计 算 机 研 究 与 发 展
Journal of Computer Research and Development
https://crad.ict.ac.cn
62(12): 3077−3092, 2025

基于水下物联网的多方密钥封装方案

徐 明 张恩博 周日贵
(上海海事大学信息工程学院 上海 201306)
(mingxu@shmtu.edu.cn)

Multi-Party Key Encapsulation Mechanism Based on the Internet of Underwater Things

Xu Ming, Zhang Enbo, and Zhou Rigui
(*College of Information Engineering*, *Shanghai Maritime University*, *Shanghai* 201306)

Abstract In order to resist attacks of quantum computing and protect the privacy and data security of underwater nodes, a multi-party key encapsulation mechanism based on the Internet of underwater things is proposed using the difficulty assumption of NTRU cryptographic system. Firstly, the pseudo-identities of device serial numbers are generated by combining ocean sensor acoustic sequences and underwater acoustic waveform factorization, and a verifiable identity ocean acoustic message code is designed. Secondly, a key generation algorithm suitable for underwater communication is designed using orthogonal frequency division multiplexing (OFDM) frequency domain oversampling technique and number theoretic transform (NTT).On this basis, a multi-party public key encryption algorithm with indistinguishability and anonymity under chosen plaintext attack (IND-Anon-CPA) security is constructed using identity-bound hybrid encryption and ocean noise-based obfuscation operation, Thirdly, a SeaFO transform based on ocean noise is introduced to develop a multi-party key encapsulation algorithm with indistinguishability and anonymity under chosen ciphertext attack (IND-Anon-CCA) security without full re-encryption process. Finally, a novel session key update mechanism is devised where autonomous underwater vehicles verify ciphertext components, and assess pseudo-identity and timestamp validity using OFDM subcarriers. The new session keys are decapsulated using SeaFO transform, which not only achieve implicit rejection in multi-party environments and but also thwart adversaries' adaptive corruption on SeaNTRU. Security analysis demonstrates that SeaNTRU has the characteristics of resistance to key replacement attack, replay attack, and man-in-the-middle attack. Experimental results show that SeaNTRU has lower computational cost and communication overhead than the existing schemes.

Key words NTRU; the Internet of underwater things; multi-party key encapsulation mechanism; number theoretic transform (NTT); obfuscation operation

摘 要 为了抵抗量子计算的攻击,保护水下节点的隐私与数据安全,利用NTRU密码体制的困难性假设提出了一种基于水下物联网的多方密钥封装方案SeaNTRU.首先,结合海洋传感器声波序列和水声声波因子生成设备序列号的伪身份并设计了一种可验证身份的海洋声波消息码.其次,利用正交频分复用(orthogonal frequency division multiplexing, OFDM)频域过采样技术和数论变换(number theoretic transform, NTT)设计了一种适用于水声通信的密钥生成算法.在此基础上,利用身份绑定的混合加密和基于海洋噪声的混淆操作构造了具有选择明文攻击下的不可区分性和匿名性(indistinguishability and anonymity under

收稿日期: 2024-08-13; **修回日期**: 2025-05-06
基金项目: 国家自然科学基金项目(62172269, 62172268)
This work was supported by the National Natural Science Foundation of China (62172269, 62172268).

chosen plaintext attack, IND-Anon-CPA)安全的多方公钥加密算法. 然后,提出了一种基于海洋噪声的SeaFO变换,并由此得到具有选择密文攻击下的不可区分性和匿名性(indistinguishability and anonymity under chosen ciphertext attack, IND-Anon-CCA)安全的多方密钥封装算法,该算法不需要执行全部的重加密过程. 最后,设计了一种新的会话密钥更新机制. 在该会话密钥更新机制中,水下自主机器人利用OFDM子载波提取密文分量并进行伪身份和时间标记有效性的检验,通过使用SeaFO变换解封装得到新的会话密钥,不仅实现了多方环境下的隐式拒绝,也防止了敌手对于SeaNTRU的自适应破坏. 通过安全性分析,证明了SeaNTRU具有抗公钥替换攻击、抗重放攻击和抗中间人攻击的特性. 实验结果表明,SeaNTRU比现有方案计算成本和通信开销小.

关键词 NTRU;水下物联网;多方密钥封装方案;数论变换;混淆操作

中图法分类号 TP309

DOI: 10.7544/issn1000-1239.202440673 **CSTR:** 32373.14.issn1000-1239.202440673

近年来,水下物联网技术通过不同设备间的互联互通与数据传输为海洋资源的探索与利用提供了新途径[1-2]. 多方密钥封装作为信息安全领域的重要组成部分,可以有效解决传统的加密手段单独向每个设备发送数据的问题. 然而,海洋环境的复杂性给多用户之间数据传输的安全性和隐私保护带来了巨大的挑战,包括海洋多普勒效应、信道多径衰减等因素的影响,以及设备能源有限、海洋传输时延等问题[3].

现有密钥封装方案提供了多种高效的加密和密钥管理方法[4-8],提高了数据传输的安全性,但是这些方案缺少了基于水下物联网的轻量级结构设计和动态更新机制,不能很好地适用于水下应用场景.

量子计算的兴起为密码学带来了革命性的变化. 20世纪80年代,Benioff[9]构建了基于量子的图灵机模型,利用量子力学的思想提出了传统计算机所无法实现的一些功能和应用. 1994年,Shor[10]提出了一种量子算法,可以有效找到整数中的质因数. Shor算法和其他量子算法的提出,让经典密码学和基于传统困难性假设构造的密钥封装方案在量子计算领域变得不再安全. 尤其是在水下物联网这种开放信道的环境中,量子攻击的潜在风险尤为突出. 如何在量子计算的背景下确保水声信道的信息安全,同时构建抗量子攻击的密钥封装方案确保水下物联网的信息安全将面临更大的挑战.

基于格的密码学被证明是抗量子攻击的,NTRU[11]作为经典的格密码体制之一得到了广泛关注. 本文从NTRU密码体制的困难性假设出发,提出一种基于水下物联网的多方密钥封装方案SeaNTRU,保护水下节点的多方隐私与数据安全. 本文的主要贡献如下:

1)结合海洋传感器声波序列和水声声波因子生成设备序列号的伪身份并设计了一种可验证身份的海洋声波消息码. 利用OFDM频域过采样技术和NTT设计了一种适用于水声通信的密钥生成算法. 在此基础上,利用身份绑定的混合加密和基于海洋噪声的混淆操作构造了在量子随机预言机中具有IND-Anon-CPA安全性的多方公钥加密算法.

2)提出了一种基于海洋噪声的SeaFO变换和一种在量子随机预言机中具有IND-Anon-CCA安全性的多方密钥封装算法. 当敌手通过产生多个无效密文导致SeaNTRU解封装失败时,水下自主机器人会生成随机信息和对应的海洋噪声,生成无效且不可区分的会话密钥,使得敌手难以通过解封装失败获取任何可以解封装密文的信息.

3)设计了一种新的会话密钥更新机制. 在该机制中水下自主机器人通过OFDM子载波提取密文分量同时进行伪身份和时间标记有效性的验证,使用SeaFO变换解封装得到新的会话密钥,不仅实现了多方环境下的隐式拒绝,也防止了敌手对SeaNTRU的自适应破坏.

1 相关工作

密钥封装是一种重要的密码学技术,它将密钥生成、封装、分发等功能集成在一起,使得只有特定的接收者可以解密并得到会话密钥. 近年来,随着信息技术的不断发展,密钥封装在保障安全通信方面的作用得到越来越多的重视. Seo等人[12]提出了一种不需要双线性对运算的无证书签密密钥封装方案,该方案使用椭圆曲线密码学(elliptic curve cryptography, ECC)基于椭圆曲线的离散对数问题进行构造,适用于物联网环境下的数据安全. Chen等人[13]提出了一

种基于医疗区块链的密钥封装方案，首先对医疗数据进行对称加密，然后使用对称加密的公钥进行非对称加密. 进一步地，将非对称加密的公钥和封装的对称密钥存储在区块链的智能合约中，提高了区块链中的隐私安全. 然而上述方案在多用户的使用过程中会产生一定的计算开销. 为了更好地将安全保护应用于多方场景中，宁建廷等人[14]提出了一种基于SM9-HIBE的密钥封装机制，面向不同层的用户支持解密外包和多密文批量审计，提出的方案适用于大规模网络的高并发环境. Wu等人[4]面向多个用户，针对侧信道攻击的威胁，在连续泄露模型下提出了一种抗泄露的无证书密钥封装模式，在双线性模型下证明了该方案的语义安全. 周彦伟等人[5]基于证书面向抗泄露密码学提出了一种多接收者密钥封装方案，在多方环境下具有更优的效率，但是该方案仅能达到Diffie-Hellman困难性假设下的选择明文安全. He等人[6]提出了一种基于ECC体制的多接收者加密方案，不需要双线性对运算和哈希点运算，降低了移动设备中的运算成本，但解密过程不够优化. Deng[7]面向智慧社区，在标准模型下设计了一种匿名多接收者加密方案，适用于社区内的管理中心向不同单位和用户传输相同的信息，但是方案中的双线性运算随着用户数量的增长而增加，可扩展性较差. Li等人[8]使用基于身份的加密结合多重线性映射的可编程哈希函数构造了一个基于身份的多接收者公钥加密模式，用于解决物联网中的隐私问题，其安全依赖于传统的多线性映射. 随着量子计算和量子算法的不断发展，上述方案中的困难性假设在量子攻击面前可能不再安全.

Lyubashevsky等人[15]使用NTT，提出了一种基于NTRU的密钥封装方案NTTRU，使用NTT友好环并基于最短向量问题和最近向量问题的困难性假设，实现了抗量子攻击. Fouque等人[16]结合Falcon[17]相似的设计原则，设计了一种改进解码器的密钥封装方案，在相同的安全等级下可以生成短的密文，但由于该方案将陷门作为私钥，使得密钥生成算法的执行时间较长，消耗的计算资源较大，因此不适用于能源有限的水下物联网环境. Kim等人[18]基于ACWC2变换和$\overline{\mathrm{FO}}^{\perp}$变换在实现底层NTRU平均情况误差(average-case error)的最坏情况正确性误差(worst-case correctness error)的同时，保障了所提密钥封装方案的安全和紧凑性. 梁志闯等人[19]设计了一种基于单向困难性假设的密钥封装方案LTRU，因其计算的高效性和密文的紧凑性，该方案适用于资源受限环境下的数据安全.

进一步，考虑到多方环境下的设计，Katsumata等人[20]提出了一种可分解的多接收者公钥加密方法并结合一种FO[21]变换的隐式拒绝形式，构建了基于后量子密码学的多接收者密钥封装方案. 然而该方案对使用FO变换隐式拒绝构造的多方密钥封装算法提出了矛盾，即在多方环境中，敌手发起自适应破坏攻击会将密文$(c_1,c_2,\cdots,c_n)$修改为$(c_1,c_2,\cdots,\hat{c}_n)$，其中$\hat{c}_n$为无效密文，如果没有验证机制，那么接收者对于$(c_1,c_2,\cdots,c_{n-1})$会正常输出会话密钥，而无法判断$c_n$的有效性对系统的安全产生威胁. 此外，文献[20]中基于可分解公钥加密的多接收者密钥封装方案使用一部分与公钥无关的公开密文作为条件来解封装与公钥关联的密文并且缺少相应的更新机制，因此容易遭受重放攻击. Hashimoto等人[22]通过后量子多接收者公钥加密来构造连续组群密钥协商，设计了一种基于承诺的链式多接受者公钥加密方案，在带宽消耗和计算效率上具有优势. 但是，该方案仅在经典随机预言机下使用FO变换的显式拒绝抵抗敌手的自适应破坏. Alwen等人[23]首先设计了一种黑盒编译器，构造自适应安全的多接收者公钥加密方案，并在文献[20, 22]的基础上使用FO变换证明了量子随机预言机下的多方安全性，但由于该方案运算的复杂性以及需要生成更多的密文，并不适用于资源受限的水下环境. 此外，由于水下时延扩展会导致文献[20, 23]中密钥生成时采样点的不稳定以及采样精度的下降，需要进行多次采样以确保密钥长度，因此不适用于高延迟的水下物联网环境. 由于国内外目前还缺少针对水下环境的密钥封装技术，而现有的密钥封装方案无法直接应用于水下环境，因此本文将重点研究如何在水下物联网环境中实现多方密钥封装.

2 模型与预备知识

2.1 系统模型

本文定义的水下物联网系统模型如图1所示. 其中，水面数据平台(DP)与水下自主机器人$\psi_1,\psi_2,\cdots,\psi_n$通过搭载的正交频分复用(orthogonal frequency division multiplexing, OFDM)调制解调器进行数据通信，通信中的OFDM信号发射方程可表示为[24]

$$x(t)=\sum_{\varsigma\in Z_s}X(\varsigma)\times \mathrm{e}^{\mathrm{j}2\pi\frac{\varsigma}{T}t}\Pi(t), \tag{1}$$

其中Z_s为子载波集合，$X(\varsigma)$为子载波要发送的符号，$\mathrm{e}^{\mathrm{j}2\pi\frac{\varsigma}{T}t}$是基带正交函数，$\Pi(t)$为矩形窗函数.

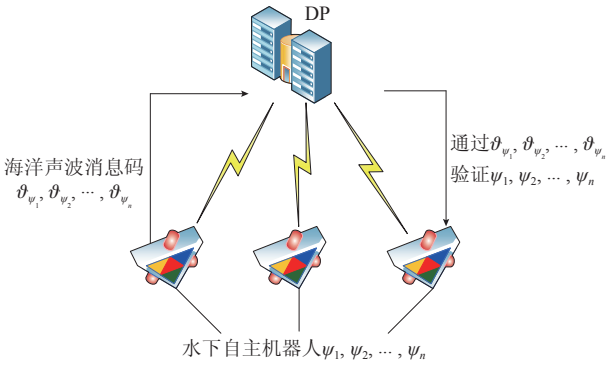


Fig. 1 The system model of Internet of underwater things

图 1 水下物联网系统模型

水下自主机器人$\psi_1,\psi_2,\cdots,\psi_n$的设备序列号表示为$ID_{\psi_1},ID_{\psi_2},\cdots,ID_{\psi_n}$, $\psi_1,\psi_2,\cdots,\psi_n$生成的海洋传感器声波序列表示为$V_{\psi_1}=[\rho_1^{\psi_1},\rho_2^{\psi_1},\cdots,\rho_\lambda^{\psi_1}],\cdots,V_{\psi_n}=[\rho_1^{\psi_n},\rho_2^{\psi_n},\cdots,\rho_\lambda^{\psi_n}]$. 其中$\rho_1^{\psi_i},\rho_2^{\psi_i},\cdots,\rho_\lambda^{\psi_i}$是组成$V_{\psi_1},V_{\psi_2},\cdots,V_{\psi_n}$的水声声波因子, 是本文水下物联网模型中的特有元素. 本文将水声声波因子和海洋传感器声波序列分别哈希后, 通过异或运算得到模型中的海洋噪声. 水下自主机器人生成的海洋声波消息码表示为$\vartheta_{\psi_1},\vartheta_{\psi_2},\cdots,\vartheta_{\psi_n}$. DP 中存储了水下自主机器人$\psi_1,\psi_2,\cdots,\psi_n$的设备序列号$ID_{\psi_1},ID_{\psi_2},\cdots,ID_{\psi_n}$和海洋传感器声波序列$V_{\psi_1},V_{\psi_2},\cdots,V_{\psi_n}$. 系统中海洋传感器声波序列、水下自主机器人的设备序列号为保密信息. DP 通过水下自主机器人生成的海洋声波消息码验证其身份. 对于身份可信的水下自主机器人, DP 生成一个会话密钥K并进行封装, 然后将密钥封装后形成的密文发送给多个水下自主机器人. 水下自主机器人提取密文并解封装得到与 DP 一致的会话密钥K.

2.2 敌手模型

本文的敌手模型如下:

1) Ⅰ型敌手可以拦截 DP 和$\psi_1,\psi_2,\cdots,\psi_n$之间传输的密文, 修改密文信息或者结构对接收者进行攻击.

2) Ⅱ型敌手可以替换$\psi_1,\psi_2,\cdots,\psi_n$的合法公钥为敌手生成的公钥.

3) Ⅲ型敌手可以截获 DP 和$\psi_1,\psi_2,\cdots,\psi_n$之间的交互信息, 并在稍后将截获的信息重新发送给$\psi_1,\psi_2,\cdots,\psi_n$发起攻击.

4) Ⅳ型敌手可以假冒 DP 或$\psi_1,\psi_2,\cdots,\psi_n$的合法身份, 对系统中的接收方或者发送方发起攻击.

2.3 预备知识

定义 1. NTRU 密码体制的困难性假设主要基于最短向量问题(shortest vector problem, SVP)和最近向量问题(closest vector problem, CVP)在量子计算环境下是难以解决的, 它们可以表示如下:

1)最短向量问题. 给定一个格Ω, 在其中寻找最短的非零向量$\boldsymbol{\ell}\in\Omega$, 使得$\boldsymbol{\ell}$的欧几里得范数在所有非零格向量中最小, 即

$$SVP_{\boldsymbol{\ell}}=\min_{\boldsymbol{\ell}\in\Omega\setminus\{0\}}\|\boldsymbol{\ell}\|. \tag{2}$$

2)最近向量问题. 给定一个格Ω, 对于一个给定且不在Ω中的向量$\boldsymbol{a}$, 找到一个向量$\boldsymbol{a}'\in\Omega$使得该向量距离$\boldsymbol{a}$最近, 即

$$CVP(\boldsymbol{a},\Omega)=\arg\min_{\boldsymbol{a}'\in\Omega}\|\boldsymbol{a}-\boldsymbol{a}'\|. \tag{3}$$

定义 2. 多方公钥加密算法 *mpPKE* 可表示为 *mpPKE*= (*mSetup*, *mKeyGen*, *mEnc*, *mExt*, *mDec*), 步骤如下:

1) *mSetup*(1^λ). 输入安全参数1^λ, 输出公共参数 *pp*. 其中安全参数λ是一个正整数, 用于定义密码学方案的安全强度, 通常与攻击者破解该方案所需的计算复杂度相关. λ越大, 安全级别越高. λ的常见取值有 128, 192, 256, 在本文中取$\lambda=256$.

2) *mKeyGen*(*pp*). 输入公共参数 *pp*, 输出公私钥对(pk_i, sk_i), $i=1,2,\cdots,n$.

3) *mEnc*($pp,pk_1,pk_2,\cdots,pk_n$). 输入公共参数 *pp* 和公钥$pk_1,pk_2,\cdots,pk_n$, 输出密文C.

4) *mExt*(i,C). 输入索引i和密文C, 输出第i个接收者的密文分量C_i, 否则提取失败.

5) *mDec*(C_i,sk_i). 输入第i个接收者的私钥sk_i和密文分量C_i, 输出消息, 否则解密失败.

定义 3. 多方密钥封装算法 *mpKEM* 可表示为 *mpKEM*= (*mSetup*, *mKeyGen*, *mEncaps*, *mExt*, *mDecaps*), 其中 *mSetup*, *mKeyGen*, *mExt* 与 *mpPKE* 中的相同. *mEncaps* 和 *mDecaps* 步骤如下:

1) *mEncaps*($pp,pk_1,pk_2,\cdots,pk_n$). 输入公共参数 *pp* 和公钥$pk_1,pk_2,\cdots,pk_n$, 输出密文C和会话密钥.

2) *mDecaps*(C_i,sk_i). 输入第 i 个接收者的私钥 sk_i 和密文分量C_i, 输出会话密钥, 否则解封装失败.

定义 4. 设 *mpPKE* 和 *mpKEM* 存在正确性误差δ, 表示为

$$E\left[\max_{m\in\mathcal{M}}Pr[mDec(sk_i,mEnc(pk_i,m))\neq m]\right]\leqslant\delta, \tag{4}$$

$$E\left[\max_{m\in\mathcal{M}}Pr[mDecaps(sk_i,c_i)\neq K|(c,K)\leftarrow Encap(pk_i)]\right]\leqslant\delta. \tag{5}$$

定义 5. 对于$(pk_i,sk_i)\leftarrow mKeyGen(1^\lambda)$, $i\in\{1,2,\cdots,n\}$, $m,m'\in\mathcal{M}$和$r,r'\in\mathcal{R}$, 有

$$Pr[mEnc(pk_i,m,r)=mEnc(pk_i,m',r')|(m,r)\neq(m',r')]\leqslant\zeta, \tag{6}$$

则称 *mpPKE* 是ζ注入性的.

定义 6. 对于 SeaNTRU 满足 $V_i \in V_v$, $\rho_j^i \in V_i$, $ID_i \in ID_{\mathrm{id}}$. 对于海洋信息 m, $m' \in \mathcal{M}$和随机数 r, $r' \in \mathcal{R}$, 有

$$Pr[\left(mEnc(pk_i,r),SeaTr(V_i,\rho_j^i,m)\oplus H(r,ID_i)\right)=\left(mEnc(pk_i,r'),SeaTr(V_i,\rho_j^i,m')\oplus H(r',ID_i)\right)|(m,r)\neq(m',r')]\leqslant \zeta-\zeta_{\Delta o}, \tag{7}$$

其中 $i \in \{\psi_1,\psi_2,\cdots,\psi_n\}$, $j \in \{1,2,\cdots,\lambda\}$. V_v是海洋传感器声波序列空间, ID_{id}是设备序列号空间, $\mathcal{M}$是海洋信息空间, $\mathcal{R}$是随机数空间, *SeaTr* 是本文方案中提出的基于海洋噪声和属性绑定的混淆操作, $\zeta-\zeta_{\Delta o}$是引入 V_i, ρ_j^i, ID_i以及海洋噪声后的注入性概率.

定义 7. 设$mpPKE=(mKeyGen,mEnc,mExt,mDec)$, $mEnc(pk_i,m)$的最小熵$\gamma(pk_i,m)=-\mathrm{lb}\|mEnc(m)\|$, 其中

$$\|mEnc(m)\|=\max_{m\in\mathcal{M},r\leftarrow\{0,1\}^\lambda} Pr[ct=mEnc(pk_i,m,r)]. \tag{8}$$

对于任意的$(pk_i,sk_i)\leftarrow mKeyGen(1^\lambda)$则称 *mpPKE* 是$\gamma$扩散的, 即$\gamma(pk_i,m)\geqslant\gamma$. 对于每一个可能的密文 ct, 有

$$E\left[\max_{m\in\mathcal{M}} Pr[mEnc(pk_i,m,r)=ct]\right]\leqslant 2^{-\gamma}. \tag{9}$$

3 本文方案

3.1 方案初始化

SeaNTRU 使用分圆多项式 $x^n-x^{n/2}+1$及其卷积多项式环$R_q=\dfrac{\mathbb{Z}_q[x]}{x^n-x^{n/2}+1}$, 公开参数满足 n 与 q 互质, 且 p 与 q 互质, 其中 n 为整数, p, q 为模数, 选择 NTT 进行加速. 海洋信息空间表示为$\mathcal{M}=\{0,1\}^\lambda$, 随机数空间表示为$\mathcal{R}=\{0,1\}^\lambda$, 海洋传感器声波序列空间表示为$V_v=\{-1,0,1\}^\lambda$, 设备序列号空间表示为$ID_{id}=\{0,1\}^\lambda$, 其中$\{0,1\}^\lambda$代表 λ个 0 或 1 的序列. $H:=\{0,1\}*\rightarrow R_q$, $G:=\{0,1\}*\rightarrow R_q$表示为基于海绵结构的 SHA-3 哈希函数, 可以建模为经典或者量子随机预言机.

1)伪身份生成

伪身份生成操作 *MaforID* 完成水下自主机器人ψ_1, $\psi_2,\cdots,\psi_n$的身份伪装, 伪装后的身份可表示为$ID_i^{\mathrm{Fake}}=MaForID(ID_i)$, $i\in\{\psi_1,\psi_2,\cdots,\psi_n\}$. 其中每次$ID_i^{\mathrm{Fake}}$生成的时间标记为$T_{\psi_1},T_{\psi_2},\cdots,T_{\psi_n}$, 具体表示为

$$ID_i^{\mathrm{Fake}}=(\rho_j^i,T_i)\oplus H(V_i)\oplus H(ID_i), \tag{10}$$

其中水声声波因子ρ_j^i从海洋传感器声波序列V_i中随机选取, $j\in\{1,2,\cdots,\lambda\}$, $T_i+\Delta T_i\leqslant\tau$, 即$ID_i^{\mathrm{Fake}}$的时间标记存在时间$T_i+\Delta T_i$不超过最长海洋时延$\tau$.

2)混淆操作

混淆操作 *SeaTr* 是一种基于海洋噪声和属性绑定的操作. 对于海洋噪声 O_i, 绑定$\psi_1,\psi_2,\cdots,\psi_n$中的属性$V_i$和从对应$V_i$中选取的$p_j^i$以生成不同的海洋噪声, 将海洋信息$m\in\mathcal{M}$混淆隐藏在$O_i$中, 具体步骤包括

$$O_i=G(p_j^i)\oplus G(V_i), \tag{11}$$

$$m_i'=m\oplus O_i. \tag{12}$$

混淆后的海洋信息可表示为$m_i'=SeaTr(m,V_i,p_j^i)$. 去混淆操作 *UnSeaTr* 为混淆操作 *SeaTr* 的逆过程, 可表示为$m=UnSeaTr(m_i',V_i,p_j^i)$. 其中$i\in\{\psi_1,\psi_2,\cdots,\psi_n\}$, $j\in\{1,2,\cdots,\lambda\}$, 拥有相应属性的接收者才可以生成相同的$O_i$. 通过 *UnSeaTr* 操作可以得到去除混淆后的m. 定理 1 证明了 *SeaTr* 可以提高海洋信息熵.

定理 1. 设海洋信息的熵为$H_{\mathrm{entropy}}(m)$, 海洋噪声的熵为$H_{\mathrm{entropy}}(O)$, 经过混淆操作后的海洋信息熵为$H_{\mathrm{entropy}}(m')$, 则有$H_{\mathrm{entropy}}(m')>H_{\mathrm{entropy}}(m)$.

证明. DP 某时刻收集海洋信息$m_1,m_2,\cdots,m_\Upsilon$, 获取信息的概率为$Pr(m_1),Pr(m_2),\cdots,Pr(m_\Upsilon)$. $m_1,m_2,\cdots,m_\Upsilon$的熵为

$$H_{\mathrm{entropy}}(m)=-\sum_{h=1}^{\Upsilon}Pr(m_h)\mathrm{lb}Pr(m_h), \tag{13}$$

当$Pr(m_h)=\dfrac{1}{\Upsilon}$时, $H_{\mathrm{entropy}}(m)$取$H_{\mathrm{entropy}}^{\max}(m)=\mathrm{lb}\Upsilon$.

设生成的海洋噪声为$O_1,O_2,\cdots,O_\mu$, 海洋噪声产生的概率为$Pr(O_1),Pr(O_2),\cdots,Pr(O_\mu)$, 则 $O_1,O_2,\cdots,O_\mu$的熵

$$H_{\mathrm{entropy}}(O)=-\sum_{k=1}^{\mu}Pr(O_k)\mathrm{lb}Pr(O_k), \tag{14}$$

当$Pr(O_k)=\dfrac{1}{\mu}$时, $H_{\mathrm{entropy}}(O)$取$H_{\mathrm{entropy}}^{\max}(O)=\mathrm{lb}\mu$.

由 *SeaTr* 有$H_{\mathrm{entropy}}(m\oplus O)=H_{\mathrm{entropy}}(m')$, m'的取值为$m_1',m_2',\cdots,m_r'$, m'的概率为$Pr(m_1'),Pr(m_2'),\cdots,Pr(m_r')$, 则$m_1',m_2',\cdots,m_r'$的熵为

$$H_{\mathrm{entropy}}(m')=-\sum_{y=1}^{\Upsilon\mu}Pr(m_y')\mathrm{lb}Pr(m_y'). \tag{15}$$

设$m_1',m_2',\cdots,m_r'$的$Pr(m_1'),Pr(m_2'),\cdots,Pr(m_r')$为$\dfrac{1}{\Upsilon\mu}$, 则

$$H_{\mathrm{entropy}}(m')=-\mathrm{lb}\frac{1}{\Upsilon\mu}=\mathrm{lb}\Upsilon\mu. \tag{16}$$

有$H_{\mathrm{entropy}}(m')=\mathrm{lb}\Upsilon\mu>H_{\mathrm{entropy}}(m)=\mathrm{lb}\Upsilon$, 则

$$H_{\mathrm{entropy}}(m')>H_{\mathrm{entropy}}(m). \tag{17}$$

证毕.

3.2 多方公钥加密算法

SeaNTRU 的多方公钥加密算法由以下 6 个步骤的算法组成.

1)密钥生成

算法 1. *SeaNTRU.mpPKE.mKeyGen* 算法.

① $z=A_z\mathrm{e}^{\mathrm{j}\phi_z}, w=A_w\mathrm{e}^{\mathrm{j}\phi_w}\leftarrow P$;

② $Z_k=\sum_{d=0}^{N-1}z_d\times\omega^{dk} \bmod q, W_k=\sum_{d=0}^{N-1}w_d\times\omega^{dk} \bmod q$;

③ $Z'_k=[z_0,z_1,\cdots,z_{d-1},[-1,0,1],\cdots,[-1,0,1]]$;

④ $W'_k=[w_0,w_1,\cdots,w_{d-1},[-1,0,1],\cdots,[-1,0,1]]$;

⑤ $z'_d=\frac{1}{N}\sum_{k=0}^{N-1}Z'_k\times\omega^{-dk} \bmod q, w'_d=\frac{1}{N}\sum_{k=0}^{N-1}W'_k\times\omega^{-dk} \bmod q$;

⑥ $z'_d=[Z'_0,Z'_1,\cdots,Z'_{d-1}]\leftarrow f'\in\{-1,0,1\}^{\lambda}$;

⑦ $w'_d=[W'_0,W'_1,\cdots,W'_{d-1}]\leftarrow g\in\{-1,0,1\}^{\lambda}$;

⑧ $f:=pf'+1$;

⑨ if $f^{-1}\notin R_q$, restart

⑩ $h:=pgf^{-1}\in R_q$;

⑪ $pk:=h$, $sk:=f$;

⑫ end if

该算法利用 OFDM 频域过采样技术和 NTT 变换得到秘密多项式 f 和 g 并生成公钥和私钥. 其中: 行①为在频域 P 中随机选取并构成的频谱方程 z 和 w, A_z 代表频谱方程 z 的振幅, A_w 代表频谱方程 w 的振幅, ϕ_z 代表方程 z 的相位, ϕ_w 代表方程 w 的相位. 行②是在频域中对 z 和 w 使用 NTT 变换为点值形式, Z_k 和 W_k 分别表示 z 和 w 变换后得到的序列中的第 k 个元素, ω 为变换参数, N 为元素序列个数. 行③④是利用过采样并采取系数填充策略后的序列 Z'_k 和 W'_k. 行⑤是逆 NTT 变换得到的时域序列 z'_d 和 w'_d. 行⑥⑦中 z'_d 和 w'_d 分别构成 f' 和 g. 行⑧~⑩中如果 f 的逆元在 R_q 中, 计算得到 h, 否则重新进行采样. 行⑪中得到公钥 pk 和私钥 sk.

2)海洋声波消息码生成

算法 2. *SeaNTRU.mpPKE.mSeaCodeGen* 算法.

① for $i\in\{\psi_1,\psi_2,\cdots,\psi_n\}$ do

② $\rho_j^i\leftarrow V_i$;

③ $\mu_i=V_i\oplus H(pk_i)\oplus H(\rho_j^i,ID_i)$;

④ $Lab_i^{\mathrm{Sea}}=\rho_j^i\oplus H(V_i)$;

⑤ $\eta_i=Lab_i^{\mathrm{Sea}}\oplus H(pk_i)\oplus H(\rho_j^i,ID_i)\oplus H(V_i)$;

⑥ $\vartheta_i=(\mu_i,\eta_i)$;

⑦ end for

其中: 行②表示水声声波因子 ρ_j^i 从海洋传感器声波序列 V_i 中随机取得, $j\in\{1,2,\cdots,\lambda\}$. 行③表示 $\psi_1,\psi_2,\cdots,\psi_n$ 分别生成 $\mu_{\psi_1},\mu_{\psi_2},\cdots,\mu_{\psi_n}$. 行④表示 $\psi_1,\psi_2,\cdots,\psi_n$ 分别生成水声广播标签 $Lab_{\psi_1}^{\mathrm{Sea}},Lab_{\psi_2}^{\mathrm{Sea}},\cdots,Lab_{\psi_n}^{\mathrm{Sea}}$. 行⑤表示 $\psi_1,\psi_2,\cdots,\psi_n$ 分别生成 $\eta_{\psi_1},\eta_{\psi_2},\cdots,\eta_{\psi_n}$. 行⑥表示 $\psi_1,\psi_2,\cdots,\psi_n$ 生成海洋声波消息码 $\vartheta_{\psi_1},\vartheta_{\psi_2},\cdots,\vartheta_{\psi_n}$. 对应的公钥和海洋声波消息码表示为 $(pk_{\psi_1},\vartheta_{\psi_1}),(pk_{\psi_2},\vartheta_{\psi_2}),\cdots,(pk_{\psi_n},\vartheta_{\psi_n})$.

3)海洋声波消息码验证

算法 3. *SeaNTRU.mpPKE.mSeaCodeVer* 算法.

① for $i\in\{\psi_1,\psi_2,\cdots,\psi_n\}$do

② 选择 ϑ_i,V_i,ID_i;

③ 计算 $(\rho_j^{i'},T_i)=ID_i^{\mathrm{Fake}}\oplus H(V_i)\oplus H(ID_i)$;

④ 计算 $ID_i'^{\mathrm{Fake}}=\rho_j^{i'}\oplus H(V_i)\oplus H(ID_i)$;

⑤ if $T_i^{\mathrm{r}}-T_i\leqslant\tau$, $\rho_j^{i'}\in V_i$, $ID_i'^{\mathrm{Fake}}=ID_i^{\mathrm{Fake}}$;

⑥ 计算 $V'_i=\mu_i\oplus H(pk_i)\oplus H(\rho_j^{i'},ID_i)$;

⑦ 计算 $\mu'_i=V'_i\oplus H(pk_i)\oplus H(\rho_j^{i'},ID_i)$;

⑧ 计算 $Lab_i^{\mathrm{Sea}}=\eta_i\oplus H(pk_i)\oplus H(\rho_j^i,ID_i)\oplus H(V_i)$;

⑨ 计算 $\rho_j^i=Lab_i^{\mathrm{Sea}}\oplus H(V_i)$;

⑩ end if

⑪ if $V'_i=V_i$, $\mu'_i=\mu_i$, $\rho_j^{i'}=\rho_j^i$

⑫ 选择 pk_i 放入集合 PK;

⑬ end if

⑭ end for

DP 对拥有 ID_i^{Fake} 和 (pk_i,ϑ_i) 的 $\psi_1,\psi_2,\cdots,\psi_n$ 使用 *mSeaCodeVer* 算法, 行②~⑤为 DP 验证 ID_i^{Fake}, 若 $T_i^{\mathrm{r}}-T_i\leqslant\tau$, $ID_i'^{\mathrm{Fake}}=ID_i^{\mathrm{Fake}}$, T_i^{r} 为验证时间, $\rho_j^{i'}\in V_i$, $j\in\{1,2,\cdots,\lambda\}$, 在行⑥~⑩中计算 μ_i, η_i, Lab_i^{Sea} 以进一步验证. 在行⑪中若 $\mu'_i=\mu_i$, $V'_i=V_i$, $\rho_j^{i'}=\rho_j^i$. 在行⑫中将验证通过的水下自主机器人的公钥 pk_i 放入集合 PK 中. 同时 DP 获取了生成 $\psi_1,\psi_2,\cdots,\psi_n$ 对应 O_i 的属性 $\rho_j^{i'}$.

4)加密

算法 4. *SeaNTRU.mpPKE.mEnc* 算法.

① $m\in\mathcal{M}$;

② $PK=\{pk_{\psi_1},pk_{\psi_2},\cdots,pk_{\psi_n}\}$;

③ $\rho_j^{\mathrm{DP}}\leftarrow V_{\mathrm{DP}}$;

④ $r_{\mathrm{DP}}=H(m,\rho_j^{\mathrm{DP}})$;

⑤ for $i\in\{\psi_1,\psi_2,\cdots,\psi_n\}$ do

⑥ $m'_i=SeaTr(m,V_i,p_j^i)$;

⑦ $c_{1i}=mEnc^{ID_i^{\mathrm{Fake}}}(PK,r_{\mathrm{DP}})$;

⑧ $c_{2i}=m'_i\oplus H(r_{\mathrm{DP}},ID_i)_{ID_i^{\mathrm{Fake}}}$;

⑨ end for

⑩ $C=(c_1,c_2)$.

在行③中, DP 从 V_{DP} 中随机选取 ρ_j^{DP}, $j\in\{1,2,\cdots,\lambda\}$, 行④为 DP 利用 m 和 ρ_j^{DP} 生成随机数 r_{DP}. 行⑤~⑨中 DP 首先利用 V_i 和 *mSeaCodeVer* 中获取的 ρ_j^i 来使用 *SeaTr* 操作混淆 m, 其次使用 PK 执行 NTRU 加密, 然

后在加密中使用各个水下自主机器人的设备序列号ID_i进行身份绑定，DP 分别生成$\psi_1,\psi_2,\cdots,\psi_n$对应的密文分量$(c_{1\psi_1},c_{2\psi_1}),(c_{1\psi_2},c_{2\psi_2}),\cdots,(c_{1\psi_n},c_{2\psi_n})$并映射到伪身份$ID_i^{\text{Fake}}$相应的 OFDM 子载波上，行⑩是将不同子载波的密文分量聚合得到的密文 C 并通过 OFDM 发送给相应的水下自主机器人.

5)密文提取算法

算法 5. *SeaNTRU.mpPKE.mExt* 算法.

① 初始化 $Tag=0$;

② $\psi_1,\psi_2,\cdots,\psi_n$ select ID_i^{Fake};

③ if $ID_i'^{\text{Fake}}=ID_i^{\text{Fake}}$, $T_i^{\text{r}}-T_i\leqslant\tau$

④ Set $Tag=1$;

⑤ 从 c_1中提取c_{1i};

⑥ 从 c_2中提取 c_{2i};

⑦ return $C_i=(c_{1i},c_{2i})$;

⑧ end if

⑨ else if $Tag=0$

⑩ return $C_i^{\text{None}}=(c_{1i},c_{2i})$;

⑪ end if

其中行①是初始化标签$Tag=0$. 行②~④是$\psi_1,\psi_2,\cdots,\psi_n$对于密文 C 选择并验证伪身份ID_i^{Fake}和时间标记条件$T_i^{\text{r}}-T_i\leqslant\tau$的有效性，验证成功设置$Tag=1$. 行⑤~⑦是从$c_1$和$c_2$中提取相应伪身份子载波的密文，记为$C_i=(c_{1i},c_{2i})$, $i\in\{\psi_1,\psi_2,\cdots,\psi_n\}$. 行⑨⑩是如果验证失败，$Tag=0$, 无效密文为$C_i^{\text{None}}=(c_{1i},c_{2i})$.

6)解密

算法 6. *SeaNTRU.mpPKE.mDec* 算法.

① $r_{\text{DP}}=mDec^{ID_i^{\text{Fake}}}(sk_i,c_{1i})$;

② 计算 $m_i'=c_{2i}\oplus H(r_{\text{DP}},ID_i)$;

③ $m=UnSeaTr(m_i',V_i,p_j^i)$;

④ if $Tag=1$, $c_{2i}'=c_{2i}$

⑤ return m;

⑥ end if

⑦ else if $Tag=0$ or $c_{2i}'\neq c_{2i}$

⑧ return $\hat{m}_i$;

⑨ end if

在行①~③中，$\psi_1,\psi_2,\cdots,\psi_n$得到 m. 行④⑤中如果$Tag=1$, $c_{2i}'=c_{2i}$, 则输出 m. 行⑦⑧中如果$Tag=0$或者$c_{2i}'\neq c_{2i}$, 密文无效，输出不可区分的无关随机信息$\hat{m}_i$, 将$\hat{m}_i$输入方程$x(t)=\sum_{\varsigma\in Z_s}X(\varsigma)\times e^{j2\pi\frac{\varsigma}{T}t}\Pi(t)$, 得到的 OFDM 发射信号$x(\hat{m}_i)=\sum_{\varsigma\in Z_s}X(\varsigma)\times e^{j2\pi\frac{\varsigma}{T}\hat{m}_i}\Pi(\hat{m}_i)$作为系统的预警信号.

3.3 多方密钥封装算法

SeaNTRU 的多方密钥封装算法由 SeaFO 变换得到. 如果解封装成功，SeaFO 使用海洋信息m和随机数r_{DP}生成有效的会话密钥$K=H(m,r_{\text{DP}})$; 如果解封装失败，SeaFO 利用每个接收者生成的不同的海洋噪声O_i和解密失败生成的$\hat{m}_i$, 采用隐式拒绝的方式生成无效且随机的会话密钥$\hat{K}_i=H(\hat{m}_i,O_i)$. SeaNTRU 中$K=H(m,r_{\text{DP}})$服从$\{0,1\}^\lambda$分布，$\hat{K}_i$也服从$\{0,1\}^\lambda$分布. 那么$\hat{K}_i$是不可区分的，敌手难以从中推断任何关于封装密文的有效信息. 在本文的 SeaFO 中验证解封装结果只需要验证轻量级的海洋噪声和哈希运算部分$c_{2i}'=c_{2i}$，提升了方案的效率.

多方密钥封装算法也包含 6 个步骤. 其中，密钥生成、海洋声波消息码生成、海洋声波消息码验证、密文提取算法与 SeaNTRU 的多方公钥加密算法相同. 密钥封装和密钥解封装的步骤如下.

1)密钥封装

算法 7. *SeaNTRU.mpKEM. mEncaps* 算法.

① $m\leftarrow\mathcal{M}$;

② $C=SeaNTRU.mpPKE.mEnc(m,PK,V_i,p_j^i,ID_i)$;

③ $K=H(m,r_{\text{DP}})$;

④ DP 使用 *mpPKE.mEnc* 得到 C, 并使用 m 和r_{DP}生成会话密钥K.

2)密钥解封装

算法 8. *SeaNTRU. mpKEM. mDecaps* 算法.

① $m=SeaNTRU.mpPKE.mDec(C_i,sk_i,V_i,p_j^i,ID_i)$;

② if $Tag=1$, $c_{2i}'=c_{2i}$

③ return $K=H(m,r_{\text{DP}})$;

④ end if

⑤ else if $Tag=0$ or $c_{2i}'\neq c_{2i}$

⑥ return $\hat{K}_i=H(\hat{m}_i,O_i)$;

⑦ end if

在算法 8 行①中$\psi_1,\psi_2,\cdots,\psi_n$得到$m$. 行②③中若$Tag=1$, $c_{2i}'=c_{2i}$, 解封装成功输出会话密钥 K. 行⑤⑥中若$Tag=0$或$c_{2i}'\neq c_{2i}$, 那么封装密文无效，令$\hat{m}_i=m$, 发射预警信号$x(\hat{m}_i)$并生成无效且不可区分的会话密钥$\hat{K}_i$.

3.4 会话密钥更新机制

若时间标记的存在时间超过最长的海洋时延，即$T_i+\Delta T_i>\tau$, SeaNTRU 启动会话密钥更新机制，步骤如下：

1)水下自主机器人$\psi_1,\psi_2,\cdots,\psi_n$更新伪装序列号$ID_i^{\text{Fake}}$为$ID_i'^{\text{Fake}}$，并从$V_i$中获取新的水声声波因子$\rho_j^{i'}\leftarrow$

V_i, 其中 $i \in \{\psi_1,\psi_2,\cdots,\psi_n\}$, $j \in \{1,2,\cdots,\lambda\}$. $\psi_1,\psi_2,\cdots,\psi_n$执行 *MaforID* 操作, $ID_i'^{\text{Fake}} = MaForID(ID_i)$, 有

$$ID_i'^{\text{Fake}} = (\rho_j^{i'}, T_i') \oplus H(V_i) \oplus H(ID_i). \tag{18}$$

2)首先, 水下自主机器人$\psi_1,\psi_2,\cdots,\psi_n$生成新的$\mu_i'$, 有

$$\mu_i' = V_i \oplus H(pk_i') \oplus H(\rho_j^{i'}, ID_i), \tag{19}$$

然后, 生成新的η_i'和水声广播标签Lab_i^{Sea}嵌入η_i'中, 有

$$Lab_i^{\text{Sea}} = \rho_j^{i'} \oplus H(V_i), \tag{20}$$

$$\eta_i' = Lab_i^{\text{Sea}} \oplus H(pk_i') \oplus H(\rho_j^{i'}, ID_i) \oplus H(V_i), \tag{21}$$

最后, 生成新的海洋声波消息码

$$\vartheta_i' = (\mu_i', \eta_i'). \tag{22}$$

3)DP 通过海洋声波消息码验证算法验证ψ_1, $\psi_2,\cdots,\psi_n$的身份.

4)DP 使用新的海洋信息m'生成新的随机数$r'_{\text{DP}} = H(m', \rho_j'^{\text{DP}})$以及新的海洋噪声$O_i' = G(\rho_j^{i'}) \oplus G(V_i)$.

5)对于 DP 验证通过的水下自主机器人, 首先对信息组合$m_{\text{list}} = m' \| r'_{\text{DP}}$进行混淆操作, 得到混淆后的信息$m_i'' = SeaTr(m_{\text{list}}, O_i')$.

6)水面数据平台 DP 使用会话密钥K通过 SeaFO 变换运行封装算法得到新的封装密文C'和新的会话密钥K',

$$C' = mEncaps(K, m_{\psi_1}'', m_{\psi_2}'', \cdots, m_{\psi_n}'', r'_{\text{DP}})_{ID_{\psi_1}'^{\text{Fake}}, ID_{\psi_2}'^{\text{Fake}}, \cdots, ID'^{\text{Fake}}_{\psi_n}}, \tag{23}$$

$$K' = H(m', r'_{\text{DP}}). \tag{24}$$

7)DP 将封装密文C'的密文分量映射到不同的 OFDM 子载波上, 通过 OFDM 发送给水下自主机器人.

8)水下自主机器人ψ_i根据伪身份$ID_i'^{\text{Fake}}$分别从对应的 OFDM 子载波中提取各自的密文分量C_i', 使用会话密钥K解密得到m_i'', 并使用去混淆操作 *UnSeaTr* 得到m'和r'_{DP}.

9)水下自主机器人通过 SeaFO 变换解封装, 根据式(24)生成新的会话密钥K'.

在 SeaNTRU 的会话密钥更新机制中, 水下自主机器人利用 OFDM 子载波提取密文分量并进行伪身份和时间标记有效性的检验, 通过使用 SeaFO 变换解封装得到新的会话密钥, 不仅实现了多方环境下的隐式拒绝, 也防止了敌手对于 SeaNTRU 的自适应破坏.

SeaNTRU 考虑了水下物联网能量受限的问题. 设计 OFDM 频域过采样技术和 NTT 结合的密钥生成算法, 提高了密钥的采样精度和生成速度, SeaNTRU 的设计中主要是多项式和哈希运算保证了算法的轻量性, 同时提出了一种基于海洋噪声的 SeaFO 变换不需要全部的重加密过程, 提高了计算效率, 上述设计减少了能源消耗, 有效解决了水下物联网能量受限问题. 此外, SeaNTRU 也考虑了水下物联网的高延迟问题. 在海洋声波消息码验证、密文提取算法中都设置了海洋时延的限制, 当超过最长的海洋时延, 在海洋声波消息码验证算法中会停止操作, 在密文提取算法中会将密文标记为无效, 并且在会话密钥更新机制中加入了最长海洋时延的限制, 增强了机制的有效性.

4 方案分析

4.1 正确性

定理 2. 在水下物联网系统中, 如果存在信道多径衰减和水下多普勒效应$\delta' = (\delta + \delta_{\Delta f})(1 + \delta_o - \delta - \delta_{\Delta f})$, 则 SeaNTRU 是$\delta$正确的.

证明.

$$\begin{aligned}\delta' =& E\left[\max_{m\in\mathcal{M}} Pr[SeaNTRU.mDec(sk_i, O_i, ID_i, \right.\\ & \left. mEnc(pk_i, m, O_i, ID_i)) \neq m]\right] \leqslant 1 - \left(1 - \right.\\ & \left. E\left[\max_{r\in\{0,1\}^{\lambda}} Pr_{c_{1i}}\left[mDec(sk_i, mEnc(pk_i, r)) \neq r\right]\right]\right) \times \left(1 - \right.\\ & \left. E\left[\max_{m\in\{0,1\}^{\lambda}} Pr_{c_{2i}}[UnSeaTr(O_i, SeaTr(O_i, m)) \oplus H(r, ID_i) \neq \right.\right.\\ & \left.\left. m]\right]\right) = 1 - \left(1 - (\delta + \delta_{\Delta f})\right)\left(1 - (\delta + \delta_{\Delta f} - \delta_o)\right) = \\ & (\delta + \delta_{\Delta f})(1 + \delta_o - \delta - \delta_{\Delta f}) = \delta.\end{aligned} \tag{25}$$

证毕.

在不考虑水下环境时, 方案的解密失败取决于c_{1i}的解密错误率, SeaNTRU 基于混合加密的设计结构, 并结合身份绑定和属性绑定对于c_{2i}的解密错误率$\delta \to 0$, 此时 SeaNTRU 是δ正确的. 但是水声信道的多径衰减和多普勒效应会对数据信号的传输产生一定的频率偏移, 对于解密会产生一个偏移错误率$\delta_{\Delta f}$, 在不使用海洋噪声隐藏信息时$\delta'' = 1 - (1 - (\delta + \delta_{\Delta f}))^2$, 则对于 SeaNTRU 存在一个海洋噪声补偿率δ_o, 有$\delta < \delta''$.

4.2 安全性分析

4.2.1 IND-Anon-CPA 安全性

定理 3. 设 *SeaNTRU.mpPKE* 中存在注入性, H和G为量子随机预言机, 对于任意的量子 IND-Anon-CPA 敌手$\mathcal{A}$, 对H的量子查询深度最多为q_H, 对G的量子查询深度最多为q_G, 对解密预言机 *Dec* 至多存

在q_{Dec}次经典查询，同时存在任意的Ⅰ型敌手$\mathcal{A}1$发起自适应破坏攻击，则对于一个量子 OW-CPA 敌手$\mathcal{B}$，有

$$Adv^{\text{IND-Anon-CPA}}_{SeaNTRU.mpPKE}(\mathcal{A}) \leqslant 2q_N\sqrt{Adv^{\text{OW-CPA}}(\mathcal{B})+\zeta-\zeta_{\Delta o}}+Adv(\mathcal{A}1),$$

其中设$q_N=(q_H+q_G+q_{Dec})$.

证明.

1）游戏 G_1. 进行原始的 IND-Anon-CPA 游戏，通过ID_i^{Fake}实现 SeaNTRU 的匿名性，因此

$$\left|Pr[G_1^{\mathcal{A}}\Rightarrow 1]-\frac{1}{2}\right|=Adv^{\text{IND-Anon-CPA}}_{SeaNTRU.mpPKE}(\mathcal{A}). \tag{26}$$

2）游戏 G_2~G_6.

① for $i\in\{\psi_1,\psi_2,\cdots,\psi_n\}$, $j\in\{1,2,\cdots,\lambda\}$ do

② $H\leftarrow\{0,1\}^{\lambda}$; /* G_2 */

③ $r\leftarrow R$, $ID_i\leftarrow ID_{\text{id}}$, $V_i\leftarrow V_v$, $\rho_j^i\leftarrow V_i$;

④ $O_i=G(V_i)\oplus G(\rho_j^i)$, $s_i=H(r,ID_i)$; /*G_2*/

⑤ $G\leftarrow\{0,1\}^{\lambda}$, $O_i\leftarrow\{0,1\}^{\lambda}$; /* G_3~G_6*/

⑥ $H=\left(G(V_i,\rho_j^i)=O_i,G(r,ID_i)=s_i\right)$; /* G_3~G_6*/

⑦ $l\leftarrow\mathcal{A}_C^H\left(((V_i,\rho_j^i),O_i),((r,ID_i),s_i)\right)$; /*$G_2$~$G_3$*/

⑧ $l\leftarrow\mathcal{A}_C^G\left(((V_i,\rho_j^i),O_i),((r,ID_i),s_i)\right)$; /* G_4*/

⑨ $d\leftarrow Dec_1\left(((V_i,\rho_j^i),O_i),((r,ID_i),s_i)\right)$; /*$G_5$~$G_6$*/

⑩ return l; /*G_2~G_4*/

⑪ return $\left((V_i,\rho_j^i),(r,ID_i)\right)\in d$; /*$G_5$~$G_6$*/

⑫ end for

/*$\mathcal{A}_C\left(((V_i,\rho_j^i),O_i),((r,ID_i),s_i)\right)$*/

⑬ for $i\in\{\psi_1,\psi_2,\cdots,\psi_n\}$, $j\in\{1,2,\cdots,\lambda\}$ do

⑭ $pp\leftarrow mSetup(1^{\lambda})$, $(pk_i,sk_i)\leftarrow mKeyGen(pp)$;

⑮ $b\leftarrow\{0,1\}$; /*G_2~G_5*/

⑯ $V_i\leftarrow V_v$, $\rho_j^i\leftarrow V_i$, $O_i=H(\rho_j^i)\oplus H(V_i)$;

⑰ $m_b'=SeaTr(m_b,O_i)$; /*G_2~G_5*/

⑱ $m_b'\leftarrow\{0,1\}^{\lambda}$; /*$G_6$*/

⑲ $(c_{1i}^*,c_{2i}^*)\leftarrow(mEnc(pk_i,r),m_b'\oplus s_i)_{ID_i^{*\text{Fake}}}$;

⑳ $b'\leftarrow\mathcal{A}(pk_i,(c_{1i}^*,c_{2i}^*))$;

㉑ return $[b=b']$;

㉒ end for

/*Oracel $Dec_1\left(((V_i,\rho_j^i),O_i),((r,ID_i),s_i)\right)$*/

㉓ $j\leftarrow\{1,2,\cdots,q_H\}$;

㉔ run $\mathcal{A}_C\left(((V_i,\rho_j^i),O_i),((r,ID_i),s_i)\right)$ until j-th query;

㉕ $d\leftarrow$ measure G-query;

㉖ return d.

对于游戏 G_2 在$\mathcal{A}_C$的执行前查询$O_i=H(V_i)\oplus(\rho_j^i)$, $s_i=H(r,ID_i)$. 因为G_2相对于G_1的变化是理论性的，所以

$$Pr[G_1^{\mathcal{A}}\Rightarrow 1]=Pr[G_2^{\mathcal{A}}\Rightarrow 1]. \tag{27}$$

在游戏 G_3 中均匀地选择G和O_i, s_i. 同时，$H=(G(V_i,\rho_j^i)=O_i,G(r,ID_i)=s_i)$，这里的 H 和 G 是相同的哈希函数，H 和O_i, s_i有着相同的分布，因此

$$Pr[G_2^{\mathcal{A}}\Rightarrow 1]=Pr[G_3^{\mathcal{A}}\Rightarrow 1]. \tag{28}$$

游戏 G_4 中通过对 H, G 和解密预言机的查询并基于文献 [25] 中的 O2H 定理，可以得到

$$\left|Pr[G_3^{\mathcal{A}}\Rightarrow 1]-Pr[G_4^{\mathcal{A}}\Rightarrow 1]\right|\leqslant 2(q_H+q_G+q_{Dec})\sqrt{Pr[G_5\Rightarrow 1]}. \tag{29}$$

基于海洋噪声的 *SeaTr* 混淆操作，m_b'独立于m_b，所以$\mathcal{A}_C$中$\mathcal{A}$的输入与b'和 b 无关，有$b=b'$，因此

$$Pr[G_4^{\mathcal{A}}\Rightarrow 1]=\frac{1}{2}. \tag{30}$$

在游戏 G_5 和游戏 G_6 中，游戏 G_6 中对于m_b', $m_b'\leftarrow\{0,1\}^{\lambda}$. 游戏 G_5 中对于 *SeaTr* 中的O_i, $O_i\leftarrow\{0,1\}^{\lambda}$. 则游戏 G_5 中的m_b'服从$\{0,1\}^{\lambda}$.

$$Pr[G_5^{\mathcal{A}}\Rightarrow 1]=Pr[G_6^{\mathcal{A}}\Rightarrow 1]. \tag{31}$$

3）游戏 G_7~G_8.

① for $i\in\{\psi_1,\psi_2,\cdots,\psi_n\}$, $j\in\{1,2,\cdots,\lambda\}$ do

② $(pk_i,sk_i)\leftarrow mKeyGen(pp)$, $m\leftarrow\{0,1\}^{\lambda}$

③ $V_i\leftarrow\{-1,0,1\}^{\lambda}$, $\rho_j^i\leftarrow V_i$, $ID_i\leftarrow\{0,1\}^{\lambda}$, $r\leftarrow\{0,1\}^{\lambda}$;

④ $(c_{1i}^*,c_{2i}^*)=SeaNTRU.mEnc(m,pk_i,V_i,p_j^i,ID_i)_{ID_i^{\text{Fake}^*}}$;

⑤ $d\leftarrow mEnc(pk_i,(c_{1i}^*,c_{2i}^*))$; /*$G_7$*/

⑥ $m_b'\leftarrow\mathcal{B}(pk_i,(c_{1i}^*,c_{2i}^*))$; /*$G_8$*/

⑦ return $\left((V_i,\rho_j^i),(r,ID_i)\right)\in d$; /*$G_7$*/

⑧ return $[m'=m_b']$; /*G_8*/

⑨ end for

/*$\mathcal{B}(pk_i,(c_{1i}^*,c_{2i}^*))$*/

⑩ for $i\in\{\psi_1,\psi_2,\cdots,\psi_n\}$ do

⑪ $d\leftarrow mEnc(pk_i,(c_{1i}^*,c_{2i}^*))$;

⑫ if $((V_i,\rho_j^i),(r,ID_i))\in d$

⑬ if $m'=SeaNTRU.mDec(sk_i,(c_{1i}^*,c_{2i}^*))_{ID_i^{*\text{Fake}}}$, $m'\in\mathcal{M}$;

⑭ return m';

⑮ end if

⑯ else

⑰ return $m'\leftarrow\{0,1\}^{\lambda}$;

⑱ end if

⑲ end for

游戏 G_7 在游戏 G_8 的构造上进行定义，因此

$$Pr[G_6^{\mathcal{A}}\Rightarrow 1]=Pr[G_7^{\mathcal{A}}\Rightarrow 1]. \tag{32}$$

在游戏 G_8 的 $\mathcal{B}(pk_i,(c_{1i}^*,c_{2i}^*))$中，由定义 6，对于 SeaNTRU，若$(c_{1i}^*,c_{2i}^*)=(c_{1i}',c_{2i}')$且$(m,r)\neq(m',r')$，则发生注入性破坏，有

$$\left|Pr[G_7^{\mathcal{A}}\Rightarrow 1]-Pr[G_8^{\mathcal{A}}\Rightarrow 1]\right|\leqslant\zeta-\zeta_{\Delta o},\tag{33}$$

其中注入性破坏概率的可能性从ζ减小为$\zeta-\zeta_{\Delta o}$的原因是引入V_i，ρ_j^i，ID_i，O_i，通过属性绑定和身份绑定，使得加密结果不仅仅取决于 m 和 r.

在游戏 G_8 如果存在$((V_i,\rho_j^i),(r,ID_i))\in d$，并且有$m^*\in M$为$(c_{1i}^*,c_{2i}^*)$的解，敌手$\mathcal{B}$获胜，有

$$Adv_{SeaNTRU.mpPKE}^{\text{IND-Anon-CPA}}(\mathcal{A})\leqslant 2q_N\sqrt{Adv^{\text{OW-CPA}}(\mathcal{B})+\zeta-\zeta_{\Delta o}}.\tag{34}$$

4）游戏 G_9.

① for $i\in\{\psi_1,\psi_2,\cdots,\psi_n\}$ do

② 选择ID_i^{Fake};

③ modify $(C_{ID_{\psi_1}^{\text{Fake}}},C_{ID_{\psi_2}^{\text{Fake}}},\cdots,C_{ID_{\psi n}^{\text{Fake}}})$ to $(C_{ID_{\psi_1}^{\text{Fake}}},C_{ID_{\psi_2}^{\text{Fake}}},\cdots,\hat{C}_{ID_{\psi n}^{\text{Fake}}})$;

④ return $(C_{ID_{\psi_1}^{\text{Fake}}},C_{ID_{\psi_2}^{\text{Fake}}},\cdots,\hat{C}_{ID_{\psi n}^{\text{Fake}}})$;

⑤ end for

/*Oracel $Dec_2\left(C_{ID_{\psi_1}^{\text{Fake}}},C_{ID_{\psi_2}^{\text{Fake}}},\cdots,\hat{C}_{ID_{\psi n}^{\text{Fake}}}\right)$*/

⑥ for $i\in\{\psi_1,\psi_2,\cdots,\psi_n\}$ do

⑦ 选择ID_i^{Fake};

⑧ if $ID_i'^{\text{Fake}}=ID_i^{\text{Fake}}$, $T_i^{\text{r}}-T_i\leqslant\tau$

⑨ $m'=SeaNTRU.mDec(sk_i,C_{ID_i^{\text{Fake}}})$;

⑩ if $c_{2i}'=c_{2i}$

⑪ return m';

⑫ end if

⑬ else

⑭ return $\hat{m}_i$, $x(\hat{m}_i)$;

⑮ end if

⑯ end for

游戏 G_9 是Ⅰ型敌手$\mathcal{A}_1$的自适应破坏游戏，$\mathcal{A}_1$截获$(C_{ID_{\psi_1}^{\text{Fake}}},C_{ID_{\psi_2}^{\text{Fake}}},\cdots,C_{ID_{\psi n}^{\text{Fake}}})$，在匿名性的情况下，假设$\mathcal{A}_1$将$C_{ID_{\psi n}^{\text{Fake}}}$修改为$\hat{C}_{ID_{\psi n}^{\text{Fake}}}$，得到$(C_{ID_{\psi_1}^{\text{Fake}}},C_{ID_{\psi_2}^{\text{Fake}}},\cdots,\hat{C}_{ID_{\psi n}^{\text{Fake}}})$，通过$ID_i'^{\text{Fake}}=ID_i^{\text{Fake}}$，$T_i^{\text{r}}-T_i\leqslant\tau$，$c_{2i}'=c_{2i}$的验证以及会话密钥更新机制的应用来防止$\mathcal{A}_1$对于 SeaNTRU 的自适应破坏并产生$\hat{m}_i$和预警信号$x(\hat{m}_i)$，如果$\mathcal{A}_1$通过解密预言机获得$m'$则赢得 G_9，$\mathcal{A}_1$的优势为

$$Adv(\mathcal{A}_1)=\left|Pr\left[m'\leftarrow Dec_2\left(C_{ID_{\psi_1}^{\text{Fake}}},C_{ID_{\psi_2}^{\text{Fake}}},\cdots,\hat{C}_{ID_{\psi n}^{\text{Fake}}}\right)\right]-\frac{1}{2}\right|.\tag{35}$$

由游戏 G_8 和游戏 G_9，得到最终结果为

$$Adv_{SeaNTRU.mpPKE}^{\text{IND-Anon-CPA}}(\mathcal{A})\leqslant 2q_N\sqrt{Adv^{\text{OW-CPA}}(\mathcal{B})+\zeta-\zeta_{\Delta o}}+Adv(\mathcal{A}_1).\tag{36}$$

在水下物联网的多方环境中，敌手可以通过产生多个无效密文以及通过观察解密结果来推测真实明文信息. 在本文的 *SeaNTRU.mpPKE* 中利用匿名性通过伪身份ID_i^{Fake}作为每个接收者密文分量的密文索引，敌手无法通过密文索引来推断密文接收者的信息，当敌手产生并添加无效密文时，接收方通过ID_i^{Fake}、时间标记T_i以及对密文分量c_{2i}的验证，可以发现无效密文证明了多方公钥加密算法是抗自适应破坏的，同时也证明了基于此的会话密钥更新机制也是抗自适应破坏的. 如果发生解密失败，不会反馈解密失败的信息. 而是如算法 6 的⑦⑧中产生一个与 m 无关且随机的$\hat{m}_i$并产生信号$x(\hat{m}_i)$，由定理 3 可知，m 服从$\{0,1\}^{\lambda}$分布，$m^*\oplus H(r,ID_i)$服从$\{0,1\}^{\lambda}$分布，则产生的$\hat{m}_i$服从$\{0,1\}^{\lambda}$分布，那么$\hat{m}_i$是不可区分的，敌手无法通过$\hat{m}_i$来推断 m 和解密多项式的任何信息.

证毕.

4.2.2 IND-Anon-CCA 安全性

定理 4. 如果 *SeaNTRU.mpPKE* 满足下面的条件

$$E\left[\max_{m\in\mathcal{M}}Pr[SeaNTRU.mEnc(m,pk_i,V_i,p_j^i,ID_i)=ct]\right]\leqslant 2^{-(\gamma+\gamma_o)}=2^{-\gamma_{\text{Sea}}},$$

则 *SeaNTRU.mpPKE* 是γ_{Sea}扩散的.

证明. 对于确定的 m 和ct_i，$i\in\{\psi_1,\psi_2,\cdots,\psi_n\}$，接收者每次的密文分量至多分别存在一个$V_i$，$p_j^i$，$ID_i$，$r$，使得$mEnc(m,PK,V_i,p_j^i,ID_i)=ct$.

假设有V_i，p_j^i，ID_i，r和V_i'，$p_j^{i'}$，ID_i'，r'，存在$mEnc(m,pk_i,V_i,p_j^i,ID_i)=mEnc(m,pk_i,V_i',p_j^{i'},ID_i')$.

那么$O_i\oplus m\oplus H(r,ID_i)=O_i'\oplus m\oplus H(r',ID_i')$，由身份和属性绑定有$V_i\neq V_i'$，$p_j^i\neq p_j^{i'}$，$ID_i\neq ID_i'$，$r\neq r'$，则对于每一次的$ct_i$至多分别存在一个$V_i$，$p_j^i$，$ID_i$，$r$满足$mEnc(m,PK,V_i,p_j^i,ID_i)=ct$.

SeaNTRU 中使用混合加密、身份以及属性的绑定，同时引入海洋噪声. 对于 m，最大化最小熵，使得$\gamma(pk_i,m)\geqslant(\gamma+\gamma_o)=\gamma_{\text{Sea}}$，有$\gamma_{\text{Sea}}(pk_i,m)\geqslant\gamma_{\text{Sea}}$，$\gamma_o$为最小熵的增加量. 可以得到

$$E\left[\max_{m\in\mathcal{M}}Pr[SeaNTRU.mEnc(m,pk_i,V_i,p_j^i,ID_i)=ct]\right]\leqslant 2^{-\gamma_{\text{Sea}}}.\tag{37}$$

对于任意的$(pk_i,sk_i)\leftarrow mKeyGen(1^{\lambda})$成立，所以 *SeaNTRU.mpPKE* 是$\gamma_{\text{Sea}}$扩散的. 证毕.

定理 5. *SeaNTRU.mpPKE* 是δ正确、γ_{Sea}扩散且存在注入性的. 对于任意的量子 IND-Anon-CCA 敌手$\mathcal{A}$，H和 G 为量子随机预言机，对H发出至多q_H次量子查询，对 G 至多发出q_G次量子查询. 最多向解封装预言机$Decap$发出q_{Decap}次经典查询，同时存在任意的Ⅰ型

敌手$\mathcal{A}_1$发起自适应破坏，则对于一个量子 IND-Anon-CPA 敌手$\mathcal{B}$，有

$$Adv^{\text{IND-Anon-CCA}}_{SeaNTRU.mpKEM}(\mathcal{A}) \leqslant 4q_N\sqrt{Adv^{\text{IND-Anon-CPA}}_{SeaNTRU.mpPKE}(\mathcal{B})+\zeta-\zeta_{\Delta o}}+ q_{N_1}\times\sqrt{\delta}+q_{Decap}\times\sqrt{2^{-\gamma_{\text{Sea}}}}+Adv(\mathcal{A}_1),$$

其中设$q_N = q_H + q_G + q_{Dec}$，$q_{N_1} = q_H + q_G + 2q_{Dec}$.

证明. 游戏 G_1 是 IND-Anon-CCA 的原始游戏，在匿名性的条件下构造，因此

$$\left|Pr[G_1^{\mathcal{A}} \Rightarrow 1]-\frac{1}{2}\right| = Adv^{\text{IND-Anon-CCA}}_{SeaNTRU.mpKEM}(\mathcal{A}). \tag{38}$$

游戏 G_2 中在通过$ID_i^{\text{Fake}}(i\in\{\psi_1,\psi_2,\cdots,\psi_n\})$对$Decap$查询之前，将查询失败的结果置为隐式拒绝的形式$H(\hat{m}_i, O_i)$，游戏的变化是概念性的有

$$Pr[G_1^{\mathcal{A}} \Rightarrow 1] = Pr[G_2^{\mathcal{A}} \Rightarrow 1]. \tag{39}$$

游戏 G_3 中判断V_i'，$p_j^{i'}$，ID_i'，r'使用的正确性，对于C_i查询$Decap$，若$m' \neq SeaNTRU.mDec(C_i, sk_i, V_i, p_j^i, ID_i)$，则记录该错误，发生的概率为$\delta$，在量子随机预言机中对 G_2 和 G_3 有

$$\left|Pr[G_2^{\mathcal{A}} \Rightarrow 1]-Pr[G_3^{\mathcal{A}} \Rightarrow 1]\right| \leqslant (q_H+q_G+2q_{Decap})\times\sqrt{\delta}. \tag{40}$$

游戏 G_4 的游戏类似定理 3 中 G_3 和 G_4 的游戏，通过 H 和 G 之间的切换，以及对 H, G, $Decap$的查询通过 O2H 定理有

$$\left|Pr[G_3^{\mathcal{A}} \Rightarrow 1]-Pr[G_4^{\mathcal{A}} \Rightarrow 1]\right| \leqslant 2(q_H+q_G+q_{Dec})\sqrt{Pr[G_5 \Rightarrow 1]}, \tag{41}$$

其中游戏 G_5 是 G_2 和 G_3 游戏的结合，游戏中允许敌手任意查询量子随机预言机和$Decap$. SeaNTRU 通过海洋噪声和哈希运算进行解封装的验证，则对于敌手有

$$Adv^{\text{IND-Anon-CCA}}_{SeaNTRU.mpKEM}(\mathcal{A}) \leqslant 4q_N\sqrt{Adv^{\text{IND-Anon-CPA}}_{SeaNTRU.mpPKE}(\mathcal{B})}+q_{N_1}\times\sqrt{\delta}. \tag{42}$$

游戏 G_6 中将(pk_i, m)和(pk_i', m)通过$ID_{\psi_1}^{\text{Fake}}, ID_{\psi_2}^{\text{Fake}}, \cdots, ID_{\psi_n}^{\text{Fake}}$对$Decap$进行查询，利用$C_i$和$m = SeaNTRU.mDec(C_i, sk_i)$进行判断，如果$(pk_i, m)$和$(pk_i', m)$均不在 SeaNTRU 中，返回隐式拒绝结果$H(\hat{m}_i, O_i)$给敌手，结果是不可区分的. 通过$\gamma_{\text{Sea}}$扩散性，选择$ct$使得$SeaNTRU.mEnc(m, pk_i, V_i, p_j^i, ID_i) = ct$的概率上界为$2^{-\gamma_{\text{Sea}}}$，那么在量子随机预言机中有

$$\left|Pr[G_5^{\mathcal{A}} \Rightarrow 1]-Pr[G_6^{\mathcal{A}} \Rightarrow 1]\right| \leqslant q_{Decap}\times\sqrt{2^{-\gamma_{\text{Sea}}}}. \tag{43}$$

游戏 G_7 中通过检查(pk_i, m)和(pk_i', m)的所有输入，检查$C_i = (c_{1i}, c_{2i})$回应$Decap$的查询，若成功，输出$H(m, r_{\text{DP}})$；否则，返回隐式拒绝的结果$H(\hat{m}_i, O_i)$. 对于 G_6 和 G_7 的游戏通过 SeaNTRU 中伪身份ID_i^{Fake}、时间标记T_i、解封装的验证以及预警信号和会话密钥更新机制的使用，若出现无效密文分量C_i，则对于整个C，游戏 G_6 和 G_7 返回隐式拒绝的结果$H(\hat{m}_i, O_i)$是不可区分的.

$$Pr[G_6^{\mathcal{A}} \Rightarrow 1] = Pr[G_7^{\mathcal{A}} \Rightarrow 1]. \tag{44}$$

游戏 G_8 中敌手进行$m^* \leftarrow \{0,1\}^\lambda$，$V_i^* \leftarrow \{-1,0,1\}^\lambda$，$\rho_j^{i*} \leftarrow V_i^*$，$ID_i^* \leftarrow \{0,1\}^\lambda$，$r^* \leftarrow \{0,1\}^\lambda$，生成$C_i^*$=$SeaNTRU.mEnc(m^*, pk_i, V_i^*, p_j^{i*}, ID_i^*)$和$K^*$，这不会对敌手产生改变，因此

$$Pr[G_7^{\mathcal{A}} \Rightarrow 1] = Pr[G_8^{\mathcal{A}} \Rightarrow 1]. \tag{45}$$

游戏 G_9 中敌手进行密文查询，获取V_i^*，ρ_j^{i*}，ID_i^*，r^*，K^*的信息，通过 SeaNTRU 中会话密钥更新机制和验证过程对于无效密文的处理，产生的K_0^*和K_1^*对于敌手是不可区分的，因此

$$Pr[G_9^{\mathcal{A}} \Rightarrow 1] = \frac{1}{2}. \tag{46}$$

此外 G_8 和 G_9 使用相同的 H 生成K^*，则 G_8 和 G_9 的结果是不可区分的.

$$Pr[G_8^{\mathcal{A}} \Rightarrow 1] = Pr[G_9^{\mathcal{A}} \Rightarrow 1]. \tag{47}$$

游戏 G_{10} 是注入性破坏的游戏，同定理 3 中的 G_8. 游戏 G_{10} 在游戏 G_9 的基础上进行，则

$$\left|Pr[G_9^{\mathcal{A}} \Rightarrow 1]-Pr[G_{10}^{\mathcal{A}} \Rightarrow 1]\right| \leqslant \zeta-\zeta_{\Delta o}. \tag{48}$$

游戏 G_{11} 同定理 3 中的 G_9 是 Ⅰ 型敌手$\mathcal{A}_1$的自适应破坏游戏，同样需要验证过程和会话密钥更新机制的使用，$\mathcal{A}_1$赢得游戏的优势

$$Adv(\mathcal{A}_1) = \left|Pr\left[m' \leftarrow Decap\left(C_{ID_{\psi_1}^{\text{Fake}}}, C_{ID_{\psi_2}^{\text{Fake}}}, \cdots, C_{ID_{\psi_n}^{\text{Fake}}}\right)\right]-\frac{1}{2}\right|. \tag{49}$$

通过以上的游戏，得到

$$Adv^{\text{IND-Anon-CCA}}_{SeaNTRU.mpKEM}(\mathcal{A}) \leqslant 4q_N\sqrt{Adv^{\text{IND-Anon-CPA}}_{SeaNTRU.mpPKE}(\mathcal{B})+\zeta-\zeta_{\Delta o}}+ q_{N_1}\times\sqrt{\delta}+q_{Decap}\times\sqrt{2^{-\gamma_{\text{Sea}}}}+Adv(\mathcal{A}_1). \tag{50}$$

证毕.

通过提出的 SeaFO 变换以及在量子随机预言机下证明 SeaNTRU 的 IND-Anon-CCA 安全性，当敌手通过产生多个无效密文导致 SeaNTRU 解封装失败时，水下自主机器人会生成随机信息和对应的海洋噪声，采用隐式拒绝的方式生成无效且不可区分的会话密钥$\hat{K}_i = H(\hat{m}_i, O_i)$并发射预警信号$x(\hat{m}_i)$，$\hat{K}_i$和有效的会话密钥$K = H(m, r_{\text{DP}})$都服从$\{0,1\}^\lambda$分布，则$\hat{K}_i$和$K$是不可区分的，使得敌手难以通过解封装失败获取任何可以解封装密文的信息. 此外，会话密钥更新机制和其中密文提取过程的有效性验证以及 SeaFO 变换的使用，不仅实现了多方环境下的隐式拒绝，也防止了敌手对于 SeaNTRU 的自适应破坏.

4.2.3 抗公钥替换攻击

定理 6. 设存在Ⅱ型敌手$\mathcal{A}_2$可以替换系统中的公钥pk_i, 并伪造ID_i^{Fake}和ϑ_i. 在量子随机预言机下 Sea-NTRU 对于任意的敌手$\mathcal{A}_2$存在不可伪造性和不可替换性.

证明. 设挑战者C_{g}根据$\mathcal{A}_2$的请求模拟ID_i^{Fake}和ϑ_i的生成, 敌手$\mathcal{A}_2$可以自适应进行如下查询. 其中$i\in\{\psi_1,\psi_2,\cdots,\psi_n\}$, $j\in\{1,2,\cdots,\lambda\}$.

1) *Setup-query*. 设C_{g}拥有列表$L^{Setup}=\{ID_i^{\text{Fake}},Setup(ID_i^{\text{Fake}})\}$, 输入$ID_i^{\text{Fake}}$, C_{g}在L^{Setup}查询成功, C_{g}返回$Setup(ID_i^{\text{Fake}})$给$\mathcal{A}_2$; 如果失败, C_{g}执行$Setup()\leftarrow R_q$将其存储在L^{Setup}, 返回结果给$\mathcal{A}_2$.

2) *KeyGen-query*. C_{g}的列表$L^{KeyGen}=\{ID_i^{\text{Fake}},KeyGen(ID_i^{\text{Fake}})\}$, 输入$ID_i^{\text{Fake}}$, 查询$L^{KeyGen}$成功, 返回$KeyGen(ID_i^{\text{Fake}})$给$\mathcal{A}_2$; 若查询失败, C_{g}执行$KeyGen()\leftarrow Setup()$, 将其存储在$L^{KeyGen}$, 返回结果给$\mathcal{A}_2$.

3) $H(V_i)$, $H(p_j^i)$-*query*. C_{g}的列表$L^V=\{ID_i^{\text{Fake}},V_i\}$, 输入$ID_i^{\text{Fake}}$, 查询$L^V$成功, $p_j^i\leftarrow V_i$, 返回V_i和p_j^i给$\mathcal{A}_2$; 若查询失败, C_{g}则执行$\hat{V}_i\leftarrow\{-1,0,1\}^{\lambda}$, $\hat{p}_j^i\leftarrow\hat{V}_i$, 将$\hat{V}_i$存储在$L^V$, 结果返回给$\mathcal{A}_2$.

4) $H(ID_i)$-*query*. C_{g}的列表$L^{ID}=\{ID_i^{\text{Fake}},ID_i\}$, 输入$ID_i^{\text{Fake}}$, 查询$L^{ID}$成功, 返回$ID_i$给$\mathcal{A}_2$; 若查询失败, C_{g}则执行$\hat{ID}_i\leftarrow\{0,1\}^{\lambda}$, 将$\hat{ID}_i$存储在$L^{ID}$, 结果返回给$\mathcal{A}_2$.

5) T_i-*query*. C_{g}的列表$L^T=\{ID_i^{\text{Fake}},T_i\}$, 输入$ID_i^{\text{Fake}}$, 查询$L^T$成功, 返回$T_i$给$\mathcal{A}_2$; 若失败, C_{g}随机产生$\hat{T}_i$, 将$\hat{T}_i$存储在L^T, 结果返回给$\mathcal{A}_2$.

6) *forgery-ID*$_i$-*query*. C_{g}查询列表L^{Setup}, L^{KeyGen}, L^V, L^{ID}, L^T, 执行$ID_i^{*\text{Fake}}=(p_j^{i*},T_i^*)\oplus H(V_i^*)\oplus H(ID_i^*)$, 返回给$\mathcal{A}_2$.

7) 公钥替换. 通过*KeyGen*()生成新公钥pk_i', 输入ID_i^{Fake}, C_{g}查询ID_i^{Fake}, 将ID_i^{Fake}的pk_i替换为pk_i', C_{g}记录替换.

8) *forgery-*ϑ. 设敌手$\mathcal{A}_2$具有一个不可忽略的概率伪造ϑ_i, $p_j^{i*}\leftarrow V_i^*$, $\mu_i^*=V_i^*\oplus H(pk_i')\oplus H(p_j^{i*},ID_i^*)$, $Lab_i^{*\text{Sea}}=\rho_j^{i*}\oplus H(V_i^*)$, $\eta_i^*=Lab_i^{*\text{Sea}}\oplus H(pk_i')\oplus H(p_j^{i*},ID_i^*)\oplus H(V_i^*)$, $\vartheta_i^*=(\mu_i^*,\eta_i^*)$.

对于$Cod_1=\{ID_i^{*\text{Fake}},pk_i',\vartheta_i^*\}$, 验证$ID_i^{*\text{Fake}}$,

① $(p_j^{i*},T_i^*)=ID_i^{*\text{Fake}}\oplus H(V_i^*)\oplus H(ID_i^*)$;

② $ID_i'^{\text{Fake}}=(p_j^{i*},T_i^*)\oplus H(V_i)\oplus H(ID_i)$;

③ if $ID_i'^{\text{Fake}}=ID_i^{*\text{Fake}}$

④ return true;

⑤ else

⑥ return false;

⑦ end if

Cod_1是第 1 种情况, 即敌手伪造得到$ID_i^{*\text{Fake}}$并且将公钥替换为pk'. 行①为验证方计算$ID_i^{*\text{Fake}}$得到(p_j^{i*},T_i^*). 行②为重新计算得到$ID_i'^{\text{Fake}}$. 行③~⑥为结果检验, 若$ID_i'^{\text{Fake}}=ID_i^{*\text{Fake}}$则当前水下自主机器人的身份是可信的并进入$Cod_2$的验证, 否则身份不可信, 过程中止.

对于$Cod_2=\{ID_i^{\text{Fake}},pk_i',\vartheta_j^*\}$, 验证$\vartheta_i^*$,

① $p_j^{i'}\in V_i$, $ID_i'^{\text{Fake}}=ID_i^{\text{Fake}}$;

② if $T_i^{\text{r}}-T_i>\tau$, 中止验证过程;

③ end if

④ $V_i'=\mu_i^*\oplus H(pk_i')\oplus H(p_j^{i'},ID_i)$;

⑤ $Lab_i'^{*\text{Sea}}=\eta_i^*\oplus H(pk_i')\oplus H(\rho_j^{i*},ID_i^*)\oplus H(V_i^*)$;

⑥ $\hat{\rho}_j^{i*}=Lab_i'^{*\text{Sea}}\oplus H(V_i)$;

⑦ if $V_i'=V_i$, $\hat{\rho}_j^{i*}=\rho_j^{i'}$, $\hat{\rho}_j^{i*}\in V_i$, $\vartheta_i'=\vartheta_i^*$

⑧ return true;

⑨ else

⑩ retrun false;

⑪ end if

Cod_2是第 2 种情况, 即敌手保持ID_i^{Fake}不变, 只将公钥替换为pk'. 行①中ID_i^{Fake}相同且计算得到的水声声波因子$p_j^{i'}\in V_i$. 行②为验证ID_i^{Fake}的时间标记T_i, 如果$T_i^{\text{r}}-T_i>\tau$则中止验证过程. 行④为验证方计算μ_i^*得到海洋传感器声波序列V'. 行⑤是验证方计算η_i^*得到水声广播标签$Lab_i'^{*\text{Sea}}$. 行⑥是验证方计算$Lab_i'^{*\text{Sea}}$得到$\hat{\rho}_j^{i*}$. 行⑦~⑪是结果的验证过程, 如果同时满足V'与验证方拥有的V_i匹配$\hat{\rho}_j^{i*}$和$\rho_j^{i'}$相等并且$\hat{\rho}_j^{i*}$在对应的V_i中以及重新运算的ϑ'与ϑ_i^*相等, 那么当前验证的海洋声波消息码是可信的, 否则海洋声波消息码是伪造并且不可信的.

在量子随机预言机下对于任意敌手$\mathcal{A}_2$伪造ID_i^{Fake}的时间复杂度为$O\left(3^{\lambda}+2^{\frac{\alpha}{2}}+\beta\right)$, ID_i^{Fake}伪造成功的概率可表示为

$$\varepsilon_1\leqslant\left(\frac{1}{3^{\lambda}}\times\frac{1}{\beta}\right)\times\left(\frac{1}{2}-\frac{1}{\Theta}\right)^{\frac{\alpha}{2}}\times\left(\frac{1}{2}-\frac{1}{\Theta}\right)^{\frac{\alpha}{2}}\leqslant\left(\frac{1}{3^{\lambda}\beta}\right)\times\left(\frac{\Theta-2}{2\Theta}\right)^{\alpha},\tag{51}$$

其中α为 SHA-3 的安全参数, β是常量级系数, $\frac{1}{\Theta}$是对 SHA-3 中海绵结构设计的考虑, $\left(\frac{1}{2}-\frac{1}{\Theta}\right)$越小则敌手攻击成功的概率越低.

同理, 任意敌手$\mathcal{A}_2$伪造ϑ_i的时间复杂度为$O\times\left(3^{\lambda^2}+3^{\lambda}+2^{\frac{\alpha}{2}}\right)$, 替换公钥并且伪造$\vartheta_i$成功的概率为

$$\varepsilon_2 \leqslant \left(\frac{1}{3^{\lambda^2}}\times\left(\frac{1}{2}-\frac{1}{\Theta}\right)^{\frac{\alpha}{2}}\right)\times\left(\frac{1}{3^{\lambda}}\times\left(\frac{1}{2}-\frac{1}{\Theta}\right)^{\frac{\alpha}{2}}\times\left(\frac{1}{2}-\frac{1}{\Theta}\right)^{\frac{\alpha}{2}}\right)\leqslant\left(\frac{1}{3^{\lambda^2+\lambda}}\right)\times\left(\frac{\Theta-2}{2\Theta}\right)^{\frac{3\alpha}{2}}. \tag{52}$$

因此，在量子随机预言机下 SeaNTRU 对于任意的敌手$\mathcal{A}_2$存在不可伪造性和不可替换性. 证毕.

4.2.4 抗重放攻击

对于任意的Ⅲ型敌手$\mathcal{A}_3$，采用 SeaNTRU 的会话密钥更新机制进行验证. 如果验证得到伪身份$ID_{\mathrm{u}}^{\mathrm{Fake}}\neq ID_{\mathrm{u}}^{r\mathrm{Fake}}$或者验证时间和时间标记的差值超过最长海洋时延即$T_{\mathrm{u}}^{r}-T_{\mathrm{u}}^{\prime}>\tau$，则将当前封装密文标记为无效，说明 SeaNTRU 是抗重放攻击的.

4.2.5 抗中间人攻击

对于任意的Ⅳ型敌手$\mathcal{A}_4$，由于 SeaNTRU 具备匿名性、抗公钥替换攻击的特性，使得敌手假冒水下自主机器人$\psi_1,\psi_2,\cdots,\psi_n$向 DP 发送消息是困难的. 如果敌手伪装 DP 向$\psi_1,\psi_2,\cdots,\psi_n$发送消息，则$\psi_1,\psi_2,\cdots,\psi_n$在去海洋噪声混淆操作中或者在基于海洋噪声和哈希运算的验证中会发生批量错误，因此 SeaNTRU 是抗中间人攻击的.

4.3 复杂度分析

4.3.1 计算复杂度

表 1 列出了文献 [20, 23] 和 SeaNTRU 的多方密钥封装方案的计算复杂度. 文献 [20, 23] 的方案中，计算复杂度主要来源于密钥封装过程中$n\times n$维矩阵和n维向量的乘法运算，其计算复杂度为$O(n^2)$. 此外，密钥解封装过程中矩阵减法运算的计算复杂度为$O(n^2)$. 因此，方案的总体复杂度为$O(n^2)$. SeaNTRU 的计算复杂度主要来源于封装和解封装过程中多项式的求模运算，通过使用 NTT 加速，其总体计算复杂度为$O(n\log n)$.

Table 1 Comparison of Computational Complexity

表 1 计算复杂度比较

方案	计算复杂度
文献 [20]	$O(n^2)$
文献 [23]	$O(n^2)$
SeaNTRU（本文）	$O(n\log n)$

注：n 表示维数.

4.3.2 通信复杂度

表 2 列出了文献 [20, 23] 和 SeaNTRU 的多方密钥封装方案的通信复杂度. 文献 [20] 中的通信复杂度主要包括公开参数的使用$O((en+n)|z_q|)$、发送方与接收方之间公钥的通信$O(en|z_q|)$、发送方将封装后的密文给接收方$O(3en|z_q|)$、会话密钥的通信$|z_q|$，则通信复杂度$O((5en+n)|z_q|+|z_q|)$. 文献 [23] 中的通信复杂度主要来源于公开参数的使用$O((en+n)|z_q|)$、发送方与接收方之间公钥的通信$O(e(n+1)|z_q|)$、发送方将封装后的密文发送给接收方$O(e(4n+1)|z_q|)$、会话密钥的通信$O(|z_q|)$，因此总体通信复杂度为$O((6en+n+2+e)|z_q|)$. SeaNTRU 的通信复杂度主要来源于公开参数的使用$O((en+n)|r_q|)$、发送方与接收方之间公钥的通信$O(en|r_q|)$、发送方将封装后的密文发送给接收方$O(2en|r_q|)$、会话密钥的通信$O(|r_q|)$，因此总体通信复杂度为$O((4en+n+1)|r_q|)$. 通过分析可以得出，SeaNTRU 的通信复杂度低于文献 [20, 23] 方案的通信复杂度.

Table 2 Comparison of Communication Complexity

表 2 通信复杂度比较

方案	通信复杂度
文献 [20]	$O((5en+n)\|z_q\|+\|z_q\|)$
文献 [23]	$O((6en+n+2+e)\|z_q\|)$
SeaNTRU（本文）	$O((4en+n+1)\|r_q\|)$

注：e 代表水下物联网中水下自主机器人的数量，$|z_q|$为$\mathbb{Z}_q$中元素的比特大小，$|r_q|$为R_q中元素的比特大小.

5 实验结果与分析

5.1 实验环境设置

为了评估本文提出的多方密钥封装方案 SeaNTRU 并与文献 [20, 23] 中提出的方案进行对比，实验均在主频 2.20 GHz 的 Intel® Core™ i9-13900HX CPU 和 16 GB 内存的测试机上进行，配置 Ubuntu 22.04 LTS 操作系统，通过 Matlab R2022b 创建 MEX 文件进行 C 语言实现和 AVX2 的实现，并使用 BELLHOP 水声工具箱配置水下环境参数. 其中声场环境数据采用了 2017 年 5 月 25 日在韩国巨济岛南岸海域进行的海试实测数据[26]. 接收方位于水下 29 m 处，频率范围为 1~3 000 Hz，载波频率为 3 000 Hz，采样率为 500 bps，海底层沉积物为泥沙型底质，表层沉积物声速约为 1 568 m/s，浪高为 0.08 m. 文献 [20, 23] 采用基于离散高斯采样[27]的密钥生成算法，SeaNTRU 采用基于 OFDM 频域过采样的密钥生成算法. 其他实验参数的默认值如表 3 所示.

5.2 实验结果与分析

表 4 给出了文献 [20, 23] 方案和 SeaNTRU 执行 1 000 次密钥生成算法的性能对比. 可以看出，SeaNTRU 的

Table 3 Default Values of Experimental Parameters

表 3 实验参数的默认值

参数	值
n	628
水下自主机器人数量 e	10
离散高斯采样标准差σ	3.2
SeaNTRU 模数 p	3
$\|z_q\|$/b	256
$\|r_q\|$/b	256
发送方与接收方的传输距离/m	800
发送方与非法检测方的传输距离/m	500
最大时延扩展/ms	20
多普勒频移/Hz	−0.71

密钥生成算法在 C 实现和 AVX2 实现的性能均优于文献 [20, 23] 的密钥生成算法. 在文献 [23] 方案的密钥生成过程中因为涉及对密钥的 2 次调用和选择的过程，所以密钥生成的时钟周期长于文献 [20]. 此外，由于文献 [20, 23] 中没有考虑水下环境中的时延扩展会导致采样点之间的间隔不稳定，降低了采样精度，因此密钥生成算法需要执行更多的采样次数以保证生成密钥的长度. SeaNTRU 的密钥生成算法将 OFDM 频域过采样的思想应用于密钥生成的过程中，并将 OFDM 频域过采样中的快速傅里叶变换替换为 NTT，避免了复杂的蝶形变换，提高了密钥生成算法的计算效率和数据的采样率，从而提高了密钥生成速率.

Table 4 Comparison of Key Generation Performance

表 4 密钥生成性能比较 kcycle

方案	C 实现			AVX2 实现		
	n=628	n=756	n=898	n=628	n=756	n=898
文献 [20]	413 600	506 000	633 600	206 800	258 600	270 700
文献 [23]	498 400	608 400	742 600	259 600	303 600	369 600
SeaNTRU（本文）	305 800	380 600	446 600	147 400	158 400	189 200

注：实验中模数设置为 3 587，n 表示实验中设置的维数.

表 5 通过 C 语言和 AVX2 实现比较了不同多方密钥封装方案的计算开销. 文献 [23] 的计算开销最大，这是因为黑盒编译器的使用让封装和解封装过程中需要处理更多的密文. 文献 [20] 的计算开销比文献 [23] 小，这是因为封装和解封装的过程中，没有文献 [23] 方案中复杂的密文生成和选择密文的过程.

Table 5 Comparison of Computational Costs for Different Schemes

表 5 不同方案的计算开销比较 kcycle

维数	实现方法	过程	文献 [20]			文献 [23]			SeaNTRU（本文）		
			e=10	e=100	e=1 000	e=10	e=100	e=1 000	e=10	e=100	e=1 000
n=628	C 实现	封装	2 382	23 439	233 801	2 776	27 197	271 412	1829	17 695	176 543
		解封装	3 025	29 796	297 513	3 460	34 181	341 509	2 207	21 518	214 626
		Total	5 407	53 235	531 314	6 236	61 378	612 921	4 036	39 213	391 169
	AVX2 实现	封装	1 218	11 736	116 805	1 421	13 768	137 136	837	7 726	76 727
		解封装	1 551	14 802	147 476	1850	18 002	180 473	1 093	10 429	103 780
		Total	2 769	26 538	264 281	3 271	31 770	317 609	1930	18 155	180 507
n=756	C 实现	封装	2 601	25 477	254 234	3 085	30 440	304 038	1921	18 892	188 412
		解封装	3 192	31 343	312 901	3 891	38 482	384 293	2 445	23 993	239 206
		Total	5 793	56 820	567 135	6 976	68 922	688 331	4 366	42 885	427 618
	AVX2 实现	封装	1 382	13 218	131 653	1 744	17 090	170 519	921	8 676	86 021
		解封装	1 599	15 411	153 435	2 105	20 693	206 400	1 152	11 051	110 063
		Total	2 981	28 629	285 088	3 849	37 783	376 919	2 073	19 727	196 084
n=898	C 实现	封装	2 868	27 987	279 459	3 504	34 471	344 232	2 114	20 663	206 211
		解封装	3 392	33 346	332 786	4 283	42 350	423 124	2 458	24 279	242 306
		Total	6 260	61 333	612 245	7 787	76 821	767 356	4 572	44 942	448 517
	AVX2 实现	封装	1 543	14 756	146 927	1 822	18 009	179 492	1 015	9 465	94 047
		解封装	1 751	16 923	168 643	2 113	20 624	205 736	1 280	12 098	120 317
		Total	3 294	31 679	315 570	3 935	38 633	385 228	2 295	21 563	214 364

注：实验中设置的模数为 3 587，e 表示实验中设置的水下自主机器人数量.

SeaNTRU 封装和解封装的计算开销均优于文献 [20, 23] 中的方案，这是因为 SeaNTRU 采用了轻量级的设计，在封装过程中只需要多项式运算和哈希运算，在解封装过程中只需要使用海洋噪声和哈希运算验证部分密文即可.

表 6 比较了不同多方密钥封装方案的通信开销. 文献 [23] 的通信开销最大，这是因为该方案中编译器的构造需要生成更多的公开参数用于通信. 此外，为了生成多组封装密文和用于选择解封装密文的信息，也会产生较大的通信开销. 文献 [20] 的通信开销比文献 [23] 小，这是因为其通信生成的封装密文量要小于文献 [23] 中通信产生的密文量. SeaNTRU 的通信开销最小，这是因为 SeaNTRU 采用了多项式运算生成了紧凑的密文结构，避免文献 [20, 23] 中矩阵运算产生的密文量增加，减少了通信开销. 此外，在 SeaNTRU 的会话密钥更新机制中，水下自主机器人利用 OFDM 子载波提取密文分量并进行伪身份和时间标记有效性的检验，进一步降低了密文的通信开销.

Table 6 Comparison of Communication Costs for Different Schemes

表 6 不同方案的通信开销比较 KB

方案	n=628			n=756			n=898		
	e=10	e=100	e=1 000	e=10	e=100	e=1 000	e=10	e=100	e=1 000
文献 [20]	1 000.9	9 832.4	98 144.7	1 204.9	11 836.2	118 148.6	1 431.2	14 059.3	140 340.6
文献 [23]	1 197.5	11 797.8	117 800.9	1 441.5	14 201.8	141 804.9	1 712.2	16 868.8	168 434.3
SeaNTRU（本文）	804.7	7 869.7	78 519.7	968.7	9 473.8	94 523.7	1 150.6	11 253.1	112 278.1

注：n 表示实验中设置的维数，e 表示实验中设置的水下自主机器人数量.

6 结 论

本文提出了一种基于水下物联网的多方密钥封装方案 SeaNTRU. SeaNTRU 通过多方公钥加密算法、多方密钥封装算法和会话密钥更新机制保护了水下节点的多方隐私与数据安全. 为了实现身份的隐私保护，利用海洋传感器声波序列和水声声波因子生成水下自主机器人的伪身份并构造了可验证身份的海洋声波消息码. 利用 OFDM 频域过采样技术和 NTT 设计了一种适用于水声通信的密钥生成算法. 基于以上的构造，结合身份绑定的混合加密和海洋噪声的混淆操作得到了 IND-Anon-CPA 安全的多方公钥加密算法. 然后，提出了一种基于海洋噪声的 SeaFO 变换得到了 IND-Anon-CCA 安全的多方密钥封装算法. 最后，设计了一种新的会话密钥更新机制，通过伪身份和时间标记有效性的检验以及 SeaFO 变换解封装得到新的会话密钥，不仅实现了多方环境下的隐式拒绝，也防止了敌手对 SeaNTRU 的自适应破坏. 理论分析与实验结果证明了 SeaNTRU 的安全性和有效性.

作者贡献声明：徐明负责论文框架设计与算法设计；张恩博负责论文算法实现与安全性证明；周日贵负责量子安全设计与分析.

参 考 文 献

[1] Wang Xijun, Lin Wenrui, Xu Chao, et al. Age of changed information: Content-aware status updating in the Internet of things[J]. IEEE Transactions on Communications, 2022, 70(1): 578−591

[2] Mohsan S A H, Mazinani A, Othman N Q H, et al. Towards the Internet of underwater things: A comprehensive survey[J]. Earth Science Informatics, 2022, 15(2): 735−764

[3] Bello O, Zeadally S. Internet of underwater things communication: Architecture, technologies, research challenges and future opportunities[J]. Ad Hoc Networks, 2022, 135(1): 102933

[4] Wu Juidi, Tseng Y M, Huang Senshan, et al. Leakage-resilient certificateless key encapsulation scheme[J]. Informatica, 2018, 29(1): 125−155

[5] Zhou Yanwei, Han Yu, Xu Ran, et al. A leakage-resilient anonymous key encapsulation mechanism with multiple recipients[J]. Acta Electronica Sinica, 2023, 51(12): 3431−3436 (in Chinese)
(周彦伟, 韩宇, 徐然, 等. 具有多接收者的抗泄露匿名密钥封装机制[J]. 电子学报, 2023, 51(12): 3431−3436)

[6] He Debiao, Wang Huaqun, Wang Lina, et al. Efficient certificateless anonymous multi-receiver encryption scheme for mobile devices[J]. Soft Computing, 2017, 21(22): 6801−6810

[7] Deng Lunzhi. Anonymous certificateless multi-receiver encryption scheme for smart community management systems[J]. Soft Computing, 2020, 24(1): 281−292

[8] Li Jing, Tang Xiangyan, Wei Zhijun, et al. Identity-based multi-recipient public key encryption scheme and its application in IoT[J]. Mobile Networks and Applications, 2021, 26(4): 1543−1550

[9] Benioff P. The computer as a physical system: A microscopic

quantum mechanical Hamiltonian model of computers as represented by Turing machines[J]. Journal of Statistical Physics, 1980, 22(5): 563−591

[10] Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring[C]//Proc of the 35th Annual Symp on Foundations of Computer Science. Piscataway, NJ: IEEE, 1994: 124−134

[11] Hoffstein J, Pipher J, Silverman J H. NTRU: A ring-based public key cryptosystem[C]//Proc of the 1998 Int Algorithmic Number Theory Symp. Berlin: Springer, 1998: 267−288

[12] Seo S H, Won J, Bertino E. pCLSC-TKEM: A pairing-free certificateless signcryption-tag key encapsulation mechanism for a privacy-preserving IoT[J]. Transactions on Data Privacy, 2016, 9(2): 101−130

[13] Chen Yanchi, Luo Haoxiang, Bian Qing. A privacy protection method based on key encapsulation mechanism in medical blockchain[C]// Proc of the 21st IEEE Int Conf on Communication Technology (ICCT). Piscataway, NJ: IEEE, 2021: 295−300

[14] Ning Jianting, Liu Kuan, Wu Wei, et al. Multi-ciphertext batch auditable outsourced SM9-HIBE key encapsulation mechanism[J]. Journal on Communications, 2023, 44(12): 158−170 (in Chinese)
(宁建廷, 刘宽, 伍玮, 等. 支持多密文批量审计的解密外包 SM9-HIBE 密钥封装机制[J]. 通信学报, 2023, 44(12): 158−170)

[15] Lyubashevsky V, Seiler G. NTTRU: Truly fast NTRU using NTT[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019, 2019(3): 180−201

[16] Fouque P A, Kirchner P, Pornin T, et al. BAT: Small and fast KEM over NTRU lattices[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022, 2022(2): 240−265

[17] Fouque P A, Hoffstein J, Kirchner P, et al. Falcon: Fast-Fourier lattice-based compact signatures over NTRU[J]. Journal of Submission to the NIST's Post-Quantum Cryptography Standardization Process, 2018, 36(5): 1−75

[18] Kim J, Park J H. NTRU+: Compact construction of NTRU using simple encoding method[J]. IEEE Transactions on Information Forensics and Security, 2023, 18(1): 4760−4774

[19] Liang Zhichuang, Zheng Jieyu, Zhao Yunlei. An efficient and compact key encapsulation mechanism based on NTRU lattice[J]. Journal of Computer Research and Development, 2024, 61(4): 1049−1069 (in Chinese)
(梁志闯, 郑婕妤, 赵运磊. NTRU 格上高效紧凑密钥封装方案[J]. 计算机研究与发展, 2024, 61(4): 1049−1069)

[20] Katsumata S, Kwiatkowski K, Pintore F, et al. Scalable ciphertext compression techniques for post-quantum KEMs and their applications[C]//Proc of the 2020 Int Conf on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2020: 289−320

[21] Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes[J]. Journal of Cryptology, 2013, 26(1): 80−101

[22] Hashimoto K, Katsumata S, Postlethwaite E, et al. A concrete treatment of efficient continuous group key agreement via multi-recipient PKEs[C]//Proc of the 2021 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2021: 1441−1462

[23] Alwen J, Hartmann D, Kiltz E, et al. Post-quantum multi-recipient public key encryption[C]//Proc of the 2023 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2023: 1108−1122

[24] Ochiai H. On spectral efficiency of OFDM signals based on windowing[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2023, 106(5): 752−764

[25] Ambainis A, Hamburg M, Unruh D. Quantum security proofs using semi-classical oracles[C]//Proc of the 39th Annual Int Cryptology Conf. Berlin: Springer, 2019: 269−295

[26] Choi K H, Choi J W, Kim S, et al. Experimental study on performance improvement of underwater acoustic communication using a single vector sensor[J]. IEEE Journal of Oceanic Engineering, 2024, 49(4): 1574−1587

[27] Howe J, Khalid A, Rafferty C, et al. On practical discrete gaussian samplers for lattice-based cryptography[J]. IEEE Transactions on Computers, 2018, 67(3): 322−334



Xu Ming, born in 1977. PhD, professor, PhD supervisor. His main research interests include cyberspace security and wireless communication network.

徐 明, 1977 年生. 博士, 教授, 博士生导师. 主要研究方向为网络空间安全、无线通信网络.



Zhang Enbo, born in 1999. Master candidate. His main research interests include post-quantum cryptography and wireless communication network.

张恩博, 1999 年生. 硕士研究生. 主要研究方向为后量子密码学、无线通信网络.



Zhou Rigui, born in 1973. PhD, professor, PhD supervisor. His main research interests include intelligent information processing and quantum computing.

周日贵, 1973 年生. 博士, 教授, 博士生导师. 主要研究方向为智能信息处理、量子计算.