基于对称矩阵分解的无线传感网密钥恢复攻击

纪祥敏[1,2]，赵波[1]，刘金会[3]，贾建卫[4]，张焕国[1]，向骕[5]

（1. 武汉大学国家网络安全学院空天信息安全与可信计算教育部重点实验室，湖北 武汉 430072；
2. 福建农林大学计算机与信息学院，福建 福州 350002；3. 陕西师范大学计算机科学学院，陕西 西安 710119；
4. 华为技术有限公司，陕西 西安 710075；5. 长江工程监理咨询有限公司，湖北 武汉 430015）

摘 要：密钥协议是保障无线传感网络（WSN, wireless sensor network）安全性的关键技术之一。Parakh 等基于矩阵分解提出一种传感网密钥协议，然而研究表明该协议存在安全隐患。利用对称矩阵和置换矩阵性质，提出针对该协议的密钥恢复攻击方法。在截获节点行、列向量信息基础上，进行初等变换，构造线性代数攻击算法，求解出等价密钥，计算复杂度为 $O(N^6)$。实验结果表明，在多项式计算复杂度内，该方法可恢复出上述协议的等价密钥，内存开销在可接受范围内。此外，为了抵抗线性代数攻击，通过引入随机扰动矩阵，给出一种密钥协商修正方案，并进行了正确性与安全性分析。

关键词：密钥协议；密钥恢复；矩阵分解；齐次线性方程组求解；无线传感网络

中图分类号：TP391

文献标识码：A

doi: 10.11959/j.issn.1000-436x.2018221

WSN key recovery attack based on symmetric matrix decomposition

JI Xiangmin[1,2], ZHAO Bo[1], LIU Jinhui[3], JIA Jianwei[4], ZHANG Huanguo[1], XIANG Shuang[5]

1. Key Laboratory of Aerospace Information Security and Trusted Computing，Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China
2. College of Computer Information Science, Fujian Agriculture and Forestry University, Fuzhou 350002, China
3. School of Computer Science, Shaanxi Normal University, Xi'an 710119, China
4. Huawei Technologies Co., Ltd., Xi'an 710075, China
5. Yangtze River Engineering Supervision Consulting Co., Ltd., Wuhan 430015, China

Abstract: The key protocol is one of the crucial technologies to ensure the security for wireless sensor network（WSN）. Parakh, et al. proposed a key agreement for WSN based on matrix decomposition. However, the study revealed that the protocol had security risks. A key recovery attack scheme against this protocol was proposed by using the properties of symmetric matrix and permutation matrix. Based on intercepting the row and column vector of the node, elementary transformation was performed to construct a linear algebraic attack algorithm and the equivalent key was obtained. The computational complexity is $O(N^6)$. Experimental results show that the method can recover the equivalent key of the above protocol within the polynomial computational complexity and the memory consumption is within an acceptable range. In addition, an improved scheme for key agreement was proposed to resist the linear algebraic attack by using a random disturbance matrix, and the correctness and security analysis were also carried out.

Key words: key protocol, key recovery, matrix decomposition, homogeneous linear equations solving, wireless sensor network

收稿日期：2017−11−02；**修回日期**：2018−07−22

通信作者：赵波，zhaobo@whu.edu.cn

基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目（No.2014CB340600）；国家高技术研究发展计划（“863”计划）基金资助项目（No.2015AA016002）；国家自然科学基金重点项目资助项目（No.61332039）；中央高校基本科研业务费基金资助项目（No.GK201803061）；中国博士后科学基金面上项目基金资助项目（No.2018M631121）；福建省自然科学基金资助项目（No.2016J01285）

Foundation Items: The National Basic Research Program of China (973 Program)(No.2014CB340600),The National High Technology Research and Development Program of China (863 Program) (No.2015AA016002), The Major Program of National Natural Science Foundation of China (No.61332039), The Fundamental Research Funds for the Central Universities (No.GK201803061), The Postdoctoral Science Foundation Project of China (No.2018M631121), The Natural Science Foundation of Fujian Province (No.2016J01285)

1 引言

当前，无线传感网络发展迅速，广泛应用于商业、军用和航空等领域。由于WSN的无线通信特性，缺乏固定基础设施，容易遭受节点俘获攻击、黑洞攻击等各种攻击，比传统无线网络面临更大的安全挑战与威胁[1-9]。

在诸多安全问题中，密钥管理是WSN安全的基础，密钥管理包括传感器节点密钥的生成、分发和维护。密钥分发协议是密钥管理的重要内容，密钥分发协议旨在2个传感器节点之间分配密钥，实现所有传输消息的认证和加密，从而达到基站数据中继或正常执行分布式计算时安全通信目的。密钥分发协议是保证WSN安全性的关键所在，目前，众多研究者针对WSN密钥分发协议展开了大量研究，并在协议设计、协议安全分析等多个方面取得了较为重要的研究成果[10-20]。

由于传感器设备资源有限，已有的解决方案大部分基于对称密钥加密，在加、解密效率和功耗等方面都具有一定优势。但是，在分发过程中攻击者容易截获共享密钥；同时，随着WSN分布式节点的增加，每个节点存储密钥数量激增，从而导致管理复杂，难以抵御节点脆弱性攻击[16]。

为了克服这些不足，Shim 等[13]设计了基于非对称加密算法的WSN密钥分发协议，旨在提高协议安全性，增加对节点攻击的抵抗力，满足一定的部署灵活性与可扩展性。

文献[21]在传感器上实现了许多非对称加密算法，并声称该方案具有实用性，但是与对称加密算法相比消耗功率更大。文献[22]提出一种混合方案，将整个传感器网络划分为簇，由网络簇头管理各节点通信，实现公钥加密和数据聚合，而单个传感器仅使用对称密钥进行加密。文献[23]使用中央密钥管理服务器建立密钥。文献[24]讨论了基于散列链的密钥分发机制。

文献[25]提出基于排列的多项式方案，通过加大多项式重构困难度，抵御基于Lagrange插值方法攻击，然而该方案无法应对大范围节点共谋攻击。对此，文献[26]给出相应攻击方法，研究表明文献[25]方案无法突破门限，也未能应对大范围节点攻击。基于全同态加密，文献[26]提出了对偶密钥建立方法，在加密环境中实现共享密钥生成，防止相关多项式信息被捕获，在一定程度上解决大范围节点捕获攻击问题。

文献[27]提出一种基于椭圆曲线数字签名算法（ECDSA, elliptic curve digital signature algorithm）的WSN 密钥协议。该方案应用椭圆曲线加密在网关到簇头、簇头到节点之间建立安全通信链路，以ECDSA 进行簇头身份验证，密钥存储在传感器节点内存中，数量不增加，定期更新，防止一般性安全问题。

显然，上述研究在一定程度上解决了密钥分发过程中的一些安全性问题，但仍然存在一定的安全性弱点与计算效率低等问题。因为基于矩阵的非交换结构具有抗攻击潜力和计算效率高优点，所以，近年来，基于矩阵的密钥协议设计和分析成为了研究热点之一[28]。

2015年，Parakh 等[16]基于矩阵分解提出了PK传感网密钥协议，每个传感器预装少量种子信息，通过矩阵行与列的乘法运算产生密钥，应用矩阵交换属性分发密钥。该算法不依赖于数学运算的困难性，计算复杂度为线性。

然而，通过本文研究发现，在弱密钥产生过程中，PK 传感网密钥协议方案容易受到潜在的线性代数攻击。在WSN环境，这种攻击对密钥协议破坏性极大，容易造成共享密钥泄露，从而导致潜在的安全隐患。在线性代数攻击方面，文献[28-29]对具有非交换结构的非对称密码协议进行线性代数攻击，只需多项式时间可以获得某些给定密钥的等价密钥，并给出了理论证明。文献[30]将线性方程组攻击算法应用到一般矩阵群环上的HKKS协议，并给出了一些修正建议。

本文创新之处在于，利用对称矩阵和置换矩阵性质，提出一种针对 PK 传感网密钥协议的密钥恢复攻击方法。在有限域上，通过构造线性代数攻击算法，在可接受的内存开销范围内，求解等价密钥，证明原方案在弱密钥产生过程中存在不安全因素。此外，应用随机产生的扰动矩阵，给出一种修正方案并进行正确性分析，旨在提高原协议密钥协商的安全性。这对于WSN环境密钥交换协议的安全设计与分析的一般理论研究具有重要意义和应用价值。

2 PK传感网密钥协议

本节简要列出涉及密钥协议分析的一些基本数学符号表示含义，如表1所示；同时，给出初等矩阵与初等变换定义，并对PK传感网密钥协议[16]

方案进行概述。

表 1　密钥协议分析基本数学符号表示

符号	释义
p	素数
$\boldsymbol{Z}_P$	有限域$\{0,1,2\cdots,p-1\}$
$\boldsymbol{Z}_P^{n\times n}$	实数域$\boldsymbol{Z}_P$上的$n\times n$矩阵
$\boldsymbol{P}^{\mathrm{Tr}}$	矩阵$\boldsymbol{P}$的转置
$\boldsymbol{K}$	对称矩阵密钥
$\tilde{\boldsymbol{K}}$	矩阵$\boldsymbol{K}$中元素的排列组合
$row_i(\boldsymbol{X})$	矩阵$\boldsymbol{X}$的行分配给i节点
$col_j(\boldsymbol{Y})$	矩阵$\boldsymbol{Y}$的列分配给j节点
$\boldsymbol{X}'$	矩阵$\boldsymbol{X}$被监听到的行向量信息
$\boldsymbol{Y}'$	矩阵$\boldsymbol{Y}$被监听到的列向量信息

定义 1　初等矩阵：在有限域上，初等矩阵定义为由单位矩阵经过一次矩阵初等变换得到的矩阵。

定义 2　初等变换主要有下列 3 种变换，即换法初等变换、倍法初等变换及消法初等变换，具体如下。

1) 换法初等变换：交换矩阵中任意两行的位置。

2) 倍法初等变换：以一非零数乘矩阵的某一行（列）。

3) 消法初等变换：将矩阵某一行（列）的k倍加到另一行（列）上。

以上 3 种初等变换统称为初等行（列）变换。

换法初等变换对应的初等矩阵如式(1)所示，称为换法变换矩阵。

$$\boldsymbol{P}_{ij}=\begin{pmatrix}1&&&&&&&&\\&\ddots&&&&&&&\\&&1&&&&&&\\&&&0&\cdots&1&&&\\&&&\vdots&\ddots&&&&\\&&&1&\cdots&0&&&\\&&&&&&1&&\\&&&&&&&\ddots&\\&&&&&&&&1\end{pmatrix}\tag{1}$$

一次换法变换矩阵具有如式(2)所示的性质。

$$\boldsymbol{P}_{ij}=\boldsymbol{P}_{ij}^{\mathrm{Tr}}=\boldsymbol{P}_{ij}^{-1}\tag{2}$$

多次换法矩阵的乘积是一个 0-1 矩阵。

针对计算资源受限的 WSN 环境，Parakh 等[16]提出 PK 传感网密钥协议。该方案在传感器上预存少量部署信息，经配置后生成会话密钥，在通信范围内可与相邻传感器交换密钥[16]。具体算法描述如下。

假设域内有 N 个随机部署的传感器，算法基于矩阵分解，以大素数 p 进行模运算。算法包含预部署阶段与密钥协商阶段。

预部署阶段主要涉及对称矩阵分解，由基站执行以下预部署计算。

1) 从 $\boldsymbol{Z}_p$ 内选择随机数构造 $n\times n$ 对称矩阵 $\boldsymbol{K}$。

2) 找到 2 个矩阵 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$，使 $\boldsymbol{XY}=\boldsymbol{K}$。

3) 将矩阵 $\boldsymbol{X}$ 的第 r 行和矩阵 $\boldsymbol{Y}$ 的第 r 列分配给各个传感器节点。假如节点 i 接收到矩阵 $\boldsymbol{X}$ 的第 r 行，那么同时也将接收矩阵 $\boldsymbol{Y}$ 的第 r 列。r 是从[1,q]之间以相等概率选择的随机数。矩阵 $\boldsymbol{X}$ 的第 r 行与矩阵 $\boldsymbol{Y}$ 的第 r 列图形表示如图 1 所示[16]。

图 1　矩阵 $\boldsymbol{X}$ 的第 r 行与矩阵 $\boldsymbol{Y}$ 的第 r 列图形表示

每个传感器按矩阵 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$ 的行−列对加载之后，找到相邻节点；当 2 个节点 i 与 j 希望约定密钥，按如下方式进行协商。

节点 i 与 j 彼此互换矩阵 $\boldsymbol{Y}$ 的列，并分别计算密钥[16]。

节点 i 计算：$\boldsymbol{K}_{ij}=row_i(\boldsymbol{X})col_j(\boldsymbol{Y})$

节点 j 计算：$\boldsymbol{K}_{ji}=row_j(\boldsymbol{X})col_i(\boldsymbol{Y})$

其中，$row_i(\boldsymbol{X})$ 表示矩阵 $\boldsymbol{X}$ 的某一行存储在 i 节点，$col_j(\boldsymbol{Y})$ 表示矩阵 $\boldsymbol{Y}$ 的某一列分配给 j 节点[16]。因为矩阵 $\boldsymbol{K}$ 是对称矩阵，所以 $\boldsymbol{K}_{ij}$=$\boldsymbol{K}_{ji}$。

3　密钥恢复攻击

3.1　密钥恢复攻击总体框架

本文研究发现，PK 传感网密钥协议在弱密钥产生过程中存在安全隐患，容易受到潜在的线性代数攻击，泄露共享密钥。为此，本文针对该协议提出一种密钥恢复攻击方法，面向弱密钥生成过程，利用对称矩阵和置换矩阵性质，通过线性代数攻击方法求解共享密钥 $\boldsymbol{K}$。密钥恢复攻击总体框架如图 2 所示。

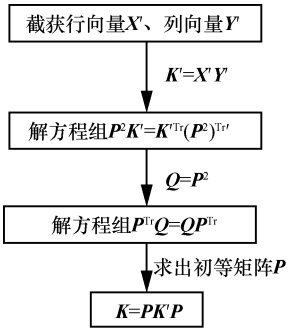

图 2 密钥恢复攻击的总体框架

密钥恢复攻击主要包括 4 个步骤。

步骤 1 截获以明文形式传输的矩阵 $\boldsymbol{X}$ 的行向量信息 $\boldsymbol{X}'$ 与矩阵 $\boldsymbol{Y}$ 的列向量信息 $\boldsymbol{Y}'$，并将二者进行乘法运算得到特殊矩阵 $\boldsymbol{K}'$，即 $\boldsymbol{K}'=\boldsymbol{X}'\boldsymbol{Y}'$。

步骤 2 构造关于未知矩阵 $\boldsymbol{P}^2$ 的齐次线性方程组 $\boldsymbol{Q}_1\boldsymbol{P}_1\boldsymbol{K}'\boldsymbol{Q}_1\boldsymbol{P}_1=\boldsymbol{P}^2\boldsymbol{K}'\boldsymbol{P}^2$，至少可以求出一个解 $\boldsymbol{P}^2=\boldsymbol{Q}_1\boldsymbol{P}_1$，由此推导出一个初等基矩阵 $\boldsymbol{Q}=\boldsymbol{P}^2$。

步骤 3 以步骤 2 结果为基础，构造齐次线性方程组 $\begin{cases}\boldsymbol{P}=\boldsymbol{P}^{\mathrm{Tr}}\boldsymbol{Q}\\ \boldsymbol{P}=\boldsymbol{Q}\boldsymbol{P}^{\mathrm{Tr}}\end{cases}$，求出初等矩阵 $\boldsymbol{P}$。

步骤 4 求解出共享密钥对称矩阵 $\boldsymbol{K}=\boldsymbol{P}\boldsymbol{K}'\boldsymbol{P}$。

由于矩阵 $\boldsymbol{Y}$ 的列向量以明文形式传输，窃听者可以截获这些列向量信息；同时，矩阵 $\boldsymbol{X}$ 的行向量也是明文传输，窃听者同样也可以截获行向量信息。对于 N 个不同节点，在信息传输过程中，窃听者能够分别监听到 N 个矩阵 $\boldsymbol{X}$ 的行信息与矩阵 $\boldsymbol{Y}$ 的列信息，将其记为

$$\boldsymbol{Y}'=\left[\boldsymbol{Y}_1,\boldsymbol{Y}_2,\cdots,\boldsymbol{Y}_N\right]$$
$$\boldsymbol{X}'=\left[\boldsymbol{X}_1,\boldsymbol{X}_2,\cdots,\boldsymbol{X}_N\right]^{\mathrm{Tr}}$$

则令 $\boldsymbol{K}'=\boldsymbol{X}'\boldsymbol{Y}'$。其中，Tr 表示矩阵转置，$\boldsymbol{K}'$ 为特殊矩阵。

因为当分配行和列时，节点 i 接收到矩阵 $\boldsymbol{X}$ 的第 r 行，同时也接收矩阵 $\boldsymbol{Y}$ 的第 r 列，所以将矩阵 $\boldsymbol{Y}'$ 进行多次列变换可以转化为矩阵 $\boldsymbol{Y}$；同理，将矩阵 $\boldsymbol{X}'$ 进行若干行变换，可以得到矩阵 $\boldsymbol{X}$。矩阵变换的数学关系式表示为

$$\begin{aligned}\boldsymbol{X}&=\boldsymbol{P}\boldsymbol{X}'\\ \boldsymbol{Y}&=\boldsymbol{Y}'\boldsymbol{P}\end{aligned}\tag{3}$$

其中，矩阵 $\boldsymbol{P}$ 中的元素为 0 或 1，并且矩阵 $\boldsymbol{P}$ 是多次换法变换矩阵乘积。

性质 1 $\boldsymbol{P}^{-1}=\boldsymbol{P}^{\mathrm{Tr}}$

证明 矩阵 $\boldsymbol{P}$ 是多个一次换法变换矩阵乘积，不妨令

$$\boldsymbol{P}=\boldsymbol{P}_1\boldsymbol{P}_2\cdots\boldsymbol{P}_t$$

其中，$t>1$。因为

$$\boldsymbol{P}^{-1}=\boldsymbol{P}_t^{-1}\cdots\boldsymbol{P}_2^{-1}\boldsymbol{P}_1^{-1}=\boldsymbol{P}_t^{\mathrm{Tr}}\cdots\boldsymbol{P}_2^{\mathrm{Tr}}\boldsymbol{P}_1^{\mathrm{Tr}}$$

因此，满足如下关系式

$$\boldsymbol{P}^{-1}=\boldsymbol{P}^{\mathrm{Tr}}$$

证毕。

根据性质 1，可得

$$\boldsymbol{K}=\boldsymbol{X}\boldsymbol{Y}=\boldsymbol{P}\boldsymbol{X}'\boldsymbol{Y}'\boldsymbol{P}=\boldsymbol{P}\boldsymbol{K}'\boldsymbol{P}=\boldsymbol{P}^{\mathrm{Tr}}\boldsymbol{K}'^{\mathrm{Tr}}\boldsymbol{P}^{\mathrm{Tr}}$$

进而存在

$$\boldsymbol{P}\boldsymbol{K}'\boldsymbol{P}=\boldsymbol{P}^{\mathrm{Tr}}\boldsymbol{K}'^{\mathrm{Tr}}\boldsymbol{P}^{\mathrm{Tr}}$$

因此，可得

$$\boldsymbol{P}^2\boldsymbol{K}'\boldsymbol{P}^2=\boldsymbol{K}'^{\mathrm{Tr}}$$

根据有限域上矩阵的初等变换矩阵，可以得到一个唯一的等式关系，如式(4)所示。

$$\begin{cases}\boldsymbol{P}_1\boldsymbol{K}'\boldsymbol{Q}_1=\begin{pmatrix}\boldsymbol{I}_r & 0\\ 0 & 0\end{pmatrix}\\ \boldsymbol{Q}_1^{\mathrm{Tr}}\boldsymbol{K}'^{\mathrm{Tr}}\boldsymbol{P}_1^{\mathrm{Tr}}=\begin{pmatrix}\boldsymbol{I}_r & 0\\ 0 & 0\end{pmatrix}\end{cases}\tag{4}$$

其中，$\boldsymbol{Q}_1$ 为初等变换矩阵。

因此，可以得到齐次线性方程组，如式(5)所示。

$$\boldsymbol{Q}_1\boldsymbol{P}_1\boldsymbol{K}'\boldsymbol{Q}_1\boldsymbol{P}_1=\boldsymbol{P}^2\boldsymbol{K}'\boldsymbol{P}^2\tag{5}$$

因此，式(5)是关于未知矩阵 $\boldsymbol{P}^2$ 具有 N^2 个方程、N^2 个变量的齐次线性方程组。将一个矩阵的左右两端通过相同的变换转化为该矩阵，假设这个矩阵不进行任何初等变换，易知，该齐次线性方程组至少有一个解 $\boldsymbol{P}^2=\boldsymbol{Q}_1\boldsymbol{P}_1$。

命题 1 在计算复杂度 $O((N^2)^3)$情况下，至少可以求出齐次线性方程组式(5)的一个解 $\boldsymbol{P}^2$。

证明 若存在另外一个解 $\tilde{\boldsymbol{P}}^2$，则特殊矩阵 $\boldsymbol{K}'$ 除外，假设

$$\boldsymbol{P}\boldsymbol{K}'\boldsymbol{P}\neq\tilde{\boldsymbol{P}}\boldsymbol{K}'\tilde{\boldsymbol{P}}$$

进而，

$$(\boldsymbol{P}^2)^{\mathrm{Tr}}\boldsymbol{Q}_1\boldsymbol{P}_1\boldsymbol{K}'\boldsymbol{Q}_1\boldsymbol{P}_1(\boldsymbol{P}^2)^{\mathrm{Tr}}\neq(\tilde{\boldsymbol{P}}^2)^{\mathrm{Tr}}\boldsymbol{Q}_1\boldsymbol{P}_1\boldsymbol{K}'\boldsymbol{Q}_1\boldsymbol{P}_1(\tilde{\boldsymbol{P}}^2)^{\mathrm{Tr}}$$

因为

$$(\boldsymbol{P}^2)^{\mathrm{Tr}}\boldsymbol{Q}_1\boldsymbol{P}_1\boldsymbol{K}'\boldsymbol{Q}_1\boldsymbol{P}_1(\boldsymbol{P}^2)^{\mathrm{Tr}}=\boldsymbol{K}'$$
$$(\tilde{\boldsymbol{P}}^2)^{\mathrm{Tr}}\boldsymbol{Q}_1\boldsymbol{P}_1\boldsymbol{K}'\boldsymbol{Q}_1\boldsymbol{P}_1(\tilde{\boldsymbol{P}}^2)^{\mathrm{Tr}}=\boldsymbol{K}'$$

所以，假设不成立。因此，

$$\boldsymbol{P}^2 = \tilde{\boldsymbol{P}}^2 = \boldsymbol{Q}_1\boldsymbol{P}_1$$

证毕。

由于 $\boldsymbol{P}$ 是初等矩阵，通过计算复杂度 $O(N^6)$可以求出矩阵 $\boldsymbol{P}$ 。初等矩阵 $\boldsymbol{P}$ 的求解过程如下。

令 $\boldsymbol{P}^2 = \boldsymbol{Q}$，可以得到一个具有 $2N^2$ 个方程、N^2 个变量的齐次线性方程组，如式(6)所示。

$$\begin{cases} \boldsymbol{P} = \boldsymbol{P}^{\mathrm{Tr}}\boldsymbol{Q} \\ \boldsymbol{P} = \boldsymbol{Q}\boldsymbol{P}^{\mathrm{Tr}} \end{cases} \tag{6}$$

求出矩阵 $\boldsymbol{P}$ 之后，可以求解出对称矩阵密钥 $\boldsymbol{K}$，从而破解了 PK 传感网密钥协议。上述齐次线性方程组式(5)和式(6)至少有一个解，进而有无穷多个解。以下，证明求解上述方程的任意一组满足齐次线性方程组式(5)和式(6)的初等矩阵的解 $\boldsymbol{P}$，都能得到相同的共享密钥 $\boldsymbol{K}$，即

$$\tilde{\boldsymbol{K}} = \tilde{\boldsymbol{P}}\boldsymbol{X}'\boldsymbol{Y}'\tilde{\boldsymbol{P}} = \tilde{\boldsymbol{P}}\boldsymbol{K}'\tilde{\boldsymbol{P}}$$

$\tilde{\boldsymbol{K}}$ 和 $\boldsymbol{K}$ 都是 $\boldsymbol{K}'$ 中元素的排列组合，并且同时满足上述齐次线性方程组式(5)和式(6)。

$\boldsymbol{P}^2 - \tilde{\boldsymbol{P}}^2 = 0$ 为可逆矩阵的概率为 $1-\frac{1}{q}$，从而 $\boldsymbol{K}'$ 为零矩阵的概率为 $1-\frac{1}{q}$。因此，能够以 $1-\frac{1}{q}$ 的概率（当有限域 q 取值足够大，概率 $1-\frac{1}{q}$ 近乎为 1）求出初等矩阵 $\boldsymbol{P}$，从而得到密钥 $\boldsymbol{K}$ 。具体理由如下。

有限域上具有 n 个方程、n 个变量的齐次线性方程组，由于该方程组至少有一个非零解(在方案中，即为私钥)，那么这个齐次线性方程组以近乎为 1 的概率得到，这个齐次线性方程组的秩是 $n-1$。进而，以近乎为 1 的概率得到这个齐次线性方程组的一组基向量，再根据所求解的矩阵是初等矩阵，从而以近乎为 1 的概率得到私钥 $\boldsymbol{K}$ 。具体概率如式(7)所示[27]。

$$\begin{aligned} P &= \frac{q^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}(q^i-1)}{q^{n^2}} \\ &= \left(1-\frac{1}{q}\right)\left(1-\frac{1}{q^2}\right)\cdots\left(1-\frac{1}{q^n}\right) \approx 1-\frac{1}{q} \end{aligned} \tag{7}$$

若上述齐次线性方程组的秩小于 $n-1$，那么本文的攻击方法只能在安全水平小于 80 bit 的情况下才能攻破，否则不能攻破。

3.2　算法描述与有效性分析

针对 PK 传感网密钥协议的密钥恢复攻击形式化描述如算法 1 所示。1)和 2)分别对矩阵 $\boldsymbol{X}$ 的行向量与矩阵 $\boldsymbol{Y}$ 的列向量进行转换，4) 对关于未知矩阵 $\boldsymbol{P}^2$ 具有 N^2 个方程、N^2 个变量的齐次线性方程组式(5)求解运算，7) 求解具有 $2N^2$ 个方程、N^2 个变量的齐次线性方程组式(6)，9)求解出对称矩阵密钥 $\boldsymbol{K}$ 。

算法 1

密钥 $\boldsymbol{K}$ 求解算法

输入

$$[\boldsymbol{Y}_1,\boldsymbol{Y}_2,\cdots,\boldsymbol{Y}_N],[\boldsymbol{X}_1,\boldsymbol{X}_2,\cdots,\boldsymbol{X}_N]$$

输出 $\boldsymbol{K}$

1) $\boldsymbol{Y}' \leftarrow [\boldsymbol{Y}_1,\boldsymbol{Y}_2,\cdots,\boldsymbol{Y}_N]$

2) $\boldsymbol{X}' \leftarrow [\boldsymbol{X}_1,\boldsymbol{X}_2,\cdots,\boldsymbol{X}_N]^{\mathrm{Tr}}$

3) $\boldsymbol{K}' \leftarrow \boldsymbol{X}' \times \boldsymbol{Y}'$

4) 求解齐次线性方程组式(5)为

$$\boldsymbol{Q}_1\boldsymbol{P}_1\boldsymbol{K}'\boldsymbol{Q}_1\boldsymbol{P}_1 = \boldsymbol{P}^2\boldsymbol{K}'\boldsymbol{P}^2$$

5) $\boldsymbol{P}^2 \leftarrow \boldsymbol{Q}_1 \times \boldsymbol{P}_1$

6) $\boldsymbol{Q} \leftarrow \boldsymbol{P}^2$

7) 求解齐次线性方程组(6)为 $\begin{cases} \boldsymbol{P} = \boldsymbol{P}^{\mathrm{Tr}}\boldsymbol{Q} \\ \boldsymbol{P} = \boldsymbol{Q}\boldsymbol{P}^{\mathrm{Tr}} \end{cases}$

8) $\boldsymbol{P} \leftarrow \boldsymbol{P}$

9) $\boldsymbol{K} \leftarrow \boldsymbol{P} \times \boldsymbol{K}' \times \boldsymbol{P}$

10) 返回 $\boldsymbol{K}$

结合上述讨论，对算法 1 进行计算复杂度评估，分析结果如表 2 所示。对于给定链路的密钥攻击恢复操作，算法 1 中 3)涉及到矩阵 $\boldsymbol{X}'$ 的行与矩阵 $\boldsymbol{Y}'$ 的列乘法运算。假定矩阵 $\boldsymbol{X}'$ 的大小为 $N\times m$，矩阵 $\boldsymbol{Y}'$ 的大小为 $m\times N$。密钥计算需 m 次乘法和 $m-1$ 次加法运算。此外，这取决于矩阵 $\boldsymbol{X}'$ 和矩阵 $\boldsymbol{Y}'$ 的大小，反过来，矩阵 $\boldsymbol{X}'$ 和矩阵 $\boldsymbol{Y}'$ 的大小又取决于期望的安全级别。在最坏情况下，矩阵 $\boldsymbol{X}'$ 和矩阵 $\boldsymbol{Y}'$ 的大小为 $N\times N$，进而密钥矩阵 $\boldsymbol{K}'$ 的计算须 N 次乘法和 $N-1$ 次加法运算，其计算复杂度为 $O(N^3)$。4)和 7)分别对关于 N^2 个变量具有 N^2、$2N^2$ 个方程构成的齐次线性方程组求解，其计算复杂度为 $O(N^6)$[28-31]。

表 2　　算法 1 的计算复杂度分析

内容	复杂度	解释
3)	$O(N^3)$	一个矩阵乘法
4)	$O(N^6)$	N^2 个方程、N^2 个变量的齐次线性方程组
7)	$O(N^6)$	$2N^2$ 个方程、N^2 个变量的齐次线性方程组
9)	$O(N^3)$	3 个 N 阶矩阵相乘

由表 2 计算复杂度分析可知，如果忽略小的常数因子，同时矩阵 $\boldsymbol{P}$ 是初等矩阵，算法 1 的总体复杂度为 $O(N^3)+O(N^6)+O(N^6)+O(N^3)\approx O(N^6)$，即按 $O(N^6)$ 计算复杂度，可以完成针对 PK 传感网密钥协议的密钥恢复攻击。

3.3 攻击实例

为了说明对 PK 传感网络密钥协议进行密码分析的步骤，本文给出一个针对 3×3 对称矩阵 $\boldsymbol{K}$ 的攻击实例。根据算法 1，通过线性代数攻击方法计算出初等变换矩阵 $\boldsymbol{P}$，由此求解对称矩阵密钥 $\boldsymbol{K}$。

假设未知信息为

$$\boldsymbol{K}=\begin{pmatrix}2&3&0\\3&1&4\\0&4&2\end{pmatrix},\boldsymbol{X}=\begin{pmatrix}1&0&3\\1&0&0\\2&2&0\end{pmatrix},\boldsymbol{Y}=\begin{pmatrix}3&1&4\\2&1&2\\3&4&2\end{pmatrix}$$

截获信息为

$$\boldsymbol{X}'=\begin{pmatrix}1&0&0\\2&2&0\\1&0&3\end{pmatrix}$$

$$\boldsymbol{Y}'=\begin{pmatrix}4&3&1\\2&2&1\\2&3&4\end{pmatrix}$$

可得

$$\boldsymbol{K}'=\boldsymbol{X}'\boldsymbol{Y}'=\begin{pmatrix}4&3&1\\2&0&4\\0&2&3\end{pmatrix}$$

因为

$$\begin{aligned}&\boldsymbol{K}=\boldsymbol{P}\boldsymbol{K}'\boldsymbol{P}\\&\Rightarrow\boldsymbol{K}^{\mathrm{Tr}}=\boldsymbol{P}^{\mathrm{Tr}}\boldsymbol{K}'^{\mathrm{Tr}}\boldsymbol{P}^{\mathrm{Tr}}=\boldsymbol{P}\boldsymbol{K}'\boldsymbol{P}\\&\Rightarrow\boldsymbol{K}'^{\mathrm{Tr}}(\boldsymbol{P}^{\mathrm{Tr}})^2=\boldsymbol{P}^2\boldsymbol{K}'\end{aligned}$$

所以根据 $\boldsymbol{P}^2\boldsymbol{K}'=\boldsymbol{K}'^{\mathrm{Tr}}(\boldsymbol{P}^{\mathrm{Tr}})^2$，推导出一个初等基矩阵 $\boldsymbol{Q}=\boldsymbol{P}^2$，进而求出初等矩阵 $\boldsymbol{P}$。

$$\boldsymbol{P}^2\begin{pmatrix}4&3&1\\2&0&4\\0&2&3\end{pmatrix}=\begin{pmatrix}4&2&0\\3&0&2\\1&4&3\end{pmatrix}(\boldsymbol{P}^{\mathrm{Tr}})^2$$

$$\Rightarrow\boldsymbol{P}^2=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}$$

$$\Rightarrow\boldsymbol{P}=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}$$

于是求解对称矩阵密钥为

$$\begin{aligned}\boldsymbol{K}&=\boldsymbol{P}\boldsymbol{K}'\boldsymbol{P}\\&=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}\begin{pmatrix}4&3&1\\2&0&4\\0&2&3\end{pmatrix}\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}\\&=\begin{pmatrix}2&3&0\\3&1&4\\0&4&2\end{pmatrix}\end{aligned}$$

4 实验与分析

为了验证算法 1 破解分析 PK 传感网密钥协议的有效性与可行性，分别从时间复杂度与空间复杂度两方面进行实验测试。为此，采用 Java 作为编程语言对算法 1 进行编程实现，具体实验环境：处理器为 AMD A10-4600M，内存 8 GB，操作系统为 Windows 7 （64-Bit）sp1。开发平台为 Eclipse Java EE IDE 的 Mars Release (4.5.0 版本)，Java（TM）SE 运行时环境为 1.7 版本。

密钥矩阵恢复实验流程如图 3 所示，在有限域内，随机产生给定维度对称矩阵密钥 $\boldsymbol{K}$，并将矩阵分解为矩阵 $\boldsymbol{X}$ 与矩阵 $\boldsymbol{Y}$，分别对矩阵 $\boldsymbol{X}$ 的行向量与矩阵 $\boldsymbol{Y}$ 的列向量进行转换，其结果作为输入 $\boldsymbol{X}'$、$\boldsymbol{Y}'$，将二者进行乘法运算，获得特殊矩阵密钥 $\boldsymbol{K}'$，

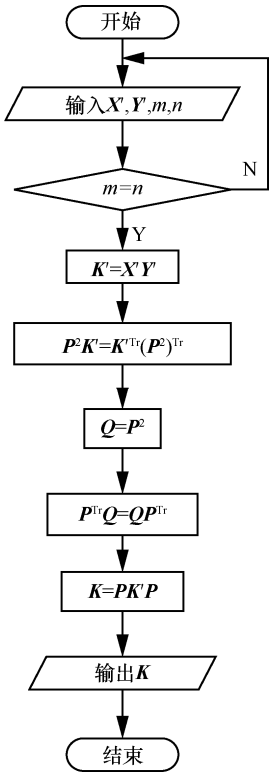

图 3 密钥矩阵恢复流程

由此对 N^2 个方程、N^2 个变量的齐次线性方程组(5)求解运算，获得未知矩阵 $\boldsymbol{P}^2$；进而对 $2N^2$ 个方程、N^2 个变量的齐次线性方程组式(6)进行求解运算，求出初等矩阵 $\boldsymbol{P}$，从而恢复密钥 $\boldsymbol{K}$。按照密钥矩阵恢复实验流程，以 3.3 节攻击实例中的密钥矩阵作为输入对照，先后获得特殊矩阵密钥 $\boldsymbol{K}'$、初等矩阵 $\boldsymbol{P}^2$ 与 $\boldsymbol{P}$ 的结果，最终恢复出密钥 $\boldsymbol{K}$，具体恢复过程结果如表 3 所示。

表 3　　密钥矩阵恢复结果

执行过程	结果
特殊矩阵密钥 $\boldsymbol{K}'$	$\begin{pmatrix}4&3&1\\2&0&4\\0&2&3\end{pmatrix}$
初等矩阵 $\boldsymbol{P}^2$	$\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}$
初等矩阵 $\boldsymbol{P}$	$\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}$
密钥 $\boldsymbol{K}$	$\begin{pmatrix}2&3&0\\3&1&4\\0&4&2\end{pmatrix}$
执行总时间	0.004 s

4.1　时间复杂度测试

为了对算法 1 进行有效的时间复杂度测试，本实验先后分别针对 3×3、4×4、5×5、6×6、10×10 对称矩阵密钥进行恢复攻击实验，根据有限域取值与矩阵维度分别统计密钥矩阵恢复计算复杂度；针对特殊矩阵密钥 $\boldsymbol{K}'$、初等矩阵 $\boldsymbol{P}^2$ 与 $\boldsymbol{P}$、密钥 $\boldsymbol{K}$ 求解运算的程序运行过程，按程序开始时间戳与结束时间戳数据统计当前程序运行时间，每个实验运行 10 次，取其平均值作为该次实验攻击时间。密钥恢复攻击时间结果统计如表 4 所示。

表 4　　算法 1 实验结果

有限域 q	矩阵维度	计算复杂度	攻击时间/s
2^{16}	3	$2^{17.509\,8}$	0.004
2^{16}	4	$2^{20.000\,0}$	0.553
2^{16}	5	$2^{21.931\,5}$	1.383
2^{18}	5	$2^{22.271\,3}$	3.150
2^{20}	5	$2^{22.575\,5}$	3.538
2^{20}	6	$2^{24.156\,3}$	259.035
2^{20}	10	$2^{28.575\,8}$	13 530.850

由表 4 可见，随着有限域值 q 与密钥矩阵维度的提升，实验计算复杂度相应增加，攻击时间随之递增。当有限域值 q 均为 2^{16}，矩阵维度为 3 时，攻击时间仅为 0.004 s；矩阵维度为 5 时，计算复杂度相应增加，攻击时间增达 1.383 s，而有限域值 q 增至 2^{20} 时攻击时间增为 2.5 倍；在矩阵维度提升为 10 时，攻击时间快速增达 13 530.850 s。显然，相对于有限域值 q，密钥矩阵维度的提升对密钥矩阵恢复攻击时间影响更为显著。但是总体而言，在多项式时间计算复杂度[28-31]内，算法 1 均能恢复出密钥矩阵，得出共享密钥。

4.2　空间复杂度测试

在某些密码破解算法中，随着目标数据维度的升高，空间复杂度呈几何指数增长，从而在高维数据破解时，空间复杂度上升到一定阶段对于常规计算机难以承受，这样有可能在针对高维数据分析时不具备可行性。因此，本文从内存开销角度对算法 1 进行空间复杂度测试。

与时间复杂度测试类似，本实验分别针对 3×3、4×4、5×5、6×6、10×10 不同维度对称矩阵密钥恢复攻击过程，分段进行内存开销峰值测试、统计。如图 4 所示，在整个密钥恢复攻击实验过程中，$\boldsymbol{K}'$、$\boldsymbol{P}^2$、$\boldsymbol{P}$、$\boldsymbol{K}$ 求解运算时的内存开销在 160 MB 左右，差异不大。对于 5×5 维度对称矩阵密钥恢复攻击测试时，在 $\boldsymbol{K}'$ 与 $\boldsymbol{K}$ 的求解运算内存开销分别为 150 MB、158 MB，而对齐次线性方程组式(5)和式(6)进行 $\boldsymbol{P}^2$、$\boldsymbol{P}$ 求解运算的内存开销分别为 163 MB、168 MB，相对较大。据图 4 统计分析，对 3×3、4×4、6×6、10×10 维度对称矩阵密钥恢复攻击测试时，也呈现类似特点。显然，针对不同维度对称矩阵密钥恢复攻击过程，内存开销峰值主要集中于齐次线性方程组式(5)和式(6)求解运算，这与表 2 算法 1 计算复杂度分析结果基本吻合。

同时，随着对称矩阵维度的提高，内存开销峰值如式(8)所示，呈现平缓的线性递增过程，并没有呈现几何指数激增趋势。

$$C_{\mathrm{m\_max}} = 4.493 d_{\mathrm{matrix}} + 135 \tag{8}$$

其中，$C_{\mathrm{m\_max}}$ 为内存开销峰值，d_{matrix} 为对称矩阵维度。

可见，在空间复杂度方面，采用算法 1 针对 PK 传感器网络密钥协议进行密钥恢复攻击具有计算可行性。

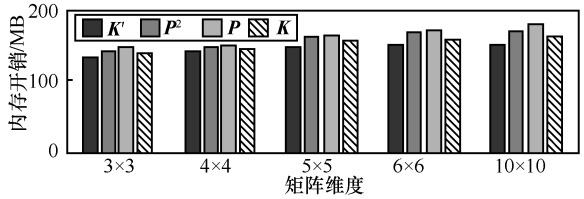

图 4 密钥矩阵恢复内存开销峰值统计

实验结果表明，在多项式计算复杂度内，提出的密钥恢复攻击方法可得到 PK 协议的共享密钥，内存开销在可接受范围内，这说明线性代数攻击对于 PK 传感网密钥协议的弱密钥攻击是可行的。

5 安全性解决方案

为了抵抗上述密钥恢复攻击方法，本文给出一种基于随机扰动矩阵的密钥协商修正方案。该方案在密钥协商过程相关计算以大素数 p 进行模运算，但不需要幂乘运算，只需要一些矩阵乘积运算，易于软件与硬件实现。具体算法描述如下。

5.1 系统建立

对于参数 n、q，$\boldsymbol{F}_q^{n\times n}$ 是一个大于 128 bit 有限域 $\boldsymbol{F}_q$ 上的 n 阶矩阵集合；$\boldsymbol{M}\in\boldsymbol{F}_q^{n\times n}$ 是一个随机均匀选择的 $n\times n$ 初始矩阵，其秩 $\mathrm{rank}(\boldsymbol{M})\leqslant\dfrac{n-1}{2}$；$\boldsymbol{S}=\{\boldsymbol{X}_1,\boldsymbol{X}_2,\cdots,\boldsymbol{X}_N\}$ 是一个具有 N 个元素的可交换矩阵集合，$\boldsymbol{X}_{pri\_i}\in\boldsymbol{F}_q^{n\times n}$，$\boldsymbol{X}_i$ 的秩 $\mathrm{rank}(\boldsymbol{X}_{\mathrm{pri}\_i})\leqslant\dfrac{n-1}{2}$，且矩阵 $\begin{bmatrix}x_1\\x_2\\\vdots\\x_N\end{bmatrix}_{nN\times n}$ 是一个列满秩矩阵；$\boldsymbol{X}_{\mathrm{pri}\_i}$ 作为节点 i 的私钥，连同随机初始矩阵（主私钥）$\boldsymbol{M}$ 一起由节点保密。

5.2 共享密钥协商

在 WSN 有效通信范围内，任意传感器节点 i 与 j 通过邻域探测发现彼此，并且按照图 5 方式协商密钥。

步骤 1 节点 i 利用保密存储的私钥 $\boldsymbol{X}_{\mathrm{pri}\_i}$ 与随机初始矩阵 $\boldsymbol{M}$ 计算节点公钥矩阵 $\boldsymbol{Y}_{\mathrm{pub}\_i}$，如式(9)所示，并把 $\boldsymbol{Y}_{\mathrm{pub}\_i}$ 发送给 j 节点。

$$\boldsymbol{Y}_{\mathrm{pub}\_i}=\boldsymbol{X}_{\mathrm{pri}\_i}\boldsymbol{M} \tag{9}$$

步骤 2 节点 j 收到 $\boldsymbol{Y}_{\mathrm{pub}\_i}$ 后，结合该节点的私钥 $\boldsymbol{X}_{\mathrm{pri}\_j}$ 计算等价密钥 $\boldsymbol{K}_{\mathrm{eqv}\_ji}$，如式(10)所示。

$$\boldsymbol{K}_{\mathrm{eqv}\_ji}=\boldsymbol{X}_{\mathrm{pri}\_j}\boldsymbol{Y}_{\mathrm{pub}\_i} \tag{10}$$

同时，计算该节点的公钥 $\boldsymbol{Y}_{\mathrm{pub}\_j}$，如式(11)所示，并把计算结果发送给 i 节点。

$$\boldsymbol{Y}_{\mathrm{pub}\_j}=\boldsymbol{X}_{\mathrm{pri}\_j}\boldsymbol{M} \tag{11}$$

步骤 3 节点 i 收到节点 j 的公钥 $\boldsymbol{Y}_{\mathrm{pub}\_j}$ 后，结合自身的私钥 $\boldsymbol{X}_{\mathrm{pri}\_i}$ 计算该节点等价密钥，如式(12)所示。

$$\boldsymbol{K}_{\mathrm{eqv}\_ij}=\boldsymbol{X}_{\mathrm{pri}\_i}\boldsymbol{Y}_{\mathrm{pub}\_j} \tag{12}$$

至此，节点 i、j 得到相同的等价密钥。

$$\boldsymbol{K}_{\mathrm{equival}}=\boldsymbol{K}_{\mathrm{eqv}\_ij}=\boldsymbol{K}_{\mathrm{eqv}\_ji} \tag{13}$$

步骤 4 节点 i 随机生成一个 $n\times n$ 扰动矩阵 $\boldsymbol{D}_i$，计算节点 j 的扰动密钥 $\boldsymbol{K}_{\mathrm{d}\_ji}$，如式(14)所示，并把结果 $\boldsymbol{K}_{\mathrm{d}\_ji}$ 发送给节点 j。

$$\boldsymbol{K}_{\mathrm{d}\_ji}=\boldsymbol{D}_i\boldsymbol{K}_{\mathrm{equival}} \tag{14}$$

步骤 5 节点 j 接收扰动密钥 $\boldsymbol{K}_{\mathrm{d}\_ji}$，随机生成一个 $n\times n$ 扰动矩阵 $\boldsymbol{D}_j$，计算共享密钥如式(15)所示。

$$\boldsymbol{K}_{\mathrm{share}\_j}=\boldsymbol{K}_{\mathrm{d}\_ji}\boldsymbol{D}_j \tag{15}$$

同时计算节点 i 的扰动密钥 $\boldsymbol{K}_{\mathrm{d}\_ij}$，如式(16)所示，并把 $\boldsymbol{K}_{\mathrm{d}\_ij}$ 发送给节点 i，并销毁扰动矩阵 $\boldsymbol{D}_j$。

$$\boldsymbol{K}_{\mathrm{d}\_ij}=\boldsymbol{K}_{\mathrm{equival}}\boldsymbol{D}_j \tag{16}$$

步骤 6 节点 i 接 $\boldsymbol{K}_{\mathrm{d}\_ij}$，计算该节点共享密钥

$$\boldsymbol{K}_{\mathrm{share}\_i}=\boldsymbol{D}_i\boldsymbol{K}_{\mathrm{d}\_ij} \tag{17}$$

同时销毁 $\boldsymbol{D}_i$。

至此，节点 i、j 获得共享密钥为

$$\boldsymbol{K}_{\mathrm{share}}=\boldsymbol{K}_{\mathrm{share}\_i}=\boldsymbol{K}_{\mathrm{share}\_j} \tag{18}$$

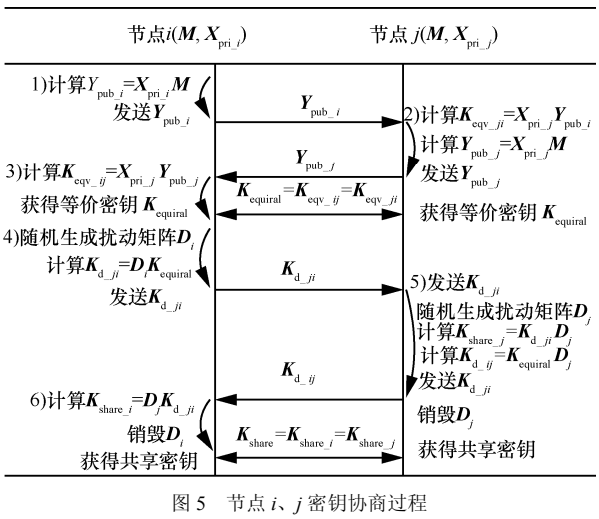

图 5 节点 i、j 密钥协商过程

5.3　正确性证明

基于随机扰动矩阵的密钥协商算法给定之后，我们给出相应的正确性证明，具体如下。

证明　对于 j 节点，它收到 i 节点发送的公钥 $\boldsymbol{Y}_{\text{pub\_}i}$，计算等价密钥

$$\begin{aligned}\boldsymbol{K}_{\text{eqv\_}ji} &= \boldsymbol{X}_{\text{pri\_}j}\boldsymbol{Y}_{\text{pub\_}i}\\ &= \boldsymbol{X}_{\text{pri\_}j}\boldsymbol{X}_{\text{pri\_}i}\boldsymbol{M}\end{aligned}$$

因为 $\boldsymbol{X}_{\text{pri\_}i}$、$\boldsymbol{X}_{\text{pri\_}j}$ 是可交换矩阵

所以 $\boldsymbol{X}_{\text{pri\_}j}\boldsymbol{X}_{\text{pri\_}i} = \boldsymbol{X}_{\text{pri\_}i}\boldsymbol{X}_{\text{pri\_}j}$

于是

$$\begin{aligned}\boldsymbol{X}_{\text{pri\_}j}\boldsymbol{X}_{\text{pri\_}i}\boldsymbol{P} &= \boldsymbol{X}_{\text{pri\_}i}\boldsymbol{X}_{\text{pri\_}j}\boldsymbol{M}\\ &= \boldsymbol{X}_{\text{pri\_}i}\boldsymbol{X}_{\text{pri\_}j}\boldsymbol{M}\\ &= \boldsymbol{X}_{\text{pri\_}i}\boldsymbol{Y}_{\text{pub\_}j}\\ &= \boldsymbol{K}_{\text{eqv\_}ij}\end{aligned}$$

显然，$\boldsymbol{K}_{\text{eqv\_}ij} = \boldsymbol{K}_{\text{eqv\_}ji}$，即节点 i、j 得到了相同的等价密钥 $\boldsymbol{K}_{\text{equival}} = \boldsymbol{K}_{\text{eqv\_}ij} = \boldsymbol{K}_{\text{eqv\_}ji}$。

当 j 节点收到 i 节点发送的 $\boldsymbol{K}_{\text{d\_}ji}$，结合随机生成的 $n\times n$ 扰动矩阵 $\boldsymbol{D}_j$，计算该节点共享密钥

$$\begin{aligned}\boldsymbol{K}_{\text{share\_}j} &= \boldsymbol{K}_{\text{d\_}ji}\boldsymbol{D}_j\\ &= \boldsymbol{D}_i\boldsymbol{K}_{\text{equival}}\boldsymbol{D}_j\\ &= \boldsymbol{D}_i\boldsymbol{K}_{\text{d\_}ij}\\ &= \boldsymbol{K}_{\text{share\_}i}\end{aligned}$$

即节点 i、节点 j 获得共享密钥 $\boldsymbol{K}_{\text{share}} = \boldsymbol{K}_{\text{share\_}i} = \boldsymbol{K}_{\text{share\_}j}$。

证毕。

5.4　安全性分析

假定节点 i、j 的公钥 $\boldsymbol{Y}_{\text{pub\_}i}$、$\boldsymbol{Y}_{\text{pub\_}j}$ 在传输过程中，被攻击者截获了，但矩阵乘法是一个单向函数，且 $\boldsymbol{X}_{\text{pri\_}i}$ 的秩 $\text{rank}(\boldsymbol{X}_{\text{pri\_}i}) \leqslant \dfrac{n-1}{2}$，$\boldsymbol{X}_{\text{pri\_}j}$ 的秩 $\text{rank}(\boldsymbol{X}_{\text{pri\_}j}) \leqslant \dfrac{n-1}{2}$，攻击者无法通过有限节点探测恢复出私钥 $\boldsymbol{X}_{\text{pri\_}i}$、$\boldsymbol{X}_{\text{pri\_}j}$；同时，矩阵 $\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_N \end{bmatrix}_{nN\times n}$ 是一个列满秩矩阵，保证了随机初始矩阵（主私钥）$\boldsymbol{M}$ 不存在等价密钥。

为了确保共享密钥生成过程的安全性，步骤 4、步骤 5 分别引入随机扰动矩阵 $\boldsymbol{D}_i$、$\boldsymbol{D}_j$，对等价密钥矩阵 $\boldsymbol{K}_{\text{equival}}$ 进行扰动，保证 i、j 2 个节点每次协商产生的共享密钥 $\boldsymbol{K}_{\text{share}}$ 均不重复。同时，一旦双方获得共享密钥 $\boldsymbol{K}_{\text{share}}$，分别立即销毁相应的随机扰动矩阵 $\boldsymbol{D}_i$、$\boldsymbol{D}_j$，这样，在等价密钥 $\boldsymbol{K}_{\text{equival}}$ 没有泄露的前提下，攻击者无法恢复出共享密钥 $\boldsymbol{K}_{\text{share}}$。因此，利用本文的线性代数攻击方法针对上述修正方案进行密钥恢复攻击不可行，即攻击者难以恢复出传感器节点用户使用的共享密钥。

6　结束语

针对 PK 协议在弱密钥生成过程中存在安全问题，本文提出一种密钥恢复攻击方法。通过构造齐次线性方程组，求解等价密钥，计算复杂度为 $O(N^6)$。本文采用的攻击方法正确、有效。与现有其他攻击方法相比，线性代数攻击方法新颖，攻击所需的数据量少，同时本文提出的攻击算法直观、易于分析理解，并且攻击计算复杂度较低。此外，为了抵抗本文攻击方法，给出一种基于随机扰动矩阵的密钥协商方案，以解决 PK 协议在 WSN 环境应用中潜在的安全隐患，为构造面向 WSN 计算环境的密钥安全协议提供一种途径。

随着 WSN 快速发展，其信息安全与隐私性受到越来越多关注。由于 WSN 设备计算能力、存储空间和能量有限，如何设计适用于资源受限设备的轻量级安全密钥分发方案是进一步研究的内容。

参考文献：

[1] 张焕国, 韩文报, 来学嘉,等. 网络空间安全综述[J]. 中国科学:信息科学, 2016, 46(2):125-164.
ZHANG H G, HAN W B, LAI X J, et al. Survey on cyberspace security[J]. Science China Information Sciences, 2016, 46(2): 125-164.

[2] 罗军舟, 杨明, 凌振, 等. 网络空间安全体系与关键技术[J]. 中国科学:信息科学, 2016, 46(8):939-968.
LUO J Z, YANG M, LING Z, et al. Architecture and key technologies of cyberspace security[J]. Science China Information Sciences, 2016, 46(8): 939-968.

[3] 陈帅, 钟先信, 巫正中, 等. 无线传感器网络混沌分组密码研究[J]. 中国科学:信息科学, 2009, 39(3):357-362.
CHEN S, ZHONG X X, WU Z Z, et al. Chaos block cipher for wireless sensor network[J]. Science China Information Sciences, 2009, 39(3): 357-362.

[4] 曾建电, 王田, 贾维嘉, 等. 传感云研究综述[J]. 计算机研究与发展, 2017, 54(5):925-939.
ZENG J D, WANG T, JIA W J, et al. A survey on sensor-cloud[J]. Journal of Computer Research and Development, 2017, 54(5): 925-939.

[5] 付帅, 马建峰, 李洪涛,等. 无线传感器网络中匿名的聚合节点选举协议[J]. 通信学报, 2015, 36(2):88-97.
FU S, MA J F, LI H T, et al. Anonymous aggregator election protocol for wireless sensor networks[J]. Journal on Communications, 2015, 36(2):88-97.

[6] ARAFATH M S, KHAN K U R. Opportunistic sensor networks: A survey on privacy and secure routing[C]//International Conference on

Anti-Cyber Crimes. IEEE, 2017:41-46.
[7] HAMZA T, KADDOUM G, MEDDEB A, et al. A survey on intelligent MAC layer jamming attacks and countermeasures in WSN[C]//2016 IEEE 84th Vehicular Technology Conference (VTC-Fall). IEEE, 2016: 1-5.
[8] TEJASWINI B S, BHAT G J. Survey on various attacks and message authentication schemes in WSN[J]. International Journal of Scientific Research Engineering & Technology (IJSRET),2015,4(3): 148-152.
[9] RAYMOND D R, MARCHANY R C, BROWNFIELD M, et al. Effects of denial-of-sleep attacks on wireless sensor network MAC Protocols[J]. IEEE Transactions on Vehicular Technology, 2009, 58(1): 367-380.
[10] GANDINO F, FERRERO R, REBAUDENGO M. A Key distribution scheme for mobile wireless sensor networks: q-s-composite[J]. IEEE Transactions on Information Forensics & Security, 2017, 12(1):34-47.
[11] HAYOUNI H, HAMDI M, KIM T H. A survey on encryption schemes in wireless sensor networks[J]. J Chem Eng Data, 2014, 3(1):91-92.
[12] RAVI K, KHANAI R, PRAVEEN K. Survey on pairing based cryptography for wireless sensor networks[C]//International Conference on Inventive Computation Technologies. IEEE, 2016: 1-4.
[13] SHIM K A. A survey of public-key cryptographic primitives in wireless sensor networks[J]. IEEE Communications Surveys & Tutorials, 2016, 18(1):577-601.
[14] MALEH Y, EZZATI A. A lightweight symmetric cryptography scheme for Identifying compromised node in WSN[J]. Indonesian Journal of Electrical Engineering and Computer Science ,2016, 2(2):431-451.
[15] YAGAN O, MAKOWSKI A M. Wireless sensor networks under the random pairwise key pre-distribution scheme: can resiliency be achieved with small key rings[J]. IEEE/ACM Transactions on Networking, 2016, 24(6):3383-3396.
[16] PARAKH A, KAK S. New key agreement techniques for sensor networks[J]. Infocommunications Journal,2015,7(1):15-21.
[17] SINGH A, AWASTHI A K, SINGH K. A key agreement algorithm based on ECDSA for wireless sensor network[C]//Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics. 2016:143-149.
[18] CHAPHEKAR P P. Survey of key distribution schemes for wireless sensor networks[J]. Computer Science, 2014, 1(1): 1-14.
[19] CHEN C Y, CHAO H. A survey of key distribution in wireless sensor networks[J]. Security and Communication Networks, 2015, 7(12): 2495-2508.
[20] CASOLA V, BENEDICTIS A D, DRAGO A, et al. Analysis and comparison of security protocols in wireless sensor networks[C]// IEEE, Symposium on Reliable Distributed Systems Workshops. 2011: 52-56.
[21] JR M A S, BARRETO P S L M, MARGI C B, et al. A survey on key management mechanisms for distributed wireless sensor networks[J]. Computer Networks, 2010, 54(15): 2591-2612.
[22] RUJ S,SAKURAI K. Secure and privacy preserving hierarchical wireless sensor networks using hybrid key management technique[C]// Global Communications Conference. 2014:402-407.
[23] SALZO S,VILLA S. SPIKE: a novel session key management protocol with time-varying secure cluster formation in wireless sensor networks[C]// Eleventh International Conference on Privacy, Security and Trust. 2013:151-160.
[24] BECHKIT W, CHALLAL Y, BOUNABDALLAH A. A new class of Hash-Chain based key pre-distribution schemes for WSN[J]. Computer Communications, 2013, 36(3):243-255.
[25] 陈燕俐, 杨庚. 适合于无线传感器网络的混合式组密钥管理方案[J]. 通信学报, 2010, 31(11): 56-64.
CHEN Y L, YANG G. Hybird group key management scheme for wireless sensor networks[J]. Journal on Communications, 2010, 31(11): 56-64.
[26] 张永, 温涛, 郭权,等. WSN 中基于全同态加密的对偶密钥建立方案[J]. 通信学报, 2012,33(10):101-109.
ZHONG Y, WEN T, GUO Q, et al. Pair-wise key establishment for wireless sensor networks based on fully homomorphic encryption[J]. Journal on Communications, 2012, 33(10): 101-109.
[27] SINGH A, AWASTHI A K, SINGH K. A key agreement algorithm based on ECDSA for wireless sensor network[C]// Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics. Springer India. 2016: 143-149.
[28] LIU J H, ZHANG H G, JIA J W, et al. Cryptanalysis of an asymmetric cipher protocol using a matrix decomposition problem[J]. Science China Information Sciences, 2016, 46(5): 1-11.
[29] LIU J H, ZHANG H G, JIA J W. A linear algebra attack on the non-commuting cryptography class based on matrix power function[C] //International Conference on Information Security and Cryptology. 2016: 343-354.
[30] 刘金会, 张焕国, 贾建卫, 等. HKKS 密钥交换协议分析[J]. 计算机学报, 2016, 39(3): 516-528.
LIU J H, ZHANG H G, JIA J W, et al. Cryptanalysis of HKKS key exchange protocols[J]. Chinese Journal of Computers, 2016, 39(3): 516-528.
[31] 张焕国, 毛少武, 吴万青, 等. 量子计算复杂性理论综述[J]. 计算机学报, 2016, 39(12): 2403-2428.
ZHANG H G, MAO S W, WU W Q, et al. Overview of quantum computation complexity theory[J]. Chinese Journal of Computers, 2016, 39(12): 2403-2428.

[作者简介]

纪祥敏（1971−），男，福建尤溪人，武汉大学博士生，主要研究方向为云安全、可信计算与信息安全。

赵波（1972−），男，山东青岛人，武汉大学教授、博士生导师，主要研究方向为可信计算、虚拟化安全、嵌入式系统安全等。

刘金会（1989−），女，河南睢县人，博士，陕西师范大学讲师，主要研究方向为抗量子计算密码、数字签名。

贾建卫（1988−），男，河南温县人，博士，华为技术有限公司工程师，主要研究方向为密码学、信息安全。

张焕国（1945−），男，河北元氏人，武汉大学教授、博士生导师，主要研究方向为密码学、信息安全等。

向騊（1984−），男，湖北荆州人，博士，长江工程监理咨询有限公司(湖北)高级工程师，主要研究方向为云安全、信息安全。