HKKS 密钥交换协议分析

刘金会 张焕国 贾建卫 王后珍 毛少武 吴万青

(武汉大学计算机学院 武汉 430072)

(空天信息安全与可信计算教育部重点实验室 武汉 430072)

摘 要 量子计算技术的发展对基于大整数因子分解、离散对数等问题具有交换代数结构的密码体制(如 RSA、ECC 和 EIGamal 密码)构成威胁,因此研究具有非交换代数结构的密码体制是一项富有挑战性的课题.针对该课题,Kahrobaei 等人于 2013 年将一般矩阵群环作为平台提出了 HKKS 密钥交换协议并且于 2014 年将有限域上的矩阵群作为平台介绍该 HKKS 密钥交换协议.该文针对基于有限域上矩阵群的 HKKS 密钥交换协议,提出了 4 种攻击方法:结构攻击、线性化方程组攻击、超定多变量方程组攻击和离散对数方法攻击,并且分别给出了对应的算法描述和有效性分析.通过分析可知:(1)结构攻击算法是确定性算法,能够在 $O(n^{2\omega})$ 计算复杂度内获得共享密钥,其中 n 是矩阵 $\boldsymbol{H}$ 的阶数,$\omega \approx 2.3755$;(2)线性化方程组攻击和超定多变量方程组攻击都利用 Halmiton-Caylay 定理将 HKKS 协议中私钥矩阵对 $(\boldsymbol{H}^a,(\boldsymbol{HM})^a)$ 和 $(\boldsymbol{H}^{-a},(\boldsymbol{HM})^a)$ 进行线性表示,采用线性方程组求解和 XL 算法求出一个相应的等价私钥矩阵进而计算共享密钥,这两种攻击方法的计算复杂度分别是 $O(n^{\omega+1})$ 和 $O(n^{2\omega})$;(3)当矩阵 $\boldsymbol{H}$(或者是矩阵 $\boldsymbol{HM}$)的特征多项式可约时,离散对数方法利用伴侣矩阵的性质分析 P-HKKS 问题进而求出该协议的私钥 a(或者 b),分析该方法的计算复杂度是 $O(n^4)$.与此同时,该文分别将结构攻击、线性化方程组攻击、超定多变量方程组攻击应用到一般矩阵群环上的 HKKS 协议,这 3 种攻击方法也分别能够在多项式计算复杂度内得到共享密钥.与 ACNS 2014 会议上提出的线性代数攻击方法相比,结构攻击方法是确定性算法并且线性化方程组攻击的计算复杂度最低.最后,该文在给出攻击算法的基础上对 HKKS 协议给出了一些修正建议.

关键词 密码学;抗量子计算密码;密钥交换协议;密码分析;矩阵分解

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2016.00516

Cryptanalysis of HKKS Key Exchange Protocols

LIU Jin-Hui ZHANG Huan-Guo JIA Jian-Wei WANG Hou-Zhen MAO Shao-Wu WU Wan-Qing

(*School of Computer, Wuhan University, Wuhan* 430072)

(*Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, Wuhan* 430072)

Abstract Advances in quantum computing technology threaten to break public key cryptosystems based oncommutative algebraic structures such as RSA, ECC, and EIGamal on the hardness of factoring or taking a discrete logarithm, while no quantum algorithms are found to solve certain mathematical problems on non-commutative algebraic structures until now. How to study a public key cryptosystem based on non-commutative algebraic structures is one of the most challenging issues. Kahrobaei et al. put forward a novel Habeeb-Kahrobaei-Koupparis-Shpilrain (HKKS) key exchange protocol based on an extension of a semigroup by automorphisms (more generally endomorphisms). They proposed a non-commutative semigroup of matrices over a Galois field as platform and matrices over group rings as platform respectively. Aiming at the

收稿日期:2014-11-18;最终修改稿收到日期:2015-05-26.本课题得到国家自然科学基金(61303212,61170080,61202386,61332019,U1135004,91018008)、国家"九七三"重点基础研究发展规划项目基金(2014CB340600)和湖北省自然科学基金(2011CDB453,2014CFB440)资助.**刘金会**,女,1989 年生,博士研究生,主要研究方向为密码学、信息安全.E-mail:jh.liu@whu.edu.cn.**张焕国**,男,1945 年生,教授,博士生导师,中国计算机学会(CCF)会员,主要研究领域为密码学、信息安全等.**贾建卫**,男,1988 年生,博士研究生,主要研究方向为密码学、信息安全.**王后珍**,男,1981 年生,讲师,主要研究方向为密码学、信息安全.**毛少武**,男,1986 年生,博士研究生,主要研究方向为密码学、信息安全.**吴万青**,男,1981 年生,博士研究生,主要研究方向为密码学、信息安全.

HKKS key agreement protocol over the platform——an extension of a semigroup of matrices over a Galois field, we show that the particular instance of the protocol suggested in their paper can be broken via four different attack methods such as a structural attack, a linearization equations attack, an overdefined systems of multivariate polynomial equations attack and a discrete logarithm method attack and that, they require polynomial time complexity to achieve the shared secret key from associated public-key respectively. In this paper, we conduct a detailed analysis on the attack methods and showed corresponding algorithmic description and efficiency analysis. Theoretic analysis shows the following conclusions: (1) the structural attack gives a polynomial time deterministic algorithm with complexity of $O(n^{2\omega})$ that recovers the secret shared key from the public key, where $\boldsymbol{H}$ is a $n\times n$ matrix over a Galois field and $\omega\approx 2.3755$. (2) Due to Halmiton-Caylay theorem, private key matrices $\boldsymbol{H}^{-a},\boldsymbol{H}^{a}$ can be represented as a linear combination of the set $\{\boldsymbol{I},\boldsymbol{H},\boldsymbol{H}^2,\cdots,\boldsymbol{H}^{n-1}\}$ and $\boldsymbol{G}^{a}$ can be represented as a linear combination of the set $\{\boldsymbol{I},\boldsymbol{G},\boldsymbol{G}^2,\cdots,\boldsymbol{G}^{n-1}\}$, where $\boldsymbol{G}=\boldsymbol{HM}$. Two pairs of equivalent private key matrices $(\boldsymbol{H}^{a},(\boldsymbol{HM})^{a})$ and $(\boldsymbol{H}^{-a},(\boldsymbol{HM})^{a})$ can be obtained by solving linear equations and XL Algorithm. Then we present two attack algorithms and they are both only require polynomial time complexity, that is to say, $O(n^{\omega+1})$ for the linearization equations attack and $O(n^{2\omega})$ for the overdefined systems of multivariate polynomial equations attack, to achieve the shared secret key. (3) When the characteristic polynomial of the matrix $\boldsymbol{H}$ (or the matrix $\boldsymbol{HM}$) is reducible, then the P-HKKS problem can be further reduced to a small set of discrete logarithm problems in an extension of the base field by using companion matrices of primitive polynomials. The private key a(or b) of HKKS key agreement protocol can be computed by an discrete logarithm attack method with the computational complexity of $O(n^4)$. At the same time, we also present that the HKKS protocol over matrix group rings is vulnerable to a structural attack, a linearization equations attack and an over defined systems of multivariate polynomial equations attack and that, they also only require polynomial time complexity respectively. Compared with a linear algebra attack proposed at ACNS 2014, the structural attack has the same computational complexity while the structural attack gives a polynomial time deterministic algorithm and computational complexity of the linearization equations attack is the smallest. In addition, we provide some improved suggestions on the HKKS protocol.

Keywords　cryptography; post-quantum computational cryptography; key exchange protocol; cryptanalysis; matrix decomposition

1　引　言

量子计算机的研制取得的进展以及一系列量子算法的相继出现，对基于计算复杂性理论的现代密码系统提出了新的挑战. 特别是，对基于交换代数结构的密码体制构成威胁，因为在量子计算环境下基于交换代数结构的许多困难问题(如大整数因子分解，离散对数问题)存在有效的量子算法. 然而基于非交换代数结构上的困难问题目前还没有有效的量子算法. 密码界普遍认为，非交换代数结构上的公钥密码具有抵抗量子算法攻击的潜力. 国际上掀起了抗量子计算公钥密码体制研究的热潮[1-6]. 近年来，越来越多的学者们关注于非交换密码的研究[7-11].

Kahrobaei 等人[12]对 Galois 域上的矩阵及其自同构扩展提出了 HKKS(Habeeb-Kahrobaei-Koupparis-Shpilrain)密钥交换协议. 该协议是在 Habeeb 和 Kahrobaei 等人[13]的非交换矩阵群环上的 HKKS 密钥交换协议基础之上提出的. Kreuzer 等人[14]采用一个线性代数方法分析了 2013 年提出的群环上的 HKKS 协议. 本文针对 Kahrobaei 等人提出的有限域上和群环上的 HKKS 协议，分别通过几种攻击方法说明其是不安全的. 需要特别指出的是，虽然在两种平台下，HKKS 协议都不安全，但是其方案较为巧妙的设计思想，确实为非交换公钥密码体制的设计作出了贡献.

本文对 Kahrobaei 等人提出的有限域上的 HKKS 协议给出了 4 种攻击方法,并且分别提供了各攻击方法对应的算法和算法复杂度. 文中主要利用结构攻击、线性化方程组攻击、超定多变量方程组攻击和离散对数方法分析有限域上的 HKKS 协议. 同时我们将前 3 种攻击方法即结构攻击、线性化方程组攻击和超定多变量方程组攻击应用到矩阵群环 $F_7[A_5]$ 上,在这种平台下,这 3 种攻击方法也都分别是多项式复杂性的. 文中介绍的这几种攻击方法都是对矩阵进行分解的应用,详细叙述参考文献[8,11]. 也就是说我们的攻击方法主要采用线性方程组和非线性方程组类型矩阵分解和标准型类型的矩阵分解对 HKKS 密钥交换协议进行分析.

本文第 2 节介绍矩阵群、矩阵的唯一的有理标准型和 Jordan 标准型的一般定义和文中使用的预备知识;第 3 节描述攻击的 HKKS 密钥交换协议;第 4 节针对两个平台上的 HKKS 协议设计上的缺陷分别给出攻击方法和相应的算法复杂性分析;第 5 节进行总结分析并且给出修正建议.

2 预备知识

这里我们首先简要介绍一些基本数学表示形式和符号:

$M_n(F_q)$表示有限域 F_q上任意的 $n\times n$ 的矩阵;

$GL_n(F_q)=\{\boldsymbol{X}\in M_n(F_q)\mid \det(\boldsymbol{X})\neq 0\}$;

$M_n(F_q[A_5])$表示群环 $F_q[A_5]$上任意的 $n\times n$ 的矩阵,其中,A_5是置换群;

$GL_n(F_q[A_5])$表示$F_q[A_5]$上任意的 $n\times n$ 的可逆矩阵;

$\vec{\boldsymbol{X}}$ 表示将 $n\times n$ 的矩阵 $\boldsymbol{X}$ 按行拉直得到一个 n^2 维的行向量;

$\otimes$表示 Kronecker 积.

定义 1(Jordan 块). 设有限域 $K=F_q$,$\overline{K}$是 K 的代数闭域. 对应于特征值 α_i是 n_i阶 Jordan 块 J_i.

$$J_i=J(\alpha_i,n_i)=\begin{pmatrix}\alpha_1 & 1 & & \\ & \ddots & 1 & \\ & & \alpha_1 & 1\\ & & & \alpha_1\end{pmatrix}_{n_i\times n_i},$$

其中,一个矩阵 $\boldsymbol{A}\in M_n(F_q)$的 Jordan 标准型 $J_{\boldsymbol{A}}$相似于矩阵 $\boldsymbol{A}$,存在可逆矩阵 $\boldsymbol{Q}\in GL_n(\overline{\boldsymbol{K}})$,使得 $\boldsymbol{Q}^{-1}\boldsymbol{A}\boldsymbol{Q}=J_{\boldsymbol{A}}$. 形式如下:

$$J_{\boldsymbol{A}}=\begin{pmatrix}J_1 & & \\ & \ddots & \\ & & J_r\end{pmatrix},$$

$J_{\boldsymbol{A}}=J(\alpha_1,n_1)\oplus\cdots\oplus J(\alpha_r,n_r)$, $\alpha_i(i=1,\cdots,r)$是矩阵 $\boldsymbol{A}$ 在$\overline{K}$中的特征值,$\sum_{i=1}^{r}n_i=n$.

定义 2(伴侣矩阵). 设有限域 F_q上一个多项式 $p(\lambda)=\lambda^n+\sum_{i=0}^{n-1}a_i\lambda^i$是度数为 n 的首一多项式函数. 则有限域 F_q上 $n\times n$ 的矩阵

$$\boldsymbol{C}_n=\begin{pmatrix}0 & 0 & \cdots & 0 & -a_0\\ 1 & 0 & \cdots & 0 & -a_1\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & \cdots & 0 & -a_{n-1}\\ 0 & 0 & \cdots & 1 & -a_n\end{pmatrix}.$$

若 $\boldsymbol{C}_n$为 n 次首一多项式 $p(\lambda)$的伴侣矩阵,容易得到如下结论.

(1) $|\lambda\boldsymbol{I}_n-\boldsymbol{C}_n|=\lambda^n+\sum_{i=0}^{n-1}a_i\lambda^i$;

(2) 伴侣矩阵 $\boldsymbol{C}_n$的不变因子为$\underbrace{1,\cdots,1}_{n-1},p(\lambda)$.

定义 3(有理标准型). 设 $\boldsymbol{A}_{rat}\in M_n(F_q)$是块对角矩阵,可以表示为 $\boldsymbol{A}_{rat}=\mathrm{diag}(\boldsymbol{A}_1,\cdots,\boldsymbol{A}_s)$. 则称 $\boldsymbol{A}_{rat}$为有限域 F_q上的一个有理标准型矩阵. 其中,$\boldsymbol{A}_i$是有限域 F_q上不变因子 $p_i(\lambda)(i=1,2,\cdots,s)$对应的伴侣矩阵,并且 $p_{i-1}(\lambda)\mid p_i(\lambda)$.

定义 4. 群环 $F_q[A_5]$是如下线性组合的集合:

$$\forall a\in F_q[A_5],\ a=\sum_{i=1}^{60}a_i\sigma_i,$$

其中,$a_i,b_i\in F_q$,置换群 $A_5=\{\sigma_1,\sigma_2,\cdots,\sigma_{60}\}$.

群环 $F_q[A_5]$上的加法和乘法按照一般的定义如下:

$$\left(\sum_{i=1}^{60}a_i\sigma_i\right)+\left(\sum_{i=1}^{60}b_i\sigma_i\right)=\sum_{i=1}^{60}(a_i+b_i)\sigma_i,$$

$$\left(\sum_{i=1}^{60}a_i\sigma_i\right)\cdot\left(\sum_{i=1}^{60}b_i\sigma_i\right)=\sum_{i=1}^{60}\left(\sum_{\sigma_j\sigma_k=\sigma_i}a_jb_k\right)\sigma_i.$$

命题 1. Kronecker 积$\otimes$有下列性质:

$(\boldsymbol{A}\otimes\boldsymbol{B})\otimes\boldsymbol{C}=\boldsymbol{A}\otimes(\boldsymbol{B}\otimes\boldsymbol{C})$;

$\boldsymbol{A}\otimes(\boldsymbol{B}+\boldsymbol{C})=(\boldsymbol{A}\otimes\boldsymbol{B})+(\boldsymbol{A}\otimes\boldsymbol{C})$;

$(\boldsymbol{A}\otimes\boldsymbol{B})^{\mathrm{T}}=\boldsymbol{A}^{\mathrm{T}}\otimes\boldsymbol{B}^{\mathrm{T}}$;

$(\boldsymbol{A}\otimes\boldsymbol{B})(\boldsymbol{C}\otimes\boldsymbol{D})=(\boldsymbol{A}\boldsymbol{C})\otimes(\boldsymbol{B}\boldsymbol{D})$.

命题 2. 符号 $\vec{\cdot}$将一个矩阵拉直为一个长的行向量,有下列性质:

$\overrightarrow{\alpha\boldsymbol{A}+\beta\boldsymbol{B}}=\alpha\vec{\boldsymbol{A}}+\beta\vec{\boldsymbol{B}}$;

$\overrightarrow{\boldsymbol{A}\boldsymbol{X}^{\mathrm{T}}}=(\boldsymbol{A}\otimes\boldsymbol{I})\vec{\boldsymbol{X}}^{\mathrm{T}}$;

$\overrightarrow{\boldsymbol{X}\boldsymbol{B}^{\mathrm{T}}}=(\boldsymbol{I}\otimes\boldsymbol{B}^{\mathrm{T}})\vec{\boldsymbol{X}}^{\mathrm{T}}$;

$\overrightarrow{\boldsymbol{A}\boldsymbol{C}\boldsymbol{B}^{\mathrm{T}}}=(\boldsymbol{A}\otimes\boldsymbol{B}^{\mathrm{T}})\vec{\boldsymbol{C}}^{\mathrm{T}}$.

3　HKKS 密钥交换协议描述

下面我们将给出在矩阵群 $M_n(F_q)$ 上分析的 HKKS 密钥交换协议[12]. 同时，为方便分析，我们仅给出参数建议中矩阵群环 $M_3(F_7[A_5])$ 上的 HKKS 协议[13]. 有限域上的 HKKS 密钥交换协议描述如下：

设 $G=M_n(F_q)$ 是公开的非交换群，矩阵 $\boldsymbol{M}\in G$，$\boldsymbol{H}\in GL_n(F_q)\subseteq G$ 满足 $\boldsymbol{MH}\neq\boldsymbol{HM}$. 自同构映射 φ 满足：$\varphi_{\boldsymbol{H}}^{k}(\boldsymbol{M})=\boldsymbol{H}^{-k}\boldsymbol{MH}^{k}$.

公钥：$\boldsymbol{M},\boldsymbol{H}$.

私钥：Alice 私钥 $a\in Z_+$，Bob 私钥 $b\in Z_+$.

步骤 1. Alice 计算 $(\boldsymbol{M},\varphi_{\boldsymbol{H}})^a=(\boldsymbol{H}^{-a+1}\boldsymbol{MH}^{a-1}\cdots\boldsymbol{H}^{-2}\boldsymbol{MH}^{2}\boldsymbol{H}^{-1}\boldsymbol{MH}^{1}\boldsymbol{M},\varphi_{\boldsymbol{H}}^{a})=(\boldsymbol{A},\varphi_{\boldsymbol{H}}^{a})$，然后 Alice 将第一个分量 $\boldsymbol{A}=\boldsymbol{H}^{-a}(\boldsymbol{HM})^a$ 发送给 Bob.

步骤 2. Bob 计算 $(\boldsymbol{M},\varphi_{\boldsymbol{H}})^b=(\boldsymbol{H}^{-b+1}\boldsymbol{MH}^{b-1}\cdots\boldsymbol{H}^{-1}\boldsymbol{MH}^{1}\boldsymbol{M},\varphi_{\boldsymbol{H}}^{b})=(\boldsymbol{B},\varphi_{\boldsymbol{H}}^{b})$，然后 Bob 将第一个分量 $\boldsymbol{B}=\boldsymbol{H}^{-b}(\boldsymbol{HM})^b$ 发送给 Alice.

步骤 3. Alice 计算 $(\boldsymbol{B},\boldsymbol{x})(\boldsymbol{A},\varphi_{\boldsymbol{H}}^{a})=(\varphi_{\boldsymbol{H}}^{a}(\boldsymbol{B})\cdot\boldsymbol{A},\boldsymbol{x}\cdot\varphi_{\boldsymbol{H}}^{a})$，密钥 $K_{\text{Alice}}=\varphi_{\boldsymbol{H}}^{a}(\boldsymbol{B})\cdot\boldsymbol{A}$，代入计算可得

$$K_{\text{Alice}}=\boldsymbol{H}^{-(a+b)}(\boldsymbol{HM})^{(a+b)}.$$

步骤 4. Bob 计算 $(\boldsymbol{A},\boldsymbol{y})(\boldsymbol{B},\varphi_{\boldsymbol{H}}^{b})=(\varphi_{\boldsymbol{H}}^{b}(\boldsymbol{A})\cdot\boldsymbol{B},\boldsymbol{y}\cdot\varphi_{\boldsymbol{H}}^{n})$，密钥 $K_{\text{Bob}}=\varphi_{\boldsymbol{H}}^{b}(\boldsymbol{A})\cdot\boldsymbol{B}$，代入计算可得

$$K_{\text{Bob}}=\boldsymbol{H}^{-(a+b)}(\boldsymbol{HM})^{(a+b)}.$$

步骤 5. 共享密钥

$$K=K_{\text{Alice}}=K_{\text{Bob}}=\boldsymbol{H}^{-(a+b)}(\boldsymbol{HM})^{(a+b)}.$$

在矩阵群环 $M_3(F_7[A_5])$ 上的 HKKS 协议分别将 $M_3(F_7[A_5])$ 替换成有限域上矩阵群 $M_n(F_q)$，$GL_3(F_7[A_5])$ 替换 $GL_n(F_q)$.

为分析有限域上 HKKS 密钥交换协议，我们主要考虑下面一个问题，为分析方便，简记为 P-HKKS 问题. 矩阵群环上的 HKKS 密钥交换协议可类似定义.

P-HKKS 问题. 即给定矩阵 $\boldsymbol{M}\in M_n(F_q)$，$\boldsymbol{H}\in GL_n(F_q)$ 满足 $\boldsymbol{MH}\neq\boldsymbol{HM}$，求解私钥 $a\in Z_+$ 或者 $\boldsymbol{H}^a\in GL_n(F_q)$，使得 $\boldsymbol{A}=\boldsymbol{H}^{-a}(\boldsymbol{HM})^a$ 成立.

直接求解 $M_n(F_q)$ 上的 HKKS 问题，即利用穷搜索算法计算 $\boldsymbol{A}=\boldsymbol{H}^{-a}(\boldsymbol{HM})^a$，根据文献[12]建议的参数 $q=2^{127}$，$n=2$，求解 HKKS 问题的复杂度是 2^{254}. 然而文献[13]中 HKKS 协议的参数建议是在矩阵群环 $M_3(F_7[A_5])$ 上，并且他们认为在这个矩阵群环平台上，从已知公钥中计算共享密钥是困难的. 下面本文将同时说明在这两种平台下，HKKS 协议都是不安全的.

4　HKKS 密钥交换协议分析

假设 Alice 和 Bob 所有通信都在攻击者的控制下，并且攻击者只能通过对公开信道传递的消息进行窃听，不能影响协议的正常执行. 通过对窃听到的消息进行观察，分析获得必要的信息，进而攻破密码方案达到预先确定的攻击目的.

这部分我们分别根据结构攻击、线性化方程组攻击、超定多变量方程组攻击、离散对数方法，说明在有限域上 HKKS 协议是不安全的. 同时也分别利用结构攻击、线性化方程组攻击、超定多变量方程组攻击说明矩阵群环 $M_3(F_7[A_5])$ 上的 HKKS 协议是不安全的.

4.1　结构攻击

攻击者获得信息

$$(\boldsymbol{H},\boldsymbol{M},\boldsymbol{A}=\boldsymbol{H}^{-a}(\boldsymbol{HM})^a,\ \boldsymbol{B}=\boldsymbol{H}^{-b}(\boldsymbol{HM})^b),$$

根据共享密钥

$$K=\varphi_{\boldsymbol{H}}^{a}(\boldsymbol{B})\cdot\boldsymbol{A}=\varphi_{\boldsymbol{H}}^{b}(\boldsymbol{A})\cdot\boldsymbol{B}=\boldsymbol{H}^{-(a+b)}(\boldsymbol{HM})^{(a+b)},$$

则有下面 4 个等式成立：

$$\boldsymbol{H}^{-(a+b)}(\boldsymbol{HM})^{(a+b)}=\boldsymbol{H}^{-b}\boldsymbol{A}(\boldsymbol{HM})^{b};$$

$$\boldsymbol{H}^{-(a+b)}(\boldsymbol{HM})^{(a+b)}=\boldsymbol{H}^{-a}\boldsymbol{B}(\boldsymbol{HM})^{a};$$

$$\boldsymbol{H}^{-(a+b)}(\boldsymbol{HM})^{(a+b)}=\boldsymbol{H}^{-a}\boldsymbol{BH}^{a}\boldsymbol{A};$$

$$\boldsymbol{H}^{-(a+b)}(\boldsymbol{HM})^{(a+b)}=\boldsymbol{H}^{-b}\boldsymbol{AH}^{b}\boldsymbol{B}.$$

分析上述 4 个等式，我们知道，求出共享密钥 K，与求出矩阵对 $(\boldsymbol{H}^{-a},(\boldsymbol{HM})^a)$ 或者矩阵对 $(\boldsymbol{H}^{-b},(\boldsymbol{HM})^b)$ 或者直接求出矩阵 $\boldsymbol{H}^{-a}$ 和矩阵 $\boldsymbol{H}^{-b}$ 密切相关，即求解 P-HKKS 问题. 因此，根据上述关系式，我们可以得到具有如下等式的线性方程组：

$$\begin{cases}\boldsymbol{XH}=\boldsymbol{HX}\\ \boldsymbol{YG}=\boldsymbol{GY}\\ \boldsymbol{XA}=\boldsymbol{Y}\end{cases}\tag{1}$$

根据命题 2，把式(1)转化为线性方程组(2)如下所示：

$$\begin{cases}(\boldsymbol{H}\otimes\boldsymbol{I}-\boldsymbol{I}\otimes\boldsymbol{H}^{\mathrm{T}})\vec{\boldsymbol{X}}^{\mathrm{T}}=\boldsymbol{O}\\ (\boldsymbol{G}\otimes\boldsymbol{I}-\boldsymbol{I}\otimes\boldsymbol{G}^{\mathrm{T}})\vec{\boldsymbol{Y}}^{\mathrm{T}}=\boldsymbol{O}\\ (\boldsymbol{I}\otimes\boldsymbol{A}^{\mathrm{T}})\vec{\boldsymbol{X}}^{\mathrm{T}}-(\boldsymbol{I}\otimes\boldsymbol{I})\vec{\boldsymbol{Y}}^{\mathrm{T}}=\boldsymbol{O}\end{cases}\tag{2}$$

令矩阵

$$\boldsymbol{Q}=\begin{pmatrix}\boldsymbol{H}\otimes\boldsymbol{I}-\boldsymbol{I}\otimes\boldsymbol{H}^{\mathrm{T}} & \boldsymbol{O}\\ \boldsymbol{O} & \boldsymbol{G}\otimes\boldsymbol{I}-\boldsymbol{I}\otimes\boldsymbol{G}^{\mathrm{T}}\\ \boldsymbol{I}\otimes\boldsymbol{A}^{\mathrm{T}} & -(\boldsymbol{I}\otimes\boldsymbol{I})\end{pmatrix}.$$

线性方程组(2)是求解 $2n^2$ 个未知量 $3n^2$ 个方程的齐次线性方程组. 设矩阵 $\boldsymbol{Q}$ 的秩 $\mathrm{rank}(\boldsymbol{Q})=r$，则

$0<r\leq 2n^2$. 若矩阵 $\boldsymbol{Q}$ 的秩是 $2n^2$,则解矩阵对$(\boldsymbol{X},\boldsymbol{Y})$是零矩阵. 令$\boldsymbol{X}_1=\boldsymbol{H}^a$,$\boldsymbol{Y}_1=\boldsymbol{G}^a$,$\boldsymbol{G}=\boldsymbol{HM}$,从而$(\boldsymbol{X}_1,\boldsymbol{Y}_1)$是上述线性方程组(1)的一个解. 求解线性方程组(2)的过程为:首先通过求解线性方程组(2)得到解空间的一组基,然后对该基中的向量进行随机线性组合,得到一组解向量$(\vec{\boldsymbol{X}},\vec{\boldsymbol{Y}})$. 最后将被拉直的向量 $\vec{\boldsymbol{X}}$ 转化为矩阵 $\boldsymbol{X}$,其中,矩阵 $\boldsymbol{X}$ 是可逆矩阵.

下面我们说明任意的一组满足上述线性方程组(1)的解$(\boldsymbol{X},\boldsymbol{Y})$矩阵有相同的共享密钥 K,其中矩阵 $\boldsymbol{X}$ 是可逆的.

根据

$$\boldsymbol{XH}=\boldsymbol{HX},\ \boldsymbol{YG}=\boldsymbol{GY},$$

对于任意的 $j\in Z_+$,可以得到

$$\boldsymbol{XH}^j=\boldsymbol{H}^j\boldsymbol{X},\ \boldsymbol{YG}^j=\boldsymbol{G}^j\boldsymbol{Y}.$$

由于

$$\boldsymbol{A}=\boldsymbol{H}^{-a}\boldsymbol{G}^a=\boldsymbol{X}^{-1}\boldsymbol{Y},$$

得

$$\begin{aligned}\boldsymbol{X}^{-1}\boldsymbol{BY}&=\boldsymbol{X}^{-1}\boldsymbol{H}^{-b}\boldsymbol{G}^b\boldsymbol{Y}\\&=(\boldsymbol{H}^b\boldsymbol{X})^{-1}\boldsymbol{G}^b\boldsymbol{Y}\\&=(\boldsymbol{XH}^b)^{-1}\boldsymbol{YG}^b\\&=\boldsymbol{H}^{-b}\boldsymbol{X}^{-1}\boldsymbol{YG}^b\\&=\boldsymbol{H}^{-b}\boldsymbol{AG}^b\\&=K.\end{aligned}$$

因此,任意的一组满足上述线性方程组的解矩阵对$(\boldsymbol{X},\boldsymbol{Y})$,通过计算 $\boldsymbol{X}^{-1}\boldsymbol{BY}$,我们都得到相同的共享密钥 K.

下面用算法 1 描述结构攻击 HKKS 密钥交换协议.

算法 1. 求解共享密钥 K.

输入:$\boldsymbol{H},\boldsymbol{M},\boldsymbol{A},\boldsymbol{B}$

输出:共享密钥 K

1. 计算齐次线性方程组 $\boldsymbol{Q}(\vec{\boldsymbol{X}},\vec{\boldsymbol{Y}})^{\mathrm{T}}=\boldsymbol{O}$,得到解空间的一组基.

2. 对该基中的向量进行随机线性组合,得到一组解向量$(\vec{\boldsymbol{X}},\vec{\boldsymbol{Y}})$.

3. 将向量 $\vec{\boldsymbol{X}},\vec{\boldsymbol{Y}}$ 转化为矩阵 $\boldsymbol{X},\boldsymbol{Y}$,直到矩阵 $\boldsymbol{X}$ 是可逆的. 若不可逆,返回步 2.

4. 计算 $\boldsymbol{X}^{-1}\boldsymbol{BY}=K$.

5. 返回 K.

下面对算法 1 评估其计算复杂度. 在 $M_n(F_q)$ 上,求解 $n\times n$ 矩阵的逆和两个 $n\times n$ 的矩阵乘法的计算复杂性是$O(n^\omega)$($\omega\approx 2.3755$),F_q操作并且每个 F_q操作需要大约 $O(\log^2 q)$ bit 操作[15-16]. 算法 1 的计算复杂性分析如表 1.

算法 1 的计算复杂性只考虑多少次有限域上的乘法操作,有限域上乘法操作与有限域的大小有很大关系(尤其是有限域比较大时),将有限域上的乘法操作转化为一般的 bit 复杂性结果(有限域上的一次乘法操作相当于 $O(\log q)^2$ bit 操作),将更有说服力. 因为研究基于有限域矩阵群上的 HKKS 密钥交换协议有限域 $q=2^{127}$.

表 1 算法 1 的计算复杂性分析

内容	bit 复杂性	解释
$\boldsymbol{Q}(\vec{\boldsymbol{X}},\vec{\boldsymbol{Y}})^{\mathrm{T}}=\boldsymbol{O}$	$O(3n^{2\omega}\log^2 q)$	$2n^2$ 未知量 $3n^2$ 方程组
解$(\boldsymbol{X},\boldsymbol{Y})$	$O(3n^2(2n^2-r)^{\omega-1}\log^2 q)$	随机解
矩阵 $\boldsymbol{X}$ 可逆	$O(n^\omega\log^2 q)$	1 个逆运算
$\boldsymbol{X}^{-1}\boldsymbol{BY}=\mathrm{K}$	$O(3n^\omega\log^2 q)$	2 个乘法运算

通过表 1 可知,忽略小的固定参数,算法 1 攻击 HKKS 密钥交换协议的 bit 复杂度是 $O(n^{2\omega}\log^2 q)$.

采用上述攻击方法分析矩阵群环 $M_3(F_7(A_5))$ 上的 HKKS 协议,同样可以得到线性方程组(2). 其中

$$\boldsymbol{X}=\Big(\sum_{k=1}^{60}x_k^{(i,j)}\sigma_k\Big)_{1\leq i,j\leq 3},\ \boldsymbol{Y}=\Big(\sum_{k=1}^{60}y_k^{(i,j)}\sigma_k\Big)_{1\leq i,j\leq 3},$$

$$\boldsymbol{H}=\Big(\sum_{k=1}^{60}h_k^{(i,j)}\sigma_k\Big)_{1\leq i,j\leq 3},\ \boldsymbol{G}=\Big(\sum_{k=1}^{60}g_k^{(i,j)}\sigma_k\Big)_{1\leq i,j\leq 3},$$

$$\boldsymbol{A}=\Big(\sum_{k=1}^{60}a_k^{(i,j)}\sigma_k\Big)_{1\leq i,j\leq 3},$$

$$x_k^{(i,j)},y_k^{(i,j)},h_k^{(i,j)},g_k^{(i,j)},a_k^{(i,j)}\in F_7.$$

矩阵群环 $M_3(F_7(A_5))$ 上的线性方程组(2)可以转化为有限域 F_7 上一个具有 $1080=120n^2$($n=3$)个未知量、$1620=180n^2$ 个方程的齐次线性方程组. 因此,利用算法 1 方法同样可以求出解矩阵 $\boldsymbol{X},\boldsymbol{Y}$. 由于任意的矩阵 $\boldsymbol{X}\in M_3(F_7(A_5))$是可逆矩阵当且仅当 $\varphi(\boldsymbol{X})\in M_{180}(F_7)$是可逆矩阵[14,17],然而在有限域 F_7上随机选择一个 180×180 的矩阵 $\varphi(\boldsymbol{X})$是可逆矩阵的概率是

$$\frac{\prod_{i=0}^{n-1}(q^i-1)}{q^{\frac{n(n+1)}{2}}}=\frac{\prod_{i=0}^{179}(7^i-1)}{7^{16290}}\approx 1.$$

因此,计算共享密钥 $K=\boldsymbol{X}^{-1}\boldsymbol{BY}$.

结构攻击矩阵群环 $M_3(F_7(A_5))$ 上的 HKKS 协议的算法与文献[14]中线性代数攻击方法的思路一致,但是本文的算法是确定性的方法,因为线性方程组的解空间中至少有一个可逆矩阵并且接近 1 的概率的都是可逆矩阵,因此,从解空间中能够找到可逆解,也就是说,攻击成功的概率是 1,然而文献[14]的攻击方法是概率算法,攻击成功的概率是 6/7. 虽然文献[14]与本文攻击的 HKKS 协议在相同参数下,计算复杂性相等,但是文献[14]并没有给出计算

复杂性分析，然而本文中我们引用了新符号，使得攻击算法更加直观、更加容易分析理解，而且本文的攻击方法提供了进一步扩展分析的思路.

4.2 线性化方程组攻击

每一个矩阵 $\boldsymbol{C}\in M_n(F_q)$，存在最小多项式 $f_{\boldsymbol{C}\min}(x)$使得 $f_{\boldsymbol{C}\min}(\boldsymbol{C})=\boldsymbol{O}$. 矩阵 $\boldsymbol{C}$ 的特征多项式

$$f_{\boldsymbol{C}}(x)=|x\boldsymbol{I}-\boldsymbol{C}|=x^n+\cdots+a_1x+a_0,$$

其中，$a_i\in F_q(i=0,\cdots,n-1)$.

根据 Halmiton-Caylay 定理，易知 $f_{\boldsymbol{C}}(\boldsymbol{C})=\boldsymbol{O}$，并且有 $f_{\boldsymbol{C}\min}(x)$整除 $f_{\boldsymbol{C}}(x)$. 因此，对于任意的 $k\in Z$，$\boldsymbol{C}^k$能够由集合$\Delta=\{\boldsymbol{I},\boldsymbol{C},\boldsymbol{C}^2,\cdots,\boldsymbol{C}^{n-1}\}$线性表示.

因此，在 HKKS 密钥交换协议中，对于任意的 $a\in Z_+$，私钥 $\boldsymbol{H}^a$能够由集合$\{\boldsymbol{I},\boldsymbol{H},\boldsymbol{H}^2,\cdots,\boldsymbol{H}^{n-1}\}$线性表示. 令

$$\boldsymbol{X}=\boldsymbol{H}^a=\sum_{i=0}^{n-1}h_i\boldsymbol{H}^i,$$

其中，$h_i\in F_q(i=0,\cdots,n-1)$.

私钥 $\boldsymbol{G}^a$（$\boldsymbol{G}=\boldsymbol{HM}$）能够由集合$\{\boldsymbol{I},\boldsymbol{G},\boldsymbol{G}^2,\cdots,\boldsymbol{G}^{n-1}\}$线性表示. 令

$$\boldsymbol{Y}=\boldsymbol{G}^a=\sum_{j=0}^{n-1}g_j\boldsymbol{G}^j,$$

其中，$g_j\in F_q(j=0,\cdots,n-1)$.

根据 $\boldsymbol{A}=\boldsymbol{H}^{-a}(\boldsymbol{HM})^a$，可得

$$\sum_{i=0}^{n-1}h_i\boldsymbol{H}^i\boldsymbol{A}=\sum_{j=0}^{n-1}g_j\boldsymbol{G}^j \tag{3}$$

同时，$\sum_{i=0}^{n-1}h_i\boldsymbol{H}^i$是可逆矩阵.

令

$$\boldsymbol{v}=(h_0,\cdots,h_{n-1},g_0,\cdots,g_{n-1}),$$

$$\boldsymbol{P}=\begin{pmatrix}\vec{\boldsymbol{A}}\\ \vdots\\ \overrightarrow{\boldsymbol{H}^{n-1}\boldsymbol{A}}\\ -\vec{\boldsymbol{I}}\\ \vdots\\ -\boldsymbol{G}^{n-1}\end{pmatrix}.$$

线性方程(3)可转化为具有 $2n$ 个变量、n^2 个方程的齐次线性方程组

$$\boldsymbol{vP}=\boldsymbol{O} \tag{4}$$

设矩阵 $\boldsymbol{P}$ 的秩 $\mathrm{rank}(\boldsymbol{P})=r$，则 $0<r\leq 2n$. 若矩阵 $\boldsymbol{P}$ 的秩为 $2n$，则 $\boldsymbol{v}$ 是零向量. 由于 $\boldsymbol{v}$ 至少有一个非零解，即私钥对. 因此，计算齐次线性方程组(4)，可以得到至少一个解 $\boldsymbol{v}$，将 $\boldsymbol{v}$ 的一半分量代入式(3)，通过计算并且直到验证矩阵 $\boldsymbol{X}$ 可逆，得到一组解矩阵 $\boldsymbol{X},\boldsymbol{Y}$.

因为

$$\begin{aligned}\boldsymbol{X}^{-1}\boldsymbol{BY}&=\boldsymbol{X}^{-1}\boldsymbol{H}^{-b}\boldsymbol{G}^b\boldsymbol{Y}\\&=(\boldsymbol{H}^b\boldsymbol{X})^{-1}\boldsymbol{G}^b\boldsymbol{Y}\\&=\Big(\boldsymbol{H}^b\sum_{i=0}^{n-1}h_i\boldsymbol{H}^i\Big)^{-1}\boldsymbol{G}^b\Big(\sum_{j=0}^{n-1}g_j\boldsymbol{G}^j\Big)\\&=\Big(\Big(\sum_{i=0}^{n-1}h_i\boldsymbol{H}^i\Big)\boldsymbol{H}^b\Big)^{-1}\Big(\sum_{j=0}^{n-1}g_j\boldsymbol{G}^j\Big)\boldsymbol{G}^b\\&=(\boldsymbol{XH}^b)^{-1}\boldsymbol{YG}^b\\&=\boldsymbol{H}^{-b}\boldsymbol{X}^{-1}\boldsymbol{YG}^b\\&=\boldsymbol{H}^{-b}\boldsymbol{AG}^b\\&=K,\end{aligned}$$

因此，任意一组满足方程组(3)的矩阵对$(\boldsymbol{X},\boldsymbol{Y})$（并且 $\boldsymbol{X}$ 可逆），可以得到相同的共享密钥.

下面用算法 2 描述线性化方程组攻击 HKKS 密钥交换协议.

算法 2.　求解共享密钥 K.

输入：$\boldsymbol{H},\boldsymbol{M},\boldsymbol{A},\boldsymbol{B}$

输出：共享密钥 K

1. 计算 $2n$ 个变量 n^2 个方程的齐次线性方程组 $\boldsymbol{vP}=\boldsymbol{O}$，得到解空间的一组基.

2. 将解空间的一组基中的向量随机进行线性组合，得到一组解 $\boldsymbol{v}$，将 $\boldsymbol{v}$ 中的前一半分量 $h_i\in F_q(i=0,\cdots,n-1)$代入$\sum_{i=0}^{n-1}h_i\boldsymbol{H}^i$，得到矩阵 $\boldsymbol{X}$.

3. 检验矩阵 $\boldsymbol{X}$ 是否可逆，若不可逆，返回步 2.

4. 计算 $\boldsymbol{X}^{-1}\boldsymbol{BY}=K$.

5. 返回 K.

下面我们对算法 2，评估其 bit 复杂性. 总结如表 2.

表 2　算法 2 的计算复杂性分析

内容	bit 复杂性	解释
$\boldsymbol{vP}=\boldsymbol{O}$	$O(n^2(2n)^{\omega-1}\log^2 q)$	$2n$ 个变量 n^2 个方程
解 $\boldsymbol{v}$	$O(n^2(2n-r)^{\omega-1}\log^2 q)$	基中向量的随机线性组合
解矩阵 $\boldsymbol{X}$	$O((n-2)n^\omega\log^2 q)$	$\sum_{i=0}^{n-1}h_i\boldsymbol{H}^i$
矩阵 $\boldsymbol{X}$ 的逆矩阵	$O(n^\omega\log^2 q)$	1 个逆运算
解矩阵 $\boldsymbol{Y}$	$O(n^\omega\log^2 q)$	$\boldsymbol{X}^{-1}\boldsymbol{A}$
$\boldsymbol{X}^{-1}\boldsymbol{BY}=K$	$O(3n^\omega\log^2 q)$	1 个逆，2 个乘法运算

根据表 2，忽略小的固定参数，算法 2 攻击 HKKS 密钥交换协议的 bit 复杂度是 $O(n^{\omega+1}\log^2 q)$.

将线性化方程组攻击应用到矩阵群环 $M_3(F_7(A_5))$上的 HKKS 协议，同样可以得到齐次线性方程组(4). 其中

$$\boldsymbol{X}=\sum_{i=0}^{n-1}h_i\boldsymbol{H}^i,\ \boldsymbol{Y}=\sum_{j=0}^{n-1}g_j\boldsymbol{G}^j,\ h_i,g_j\in F_7(A_5),$$

$$h_i=\Big(\sum_{k=1}^{60}h_k^{(i)}\sigma_k\Big)_{0\leq i\leq 2},\ g_j=\Big(\sum_{k=1}^{60}g_k^{(j)}\sigma_k\Big)_{0\leq j\leq 2},\ h_k^{(i)},g_k^{(j)}\in F_q,$$

$\boldsymbol{v}=\left(\sum_{k=1}^{60}v_k^{(i)}\sigma_k\right)_{1\le i\le 6}$, $\boldsymbol{P}=\left(\sum_{k=1}^{60}p_k^{(i,j)}\sigma_k\right)_{1\le i\le 6,1\le j\le 9}$, $v_k^{(i)},p_k^{(i,j)}\in F_7$.

将矩阵群环 $M_3(F_7(A_5))$上的线性方程组 $\boldsymbol{vP}=\boldsymbol{O}$ 转化为有限域 F_7 上的一个具有 $360=120n(n=3)$ 个未知量、$540=60n^2$ 个方程的齐次线性方程组. 利用算法 2 方法同样可以求出解矩阵 $\boldsymbol{X},\boldsymbol{Y}$,并且计算出共享密钥 $K=\boldsymbol{X}^{-1}\boldsymbol{BY}$.

4.3 超定多变量方程组攻击

根据 4.2 节,可以知道在 HKKS 密钥交换协议中,对于任意的 $m\in Z_+$,私钥 $\boldsymbol{H}^{-m}$ 能够由集合 $\{\boldsymbol{I},\overline{\boldsymbol{H}},\overline{\boldsymbol{H}}^2,\cdots,\overline{\boldsymbol{H}}^{n-1}\}$ 线性表示. 其中,$\overline{\boldsymbol{H}}=\boldsymbol{H}^{-1}$. 令

$$\boldsymbol{X}=\boldsymbol{H}^{-m}=\sum_{i=0}^{n-1}\tilde{h}_i\overline{\boldsymbol{H}}^i,$$

其中,$\tilde{h}_i\in F_q(i=0,\cdots,n-1)$.

私钥 $\boldsymbol{G}^a(\boldsymbol{G}=\boldsymbol{HM})$ 由集合 $\{\boldsymbol{I},\boldsymbol{G},\boldsymbol{G}^2,\cdots,\boldsymbol{G}^{n-1}\}$ 线性表示. 令

$$\boldsymbol{Y}=\boldsymbol{G}^a=\sum_{j=0}^{n-1}\tilde{g}_j\boldsymbol{G}^j,$$

其中,$\tilde{g}_j\in F_q(i=0,\cdots,n-1)$.

因此,根据 $\boldsymbol{A}=\boldsymbol{H}^{-a}(\boldsymbol{HM})^a$,可得

$$\boldsymbol{A}=\sum_{i=0}^{n-1}\tilde{h}_i\overline{\boldsymbol{H}}^i\sum_{j=0}^{n-1}\tilde{g}_j\boldsymbol{G}^j=\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}\tilde{h}_i\tilde{g}_j\overline{\boldsymbol{H}}^i\boldsymbol{G}^j \quad (5)$$

同时,$\sum_{i=0}^{n-1}\tilde{h}_i\overline{\boldsymbol{H}}^i$ 是可逆矩阵.

将式(5)中的矩阵按行拉直,等价转化为式(6)如下:

$$\boldsymbol{A}=\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}\tilde{h}_i\tilde{g}_j\overrightarrow{\overline{\boldsymbol{H}}^i\boldsymbol{G}^j} \quad (6)$$

式(6)是求解 $k=n^2$ 个方程、$m=2n$ 个未知量的超定多变量方程组.

利用 XL 算法计算超定多变量方程组,易得式(6)的至少一个解 $\boldsymbol{X}=\sum_{i=0}^{n-1}\tilde{h}_i\overline{\boldsymbol{H}}^i$,同时矩阵 $\boldsymbol{X}$ 可逆. 进而可以得到一组解矩阵 $\boldsymbol{X},\boldsymbol{Y}$.

根据

$$\begin{aligned}\boldsymbol{XBY}&=\boldsymbol{X}\overline{\boldsymbol{H}}^b\boldsymbol{G}^b\boldsymbol{Y}\\&=\left(\sum_{i=0}^{n-1}\tilde{h}_i\overline{\boldsymbol{H}}^i\right)\overline{\boldsymbol{H}}^b\boldsymbol{G}^b\left(\sum_{j=0}^{n-1}\tilde{g}_j\boldsymbol{G}^j\right)\\&=\overline{\boldsymbol{H}}^b\left(\sum_{i=0}^{n-1}\tilde{h}_i\overline{\boldsymbol{H}}^i\right)\left(\sum_{j=0}^{n-1}\tilde{g}_j\boldsymbol{G}^j\right)\boldsymbol{G}^b\\&=\boldsymbol{H}^{-b}\boldsymbol{XYG}^b\\&=\boldsymbol{H}^{-b}\boldsymbol{AG}^b\\&=K,\end{aligned}$$

可知,任意一组满足方程(6)的多变量系统多项式方程得到的解矩阵$(\boldsymbol{X},\boldsymbol{Y})$并且解矩阵 $\boldsymbol{X}$ 可逆,都可以得到相同的共享密钥 K.

我们知道利用 XL 算法(又称乘法和线性化方法)求解 m 个方程、k 个未知量的二元多项式方程组,基本思想是将系统扩大并线性化,具体方法是将每一个多元方程乘以次数小于某一上界所有可能的单项式,使原方程组扩充为具有大数量的高阶多元方程组,然后将扩充的方程组线性化.

当 $k\ge\varepsilon m^2$ 时,即 $n^2\ge\varepsilon(2n)^2$,令 $\varepsilon=0.25$,XL 算法可以大约在 $O((2n)^{2\omega}/2)$的时间内运行成功[18-19].

下面用算法 3 描述多变量系统方程组攻击 HKKS 密钥交换协议.

算法 3. 求解共享密钥 K.

输入:$\boldsymbol{H},\boldsymbol{M},\boldsymbol{A},\boldsymbol{B}$

输出:共享密钥 K

1. 利用 XL 算法计算 $2n$ 个变量 n^2 个方程的齐次线性方程组 $\vec{\boldsymbol{A}}=\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}\tilde{h}_i\tilde{g}_j\overrightarrow{\boldsymbol{H}^i\boldsymbol{G}^j}$,得到解空间的一组基.

2. 将解空间的一组基中的向量进行随机线性组合,得到一组解,将解的一半分量 $\tilde{h}_i\in F_q(i=0,\cdots,n-1)$ 代入 $\sum_{i=0}^{n-1}\tilde{h}_i\boldsymbol{H}^i$,可得矩阵 $\boldsymbol{X}$.

3. 检验矩阵 $\boldsymbol{X}$ 是否可逆,若不可逆,返回步 2.

4. 计算 $\boldsymbol{X}^{-1}\boldsymbol{BY}=K$.

5. 返回 K.

下面对算法 3 评估其 bit 复杂度. 总结如表 3.

表 3 算法 3 的复杂性分析

内容	bit 复杂性	解释
式(6)	$O\left(\frac{(2n)^{2\omega}}{2}\log^2 q\right)$	XL 算法
式(6)一个随机解	$O(n^2(2n-r)^{\omega-1}\log^2 q)$	基中一组向量线性组合
解矩阵 $\boldsymbol{X}$	$O((n-2)n^{\omega}\log^2 q)$	$\sum_{i=0}^{n-1}\tilde{h}_i\boldsymbol{H}^i$
矩阵 $\boldsymbol{X}$ 是可逆的	$O(n^{\omega}\log^2 q)$	1 个逆运算
解矩阵 $\boldsymbol{Y}$	$O(n^{\omega}\log^2 q)$	1 个乘法 $\boldsymbol{XA}$
$\boldsymbol{X}^{-1}\boldsymbol{BY}=K$	$O(2n^{\omega}\log^2 q)$	2 个乘法运算

根据表 3 可知,忽略小的固定参数,利用算法 3 分析 HKKS 协议的 bit 复杂度是 $O(n^{2\omega}\log^2 q)$.

矩阵群环 $M_3(F_7(A_5))$上的 HKKS 协议运用超定多变量方程组攻击,可以得到式(6),将矩阵群环 $M_3(F_7(A_5))$上的式(6)转化为有限域 F_7 上一个具有 $360=120n(n=3)$ 个未知量、$540=60n^2$ 个方程的超定多变量方程组. 其中

$$\boldsymbol{A}=\left(\sum_{k=1}^{60}a_k^{(i)}\sigma_k\right)_{1\le i\le 9},\ a_k^{(i)}\in F_q,$$

$$\widetilde{h}_i=\Big(\sum_{k=1}^{60}\widetilde{h}_k^{(i)}\sigma_k\Big)_{0\le i\le 2},\ \widetilde{g}_j=\Big(\sum_{k=1}^{60}\widetilde{g}_k^{(j)}\sigma_k\Big)_{0\le j\le 2},$$
$$\widetilde{h}_k^{(i)},\widetilde{g}_k^{(j)}\in F_q.$$

利用算法 3 方法求出解矩阵 $\boldsymbol{X},\boldsymbol{Y}$，进而计算出共享密钥 K.

4.4　离散对数方法

这部分我们用离散对数方法分析 P-HKKS 问题，即根据 $\boldsymbol{A}=\boldsymbol{H}^{-a}(\boldsymbol{HM})^a=\boldsymbol{H}^{-a}\boldsymbol{G}^a$，利用离散对数方法求解私钥 $a\in Z_+$，进而分析 HKKS 密钥交换协议.

将矩阵 $\boldsymbol{H}$ 和 $\boldsymbol{G}$ 分别转化为 Jordan 标准型，即分别存在可逆矩阵 $\boldsymbol{P},\boldsymbol{Q}$，表示如下：

$$\boldsymbol{P}^{-1}\boldsymbol{HP}=J_{\boldsymbol{H}},$$
$$\boldsymbol{Q}^{-1}\boldsymbol{GQ}=J_{\boldsymbol{G}}.$$

其中，$J_{\boldsymbol{H}}=J(\lambda_1,n_1)\oplus\cdots\oplus J(\lambda_t,n_t)$，$\lambda_i(i=1,\cdots,t)$ 是矩阵 $\boldsymbol{H}$ 在 $\overline{K}$ 中的特征值，$\sum_{i=1}^{t}n_i=n$；$J_{\boldsymbol{G}}=J(\tilde{\lambda}_1,\tilde{n}_1)\oplus\cdots\oplus J(\tilde{\lambda}_s,\tilde{n}_s)$，$\tilde{\lambda}_i(i=1,\cdots,s)$ 是矩阵 $\boldsymbol{G}$ 在 $\overline{K}$ 中的特征值，$\sum_{i=1}^{s}\tilde{n}_i=n$.

将矩阵 $J_{\boldsymbol{H}}$ 和 $J_{\boldsymbol{G}}$ 分别代入 $\boldsymbol{A}=\boldsymbol{H}^{-a}\boldsymbol{G}^a$，通过化简可得

$$J_{\boldsymbol{H}}^a\boldsymbol{P}^{-1}\boldsymbol{AQ}^{-1}=\boldsymbol{P}^{-1}\boldsymbol{Q}^{-1}J_{\boldsymbol{G}}^a \tag{7}$$

为了通过式(7)求出私钥 a，首先，需要分别求出 $J_{\boldsymbol{H}}$、$J_{\boldsymbol{G}}$ 和 $\boldsymbol{P}$、$\boldsymbol{Q}$，然后我们根据矩阵标准型 $J_{\boldsymbol{H}}$ 和 $J_{\boldsymbol{G}}$ 的类型(如对角矩阵和一般类型的矩阵等)分析求解私钥 a.

下面以矩阵 $\boldsymbol{G}$ 为例，计算其 Jordan 标准型 $J_{\boldsymbol{G}}$ 和相应的转换矩阵 $\boldsymbol{Q}$. 因为计算转换矩阵 $\boldsymbol{Q}$ 需要在分裂域上进行计算，我们采用 Menezes-Wu 的思想[20]，同时也进行改进，给出计算矩阵 $\boldsymbol{G}$ 的 Jordan 标准型 $J_{\boldsymbol{G}}$ 和对应的转换矩阵 $\boldsymbol{Q}$ 的算法.

算法 4.　计算矩阵的 Jordan 标准型和相应的转换矩阵.

输入：矩阵 $\boldsymbol{G}$

输出：Jordan 标准型 $J_{\boldsymbol{G}}$ 和对应的转换矩阵 $\boldsymbol{Q}$

1. 计算计算矩阵 $\boldsymbol{G}$ 的有理标准型 $\boldsymbol{G}_{rat}$[21]，得到所有的不变因子 $f_{G_0}(\lambda),\cdots,f_{G_{k-1}}(\lambda)$，并满足 $f_{G_i}(\lambda)\mid f_{G_{i+1}}(\lambda)$ 对于 $i=0,\cdots,k-1$. 矩阵 $\boldsymbol{G}$ 的特征多项式

$$p_{\boldsymbol{G}}(\lambda)=|\lambda\boldsymbol{I}-\boldsymbol{G}|=f_{G_0}(\lambda),\cdots,f_{G_{k-1}}(\lambda).$$

2. $f_{G_{k-1}}(\lambda)$ 在 F_q 上进行因式分解[22]，因此，分解特征多项式 $p_{\boldsymbol{G}}(\lambda)=f_1^{e_1}(\lambda)f_2^{e_2}(\lambda)\cdots f_t^{e_t}(\lambda)$，其中，$f_i(\lambda)$ 是度数为 m_i 的首一不可约多项式($i=1,2,\cdots,t$)，$e_i\in Z_+$.

3. 计算 $f_i(\lambda)$ 在 $F_{q^{m_i}}$ 上的一个本原根 λ_i，进而得所有的根为 $\lambda_i,\lambda_i^q,\cdots,\lambda_i^{q^{m_i-1}}$. 令 $\alpha_{i1}=\lambda_i$，

$$\alpha_{ij}=\lambda_i^{q^{j-1}}\bmod(f_i(\lambda)),\quad 2\le j\le m_i.$$

4. 当 $i=1:t$，进行如下操作：

4.1. $r_0\leftarrow n$.

4.2. 计算 $(\boldsymbol{G}-\alpha_{i1}\boldsymbol{I})^l$，并计算 $r_l=\mathrm{rank}((\boldsymbol{G}-\alpha_{i1}\boldsymbol{I})^l)$，$l=1,2,\cdots,c,c+1$. 其中，$c$ 是使得 $r_c=r_{c+1}$ 的最大正整数.

4.3. J_{i1} 是对应于特征值 α_{i1} 阶数为 $l(1\le l\le c)$ 的 $r_{l+1}-2r_l+r_{l-1}$ 个 Jordan 块的直和. 返回步 4.2.

4.4. J_{ij} 是对应于特征值 α_{ij} ($2\le j\le m_i$) 阶数为 $l(1\le l\le c)$ 的 $r_{l+1}-2r_l+r_{l-1}$ 个 Jordan 块的直和.

4.5. $J_i\leftarrow J_{i1}\oplus J_{i2}\oplus\cdots\oplus J_{im_i}$.

4.6. 求解齐次线性方程组 $(\boldsymbol{G}-\alpha_{i1}\boldsymbol{I})\boldsymbol{y}=\boldsymbol{0}$，得到对应于特征值 α_{i1} 的特征向量 $\boldsymbol{\mu}_i$.

4.7. 将 $\boldsymbol{\mu}_i$ 作为第 1 列构造矩阵 $\boldsymbol{P}_i\in GL_n(F_{q^{m_i}})$.

5. $J_{\boldsymbol{G}}\leftarrow J_1\oplus J_2\oplus\cdots\oplus J_t$.

6. t 是使得 $r_c=r_{c+1}$ 的 c 的最大值. 若 $t>1$，则进行如下操作：

6.1. 设 $\lambda\in F_{q^m}$ 是对应于 t 阶若当块的特征值.

6.2. 计算 $(\boldsymbol{G}-\lambda\boldsymbol{I})^{t-1}$ 的幂零空间的一组基 $\boldsymbol{B}_1$.

6.3. 计算 $(\boldsymbol{G}-\lambda\boldsymbol{I})^t$ 的幂零空间的一组基 $\boldsymbol{B}_2$.

6.4. 检验基 $\boldsymbol{B}_2$ 是不是基 $\boldsymbol{B}_1$ 中生成子空间的一个向量 $\boldsymbol{u}$.

6.5. $\boldsymbol{u}_t\leftarrow\boldsymbol{u}$，$\boldsymbol{u}_j\leftarrow(\boldsymbol{G}-\lambda\boldsymbol{I})\boldsymbol{u}_{j+1}(j=t-1,\cdots,2,1)$.

6.6. $\boldsymbol{u}_1,\boldsymbol{u}_2,\cdots,\boldsymbol{u}_t$ 作为前 t 列，构造矩阵 $\boldsymbol{Q}\in GL_n(F_{q^m})$.

7. 返回 Jordan 标准型 $J_{\boldsymbol{G}}$ 和转换矩阵 $\boldsymbol{Q}$.

通过算法 4，可以分别求出式(7)中的转换矩阵 $\boldsymbol{P}$、$\boldsymbol{Q}$ 和若当标准型 $J_{\boldsymbol{H}}$、$J_{\boldsymbol{G}}$. 现在通过标准型为 $J_{\boldsymbol{H}}$、$J_{\boldsymbol{G}}$ 的类型(对角阵或者三角形矩阵)，并将其分别代入式(7)

$$J_{\boldsymbol{H}}^a\boldsymbol{P}^{-1}\boldsymbol{AQ}^{-1}=\boldsymbol{P}^{-1}\boldsymbol{Q}^{-1}J_{\boldsymbol{G}}^a,$$

求解私钥 a. 令

$$\boldsymbol{P}^{-1}\boldsymbol{AQ}^{-1}=(a_{ij})_{n\times n},\ \boldsymbol{P}^{-1}\boldsymbol{Q}^{-1}=(b_{ij})_{n\times n}.$$

这里把 $J_{\boldsymbol{H}}$，$J_{\boldsymbol{G}}$ 分为如下 3 种情况：两者都是对角阵，其中一个是对角阵，两个都不是对角阵.

情况 1.　当 $J_{\boldsymbol{H}}$，$J_{\boldsymbol{G}}$ 都是 n 阶对角阵时.

式(7)用矩阵形式表示如下：

$$\begin{pmatrix}\lambda_1^a & & \\ & \ddots & \\ & & \lambda_n^a\end{pmatrix}\begin{pmatrix}a_{11} & \cdots & a_{1n}\\ \vdots & \ddots & \vdots\\ a_{n1} & \cdots & a_{nn}\end{pmatrix}=$$
$$\begin{pmatrix}b_{11} & \cdots & b_{1n}\\ \vdots & \ddots & \vdots\\ b_{n1} & \cdots & b_{nn}\end{pmatrix}\begin{pmatrix}\tilde{\lambda}_1^a & & \\ & \ddots & \\ & & \tilde{\lambda}_n^a\end{pmatrix}.$$

从而得到如下关系：

$$\begin{pmatrix}a_{11}\lambda_1^a & \cdots & a_{1n}\lambda_1^a\\ \vdots & \ddots & \vdots\\ a_{n1}\lambda_n^a & \cdots & a_{nn}\lambda_n^a\end{pmatrix}=\begin{pmatrix}b_{11}\tilde{\lambda}_1^a & \cdots & b_{1n}\tilde{\lambda}_n^a\\ \vdots & \ddots & \vdots\\ b_{n1}\tilde{\lambda}_1^a & \cdots & b_{nn}\tilde{\lambda}_n^a\end{pmatrix}.$$

根据上式矩阵两端对应元素相等，将式(7)转化为求解 n^2 个分裂域上的离散对数问题. 因此可知，当 $J_{\boldsymbol{H}}$、$J_{\boldsymbol{G}}$ 都是对角阵时，分析求解式(7)中未知量 a

的困难性与 n^2 个相对小的分裂域上的离散对数问题有关.

情况 2. 当 J_H, J_G 只有一个是对角阵时.

当若当标准型 J_H 是对角矩阵,若当标准型 J_G 有 s 个若当块 $J_i(i=1,2,\cdots,s)$ 时,式(7)用矩阵形式表示得到如下关系:

$$\begin{pmatrix} a_{11}\lambda_1^a & \cdots & a_{1n}\lambda_1^a \\ \vdots & \ddots & \vdots \\ a_{n1}\lambda_n^a & \cdots & a_{nn}\lambda_n^a \end{pmatrix} = \begin{pmatrix} b_{11}\tilde{\lambda}_1^a & \cdots & b_{1,n_1+1}\tilde{\lambda}_2^a & \cdots & b_{1,n_{s-1}+1}\tilde{\lambda}_s^a & \cdots \\ b_{21}\tilde{\lambda}_1^a & \cdots & b_{2,n_1+1}\tilde{\lambda}_2^a & \cdots & b_{2,n_{s-1}+1}\tilde{\lambda}_s^a & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ b_{n1}\tilde{\lambda}_1^a & \cdots & b_{n,n_1+1}\tilde{\lambda}_2^a & \cdots & b_{n,n_{s-1}+1}\tilde{\lambda}_s^a & \cdots \end{pmatrix}.$$

因此可知,当 J_H 是对角矩阵时,分析求解式(7)中未知量 a 的困难性与分裂域上 ns 个离散对数问题有关.

当若当标准型 J_G 是对角矩阵,若当标准型 J_H 有 t 个若当块 $J_i(i=1,2,\cdots,t)$ 时,式(7)可以转化为如下矩阵形式:

$$\begin{pmatrix} \vdots & \vdots & \cdots & \vdots \\ a_{n_1,1}\lambda_1^a & a_{n_1,2}\lambda_1^a & \cdots & a_{n_1,n}\lambda_1^a \\ \vdots & \vdots & \cdots & \vdots \\ a_{n_2,1}\lambda_2^a & a_{n_2,2}\lambda_2^a & \cdots & a_{n_2,n}\lambda_2^a \\ \vdots & \vdots & \cdots & \vdots \\ a_{n_t,1}\lambda_t^a & a_{n_t,2}\lambda_t^a & \cdots & a_{n_t,n}\lambda_t^a \\ \vdots & \vdots & \cdots & \vdots \end{pmatrix} = \begin{pmatrix} b_{11}\tilde{\lambda}_1^a & \cdots & b_{1n}\tilde{\lambda}_n^a \\ \vdots & \ddots & \vdots \\ b_{n1}\tilde{\lambda}_1^a & \cdots & b_{nn}\tilde{\lambda}_n^a \end{pmatrix}.$$

因此可知,当 J_G 是对角矩阵时,分析求解式(7)中未知量 a 的困难性与 nt 个相对小的分裂域上离散对数问题有关.

情况 3. 当 J_H、J_G 都不是对角阵时,J_H 有 t 个若当块 $J_i(i=1,2,\cdots,t)$,J_G 有 s 个若当块 $J_i(i=1,2,\cdots,s)$. 式(7)可以转化为如下形式:

$$\begin{pmatrix} \vdots & \vdots & \cdots & \vdots \\ a_{n_1,1}\lambda_1^a & a_{n_1,2}\lambda_1^a & \cdots & a_{n_1,n}\lambda_1^a \\ \vdots & \vdots & \cdots & \vdots \\ a_{n_2,1}\lambda_2^a & a_{n_2,2}\lambda_2^a & \cdots & a_{n_2,n}\lambda_2^a \\ \vdots & \vdots & \cdots & \vdots \\ a_{n_t,1}\lambda_t^a & a_{n_t,2}\lambda_t^a & \cdots & a_{n_t,n}\lambda_t^a \\ \vdots & \vdots & \cdots & \vdots \end{pmatrix} = \begin{pmatrix} b_{11}\tilde{\lambda}_1^a & \cdots & b_{1,n_1+1}\tilde{\lambda}_2^a & \cdots & b_{1,n_{s-1}+1}\tilde{\lambda}_s^a & \cdots \\ b_{21}\tilde{\lambda}_1^a & \cdots & b_{2,n_1+1}\tilde{\lambda}_2^a & \cdots & b_{2,n_{s-1}+1}\tilde{\lambda}_s^a & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ b_{n1}\tilde{\lambda}_1^a & \cdots & b_{n,n_1+1}\tilde{\lambda}_2^a & \cdots & b_{n,n_{s-1}+1}\tilde{\lambda}_s^a & \cdots \end{pmatrix}.$$

因此,求解式(7)中未知量 a 的困难性与 st 个相对小的分裂域上离散对数问题有关.

根据上述分析,下面给出求解 HKKS 密钥交换协议中私钥 a 的算法.

算法 5. 计算HKKS密钥交换协议中的私钥 a.

输入:矩阵 $\boldsymbol{A},\boldsymbol{H},\boldsymbol{G}$

输出:私钥 a

1. 利用算法 4 分别计算矩阵 $\boldsymbol{H}$ 和 $\boldsymbol{G}$ 的 Jordan 标准型 J_H, J_G 和对应的转换矩阵 $\boldsymbol{P},\boldsymbol{Q}$.

2. 计算 $\boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{Q}^{-1}=(a_{ij})_{n\times n}$,$\boldsymbol{P}^{-1}\boldsymbol{Q}^{-1}=(b_{ij})_{n\times n}$.

3. 当 J_H, J_G 都是对角阵时,对于 $i=1:n$; $j=1:n$.

3.1. 式(7)左右两端的(i,j)元分别是 $a_{ij}\lambda_i^a$,$b_{ij}\tilde{\lambda}_j^a$.

3.2. $q^{\delta_{ij}} \leftarrow lcm(ord(\lambda),ord(\tilde{\lambda}))$.

3.3. 计算 $F_{q^{\delta_{ij}}}$ 上的离散对数问题,得 $a \bmod (q^{\delta_{ij}})$.

4. 当 J_H 都是对角阵时,J_G 有 s 个若当块 $J_i(i=1,2,\cdots,s)$. 对于 $i=1:n$; $j=1,n_1+1,\cdots,n_{s-1}+1$,执行步 3.1~3.3.

5. 当 J_G 是对角矩阵,J_H 有 t 个若当块 $J_i(i=1,2,\cdots,t)$. 对于 $i=n_1,n_2,\cdots,n_t$; $j=1:n$,执行步 3.1~3.3.

6. J_H 有 t 个若当块 $J_i(i=1,2,\cdots,t)$,J_G 有 s 个若当块 $J_i(i=1,2,\cdots,s)$. 对于 $i=n_1,n_2,\cdots,n_t$; $j=1,n_1+1,\cdots,n_{s-1}+1$,执行步 3.1~3.3.

7. 利用广义的中国剩余定理,求解私钥 a.

命题 3. 算法 5 将式(7) $J_H^a\boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{Q}^{-1}=\boldsymbol{P}^{-1}\boldsymbol{Q}^{-1}J_G^a$ 平均多项式时间规约到小的分裂域 $F_{q^{\delta_{ij}}}$ 上的离散对数问题,其中 $1\le i\le n, 1\le j\le n$.

证明. 算法 4 求解 $M_n(F_q)$ 上的矩阵的 Jordan 标准型是多项式计算复杂度. 对于一般矩阵,计算其有理标准型和转换矩阵的计算复杂度是 $O(n^4)$,因此矩阵分解为有理标准型的计算复杂度小于 $O(n^4)$. 有限域上多项式分解的计算复杂度大约是 $O(n^{(2+o(1))})$[21-22]. 因此,把 $M_n(F_q)$ 上的矩阵转化为 Jordan 标准型是多项式计算复杂度. 算法 4 中求解转换矩阵是求解线性方程组,其计算复杂度也是多项式的. 算法 5 中步骤 4、5 或 6,最多迭代 n^2 次. 证毕.

命题 3 也说明,利用离散对数方法将 HKKS 问题多项式时间转化为求解相对小的分裂域 $F_{q^{\delta_{ij}}}$ $(1\le i\le n, 1\le j\le n)$ 上的离散对数问题. 若命题 3 成立,则攻击者可以在 $O(n^4\log^2 q)$bit 复杂度内转化为相对小的分裂域上的离散对数问题. 进而我们能够攻破 HKKS 密钥交换协议.

下面我们对算法 5,评估其 bit 复杂度. 总结如表 4.

表 4　算法 5 的计算复杂性分析

内容	bit 复杂性	解释
步骤 1	$O(n^4\log^2 q)$	算法 4
步骤 2	$O(5n^\omega\log^2 q)$	2 个逆，3 个乘法运算
步骤 3	$O(n^2\log^2 q)$	迭代 n^2 次
步骤 4,5,6	$O(n^2\log^2 q)$	迭代小于 n^2 次
步骤 7	$O(n^2\log^2 q)$	广义的中国剩余定理

根据表 4 可知，若小的分裂域上的离散对数问题都可解，则利用算法 5 分析 HKKS 密钥交换协议是以 $O(n^4\log^2 q)$bit 复杂度转化为小的分裂域上的离散对数问题.

为容易理解离散对数方法，下面我们通过 3 个例子说明上述离散对数方法对 HKKS 密钥交换协议分析的应用，令 $q=2^{16}$.

例 1.　当 J_H，J_G都是 2 阶对角阵时，

公钥

$$\boldsymbol{M}=\begin{pmatrix}50501 & 18859\\ 15842 & 36329\end{pmatrix},\ \boldsymbol{H}=\begin{pmatrix}54721 & 720\\ 22682 & 54665\end{pmatrix}.$$

计算

$$\boldsymbol{G}=\boldsymbol{MH}=\begin{pmatrix}24771 & 63557\\ 33158 & 24778\end{pmatrix}.$$

计算 Jordan 标准型 J_H、J_G和转换矩阵 $\boldsymbol{P}$、$\boldsymbol{Q}$ 分别为

$$J_H=\begin{pmatrix}9 & \\ & 65\end{pmatrix},\ J_G=\begin{pmatrix}9 & \\ & 0\end{pmatrix},$$

$$\boldsymbol{P}=\begin{pmatrix}10 & 1\\ 817 & 120\end{pmatrix},\ \boldsymbol{Q}=\begin{pmatrix}149 & 22\\ 168 & 738\end{pmatrix}.$$

在密钥交换协议中，攻击者截获 Alice 发送的密钥

$$\boldsymbol{A}=\begin{pmatrix}5028 & 21219\\ 57792 & 6149\end{pmatrix}.$$

依据式(7) $J_H^a\boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{Q}^{-1}=\boldsymbol{P}^{-1}\boldsymbol{Q}^{-1}J_G^a$，

计算可得

$$\begin{pmatrix}9^a & \\ & 65^a\end{pmatrix}\begin{pmatrix}15024 & 0\\ 3650 & 0\end{pmatrix}=\begin{pmatrix}15024 & 1138\\ 45182 & 11106\end{pmatrix}\begin{pmatrix}9^a & \\ & 0\end{pmatrix}.$$

我们得到 4 个有限域上的离散对数问题，整理可得

$$3650\cdot 65^a=45182\cdot 9^a.$$

利用小的有限域 $F_{2^{16}}$ 上离散对数的穷搜索方法，求解上式得

$$a=962.$$

例 2.　当只有 J_G都是 2 阶对角阵时，

公钥

$$\boldsymbol{M}=\begin{pmatrix}54634 & 56280\\ 46651 & 28025\end{pmatrix},\ \boldsymbol{H}=\begin{pmatrix}33479 & 29866\\ 54870 & 33479\end{pmatrix}.$$

计算

$$\boldsymbol{G}=\boldsymbol{MH}=\begin{pmatrix}28496 & 57820\\ 53610 & 28538\end{pmatrix}.$$

计算 Jordan 标准型 J_H、J_G和转换矩阵 $\boldsymbol{P}$、$\boldsymbol{Q}$ 分别为

$$J_H=\begin{pmatrix}59 & 1\\ & 59\end{pmatrix},\ J_G=\begin{pmatrix}42 & \\ & 0\end{pmatrix},$$

$$\boldsymbol{P}=\begin{pmatrix}273 & 62\\ 1 & 278\end{pmatrix},\ \boldsymbol{Q}=\begin{pmatrix}370 & 449\\ 1 & 501\end{pmatrix}.$$

在密钥交换协议中，攻击者截获 Alice 发送的密钥

$$\boldsymbol{A}=\begin{pmatrix}10381 & 4737\\ 11694 & 52755\end{pmatrix}.$$

依据式(7) $J_H^a\boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{Q}^{-1}=\boldsymbol{P}^{-1}\boldsymbol{Q}^{-1}J_G^a$，计算可得

$$\begin{pmatrix}59^a & *\\ & 59^a\end{pmatrix}\begin{pmatrix}2281 & 0\\ 18059 & 0\end{pmatrix}=$$

$$\begin{pmatrix}55583 & 55851\\ 58542 & 39344\end{pmatrix}\begin{pmatrix}42^a & \\ & 0\end{pmatrix}.$$

进而得到 2 个有限域上的离散对数问题，整理可得

$$18059\cdot 59^a=58542\cdot 42^a.$$

利用小的有限域 $F_{2^{16}}$ 上离散对数的穷搜索方法，求解上式得未知量

$$a=693.$$

例 3.　当 J_H，J_G都不是 2 阶对角阵时，

公钥

$$\boldsymbol{M}=\begin{pmatrix}50253 & 53575\\ 60830 & 10866\end{pmatrix},\ \boldsymbol{H}=\begin{pmatrix}33479 & 29866\\ 54870 & 33479\end{pmatrix}.$$

计算

$$\boldsymbol{G}=\boldsymbol{MH}=\begin{pmatrix}33576 & 32959\\ 35867 & 33576\end{pmatrix}.$$

计算 Jordan 标准型 J_H、J_G和转换矩阵 $\boldsymbol{P}$、$\boldsymbol{Q}$ 分别为

$$J_H=\begin{pmatrix}59 & 1\\ & 59\end{pmatrix},\ J_G=\begin{pmatrix}42 & 1\\ & 42\end{pmatrix},$$

$$\boldsymbol{P}=\begin{pmatrix}273 & 62\\ 1 & 278\end{pmatrix},\ \boldsymbol{Q}=\begin{pmatrix}370 & 449\\ 1 & 501\end{pmatrix}.$$

在密钥交换协议中，攻击者截获 Alice 发送的密钥

$$\boldsymbol{A}=\begin{pmatrix}37030 & 36213\\ 19142 & 35209\end{pmatrix}.$$

依据式(7) $J_H^a\boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{Q}^{-1}=\boldsymbol{P}^{-1}\boldsymbol{Q}^{-1}J_G^a$，计算可得

$$\begin{pmatrix} 59^a & * \\ & 59^a \end{pmatrix}\begin{pmatrix} 45970 & 11987 \\ 51639 & 17117 \end{pmatrix}=$$
$$\begin{pmatrix} 55583 & 55851 \\ 58542 & 39344 \end{pmatrix}\begin{pmatrix} 42^a & * \\ & 42^a \end{pmatrix}.$$

我们得到 1 个有限域上的离散对数问题，整理得

$$45970 \cdot 59^a = 58542 \cdot 42^a.$$

利用小的有限域 $F_{2^{16}}$ 上离散对数的穷搜索方法，求出未知量

$$a = 1201.$$

通过例 1～3 求出 Alice 的私钥 a，将其代入 $\boldsymbol{H}^{-a}\boldsymbol{B}(\boldsymbol{MH})^a$，得到共享密钥 K. 也可以利用同样方法，求出 Bob 的私钥 b，进而求出共享密钥 K.

尽管离散对数方法在有限域上进行分析相对来说比较复杂，但是计算复杂度并不高，故该攻击方法也不失为一种分析方法. 然而在矩阵群环 $M_3(F_7(A_5))$ 上离散对数方法将会更加复杂，文中我们没有利用离散对数方法对 $M_3(F_7(A_5))$ 上的 HKKS 协议进行分析.

4.5 算法总结分析

我们根据文献[12]对 HKKS 协议给出建议的参数 $q=2^{127}$、$n=2$，文献[13]在矩阵群环 $M_3(F_7(A_5))$ 上设计的 HKKS 协议，对上述几种攻击算法总结如表 5.

表 5 攻击 HKKS 协议的算法复杂性总结

算法	$q=2^{127}, n=2$	$M_3(F_7(A_5))$	成功概率
1	$2^{18.7}$	$2^{34.4}$	1
2	$2^{17.4}$	$2^{31.6}$	1
3	$2^{18.7}$	$2^{43.3}$	1
5	$2^{18.0}$	—	$\boldsymbol{H}$ 特征多项式可约

由表 5 可知，在有限域上，算法 1 和算法 3 的运行时间几乎是相同的，而算法 2 的运行时间是最少的. 从表 5 可知，在有限域上，这 4 种分析方法的 bit 复杂度都不超过 2^{30}. 然而，离散对数方法需要矩阵 $\boldsymbol{H}$ 的特征多项式可约，这样不会出现求解有限域 $F_{2^{254}}$ 上的离散对数问题，并且经过几个小时 Coppersmith 算法的预计算后，几秒钟就找到 $F_{2^{127}}$ 上的一个离散对数[23].

在矩阵群环 $M_3(F_7(A_5))$ 上的 HKKS 协议，算法 1,2,3 都是多项式复杂度，并且线性化方程组攻击的复杂度最小.

对于算法攻击成功的概率，一方面，当 $n<q$ 时，随机选取 F_q 上的 $n\times n$ 矩阵 $\boldsymbol{X}$ 是可逆矩阵的概率大于等于 $1-\frac{n}{q}$[8]，因此，在有限域 $F_{2^{127}}$ 上随机选择一个 2×2 的矩阵是可逆矩阵的概率 $\geq 1-\frac{1}{2^{126}}\approx 1$. 另一方面，在有限域 $F_{2^{127}}$ 上随机选择一个 2×2 的矩阵是可逆矩阵的概率是

$$\frac{\prod_{i=0}^{n-1}(q^i-1)}{q^{\frac{n(n+1)}{2}}}=\left(1-\frac{1}{2^{127}}\right)\left(1-\frac{1}{2^{254}}\right)\approx 1.$$

然而，求解线性方程组得到的所有解是可逆解的概率几乎为 1，故利用算法 1、2、3 能够成功攻击在有限域上的 HKKS 密钥交换协议. 在矩阵群环上算法 1、2、3(将其转化到有限域上)攻击 HKKS 协议的成功概率可作类似分析.

5 总结与下一步工作

本文针对文献[12]在有限域上 HKKS 协议，给出了 4 种攻击方法. 通过分析可知，HKKS 密钥交换协议在 $M_n(F_q)$ 上是不安全的，并且可以在不超过 2^{30} 的 bit 复杂度内攻破给定安全参数建议的 HKKS 密钥交换协议. 对于一般的矩阵环上的 HKKS 协议[13]，结构攻击、线性化方程组攻击和超定多变量方程组攻击都是成立的，并且在矩阵群环 $M_3(F_7(A_5))$ 的平台下，线性化方程组攻击的复杂度小于文献[14]线性代数攻击的复杂度. 本文的分析方法对一般的矩阵群环也是成立的.

本文主要采用线性方程组和非线性方程组类型矩阵分解和标准型类型的矩阵分解对 HKKS 密钥交换协议进行分析，介绍矩阵分解在密码分析方面的一些应用. 矩阵分解在许多抗量子密码设计和分析中处于核心地位，例如基于纠错码的密码、格密码和 MQ 密码等. 与经典密码相比，目前量子环境下的密码设计和密码分析工作还远远不够，并且基于非交换密码还没有有效的量子算法. 因此，是否存在其他的群使得 HKKS 协议是安全的，是一个公开问题，同时在其他群上构造 HKKS 协议，仍需考虑上面几种攻击方法. 我们注意到，HKKS 协议在有限域的矩阵群上计算快的优势很明显，如何在该协议的基础上，提出安全性更高的密钥交换协议是下一步值得研究的问题. 如何运用矩阵分解设计非交换密码是一个有意义的研究方向，也仍将是一个需要深入研究的问题.

致 谢 匿名审稿专家对本文提出了宝贵的修改意见，在此对审稿专家表示由衷的感谢！

参 考 文 献

[1] Li Hui-Xian, Chen Xu-Bao, Pang Liao-Jun, Wang Yu-Min. Certificateless multi-receiver signcryption scheme based on multivariate public key cryptography. Chinese Journal of Computers, 2012, 35(9): 1881-1889(in Chinese)
(李慧贤，陈绪宝，庞辽军，王育民. 基于多变量公钥密码体制的无证书多接收者签密体制. 计算机学报，2012，35(9)：1881-1889)

[2] Wang H Z, Zhang H G, Wang Z Y, Tang M. Extended multivariate public key cryptosystems with secure encryption function. Science China Information Sciences, 2011, 54(6): 1161-1171

[3] Mosca M. Post-Quantum Cryptography. Switzerland: Springer International Publishing, 2014

[4] Gaborit P. Post-Quantum Cryptography. Berlin Heidelberg: Springer, 2013

[5] Wang S B, Zhu Y, Ma D, et al. Lattice-based key exchange on small integer solution problem. Science China Information Sciences, 2014, 57(11): 1-12

[6] Jarvis K, Nevins M. ETRU: NTRU over the Eisenstein integers. Designs, Codes and Cryptography, 2015, 74(1): 1-12

[7] Cao Z. New Directions of Modern Cryptography. Boca Raton: CRC Press, 2012

[8] Tsaban B. Polynomial-time solutions of computational problems in noncommutative algebraic cryptography. Journal of Cryptology, 2015, 28(3): 601-622

[9] Armknecht F, Gagliardoni T, Katzenbeisser S, Peter A. General impossibility of group homomorphic encryption in the quantum world//Proceedings of the Public-Key Cryptography—PKC 2014. Buenos Aires, Argentina, 2014: 556-573

[10] Mao S W, Zhang H G, Wu W Q, et al. A resistant quantum key exchange protocol and its corresponding encryption scheme. China Communications, 2014, 11(9): 131-141

[11] Zhang Huan-Guo, Liu Jin-Hui, Jia Jian-Wei, et al. A survey on applications of matrix decomposition in cryptography. Journal of Cryptologic Research, 2014, 1(4): 341-357(in Chinese)
(张焕国，刘金会，贾建卫等. 矩阵分解在密码中应用研究. 密码学报，2014，1(4)：341-357)

[12] Kahrobaei D, Ha T Lam, Shpilrain V. Public key exchange using extensions by endomorphisms and matrices over a Galois field//Proceedings of the DIMACS Workshop on Multicore and Cryptography. Hoboken NJ, USA, 2014: 1-9

[13] Habeeb M, Kahrobaei D, Koupparis C, Shpilrain V. Public key exchange using semidirect product of (semi) groups//Proceedings of the Applied Cryptography and Network Security. Banff, Canada, 2013: 475-486

[14] Kreuzer M, Myasnikov A D, Ushakov A. A linear algebra attack to group-ring-based key exchange protocols//Proceedings of the Applied Cryptography and Network Security. Lausanne, Switzerland, 2014: 37-43

[15] Gashkov S B, Sergeev I S. Complexity of computation in finite fields. Journal of Mathematical Sciences, 2013, 191(5): 661-685

[16] Fu Xiang-Qun, Bao Wan-Su, Wang Shuai. Quantum algorithm for discrete logarithm over Z_N. Chinese Journal of Computers, 2014, 37(5): 1058-1062(in Chinese)
(付向群，鲍皖苏，王帅. Z_N上离散对数量子计算算法. 计算机学报，2014，37(5)：1058-1062)

[17] Myasnikov A D, Ushakov A. Quantum algorithm for discrete logarithm problem for matrices over finite group rings. Groups Complexity Cryptology, 2014, 6(1): 31-36

[18] Courtois N, Klimov A, Patarin J, Shamir A. Efficient algorithms for solving overdefined systems of multivariate polynomial equations//Proceedings of the EUROCRYPT 2000. Bruges, Belgium, 2000: 392-407

[19] Liu Niu, Tan Shaohua, Li Xiaoyu, Xu Lingling. Cryptanalysis of a key agreement protocol over the ring of multivariate polynomials. Journal of Computational Information Systems, 2014, 10(13): 5431-5436

[20] Menezes A J, Wu Y. The discrete logarithm problem in $GL(n,p)$. Ars Combinatoria, 1998, 47: 23-32

[21] Fortuna E, Gianni P. Square-free decomposition in finite characteristic: An application to Jordon Form computation. ACM SIGSAM Bulletin, 1999, 33(4): 14-32

[22] Ke Shan-Xue, Zeng Ben-Sheng, Han Wen-Bao, Zhu Wei-Hua. Fast algorithm for factoring polynomials over finite fields. Journal of Information Engineering University, 2004, 4(4): 8-14(in Chinese)
(柯善学，曾本胜，韩文报，祝卫华. 有限域上多项式分解的一种快速算法. 信息工程大学学报，2004，4(4)：8-14)

[23] Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd Edition. Hoboken: Wiley, 2007

LIU Jin-Hui, born in 1989, Ph. D. candidate. Her current research interests include cryptography and information security.

ZHANG Huan-Guo, born in 1945, professor, Ph. D. supervisor. His current research interests include information security and trusted computing.

JIA Jian-Wei, born in 1988, Ph.D. candidate. His current research interests include cryptography and information security.

WANG Hou-Zhen, born in 1981, lecturer. His current research interests include cryptography and information security.

MAO Shao-Wu, born in 1986, Ph. D. candidate. His current research interests include cryptography and information security.

WU Wan-Qing, born in 1981, Ph. D. candidate. His current research interests include cryptography and information security.

Background

The research activities were accomplished at the Key Laboratory of Aerospace Information security and trusted computing Ministry of Education within School of Computer Science and the research was sponsored by the National Natural Science Foundation of China (Grant Nos. 61303212, 61170080, 61202386, 61332019, U1135004, 91018008), Major State Basic Research Development Program (973 Program) of China (No. 2014CB340600), the Hubei Natural Science Foundation of China (Grant Nos. 2011CDB453 and 2014CFB440).

Advances in quantum computers threaten to break the currently used public key cryptosystems on commutative algebraic structures such as RSA, ECC, and EIGamal. This is because of Shor's quantum algorithms for integer factoring and solving the DLP, the known public-key systems will be insecure when quantum computers become practical, while no quantum algorithms are found to solve certain mathematical intractable problems on non-commutative algebraic structures. Most of experts believe that many public-key cryptosystems on non-commutative algebraic structures have the potential to resist known quantum algorithms attacks. These are some reasons which motivate researchers to develop a new family of cryptosystems that can resist quantum computing attacks and that are more efficient in terms of computation.

Our group mainly undertake the State Key Program of National Natural Science of China "A Survey on Public Key Cryptosystems and Key Technology Based on Quantum Computers Features under the Quantum Computing Environment". So how to study a key agreement protocol based on non-commutative algebraic structures which has the potential to resist quantum algorithms attack is one of the most challenging issues.

In this paper, we showed that the HKKS protocol over an extension of a semigroup of matrices over a Galois field and matrix group ring respectively are insecure in the sense that an attacker, who is able to solve the linear equations with high efficiency in finite fields, is able to break the HKKS scheme. The question, whether there exists groups on which the HKKS protocol is secure, remains open. When studying the HKKS protocol on other groups, the considerations of the previous section must be taken into account. How to use several nonabelian algebraic structures make a public-key cryptosystem which has the potential to resist known quantum algorithms attacks, also remains open.

This research work is based on author's research direction which aimed at designing public key cryptosystems which has the potential to resist quantum algorithms attack. In the past years, the second author engaged in theoretical research on information security and trusted computing and published many impressive papers on computer related scientific journals and conference.