计算机科学
COMPUTER SCIENCE

基于海洋水声信道的密钥协商方案

梁珍珍，徐明

引用本文

梁珍珍，徐明. 基于海洋水声信道的密钥协商方案[J]. 计算机科学, 2022, 49(6): 356-362.

LIANG Zhen-zhen, XU Ming. Key Agreement Scheme Based on Ocean Acoustic Channel[J]. Computer Science, 2022, 49(6): 356-362.

相似文章推荐（请使用火狐或 IE 浏览器查看文章）

Similar articles recommended (Please use Firefox or IE to view the article)

基于格的抗量子认证密钥协商协议研究综述

Research on Lattice-based Quantum-resistant Authenticated Key Agreement Protocols:A Survey

计算机科学, 2020, 47(9): 293-303. https://doi.org/10.11896/jsjkx.200400138

面向边缘计算环境的密码技术研究综述

Research on Application of Cryptography Technology for Edge Computing Environment

计算机科学, 2020, 47(11): 10-18. https://doi.org/10.11896/jsjkx.200500003

多重 PKG 环境中高效的身份基认证密钥协商协议

Efficient Identity-based Authenticated Key Agreement Protocol with Multiple Private Key Generators

计算机科学, 2020, 47(11): 68-72. https://doi.org/10.11896/jsjkx.191000008

一种从设备零秘密存储的蓝牙密钥协商方案

Bluetooth Key Agreement Scheme with Zero Secret Storage in Slave Device

计算机科学, 2019, 46(4): 151-157. https://doi.org/10.11896/j.issn.1002-137X.2019.04.024

一个前向安全的基于 RSA 的多服务器的认证协议

Forward-secure RSA-based Multi-server Authentication Protocol

计算机科学, 2019, 46(11A): 409-413.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210400097

基于海洋水声信道的密钥协商方案

梁珍珍[1] 徐 明[1,2]
1 上海海事大学信息工程学院 上海 201306
2 同济大学电子与信息工程学院 上海 201804

摘 要 针对海洋环境不确定性导致水声信道容易受到各种威胁和攻击的问题,提出了一种基于海洋水声信道的密钥协商方案。该方案首先对海洋环境的不确定性进行建模,构造计算噪声、多径、多普勒参数表达式,提出了基于 Rényi 熵的水声信道干扰因子概念;其次,基于 Twisted Edwards 椭圆曲线构造 Hash 函数,进行身份的认证与初始密钥的提取;然后,使用分段初始密钥的典型序列作为初始化种子,生成分段 Toeplitz 矩阵,并对 Toeplitz 矩阵与初始密钥的矩阵乘法采用分块运算生成标签,进行初始密钥的安全传输;最后,初始密钥经再次 Hash,实现了保密增强并生成了最终的安全密钥。通过信息理论证明了所提方案的正确性、健壮性和保密性,并得出了敌手主动攻击成功概率的上界。仿真结果表明,当初始信息量为 50 000 bit 时,敌手主动攻击成功率的上界为 4.3×10^{-23},密钥生成率为 631 bit/s。与现有方案相比,所提方案在密钥生成率和误比特率方面具有明显的优势。

关键词:密钥协商;保密增强;水声信道;主动攻击;Toeplitz 矩阵
中图法分类号 TP309

Key Agreement Scheme Based on Ocean Acoustic Channel

LIANG Zhen-zhen[1] and XU Ming[1,2]
1 College of Information Engineering, Shanghai Maritime University, Shanghai 201306, China
2 College of Electronics and Information Engineering, Tongji University, Shanghai 201804, China

Abstract Aiming at the problem that underwater acoustic channel is vulnerable to various threats and attacks due to the uncertainty of marine environment, a key agreement scheme based on ocean acoustic channel is proposed. Firstly, the uncertainty of marine environment is modeled, and the expressions of calculated noise, multipath and Doppler parameter expressions are constructed, and the concept of interference factor of underwater acoustic channel based on Rényi entropy is proposed. Secondly, a Hash function based on Twisted Edwards elliptic curve equation is constructed for conducting identity authentication and extracting the initial key. Then, the typical sequence of piecewise initial keys is used as initial seed to generate piecewise Toeplitz matrix, and the matrix multiplication of Toeplitz matrix and the initial key are used to generate the label by piecewise operation, and securely transfer the initial key. Finally, the initial key is hashed again for privacy amplification and a final secure key generated. The correctness, robustness and confidentiality of the scheme are proved by the information theory, and the upper bound of the probability of success of the active attack is obtained. Simulation results demonstrate that when the initial information amount is 50 000 bit, the upper bound of the success rate of adversary's active attack is 4.3×10^{-23}, and the key generation rate is 631 bit/s. Compared with existing schemes, the proposed scheme has obvious advantages in key generation rate and bit error rate.

Keywords Key agreement, Privacy amplification, Underwater acoustic channel, Active attack, Toeplitz matrix

1 引言

在国家海洋强国战略背景下,海洋信息的通信安全变得越来越重要。目前,水声通信是水下通信的主要手段,然而,海洋环境干扰以及水声信道的多径效应和多普勒效应,使得信息传输更容易被敌手窃听,甚至发起主动攻击[1-3],因此有必要针对海洋水声信道设计出高度保密的密钥协商方案。

密钥协商是合法双方获取共享密钥的主要手段。Diffie 等[4]首次提出公钥密码交换协议,通信双方经过验证后可以使用不安全的信道进行通信,但协议与双方的身份信息无关,容易受到中间人攻击。Sweeney 等[5]基于 Diffie-Hellman 公钥技术中有限域上的离散对数难题,采用证书与公钥结合的

到稿日期:2021-04-09 返修日期:2021-10-15
基金项目:国家自然科学基金(61202370);中国博士后科学基金(2014M561512)
This work was supported by the National Natural Science Foundation of China(61202370) and China Postdoctoral Science Foundation Project (2014M561512).
通信作者:梁珍珍(1174205915@qq.com)

方式进行密钥协商，可以有效抵御中间人攻击。近年来，诸多学者在密钥协商协议中利用 Hash 函数进行通信双方的身份认证，增强数据传输的安全性[6-8]，但他们使用的 Hash 函数都是基于有限域到有限域的映射，映射范围的局限性会增加敌手成功暴力破解的概率，而且其使用的算法是随机选择算法，可能导致计时攻击[9]，即敌手通过在随机算法的物理实现中获取加密时间、功率消耗等相关信息来破解密钥。此外，已有的密钥协商协议主要基于空中无线通信网络，与海洋水声通信网络有较大的差别，主要表现在水声信道传播的高延迟性以及干扰因素的高不确定性。因此，简单地把基于无线电通信的密钥协商协议直接用于水声信道是不可取的，会导致生成的密钥具有较高的误比特率。为此，目前基于海洋水声信道的密钥协商方案主要利用水声信道的特性进行密钥协商方案的设计，以达到降低误比特率的目的。例如，Murthy 等[10]提出了基于水声信道频率响应(Channel Frequency Response，CFR)的自适应生成密钥协议，该协议利用 Turbo 码对编码过程进行差错控制，降低了误比特率，但是对干扰水声通信的因素考虑得不够全面，这将会导致误比特率结果的误差较大。Liu 等[11]设计了一种基于双扩频码(Dual Spread Spectrum Code，DSSC)的数据帧结构，并使用零序列作为每个有效数据段前后的保护间隔，消除了码间干扰，降低了信息传输的误比特率，但是保护间隔的方法会降低数据传输速率，导致密钥生成率较低。Luo 等[12]提出了多通道密钥生成方案，使通信双方能在多个子信道上提取密钥，在一定程度上提高了密钥的生成速率。Shen 等[13]利用本地试点辅助协议对水声通信进行研究，使用双层补偿集中量化与自适应保护间隔相结合的方法，在提高密钥生成率的同时增强了对邻近敌手窃听的防御能力，但是对防御敌手进行主动攻击的能力较弱。在密钥协商的最新研究中，有学者基于车联网应用场景设计了多车辆与多云计算服务之间的密钥协商协议[14]，利用椭圆曲线与 Rijndael 加密算法进行混合加密，在信息传输过程中对车辆的伪身份与云计算服务的匿名身份进行认证，保证了该协议的安全性，提高了抗主动攻击的能力。Jiang 等[15]提出了基于生物特征识别的密钥协商协议，该协议通过构造 BCH 编码与 Hash 消息认证码，采用基于生物特征分布的参数优化算法选择 BCH 参数，能够有效抵御被动攻击和主动攻击。通过分析可知，目前基于海洋水声信道的密钥协商旨在降低密钥的误比特率，对于敌手的主动攻击考虑得较少。然而，如果敌手对通信信道发起主动攻击，即敌手利用窃听到的信息来猜测密钥或者利用窃听到的已认证信息去替换合法通信双方在信道中的通信内容，则合法通信双方无法判断出通信内容是否被篡改。因此，若信道没有抗主动攻击的能力，则会大大降低水声信道信息通信的安全性。

为了降低敌手主动攻击成功的概率，提高水声通信的安全性，可以通过保密增强协议来压缩密钥，增加敌手对密钥的不确定度[16-18]。为此，本文提出了一种水声信道密钥协商方案，该方案分为两个阶段：密钥提取与保密增强。在密钥提取阶段，利用椭圆曲线构造 Hash 函数生成初始密钥，经纠错后提取出几乎无差错的初始密钥信息；在保密增强阶段，利用 Toeplitz 矩阵规则的对角线结构对 Toeplitz 矩阵乘法采用分块并行运算，并与全域 Hash 函数相结合，提取出用于合法双方通信的最终密钥。

2 预备知识

2.1 保密增强

保密增强，即在敌手 Eve 获得关于密钥部分信息的情况下，利用全域 Hash 函数对密钥进行进一步提取，使合法通信双方 Alice 和 Bob 最终得到几乎完全保密的密钥并用于通信。

定义 1[19] 假设 Alice 和 Bob 共享一个 N bit 的密钥串 S，随机变量 V 表示包含 Eve 知道的关于 S 的所有信息，φ 为 N 位二进制串的所有概率分布集合中的一个子集。设 l 是任意一个正整数，$\varepsilon,\delta>0$，则在非认证信道上存在一个$(N,\varphi,l,\varepsilon,\delta)$保密增强协议且满足以下性质。

(1)正确性和保密性。假设 Eve 是一个知道特定信息 $V=v$ 的敌手，其中 $P_{S|V=v}\in\varphi$，如果合法节点 Alice 和 Bob 存在一个二进制串 S' 满足 $S_A'=S_B'=S'$，并且有 $H(S'|C,V=v)\geqslant l-\varepsilon$ 成立，其中 C 表示信道上所有的通信内容。在这种情况下，我们称保密增强协议是成功的。

(2)健壮性。假设 $P_{S|V=v}\in\varphi$，对于敌手 Eve 的任何一种可能攻击的策略，Alice 和 Bob 在协议的最后都拒绝所协商出的密钥或者保密增强成功的概率至少为 $1-\delta$。

2.2 分段 Toeplitz 矩阵

Toeplitz 矩阵又称对角线常数矩阵，根据其特殊的对角线结构，只要确定 Toeplitz 矩阵的第一行和第一列的元素，就可以构造出完整的 Toeplitz 矩阵[20]。阶数为 $l\times jk$ 的 Toeplitz 矩阵的一般表示形式为：

$$\boldsymbol{T}=\begin{bmatrix} t_0 & t_1 & \cdots & t_{jk-1} \\ t_1 & t_2 & \cdots & t_{jk} \\ \vdots & \vdots & & \vdots \\ t_l & t_{l+1} & \cdots & t_{l+jk-1} \end{bmatrix}$$

在 Toeplitz 矩阵一般定义的基础上提出分段 Toeplitz 矩阵的概念。若称阶数为 $l\times jk$ 的一组矩阵 $\boldsymbol{T}=[\boldsymbol{T}_1\ \ \boldsymbol{T}_2\ \ \cdots\ \boldsymbol{T}_M]$为分段 Toeplitz 矩阵，则满足：

$$t_1=vec(\boldsymbol{T}_1)^{\mathrm{T}}=[t_{11}^{\mathrm{T}}\ \ t_{12}^{\mathrm{T}}\ \ \cdots\ \ t_{1jk}^{\mathrm{T}}]$$

$$t_2=vec(\boldsymbol{T}_2)^{\mathrm{T}}=[t_{21}^{\mathrm{T}}\ \ t_{22}^{\mathrm{T}}\ \ \cdots\ \ t_{2jk}^{\mathrm{T}}]$$

$$\vdots$$

$$t_M=vec(\boldsymbol{T}_M)^{\mathrm{T}}=[t_{M1}^{\mathrm{T}}\ \ t_{M2}^{\mathrm{T}}\ \ \cdots\ \ t_{Mjk}^{\mathrm{T}}]$$

其中，t_{ij} 为矩阵 $\boldsymbol{T}_i$ 的第 j 列。

3 方案设计

本文方案主要包括 3 个部分：海洋水声信道建模、初始密钥提取协议、保密增强协议。在海洋水声信道建模部分，对影响水声通信的海洋噪声、多普勒效应以及多径效应构造计算表达式，并提出干扰因子的概念。在初始密钥提取部分，将干扰因子引入密钥协商的过程中，利用椭圆曲线构造 Hash 函数生成初始密钥。最后，在保密增强部分采用分块的方式对 Toeplitz 矩阵与初始密钥的乘法进行并行运算以生成标签，经过 Hash 函数压缩后，提取出高度安全的密钥。

3.1 海洋水声信道建模

海洋噪声是声场干扰因子的影响因素之一，其主要来源

有海洋湍流、波浪及航船噪声。设某一点接受源与发射源的水平距离为 r，深度为 z_r，表示为 $\Omega(z_r,r)$，则每一个可能的噪声源都会对该点造成影响，因此在点 $\Omega(z_r,r)$ 处的噪声强度可表示为：

$$I(z_r,r)=\sum_p A_p(\theta_s,z_r,r)N(\theta_s) \tag{1}$$

其含义为各噪声源的声线累加。其中，θ_s 为掠射角（单位为 rad），p 为每一条噪声的声线路径，A_p 为单条噪声声线的幅度，$N(\theta_s)$ 为相关函数。

多普勒效应严重影响了水声信道的通信质量，而造成多普勒效应的主要原因是声速梯度的跃层以及海面波浪和湍流的涌动导致收发信号双方处于相对运动状态[1]。其中，多普勒效应对信号传输的频域影响最大，可产生多普勒频移，因此本文将多普勒频移程度作为衡量多普勒效应大小的主要指标。由文献[1]可知，收发两端的相对移动导致的多普勒频移可表示为 $\Delta f=\frac{\Delta v}{c}\cdot f\cdot\cos\phi$，$f$ 是信号传输频率，单位为 Hz；c 为声波传播速度，单位为 m/s。设 $f(c)$ 表示其他相关运动导致的多普勒效应，因此多普勒效应指标为：

$$P_f=\Delta f+f(c) \tag{2}$$

多径效应是信号在传播过程中发生畸变的根本原因，主要是由于通信双方发射信号时产生了不同的掠射角，并在信道中发生了弯曲以及声线发生各种类型的反射造成的。本征声线是能够从声源到达接受点的所有声线，而经不同路径到达接受点的声线所需要的时间是不一样的，因此多径效应会导致严重的时延扩展。设 $s(t)$ 为信源发送的信号，信道增益为 g_i，因此多径效应因子可表示为：

$$R_f=\sum_{i=1}^{N_{ray}}A_i g_i s(t+\Delta t_i) \tag{3}$$

其中，N_{ray} 为总的声波本征声线数，A_i 为第 i 条本征声线的幅度值，Δt_i 为第 i 条本征声线的时延。

根据 Rényi 熵能够量化信息的不确定性这一性质，定义 $H_\alpha(I_f,P_f,R_f)$ 为在噪声、多普勒效应及多径效应共同作用下对水声信道的总干扰度量。联合 Rényi 熵展开公式对总干扰度量进行计算，$H_\alpha(I_f,P_f,R_f)$ 展开式如下：

$$H_\alpha(I_f,P_f,R_f)=H_\alpha(I_f)+H_\alpha(P_f|I_f)+H_\alpha(R_f|P_f,I_f) \tag{4}$$

定义 2 设信源的发送信号为 $s(t)$，在海洋环境距离域 Ω 中不同位置的干扰因子可定义为：

$$L_f(\Omega(z_r,r))\triangleq\frac{(H_\alpha(s_\Omega(t)|H_\alpha(I_f,P_f,R_f|\Omega(z_r,r)))}{H_\alpha(s_\Omega(t))} \tag{5}$$

下文简称为 L_f^r 且 $L_f^r\in(0,1)$。其中，$s_\Omega(t)$ 与 $s(t)$ 的关系为 $s_{D_\Omega}(t)=\sum_p A_p s(t-\Delta t)^{2\pi jvt}$，$\Delta t$ 为信号传播时延。L_f^A，L_f^B 和 L_f^E 分别表示 Alice，Bob 和 Eve 所在位置的干扰因子，且满足 L_f^A 和 L_f^B 大于 L_f^E。

3.2 初始密钥提取协议

密钥提取旨在经双方交流认证后提取出初始密钥信息，并用于保密增强。受椭圆曲线密码学的启发[21]，椭圆曲线域的映射范围广且在同等密钥长度下其破解时间较长，且有限域映射到椭圆曲线是固定多项式时间，也就是说，由椭圆曲线构造到有限域的 Hash 函数为常数操作步骤，能够抵抗计时攻击。另外，在 NISF 的标准中，攻破时间为 MIPS 年时，所需 RSA 密钥的长度为 512，所需椭圆曲线生成密钥的长度为 106；攻破时间为 MIPS 年时，所需 RSA 密钥的长度为 21 000，所需椭圆曲线生成密钥的长度为 600。由此可以看出，椭圆曲线具有高安全性且在保证同等安全程度的情况下所协商的密钥长度较短。因此，本文基于 Twisted Edward 椭圆曲线构造 Hash 函数，以进行初始密钥的提取。Twisted Edwards 椭圆曲线的一般表达式为 $E_{ad}:ax^2+y^2=1+dx^2y^2$，其中，$a$，$d\in\mathbb{R}_q$，$\mathbb{R}_q$ 为 q 阶有限域，q 满足 $q\equiv 2 \bmod 3$ 的大随机素数且 $ad(a-d)\neq 0$。则由 E_{ad} 椭圆曲线域构造用于密钥提取的 Hash 函数 $H(x)$ 为 $H(x)=(f(h_1(x))+f(h_2(x))) \bmod Se$。其中，$Se\in\mathbb{Z}_q^m$ 为合法通信双方 Alice 和 Bob 随机选取的共享秘密整数，$\mathbb{Z}_q^m$ 表示长度为 m 位、阶为 q 的整数集合且满足 $q\equiv 2 \bmod 3$，$f:\mathbb{R}_q\rightarrow E_{ad}(\mathbb{R}_q)$ 表示有限域到椭圆曲线的编码映射：

$$h_1(x):\{0,1\}^{m_1}\rightarrow\{0,1\}^{k_1},\ h_2(x):GF(m_2)\rightarrow GF(k_2)$$

其中，m_1，m_2，k_1，k_2 均为正整数。

初始密钥提取协议的流程图如图 1 所示。假设合法双方 Alice 和 Bob 从中继站接收到的信息 X 和 Y 为双方进行密钥提取的信息源，其中 $X=[x_1,x_2,\cdots,x_n]$，$Y=[y_1,y_2,\cdots,y_n]$。双方接收到信息后首先进行 Hash 函数的认证。首先，Alice 将 $H(x)$ 发送给 Bob，Bob 验证 $h_1(ID_A)=0$，$h_2(ID_B)=0$（ID_A，ID_B 分别为 Alice 和 Bob 的身份标识且对敌手 Eve 保密），若两式同时满足则认为信息是 Alice 发送的，Bob 发送确认信号给 Alice，并将 $[y_1,y_2,\cdots,y_n]$ 代入 $H(x)$ 计算得出结果序列 $[c_1,c_2,\cdots,c_n]$，同时 Alice 将 $[x_1,x_2,\cdots,x_n]$ 代入 $H(x)$ 计算得出字符序列 $[c_1',c_2',\cdots,c_n']$；若两式不能同时满足，则将该信息丢弃。

随后双方对密钥信息进行协商和纠错处理，Alice 将 $[c_1',c_2',\cdots,c_n',ID_A]$ 通过未经认证的信道发送给 Bob，Bob 收到字符串信息后计算最后一个元素 $h_1(ID_A)=0$，若成立则将 c_i 与接收到的 Alice 发送的 c_i'（i=1，2，…，n）字符串进行比较：1）若 $Len(c_i)=Len(c_i')=l$，则直接计算字符串的汉明距离 $d=\sum c_i\oplus c_i'$（$d\geqslant 0$），$Len(*)$ 表示字符串信息的长度，若 $d(c_i,c_i')>0$ 则直接舍弃掉 (c_i,c_i')，否则记录 c_i 的信息；2）若 $Len(c_i)\neq Len(c_i')\neq l$，则长度较小的字符串后缀使用 01 补齐，使 $Len(c_i)=Len(c_i')=l$ 成立后再执行步骤 1）。同理，Bob 将 $[c_1,c_2,\cdots,c_n,ID_B]$ 发送给 Alice，Alice 进行身份验证，计算 $h_2(ID_B)=0$，若成立则进行以上步骤的纠错，否则丢弃。最后，密钥信息经协商纠错后会得到长度为 l 的几乎无差错的密钥序列 $[u_1,u_2,\cdots,u_l]$。

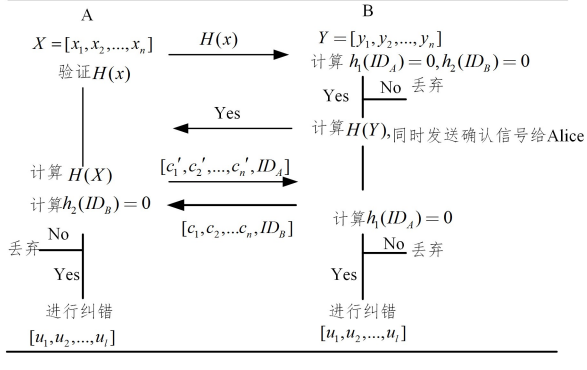

图 1 初始密钥提取协议流程图

Fig. 1 Flow chart of initial key extraction protocol

3.3 保密增强协议

由于本文假设 L_f^A 和 L_f^B 大于 L_f^E，因此会导致部分初始密钥信息被泄露或被敌手进行主动攻击，保密增强可以在降低敌手主动攻击成功概率的情况下从部分保密的初始密钥中提取出高度保密的密钥。在保密增强协议中，全域 Hash 函数可以用于密钥的认证与提取，然而对于密钥的存储往往会消耗大量的存储空间。本文利用 $l\times jk$ 阶 Toeplitz 矩阵进行保密增强协议的设计，由于 Toeplitz 矩阵只需要存储第一行和第一列的元素，因此使用 Toeplitz 矩阵可以提高存储效率，相比普通矩阵可减少$(ljk-l-jk)$个存储单元。不足的是，Toeplitz 矩阵进行密钥压缩是基于硬件来实现关于 Toeplitz 矩阵与密钥的乘法运算，一般情况下 Toeplitz 矩阵在单比特运算操作过程中速度较慢，耗费的时间较长。因此，本文借助 Toeplitz 矩阵有规则的对角线结构，提出使用矩阵乘法分块并行运算，将矩阵乘法分为若干 B 块，使单比特乘法在并行累加器中并行计算，提高计算效率。

图 2 为 Toeplitz 矩阵的工作原理示意图。其中每一个矩阵乘法运算 B 块由 3 个并行累加器组成，每个累加器在有限域上执行 3 位乘法运算。此外，图 2 中黑色实心圆圈表示分段 Toeplitz 矩阵元素，在图 2 中首先把 11×12 阶 Toeplitz 矩阵扩展为 12×18 阶 Toeplitz 矩阵，目的是为了使 B 块乘法运算操作覆盖 Toeplitz 矩阵中的所有元素。通常情况下，长度为 r 的累加器需要 r 个时钟来完成一次操作，则 Toeplitz 矩阵与 l 长的密钥进行单比特乘运算需要 lr 个时钟周期，而本文提出的分若干 B 块进行矩阵乘法运算时需要$\frac{lr}{M\times N}$个时钟周期，相比未分块运算的情况下处理完 l 长的密钥可减少$\left(lr-\frac{lr}{M\times N}\right)$个时钟周期，$r$ 为累加器长度，$M\times N$ 为转换后的等价 B 块操作矩阵的阶数。根据图 2 中的 Toeplitz 矩阵，其等价 B 块矩阵如图 3 所示，等价 B 块矩阵的阶数为 4×5。

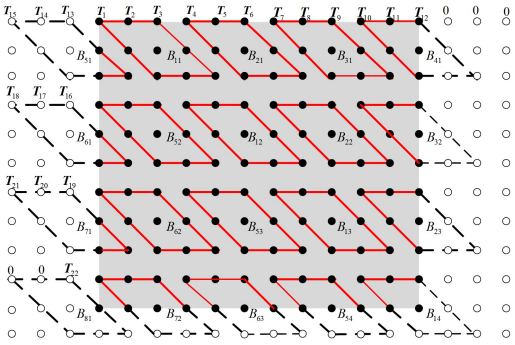

图 2 分段 Toeplitz 矩阵的工作原理示意图

Fig. 2 Diagram of working principle of piecewise Toeplitz matrix

$$\begin{bmatrix} T_1 & T_2 & T_3 & \cdots & T_{11} & T_{12} \\ T_{13} & T_1 & T_2 & \cdots & T_{10} & T_{11} \\ T_{14} & T_{13} & T_1 & \cdots & T_9 & T_{10} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \\ T_{22} & T_{21} & T_{20} & \cdots & T_1 & T_2 \end{bmatrix} \rightarrow \begin{bmatrix} B_{51} & B_{11} & B_{21} & B_{31} & B_{41} \\ B_{61} & B_{52} & B_{12} & B_{22} & B_{32} \\ B_{71} & B_{62} & B_{53} & B_{13} & B_{23} \\ B_{81} & B_{72} & B_{63} & B_{54} & B_{14} \end{bmatrix}$$

图 3 等价 B 块矩阵

Fig. 3 Equivalent B block matrix

在保密增强协议的设计中，将提取出的初始密钥 S 随机分为 $M+1$ 段，取最短的分段作为分段 Toeplitz 矩阵的初始化种子，生成典型序列 $T_S(L,\varepsilon)$，然后与随机序列一起用于构造分段 Toeplitz 矩阵。另外的 M 个分段 $S=[S_1\ \ S_2\ \ \cdots\ S_M]$ 作为保密增强的输入消息，与分段 Toeplitz 矩阵进行矩阵乘法运算后作为消息标签(Tag)，与消息 S 一起发送给 Bob。

算法 1 保密增强协议

输入：$S=[S_1\ \ S_2\ \ \cdots\ S_M]$，$\mathbf{T}=[\mathbf{T}_1\ \ \mathbf{T}_2\ \ \cdots\ \mathbf{T}_M]$

输出：S'

1. for $S_i\neq$null do
2. $\quad Tag_i\leftarrow T_{i(m\times jk)}\,\mathrm{vec}(S_i)_{m\times1}$
3. $\quad Bob\leftarrow(S_i,Tag_i)$
4. $\quad Tag_i'\leftarrow Encode(S_i)$
5. $\quad$if$(Tag_i==Tag_i')$
6. $\quad\quad S_i'\leftarrow h_d(S_i)$
7. $\quad$else then
8. $\quad\quad$discarded
9. end if
10. return $S'=S_1'\,\|\,S_2'\,\|\,S_3'\,\|\cdots\|\,S_l'$
11. end for

在算法 1 描述的保密增强协议中，首先将分段 Toeplitz 矩阵与相应的分段密钥进行矩阵乘法运算，将运算结果作为标签 Tag_i 与相应的分段密钥一起发送给 Bob。Bob 接收到消息标签 Tag_i 后与自身的 Tag_i' 进行比较，若相同则表明该消息是 Alice 发送的，然后利用全域 Hash 函数 $h_d(x)$[19]，$h_d(x)=\sum_{i=0}^{N/l-1}d^i x_i$ 对初始密钥 S 进行最终的提取以完成保密增强，并生成密钥 $S'=[s_1',s_2',\cdots,s_{l'}']$。其中 $N,l>0$，$2^l\geqslant N/l$，$d\in GF(2^l)$。

4 安全性证明

定理 1 已知密钥提取的初始密钥串为 S，且 S 为 XY 函数，$I(S;Z)$表示初始密钥串 S 和 Z 之间的互信息，随机变量 Z 表示 Eve 知道的关于 S 的全部信息，$P_Y(y)$为已知的均匀概率分布，$\lambda>0$，$\varepsilon>0$，则经密钥提取后可得：

$$I(S;Z)\leqslant\lambda n(1-L_f^A)-\lambda\varepsilon-\frac{1}{1-\alpha}\mathrm{lb}\sum_{y\in\varphi}P_Y(y)2^{\eta}$$

$$\eta=(\alpha-1)\mathrm{lb}P_Y(y)+(1-\alpha)H_a(X|Y=y)$$

证明：

$$I(S;Z)=H(S)-H(S|Z)\leqslant Len(S)-H(XY|Z)$$

$$\leqslant Len(S)-H_a(XY|Z)=\lambda(n(1-L_f^A)-\varepsilon)-H_a(XY|Z)$$

$$=\lambda n(1-L_f^A)-\lambda\varepsilon-\frac{1}{1-\alpha}\mathrm{lb}\sum_{y\in\varphi}P_Y(y)2^{(\alpha-1)\mathrm{lb}P_Y(y)+(1-\alpha)H_a(X|Y=y)}$$

令 $\eta=(\alpha-1)\mathrm{lb}P_Y(y)+(1-\alpha)H_a(X|Y=y)$。证毕。

定理 1 说明了敌手 Eve 关于二次提取后的初始密钥串 S 的信息有上界，因此初始密钥串 S 可用于保密增强。

引理 1[22] 设 X 为取值于集合 $\wp$ 的随机变量，$p_{\max}=\max_{x\in\wp}p_X(x)$则 $p_{\max}\leqslant2^{-H_a(X)+r_1n}$至少以概率 $1-2^{-(\alpha-1)r_1n}$成立，$0<r_1<1$，n 为初始密钥长度。

定理 2 设 $H_\alpha(S|Z)\geqslant\omega-\frac{r}{\alpha-1}$，$U$ 表示 Eve 主动攻击情况下攻击成功的事件，且 $\omega\geqslant n(1-L_f^A)$ 成立，则可以得到 Eve 主动攻击成功的概率满足：

$$P(U|Z=z)\leqslant r_2(1-L_f^E)^3 2^{-\tau_1(n)}$$

证明：(1)Eve 在模仿攻击时尝试猜出密钥。假设 Eve 知道用于保密增强的全域 Hash 函数 $h_d(x)=\sum_{i=0}^{N/l-1}d^i x_i$，其中 $N,l>0$，$2^l\geqslant N/l$，$d\in GF(2^l)$。设模仿攻击成功的概率为 P_{imp}，故：

$$\begin{aligned}P_{imp}&=\frac{1-L_f^E}{l^2}(1-2^{-(\alpha-1)r_1 n})P_{\max}(S|Z=z)\\&\leqslant\frac{1-L_f^E}{l^2}(1-2^{-(\alpha-1)r_1 n})2^{-H_\alpha(S|Z=z)+r_1 n}\\&\leqslant\frac{1-L_f^E}{l^2}(1-2^{-(\alpha-1)r_1 n})2^{r_1 n-\omega+\frac{r}{\alpha-1}}\leqslant\frac{(1-L_f^E)}{l^2}2^{-\tau(n)}\end{aligned}$$

(2)Eve 在替换攻击时尝试用已知的正确的已认证消息来替换窃听到的认证消息。

设 Alice 向 Bob 发送 (X,Y,F)，其中 (X,Y) 为消息对，F 为临时密钥，Z 为 Eve 已知的关于 S 的信息。设替换攻击成功的概率为 p_{sub}，则：

$$\begin{aligned}&P_{\max}(S|X=x,Y=y,F=f,Z=z)\\&\leqslant 2^{-H_\alpha(S|X=x,Y=y,F=f,Z=z)+r_1 n}\\&\leqslant 2^{(l-\frac{2^l-H(XY|F=f,Z=z)}{\ln^2}+r_1 n)}\end{aligned}$$

此式成立的概率为：

$$\begin{aligned}&r_2(1-L_f^A)(1-L_f^B)(1-L_f^E)(1-2^{-(\alpha-1)r_1 n})\leqslant\\&r_2(1-L_f^E)^3(1-2^{-(\alpha-1)r_1 n})\end{aligned}$$

综上分析得：

$$\begin{aligned}p_{\text{sub}}&\leqslant r_2(1-L_f^E)^3(1-2^{-(\alpha-1)r_1 n})\times 2^{(l-\frac{2^l-H_\alpha(XY|F=f,Z=z)}{\ln^2}+r_1 n)}\\&=r_2(1-L_f^E)^3 2^{-\tau_1(n)}\end{aligned}$$

又 $P(U|Z=z)=\max(P_{\text{imp}},P_{\text{sub}})$

$$\begin{aligned}&=\max\left(\frac{(1-L_f^E)}{l^2}2^{-\tau(n)},r_2(1-L_f^E)^3 2^{-\tau_1(n)}\right)\\&\leqslant r_2(1-L_f^E)^3 2^{-\tau_1(n)}\end{aligned}$$

故 $P(U|Z=z)\leqslant r_2(1-L_f^E)^3 2^{-\tau_1(n)}$。证毕。

定理 3 假设保密增强前 Alice 和 Bob 共享长度为 l 位的密钥串 S,S' 为经保密增强后的密钥。Eve 关于 S 的信息为 Z，D 为 l 比特概率集合的子集，且 $P_{S|Z=z}\in D$。$(l,D,H_\alpha(S',L_f^E)-s',\varepsilon,\delta)$ 为保密增强协议，其中

$$\varepsilon=\text{lb}\left(\frac{(L_f^A+L_f^B)N}{2l}-\varepsilon'\right)\cdot|Z|,\delta=r_2(1-L_f^E)^3 2^{-\tau_1(n)}$$

证明：(1)正确性和保密性

$$\begin{aligned}H_\alpha(S'|C,Z=z)&\geqslant H_\alpha(S'|L_f^E)-\text{lb}|Z|-s'\\&=H_\alpha(S',L_f^E)-H_\alpha(S')-\text{lb}|Z|-s'\\&\geqslant H_\alpha(S',L_f^E)-s'-\\&\quad\text{lb}\left(\frac{(L_f^A+L_f^B)N}{2l}-\varepsilon'\right)\cdot|Z|\end{aligned}$$

故得 $\varepsilon=\text{lb}(\frac{(L_f^A+L_f^B)N}{2l}-\varepsilon')\cdot|Z|$。

(2)健壮性

由定理 3 中 $P(U|Z=z)=\max(P_{imp},P_{sub})\leqslant r_2(1-L_f^E)^3 2^{-\tau_1(n)}$ 得知 Eve 攻击成功的最大概率为 $r_2(1-L_f^E)^3 2^{-\tau_1(n)}$，也即保密增强事件成功的概率至少为 $1-r_2(1-L_f^E)^3 2^{-\tau_1(n)}$，因此 $\delta=r_2(1-L_f^E)^3 2^{-\tau_1(n)}$。

证毕。

5 仿真结果及分析

本节通过仿真实验来验证本文提出的水声信道干扰因子及水声信道密钥协商方案的有效性。仿真软件使用 MATLAB R2014b，若无特殊说明，仿真参数设为定值。表 1 列出了仿真参数的默认值，发射角度设置为与水平方向夹角 15°。在仿真实验中采用了 BELLHOP 水声信道计算模型，此方法需要在 MATLAB R2014b 中添加 BELLHOP 路径即 actup.m 程序文件，并利用了高斯波束跟踪方法，生成了图 4 所示的通信信道模型。此外，为了说明本文密钥协商方案的优势，我们选择了 3 种方案，在密钥生成率、误比特率方面对其进行了对比。为了与经典的 CFR 方法进行对比，我们选择了文献[10]中的基于 CFR 自适应生成密钥方案；另外我们选择了最新的以海洋水声信道为背景的密钥协商方案，即文献[11]中的 DSSC 方案及文献[13]中的 DLCC_AGI 方案，这两种方案使用的方法先进而且与海洋水声信道结合紧密。通过实验结果可以看出，本文方案不仅可以防御敌手的主动攻击，在密钥生成率和误比特率方面也具有明显的优势。

表 1 参数默认值

Table 1 Default value of parameter

参数	数值
发射端深度/m	10
合法双方水平通信范围/m	[0,1000]
中心频率/kHz	13
带宽/kHz	11.33
多径数/个	50
最大多普勒频移/Hz	16.67
合法双方通信的深度范围/m	[0,500]

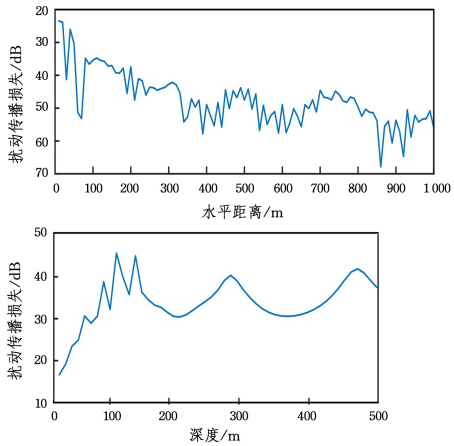

图 4 扰动传播损失

Fig. 4 Disturbance propagation loss

图 5 给出了未经保密增强的密钥信息熵与保密增强后密钥信息熵随着初始信息长度的变化而变化的情况。可以看出，随着初始信息长度的增加，经过保密增强后密钥的信息熵也随之增长，但增长的幅度远小于未经保密增强后密钥的信息熵，这说明了本文经过保密增强的密钥协商方案的安全性，

而且从图中可以看出，当初始信息长度较大时本文方案具有明显优势。图 6 给出了当初始信息量为 50000 bit 时，该保密增强协议中敌手进行主动攻击成功的概率与 Eve 干扰因子 L_f^E 及信息熵阶数 $\alpha(\alpha>1)$ 的关系，可以观察到 L_f^E 与主动攻击成功的概率成反比，α 与主动攻击成功的概率成反比。当 α 相同时，L_f^E 越大，Eve 主动攻击成功的概率越低，这可能是因为 L_f^E 越大，Eve 通信信道受到的干扰就越严重，拦截的有效信息较少，所以主动攻击成功的概率较低。由图中的数据可知，经保密增强后敌手主动攻击成功概率的上界为 4.3×10^{-23}。

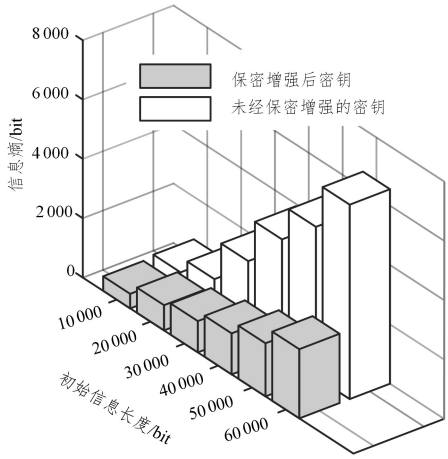

图 5 密钥信息熵的比较

Fig. 5 Comparison of key information entropy

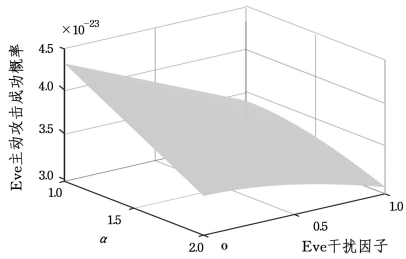

图 6 主动攻击成功概率关系图

Fig. 6 Probabilistic relation of success of active attack

在如图 7、图 8 所示的比较实验中，通信距离设置为 500 m，最大多普勒频移为 16.67 Hz，相干时间为 0.03 s，多径数为 25 条，发送数据长度设置为 50000 bit，忽略影响信道的其他因素。图 7 的实验数据表明，当信道信噪比为 30 dB 时，文献[11]中的方案、文献[10]中的方案及文献[13]中的方案的密钥生成率分别为 355 bit/s，421 bit/s 和 600 bit/s，而本文方案的密钥生成率可达 631 bit/s。相比文献[11]中的方案基于双扩频码数据帧结构分步执行，文献[10]中的方案由于允许在一个步骤中联合执行误差控制和自适应编码，缩减了计算时间，因此文献[10]中的方案在密钥生成率方面的性能优于文献[11]中的方案。此外，文献[13]中的方案采用集中式双层补偿和自适应保护区间量化相结合的方法，量化值由累积函数自适应生成，改善了密钥生成率，经仿真结果表明，当信噪比大于 −10 dB 时，密钥生成率大于 600 bit/s，明显优于文献[10]和文献[11]中的方案。

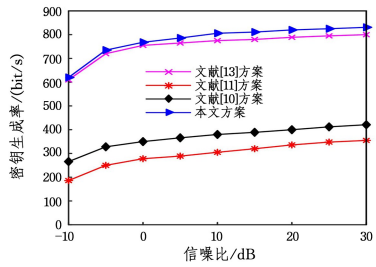

图 7 4 种方案的密钥生成率比较

Fig. 7 Comparison of key generation rate of four schemes

图 8 中的实验数据表明，相比文献[13]和文献[10]中的方案，文献[11]中的方案具有较低的误比特率，当信噪比大于 −10 dB 时误比特率小于 10^{-6}，这是由于文献[11]中的方案采用双扩频码数据帧结构，该系统具有良好的抗多径、抗干扰和抗多普勒的性能，不仅提高了密钥生成率，而且误比特率低。而文献[13]中的方案在信道估计方面未考虑到水声信道中的噪声干扰，因此文献[11]中的方案的误比特率相对较低。当信噪比小于 5 dB 时，文献[11]中的方案的误比特率较低，当信噪比大于 5 dB 时，本文方案的误比特率低于文献[11]中的方案，这说明了在信噪比低即海洋环境干扰比较严重的情况下，文献[11]中的方案优于本文方案，而本文方案在海洋环境干扰较小的情况下误比特率较低。这是因为在海洋环境干扰较为严重的情况下，干扰因子较大，敌手篡改消息成功的概率也稍大，又因为文献[11]中的方案没有考虑抗主动攻击，所以当海洋环境干扰比较严重时文献[11]中的方案的密钥生成速率优于本文方案。但是随着信噪比的增加，本文方案中敌手主动攻击成功的概率是趋于零的，因此本文方案整体上优于文献[11]中的方案。

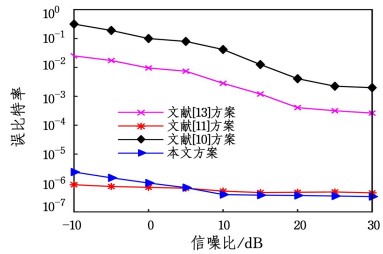

图 8 4 种方案的误比特率比较

Fig. 8 Comparison of bit error rate of four schemes

结束语 本文针对海洋环境不确定性的水声信道容易被攻击的问题，提出了安全的密钥协商方案，通过构造有限域到椭圆曲线映射的 Hash 函数进行初始密钥的提取，并利用汉明距离进行纠错，提高了通信的安全性，降低了误码率。此外，为降低敌手 Eve 进行主动攻击的概率，考虑到密钥存储效率和密钥生成率问题，将 Toeplitz 矩阵与密钥的矩阵乘法进行分块并行运算并结合全域 Hash 函数进行保密增强协议的设计，进一步提高了密钥生成率和保密性。安全性分析与仿真结果表明，本文方案在抗主动攻击、密钥生成率和误比特率方面实现了较好的平衡。在后续工作中将研究保密增强算法的硬件实现问题，并对算法的硬件资源消耗进行分析。

参 考 文 献

[1] ZHAO S D, YAN S F, XU L J. Doppler estimation based on

HFM signal for underwater acoustic time-varying multipath channel[C] // 2019 IEEE International Conference on Signal Processing, Communications and Computing. Dalian, China, 2019:1-6.

[2] STAMATION K, CASARI P, ZORZI M. The throughput of underwater networks: Analysis and validation using a ray tracing simulator[J]. IEEE Transactions on Wireless Communications, 2013, 12(3):1108-1117.

[3] QARABAQI P, STOJANOVIC M. Statistical characterization and computationally efficient modeling of a class of underwater acoustic communication channels[J]. IEEE Journal of Ocean Engineering, 2013, 38(4):701-717.

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

[5] SWEENEY P, SEOHWI D. Simple authenticated key agreement algorithm[J]. Electronics Letters, 1999, 35(13):1073-1074.

[6] VINOTH R, DEBORAH L J, VIJAYAKRUMAR P, et al. Secure multifactor authenticated key agreement scheme for industrial IoT[J]. IEEE Internet of Things Journal, 2021, 8(5):3801-3811.

[7] SARKAR A, SINGH B. A cancelable biometric based secure session key agreement protocol employing elliptic curve cryptography[J]. International Journal of System Assurance Engineering and Management, 2019, 10(5):1023-1042.

[8] NIU S F, HAN S, YU F, et al. Ciphertext Retrieval Scheme Based on Key Aggregation for Electronic Medical Record on Blockchain[J]. Computer Engineering, 2021, 47(5):36-43.

[9] BOYD C, MONTAGUE P, NGUYEN K. Elliptic curve based password authenticated key exchange protocols[C] // Australasian Conference on Information Security and Privacy. Berlin, Heidelberg: Springer, 2001, 2119:487-501.

[10] MURTHY T S N, SATISH R G, PADMARAJU K. Adaptive secret key generation in underwater acoustic system[C] // International Conference on Power, Control, Signals and Instrumentation Engineering. Chennai, India: IEEE, 2017:698-702.

[11] LIU L J, LI J F, ZHOU L, et al. An underwater acoustic direct sequence spread spectrum communication system using dual spread spectrum code[J]. Rontiers of Information Technology & Electronic Engineering, 2018, 19(8):972-983.

[12] LUO Y, PU L, PENG Z, et al. RSS-based secret key generation in underwater acoustic networks: advantages, challenges and performance improvements[J]. IEEE Communications Magazine, 2016, 54(2):32-38.

[13] SHEN Z W, LIU J M, HAN Q Q. A local pilot auxiliary key generation scheme for secure underwater acoustic communication[J]. Information Sciences, 2019, 473:1-12.

[14] ZHANG J, ZHONG H, CUI J, et al. SMAKA: secure many-to-many authentication and key agreement scheme for vehicular networks[J]. IEEE Transactions on Information Forensics and Security, 2021, 16:1810-1824.

[15] JIANG Q, CHEN Z R, MA J F, et al. Optimized fuzzy commitment based key agreement protocol for wireless body area network[J]. IEEE Transactions on Emerging Topics in Computing, 2021, 9(2):839-853.

[16] BENNETT C H, BRASSARD G, ROBERT J. Privacy amplification by public discussion[J]. SIAM Journal on Computing, 1988, 17:210-229.

[17] TANG B Y, LIU B, ZHAI Y P, et al. High-speed and Large-scale Privacy Amplification Scheme for Quantum Key Distribution[J]. Scientific Reports, 2019, 1(9):15733.

[18] HAYASHI M, TAURUMARU T. More efficient privacy amplification with Less random seeds via dual universal Hash function[J]. IEEE Transactions on Information Theory, 2016, 62(4):2213-2232.

[19] MAURER U, WOLF S. Secret-Key agreement over unauthenticated public channels part III: Privacy amplification[J]. IEEE Transactions on Information Theory, 2003, 49(4):839-850.

[20] WANG X Y, ZHANG Y C, YU S, et al. High-Speed Implementation of Length-Compatible Privacy Amplification in Continuous-Variable Quantum Key Distribution[J]. IEEE Photonics Journal, 2018, 10(3):1-9.

[21] HE X Y, YU W, WANG K P. On construction and application of deterministic encoding functions into elliptic curves[J]. Journal of Cryptologic Research, 2018, 5(3):301-314.

[22] YANG B, ZHANG T, WANG Y M. Distillation of unconditionally-secure secret-key against active adversaries based on smooth entropy[J]. Acta Electronica Sinica, 2001, 29(10):1348-1350.

LIANG Zhen-zhen, born in 1996, postgraduate. Her main research interests include underwater acoustic sensor network and information security.

(责任编辑:喻藜)