对密钥不匹配攻击的进一步理论分析——以NTRU-HRSS为例

张晓涵[1,2],程 池[1,2],余天润[1,2]
(1. 中国地质大学(武汉)计算机学院智能地学信息处理湖北省重点实验室,湖北武汉 430074;
2. 桂林电子科技大学广西可信软件重点实验室,广西桂林 541004)

摘 要: 目前,由美国国家标准技术研究院发起的对抗量子密码算法标准化的进程已进入最后一轮,其中基于格上困难问题的方案备受青睐. 已有研究表明,若公私钥对被重复使用,则可以对选择明文攻击安全的格密钥封装机制发起密钥不匹配攻击;甚至在侧信道信息的辅助下,相关攻击能对选择密文攻击安全的格KEM奏效. 在现有的针对格KEM方案的密钥不匹配攻击中,大多数攻击方案假设敌手一次只能恢复一个私钥系数,然而一次性恢复多个私钥系数是更为合理的假设,并且也将进一步减少密钥不匹配攻击所需的平均问询次数. 鉴于此,本文进一步分析了密钥不匹配攻击中恢复私钥系数所需的平均问询次数的理论值下界的问题. 其基本思路是将该问题转化为寻找一棵最优二叉恢复树的问题,进而证明了平均问询次数的理论值下界十分接近香农熵. 在此基础上,本文提出了一套计算模型,并将其应用于NTRU-HRSS KEM方案,得到了更为准确的理论值下界;进一步地,据此提出了一种成对恢复NIST第三轮入选方案NTRU-HRSS KEM私钥的密钥不匹配攻击方案. 实验结果表明,与现有的攻击方案相比,在成功率基本持平的基础上,平均问询次数减少了35.3%,耗时减少了47.3%. 此外,本文提出的攻击方案也能够用于优化现有的针对CCA安全的NTRU-HRSS KEM方案的侧信道攻击,并将所需的问询次数由2 447减少到1 193.

关键词: 抗量子密码算法;格密码学;NTRU-HRSS KEM;密钥重用;密钥不匹配攻击

基金项目: 国家自然科学基金(No.62172374);广西可信软件重点实验室研究课题(No.KX202038);智能地学信息处理湖北省重点实验室开放基金(No.KLIGIP2022B06)

中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112(2023)04-1081-12

电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20220447

Further Theoretical Analysis of Key Mismatch Attacks —A Case Study of NTRU-HRSS

ZHANG Xiao-han[1,2], CHENG Chi[1,2], YU Tian-run[1,2]
(1. *Hubei Key Laboratory of Intelligent Geo-Information Processing, School of Computer Science, China University of Geosciences, Wuhan, Hubei* 430074, *China*; 2. *Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin, Guangxi* 541004, *China*)

Abstract: Currently, the standardization process of post-quantum cryptographic algorithms initiated by the National Institute of Standards and Technology (NIST) has entered into the last round. Among them, lattice-based algorithms draw significant attention. Existing research shows that if the public-secret key pair is reused, key mismatch attacks can be launched on the chosen-plaintext attack (CPA)-secure or side-channel information assisted chosen-ciphertext attack (CCA)-secure lattice-based key encapsulation mechanisms (KEMs). Among the existing key mismatch attacks against NIST KEM algorithms, most attacks assume that the adversary can recover one coefficient of the secret key each time. However, a more reasonable assumption is recovering multiple secret key coefficients each time, which will further reduce the average number of queries needed for key mismatch attacks. Therefore, we analyze the problem of lower bounds on the average number of queries for recovering multiple secret key coefficients each time in the key mismatch attack. The problem can be transformed into searching for an optimum binary recovery tree, and the lower bound is proved to be near the Shannon entropy. Then we propose a calculation model applied to NTRU-HRSS KEM and obtain a more accurate theoretical lower

收稿日期:2022-04-24;修回日期:2022-12-22;责任编辑:李勇锋

bound. Furthermore, we propose a full key mismatch attack for pairwise recovering the secret key of NTRU-HRSS KEM. Experiments demonstrate that compared to the existing attack, based on almost the same accuracy, the average number of queries is reduced by 35.3%, and the average time is also reduced by 47.3%. Moreover, our proposed method can also be used to improve the existing side-channel attack against CCA-secure NTRU-HRSS KEM and reduce the average number of queries from 2 447 to 1 193.

Key words: post-quantum cryptography; lattice-based cryptography; NTRU-HRSS KEM; key reuse; key mismatch attack

Foundation Item(s): National Natural Science Foundation of China (No. 62172374); Guangxi Key Laboratory of Trusted Software (No.KX202038); Open Research Project of Hubei Key Laboratory of Intelligent Geo-Information Processing (No.KLIGIP2022B06)

1 引言

众所周知,在量子计算机帮助下,大整数因子分解问题和离散对数问题能被Shor算法[1]在多项式时间内破解. 因此,一旦有相当规模的量子计算机成为现实,基于上述困难问题的密码体制将会不再安全. 在此背景下,各国政府和科研机构纷纷开始研究能够抵抗量子计算机攻击的密码算法,以达到在量子时代仍然保护信息安全的目的. 这一类可以在量子计算机出现后仍然保证安全的密码算法被称为抗量子密码算法(Post-Quantum Cryptography,PQC). 抗量子密码算法可以在经典计算机上运行,并基于特定的数学困难问题,可以抵御已知的所有量子攻击. 并且它可以较高程度地兼容目前的网络系统,从而降低了将目前的密码系统迁移到抗量子密码系统过程的难度.

2021 年 10 月,美国国土安全部(Department of Homeland Security,DHS)与美国国家标准技术研究院(National Institute of Standards and Technology,NIST)合作发布了一份路线图,以指导各个部门如何过渡到新的抗量子密码标准[2]. 该路线图明确指出抗量子密码标准预计将在2022–2023年间制定完成,并计划在2030年前过渡到新的抗量子密码标准.

从2016年开始,NIST启动了对PQC算法的标准化进程,公开向全球征集新一代PQC算法. 截至目前,NIST对PQC算法的第三轮筛选工作已经结束,第四轮筛选工作正在进行中. 在2022年7月公布的第三轮终选名单中[3],NIST只保留了1个密钥封装机制(Key Encapsulation Mechanism,KEM)算法和3个数字签名算法,其中有3个是基于格上困难问题的. NIST将基于这四个算法起草标准,并预计到2024年完成标准的制定. 同样地,我国也十分重视抗量子密码算法的研究[4-6]. 在由国家密码管理局指导举办的全国密码算法设计竞赛中,获得一、二等奖的公钥密码算法有7个,其中6个是基于格的. 这些充分说明了基于格的密码算法在未来抗量子密码标准、特别是在KEM算法中处于举足轻重的地位.

根据不同的格上困难问题,基于格KEM算法大致可分为两类. 基于带错误的学习(Learning With Errors,LWE)问题及其衍生版本的方案属于第一类[7~10],第二类是基于NTRU问题的方案[11,12]. 在NIST公布的针对第三轮方案的报告(18页,注6)中专门指出[3],若在2022年底前未与入选的Kyber方案就专利问题达成一致,则会考虑选择NTRU方案,因此对NTRU类方案的研究仍然具有重要的理论和实践意义.

而对于格KEM方案,在实际中若公私钥对被重复使用,则可以对选择明文攻击(Chosen-Plaintext Attack,CPA)安全的格密钥封装机制发起密钥不匹配攻击;甚至在侧信道信息的辅助下,相关攻击能对选择密文攻击(Chosen-Ciphertext Attack,CCA)安全的格KEM奏效. 因此,研究CPA安全的方案在密钥重用背景下引发的安全问题十分重要.

大体上,密钥重用攻击分为信号泄露攻击(Signal Leakage Attack)和密钥不匹配攻击(Key Mismatch Attack). 引发信号泄露攻击的原因为密钥协商过程中的信号函数泄露了私钥的相关信息;而密钥不匹配攻击只需知晓通信双方的共享密钥是否匹配便可恢复私钥. 2018年,Ding,Fluhrer和Saraswathy首次提出了密钥不匹配攻击的想法[13],他们利用这一想法攻击了单轮交互模式的 Ding12-KE. 在2019 CT-RSA大会上,Bauer等人提出了一种针对NewHope KEM的密钥不匹配攻击[14]. 然而,在文献[15]中,Qin,Cheng和Ding指出Bauer等人的恢复方式是不完整的,据此他们提出了一种完整且更优的密钥不匹配攻击方案. 此后,Okada,Wang和Takagi[16]又在Qin等人的基础上进一步减少了攻击所需的问询次数,提升了攻击效率. 在2021年的亚密会上,Qin等人[17]提出了一种针对所有格NIST候选KEM方案的统一评估方法,以寻找密钥不匹配攻击的理论值下界,即平均最少所需的问询次数. 特别地,它能极大地减少针对CCA安全的基于格的KEM方案的侧信道攻击所需的问询次数.

上述攻击均是针对第一类即基于LWE问题及其衍生版本的方案,而基于NTRU问题的方案与前者结构有

很大的不同,因而很难直接将此前的攻击应用于后者.

2019年,Ding等人提出了一种针对NTRU的密钥不匹配攻击[18],但该攻击针对的是最原始的NTRU方案,而不是提交至NIST第三轮的NTRU-HRSS KEM方案. 2021年,Zhang,Cheng和Ding提出了一种高效的针对CPA安全的NTRU-HRSS KEM方案的密钥不匹配攻击[19],该攻击方法能够以93.6%的概率成功恢复出一个完整的私钥,且所需的平均问询次数是1 844. 根据Qin等人[17]的基本思想,通过利用哈夫曼编码技术,我们可以为NTRU-HRSS KEM方案成功构建起一棵最优二叉恢复树(Optimal Binary Recovery Tree),且得到其平均问询次数的下界为1 183,可见在针对NTRU-HRSS KEM方案的密钥不匹配攻击中仍存在很大的优化区间.

此外,在现有的针对NTRU-HRSS KEM方案的密钥不匹配攻击中,大多数攻击方案假设敌手一次问询仅能恢复一个私钥系数;然而一次性恢复多个私钥系数是更为合理的假设,并且也将进一步减少密钥不匹配攻击所需的平均问询次数. 因此,在一次性恢复多个私钥系数的前提下,寻找密钥不匹配攻击的理论值下界是本文所关注的.

主要贡献:本文分析了密钥不匹配攻击中一次性恢复多个私钥系数所需的平均问询次数的理论值下界的问题,将其应用于NTRU-HRSS KEM方案,得到了更准确的理论值下界,并以此作为理论指导,提出了一种成对恢复NTRU-HRSS KEM私钥的密钥不匹配攻击方案.

(1)本文分析了密钥不匹配攻击中一次性恢复多个私钥系数的理论值下界的问题. 其基本想法是将该问题转化为寻找一棵最优二叉恢复树的问题. 通过使用哈夫曼编码技术,成功构建出了一棵最优二叉恢复树,并得到了对应的理论值下界. 通过进一步分析,发现平均问询次数的理论值下界十分接近某种香农熵. 之后,提出了一套计算模型,将其成功应用于NTRU-HRSS KEM方案,得到了更为准确的理论值下界.

(2)与得到的理论值下界相比,现有攻击所需的平均问询次数与其仍有很大的差距. 因此,基于锚链恢复策略和最优二叉恢复树的方法,本文提出了一种成对恢复NTRU-HRSS KEM私钥的密钥不匹配攻击方案,该方案所需的平均问询次数与理论值下界仅相差6.96%,与现存的攻击结果[19]相比,平均问询次数减少了35.3%. 仿真实验的结果与理论结果匹配的非常好,充分证实了所提方案的有效性.

(3)进一步地,本文提出的攻击方案也可以用于优化针对CCA安全的NTRU-HRSS KEM方案的侧信道攻击,并能够极大地减少所需的平均问询次数,例如可以将文献[20]中所需的问询次数由2 447减少到1 193.

2　预备知识

2.1　符号的定义

本文用Z表示一个有理数整环,对于整数$q\geqslant 1$,Z_q则表示一个模q的整数环. $Z_q[x]$表示一个整数多项式环,其中多项式的系数取自Z_q. ϕ_i表示第i个分圆多项式,特别地,$\phi_1=x-1$,$\phi_n=x^{n-1}+x^{n-2}+\cdots+1$,$\phi_1\phi_n=x^n-1$.

接下来,定义一个多项式环$R_q=Z_q[x]/\left(x^n-1\right)$,其中属于$R_q$的每个多项式$f(x)=a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1}\in R_q$,系数$a_i\in Z_q(0\leqslant i\leqslant n-1)$,而且多项式之间的加法和乘法均需要模$x^n-1$. 同理,定义多项式环$T_q=Z_q[x]/(\phi_n)$和$T_p=Z_p[x]/(\phi_n)$. 在本文中,所有的多项式均用黑体表示. 另外,用$\lceil x\rceil$表示x的向上取整函数.

2.2　CPA安全的NTRU-HRSS KEM方案

原始的NTRU方案是由Hoffstein等人于1998年[21]提出的,它是一种概率性的公钥加密(Probabilistic Public Key Encryption,PPKE)模式,而之后提交至NIST PQC第三轮的NTRU方案则替换成了确定性的公钥加密(Deterministic Public Key Encryption,DPKE)模式,并且最新的NTRU方案包括两个版本,分别是NTRU-HPS和NTRU-HRSS. 关于不同版本的NTRU方案的细节请参阅文献[11]. 在本文中,我们关注的是入选NIST PQC第三轮的NTRU-HRSS KEM方案,其执行流程如下算法1所示.

NTRU-HRSS KEM方案主要包括三个多项式环,分别是$R_q=Z_q[x]/(x^n-1)$,$T_q=Z_q[x]/(\phi_n)$,$T_p=Z_p[x]/(\phi_n)$,其中$n=701$,$q=8\,192$,$p=3$. 在NTRU-HRSS KEM中,私钥的取值范围是$\{-1,0,1\}$,且对应的概率分别为$\frac{85}{256}$,$\frac{86}{256}$和$\frac{85}{256}$,通过计算$(\sum_{i=0}^{7}2^ib_i)\bmod 3$可得到私钥的概率,其中$b_i$是从$\{0,1\}$中随机选取的. 以下是NTRU-HRSS KEM中两个重要的定义.

定义1[11]　Lift函数将参数m从T_p映射到$Z[x]$,确保了密文$c\equiv 0\,(\mathrm{mod}\left(q,\phi_1\right))$,其定义为$u=\mathrm{Lift}(m)$,

$$u=m\left(\phi_1^{-1}\in T_p\right)\phi_1 \tag{1}$$

定义2[11]　T_p^+是T_p的子集,且满足非负相关性,其定义为

$$T_p^+=\left\{z\in T_p:\langle xz,\ z\rangle\geqslant 0\right\} \tag{2}$$

在算法1中,我们描述了CPA安全的NTRU-HRSS KEM方案的具体过程. 令Alice和Bob为通信过程的两个参与者,他们的目标是协商出一致的共享密钥,这个过程分为三步.

(1) KeyGen:Alice首先从T_p^+中均匀随机抽样得到

算法1 CPA安全的NTRU-HRSS KEM

Alice		Bob
1:▷KeyGen()		
1.1: $f \in T_p^+$, $g \in T_p^+$		
1.2: $f_q \leftarrow f^{-1} \in T_q$		
1.3: $f_p \leftarrow f^{-1} \in T_p$		
1.4: $h \leftarrow pg\phi_1 f_q \in R_q$	$\overset{h}{\rightarrow}$	2. ▷Encaps(h)
1.5: $h_q \leftarrow h^{-1} \in T_q$		
		2.1: $r \in T_p$, $g \in T_p$
		2.2: $c \leftarrow rh + \text{Lift}(m) \in R_q$
3. ▷Decaps(f, f_p, h_q, c)	$\overset{c}{\leftarrow}$	
3.1: $a \leftarrow cf \in R_q$		
3.2: $m' \leftarrow af_p \in T_p$		
3.3: $r' \leftarrow (c - \text{Lift}(m'))h_q \in T_q$		
3.4: IF$(r', m') \in T_p \times T_p$		
3.5: RETURN $(r', m', 0)$		
3.6: ELSE		
3.7: RETURN $(0, 0, 1)$		
3.8: END IF		

私钥f和g,并计算f在多项式环T_q和T_p下的逆元,记作f_q和f_p;之后她计算公钥$h \leftarrow pg\phi_1 f_q$,以及$h$在多项式环$T_q$下的逆元$h_q$. 最后Alice将$h$发送给Bob.

(2) Encaps:Bob在接收到h之后,他将从T_p中随机抽样生成r和共享密钥m,并计算密文$c \leftarrow rh + \text{Lift}(m)$,最后Bob将$c$发送给Alice. 其中,多项式$r$增加了密文$c$的随机性,若无多项式$r$,则共享密钥$m \equiv (c - h) \in T_p$,方案的安全性将大大降低.

(3) Decaps:在Alice接收到c之后,她将依次计算$a \leftarrow cf, m' \leftarrow af_p$,以及$r' \leftarrow (c - \text{Lift}(m'))h_q$. 最后她将检验$(r', m')$是否在消息空间中.

2.3 密钥不匹配攻击的谕言机Oracle

在针对CPA安全的NTRU-HRSS KEM方案的密钥不匹配攻击中,Alice将正常执行协议,而敌手A将冒充算法1中的Bob. 为了便于阐明密钥不匹配攻击的工作原理,本文构造了一个谕言机Oracle O用于模拟算法1中的Decaps部分. 假设在密钥不匹配攻击中,Alice的公私钥对(f, g, h)被重复使用,敌手A只知晓公钥h,则A的目标便是选择合适的参数并通过多次访问Oracle以恢复出Alice的私钥.

如算法2所示,Oracle O的输入是敌手A选择的密文c和共享密钥m,当Oracle在接收到(c, m)之后,他将分别计算出a、m'和r',之后检验(r', m')是否在消息空间中,最后比对m与m'是否一致,若均通过检验,Oracle返回1,否则返回0. 如果Oracle返回0,则说明m与m'不匹配;如此一来,敌手A便可以通过Oracle的返回值获得m与m'是否匹配这一有效信息,进而恢复出私钥.

算法2 谕言机Oracle O

输入:c,m
输出:1 or 0
1: $a \leftarrow cf \in R_q$
2: $m' \leftarrow af_p \in T_p$
3: $r' \leftarrow (c - \text{Lift}(m'))h_q \in T_q$
4: IF $(r', m') \in T_p \times T_p$ AND $m = m'$ THEN
5: RETURN 1
6: ELSE
7: RETURN 0
8: END IF

3 密钥不匹配攻击中平均问询次数的理论值下界

在密钥不匹配攻击中,敌手A为了获得Alice的私钥,他将多次访问谕言机O,并根据O的一系列返回值恢复出完整的私钥.

不失一般性地,我们假设敌手A一次能够恢复一个或多个私钥系数,则对应攻击方案中所需的平均问询次数也将不同. 我们可以很明显地注意到平均问询次数是评估攻击方案是否高效的一个重要指标. 因此,计算出平均问询次数的理论值下界对于高效地进行密钥不匹配攻击至关重要.

3.1 最优二叉恢复树的理论值下界

本小节具体描述了如何将计算平均问询次数的理论值下界问题转化为寻找一棵最优二叉恢复树的问题.

已知待恢复私钥的维度为n,且私钥系数有t种取值情况,令$S = \{\alpha_0, \alpha_1, \cdots, \alpha_{t-1}\}$表示私钥的取值集合. 假设敌手$A$一次能够恢复$k$个私钥系数,令$S^k = \{S_0^k, S_1^k, \cdots, S_{t^k-1}^k\}$表示所有$k$元私钥组的集合,例如:在NTRU-HRSS KEM中,私钥的取值范围是$\{-1, 0, 1\}$,则对应的集合$S = \{-1, 0, 1\}$,若敌手A一次能够恢复2个私钥系数,则集合S^2中的每个元素都包含了集合S的两个系数,即$S^2 = \{(-1,-1), (-1,0), (-1,1), (0,-1), (0,0), (0,1), (1,-1), (1,0), (1,1)\}$. 进一步地,令$P^k = \{P_0^k, P_1^k, \cdots, P_{t^k-1}^k\}$表示集合$S^k$中元素对应的概率集合,不失一般性地,集合$P^k$满足$\sum_{i=0}^{t^k-1} P_i^k = 1$.

在密钥不匹配攻击中,敌手A为恢复集合S^k中的每个元素,他将多次访问谕言机O,令Q_i表示敌手A恢复S_i^k所需的问询次数,则敌手A恢复集合S^k中一个元素所需的平均问询次数为$E(S^k)$,可以用下式表示:

$$E\left(S^k\right)=\sum_{i=0}^{t^k-1}P_i^k\cdot Q_i \tag{3}$$

进一步地,敌手A恢复单个私钥系数的平均问询次数为$E_k\left(S^k\right)$,且可以用下式表示:

$$E_k\left(S^k\right)=\frac{E\left(S^k\right)}{k} \tag{4}$$

我们的基本思想是将攻击方法与二叉恢复树联系起来以得到$E_k\left(S^k\right)$的理论值下界. 二叉恢复树的定义如下:二叉恢复树T有一个根结点,我们将集合S^k中的所有元素作为T的叶子结点,则T有t^k个叶子结点,且每一个叶子结点对应一个S_i^k,称T中的非叶子结点为关键字K_i,每个K_i均有两个孩子结点,用0标识K_i的左孩子结点,相应地,用1标识K_i的右孩子结点.

对于敌手A而言,他试图根据谕言机O的一系列返回值恢复出集合S^k的每个元素,此处使用$\bar{b}$表示这一系列返回值,由于集合S^k中的每个元素S_i^k互不相同,则S_i^k对应的$\bar{b}_i$也应互不相同,更具体地,对于$i\neq j$,$\bar{b}_i$和$\bar{b}_j$互不为对方的前缀. 如此一来,我们便可以构造出一棵二叉恢复树T,其叶子结点集合$S^k=\left\{S_0^k,\ S_1^k,\ \cdots,\ S_{t^k-1}^k\right\}$,$\bar{b}_i$表示从二叉恢复树$T$的根结点至叶子结点$S_i^k$的路径标识,则$\bar{b}_i$的长度即为上述定义的$Q_i$,也就是叶子结点$S_i^k$在二叉恢复树$T$中的深度$\mathrm{depth}_T\left(S_i^k\right)$,将其代入式(4)中,则得到下式:

$$E_k\left(S^k\right)=\frac{\sum_{i=0}^{t^k-1}P_i^k\cdot\mathrm{depth}_T\left(S_i^k\right)}{k} \tag{5}$$

我们的目标是求解$E_k\left(S^k\right)$的理论值下界,为了实现这一目标,必须考虑所有的攻击方法,所以不妨将这个目标放大化,即将目标转化为求解所有二叉恢复树的平均问询次数的理论值下界. 我们称满足这一目标且具有最小带权路径长度的二叉恢复树为最优二叉恢复树,并用$\min E_k\left(S^k\right)$表示最优二叉恢复树的平均问询次数,即为敌手A恢复单个私钥系数所需平均问询次数的理论值下界.

目前已知的求解最优二叉恢复树的方法是哈夫曼编码. 哈夫曼编码的基本思想是每次合并当前符号集合中概率最小的两个符号. 具体来说,我们首先需要根据概率P_i递减的顺序将集合$S^k=\left\{S_0^k,\ S_1^k,\ \cdots,\ S_{t^k-1}^k\right\}$重新排列,即$P_0^k\geqslant P_1^k\geqslant\cdots\geqslant P_{t^k-1}^k$;之后将0和1分配给集合$S^k$中概率最小的两个符号$S_i^k$和$S_j^k$,并将其合并成一个新符号,且新符号的概率为$S_i^k$和$S_j^k$的概率之和,从而得到一个包含$(t^k-1)$个符号的新集合;通过不断重复该过程,最后将构造出一棵最优二叉恢复树,并求解出相应的理论值下界$\min E_k\left(S^k\right)$,具体过程请见算法3和算法4.

算法3　构造一棵哈夫曼树

输入:$P_0^k,P_1^k,\ \cdots,\ P_{t^k-1}^k$

输出:哈夫曼树T

FOR $i=0$ TO t^k-1 DO
　插入叶子结点$T[i]$
　$T[i].\mathrm{weight}=P_i^k$
END FOR
FOR $i=0$ TO t^k-1 DO
　FOR $j=0$ TO $n+i-1$ DO
　　寻找概率最小的且无父结点的两个结点x_1和x_2
　END FOR
　合并结点x_1和x_2并插入新合成的结点$T[n+i]$
　$T[n+i].\mathrm{weight}=P_{x_1}^k+P_{x_2}^k$
END FOR

算法4　哈夫曼编码

输入:哈夫曼树T

输出:哈夫曼编码C

$E_k\left(S^k\right)=0$
FOR $i=0$ TO t^k-1 DO
　$C[i].\mathrm{length}=0$
　$j=i$
　WHILE $T[j].\mathrm{parent}\neq\mathrm{NULL}$ DO
　　IF $T[j].\mathrm{leftchild}=j$ THEN
　　$C[i].\mathrm{string}[C[i].\mathrm{length}]=0$
　　ELSE
　　$C[i].\mathrm{string}[C[i].\mathrm{length}]=1$
　　END IF
　　$C[i].\mathrm{length}=C[i].\mathrm{length}+1$
　　$j=T[j].\mathrm{parent}$
　END WHILE
　$E_k\left(S^k\right)=E_k\left(S^k\right)+(C[i].\mathrm{length}\cdot T[i].\mathrm{weight})/k$
END FOR

为了证明$\min E_k\left(S^k\right)$是恢复单个私钥系数的理论值下界,本文给出了定理1. 在定理1的证明中需要以下定义和引理.

香农熵[22]给定一个集合$S=\left\{\alpha_0,\ \alpha_1,\ \cdots,\ \alpha_{t-1}\right\}$及其对应的概率集合$P=\left\{\beta_0,\beta_1,\ \cdots,\ \beta_{t-1}\right\}$,则$H(S)$为集合$S$的香农熵,定义如下:

$$H(S)=\sum_{i=0}^{t-1}\beta_i\cdot\log\frac{1}{\beta_i} \tag{6}$$

引理1[17]　在针对基于格的KEM方案的密钥不匹配攻击中,给定私钥集合$S=\left\{\alpha_0,\ \alpha_1,\ \cdots,\ \alpha_{t-1}\right\}$及其对应的概率集合$P=\left\{\beta_0,\beta_1,\ \cdots,\ \beta_{t-1}\right\}$,则其平均问询次数的理论值下界为$\min E(S)$,进一步地,令$H(S)$为集合$S$的

香农熵,则有

$$H(S)\leqslant \min E(S)<H(S)+1 \tag{7}$$

引理 2[23] 给定私钥集合 $S=\{\alpha_0,\alpha_1,\cdots,\alpha_{t-1}\}$,并令 $S^k=\{S_0^k,S_1^k,\cdots,S_{t^k-1}^k\}$ 表示所有 k 元私钥组的集合,且令 $H(S^k)$ 为集合 S^k 的香农熵,则有

$$H(S^k)=kH(S) \tag{8}$$

定理 1 在针对基于格的KEM方案的密钥不匹配攻击中,给定私钥集合 $S=\{\alpha_0,\alpha_1,\cdots,\alpha_{t-1}\}$, $S^k=\{S_0^k,S_1^k,\cdots,S_{t^k-1}^k\}$ 表示所有 k 元私钥组的集合,集合 S^k 对应的概率集合 $P^k=\{P_0^k,P_1^k,\cdots,P_{t^k-1}^k\}$,则在单次恢复 k 个私钥系数的过程中,一个私钥系数所需平均问询次数的理论值下界为 $\min E_k(S^k)$,令 $H(S)$ 和 $H(S^k)$ 分别为集合 S 和集合 S^k 的香农熵,则有

$$H(S)\leqslant \min E_k(S^k)<H(S)+\frac{1}{k} \tag{9}$$

证明 设私钥集合 S 及其概率集合 P 为

$$\begin{bmatrix}S\\P\end{bmatrix}=\begin{bmatrix}\alpha_0, & \alpha_1, & \cdots & \alpha_{t-1}\\ \beta_0, & \beta_1, & \cdots & \beta_{t-1}\end{bmatrix},$$

$$\sum_{i=0}^{t-1}\beta_i=1,\quad(\beta_i\geqslant 0)$$

k 元私钥组的集合 S^k 及其概率集合 P^k 为

$$\begin{bmatrix}S^k\\P^k\end{bmatrix}=\begin{bmatrix}S_0^k, & S_1^k, & \cdots & S_{t^k-1}^k\\ P_0^k, & P_1^k & \cdots & P_{t^k-1}^k\end{bmatrix},$$

$$\sum_{i=0}^{t^k-1}P_i^k=1,\quad(P_i^k\geqslant 0)$$

其中,

$$S_i^k=(\alpha_{i_0},\alpha_{i_1},\cdots,\alpha_{i_{k-1}})$$

$$i_0,i_1,\cdots,i_{k-1}=0,1,\cdots,t-1$$

$$P_i^k=\beta_{i_0}\cdot\beta_{i_1}\cdot\cdots\cdot\beta_{i_{k-1}}$$

将引理1应用于集合 S^k 得

$$H(S^k)\leqslant \min E(S^k)<H(S^k)+1 \tag{10}$$

根据引理2可知,集合 S^k 的香农熵是集合 S 的香农熵的 k 倍,将式(8)代入式(10)得

$$kH(S)\leqslant \min E(S^k)<kH(S)+1$$

上式两边同除以 k,即得

$$H(S)\leqslant \frac{\min E(S^k)}{k}<H(S)+\frac{1}{k}$$

将式(4)代入上式得

$$H(S)\leqslant \min E_k(S^k)<H(S)+\frac{1}{k}$$

由此,我们便成功证明了在单次恢复 k 个私钥系数的过程中,一个私钥系数所需平均问询次数的理论值下界即为 $\min E_k(S^k)$.

3.2 $E_k(S^k)$的下界计算问题

在这一小节中,我们进一步分析 $E_k(S^k)$ 的下界计算问题.

若集合 S^k 中元素对应的概率相差较大时,$E_k(S^k)$ 的具体值只与最优二叉恢复树的构建过程紧密相关,因此无法直接计算出 $E_k(S^k)$ 的下界值;但是,若集合 S^k 中元素对应的概率均相等时,即 $P_0^k=P_1^k=\cdots=P_{t^k-1}^k$,此时根据集合 S^k 构建的最优二叉恢复树十分特殊,它既是一棵平衡二叉树,也是一棵完全二叉树,并且可以根据 t 和 k 的值计算出 $E_k(S^k)$ 的下界值.

接下来,我们首先描述平衡二叉树,满二叉树和完全二叉树的特征以及三个二叉树的性质,其次介绍如何根据 t 和 k 的值计算 $E_k(S^k)$ 的下界值.

每一棵平衡二叉树 T_b 及其任意子树都满足以下特征[24]:(1)T_b 可以是空树;(2)若 T_b 不是空树,则任何一个结点的左子树和右子树都是平衡二叉树,且左右子树的高度之差的绝对值不超过1.

满二叉树[24] 在一棵二叉树中,若所有的非叶子结点都存在左右子树,且叶子结点都在同一层,则这棵二叉树为满二叉树.

完全二叉树[24] 在一棵具有 n 个结点的二叉树中,若其结构与满二叉树前 n 个结点的结构一致,则这棵二叉树为完全二叉树.

性质 1[24] 对于一棵非空的二叉树,如果叶子结点数为 n_0,度为2的结点数为 n_2,则 $n_0=n_2+1$.

性质 2[24] 若规定只有根节点的二叉树的深度为0,则深度为 d 的二叉树的最大结点数是 $2^{d+1}-1$.

性质 3[24] 具有 n 个结点的完全二叉树的深度 $d=\lceil\log_2(n+1)-1\rceil$.

引理 3[24] 若一棵最优二叉恢复树有 t^k 个叶子结点,则它的总结点数为 $2t^k-1$.

根据上述概念以及二叉树的三个性质,我们可以依次得到三个推论,其中推论3描述了如何使用 t 和 k 的值计算出 $E_k(S^k)$ 的下界值.

推论 1 若一棵最优二叉恢复树有 t^k 个叶子结点,且所有叶子结点的概率均相等,则该棵最优二叉恢复树是一棵平衡二叉树.

证明 使用反证法,假设该棵最优二叉恢复树不是一棵平衡二叉树,根据平衡二叉树的定义,其中至少存在一个结点的左右子树的高度之差的绝对值超过1,

不妨设其高度差 $e=2$,则满足该要求的最简单的结构如下图1所示:

根据哈夫曼编码的构造原则可知,这五个结点的概率值排列为:$P_1+P_2\leqslant P_3+P_4\leqslant P_5$,但是根据题设这五个结点的概率值应为:$P_1=P_2=P_3=P_4=P_5$,则上述假设

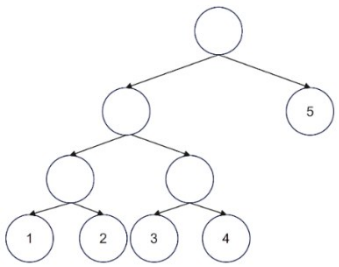

图1　平衡二叉树的反例

不成立,故原命题成立,即该棵最优二叉恢复树是一棵平衡二叉树,故推论即证. 证毕.

推论2

若一棵最优二叉恢复树有t^k个叶子结点,且所有叶子结点的概率均相等,则该棵最优二叉恢复树是一棵完全二叉树.

证明　类似地,使用反证法,假设这棵二叉树不是一棵完全二叉树,根据完全二叉树的定义可知,其中至少存在一个结点的左右子树结构与满二叉树的结构不一致,由于推论1已证明了该棵二叉树是一棵平衡二叉树,则其左右子树的高度之差的绝对值不会超过1,因此满足该要求的最简单的结构如图2所示.

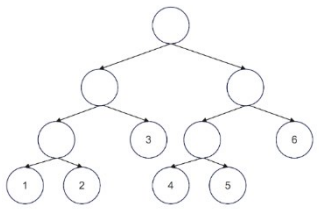

图2　完全二叉树的反例

根据哈夫曼编码的构造原则可知,这六个结点的概率值排列应为:$P_1+P_2\leqslant P_3\leqslant P_4+P_5\leqslant P_6$,但是根据题设这六个结点的概率值应为:$P_1=P_2=P_3=P_4=P_5=P_6$,则上述假设不成立,故原命题成立,即该棵最优二叉恢复树是一棵完全二叉树,故推论即证. 证毕.

推论3　给定集合$S^k=\left\{S_0^k, S_1^k, \cdots, S_{t^k-1}^k\right\}$以及对应的概率集合$P^k=\left\{P_0^k, P_1^k, \cdots, P_{t^k-1}^k\right\}$,$P_0^k=P_1^k=\cdots=P_{t^k-1}^k$,且集合$P^k$满足$\sum_{i=0}^{t^k-1}P_i^k=1$,根据集合$S^k$可以构造出一棵最优二叉恢复树$T$,则其对应的平均问询次数的理论值下界为:

$$E_k\left(S^k\right)=\frac{\lceil\log_2 t^k\rceil+1}{k}-\frac{2^{\lceil\log_2 t^k\rceil}}{k\cdot t^k}$$

证明　首先,在集合P^k中,$P_0^k=P_1^k=\cdots=P_{t^k-1}^k$,且满足$\sum_{i=0}^{t^k-1}P_i^k=1$,即概率$P_0^k=P_1^k=\cdots=P_{t^k-1}^k=\frac{1}{t^k}$.

其次,根据引理3可知,最优二叉恢复树T共有$2t^k-1$个结点;又根据推论2可知,最优二叉恢复树T是一棵完全二叉树,因此T满足性质3,即T的深度$d=\lceil\log_2 2t^k-1\rceil=\lceil\log_2 t^k\rceil$.

根据推论1可知,最优二叉恢复树T也是一棵平衡二叉树,所以其左右子树的高度之差不超过1,则其左右子树高度差最多为1,且T是一棵完全二叉树,所以T的叶子结点S_i^k的深度只有两种取值情况,即$\mathrm{depth}_T\left(S_i^k\right)\in\left\{\lceil\log_2 t^k\rceil,\lceil\log_2 t^k\rceil-1\right\}$.

根据性质2可知,最优二叉恢复树T中最后一层的叶子结点数为$2t^k-1-\left(2^{\lceil\log_2 t^k\rceil}-1\right)=2t^k-2^{\lceil\log_2 t^k\rceil}$,而$T$的叶子结点数为$t^k$,则倒数第二层的叶子结点数为$t^k-\left(2t^k-2^{\lceil\log_2 t^k\rceil}\right)=2^{\lceil\log_2 t^k\rceil}-t^k$,所以在$t^k$个叶子结点中,$\left(2t^k-2^{\lceil\log_2 t^k\rceil}\right)$个叶子节点的深度为$\lceil\log_2 t^k\rceil$,$\left(2^{\lceil\log_2 t^k\rceil}-t^k\right)$个叶子结点的深度为$\lceil\log_2 t^k\rceil-1$.

进一步地,将上述结果代入式(5),可以得到式(11):

$$\begin{aligned}E_k\left(S^k\right)&=\frac{\sum_{i=0}^{t^k-1}P_i^k\cdot\mathrm{depth}_T\left(S_i^k\right)}{k}\\&=\lceil\log_2 t^k\rceil\cdot\left(2t^k-2^{\lceil\log_2 t^k\rceil}\right)\cdot\frac{1}{k\cdot t^k}\\&\quad+\left(\lceil\log_2 t^k\rceil-1\right)\cdot\left(2^{\lceil\log_2 t^k\rceil}-t^k\right)\cdot\frac{1}{k\cdot t^k}\\&=\frac{\lceil\log_2 t^k\rceil+1}{k}-\frac{2^{\lceil\log_2 t^k\rceil}}{k\cdot t^k}\end{aligned}\tag{11}$$

由此证得推论3. 证毕.

最后,我们便可以得到恢复n个私钥系数所需的平均问询次数,如下所示:

$$\begin{aligned}E\left(\mathrm{Queries}\right)&=E_k\left(S^k\right)\cdot n\\&=\left(\frac{\lceil\log_2 t^k\rceil+1}{k}-\frac{2^{\lceil\log_2 t^k\rceil}}{k\cdot t^k}\right)\cdot n\end{aligned}\tag{12}$$

3.3　计算NTRU-HRSS KEM的理论值下界

如2.2小节所述,在NTRU-HRSS KEM中,私钥g的维度$n=700$,即敌手A能够一次恢复的私钥系数个数$k\in[1,700]$,且私钥系数的取值范围是$\{-1,0,1\}$,即$t=3$;另外,其私钥系数对应的概率分别为$\frac{85}{256}$,$\frac{86}{256}$和$\frac{85}{256}$,可见私钥系数的概率近似相等,符合3.2小节中分析的情况,因此我们将k和t的值一并代入式(11)中,则得到:

$$E_k\left(S^k\right)=\frac{\lceil\log_2 3^k\rceil+1}{k}-\frac{2^{\lceil\log_2 3^k\rceil}}{k\cdot 3^k}\tag{13}$$

为了计算出对NTRU-HRSS KEM进行密钥不匹配

攻击的平均问询次数的理论值下界，我们绘制出了$E_k(S^k)$随着k的取值范围变化的图像，如图3所示.

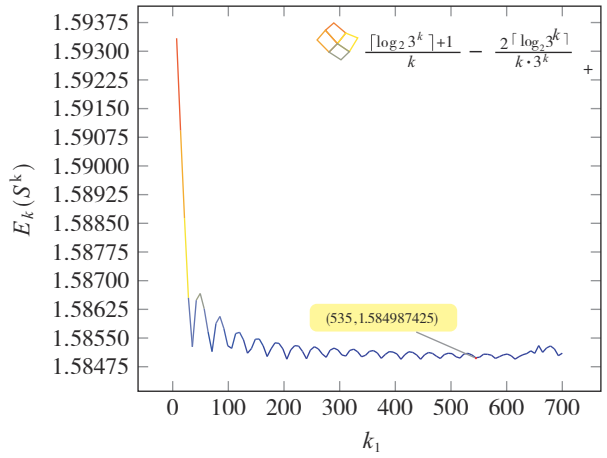

图3 $E_k(S^k)$与k之间的关系

如图3所示，当$k=535$时，$E_k(S^k)$达到了最小值1.584 987 425；进一步地，我们将此值代入式(12)中：

$$\begin{aligned} E(\text{Queries}) &= E_k(S^k)\cdot n \\ &= 1.584\,987\,425\times 700 \\ &= 1\,109.491\,197\,5 \end{aligned}$$

最后，我们便计算出了对NTRU-HRSS KEM进行密钥不匹配攻击的平均问询次数的理论值下界为1 109.491 197 5.

4 我们的攻击方案

在本章中，我们将详细介绍一种针对NTRU-HRSS KEM的密钥不匹配攻击方案.

4.1 基本攻击想法

我们的攻击方案是基于锚链恢复策略和最优二叉恢复树的. 其中锚链恢复策略包括两部分，首先在待恢复的私钥多项式中找到一条最长链，这条链由连续的且绝对值均为最大的系数构成，即为锚链；之后，我们便可以利用这条锚链恢复出剩余的私钥系数. 最优二叉恢复树的构造原则为自底向上每次选择当前概率最小的两个结点以合成一个新的结点，此处的最优二叉恢复树同时也是一棵平衡二叉树，所以任意一个结点的左右子树的高度差的绝对值不会超过1.

4.2 理论值下界的应用

在3.3小节中，我们计算了对NTRU-HRSS KEM进行密钥不匹配攻击的平均问询次数的理论值下界，当单次恢复的系数个数$k=535$时，可以达到理论值下界，并实现最高效的攻击. 然而，当$k=535$时，由于NTRU-HRSS KEM中的私钥系数范围是$\{-1,0,1\}$，即$t=3$，则总的私钥组合数$t^k=3^{535}$，显然为3^{535}个私钥组合构造一棵最优二叉恢复树的计算复杂度和空间复杂度均过高.

但是这并不意味着关于理论值下界的讨论是毫无意义的，我们可以尝试在较低计算复杂度和空间复杂度的基础上寻找接近理论值下界的k值. 为了使私钥组合数不超过30000，令$k\in[1,31]$，可绘制出$E_k(S^k)$随之变化的图像，如图4所示.

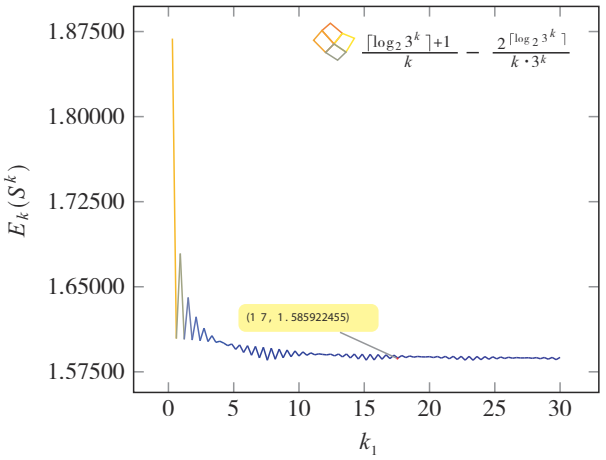

图4 $E_k(S^k)$与$k\in[1,31]$之间的关系

如图4所示，当$k=17$时，根据式(12)，我们在私钥组合数不超过30 000的前提下得到了最为接近理论值下界的问询次数$E(\text{Queries})=1\,110.145\,715$，这与理论值下界仅相差0.654 517 5个问询次数.

可此时的计算量仍然较大，所以我们进一步减少k值，当$k=2$时，根据式(13)，可以得到$E_k(S^k)=1.611\,111\,1$，代入式(12)中，$E(\text{Queries})=1\,127.777\,77$；这与理论值下界的距离也仅为18.286 572 5个问询次数，但此时仅需要为$3^2=9$个私钥组合构造一棵最优二叉恢复树即可. 因此，在综合考虑攻击效率和计算复杂度两方面的前提下，我们一次恢复两个系数，并用于构造具体的攻击方案.

4.3 具体的攻击过程

如上所述，在密钥不匹配攻击中，Alice的公私钥对被重复使用，而敌手A的目标是获取Alice的私钥g. 为了实现这一目标，敌手A需要精心设置合适的参数，具体过程如下.

阶段1：在该阶段中，敌手A需要在G中找到一条最长链，其中$G=g(x-1)$，这条最长链的形式为$(2,-2,2,-2,\cdots,2\cdot(-1)^{w-1})$，其对应$G$的前$w$个系数，即为$(G[0],\cdots,G[w-1])$.

为了找到这条最长链，敌手A需要选择合适的参数r和m，具体如下：

(1) 首先，敌手A始终令$m=0$，并仅给r的前l个系数赋值，即r的形式为$(r[0],\cdots,r[l-1],0,\cdots,0)$，其中$l\geqslant$

2, $0\leqslant i\leqslant l-1$,具体取值为

$$r[i]=\begin{cases}\left\lceil\dfrac{q}{2p\cdot 2l}\right\rceil, & \text{当}i\text{为偶数},\\ -\left\lceil\dfrac{q}{2p\cdot 2l}\right\rceil, & \text{当}i\text{为奇数}.\end{cases}$$

之后,A 计算 $c=rh+\mathrm{Lift}(m)=rh$,并发送参数 (c,m)给Oracle.

(2) 紧接着,在Oracle接收到(c,m)之后,首先计算

$$\begin{aligned}a&=cf\\&=rhf\\&=prg(x-1)f_q f\\&=prg(x-1)\\&=prG\end{aligned}\tag{14}$$

因为 $a\in R_q$, 且 $x^n\equiv 1\ (\mathrm{mod}(x^n-1))$, $x^{n+1}\equiv x\ (\mathrm{mod}(x^n-1))$,$\cdots$,Oracle可以得到下式,其中$0\leqslant i,j,v\leqslant n-1$:

$$\begin{aligned}a[j]&=\sum_{i+v\equiv j\ (\mathrm{mod}\ n)}pr[i]G[v]\\&=p\left(r[0]G[j]+\cdots+r[l-1]G[(j-l+1)]\right)\end{aligned}\tag{15}$$

对于式(15),当$l\leqslant w$时,$|a[j]|=p\cdot\left\lceil\dfrac{q}{2p\cdot 2l}\right\rceil\cdot 2l>\dfrac{q}{2}$,根据NTRU-HRSS KEM算法中的规定,相对应的$m'[j]\neq 0$,即$m'\neq m$,所以Oracle的返回值为0;直到敌手A将l增大至$w+1$时,此时$|a[j]|=p\cdot\left\lceil\dfrac{q}{2p\cdot 2(w+1)}\right\rceil\cdot(2w+1)<\dfrac{q}{2}$,相对应的$m'[j]=0$,即$m'=m$,所以Oracle返回1.

(3) 最后,敌手A只需要不断增大l的值,并观察Oracle的返回值;当敌手A观察到Oracle的返回值为1时,计算$w=l-1$,便得到了最长链的长度,即恢复了G的前w个系数$(G[0],\cdots,G[w-1])$. 由于$G=g(x-1)$,则相当于恢复了$(g[0],\cdots,g[w-1])$.

阶段2:在阶段1之后,敌手A已经在G中找到了一条最长链. 在阶段2中,敌手A借助这条最长链,并辅以最优二叉恢复树的方法恢复出G的剩余系数,即$(G[w],\cdots,G[n-1])$.

如4.2小节所示,我们只需要为9个私钥组合构造出一棵最优二叉恢复树即可. 由于$G=g(x-1)$,则对于$0\leqslant i\leqslant n-1$,其系数形式为

$$G[i]=\begin{cases}g[n-1]-g[0], & \text{if } i=0,\\ g[i-1]-g[i], & \text{if } i\neq 0.\end{cases}$$

因为$w\neq 0$,则对于$w\leqslant i\leqslant n-1$,$G[i]=g[i-1]-g[i]$,且$g[i-1],g[i]\in\{-1,0,1\}$,而在阶段1中已得到了$g[w-1]$的值,之后便可以根据$g[w-1]$的值将$G[w]$划分到三个集合中;同样地,根据$g[i-1]$和$g[i]$的不同取值,$G[i]$和$G[i+1]$也可以分别被划分到三个集合中;最后,便可以根据$g[i-1]$的值,将私钥组合$(G[i],G[i+1])$划分到3个集合$S_0,S_1$和$S_2$中,具体为

(a) 当$g[i-1]=-1$,$(G[i],G[i+1])\in S_0$,

$S_0=\{(-2,2),(-2,1),(-2,0),(-1,1),(0,-2),(-1,-1),(0,0),(-1,0),(0,-1)\}$.

(b) 当$g[i-1]=0$,$(G[i],G[i+1])\in S_1$,

$S_1=\{(-1,2),(1,0),(0,1),(-1,1),(1,-1),(0,0),(-1,0),(1,-2),(0,-1)\}$.

(c) 当$g[i-1]=1$,$(G[i],G[i+1])\in S_2$,

$S_2=\{(2,-2),(2,-1),(2,0),(1,-1),(0,2),(1,1),(0,0),(1,0),(0,1)\}$.

根据上述三个集合,我们分别构造出了对应的最优二叉恢复树,其构造思路为:(1)首先,以私钥组合的概率为标准,将集合$S_i(i=0,1,2)$中的元素降序排列,即$P(S_i[0])\geqslant P(S_i[1])\geqslant\cdots P(S_i[8])$;(2)之后,用0和1分别标识概率最小的两个私钥组合,并将其合并成一个关键字$K_j(j=0,1,\cdots,7)$,且关键字K_j的概率为两者概率之和,从而得到一个新的集合;(3)接下来,将新集合中的元素仍按照概率递减的顺序排列,再将其中概率最小的两个私钥组合合并成一个新的关键字K_j;(4)不断重复该过程,直至集合中只包含两个元素,分别用0和1标识这两个元素,两者的概率之和必为1;(5)由于集合S_i中元素的概率十分接近,每次合并时可供选择的可能性很多,所以为了明确如何选择私钥组合,我们增加了一项选择依据,即私钥组合中系数的绝对值之和,且基本遵循优先选择绝对值之和较小的私钥组合的原则,在选定了两个私钥组合之后,用0标识绝对值之和较大的一方,并用1标识绝对值较小的一方.

遵循上述构造思路,根据集合S_0,S_1和S_2,我们分别构造出了相应的最优二叉恢复树,接下来以$g[i-1]=-1$时的集合S_0为例进行说明.

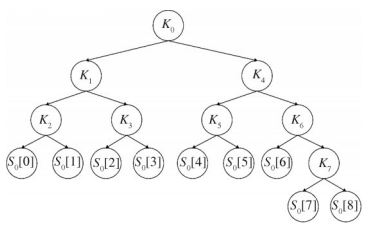

图5　集合S_0的最优二叉恢复树

如图5所示,在根据集合S_0构造出的最优二叉恢复树中,我们用K_i表示其中的非叶子结点$(i=0,1,\cdots,7)$,并用$S_0[j]$表示集合S_0中第j个私钥组合$(j=0,1,\cdots,8)$,

即最优二叉恢复树中的叶子结点;在成功构建出最优二叉恢复树之后,敌手A便可以选择合适的参数,从而利用这棵最优二叉恢复树成对恢复出G的剩余系数,即$(G[w],\cdots,G[n-1])$. 由于$G=g(x-1)$,则相当于恢复了$(g[w],\cdots,g[n-1])$. 假设敌手A想要恢复出二元组$(G[w],G[w+1])$,其详细的参数选择过程如下.

(1) 首先,敌手A令$m=0$,并只给r的前$w+2$个系数赋值,则r的形式为$(r[0],\ldots,r[w-1],r[w],r[w+1],0,\cdots,0)$,其中$0\leqslant i\leqslant w-1$,

$$r[i]=\begin{cases}\left\lceil\dfrac{q}{2p\cdot P}\right\rfloor, & \text{当}i\text{为偶数}\\ -\left\lceil\dfrac{q}{2p\cdot P}\right\rfloor, & \text{当}i\text{为奇数}\end{cases}$$

$(r[w],r[w+1])=(-\left\lceil\dfrac{q}{2p\cdot P}\right\rfloor,\left\lceil\dfrac{q}{2p\cdot P}\right\rfloor)$. 其中参数$P$的取值如表1所示.

表1 集合S_0的参数P取值表

	K_0	K_1	K_2	K_3
P	$2w+2$	$2w+3$	$2w+4$	$2w+2$
O->0	K_1	K_2	$S_0[0]$	$S_0[2]$
O->1	K_4	K_3	$S_0[1]$	$S_0[3]$
	K_4	K_5	K_6	K_7
P	$2w+2$	$2w+2$	$2w+1$	$2w+1$
O->0	K_5	$S_0[4]$	$S_0[6]$	$S_0[7]$
O->1	K_6	$S_0[5]$	K_7	$S_0[8]$

(2)如表1所示,

(a)首先,敌手A令$P=2w+2$,之后他根据Oracle第一次的返回值将集合S_0分成两部分;

(b)若敌手A切换到了K_1,则令$P=2w+3$;

(c)此时,如果敌手A切换到了K_2,则令$P=2w+4$;

(d)当$(G[w],G[w+1])\in\{S_0[0],S_0[1],S_0[2],S_0[3]\}$,敌手$A$将依次赋予参数$P$不同的取值($P=2w+4$,$2w+2$),具体的细节见表1;通过不断重复上述过程,最终$A$能确定$(G[w],G[w+1])$的具体取值;

(e)类似地,当$(G[w],G[w+1])\in\{S_0[4],S_0[5],S_0[6],S_0[7],S_0[8]\}$,敌手$A$同样赋予参数$P$不同的取值,其中$P=2w+2$,$2w+1$;$A$最终可以确定$(G[w],G[w+1])$的具体取值.

上述即为当$g[w-1]=-1$时,参数P的具体选择过程,另外两种情况与其相类似. 通过不断重复该过程,敌手A便可以恢复出Alice的私钥g.

5 实验结果与分析

在本章中,我们将从攻击成功率和攻击效率两个方面来分析所提出的对NTRU-HRSS KEM密钥不匹配攻击方案的优势. 其中,攻击成功率是指敌手能够完整且正确地恢复出私钥的概率,而攻击效率则是敌手恢复出一个完整的私钥需要访问Oracle的次数.

实验环境是两颗主频为2.1 GHz的Intel Xeon E5-2620 CPU处理器,64 GB运行内存,操作系统为Ubuntu 18.04,编译环境为GCC 7.5.0. 为了让我们的实验更有说服力,实验中的所有攻击代码均是在NTRU-HRSS KEM设计者提交给NIST的标准代码的基础上修改的. 在实验中,我们使用NTRU-HRSS KEM的源代码生成1 000个私钥,然后用所提的攻击方案对其进行恢复. 每当敌手访问一次Oracle,问询次数便会加一,此处我们将恢复1 000个私钥所需问询次数的平均值作为攻击效率的衡量指标.

我们对NTRU-HRSS KEM的密钥不匹配攻击实验的具体结果如表2和图6所示. 除了在第四节中提出的攻击方案之外,我们还列出了Zhang,Cheng和Ding提出的攻击方案的实验结果,他们完整地恢复出一个私钥的概率是93.6%,且平均问询次数为1 844.

表2 对NTRU-HRSS KEM的密钥不匹配攻击的实验结果

攻击方案	成功率/%	平均问询次数	平均耗时/s
Zhang等人的方案[19]	93.6	1 844	11.983
我们的方案	92.8	1 193	6.315

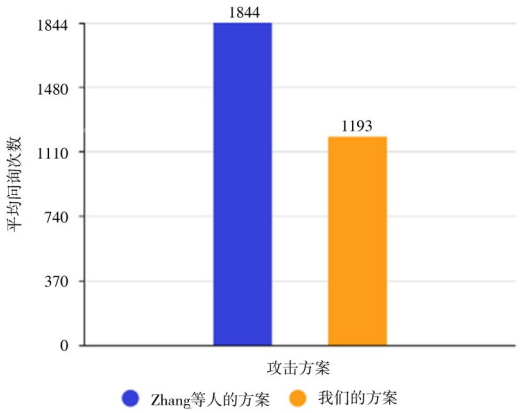

图6 对NTRU-HRSS KEM的密钥不匹配攻击的平均问询次数对比

如表2所示,从攻击成功率来看,我们的方案与之前Zhang等人的方案基本持平;但是攻击所需的平均问询次数减少了35.3%,且与3.3小节中的理论值下界相比,它们之间的差距仅为6.96%,这进一步证实了之前的理论分析,此外,平均耗时也减少了47.3%. 因此,综合考虑攻击成功率和攻击效率两方面,我们在第四章中提出的对NTRU-HRSS KEM的密钥不匹配攻击方案是目前最优的.

Zhang等人的方案之所以效率很差是因为敌手首先恢复概率较小的私钥组合,之后再逐个恢复私钥,这样便造成了问询次数的大量增长. 而在我们的方案中,

考虑到私钥的生成概率是不同的,我们使用最优二叉恢复树优化了选参方案,即让敌手在恢复概率越大的私钥时所需的问询次数越少,且保证了恢复概率大的私钥所需的问询次数一定小于或等于恢复概率小的私钥所需的问询次数,因此提升了方案的攻击效率,也进一步减少了攻击所需的平均耗时.

如前所述,在CPA安全的KEM方案中,若公私钥对被重用,则会遭受密钥不匹配攻击. 然而,所有入选NIST PQC标准化进程的算法均达到了CCA安全等级,这些算法通常采用FO变换将CPA安全的方案转换为CCA安全的方案. 其中,FO变换主要包括两个过程:解密过程和重加密过程. 其中解密过程与CPA安全的方案一致;而重加密过程是将解密过程得到的明文重新加密得到新密文,之后将其与最初收到的密文进行对比,若二者相等,继续计算共享密钥,否则拒绝此次的密文. 可见FO变换实质上保护了密文的合法性,因此如果敌手恶意构造密文,他将无法直接得到任何有效信息. 但是,在2022年的CHES会议上,Ravi等人[20]使用侧信道攻击绕过了FO变换的限制,并通过精心构造密文,得到了关于解密输出是否匹配的有效信息,从而成功攻击了CCA安全的KEM方案. 换言之,Ravi等人选择密文攻击的思想与密钥不匹配攻击是一致的,只是敌手需要访问解封装的设备以得到解密输出是否匹配的有效信息,因此我们的攻击方案可用于优化针对CCA安全的NTRU-HRSS KEM的侧信道攻击. Ravi等人针对NTRU-HRSS KEM方案恢复完整私钥的平均问询次数是2 447,而我们的攻击方案平均仅需要1 193个问询次数,与之相比减少了51.2%.

在文献[25]中,Xagawa等人针对NIST第三轮的候选KEM方案进行了一种比较特殊的侧信道攻击——错误注入攻击. 该类攻击方法需要与设备进行物理接触,并且通过特殊方法使设备出现故障,例如发射激光以重置静态存储器的一个比特位. 与Ravi等人的侧信道攻击不同,错误注入攻击对攻击方要求更高;此外,错误注入攻击的成功率很低,经常无法获得预期结果,因此单次攻击的错误数越少越好,而Xagawa等人关注的就是单个错误的注入攻击. 他们的主要想法是通过在CCA安全方案的解密谕言机中注入错误,以越过FO变换的限制,进而使用密钥不匹配攻击恢复出相应的私钥. 然而,他们仅列出了针对NTRU-HPS KEM的实验结果;另一方面,由于我们的结果是通用的,因而,可直接将本文的结果用于改进针对NTRU-HRSS KEM的错误注入攻击. 最近,Rajendran等人通过一次性恢复多个私钥系数改进针对Kyber KEM的侧信道攻击,他们从实验角度得到的密钥不匹配攻击所需的平均问询次数也是接近香农熵[26],这与本文所给出的理论界是完全一致的,进一步印证了本文结果的正确性和可扩展性.

6　总结

本文分析了密钥不匹配攻击中一次性恢复多个私钥系数的理论值下界的问题,据此提出了一种成对恢复NTRU-HRSS KEM私钥的密钥不匹配攻击方案. 实验结果表明在成功率基本相近的前提下,与Zhang等人的方案相比,攻击所需的平均问询次数减少了35.3%,且与其理论值下界的差距也仅为6.96%. 不仅如此,我们提出的攻击方案也能够用于优化针对CCA安全的NTRU-HRSS KEM的侧信道攻击. 进一步地,本文也揭示了密钥重用带来的安全性问题,能够为基于格的认证密钥交换方案设计与安全性分析提供一定的理论基础.

参考文献

[1] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithmson a quantum computer[J]. Society for Industrial and Applied Mathematics Review (SIREV), 1999, 41(2): 303-332.

[2] NIST, DHS. Preparing for Post-Quantum Cryptography [EB/OL]. [2021-05-08]. https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf.

[3] MOODY D, ALAGIC G, APON DC, et al. Status report on the third round ofthe NIST post-quantum cryptography standardization process[R/OL]. [2022-07-05]. https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf.

[4] 王小云, 刘明洁. 格密码学研究[J]. 密码学报, 2014, 1(1): 13-27.
WANG X Y, LIU M J. Survey of lattice-based cryptography[J]. Journal of Cryptologic Research, 2014, 1(1): 13-27. (in Chinese)

[5] 杨昊, 刘哲, 黄军浩, 等. AKCN-MLWE算法AVX2高效实现[J]. 计算机学报, 2021, 44(12): 2560-2572.
YANG H, LIU Z, HUANG J H, et al. High-speed AVX2 implementation of AKCN-MLWE[J]. Chinese Journal of Computers, 2021, 44(12): 2560-2572. (in Chinese)

[6] 李子臣, 谢婷, 张卷美. 基于RLWE问题的后量子口令认证密钥交换协议[J]. 电子学报, 2021, 49(2): 260-267.
LI ZC, XIE T, ZHANG J M. Post quantum password-based authentication key exchange protocol based on ring learning with errors problem[J]. Acta Electronica Sinica, 2021, 49(2): 260-267. (in Chinese)

[7] ALKIM E, AVANZI R, BOS J, et al. Newhope algorithm specification and supporting documentation[EB/OL]. [2020-04-10]. https://newhopecrypto.org/data/NewHope_2020_04_10.pdf.

[8] ALKIM E, BOS J, DUCAS L, et al. Frodokem learning

with errors key encapsulation: Algorithm specification and supporting documentation[EB/OL]. [2019-07-02]. https://frodokem.org/files/FrodoKEM-specification-20190702.pdf.

[9] AVANZI R, BOS J, DUCAS L, et al. Crystals-kyber: Algorithm specification and supporting documentation (version 2.0)[EB/OL]. [2019-04-01]. https://pq-crystals.org/kyber/data/kyber-specification-round2.pdf.

[10] D'ANVERS J P, KARMAKAR A, et al. Saber: Mod-lwr based KEM algorithm specification and supporting documentation[EB/OL]. [2021-10-12]. https://www.esat.kuleuven.be/cosic/pqcrypto/saber/files/saberspecround3.pdf.

[11] CHEN C, DANBA O, HOFFSTEIN J, et al.NTRUa-logarithm specifications and supporting documentation[EB/OL]. [2019-03-30]. https://ntru.org/f/ntru-20190330.pdf.

[12] BERNSTEIN D J, CHUENGSATIANSUP C, LANGE T, et al. NTRU prime: Round 2[EB/OL]. [2019-03-30]. https://ntruprime.cr.yp.to/nist/ntruprime-20190330.pdf.

[13] DING J, FLUHRER S, RV S. Complete attack on rlwe key exchange with reusedkeys, without signal leakage [C]//Australasian Conference on Information Security and Privacy (ACISP). Wollongong, Australia: Springer, 2018: 467-486.

[14] BAUER A, GILBERT H, RENAULT G, et al. Assessment of the key-reuse resilience of newhope[C]//Cryptographers' Track at the RSA Conference (CT-RSA). San Francisco, USA: Springer,2019: 272-292.

[15] QIN Y, CHENG C, DING J. A complete and optimized key mismatch attack on nist candidate newhope[C]//European Symposium on Research in Computer Security (ESORICS). Luxembourg: Springer, 2019: 504-520.

[16] OKADA S, WANG Y, TAKAGI T. Improving key mismatch attack on new hope with fewer queries[C]//Australasian Conference on Information Security and Privacy (ACISP). Cham, Switzerland: Springer, 2020: 505-524.

[17] QIN Y, CHENG C, ZHANG X, et al. A systematic approach and analysis of key mismatch attacks on CPA-secure lattice-based NIST candidate KEMs[C]//International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Singapore: Springer, 2021: 92-121.

[18] DING J, DEATON J, SCHMIDT K, et al. A simple and practical key reuse attack on NTRU cryptosystem[J]. IACR Cryptology EPrint Archive, 2019.

[19] ZHANG X, CHENG C, DING R. Small leaks sink a great ship: An evaluation of key reuse resilience of PQC third round finalist NTRU-HRSS[C]//International Conference on Information and Communications Security (ICICS). Chongqing, China:Springer, 2021: 283-300.

[20] RAVI P, EZERMAN MF, et al. Will you cross the threshold for me? Generic side-channel assisted chosen-ciphertext attacks on NTRU-based kems[C]//IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES). Leuven, Belgium: Springer, 2022: 722-761.

[21] HOFFSTEIN J, PIPHER J, SILVERMAN J H. NTRU: A ring-based public key cryptosystem[C]//International Algorithmic Number Theory Symposium (ANTS). Portland: Springer, 1998: 267-288.

[22] SHANNON C E. A mathematical theory of communication[J]. The Bell System Technical Journal, 1948, 27(3): 379-423.

[23] COVER T M. Elements of Information Theory[M]. 1st Edition. New York: John Wiley & Sons, 1999.

[24] WEISS M A. Data Structures and Algorithm Analysis in C++[M]. 4th Edition. New York: Pearson, 2014.

[25] XAGAWA K, ITO A, UENO R, et al. Fault-injection attacks against NIST's post-quantum cryptography round 3 KEM candidates[C]//International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Singapore: Springer, 2021: 33-61.

[26] RAJENDRAN G, RAVI P, D'ANVERS JP, et al. Pushing the limits of generic side-channel attacks on LWE-based KEMs-parallel PC oracle attacks on Kyber KEM and beyond[J]. IACR Cryptology EPrint Archive, 2022.

作者简介

张晓涵 男,1998年6月出生于山西省临汾市侯马市,现为中国地质大学(武汉)计算机学院硕士研究生. 目前研究方向为NTRU算法在密钥不匹配攻击下的安全性分析.

E-mail: zxh_is@foxmail.com

程 池(通讯作者) 男,1981年9月出生于湖北省天门市. 现为中国地质大学(武汉)计算机学院副教授、博士生导师. 主要研究方向为格密码学理论及其应用等.

E-mail: chengchi@cug.edu.cn