化简后的结果就是给出的值，即得到如下一般的热带非线性方程组：

$$\begin{cases} k_1\otimes k_3\otimes(-53)\oplus k_1\otimes m_{12}\otimes(-16)\oplus k_1\otimes m_{13}\otimes 19\oplus n_{21}\otimes k_3\otimes 65\oplus n_{21}\otimes m_{12}\otimes(-23)\oplus n_{21}\otimes m_{13}\otimes 33\\ \oplus n_{31}\otimes k_3\otimes 75\oplus n_{31}\otimes m_{12}\otimes 0\oplus n_{31}\otimes m_{13}\otimes(-4)=-84\\ n_{12}\otimes k_3\otimes(-53)\oplus n_{12}\otimes m_{12}\otimes(-16)\oplus n_{12}\otimes m_{13}\otimes 19\oplus k_1\otimes k_3\otimes 65\oplus k_1\otimes m_{12}\otimes(-23)\oplus k_1\otimes m_{13}\otimes 33\\ \oplus n_{32}\otimes k_3\otimes 75\oplus n_{32}\otimes m_{12}\otimes 0\oplus n_{32}\otimes m_{13}\otimes(-4)=-41\\ n_{13}\otimes k_3\otimes(-53)\oplus n_{13}\otimes m_{12}\otimes(-16)\oplus n_{13}\otimes m_{13}\otimes 19\oplus n_{23}\otimes k_3\otimes 65\oplus n_{23}\otimes m_{12}\otimes(-23)\oplus n_{23}\otimes m_{13}\otimes 33\\ \oplus k_1\otimes k_3\otimes 75\oplus k_1\otimes m_{12}\otimes 0\oplus k_1\otimes m_{13}\otimes(-4)=-36\\ k_1\otimes m_{21}\otimes(-53)\oplus k_1\otimes k_3\otimes(-16)\oplus k_1\otimes m_{23}\otimes 19\oplus n_{21}\otimes m_{21}\otimes 65\oplus n_{21}\otimes k_3\otimes(-23)\oplus n_{21}\otimes m_{23}\otimes 33\\ \oplus n_{31}\otimes m_{21}\otimes 75\oplus n_{31}\otimes k_3\otimes 0\oplus n_{31}\otimes m_{23}\otimes(-4)=-65\\ n_{12}\otimes m_{21}\otimes(-53)\oplus n_{12}\otimes k_3\otimes(-16)\oplus n_{12}\otimes m_{23}\otimes 19\oplus k_1\otimes m_{21}\otimes 65\oplus k_1\otimes k_3\otimes(-23)\oplus k_1\otimes m_{23}\otimes 33\\ \oplus n_{32}\otimes m_{21}\otimes 75\oplus n_{32}\otimes k_3\otimes 0\oplus n_{32}\otimes m_{23}\otimes(-4)=-54\\ n_{13}\otimes m_{21}\otimes(-53)\oplus n_{13}\otimes k_3\otimes(-16)\oplus n_{13}\otimes m_{23}\otimes 19\oplus n_{23}\otimes m_{21}\otimes 65\oplus n_{23}\otimes k_3\otimes(-23)\oplus n_{23}\otimes m_{23}\otimes 33\\ \oplus k_1\otimes m_{21}\otimes 75\oplus k_1\otimes k_3\otimes 0\oplus k_1\otimes m_{23}\otimes(-4)=-31\\ k_1\otimes m_{31}\otimes(-53)\oplus k_1\otimes m_{32}\otimes(-16)\oplus k_1\otimes k_3\otimes 19\oplus n_{21}\otimes m_{31}\otimes 65\oplus n_{21}\otimes m_{32}\otimes(-23)\oplus n_{21}\otimes k_3\otimes 33\\ \oplus n_{31}\otimes m_{31}\otimes 75\oplus n_{31}\otimes m_{32}\otimes 0\oplus n_{31}\otimes k_3\otimes(-4)=-56\\ n_{12}\otimes m_{31}\otimes(-53)\oplus n_{12}\otimes m_{32}\otimes(-16)\oplus n_{12}\otimes k_3\otimes 19\oplus k_1\otimes m_{31}\otimes 65\oplus k_1\otimes m_{32}\otimes(-2\ 3)\oplus k_1\otimes k_3\otimes 33\\ \oplus n_{32}\otimes m_{31}\otimes 75\oplus n_{32}\otimes m_{32}\otimes 0\oplus n_{32}\otimes k_3\otimes(-4)=-34\\ n_{13}\otimes m_{31}\otimes(-53)\oplus n_{13}\otimes m_{32}\otimes(-16)\oplus n_{13}\otimes k_3\otimes 19\oplus n_{23}\otimes m_{31}\otimes 65\oplus n_{23}\otimes m_{32}\otimes(-23)\oplus n_{23}\otimes k_3\otimes 33\\ \oplus k_1\otimes m_{31}\otimes 75\oplus k_1\otimes m_{32}\otimes 0\oplus k_1\otimes k_3\otimes(-4)=-35 \end{cases} \tag{20}$$

可见采用 3 阶的热带 LP 矩阵，求矩阵 M_1 和 N_1 需求解 14 个未知数和 9 个热带非线性方程构成的方程组。而解这类热带非线性方程组是 NP 困难问题。

4.1 可能遭受的攻击

针对 Grigoriev 和 Shpilrain 提出的密钥交换协议，Kotov 和 Ushakov 在 2018 年提出了一种启发式的攻击方案。他们是对 U,V 是可以用下列方程找到 X 和 Y。即：

$$\begin{cases} X\otimes A=A\otimes X\\ Y\otimes B=B\otimes Y\\ X\otimes Y=U \end{cases} \tag{21}$$

我们可以把和设成如下的形式：

$$\begin{aligned} &X=\bigoplus_{i=0}^{D}x_i\otimes A^{\otimes i},\qquad Y=\bigoplus_{j=0}^{D}y_j\otimes B^{\otimes j}\\ &X\otimes Y=\bigoplus_{i,j=0}^{D}x_i\otimes y_j\otimes A^{\otimes i}\otimes B^{\otimes j} \end{aligned} \tag{22}$$

破解 Grigoriev 和 Shpilrain 的密码机制我们需要找 $x_0,\cdots,x_D,y_0,\cdots,y_D$，使得 s：

$$\bigoplus_{i,j=0}^{D}x_i\otimes y_j\otimes V^{ij}=U,\text{其中}\ V^{ij}=A^{\otimes i}\otimes B^{\otimes j} \tag{23}$$

而本文所设计的密钥交换协议和公钥加密方案是可以抵抗这种 KU 攻击。这是因为在密钥交换过程中，我们的使用的热带 LP 矩阵是保密不公开的。因此，敌手采用 KU 攻击破解这个协议时，不能通过设未知数的方式来表达所求的，从而破解出保密的热带 LP 矩阵。所以该方案可以成功抵御 KU 攻击。

同样地，本文设计的密钥交换协议和公钥加密方案也可以抵抗 RM 攻击。RM 攻击是 Rudy 和 Monico 针对 Grigoriev 和 Shpilrain 所设计的。Grigoriev 和 Shpilrain 基于半直积的作用设计了另一个密钥交换协议，但是在这个密钥交换过程中使用了热带矩阵的加法运算，而热带矩阵的加法具有幂等的性质，因此对于这一部分半直积的幂具有部分保序性，Rudy 和 Monico 利用这一性质设计出一种二分法搜索方案，逐渐找到这个保密的幂参数，从而破解该密钥交换协议。而本文所设计的密钥交换协议方案中，没有仅使用热带矩阵的加法运算，因此使用 RM 攻击对本文的密码系统无效。下面将列出表格进行比较，如表 1 和表 2 所示：

表 1 热带矩阵的密钥交换协议的攻击比较

Table 1 A comparison of attacks on key exchange protocols for tropical matrices

方案	数学问题	KU 攻击	RM 攻击
Grigoriev[4]	双边矩阵作用问题	×	√
Grigoriev[5]	半直积作用问题	√	×
我们的方案	热带 LP 矩阵作用问题	√	√

注意：√ 表示该方案可以抵抗对应的攻击，×则表示该方案不可以抵抗对应的攻击。

表 2 不同参数下本文方案的效率比较

Table 2 Comparison of the efficiency of this paper's solutions under different parameters

矩阵阶数	对角线上元素的取值范围	非对角线上元素的取值范围	解热带 LP 矩阵问题的穷举复杂度
30	[-50,0)	[50,100)	O(2^980)
40	[-50,0)	[50,100)	O(2^1070)
50	[-50,0)	[50,100)	O(2^1130)
30	[-100,0)	[100,200)	O(2^1953)
40	[-100,0)	[100,200)	O(2^2133)
50	[-100,0)	[100,200)	O(2^2253)

注：利用本文的极小加代数半环，将两个不同的 n 阶热带 LP 矩阵进行热带代数的乘法运算时需要对矩阵进行比较最小

值以及一般的整数加法运算，因此其比特复杂度为$O(n^3 \lg m)$。

求解热带 LP 矩阵作用问题的复杂度可以采用穷举的方法。对于一个 n 阶的热带 LP 矩阵，总共有 n^2 个元素，除了对角线上的元素是相等以外，其余位置都是不相同的，不相同的元素一共有 n^2-n 个。这些不同的元素将会在给定的热带 LP 矩阵设置的取值范围内随机选取，同样的，对角线上的元素只有一个值，也将会在给定的热带 LP 矩阵设置的取值范围内随机选取。综合这两种情形，就可以穷举出一个热带 LP 矩阵中的所有情形。因为热带 LP 矩阵作用问题有两个不同的热带 LP 矩阵，最后将这两种矩阵的情形相乘即可得到求解热带 LP 矩阵问题的穷举复杂度，如表 3 所示。

表 3 对比本方案在不同参数下公钥与私钥的最大上界

Table 3 Compare the maximum upper bound of the public and private keys of this scheme under different parameters

矩阵阶数	对角线上元素的取值范围	非对角线上元素的取值范围	公钥大小	私钥大小
30	[-50,0)	[50,100)	2.64kb	3.57kb
40	[-50,0)	[50,100)	4.69kb	6.33kb
50	[-50,0)	[50,100)	7.32kb	9.86kb
30	[-100,0)	[100,200)	3.52kb	5.33kb
40	[-100,0)	[100,200)	6.25kb	9.45kb
50	[-100,0)	[100,200)	9.77kb	14.75kb

公钥与私钥的最大上界的值是根据矩阵的阶数决定的。一个 阶矩阵里的每一个元素都在取值范围内随机选取一个值，将每个元素随机选取值的比特大小累加，就可得到对应的公钥与私钥的最大上界。

5 结语

本文利用极小加热带半环的 Linde-de-la Puente 型矩阵设计了基于热带 LP 矩阵作用问题的密钥交换协议和公钥加密方案。热带 LP 矩阵具有和 Linde-de-la Puente 矩阵一样的交换性的性质，因此双方在进行密钥交换协议过程中，可以得到相同的密钥，从而达到明文消息在公开信道上可以进行加密通讯的目的。最后还对一些可能对本方案造成的攻击进行了分析，并说明其不可行性。

还有待研究的问题包括：(1)研究求解热带半环的非线性方程组的算法，虽然一般该问题是 NP 困难的，但在某些特殊情形下，有可能存在有效的算法。(2)利用其他热带交换矩阵设计类似的公钥密码系统。

参考文献：

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

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

[3] Gerard M, Chris M, Joachim R. A public key cryptosystem based on actions by semigroups[C]//IEEE International Symposium on Information Theory-Proceedings. 2002:266-289.

[4] Maze, G.; Monico. C.; Rosenthal. J.Public Key Cryptography based on semigroup Actions[J]. Adv. Math. Commun. 2007, 1(4),489-507.

[5] Stickel. A new method for exchanging secret keys[C]. In Third International Conference on Information Technology and Applications (ICITA'05), volume 2, pages 426-430. IEEE, 2005.

[6] Vandiver H S . Note on a simple type of algebra in which the cancellation law of addition does not hold[J]. Plant Physiology, 1934, 125(4):1854-1869.

[7] Simon I.Recognizable sets with multiplicities in the tropical semiring[C]//International Symposium on Mathematical Foundations of Computer Science. Springer, Berlin, Heidelberg, 1988:107-120.

[8] Simon I. On semigroups of matrices over the tropical semiring [J]. RAIRO-Theoretical Informatics and Applications, 1994, 28(3-4): 277-294.

[9] Grigoriev D, Shpilrain V. Tropical cryptography [J]. Communications in Algebra, 2014, 42(6):2624-2632.

[10] Kotov M , Ushakov A . Analysis of a key exchange protocol based on tropical matrix algebra[J]. Journal of Mathematical Cryptology, 2018, 12(3):137-141.

[11] Grigoriev, D.; Shpilrain, V. Tropical cryptography II-Extensions by homomorphisms. [J].Communications in Algebra, 2019, 47(10), 4224-4229.

[12] Rudy, D.; Monico, C. Remarks on a Tropical Key Exchange System[J].Journal of Mathematical Cryptology, 2021, 15(1), 280-283.

[13] Isaac S, Kahrobaei D. A closer look at the tropical cryptography[J].International Journal of Computer Mathematics: Computer Systems Theory, 2021, 6(2):137-142.

[14] Huang H, Li C, Deng L.Public-Key Cryptography Based on Tropical Circular Matrices[J].Applied Sciences,2022,12(15):7401.

[15] Ahmed K, Pal S, Mohan R.Key exchange protocol based upon a modified tropical structure[J].Communications in Algebra, 2022:1-10.

[16] Linde J,De L.Matrices commuting with a given normal tropical matrix[J].Linear Algebra & Its Applications,2015, 482:101-121.

[17] Muanalifah A,Sergeev S . Modifying the tropical version of Stickel's key exchange protocol[J].Applications of Mathematics, 2020, 65(6):727-753.

(上接第 23 页)

[9] Dunker K F, Rabbat B G. Why America's bridges are crumbling[J]. Scientific American, 1993, 268(3): 66-72.

[10] Love P E D, Li H. Quantifying the causes and costs of rework in construction[J]. Construction management & economics, 2000, 18(4): 479-490.

[11] Mills A, Love P E, Williams P. Defect costs in residential construction [J]. Journal of Construction Engineering and Management, 2009, 135(1):12-16.

[12] Criminisi A. Accurate visual metrology from single and multiple uncalibrated images[M]. Springer Science & Business Media, 2001.

[13] 张剑清,王强.基于近景单影像的房檐改正计算方法[J].武汉大学学报(信息科学版),2007(12):1091-1094.

[14] Rother C. A new approach to vanishing point detection in architectural environments[J].Image and Vision Computing, 2002, 20(9-10): 647-655.

[15] Lei G. Recognition of planar objects in 3-D space from single perspective views using cross ratio[J].IEEE Transactions on Robotics and Automation, 1990, 6(4):432-437.