Computer Science and Application 计算机科学与应用, 2020, 10(6), 1180-1184
Published Online June 2020 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2020.106122

Hans汉斯

Optimization and Improvement of Key Agreement Based on Generalized Inverse Matrix

Zhenliang Chang, Pan Huang, Xiaogang Yang, Ruitao Lu

Rocket Force Engineering University, Xi'an Shaanxi
Email: 554396337@qq.com

Received: May 26th, 2020; accepted: Jun. 5th, 2020; published: Jun. 12th, 2020

Abstract

The key negotiation scheme based on generalized inverse matrix has important application value in the field of communication. With the leap in computing power in recent years, the security of traditional schemes has declined. In this paper, the security of the traditional scheme is optimized, and the initial cipher matrix is encrypted by setting a random codon before information transmission, which further improves the security of the protocol.

Keywords

Generalized Inverse Matrix, Matrix, Key Agreement

对基于广义逆矩阵密钥协商协议的优化改进

常振良，黄　攀，杨小冈，卢瑞涛

火箭军工程大学，陕西　西安
Email: 554396337@qq.com

收稿日期：2020年5月26日；录用日期：2020年6月5日；发布日期：2020年6月12日

摘　要

基于广义逆矩阵的密钥协商方案在通信领域具有重要的应用价值。近些年随着计算机计算能力的跃升，传统方案的安全性有所下降。本文对传统方案的安全性进行优化，采用在信息传输之前，设置一枚随机密码子的方法，对初始密码矩阵进行加密，使得协议安全性进一步提高。

关键词

广义逆矩阵，矩阵，密钥协商

文章引用: 常振良, 黄攀, 杨小冈, 卢瑞涛. 对基于广义逆矩阵密钥协商协议的优化改进[J]. 计算机科学与应用, 2020, 10(6): 1180-1184. DOI: 10.12677/csa.2020.106122

1. 引言

密钥协商是密码学和密码工程中的关键技术之一，随着信息化进程的加快，特别是在信息安全日益受到重视的今天，计算机网络更需要安全、可靠的密钥协商协议来完成其保密性等安全服务。

文献[1]作者对有限域上广义逆矩阵进行了研究，并将其研究成果应用于密码学，提出了基于广义逆矩阵密钥协商协议，然而该方案并不是安全的，用户在传输密码矩阵的过程中存在泄露公共密钥的风险。文献[2]在文献[1]的基础上增加了密码矩阵传输步骤，使得明传信息过多，泄露公共密钥风险增加，原方案与修改方案的不安全的本质在于密钥协商过程所交换的信息给攻击者提供了足以计算出所协商密钥的数据信息。文献[3]采用了对两个原始密码矩阵分别进行加密操作，加密过程中用到公共矩阵 X，在经过大量数据支撑的情况下，仍然能通过枚举法破解出来。

本文主要解决攻击者仍能通过比较繁琐的方法破解密钥漏洞的问题。文章简要介绍广义逆矩阵的基本知识，以及文献[1] [2]分别提出的密钥协商协议及相应的修改，同时论述文献[3]中对原方案和修改方案进行的改进。最后，针对文献[3]中的缺陷，本文采用在信息传输之前，对初始密码矩阵进行随机加密(即乘上一个随机矩阵)，在信息传输过程中，将得到的明传信息与已知信息进行解密，通过广义逆矩阵将随机密码子消去，得到公共密钥，随机加密的密码子会单独传递，使得安全性进一步提高，避免密钥协商协议的安全漏洞。

2. 广义逆矩阵

广义逆矩阵理论是本世纪中期提出的，这一理论应用广泛，广义逆矩阵的密钥协定方案于 1997 年由 Dawson 和 Chuan-Kuan Wu [1]提出，首次将此理论应用于密码学。1999 年王永传等[2]人修改了此方案。

文献[1]中对有限域上的广义逆矩阵进行了研究，并首次将此理论应用于密码学，提出了基于此理论的一种密钥协同方案，但这一方案必须遵守 $m \neq n$ 。文献[2]对文献[1]提出的方案进行了修正，使其可以遵守任何情况，包括 $m = n$ 。

而文献[2]中定义的广义逆：

记 $M(k,n) = \{A : A为k \times n矩阵\}$，对于 $A \in M(n,k)$，如果存在矩阵 $B \in M(n,k)$，使得

$$ABA = A,\ BAB = B$$

根据定义，A, B 互为 $\{1,2\}$ -逆。对于实数域上的矩阵的广义逆矩阵个数可能是无穷的，而在有限域上只有有限个。

定理 1 [4] {1}-逆的主要应用是关于线性方程组解的表示

设 $A \in C^{m\times n}, B \in C^{p\times q}, W \in C^{m\times q}$，则矩阵方程 $AXB = W$ 相容，当且仅当存在 $A^{(1)}$ 和 $B^{(1)}$，使得 $AA^{(1)}WB^{(1)}B = W$，则通解为

$$X = A^{(1)}WB^{(1)} + Y - A^{(1)}AYBB^{(1)}$$

其中 Y 为任意 $n \times p$ 矩阵，$A^{(1)}$ 和 $B^{(1)}$ 为任意广义逆。

定理 2 [5] 设 $M \in M^{m\times n}, N \in M^{p\times q}$，矩阵方程 $MX = C, XN = D$ 有公共解的充要条件是 $MD = CN$，其公共解的一般形式为

$$X = M^{-}C + DN^{-} - M^{-}MDN^{-} + \left(I - M^{-}M\right)Y\left(I - NN^{-}\right)$$

其中 Y 为任意的 $n \times p$ 矩阵。

推论：对于任意矩阵 $A^{k\times m}$ 和 $B^{m\times n}$，总存在 $X^{m\times k}$，使得下式成立：

$$ABB^{-}XAB = AB$$

由定理 1，得 $X = \left(ABB^{-}\right)^{-} AB\left(AB\right)^{-}$ 为方程的一个解。

3. 文献[1]中的基于有限域上广义逆矩阵的密钥协同方案

假设用户甲与用户乙为了进一步的秘密通信，要通过公用信道建立公共密钥，文献[1]给出如下方案：

1) 甲随机选择一个有限域上的矩阵 $A^{k\times n}$ 和任一个 A 的广义逆矩阵 A^{-}；

2) 甲传送 $A^{-}A$ 给乙；

3) 乙随机选择一个有限域上的矩阵 $B^{m\times n}$ 和任一个 B 的广义逆矩阵 B^{-}；

4) 乙将矩阵 $A^{-}AB$ 和 $A^{-}ABB^{-}$ 传送给甲；

5) 甲计算 $A\left[A^{-}ABB^{-}\right] = ABB^{-}$ 传送给乙；

6) 甲和乙可以生成钥 $K = AB$，甲计算：$A\left[A^{-}AB\right] = AB$，乙计算：$\left[ABB^{-}\right]B = AB$。

这个方案存在的缺陷在于，若第(3)步中，乙用户选择的矩阵若是 $m = n$，则第(4)步中，甲用户得到的 $S = \left[A^{-}AB\right]$、$T = \left[A^{-}ABB^{-}\right]$ 均为 $m \times m$ 矩阵，此时甲用户无法区分 S 和 T，如果甲错选为 S，将 AS 在公共信道上传送给乙，则密钥已公开($AS = AA^{-}AB = AB$)，方案即为不安全的。

4. 文献[2]中的基于广义逆矩阵的密钥协同方案修正

文献[2]方案通过修正步骤，补充了原方案，得到一个较为完善的密钥协同方案。但本方案仍存在缺陷，文献[2]提出的上述方案与原方案并无本质区别，只是将易混淆的信息分开传递。经过在通信协议中进行简单处理后文献[2]所指出的不足可以避免。但他们在安全性方面的共同弱点在于攻击者可以利用信息是信道上的明传信息 $\left[A^{-}ABB^{-}\right]$、$\left[ABB^{-}\right]$、$\left[A^{-}AB\right]$，可以通过计算得到密钥 AB。

方案具体步骤如下：

1) 甲随机选择一个有限域上的矩阵 $A^{k\times n}$ 和任一个 A 的广义逆矩阵 A^{-}；

2) 甲传送 $A^{-}A$ 给乙；

3) 乙随机选择一个有限域上的矩阵 $B^{m\times n}$ 和任一个 B 的广义逆矩阵 B^{-}；

4) 乙将矩 $A^{-}ABB^{-}$ 传送给甲；

5) 甲计算 $A\left[A^{-}ABB^{-}\right] = ABB^{-}$ 传送给乙；

6) 乙传送矩阵 $A^{-}AB$ 给甲；

7) 甲和乙可以生成钥 $K = AB$，甲计算：$A\left[A^{-}AB\right] = AB$，乙计算：$\left[ABB^{-}\right]B = AB$。

由于用户甲和乙之间的信息交换对攻击者来说是可以获取的，所以针对上述方案提出修正后的密钥协商协议，在这里给出一种对其攻击方法的推导：记 $Z = A^{-}A$，由推论知我们道，存在 $X^{m\times m}$ 使得方程：

$$\left(ZBB^{-}\right)X\left(ZB\right) = ZB$$

成立。其中 ZBB^{-} 和 ZB 都是信道上的明传信息，利用定理 1 我们可以求得该方程的一个解：

$$X = \left(ZBB^{-}\right)^{-} ZB\left(ZB\right)^{-}$$

再由 ABB^{-} 也已知，可以解得密钥

$$K = AB = ABB^{-}XZB$$

这是因为：

$$ABB^{-}XZB=\left(AA^{-}A\right)BB^{-}XZB=A\left(A^{-}ABB^{-}\right)XZB=A\left(ZBB^{-}\right)XZB=AZB=AA^{-}B=AB=K$$

我们注意到，其中的$\left[ZBB^{-}\right]$、$\left[ABB^{-}\right]$、$[ZB]$均为信道上的明传信息。由此，对上述方案的密钥攻击就告成功。

5. 文献[3]对文献[2]中修正方案的改进

文献[3]提出上述方案在进行针对性攻击后可以成功破解密钥，所以以上方案并不安全，从而提出改进。设置一个装置满足矩阵方程，做到对公共解，也就是密钥的加密。

方案具体步骤如下：

1) 用户甲取任意一个矩阵$A^{k\times n}$和任一个A的广义逆矩阵A^{-}。在甲中设计一个装置使A满足矩阵方程$AX=C$；

2) 甲传送$A^{-}A$给乙，A和A^{-}由甲秘密保管；

3) 用户乙取任意一个矩阵$B^{n\times m}$和任一个B的广义逆矩阵B^{-}。在甲中设计一个装置使B满足矩阵方程$XB=D$；

4) 乙将矩阵$A^{-}AB$和$A^{-}ABB^{-}$传送给甲，B和B^{-}由乙秘密保管；

5) 甲计算$A\left[A^{-}ABB^{-}\right]=ABB^{-}$传送给乙；

6) 甲计算：$A\left[A^{-}AB\right]=AB$，乙计算：$\left[ABB^{-}\right]B=AB$，则甲和乙就得到了所协商的共享密钥K。

除此之外，使$AX=C$和$XB=D$有公共解的等价条件是$AD=CB$，其中C,D都不公开，这样就无法得到公共解X，只有用户相互协商才能得到X。

其中，攻击者可以从明传信道上获取$\left[A^{-}ABB^{-}\right]$、$\left[ABB^{-}\right]$、$\left[A^{-}AB\right]$，我们知道$A^{-}A$和$BB^{-}$是幂等矩阵，且$r\left(A^{-}A\right)=r\left(A\right)$，$r\left(BB^{-}\right)=r\left(B\right)$。

可见在矩阵方程：$A^{-}AX=A^{-}AB\left(X\in F^{m\times n}\right)$中，当$r\left(A\right)=n$时，方程有唯一解，因此可求出$N$。同理当$r\left(B\right)=n$时，也可求出$A$，这样$A$和$B$已知，即可求出密钥$K$。而当$r\left(A\right)<n$时，矩阵方程的解不唯一，尽管攻击者可通过穷举法搜索来求出K，但难度较大，所以上述方案是比较安全的。

6. 对上述方案的优化改进

上述讨论表明文献[3]在大量数据的支持下，通过枚举法等方法仍旧能够破解其密钥，最主要的问题在于传输信道上的信息并未进行加密，攻击者仍可使用其进行密钥破解，安全性还有一定的缺陷。为避免上述缺陷，设计一个随机算子矩阵，使其对传输信息进行加密，从而使得攻击者无法从窃取的信息中推导出真正的密钥。

对上述方案的优化设计如下，见图 1：

1) 甲随机选择一个有限域上的矩阵$A^{k\times n}$和任一个A的广义逆矩阵A^{-}，并由计算机根据A随机生成一个矩阵$C^{n\times n}$为随机算子；

2) 甲传送$CA^{-}A$给乙；

3) 乙随机选择一个有限域上的矩阵$B^{m\times n}$和任一个B的广义逆矩阵B^{-}，并由计算机根据B随机生成一个矩阵$D^{m\times m}$为随机算子；

4) 乙将计算得到的矩$CA^{-}ABB^{-}D$传送给甲；

5) 甲计算$AC^{-}\left[CA^{-}ABB^{-}\right]D=ABB^{-}D$传送给乙；

6) 乙传送矩阵$CA^{-}AB$给甲；

7) 甲和乙均可以生成密钥 $K = AB$，甲计算：$AC^{-}\left[CA^{-}AB\right] = AB$，乙计算：$\left[ABB^{-}D\right]D^{-}B = AB$。

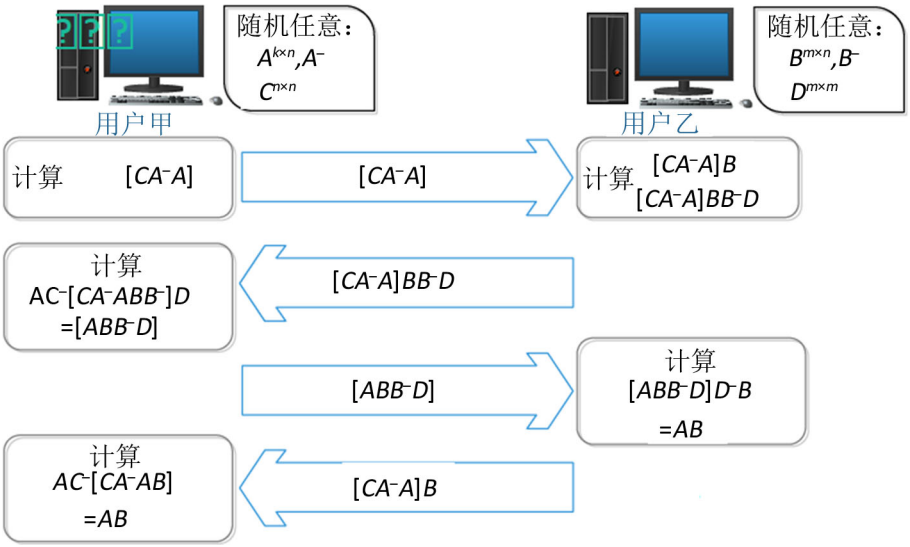

Figure 1. Scheme flow chart
图 1. 方案流程图

7. 总结

本方案对明传信道上的信息进行加密，分别左乘及右乘各自计算机生成的随机算子矩阵 C 和 D，矩阵 C 和 D 并不进行公开或单独传递，仅由计算机记录。最终在进行密钥解密计算时，分别由计算机加入随机密码子，计算得到密钥。而攻击者即使在明传信道上获得信息时，在不知道随机算子的情况下也无法进行强行破解，既可以保证共享密钥的安全、可靠，又可保证明传信道信息的安全，所以本方案是更为安全的。

基金项目

国家自然科学基金(61806209)，陕西省组合与智能导航重点实验室开放基金(SKLIIN-20180103)。

参考文献

[1] Pinch, R.G.E. (1998) Key Agreement Scheme Based on Generalized Inverses of Matrices. *Electronics Letters*, **34**, 652-653. https://doi.org/10.1049/el:19980488

[2] 王永传, 杨义先, 王永忠. 关于“Key agreement scheme based on generalized inverses of matrices”的一点补充[J] .通信保密, 1999(2): 50-51.

[3] 王锦玲. 对基于广义逆矩阵密钥协商协议的改进[J] .通信技术, 2001(7): 99-108.

[4] 马秀珍, 韩静华. 关于几种广义逆矩阵及其应用的探讨[J]. 沈阳航空工业学院学报, 2005, 22(2): 74-75.

[5] 李代高. 矩阵理论及其应用[M] .重庆: 重庆大学出版社, 1989.