·网络空间安全· 文章编号：1000-3428(2020)07-0122-07 文献标志码：A 中图分类号：TP309

格上基于 KEM 的认证密钥交换协议

赵宗渠，黄鹏娟，范 涛，马少提

（河南理工大学 计算机科学与技术学院，河南 焦作 454000）

摘 要： 针对现有认证密钥交换协议计算复杂度高且无法抵抗量子攻击的问题，提出一种格上基于 R-LWE 问题的认证密钥交换协议。将基于 R-LWE 问题构造的 KEM 方案与带消息恢复功能的数字签名算法相结合实现认证性，并使用加密的构造方法代替 Peikert 式错误协调机制，获取随机均匀的会话密钥。分析结果表明，与 BOS 等人设计的协议相比，该协议计算复杂度较低，可大幅减少通信量，并且能够有效抵抗量子攻击。

关键词： 格密码；密钥封装机制；认证密钥交换协议；R-LWE 问题；数字签名

开放科学(资源服务)标志码(OSID)：

中文引用格式： 赵宗渠，黄鹏娟，范涛，等. 格上基于 KEM 的认证密钥交换协议[J]. 计算机工程，2020，46(7)：122-128.

英文引用格式： ZHAO Zongqu，HUANG Lijuan，FAN Tao，et al. KEM-based authenticated key exchange protocol on lattice[J]. Computer Engineering，2020，46(7)：122-128.

KEM-based Authenticated Key Exchange Protocol on Lattice

ZHAO Zongqu，HUANG Lijuan，FAN Tao，MA Shaoti

（College of Computer Science and Technology，Henan Polytechnic University，Jiaozuo，Henan 454000，China）

【Abstract】 To solve the problem that existing Authenticated Key Exchange(AKE) protocols have high computational complexity and cannot resist quantum attacks，this paper proposes an AKE protocol based on R-LWE problem on lattice. The KEM scheme constructed based on R-LWE problem is combined with the digital signature algorithm with the message recovery function to achieve authentication，and the Peikert-type error coordination mechanism is replaced by the encrypted construction method to obtain the random and uniform session key. Analysis results show that，compared with the protocol designed by BOS，et al.，the proposed protocol has lower computational complexity，significantly reduces traffic，and effectively resists quantum attacks.

【Key words】 lattice-based cryptography；Key Encapsulation Mechanism(KEM)；Authenticated Key Exchange(AKE) protocol；R-LWE problem；digital signature

DOI： 10.19678/j.issn.1000-3428.0055076

0 概述

认证密钥交换(Authenticated Key Exchange，AKE)协议可使通信方在有主动敌手的信道上建立安全的共享会话密钥，同时实现彼此身份的相互认证，在后续的对称密码中能够保证数据的完整性和真实性。目前多数 AKE 协议的安全性依赖于大整数分解和离散对数的 Diffie-Hellman[1] 困难问题，随着量子计算技术的发展，此类问题在多项式时间算法下是可解的，这将给现有协议带来安全威胁。格上构造的公钥密码体制因其运算简单、可并行性和抗量子攻击的优点，将在后量子时代成为最有效的解决方案之一，基于格的 AKE 协议因此成为学术界的研究热点。

基于格的 AKE 协议[2-4] 可以抵抗量子攻击，解决经典困难问题下协议的安全性问题，但不能降低通信复杂度并实现认证。文献[5]在标准模型下构造高效的口令认证密钥交换协议，但该协议不能抵抗量子攻击。文献[6]基于 LWE 构造了无环密钥交换协议，虽然该协议可以抵抗量子攻击，但无法实

基金项目： 国家自然科学基金(61802117)；“十三五”国家密码发展基金(MMJJ20170122)；河南省科技厅项目(182102310923)；河南理工大学博士基金(B2016-39)。

作者简介： 赵宗渠(1974—)，男，讲师、博士，主研方向为密码学、网络安全、恶意代码分析；黄鹏娟、范 涛(通信作者)、马少提，硕士研究生。

收稿日期： 2019-05-30 **修回日期：** 2019-08-10 **E-mail：** 870992788@qq.com

现客户和服务器的相互认证。文献[7]提出一个基于理想格的密钥交换协议,使通信方以显著概率计算得到一个相同的会话密钥,然而该协议提取的会话密钥只具有高熵,并不是均匀分布的,虽然通信方可以利用随机提取器得到均匀分布的共同比特,但这会降低协议的效率。文献[8]提出一种基于理想格的密钥封装机制(Key Encapsulation Mechanism,KEM),文献[9]在此基础上结合一种简单的低带宽协调技术提出一种变形的错误协调机制,结合环 LWE 困难问题构造密钥交换协议,使加密方案的密文长度缩短了近两倍,通信方可以直接得到均匀的共同比特。

文献[10]结合 Peikert 式错误协调机制构造了适用于 TLS 协议的 Diffie-Hellman 式密钥交换协议,并给出具体的实现参数,其中会话密钥能达到较高的量子安全级别,但错误协调机制模数较大,使得通信量较大,降低了协议的效率。文献[11]基于 R-LWE 困难问题,利用格解码算法结合中心二项分布提出了 NewHope 密钥交换协议,优化了文献[10]的密钥交换协议,扩大了可容忍的错误范围,减少了模数,节省了通信量。文献[12]提出的 NewHopeSimple 方案,使用加密的构造方法代替调和技术,降低了协议的计算复杂度。文献[13]基于加密的构造方法提出抗选择密文攻击安全的 Kyber 系列密钥封装算法,其采用密钥压缩技术对需要发送的公钥和密文进行压缩,降低了通信量。

随着格密码的快速发展,密钥交换协议的效率已得到大幅提高,但目前多数协议都是 Diffie-Hellman 式密钥交换协议[7,10,14-16],只能提供被动安全性,不能实现相互认证,也不能抵抗中间人攻击,而实际应用中必须要考虑网络上的主动攻击者。因此,构造认证密钥交换协议来抵御主动攻击是研究趋势所向,而基于 KEM 方案构造认证密钥交换协议是一种可行的方法。

文献[17]在 NTRU 格 Diffie-Hellman 式密钥交换协议的基础上,结合带消息恢复功能的签名算法与 KEM 方案实现协议的认证性。与传统签名算法相比,该方案既增加了安全性又提高了通信效率。文献[18]将具有 CCA 安全和 CPA 安全的 KEM 方案相结合,提出了适用于格的可认证密钥交换协议的通用架构,即 GC 协议,其将 KEM 方案作为基本的设计原语,在 CK^+ 模型下是可证明安全的。文献[19]提出的 CCA 安全的密钥封装机制,可由基本的 CPA 安全的密钥封装机制获得,使用这一方法,Kyber 构造了具有认证性的密钥交换协议 Kyber.AKE。文献[20]设计了格上基于 R-LWE 的三方 PAKE 协议,实现了通信方的显式认证,可避免两方认证密钥交换协议的局限性,但该协议存在会话密钥的不一致性问题。

为实现 Diffie-Hellman 式密钥交换协议的认证性并使其能够抵抗量子攻击,本文结合带消息恢复功能的签名算法,基于 R-LWE 构造一个 KEM 方案。在协议执行时采样随机种子生成协议双方的公共参数,防止攻击者利用固定公共参数攻击协议,以保证前向安全性。发送方选择定比特长的随机字符串,每 4 个元素使用 Encode 函数[12]编码其中的一个比特,编码后的环元素可容忍更大的错误,从而降低模数,缩减通信量。此外,在保证密文恢复完整性的前提下对密文元素使用 Compress 压缩函数进行压缩,减轻服务器的传输负荷,同时利用带有消息恢复功能的签名算法实现协议的认证性。

1　相关知识

引理 1　令 $\boldsymbol{X}\in\mathbb{R}^{n\times m}$ 为一个带有参数 s 的 δ-亚高斯随机矩阵。存在一个常数 $C>0$,对于任何 $t\geqslant 0$,有 $s_1(\boldsymbol{X})\leqslant C\cdot s\cdot\left(\sqrt{m}+\sqrt{n}+t\right)$。

引理 2　设 $\Lambda\subset\mathbb{R}^n$ 是一个格,对于 $\varepsilon\in(0,1)$,令 $r\geqslant\eta_\varepsilon(\Lambda)$,则对于任何 $c\in\mathrm{span}(\Lambda)$,得到 $\Pr\left[\|D_{\Lambda+c,r}\|\geqslant r\sqrt{n}\right]\leqslant 2^{-n}\cdot\frac{1+\varepsilon}{1-\varepsilon}$。

引理 3(剩余散列)设 $\boldsymbol{H}$ 是一个 2-universal 的,从定义域 $\boldsymbol{X}$ 到值域 $\boldsymbol{Y}$ 的哈希函数簇,则对于均匀独立选取的 $h\leftarrow\boldsymbol{H}$ 和 $h(\boldsymbol{X})\leftarrow\boldsymbol{X}$,$(h,h(\boldsymbol{X}))$ 在 $\boldsymbol{H}\times\boldsymbol{Y}$ 上是 $\frac{1}{2}\sqrt{\boldsymbol{Y}/\boldsymbol{X}}$ 均匀分布的。

引理 4　对于任意的秘密值 $s\geqslant\omega\left(\sqrt{\mathrm{lb}\,n}\right)$,有 $\Pr\limits_{e\leftarrow\chi^n,s}\left[\,|\,|x'|\,|>s\sqrt{n}\right]\leqslant 2^{-n}$。

1.1　密文压缩算法

密文压缩技术是减少用户通信量的有效方法,其对密文元素进行压缩,丢掉密文元素的低位比特,即部分噪音信息。在保证密文恢复完整性的前提下,有效减少通信量,减轻服务器的传输负荷。将密文元素从 $\mathbb{Z}_q$ 映射到 $\mathbb{Z}_{2^d}$ 上,其中 $d<\mathrm{lb}\,q$。

定义 1　一个密文压缩算法包括 2 个多项式时间算法,即压缩算法 $\mathrm{Compress}_q(x,d)$ 和解压缩算法 $\mathrm{Decompress}_q(x,d)$。

1)压缩函数:

$$\mathrm{Compress}_q(x,d)=\lfloor(2^d/q)\cdot x\rfloor\bmod^+2^d$$

其中,$x\in\mathbb{Z}_q$,$d\in\mathbb{N}^*$,$\mathrm{Compress}_q(x,d)\in\{0,1,\cdots,2^d-1\}$,满足 $d<\lceil\mathrm{lb}\,q\rceil$。

2)解压缩函数:

$$\mathrm{Decompress}_q(c,d)=\lceil(q/2^d)\cdot c\rceil$$

其中,$c\in\{0,1,\cdots,2^d-1\}$,$d\in\mathbb{N}^*$,满足 $d<\lceil\mathrm{lb}\,q\rceil$。

引理 5　令 $c=\mathrm{Compress}_q(x,d)$,$x'=\mathrm{Decompress}_q(c,d)$,满足 $|x'-x\bmod^\pm q|\leqslant B_q=\left\lceil\frac{q}{2^{d+1}}\right\rceil$,其中,$|x'-x\bmod^\pm q|$ 在 B_q 上服从均匀分布,且在 B_q-1 上此分布整数大小相等。

1.2 带消息恢复的签名算法

文献[14]提出带消息恢复的签名算法,其中每一个用户都有一对密钥,即一个需要公开的公钥和一个需要秘密保存的私钥。当用户需要对某个消息 m 进行签名产生对应的数字签名 Sig 时,即需要使用自己的私钥和消息 $m=(m_1 \| m_2)$ 进行签名运算,运算结果就是签名值。签名值只需要消息 m 中的部分消息 m_2 表示。任何人都可以使用该用户的公钥来恢复消息和验证签名是否正确,并且没有人能够在用户私钥未知的前提下伪造出一个合法的消息签名对。此算法可解决签名消息过长的问题。

定义 2 1 个带消息恢复的签名算法包括 3 个多项式时间算法,即签名密钥生成算法 SigKeyGen(1^λ)、签名算法 Sig($(f,g),m=(m_1 \| m_2)$)和验证算法 Ver($h,\sigma=(s_1,s_2,m_2)$)。

1)签名密钥生成算法 SigKeyGen(1^λ):$\{f,g \leftarrow D_f, h \leftarrow f/g \bmod q\}$ 得到(K_s,K_v)=(g,h)。

2)签名算法 Sig($(f,g),m=(m_1 \| m_2)$):$\{t=(m_1+F(H'(m))) \bmod q \| H'(m))s_1, s_2 \leftarrow D_s$ 满足 $(f/g)s_1+s_2=t \bmod q$,得到 $\sigma=(s_1,s_2,m_2)$。

3)验证算法 Ver($h,\sigma=(s_1,s_2,m_2)$):$(t_1 \| t_2) \leftarrow hs_1+s_2 \bmod q, m_1 \leftarrow t_1-F(t_2) \bmod q$,若 $(s_1,s_2) \| < B$ 并且 $H'(m_1 \| m_2)=t_2$,则接受;否则拒绝。

1.3 Encode 函数与 Decode 函数

定义 3[10] 用户 A 选取 $v \in \{0,1\}^n$ 环元素 k,即每 4 个 $\mathbb{Z}_q$ 元素中编码 v 的一个比特,用户 B 根据收到的 k',取在 $\{0,1,\cdots,q-1\}$ 范围中的 4 个系数减去 $\lfloor q/2 \rfloor$,累积它们的绝对值,若得到的结果小于 q 则 v_i 取 1,否则取 0。可容忍更大的错误,从而降低了模数,缩减了通信量。Encode 函数和 Decode 函数的具体描述如下:

Encode($v \in \{0,1\}^n$)
输入 k
对于 i 从 0 到 n-1 循环执行:
$k_i \leftarrow v_i \cdot \lfloor q/2 \rfloor$;
$k_{i+n} \leftarrow v_i \cdot \lfloor q/2 \rfloor$;
$k_{i+2n} \leftarrow v_i \cdot \lfloor q/2 \rfloor$;
输出 k

Decode($k' \in \mathbb{R}_q$)
输入 k',对于 i 从 0 到 n-1 循环执行:
$t \leftarrow \sum_{j=0}^{3} | k_i' + n \cdot j - \lfloor q/2 \rfloor |$;
若 t<q 则 $k_i' \leftarrow 1$;
否则 $k_i' \leftarrow 0$;
输出 k'

1.4 AKE 协议安全模型

模型中的参与者包含有限元素的集合 P_i 和攻击者 A。参与者之间的通信网络被攻击者 A 完全控制,攻击者 A 可以任意地窃听、重放、插入消息。协议参与者刻画为预言机 $\Pi_{i,j}^s$ 表示参与者 i 与参与者 j 进行会话的第 s 个实例。

模型中会话密钥的安全性通过模拟者和攻击者之间的游戏定义。首先攻击者 A 选择一定数量的诚实参与者,通过提供攻击者以下查询来建模攻击者的能力:

1)Send($\Pi_{i,j}^s,M$)。攻击者 A 向预言机 $\Pi_{i,j}^s$ 发送消息 M。$\Pi_{i,j}^s$ 按照协议规范做出对消息 M 的应答,接受(Accept)或拒绝(Refuse)本次会话。

2)Reveal($\Pi_{i,j}^s$)。收到此查询,预言机 $\Pi_{i,j}^s$ 返回已经完成的会话密钥,如果该预言机返回的状态不是已接受(Accepted),则返回空值符号 $\perp$。

3)Corrupt(i)。攻击者 A 通过此查询来腐化参与者 i。要求被询问的协议参与者返回参与者 i 的长期私钥,同时称参与者 i 被腐化(Corrupted)。

4)Test($\Pi_{i,j}^s$)。在某个时刻,攻击者 A 可以向一个新鲜的预言机 $\Pi_{i,j}^s$ 发送 Test 查询。预言机 $\Pi_{i,j}^s$ 随机选择 $b \in \{0,1\}$ 回答此查询。若 $b=1$,则令 $K \leftarrow$ Reveal($\Pi_{i,j}^s$)并返回 K;否则返回会话密钥空间 $\{0,1\}^\lambda$ 的一个随机值,λ 表示会话密钥的位长度,攻击者只可以发送一次 Test 查询。

如果 2 个预言机 $\Pi_{i,j}^s$ 和 $\Pi_{i,j}^{s'}$ 在一次协议运行完成后,具有相同的会话标识,则称它们互为匹配会话。

通过模拟一个挑战者与攻击者之间的游戏定义 AKE 协议的安全性。游戏分为以下 4 个阶段:

第 1 阶段 攻击者 A 可以进行任意除 Test 以外的查询,预言机并给出相应答案。

第 2 阶段 在游戏的某一时刻,攻击者 A 对一个新鲜的预言机 $\Pi_{i,j}^s$ 进行 Test 查询。预言机 $\Pi_{i,j}^s$ 随机选择 $b \in \{0,1\}$ 回答此查询。若 $b=1$,则令 $K \leftarrow$ Reveal($\Pi_{i,j}^s$),并返回 K;否则返回会话密钥空间 $\{0,1\}^\lambda$ 的一个随机值,λ 表示会话密钥的位长度。

第 3 阶段 攻击者 A 仍然可以进行任意除 Test 以外的查询,预言机给出相应答案,但攻击者询问受到协议会话新鲜性约束,即预言机 $\Pi_{i,j}^s$ 满足:1)攻击者没有向预言机 $\Pi_{i,j}^s$ 及其匹配会话 $\Pi_{i,j}^{s'}$ 进行 Reveal 查询;2)参与者 j 都没有被腐化,则称预言机 $\Pi_{i,j}^s$ 是新鲜的。

第 4 阶段 攻击者 A 结束游戏,输出猜测值 b'。

对于任意攻击者 A,如果 A 赢得上述游戏的优势 $\mathrm{Adv}_A=|2\Pr[b'=b]-1|$ 是可忽略的,则称该认证密钥协商协议是安全的。

2 算法设计及方案构造

认证密钥交换协议包括 2 个阶段,即系统建立阶段 Setup 和会话密钥的协商阶段 KeyExchange。

2.1 系统建立阶段

H_1 和 H_2 分别是在 $\{0,1\}^{l_1}$ 和 $\{0,1\}^{l_2}$ 上的抗碰撞哈希函数,通信双方分别使用带消息恢复功能的签名算法,选取 $\{f,g \leftarrow D_f, h \leftarrow f/g \bmod q\}$,生成自己的

签名密钥对:

$\text{SigKeyGen}(1^\lambda)\rightarrow(K_{SA},K_{VA})=(g_A,h_A)$

$\text{SigKeyGen}(1^\lambda)\rightarrow(K_{SB},K_{VB})=(g_B,h_B)$

2.2　会话密钥的协商阶段

用户 U_A 和用户 U_B 通过交换公共信息来协商出一个共享的会话密钥,具体过程如下:

1)用户 U_A 随机选取种子参数 $\rho\leftarrow\{0,1\}^n$,获取公共参数 $a\leftarrow\text{Sam}(\rho)$,采样 $s,e\leftarrow\chi_\alpha$,计算环元素 $b=as+e\in\mathbb{R}_q$,将环元素 b 分为 $(b_1\parallel b_2)$ 作签名消息,用带消息恢复功能的签名算法对 $(b_1\parallel b_2)$ 进行签名,得到 $t=(b_1+F(H'(b))\bmod q\parallel H'(b))$,采样 $s_1,s_2\leftarrow D_s$,使其满足 $(f_A/g_A)s_1+s_2=t \bmod q$。生成签名值 $\text{Sig}(K_{SA},(b_1\parallel b_2))\rightarrow(s_1,s_2,b_2)=\sigma_1$,其中 σ_1 包含可恢复全部消息的 b_2,最后将签名值 σ_1 和种子 ρ 发送给用户 U_B。

2)用户 U_B 收到 σ_1、ρ 后,使用验证算法得到 $(t_1\parallel t_2)\leftarrow h_As_1+s_2\bmod q, b_1\leftarrow t_1-F(t_2)\bmod q$ 验证并恢复得到 $\text{Ver}(K_{VA},\sigma_1)\rightarrow(b_1\parallel b_2)=b$,同时根据验证算法中的要求验证用户 U_A 发送的信息是否满足要求,若 $(s_1,s_2)\parallel<B$ 同时满足 $H'(b_1\parallel b_2)=t_2$,若不满足要求则终止并输出 $\perp$,反之用户 U_B 根据收到的种子参数 ρ,计算 $a\leftarrow\text{Sam}(\rho)$,采样选择 $s',e',e''\leftarrow\chi_\alpha$,计算 $u=as'+e'$。选取 $v\leftarrow\{0,1\}^n$,并利用 Encode 编码函数将 v 编码成环元素 $k=\text{Encode}(H_1(v))\in\mathbb{R}_q$,接着使用编码后得到的 k 加密计算得到环元素 $c=bs'+e''+k\in\mathbb{R}_q$,使用哈希函数得到 $\text{Auth}\leftarrow H_2(\sigma_1,(u,c),k)$,将计算得到的 Auth 和密文 (u,c) 水平拼接得到 $C\leftarrow((u,c)\parallel\text{Auth})$,用带消息恢复功能的签名算法对 C-进行签名:首先,令 $(\overline{C}_1\parallel\overline{C}_2)=\overline{C}$,选取 $s_1',s_2'\leftarrow D_s$,计算得到 $t'=(\overline{C}_1+F(H'(\overline{C}))\bmod q\parallel H'(\overline{C}_1))$,使其满足 $(f_B/g_B)s_1'+s_2'=t'\bmod q$。得到签名值 $\text{Sig}(K_{SB},(\overline{C}_1\parallel\overline{C}_2))\rightarrow(s_1',s_2',\overline{C}_2)=\sigma_2$,其中 σ_2 包含可恢复全部消息的 $\overline{C}_2$,将 σ_2、Auth 发送给用户 U_A,最后计算得到会话密钥 $SK_B\leftarrow H_1(\sigma_1,\sigma_2,H_1(v))$。

3)用户 U_A 收到 σ_2、Auth 后,使用验证算法得到 $(t_1'\parallel t_2')\leftarrow h_Bs_1'+s_2'\bmod q,\overline{C}_1\leftarrow t_1'-F(t_2')\bmod q$ 验证并恢复得到 $\text{Ver}(K_{VA},\sigma_1)\rightarrow(\overline{C}_1\parallel\overline{C}_2)=\overline{C}=(u,c)$,同时并根据验证算法中的要求验证用户 U_A 发送的信息是否满足要求,验证 $(s_1',s_2')\parallel<B$ 与 $H'(\overline{C}_1\parallel\overline{C}_1)=t_2'$,若不满足要求则终止并输出 $\perp$,反之则计算 $k'=c-us$,使用哈希函数验证 $\text{Auth}\overset{?}{=}H_2(\sigma_1,(u,c),k')$,若不满足要求则终止并输出 $\perp$,反之则使用解码函数 $\text{Decode}(k')$ 计算得到 $H_1(v)$,最后使用哈希函数得到会话密钥 $SK_A\leftarrow H_1(\sigma_1,\sigma_2,H_1(v))$。

若按照上述协议执行,最终交易双方得到相同的会话密钥,即 $SK_A=SK_B$,具体的交换过程如图 1 所示。

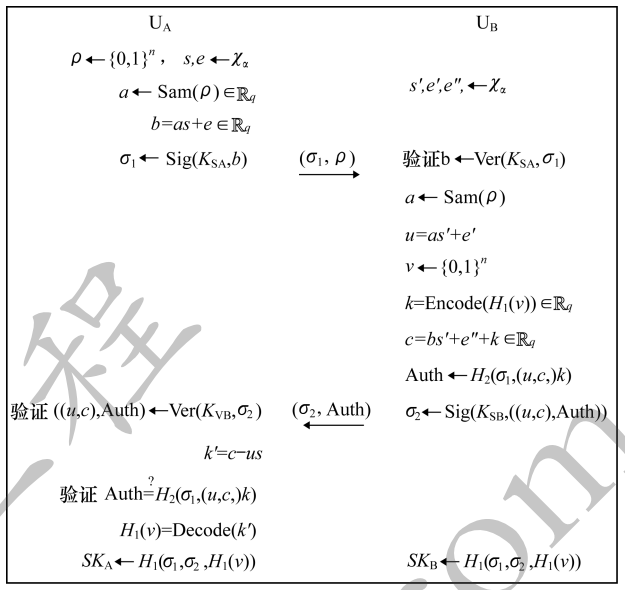

图 1　格上基于 KEM 的 AKE 协议交换过程

Fig. 1　Exchange process of KEM-based AKE protocol on lattice

3　安全性分析

3.1　正确性证明

若用户 U_A 和用户 U_B 诚实地运行协议,那么双方获得相同的密钥 $SK_A=SK_B$ 成立。

证明　用 U_A 计算得到 $k'=c-us=c-ass'-e's$,用户 U_B 计算得到 $k=c-bs'-e''=c-ass'-e's'-e''$,即 $k=k'+e's-es'-e''$,令 $e_2=e's-es'-e''$,其中 $s,s',e,e',e''\leftarrow\chi_\alpha$,根据引理 4,得到 $|e_2|\leqslant8\cdot(\alpha q\sqrt{n})\cdot(\alpha q\sqrt{n})=8(\alpha q)\cdot n\leqslant\frac{q}{4}-2$,由定义 3 可知,取 k'在 $\{0,1,\cdots,q-1\}$ 范围中的 4 个系数减去 $\lfloor q/2\rfloor$,累积其绝对值,即 $t\leftarrow\sum_{j=0}^{3}|v_i+n\cdot j-\lfloor q/2\rfloor|$。又因为 $k=k'+e_2$,$\sum_{j=0}^{3}|v_i+k'\cdot j-\lfloor q/2\rfloor+|e_2||\leqslant\frac{q}{4}+1+|e_2|\leqslant\frac{q-1}{2}$,即 $\text{Decode}(k')=\text{Decode}(k)=H_1(v)$,所以 $SK_A=SK_B$。证毕。

3.2　安全性证明

设 n 是安全参数,$\alpha<(\text{lb}\ n/n)^{1/2}$,$q=1 \bmod m$ 是一个多项式有界的素数且 $\alpha q\geqslant\omega(\sqrt{\text{lb}\ n})$。若 $\text{RLWE}_{q,\chi}$ 是困难问题,则本文方案在标准模型下是 CK 安全的。

证明:通过一系列得模拟游戏,证明通信内容不会泄露秘密的信息,并证明通信双方交换的密钥与随机数不可区分。设 sid^* 表示测试会话标示符,攻击者 A 尝试区分会话密钥 SK 和均匀随机密钥 SK′,

定义攻击者 A 赢得游戏的优势为：

$$\mathrm{Adv}(\mathrm{A})=\left|\Pr[b'=1|b=1]-\Pr[b'=1|b=0]\right|$$

游戏 $\mathbf{G_0}$ 最初的游戏是对所有拥有签名密钥对(K_s,K_v)的诚实用户的攻击。在游戏中，攻击者 A 发送消息 M 进行询问使模拟器 使用他的密钥应答。当攻击者使用 Test-query 对模拟器 进行查询，模拟器 随机选取 $b\in\{0,1\}$ 回答查询，若 $b=1$，返回真实密钥给 A；否则返回 $sk\leftarrow\{0,1\}^{l_1}$。根据定义有：$\mathrm{Adv}_{\mathrm{AKE}}^{\text{fs-ind}}=\mathrm{Adv}_{\mathrm{G}_0}(\mathrm{A})=\left|\Pr[b'=1|b=1]-\Pr[b'=1|b=0]\right|$。

游戏 $\mathbf{G_1}$ 此游戏与游戏 G_0基本相同，不同之处在于：模拟器 P 选取 $s'_b,e'_b,e''_b\leftarrow\chi_\alpha$，选取 $s_a,e_a,\leftarrow\chi_\alpha$，计算 $u=a\,s'_b+e'_b$，选取 $k\in\{0,1\}^n$，计算 $c=bs'_b+e''_b+a\times k\in\mathbb{R}_q$，选取 $\mathrm{Auth}\leftarrow\mathbb{R}_q$ 按照协议计算出 σ_2、并将 σ_2、Auth 发送给攻击者 A。

在签名方案的强不可伪造性下，此修改不会改变攻击者 A 的优势。一旦伪造文件被发现，不需要运行完整个协议，签名方案立即被破坏。同时，c 的分布与其他一般分布不可区分，所以，猜测出 $c=bs'_b+e''_b+a\times k$ 的概率可以忽略。因为 $c=a(s_as'_b+k)+e''_b+e_a$，根据引理 2 可知，$s_as'_b+k$ 的分布与χ_α的分布小于4ε，基本可以忽略，则游戏 G_1 中 c 的分布接近游戏 G_0 中 c 的分布，即 A 无法区分。若$\mathrm{RLWE}_{q,\chi}$是困难问题，则：

$$\left|\mathrm{Adv}_{\mathrm{G}_1}(\mathrm{A})-\mathrm{Adv}_{\mathrm{G}_0}(\mathrm{A})\right|\leqslant\mathrm{negl}(n)$$

游戏 $\mathbf{G_2}$ 此游戏与游戏 G_1基本相同，不同之处在于：模拟器 P 选取 $u\leftarrow\mathbb{R}_q,k\in\{0,1\}^n$，选取 $c\leftarrow\mathbb{R}_q$，计算 $\mathrm{Auth}\leftarrow H_2(\sigma_1,(u,c),k)$，按协议计算 $\sigma_2\leftarrow\mathrm{Sig}(K_{\mathrm{SB}},((u,c),\mathrm{Auth}))$，选取 $SK_{\mathrm{B}}\leftarrow(0,1)^n$，并将 σ_2、Auth 发送给攻击者 A。将游戏 G_2 中随机选取的 SK_{B} 代替游戏 G_1 中的最终密钥，在满足带消息恢复功能签名验证算法条件下，得到验证后的信息满足$(s_1,s_2)\parallel<\mathrm{B}$和$H'(m_1\parallel m_2)=b_2$，并得到$(((u,c),\mathrm{Auth})\leftarrow\mathrm{Ver}(K_{\mathrm{VB}},\sigma_2)$的输出统计接近均匀分布，游戏与游戏计算不可区分，有$\left|\mathrm{Adv}_{\mathrm{G}_2}(\mathrm{A})-\mathrm{Adv}_{\mathrm{G}_1}(\mathrm{A})\right|\leqslant\mathrm{negl}(n)$。会话状态完全随机化，则敌手不能通过 Test 询问获得任何优势。

游戏 $\mathbf{G_3}$ 此游戏与游戏 G_2基本相同，不同之处在于：A 可以重放之前的数据。为抵抗重放攻击，需要猜测哪个会话将要被测试，通过密钥生成算法和加密算法产生：$(K_d^*,K_e^*)\leftarrow\mathrm{KEMKeyGen}(1^\lambda)$和$(c^*,k^*)\leftarrow\mathrm{Enc}(K_e^*)$，嵌入一个特定的元组$(K_d^*,K_e^*,c^*,k^*)$。通过第 q_1 次的 Send-query 猜测第一次发送的 K_e^* 的时间，通过第 q_2 次的 Send-query 查询 c^* 被发送回来的时间。确切而言，之前的测试会话涉及密钥对(K_e^*,c^*)，第一个数据 σ_1^* 是对第q_1 次的 Send-query 的重放，c^* 包含在 σ_1^* 输出到第q_2 次的 Send-query。

模拟器 P 生成一个特定的元组(K_d^*,K_e^*,c^*,k^*)，并猜测 $q_1,q_2\leftarrow\{1,2,\cdots,q_s\}$，$q_s$ 是 Send-query 次数的上限。如果 Send-query 的输入是 σ_1^*，则除了第 q_1 次的 Send-query 用一个签名的 K_e^* 来回答和第 q_2 次的 Send-query 用一个签名的(c^*,Auth^*)来回答，其他所有的查询都像往常一样回答。如果输入的 Send-query 不是 σ_1^*，则中止模拟并输出一个随机的 b_0。概率大于 $1/q_s^2$ 的概率，则猜测是正确的。

通过以上方法，模拟器 P 可以检测出是否攻击者 A 存在重放攻击，攻击者 A 无法获得这些猜测信息，因为模拟器 P 仍然存在使用 K_d^* 用于完成协议的执行，所以重放攻击无效，有$\left|\mathrm{Adv}_{\mathrm{G}_3}(\mathrm{A})-\mathrm{Adv}_{\mathrm{G}_2}(\mathrm{A})\right|\leqslant\mathrm{negl}(n)$。

游戏 $\mathbf{G_4}$ 此游戏与游戏 G_3基本相同，不同之处在于：不再使用 K_d^* 来进行模拟。只有第一个生成 σ_1^* 的实例才会使用 K_d^*，因此攻击者 A 会发送其他的 σ_1^*。在重放的情况下，A 不能提出 Reveal 或 Test 查询，但对于模拟器 P，K_{AS}可以在没有 K_d^* 的情况下进行模拟。所以游戏 G_4 中 A 的优势相比于游戏 G_3 可忽略不计，即$\left|\mathrm{Adv}_{\mathrm{G}_4}(\mathrm{A})-\mathrm{Adv}_{\mathrm{G}_3}(\mathrm{A})\right|\leqslant\mathrm{negl}(n)$。

游戏 $\mathbf{G_5}$ 此游戏与游戏 G_4基本相同，不同之处在于：对于第一次发送 σ_1^* 的特定会话，在 A 提出 Reveal 或 Test 查询的情况下，当 $k'\neq k$ 解密失败时，即使通过 $\mathrm{Ver}(\mathrm{h},\sigma=(s_1,s_2,m_2))$算法认证匹配，也会输出 $sk\rightarrow\perp$。当 $k'\neq k$ 只有在 $H_2(\sigma_1,c,k')=\mathrm{Auth}$ 时存在小的差异：$\mathrm{Adv}_{\mathrm{G}_4}(\mathrm{A})\leqslant\mathrm{Adv}_{\mathrm{G}_3}(\mathrm{A})+\dfrac{1}{2^{l_2}}$。

定义标记 CorrectGuess 来表示是否 $sk\rightarrow\perp$ 解密失败或者 $sk_1\leftarrow sk_2$ 解密成功，模拟器 P 不会显式地计算 CorrectGuess 的值。有：

$$\begin{aligned}\mathrm{Adv}_{\mathrm{G}_5}(\mathrm{A})=&\left|\Pr_{\mathrm{G}_5}[b'=1\wedge\mathrm{CorrectGuess}|b=1]-\right.\\&\left.\Pr_{\mathrm{G}_5}[b'=1\wedge\mathrm{CorrectGuess}|b=0]\right|=\\&\left|\Pr_{\mathrm{G}_4}[b'=1\wedge\mathrm{CorrectGuess}|b=1]-\right.\\&\left.\Pr_{\mathrm{G}_4}[b'=1\wedge\mathrm{CorrectGuess}|b=0]\right|\end{aligned}$$

标记 CorrectGuess 对游戏 G_5 的比特 b'无影响，这两个事件是独立的：$\mathrm{Adv}_{\mathrm{G}_5}(\mathrm{A})=\mathrm{Adv}_{\mathrm{G}_4}(\mathrm{A})/2$。

游戏 $\mathbf{G_6}$ 此游戏与游戏 G_5基本相同，不同之处在于：模拟器 P 不需要 K_d^*，因此，生成元组(K_e^*,c^*,k^*)来稍微修改游戏 G_5，同样，元组中的数值由$(K_d^*,K_e^*)\leftarrow\mathrm{KEMKeyGen}(1^\lambda)$和$(c^*,k^*)\leftarrow\mathrm{Enc}(K_e^*)$生成的，所以得到$\left|\mathrm{Adv}_{\mathrm{G}_6}(A)-\mathrm{Adv}_{\mathrm{G}_5}(\mathrm{A})\right|\leqslant\mathrm{negl}(n)$。

游戏 $\mathbf{G_7}$ 此游戏与游戏 G_6基本相同，不同之处在于：模拟器 不需要 k^*，只给出元组(K_e^*,c^*)，模拟器 P 设置 $\mathrm{Auth}\leftarrow\{0,1\}^{l_2}$和 $sk^2\leftarrow\{0,1\}^{l_1}$。只有攻击者 A 要求将实际封装的密钥 k^* 到 H_1 或 H_2，否则其与真实协议是完美的无法区分。

在最后的游戏中，测试会话的会话密钥是真实随机的，因此与随机的情况没有区别：$\mathrm{Adv}_{\mathrm{G}_7}(\mathrm{A})=0$。

通过以上游戏，可知攻击者 A 的优势是可忽略的。证毕。

4　性能分析

本节对所提出的格上基于 KEM 的认证密钥交换协议方案进行性能分析,性能主要体现在 3 个方面:

1)发送方选择定比特长的随机字符串,将这个随机字符串中每 4 个元素使用 Encode 函数编码其中的一个比特,编码后的环元素可容忍更大的错误,从而降低了模数,缩减了通信量。

2)使用 Compress 压缩函数,对密文元素进行压缩,在保证密文恢复完整性的前提下,有效减少通信量,减轻服务器的传输负荷。

3)利用带消息恢复功能的签名算法,对方案中发送消息进行签名,在发送的过程中,用户双方只需要发送消息的部分值,有效降低了传输过程中的通信量。

定义环 $\mathbb{R}_q=\mathbb{Z}_q[X]/(X^n+1)$,设置 $n=1\ 024$,$q=12\ 289$。从认证性、困难假设和构造方式等方面与同类协议进行比较。方案效率由计算复杂度和通信量组成。计算复杂度主要考虑向量乘法和抽样。通信量考虑发送字节总数。与文献[6,10]方案的分析对比结果如表 1所示。

表 1　AKE 协议效率分析与对比

Table 1　Efficiency analysis and comparison of AKE protocols

方案	认证性	困难假设	构造方式	计算复杂度	通信量/Byte
文献[6]方案	√	LWE	调和机制	$(\bar{n}+\bar{m})(n\,\mathrm{lb}\,q+1)$	22 673
文献[10]方案	×	R-LWE	调和机制	$n+2n\,\mathrm{lb}\,q$	8 320
本文(常规签名算法)	√	R-LWE	加密机制	$3n+2n\,\mathrm{lb}\,q$	4 000
本文(带消息恢复功能签名算法)	√	R-LWE	加密机制	$3n+2n\,\mathrm{lb}\,q$	3 293

本文方案和所对比的方案均为标准模型下构造。由表 1 可以看出,在通信量方面,本文方案采用 Encode 函数和 Compress 压缩函数,大幅缩短了密文的尺寸,有效降低了通信代价,同时使用带消息恢复功能的签名算法,在保证协议认证性的同时,也降低了通信量,与文献[10]方案相比,本文协议不但可实现相互认证,降低了通信量同时避免使用计算复杂的调和机制而使用计算简单的加密机制,方案计算更加简洁高效。本文协议的封装和解封装采用 R-LWE困难假设,与文献[6]相比,解决了密文尺寸过长的问题。

综上可知,与同类方案相比,本文方案具有较低的通信量,计算复杂度也在可接受范围内。因此,从方案的效率参数和计算效率分析,本文协议更具有实际应用价值。

5　结束语

认证密钥交换协议被广泛应用于互联网安全协议和传输层安全协议中,可有效提高实体间的通信效率。本文基于 R-LWE 困难假设,以加密的构造方法代替 Peikert 错误协调机制,提出一种基于 KEM 的认证密钥交换协议。将 KEM 和带消息恢复功能的数字签名相结合,实现协议的认证性,同时降低需要发送的签名密文长度,大幅减少通信量。利用格上基于 R-LWE 问题构造的密码系统具有密钥、密文尺寸小的优点,可提高 AKE 协议效率,并且有效抵抗量子攻击。本文方案基于 R-LWE 困难假设构造,而 LWE 的安全性较 R-LWE 更为稳健,下一步将考虑在维持较低通信量的情况下,基于 LWE 构造强安全的认证密钥交换方案。

参考文献

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

[2] LI Zichen, ZHANG Yaze, ZHANG Fengjuan. A new authenticated key exchange protocol based on binary-LWE[J]. Computer Applications and Software, 2017, 34(11):290-295. (in Chinese)
李子臣,张亚泽,张峰娟. 一种新型基于 Binary-LWE 的认证密钥交换协议[J]. 计算机应用与软件,2017,34(11):290-295.

[3] WANG Shanbiao,ZHU Yan,MA Di,et al. Lattice-based key exchange on small integer solution problem[J]. Science China (Information Sciences),2014,57(11):145-156.

[4] JING Zhengjun,GU Chunsheng,YU Zhimin. Cryptanalysis of lattice-based key exchange on small integer solution problem and its improvement[J]. Cluster Computing, 2018,22:1717-1727.

[5] WEI Fushan, MA Jianfeng, LI Guangsong, et al. Efficient three-party password-based authenticated key exchange protocol in the standard model[J]. Journal of Software,2016,27(9):2389-2399. (in Chinese)
魏福山,马建峰,李光松,等. 标准模型下高效的三方口令认证密钥交换协议[J]. 软件学报,2016,27(9):2389-2399.

[6] BOS J, COSTELLO C J, DUCAS L, et al. Frodo: take off the ring! practical, quantum-secure key exchange from LWE [C]//Proceedings of ACM SIGSAC Conference on Computer and Communications Security. New York,USA:ACM Press,2016:1006-1018.

[7] DING Jintai, XIE Xiang, LIN Xiaodong. A simple provably secure key exchange scheme based on the learning with errors problem[EB/OL]. [2019-05-10]. https://eprint.iacr.org/2012/688.pdf.

[8] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings[J]. Journal of the ACM,2010,60(6):1-23.

[9] PEIKERT C. Lattice cryptography for the Internet[C]// Proceedings of the 6th International Workshop on Post-Quantum Cryptography. Waterloo, Canada: [s. n.], 2014:197-219.

[10] BOS J W, COSTELLO C, NAEHRIG M, et al. Post-quantum key exchange for the TLS protocol from the ring learning with errors problem[C]//Proceedings of 2015 IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 2015:553-570.

[11] ALKIM E, DUCAS L, POPPELMANN T, et al. Post-quantum key exchange: a new hope[C]//Proceedings of USENIX Security Symposium. [S. l.]: USENIX, 2016: 327-343.

[12] ALKIM E, DUCAS L, POPPELMANN T, et al. NewHope without reconciliation[EB/OL]. [2019-05-10]. https://cryptojedi. org/papers/newhopesimple-20161217. pdf.

[13] BOS J, DUCAS L, KILTZ E, et al. CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM[EB/OL]. [2019-05-10]. https://eprint. iacr. org/2017/634. pdf.

[14] JIAN Hongyu. Provably secure authenticated Diffie-Hellman key exchange for resource-limited smart card[J]. Journal of Shanghai Jiaotong University (Science), 2014, 19(4): 436-439.

[15] ZHANG Chao, ZHANG Quan, TANG Chaojing. Computationally sound mechanized proofs for Diffie-Hellman key exchange protocols[J]. Journal of Communications, 2011, 32(10): 118-126. (in Chinese)
冯超, 张权, 唐朝京. 计算可靠的 Diffie-Hellman 密钥交换协议自动证明[J]. 通信学报, 2011, 32(10): 118-126.

[16] ALBRECHT M R, ORSINI E, PATERSON K G, et al. Tightly secure ring-LWE based key encapsulation with short ciphertexts[C]//Proceedings of European Symposium on Research in Computer Security. Berlin, Germany: Springer, 2017:29-46.

[17] PINO R D, LYUBASHEVSKY V, POINTCHEVAL D. The whole is less than the sum of its parts: constructing more efficient lattice-based AKEs[C]//Proceedings of International Conference on Security and Cryptography for Networks. Berlin, Germany: Springer, 2016:273-291.

[18] FUJIOKA A, SUZUKI K, XAGAWA K, et al. Strongly secure authenticated key exchange from factoring, codes, and lattices[J]. Designs, Codes and Cryptography, 2015, 76(3):469-504.

[19] FUJIOKA E, OKAMOTO T. How to enhance the security of public-key encryption at minimum cost[C]// Proceedings of International Workshop on Public Key Cryptography. Berlin, Germany: Springer, 1999:53-68.

[20] WANG Caifen, CHEN Li. Three-party password authenticated key agreement protocol with user anonymity based on lattice[J]. Jourhal of Communications, 2018, 39(2):21-31. (in Chinese)
王彩芬, 陈丽. 基于格的用户匿名三方口令认证密钥协商协议[J]. 通信学报, 2018, 39(2):21-31.

编辑 金胡考