基于特征值的可验证三方安全密钥交换协议

张艳硕[1,2]，王泽豪[3]，王志强[1]，陈辉焱[1]

（1. 北京电子科技学院密码科学与技术系，北京 100070；2. 密码科学技术国家重点实验室，北京 100878；
3. 数据通信科学技术研究所系统安全部，北京 100191）

摘 要：为解决传统密钥交换协议无法进行三方密钥协商，不够灵活且安全性存在缺陷的问题，借助于秘密矩阵特征值，首先提出了一种可以抵御中间人攻击且简单灵活的三方密钥交换方案，但该方案无法对密钥交换的有效性进行验证，即无法防止不被中间人伪造。在此基础上，对秘密矩阵进行重新构建，其中矩阵阶数为大偶数，所有的特征值成对出现，相似于对角阵。基于所提的特殊秘密矩阵，引入验证环节对通信方的合法性进行验证，给出了基于特征值的可验证三方密钥交换协议。该协议既解决了三方密钥交换的问题，又可对身份合法性进行验证，证明基于特征值进行三方密钥交换协议设计是可行的，最终设计的协议兼具安全性和高效性。

关键词：密钥交换；三方；特征值；中间人攻击；矩阵

中图分类号：TN911.7

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2019233

Verifiable three-party secure key exchange protocol based on eigenvalue

ZHANG Yanshuo[1,2], WANG Zehao[3], WANG Zhiqiang[1], CHEN Huiyan[1]

1. Department of Cryptology Science and Technology, Beijing Electronic Science & Technology Institute, Beijing 100070, China
2. State Key Laboratory of Cryptology, Beijing 100878, China
3. Department of System Security, Data Communication Science and Technology Research Institute , Beijing 100191, China

Abstract: In order to solve the problem that the traditional key exchange protocol, which was not flexible enough and flawed in security, cannot provide the function of three-party key negotiation,firstly, a simple and flexible three-party key exchange scheme that can resist man-in-the-middle attacks was proposed with the help of secret matrix eigenvalues. However, the validity of key exchange cannot be verified by the scheme, and counterfeiting by middlemen can't be prevented. Then based on it, the secret matrix was reconstructed, where the matrix order was a large even number, and all the eigenvalues appeared in pairs, similar to the diagonal matrix. Based on the special secret matrix, the verification part which can be used to verify the legitimacy of the communication party was introduced to the scheme, and the verifiable three-party key exchange protocol based on the eigenvalue was given. The protocol not only solved the problem of three-party key exchange, but also verified identity legitimacy. It is proved that it's feasible to design a three-party key exchange protocol by the eigenvalue. The final protocol is both secure and efficient.

Key words: key exchange, three party, eigenvalue, man-in-the-middle attack, matrix

收稿日期：2019–06–12；**修回日期**：2019–10–10

基金项目：中国民航信息技术科研基金资助项目（No.CAAC-ITRB-201705）；信息网络安全公安部重点实验室开放基金资助项目（No.C17608）；中央高校基本科研业务费项目（No.328201902）

Foundation Items: China Civil Aviation Information Technology Research Base Funded Project (No.CAAC-ITRB-201705), The Opening Project of Key Lab of Information Network Security of Ministry of Public Security (No.C17608), Fundamental Research Funds for the Central Universities (No.328201902)

1 引言

密钥交换协议是重要的密码机制。利用密钥交换协议，通信双方可以通过一个公开的不安全的信道产生一个秘密的会话密钥，以实现秘密性和数据的完整性。密钥交换协议有着丰富而广泛的实际应用。如 TCP/IP 中，IPSec 安全协议套件中的因特网密钥交换（IKE, Internet key exchange）协议通过建立安全通道、协商安全联盟的方式，建立经过认证的密钥材料[1]。在 Web 安全中，针对面向上传下发和登录过程的安全防护，应用了以 DH（Diffie-Hellman）密钥交换为基础的加密，来代替全面部署安全套接层（SSL, secure sockets layer）的方案[2]。

基于三方的口令认证密钥交换（3PAKE, three-party password authenticated key exchange）允许不安全信道上的 2 个用户协商安全会话密钥，并通过认证服务器的帮助建立安全信道，以保护其后续通信[3]。现阶段，已有多种不同思路用于设计三方密钥交换协议，如基于混淆设计的三方密钥交换协议[4-5]、基于格的三方密钥交换协议[6]、强三方安全模型下的密钥交换协议[7]和基于口令的三方密钥交换协议[8]等。但许多已提出的协议又被证明存在不同的安全隐患，如 Yoon 等[9]指出，Wang 等[5]提出的协议易受消息修改攻击。Zhao 等[10]证明，使用扩展 Chebyshev 混沌映射的匿名认证协议易受特权攻击和线下密码猜测攻击。模幂运算和对称密钥密码系统的 3PAKE 协议[11-12]也被证明存在计算成本高、不实用的缺陷。

因此，本文基于特征值方法，构造了一个安全高效的可验证三方密钥交换协议，并给出密钥规模和相关参数。与经典 DH 协议以及 3 个不同构造的三方密钥交换协议[6-8]对比后发现，本文所设计的协议具有良好的安全性和高效性，并且给出了基于特征值的设计多方安全密钥交换协议的新方法和新思路。

2 经典密钥交换协议

2.1 DH 密钥交换协议

DH 密钥交换的思想于 1976 年在公钥密码学文章《New directions in cryptography》[13]中提出。通信双方 Alice 和 Bob 首先协商一个大素数 n 和 g，其中 g 为 n 的本原元。n 和 g 不必是秘密的，即他们可以在不安全的途径中进行协商，甚至在一组用户中公用。n 和 g 的选取对安全性有着极大影响。对 n 的要求是，n 必须是一个大素数，且 $\frac{n-1}{2}$ 也必须为素数。这是因为系统的安全性依赖于与 n 长度相同的数的分解难度。g 虽然不必是素数，且所有模为 n 的本原元 g 都可以被选择，但 g 必须能产生一个大的模 n 的乘法组子群。

DH 密钥交换过程，Alice 选择秘密的 X_{A}，计算公开的 Y_{A}，$Y_{\mathrm{A}}=g^{X_{\mathrm{A}}} \bmod q$。Bob 选择秘密的 X_{B}，计算公开的 Y_{B}，$Y_{\mathrm{B}}=g^{X_{\mathrm{B}}} \bmod q$。Alice 把 Y_{A} 发送给 Bob，Bob 把 Y_{B} 发送给 Alice。最后，Alice 和 Bob 协商出的会话密钥为

$$K=Y_{\mathrm{B}}^{X_{\mathrm{A}}}=Y_{\mathrm{A}}^{X_{\mathrm{B}}}=g^{X_{\mathrm{A}}X_{\mathrm{B}}} \bmod q$$

DH 密钥交换将离散对数问题作为困难问题，是最经典的密钥交换协议，可以抵抗公开信道的抗窃听攻击。

2.2 可认证的密钥交换协议

传统的 DH 密钥交换协议无法抵抗中间人攻击。中间人攻击的原理在于，通信双方 Alice 和 Bob 都与中间人用 DH 算法协商密钥，然后分别用协商好的密钥 K_{A} 和 K_{B} 进行通信。中间人在通信双方之间传递信息，这样，通信双方就在不知不觉间泄露了通信内容。

为了抵抗中间人攻击的风险，发展出许多可认证的密钥交换协议[14]，其中最经典的 2 种为 MTI（Matsumoto, Takashima, Imai）密钥协商和 STS（station to station）密钥协商。MTI 密钥协商[15]能够在 2 条消息中产生带有抵抗中间人攻击的隐式密钥认证的共享密钥。STS 密钥协商[16]是对 DH 密钥协商的三步交换变体，允许在双方之间建立一个共享密钥，并带有相互实体认证和相互显示密钥认证。STS 密钥交换协议可以起到抵抗中间人攻击的作用，使通信双方可以确信在网络中只有合法的用户可以计算出密钥。

MTI 密钥交换无法提供实体认证，也不能进行密钥确认，因此，其只能用于被动攻击情景中。STS 密钥交换用于被动攻击和主动攻击的情景中的安全性都没得到证明。这 2 种协议都存在一定的安全缺陷。

3 基于特征值的三方安全密钥交换协议

3.1 特征值简介

特征值定义如下。

定义 1[17] 设 $\boldsymbol{A}$ 是 n 阶矩阵，$\boldsymbol{E}$ 为单位矩阵，如果数 λ 和 n 维非零列向量 $\boldsymbol{x}$ 使式(1)成立，那么，

这样的数 λ 称为矩阵 $\boldsymbol{A}$ 的特征值，非零向量 $\boldsymbol{x}$ 称为 $\boldsymbol{A}$ 的对应于特征值 λ 的特征向量。

$$\boldsymbol{A}\boldsymbol{x}=\lambda\boldsymbol{x} \tag{1}$$

式(1)也可写成

$$(\boldsymbol{A}-\lambda\boldsymbol{E})\boldsymbol{x}=0 \tag{2}$$

式(2)是 n 个未知数 n 个方程的齐次线性方程组。

3.2　三方密钥交换协议

本节方案基于矩阵特征值进行构造，通信三方可以确保只有合法用户才能计算出会话密钥。具体方案如下。

设密钥交换的三方分别为 Alice、Bob 和 Carol。选择一个秘密 n 阶矩阵 $\boldsymbol{A}$。设 $\boldsymbol{A}$ 的特征值 $\lambda_i(1\leqslant i\leqslant n)$ 所对应的特征向量为 $\boldsymbol{p}_i(1\leqslant i\leqslant n)$。具体步骤介绍如下。

Step1　用户 Alice 随机选择 $\boldsymbol{A}$ 的一个特征向量 $\boldsymbol{p}_a$，其中 $1\leqslant a\leqslant n$，将 $\boldsymbol{p}_a$ 传给 Bob 和 Carol。

Step2　用户 Bob 随机选择 $\boldsymbol{A}$ 的一个特征向量 $\boldsymbol{p}_b$，其中 $1\leqslant b\leqslant n$，将 $\boldsymbol{p}_b$ 传给 Alice 和 Carol。

Step3　用户 Carol 随机选择 $\boldsymbol{A}$ 的一个特征向量 $\boldsymbol{p}_c$，其中 $1\leqslant c\leqslant n$，将 $\boldsymbol{p}_c$ 传给 Alice 和 Bob。

Step4　用户 Alice、Bob、Carol 根据式(1)由 $\boldsymbol{p}_a$、$\boldsymbol{p}_b$、$\boldsymbol{p}_c$ 计算 λ_a、λ_b、λ_c，得出会话密钥 $\lambda_a+\lambda_b+\lambda_c$。

对于该密钥交换协议，由于攻击方无法掌握秘密矩阵 $\boldsymbol{A}$，故其无法伪造会话密钥进行常规的中间人攻击。

但是可以证明，如果存在攻击方 C，且 C 掌握秘密矩阵 $\boldsymbol{A}$ 的所有特征向量 $\boldsymbol{p}_i(1\leqslant i\leqslant n)$，那么 C 就可以从中任选 3 个特征向量分别发送给 Alice、Bob 和 Carol。这样 Alice、Bob 和 Carol 等合法用户便会建立起错误的会话密钥，从而该次密钥协商被 C 所破坏。

3.3　可验证的三方密钥交换协议

针对上述安全漏洞，本文借鉴 3.2 节三方用户交换矩阵特征向量的思路，在其基础上，利用矩阵特征值的重根特性，对秘密矩阵的构造进一步限定，构造一个添加了用户身份验证功能的密钥交换协议。

首先，构造一个 $2n$ 阶秘密矩阵 $\boldsymbol{A}$，该矩阵满足如下要求。

1) 所有特征值 $\lambda_i(1\leqslant i\leqslant n)$ 均为二重根，即有 n 个不同的 λ。

2) 矩阵 $\boldsymbol{A}$ 相似于对角阵。

矩阵 $\boldsymbol{A}$ 为以下方案中 3 个合法通信方共同保有的信息，即 $\boldsymbol{A}$ 可被视为密钥。

合法用户共享一个满足上述要求的 $2n$ 阶秘密矩阵 $\boldsymbol{A}$，并设 $\boldsymbol{A}$ 的每个特征值 $\lambda_i(1\leqslant i\leqslant n)$ 所对应的 2 个特征向量为 $\boldsymbol{p}_{i_1}$ 和 $\boldsymbol{p}_{i_2}$ $\left(1\leqslant i\leqslant n\right)$。设通信三方为 Alice、Bob 和 Carol。方案过程介绍如下。

Step1　Alice 随机选择特征向量对 $\boldsymbol{p}_a=\left(\boldsymbol{p}_{i_1},\boldsymbol{p}_{i_2}\right)$，发送 $\boldsymbol{p}_a$ 给 Bob 和 Carol。

Step2　Bob 随机选择特征向量对 $\boldsymbol{p}_b=\left(\boldsymbol{p}_{j_1},\boldsymbol{p}_{j_2}\right)$，发送 $\boldsymbol{p}_b$ 给 Alice 和 Carol。

Step3　Carol 随机选择特征向量对 $\boldsymbol{p}_c=\left(\boldsymbol{p}_{k_1},\boldsymbol{p}_{k_2}\right)$，发送 $\boldsymbol{p}_c$ 给 Alice 和 Bob。

Step4　用户 Alice 收到 $\boldsymbol{p}_b$ 和 $\boldsymbol{p}_c$ 之后，首先进行合法性验证，即判断 $\boldsymbol{p}_b$、$\boldsymbol{p}_c$ 包含的特征向量是否成对。验证通过后，根据式(1)通过秘密矩阵 $\boldsymbol{A}$ 由 $\boldsymbol{p}_a$ 计算出 λ_a，由 $\boldsymbol{p}_b$ 计算出 λ_b，由 $\boldsymbol{p}_c$ 计算出 λ_c，计算会话密钥 $K_{abc}=\lambda_a+\lambda_b+\lambda_c$。

Step5　用户 Bob 收到 $\boldsymbol{p}_a$ 和 $\boldsymbol{p}_c$ 后，首先进行合法性验证，即判断 $\boldsymbol{p}_a$、$\boldsymbol{p}_c$ 包含的特征向量是否成对。验证通过后，根据式(1)通过秘密矩阵 $\boldsymbol{A}$ 由 $\boldsymbol{p}_a$ 计算出 λ_a，由 $\boldsymbol{p}_b$ 计算出 λ_b，由 $\boldsymbol{p}_c$ 计算出 λ_c，计算会话密钥 $K_{abc}=\lambda_a+\lambda_b+\lambda_c$。

Step6　用户 Carol 收到 $\boldsymbol{p}_a$ 和 $\boldsymbol{p}_b$ 之后，首先进行合法性验证，即判断 $\boldsymbol{p}_a$、$\boldsymbol{p}_b$ 包含的特征向量是否成对。验证通过后，根据式(1)通过秘密矩阵 A 由 $\boldsymbol{p}_a$ 计算出 λ_a，由 $\boldsymbol{p}_b$ 计算出 λ_b，由 $\boldsymbol{p}_c$ 计算出 λ_c，计算会话密钥 $K_{abc}=\lambda_a+\lambda_b+\lambda_c$。

4　安全性分析

4.1　矩阵构造与合法性认证

首先，由于 3.3 节的密钥交换协议是基于 3.2 节所述密钥交换协议而构造的，故其可以抵御传统的中间人伪造会话密钥，窃听合法用户通信的攻击。同时，该协议还可以抵御 3.2 节所述的中间人对密钥协商过程的干预，即避免攻击方 C 使 3 个合法通信方误以为自己与对方建立起会话密钥这种安全漏洞。

定理 1　矩阵 $\boldsymbol{A}$ 相似于对角阵的充要条件为，$\boldsymbol{A}$ 有 n 个线性无关的特征向量。

由于选取的 $2n$ 阶秘密矩阵 $\boldsymbol{A}$ 相似于对角阵，由定理 1 可知，$\boldsymbol{A}$ 有 $2n$ 个线性无关的特征向量。又由于所构造的 $\boldsymbol{A}$ 的特征值均为二重，因此 $\boldsymbol{A}$ 的每个

特征值都有 2 个特征向量。

方案的合法性认证正是基于这种秘密矩阵的特殊构造的。通信方在接收到另两方的特征向量对时，验证特征向量是否成对是保证通信方身份是否合法的一个关键步骤。如果出现特征向量不成对的情况，便认为对方身份合法性存疑，认证不通过。

4.2 密钥量计算

为了防止攻击方对秘密矩阵 $\boldsymbol{A}$ 的穷举攻击，需要对密钥量进行估计，即计算 $\boldsymbol{A}$ 有多少种选择。

设方案基于有限域 Z_q，按照 3.3 节的矩阵设计要求，对于同 $2n$ 阶矩阵 $\boldsymbol{A}$ 相似的对角阵 $\boldsymbol{\Lambda}$ 而言，其每个对角元素有 q 种取值，又因为需保证 n 个特征值两两不同，故 $\boldsymbol{\Lambda}$ 所有的特征值组合方案个数 N_c 为

$$N_c = q(q-1)(q-2)\cdots(q-n+1)=\frac{q!}{(q-n)!}$$

其中，$q>n$。因此，可得出 $\boldsymbol{\Lambda}$ 所有的特征值排列方案个数 N_p 为

$$N_p = N_c\frac{(2n)!}{2^n}=\frac{q!}{(q-n)!}\frac{(2n)!}{2^n}$$

又因为 $\boldsymbol{P}$ 为可逆矩阵，有定理 2 成立。

定理 2 若 $\boldsymbol{A}$ 为可逆矩阵，则矩阵乘法 $\boldsymbol{AB}=\boldsymbol{AC}$ 或 $\boldsymbol{BA}=\boldsymbol{CA}$ 满足消去律。

因为方案中 $\boldsymbol{P}$ 为可逆矩阵，因此根据定理 2 有 $\boldsymbol{P\Lambda}_1\boldsymbol{P}^{-1}\neq\boldsymbol{P\Lambda}_2\boldsymbol{P}^{-1}$。这意味着不同的对角阵一定对应着不同的秘密矩阵 $\boldsymbol{A}$。即对于固定的一个 $\boldsymbol{P}$，可以生成 N_p 个不同的 $\boldsymbol{A}$，方案密钥量为 N_p。

4.3 复杂性分析

假设 Alice、Bob 和 Carol 为合法的通信用户，攻击方 C 若要对通信进行破坏，要进行两步攻击，首先需要得到密钥，即矩阵 $\boldsymbol{A}$。根据 4.2 节的密钥量计算，可知 C 掌握正确密钥的概率为 $\frac{1}{N_p}$。

若要伪造其中的一个合法用户发送信息，就需要从全部特征向量中选取 2 个成对的 $(\boldsymbol{p}_{i_1},\boldsymbol{p}_{i_2})$ 发送出去。假设矩阵的阶为 $2n$，则 C 成功的选取到成对特征向量的概率为

$$\frac{n}{\mathrm{C}_{2n}^2}=\frac{1}{2n-1}$$

当 q 的远大于 n 时，C 成功对通信进行破坏的概率为

$$\frac{1}{N_p(2n-1)}=\frac{2^n(q-n)!}{(2n)!q!(2n-1)}<$$

$$\frac{1}{n!}\frac{1}{\left(\frac{q}{2}\right)!}\frac{1}{2n-1}<\frac{1}{n!\left(\frac{q}{2}\right)!}$$

可以看出，攻击成功的复杂度非常高，攻击成功的概率小到几乎可以忽略不计，攻击方对通信进行破坏的概率极低，这意味着攻击方对密钥协商过程进行干预的成功率将非常小，很难通过合法一方的合法性验证。

5 协议性能比较

本节将本文设计的密钥交换协议与传统的 DH 协议、基于格的密钥交换协议[6]、强三方安全模型下的密钥交换协议[7]、基于口令的密钥交换协议[8]进行比较。各类密钥交换协议性能比较如表 1 所示，其中，Type 表示协议类型，Mutu-Auth 表示协议是否提供双向认证的功能，Round 表示协议所需的轮数。

表 1 各类密钥交换协议性能比较

协议	Type	Mutu-Auth	Round/轮
传统的 DH 协议	双方	否	1
文献[6]协议	三方	是	3
文献[7]协议	三方	是	2
文献[8]协议	三方	是	2
本文协议	三方	是	1

从表 1 中可以看出，本文提出的三方交换协议支持双向认证，具有安全性上的优势。在效率方面，本文在基于秘密矩阵的前提下，实现了只需一轮即可达到可验证密钥交换的目的，效率更高。

在本文涉及的密钥量方面，根据 4.2 节的数据和 4.3 节对复杂性的分析可知，密钥量 N_p 可规约为阶乘运算 $n!\left(\frac{q}{2}\right)!$，密钥空间足够大，可以保证协议的安全性。

在计算复杂性方面，密钥交换要保证在基本的多项式时间内无法进行有效攻击。传统的 DH 密钥交换协议基于离散对数问题进行设计，是典型的 NP 问题。文献[6]所提的基于格的密钥交换最终被规约为 SVP（shortest vector problem）问题，是 NP 完全问题。文献[7]的密钥交换被证明为包含密钥确认的认证密钥交换协议（AKC, authenticated key exchange protocol with key confirmation）安全，其

复杂性可阐述为多项式时间内，攻击者成功猜出输出为会话密钥还是随机数的概率可忽略。文献[8]所提的 3PAKE 协议被证明在随机预言机模型下，基于计算 DH 困难性假设是安全的。本文所提方案在 4.3 节中被证明其计算复杂性为阶乘级，这意味着多项式时间内中间人攻击成功的概率可忽略，满足了密钥交换协议的基本设计要求。

6　三方密钥交换协议举例

6.1　基于特征值的三方密钥交换协议举例

设通信三方为 Alice、Bob 和 Carol。在有限域 Z_{11} 上构造秘密矩阵 $\boldsymbol{A}=\begin{pmatrix}8&0&2\\6&2&2\\0&0&10\end{pmatrix}$，可计算得到 $\boldsymbol{A}$ 的 3 个特征值为 λ_1=2，$\lambda_2=8$，$\lambda_3=10$，其对应的特征向量依次为 $\boldsymbol{p}_1=(0,1,0)$，$\boldsymbol{p}_2=(1,1,0)$，$\boldsymbol{p}_3=(1,1,1)$。具体步骤介绍如下。

Step1　用户 Alice 随机选择 $\boldsymbol{A}$ 的一个特征向量 $\boldsymbol{p}_a$=(0,1,0)，将其传给 Bob 和 Carol。

Step2　用户 Bob 随机选择 $\boldsymbol{A}$ 的一个特征向量 $\boldsymbol{p}_b=(1,1,1)$，将其传给 Alice 和 Carol。

Step3　用户 Carol 随机选择 $\boldsymbol{A}$ 的一个特征向量 $\boldsymbol{p}_c=(1,1,0)$，将其传给 Alice 和 Bob。

Step4　用户 Alice、Bob 和 Carol 都根据式(1)，由 $\boldsymbol{p}_a$、$\boldsymbol{p}_b$、$\boldsymbol{p}_c$ 计算得到 λ_a=2，λ_b=10，λ_c=8，得出会话密钥 $K_{ab}=\lambda_a+\lambda_b+\lambda_c$=20。

6.2　基于特征值可验证的三方密钥交换协议举例

为了方便演示且限于篇幅，本文选取秘密矩阵为 4 阶矩阵，但实际应用中需要一个远大于该阶数的矩阵。秘密矩阵的构造方法可以通过先设定特征值和特征向量，再以此倒推出秘密矩阵的方式进行。

按照 3.3 节所述的矩阵构造要求，在有限域 Z_{11} 上构造秘密矩阵为

$$\boldsymbol{A}=\begin{pmatrix}4&0&0&0\\3&4&0&8\\0&0&1&0\\3&0&0&1\end{pmatrix}$$

因为存在可逆矩阵 $\boldsymbol{P}$，使

$$\boldsymbol{PAP}^{-1}=\boldsymbol{\Lambda}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&4&0\\0&0&0&4\end{pmatrix}$$

其中，$\boldsymbol{P}=\begin{pmatrix}0&0&0&1\\1&1&1&1\\1&0&0&0\\1&1&0&1\end{pmatrix}$，可知该矩阵的特征值为二重根 λ_1=1，$\lambda_2=4$，其各自对应的特征向量依次为 $\boldsymbol{p}_1=((0,1,1,1)^{\mathrm{T}},(0,1,0,1)^{\mathrm{T}})$ 和 $\boldsymbol{p}_2=((0,1,0,0)^{\mathrm{T}},(1,1,0,1)^{\mathrm{T}})$。

设通信三方为 Alice、Bob、Carol，方案过程如下。

1) 用户 Alice 随机选取特征向量对 $\boldsymbol{p}_a=((0,1,1,1)^{\mathrm{T}},(0,1,0,1)^{\mathrm{T}})$。

2) 用户 Bob 随机选取特征向量对 $\boldsymbol{p}_b=((0,1,0,0)^{\mathrm{T}},(1,1,0,1)^{\mathrm{T}})$。

3) 用户 Carol 随机选取特征向量对 $\boldsymbol{p}_c=((0,1,0,0)^{\mathrm{T}},(1,1,0,1)^{\mathrm{T}})$。

4) 合法用户在获得另两方发来的特征向量对之后，首先进行合法性验证，即判断特征向量是否成对。验证通过后，根据式(1)由秘密矩阵 $\boldsymbol{A}$ 计算得到 λ_a=1，λ_b=4，λ_c=4。计算会话密钥为

$$K_{abc}=\lambda_a+\lambda_b+\lambda_c=9$$

7　结束语

本文在基于矩阵特征值的思路之上，首先提出一种简单的三方密钥交换协议。该协议可以抵抗中间人攻击，但无法抵御中间人对密钥交换过程的干预。针对这一问题，本文对秘密矩阵进行限制，基于二重特征值提出了一种既可抵御中间人攻击，又可以进行用户合法性认证的三方密钥交换协议。对比分析证明，该协议具有良好的安全性和高效性。同时，该协议每次都可以重新协商新的会话密钥，防止一个密钥多次使用带来的安全隐患，具有很好的灵活性，为三方或多方密钥交换协议设计提供了一种新方法和新思路。

参考文献：

[1] ZHANG W, WANG F Y. The GRE over IPsec VPN research and implementation of combining with the construction scheme of NAT[J]. Journal of Shandong University of Technology, 2017(3): 87-90.

[2] ZAGHAL R, SALAH S, JABALI N. Extending AES with DH key-exchange to enhance VoIP encryption in mobile networks[C]// World Conference on Information Systems and Technologies. IEEE, 2018: 435-462.

[3] LI C T, CHEN C L, LEE C C, et al. A novel three-party password-based authenticated key exchange protocol with user anonymity based on chaotic maps[J]. Soft Computing, 2017(6):1-12.

[4] FARASH M S, ATTARI M A. An efficient and provably secure

three-party password-based authenticated key exchange protocol based on Chebyshev chaotic maps[J]. Nonlinear Dynamics, 2014, 77(1-2): 399-411.

[5] WANG X, ZHAO J. An improved key agreement protocol based on chaos[J]. Communications in Nonlinear Science and Numerical Simulation, 2010, 15(12):4052-4057.

[6] 叶茂, 胡学先, 刘文芬. 基于格的三方口令认证密钥交换协议[J]. 电子与信息学报, 2013, 35(6): 1376-1381.
YE M, HU X X, LIU W F. Password authenticated key exchange protocol in the three party setting based on lattices[J]. Journal of Electronics and Information Technology,2013, 35(6): 1376-1381.

[7] 王元元.三方认证密钥交换协议研究[D].上海: 上海交通大学, 2010.
WANG Y Y. Research on three-party authenticated key exchange protocol [D]. Shanghai: Shanghai Jiao Tong University, 2010.

[8] 林远辉.基于口令的三方认证密钥交换协议研究[D].济南: 山东大学, 2014.
LIN Y H. Research on three-party authentication key exchange protocol based on password[D]. Jinan: Shandong University, 2014.

[9] YOON E J, JEON I S. An efficient and secure Diffie–Hellman key agreement protocol based on Chebyshev chaotic map[J]. Communications in Nonlinear Science and Numerical Simulation, 2011, 16(6):2383-2389.

[10] ZHAO F, GONG P, LI S, et al. Cryptanalysis and improvement of a three-party key agreement protocol using enhanced Chebyshev polynomials[J]. Nonlinear Dynamics, 2013, 74(1-2):419-427.

[11] LIN T H, LEE T F. Secure verifier-based three-party authentication schemes without server public keys for data exchange in telecare medicine information systems[J]. Journal of Medical Systems, 2014, 38(5):30.

[12] LV C, MA M, LI H, et al. An novel three-party authenticated key exchange protocol using one-time key[J]. Journal of Network and Computer Applications, 2013, 36(1):498-503.

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

[14] KODALI R K, NAIKOTI A. ECDH based security model for IoT using ESP8266[C]//International Conference on Control, Instrumentation, Communication and Computational Technologies. IEEE, 2017:629-633.

[15] DING J, ALSAYIGH S, LANCRENON J, et al. Provably secure password authenticated key exchange based on RLWE for the post-quantum world[C]//Cryptographers' Track at the RSA Conference. Springer International Publishing, 2017:183-204.

[16] MATSUMOTO T. On seeking smart public-key distribution systems[J]. IEICE Trans Fundamental, 1986, 69(2): 224-231.

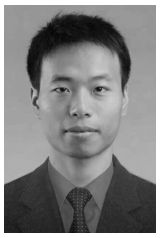
[17] ZHANG L, WU Q, DOMINGO-FERRER J, et al. Round-efficient and sender-unrestricted dynamic group key agreement protocol for secure group communications[J]. IEEE Transactions on Information Forensics & Security, 2017, 10(11):2352-2364.

[18] LENZ J, MUBAYI D. Eigenvalues of non-regular linear quasirandom hypergraphs[J]. Discrete Mathematics, 2017, 340(2):145-153.

[作者简介]

张艳硕（1979– ），男，陕西宝鸡人，博士，北京电子科技学院副教授，主要研究方向为密码理论及其应用。

王泽豪（1994– ），男，河南新乡人，数据通信科学技术研究所助理工程师，主要研究方向为信息隐藏技术及其应用。



王志强（1984– ），男，安徽宿州人，博士，北京电子科技学院讲师，主要研究方向为密码技术及其应用。

陈辉焱（1968– ），男，山东菏泽人，博士，北京电子科技学院研究员级高级工程师，主要研究方向为公钥密码。