Software Engineering and Applications 软件工程与应用, 2021, 10(2), 185-194
Published Online April 2021 in Hans. http://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2021.102022

Hans汉斯

基于RLWE认证密钥协商算法的设计

黄秀菊，李子臣

北京印刷学院信息工程学院，北京
Email: xiujuhuang@163.com

收稿日期：2021年2月18日；录用日期：2021年4月22日；发布日期：2021年4月29日

摘　要

密钥协商算法允许参与者在非安全信道中交换信息共同协商会话密钥用于保密通信，是密码学中最关键技术之一。本文基于RLWE困难问题，利用四舍五入密钥共识算法，Filtering引理及哈希函数，设计了一个新的基于RLWE困难问题的认证密钥协商算法。新的认证密钥协商算法具有高效与可证明安全的特点。

关键词

RLWE，数字签名，密钥协商

Design of Authenticated Key Agreement Algorithm Based on RLWE

Xiuju Huang, Zichen Li

School of Information Engineering, Beijing Institute of Graphic Communication, Beijing
Email: xiujuhuang@163.com

Received: Feb. 18th, 2021; accepted: Apr. 22nd, 2021; published: Apr. 29th, 2021

Abstract

Key agreement algorithm allows participants to exchange information in the open channel to generate a secure temporary session key to ensure secret communication, which is one of the key technologies in cryptography. In this paper, a novel authenticated key agreement algorithm based on RLWE difficulty problem is proposed using rounded key consensus algorithm, filtering lemma and hash function. The new authenticated key agreement algorithm is proved to be efficient and provably secure.

文章引用: 黄秀菊, 李子臣. 基于 RLWE 认证密钥协商算法的设计[J]. 软件工程与应用, 2021, 10(2): 185-194.
DOI: 10.12677/sea.2021.102022

Keywords

RLWE, Digital Signature, Key Agreement

1. 引言

格是一种建立在偏序集合上的代数结构，起源于 1611 年开普勒提出的关于容器内堆放等半径小球所达最大密度的猜想。后来格作为一种密码分析工具用于攻击破解密码体制[1] [2]。1996 年，美国布朗大学的 Jeffrey Hoffstein、Jill Pipher 和 Joseph H. Silverman 三位数学教授发明了一种公钥密码体制 NTRU [3]。2009 年，Gentry 基于格密码构造了首个全同态密码方案[4]，格密码得到极大的发展。2015 年美国国家标准研究和技术研究学院发布了“后量子密码报告”[5]。报告表明，由于计算机运算速度的不断提高，现有的公钥密码在未来面临着极大的挑战。NIST 在全球范围内征集后量子密码算法标准。具有抗量子计算的格密码公被认为最具竞争力的后量子算法。尤其近几年格密码得到快速发展，许多优秀的研究成果[6] [7] [8]如雨后春笋一般出现。

近几年国内在后量子密码算法研究方面也取得了很大的进展。2018 年 6 月，由国家密码管理局指导，中国密码学会同密码行业标准化技术委员会，商用密码检测中心共同组织实施，全国密码算法设计竞赛开始，历时一年半，于 2019 年 12 月分别遴选出公钥密码算法和分组密码算法一、二、三等奖[9]。

国内外格密码发展一片欣欣向荣，产生很多优秀的算法。[10] [11]等论文直接使用格困难问题设计密钥封装方案，具有高效与可证明安全性的特点。J. W. Bos，L. Ducas，E. Kiltz，T. Lepoint 等人提出了一种基于 CCA 安全加密的可认证密钥交换通用结构[12]，在此论文中提到了一种通用的数字签名方案，具有简单直接的特点，但签名过程较为繁琐效率低，且有私钥泄露的风险，不具备完全向前保密性。[13] [14]提出将密钥共识机制与 RLWE 困难问题相结合的方案，此类方案较为成熟，现在仍未发现有效的破解方案，丰富了密钥封装方案的思路。但是这些密钥协商方案没有认证的功能，也就是在密钥协商过程中没有对双方的身份和收到的消息进行认证。

本文基于 RLWE 困难问题，结合数字签名技术，设计了一种更加安全高效的具有认证功能的密钥协商算法。算法仅用一对密钥对进行加密处理，通过中止技术来解决私钥泄露问题。由于在签名方案中，不存在交互，因此签名者不需要将中止的签名包含到最终签名中。如果签名者需要中止，他只需重新运行协议，直到获得正确范围内的签名。这样可以提高签名效率，从而保证通信的安全性，高效性，真实性，不可抵赖性和完整性。

2. 基础知识

2.1. 定义与符号

本文将用粗体小写字母表示矢量，大写字母表示矩阵。比如，$\boldsymbol{a}_1$，$\boldsymbol{a}_2$ 是 Z^n 的两个元素，$A=(\boldsymbol{a}_1,\boldsymbol{a}_2)$。默认情况下，所有向量都是列向量。对于一个向量 $\boldsymbol{a}$ (或矩阵 A)，我们用 $\boldsymbol{a}^{\mathrm{T}}$ (或 A^{T})表示它的转置。对于实数 $x\in R$，我们使用$\lfloor x\rfloor$表示向下取整，即$\lfloor x\rfloor$表示不大于 x 的最大整数。定义 x 的四舍五入表示：$\lfloor x\rceil=\lfloor x+1/2\rfloor$，当 $\boldsymbol{x}$ 为向量、矩阵或者多项式运算时，上面所定义的四舍五入和向下取整均是对分量或

系数进行的运算。

设 Z 是有理整数环，设 $R=Z[X]/(\Phi_m(X))$ 是第 m 个割圆数域的整数环，$\Phi_m \in Z[X]$ 是 m 次割圆多项式。本文中采用 $\Phi_m = x^n+1$，$n=2^r$，$r>0$，$m=2n$。本文规定 q 是素数且 $q \equiv 1(\bmod 2n)$，$R_q = R/qR \cong Z_q[X]/(X^n+1)$，其中 $Z_q = Z/qZ$。$\boldsymbol{y} \leftarrow R_q$，表示 y 的每个分量或系数均独立地服从分布 R_q，且 $\boldsymbol{y}$ 的系数属于集合 $[-(q-1)/2,(q-1)/2]$。用符号 $\boldsymbol{x}' = \boldsymbol{x} \bmod q$，$q$ 为正整数，表示 $\boldsymbol{x}'$ 的系数属于集合 $[0,q-1]$，$\boldsymbol{x}' = \boldsymbol{x} \bmod^{\pm} q$，$q$ 为正整数，表示 $\boldsymbol{x}'$ 的系数范围属于集合 $\left[-\lfloor (q-1)/2 \rfloor, \lfloor (q-1)/2 \rfloor\right]$。$a$ 的无穷范数写做 $\|\boldsymbol{a}\|_\infty$，对于 $A=(\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_m)$，$\|\boldsymbol{A}\|_\infty = \max_i \|\boldsymbol{a}\|_\infty$。最后本文采用与 Kyber [12]原算法中同样的噪声分布 B_η，其定义如下：

$$(a_1,\cdots,a_\eta,b_1,\cdots,b_\eta) \leftarrow (0,1)^{2\eta} \text{ 输出 } \sum_{i=1}^{\eta}(a_i-b_i) \tag{1}$$

2.2. 格

定义：设 $x_1,x_2,\cdots,x_m$ 是 n 维空间 R^n 上线性无关的向量，m 维格 $L(x_1,x_2,\cdots,x_m)$ 是由向量 $x_1,x_2,\cdots,x_m$ 生成的一个向量集，形式表示为

$$L(x_1,x_2,\cdots,x_m) = \sum_{i=1}^{m} a_i x_i, a_i \in Z \tag{2}$$

其中，$\{x_1,x_2,\cdots,x_m\}$ 是格 L 的一组基，记为 $\mathrm{Dim}(L)=m$，(m, n)分别为格 L 的维数和秩，当 $m = n$ 时称为格 L 是满秩。同样的一个格可以采用不同的基底来表示，但是从 m 维格中选出 m 个线性无关的向量却不一定能成为这个格的一组基。一个格基通过左乘一个特定矩阵可以转化成另一个格基，这个特定的矩阵是由整数构成，且其行列式为±1。因此格具有离散性和格基多样性。

2.3. 基于格的困难性假设

2009 年 REGEV O 首先提出了 LWE (learning with errors)问题[15]，是对最坏情况格困难问题如 GAPSVP 和 SIVP 的一个简化，并证明 LWE 的安全性基于 GAPSVP 和 SIVP 最坏情况的困难问题，近年来它已经成为很多密码应用的基础。

LWE 可看作随机线性码的译码问题，给出如下定义：$x \in Z_p^n$ 是某个向量矩阵，存在矩阵 $Q \in Z_p^{m\times n}$，使得 $y = Qx+e$，e 是一个服从 $e \in Z_p^m$ 的干扰信号，LWE 问题就是已知 Q 和 y，求 x。由于 LWE 在实际生产应用过程中效率较低，Lyubashevsky，C. Peikert 和 O. Regev 在 LWE 的基础上变形出了一种效率更高，安全性和复杂性规约为 SVP 问题的新问题 R-LWE (Learning with Errors over Rings) 困难问题[16]。R-LWE 问题和 LWE 问题的定义很相似，可以视为一个样本结构固定了的 LWE 问题。现 R-LWE 困难问题是基于格密码学一个活跃的研究领域，在这个困难问题上产生了很多优秀成果[17] [18] [19]。

2.4. 基于格 R-LWE 的数字签名算法

数字签名是一种以电子形式给一个消息签名的过程，只有消息发送方可以对自己信息进行签名，任意知道公钥的验证者都可以对其进行验证。数字签名可以起到身份认证，保证信息完整性，不可否认性以及匿名性等作用，具有不可伪造性和不可抵赖性。

一个数字签名的形式化定义如下：

系统初始化过程：数字签名含有基本元素为(*P*, *M*, *K*, *S*, *V*)，其中 *P* 为消息集，*M* 为签名集，*K* 为密钥集合，*S* 为签名算法集合，*V* 为验证算法集合。

签名产生过程：$k \in K$ 对于每一个消息 $p \in P$ 和 $m \in M$，存在 $sig_k \in S$，$sig_k : P \to M$。将签名消息

组(p, m)发送给消息验证者进行验证。

签名认证过程：对于每一个$k \in K$存在一个相应的验证算法$ver_k \in V$，对收到的签名消息组进行验证，$ver_k : P \times M \to \{T, F\}$，

$$ver_k(p,m) = \begin{cases} T, m = sig_k(p) \\ F, m \neq sig_k(p) \end{cases} \tag{3}$$

若$ver_k(p,m) = T$，则签名验证通过，签名有效，否则签名无效。

本文要用的是基于格 R-LWE 的数字签名方案。构造格的数字签名算法大部分分为两种途经，一种是利用限门函数[20]进行设计的，另一种是基于 Fiat-Shamir 方法进行转化，后者具有简单高效的特点，因此成为这个算法的首要选择方案。由于格的特殊代数结构，如果直接输出算法的签名，会泄露密钥，为解决这个问题 VadimLyubashevsky 提出“异常终止”的概念[21]。中止协议的目的是，验证方可以选择中止协议，以保护有关其密钥的一些信息。本文使用的是均匀分布拒绝抽样格签名，使用的技术为 Filtering 引理。

Filtering引理，即涉及均匀分布的拒绝抽样算法。只有签名者输出的签名当且仅当落在一个固定的区间之内，签名的输出分布就会服从该区间上的均匀分布，故不会泄露私钥的信息。

Filtering引理定义：设k是一个正整数，$a \in \{v \in Z^k : \|\mathbf{v}\|_\infty \le A\}$，随机均匀地选取$b \leftarrow \{v \in Z^k : \|\mathbf{v}\|_\infty \le B\}$，其中$B > A$。设随机变量$c = a + b$，那么$c$服从于集合$\{v \in Z^k : \|\mathbf{v}\|_\infty \le B - A\}$的均匀分布。

基于格 R-LWE 的数字签名算法的步骤如下：

签名者

密钥产生Gen:

$(s,e) \leftarrow S_\eta^{L\times 1} \times S_\eta^{L\times 1}$，且其系数服从某个窄的分布

$a \leftarrow R_q^{L\times L}$

$t := as + e \in R_q^{L\times 1}$

返回公钥 $pk = (a,t)$和私钥 $sk(s,e)$验证者

签名算法$\sigma = (z_1, z_2, c) \leftarrow Sign(sk, \mu)$：

1 $(y_1, y_2) \leftarrow R_q^{L\times 1} \times R_q^{L\times 1}$且系数属于$[-k, k]$

2 $w := ay_1 + y_2 \in R_q^{L\times 1}$

3 $c := H(w, \mu)$

4 $z_1 := sc + y_1, z_2 := ec + y_2$

$L_1 := |sc|_\infty, L_2 := |ec|_\infty$

5 如果$|z_1|_\infty > k - L_1$或者$|z_2|_\infty > k - L_2$返回步骤 1

返回签名$\sigma = (z_1, z_2, c)$

验证算法$Verify(pk, \mu, \sigma)$：

如果$|z_1|_\infty > k - L_1$或者$|z_2|_\infty > k - L_2$，返回拒绝

当$c \neq H(az_1 + z_2 - tc, \mu)$，返回拒绝

其他情况返回接受

事实上，

$$\begin{aligned} az_1 + z_2 - tc &= a(sc + y_1) + ec + y_2 - tc = asc + ay_1 + ec + y_2 - tc \\ &= (as + e)c + ay_1 + y_2 - tc = tc + ay_1 + y_2 - tc = ay_1 + y_2 = w \end{aligned}$$

故，$H(w, \mu) = H(az_1 + z_2 - tc, \mu)$

本方案的安全性主要取决于它的可靠性和在哈希函数中发现冲突的难度，只要我们设置合适的参数，以目前的已知技术在哈希函数中寻找冲突是不可行的。

2.5. 密钥协商机制

密钥协商机制是指两人或者多人，在不需要可信第三方的情况下，所有参与者在一个开放网络环境中，利用自己长期密钥对等信息，通过某种密钥协商协议，生成一个共享的临时会话密钥。密钥协商协议是一类极其重要的基础性安全协议。现存的比较高效成熟的密钥协商机制主要是利用 RSA 公钥体制、传统椭圆曲线公钥体制 ECC 和 Diffie-Hellman 密钥协商体制来实现的。这些传统的算法大都基于大数分解问题，椭圆曲线等数学问题。随着量子的不断发展，计算速度的不断加快，这些算法抵制不了量子计算机时代的带来。基于后量子密码的密钥协商问题也成为热门话题。本文使用的是密钥共识与格困难问题相结合的方法，在这里我们先介绍一种带噪音的四舍五入密钥共识算法。

密钥共识算法 KC 如下定义：

KC = (*parameters*, *com*, *che*)，其中参数 $\text{parameters}=(q,r,b,e,aupa)$，$q$ 控制安全性和效率，r 控制共识密钥的范围，b 控制带宽，e 控制错误率，*aupa* 表示辅助参数，且满足 $2re\le q(1-1/b)$，$r\ge 2$，$b\le q$，$0\le e\le \lfloor q/2\rfloor$

含噪声的四舍五入算法

1：$\text{parameters}=(q,r,b,e,aupa)$，$aupa=\{q'=lcm(q,r),\alpha=q'/q,\beta=q'/r\}$

2：**procedure** $Com(\sigma_1, parameters)$ ▷表示在 $\sigma_1, parameters$ 的输入下*Com*输出k_1，v

3：$\sigma_1'=\sigma_1 \bmod q$ ▷把 σ_1' 的系数范围变成$[0,q-1]$

4：$w\leftarrow\left[-\lfloor(\alpha-1)/2\rfloor,\lfloor(\alpha-1)/2\rfloor\right]$

5：$\sigma_A=(\alpha\sigma_1'+w)\bmod q'$

6：$k_1=\lfloor\sigma_A/\beta\rceil \bmod r\in Z_r$

7：$v'=\sigma_A \bmod^{\pm}\beta$

8：$v''=\lfloor v'b/\beta\rceil$

9：$v=v''\bmod^{\pm} q$

10：**return** (k_1, v)

11：**end procedure**

12：**procedure** $Che(\sigma_2, v, parameters)$ ▷表示在 $\sigma_2, v, parameters$ 的输入下*Che*输出k_2

13：$\sigma_2'=\sigma_2 \bmod q$ ▷$\sigma_2'\in[0,q-1]$

14：$v'''=v\bmod q$

15：$k_2=\lfloor\alpha\sigma_2'/\beta-v'''/b\rceil \bmod r$

16：**return** k_2

17：**end procedure**

KC 算法正确性证明：对于任意 $\sigma_1,\sigma_2\in Z_q$，且 $|\sigma_1-\sigma_2|_q\le e$，都有 $k_1=k_2$。

证明：假设 $|\sigma_1-\sigma_2|_q\le e$，存在 $\theta\in Z$ 并且 $\delta\in[-e,e]$ 使得 $\sigma_2=\sigma_1+\theta q+\delta$。从算法 KC 的第 5 行到第 7 行可知，存在 $\theta'\in Z$，使得 $\alpha\sigma_1+w+\theta' q'=\sigma_A=k_1\beta+v'$。从 α 和 β 的定义中，我们有 $\alpha/\beta=r/q$。将这两个等式带入到 *Che* (算法 1 的第 15 行)中 k_2 的等式中可知

$$\begin{aligned}k_2 &= \lfloor \alpha\sigma_2'/\beta - v'''/b \rceil \bmod r\\ &= \lfloor \alpha(\theta q + \sigma_1 + \delta)/\beta - v''/b \rceil \bmod r\\ &= \lfloor \alpha\theta q/\beta + \alpha\sigma_1/\beta + \alpha\delta/\beta - v''/b \rceil \bmod r\\ &= \lfloor r(\theta - \theta') + 1/\beta(k_1\beta + v' - w) + \alpha\delta/\beta - v''/b \rceil \bmod r\\ &= \lfloor k_1 + (v'/\beta - v''/b) - w/\beta + \alpha\delta/\beta \rceil \bmod r\end{aligned}$$

注意到$|v'/\beta - v''/b| = |v'b - \beta v''|/\beta b \le 1/2b$，故

$$|(v'/\beta - v''/b) - w/\beta + \alpha\delta/\beta| \le 1/(2b) + \alpha/\beta(e + 1/2)$$

由假设的条件$2re \le q(1-1/b)$,我们可以得到右边的严格小于 1/2，因此，在取整之后，有$k_1 = k_2$。

KC 算法安全性证明：当变量满足$\sigma_1 \to Z_q$，k_1，v 是相互独立且 k_1 均匀分布，因此 KC 算法具有安全性。

证明：定义一个映射 $f: Z_r \times Z_\beta \to Z_{q'}$，$f(k_1, v') = \beta k_1 + v'$ 显然 f 满足一一映射关系，有 KC 算法第 7 行可以知道 $f(k_1, v') = \beta k_1 + v' = \sigma_A$，因此 σ_A 服从 $Z_{q'}$ 中均匀分布。所以 (k_1, v') 服从 $Z_r \times Z_\beta$ 中均匀分布，且相互独立，而 v 只受 v' 影响不受 k_1 影响，可证明 k_1，v 是相互独立且 k_1 均匀分布。

3. 基于 RLWE 认证密钥协商算法

根据我们在预备知识中介绍的数字签名与密钥协商的知识，本文提出一个基于格的可认证密钥协商方案，方案介绍如下：

密钥生成：这里使用种子*seed*生成矩阵

(1) $seed \leftarrow \{0,1\}^k$ $A = Gen(seed) \in R_q^{L\times L}$ R_q的系数$\in \left[-\lfloor (q-1)/2 \rfloor, \lfloor (q-1)/2 \rfloor\right]$

(2) $X_1, E_1 \leftarrow B_\eta^{L\times 1}$ 随机生成私钥 $sk_1(X_1, E_1)$

(3) $Y_1 = AX_1 + E_1$ 生成公钥 Y_1

数字签名验证：

Initiator → Responder

(1) $\sigma_1 = (z_1, z_2, c) \leftarrow Sign(sk_1, Y_1)$ 使用密钥对对Initiator公钥进行数字签名

(2) $Verify(Y_1, \sigma_1)$，对Y_1进行验证

Responder → Initiator

(1) $\sigma_2 = (z_1, z_2, c) \leftarrow Sign(sk_2, Y_2, V)$，　　使用临时密钥对 Y_2 和V进行数字签名

(2) $Verify(Y_2, V, \sigma_2)$

密钥协商：

(1) $X_2, E_2 \leftarrow B_\eta^{L\times 1}$，$E_\sigma \leftarrow B_\eta$

(2) $Y_2 = A^T X_2 + E_2$　　$sk_2(X_2, E_2)$

(3) $\sum_2 = Y_1^{\mathrm{T}} X_2 + E_\sigma$

(4) $(K_2, V) \leftarrow Com(\sum_2, parameters)$

(5) $\sum_1 = X_1^{\mathrm{T}} Y_2$

(6) $K_1 = Che(\sum_1, V, parameters)$

总流程图如下所示：

Initiator Responder

$seed \leftarrow \{0,1\}^k$

$A = Gen(seed) \in R_q^{L\times L}$ R_q的系数$\in \left[-\lfloor (q-1)/2 \rfloor, \lfloor (q-1)/2 \rfloor\right]$

$X_1, E_1 \leftarrow B_\eta^{L\times 1}$

$Y_1 = AX_1 + E_1$ 公钥Y_1和私钥$sk_1(X_1, E_1)$

$\sigma_1 = (z_1, z_2, c) \leftarrow Sign(sk_1, Y_1)$ σ_1为对Y_1数字签名返回值

z_1, z_2为返回的辅助验证信号，c为返回HASH值

$\sigma_1, Y_1, seed$ →

Verify(Y_1，σ_1)

通过验证算法继续，未通过算法中断，重新开始

A = Gen(seed)

$X_2, E_2 \leftarrow B_\eta^{L\times 1}$， $E_\sigma \leftarrow B_\eta$

$Y_2 = A^T X_2 + E_2$ 私钥$sk_2(X_2, E_2)$

$\sum_2 = Y_1^T X_2 + E_\sigma$

$(K_2, V) \leftarrow Com(\sum_2, parameters)$

$\sigma_2 = (z_1, z_2, c) \leftarrow Sign(sk_2, Y_2, V)$

← σ_2, Y_2, V

Verify(Y_2, V, σ_2)

通过验证算法继续，未通过算法中断，重新开始

$\sum_1 = X_1^T Y_2$

$K_1 = Che(\sum_1, V, parameters)$

4. 算法分析

4.1. 正确性分析

由第二章方案流程图可知：$\sum_2 = Y_1^T X_2 + E_\sigma = (AX_1 + E_1)^T X_2 + E_\sigma = X_1^T A^T X_2 + E_1^T X_2 + E_\sigma$

$\sum_1 = X_1^T Y_2 = X_1^T (A^T X_2 + E_2) = X_1^T A^T X_2 + X_1^T E_2$。

故

$$\left|\sum_2 - \sum_1\right|_q = \left|X_1^T A^T X_2 + E_1^T X^2 + E_\sigma - \left(X_1^T A^T X_2 + X_1^T E_2\right)\right|_q = \left|E_1^T X_2 + E_\sigma - X_1^T E_2\right|_q$$

因为我们X_1, E_1, X_2, E_2均随机取自均匀二项分布$B_\eta^{L\times 1}$，他们都是很小的取值，因此可以确定$\left|\sum_2 - \sum_1\right|_q \le e$，由 1.5 可知，当我们密钥共识的两个输入值距离$\left|\sum_2 - \sum_1\right|_q \le e$，时，就可以推出$K_1 = K_2$。密钥共识算法的正确性与安全性已证，请看 1.5。

4.2. 安全性分析

1) CCA2 可证明安全。我们在这里设计一个游戏 G0

Game G0：

1: $A \leftarrow R_q^{L\times L}$

2: $X_1, E_1 \leftarrow B_\eta^{L\times 1}$

3: $Y_1 = AX_1 + E_1$

Continued

4: $X_2, E_2 \leftarrow B_\eta^{L\times 1}$

5: $Y_2 = A^{\mathrm{T}} X_2 + E_2$

6: $E_\sigma \leftarrow B_\eta$

7: $\sum_2 = Y_1^{\mathrm{T}} X_2 + E_\sigma$

8: $\left(K_2^0, V\right) \leftarrow Con\left(\sum_2, params\right)$

9: $K_2^1 \leftarrow Z_m^n$

10: $\boldsymbol{b} \leftarrow \{0,1\}$

11: $\boldsymbol{b}' \leftarrow A\left(A, Y_1, \lfloor Y_2 / 2^{t1} \rceil, K_2^b, V\right)$

在此游戏中，任意一个敌手 A 都不能以绝对的优势可以分辨出 K_2^1 和 K_2^0 那个是算法产生的，那个是随机选取的，即绝对值 $\left|\Pr\left[b' = b\right] - 1/2\right|$ 是可忽略的。

2) 已知密钥安全：对于参与多个协议的参与者，一次共享密钥的泄露不会影响其他共享密钥的安全进行，换句话说，攻击者 A 无法根据本次的共享密钥得出参与者的其他共享密钥，称为该方案满足已知密钥安全。

此方案共享密钥的生成不仅与参与者的公钥和私钥有关，且与含噪声的四舍五入 KC 协议有关，K_1，K_2 是在一个范围内近似相同，所以攻击者即使知道共享密钥的值，也不能推测出关于密钥对的相关信息，即满足已知密钥安全。

3) 可抵抗中间人攻击：由于数字签名的存在，此算法可以抵抗中间人攻击。此数字签名具有安全性与不可复制性。有主动性敌手，在不知道私钥的情况下，没有办法攻击成功。由于数字签名特点，也使这个算法具有了密钥泄露伪装安全，即在一方长期泄露密钥的情况下，仍没有办法通过数字签名认证，从而实现共享密钥生成。

4) 密钥控制安全：由于本方案中密钥的建立是由所有参与者的密钥对信息共同参与生成，因此共享密钥的生成是具有随机性和不可预测性，任何一个参与者或者敌手都不能把共享密钥设定为某个确定的值，此方案符合密钥控制安全。

4.3. 效率分析

本方案是在环格的基础上设计的一个带数字签名的密钥协商方案，相对于标准格，R-LWE 相对于 LWE 允许在相同通信量的情况下传输更大的消息。此方案中使用的基于 RLWE 的密钥协商协议与其他协议方案相比较，相应计算量和通信量明显减少，是一种简洁高效的后量子 PAKE 协议，这里[14]对此密钥协商方案有详细效率分析。而我们在前面讲过，CCA 安全公钥加密的认证密钥交换通用构造在数字签名部分具有效率低的缺点，而我们改进使用基于 R-LWE 带异常终止的数字签名，相对于其他数字签名具有更好安全性与高效性。因此整个方案相对于使用 CCA 安全公钥加密的认证密钥交换通用构造效率更高。

5. 总结

本文是在阅读大量相关文献后设计的一个在格 R-LWE 困难问题上可认证密钥协商方案。该方案使用了密钥协商与数字签名，具有安全性，高效性，真实性，不可抵赖性和完整性的特点，但仍存在着效率以及实用性的问题，下一步准备把这个方案与现实场景相结合，提高它的实际工作效率，实现这个方案

的价值。

基金项目

国家自然科学基金(61370188)；北京市教委科研计划一般项目(KM202010015009)；北京市教委科研计划资助(No. KM202110015004)；北京印刷学院博士启动金项目(27170120003/020)；BIGC Project (Ec202007)。

参考文献

[1] Shamir, A. (1984) A Polynomial-Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem. *IEEE Transactions on Information Theory*, **30**, 699-704. https://doi.org/10.1109/TIT.1984.1056964

[2] Coppersmith, D. (1996) Finding a Small Root of a Univariate Modular Equation. *International Conference on the Theory and Applications of Cryptographic Techniques*, Vol. 1070, 155-165. https://doi.org/10.1007/3-540-68339-9_14

[3] Hoffstein, J., Pipher, J. and Silverman, J.H. (1998) NTRU: A Ring-Based Public Key Cryptosystem. *International Algorithmic Number Theory Symposium*, Vol. 1423, 267-288. https://doi.org/10.1007/BFb0054868

[4] Gentry, C. (2009) Fully Homomorphic Encryption Using Ideal Lattices. *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, Bethesda, MD, May 2009, 169-178. https://doi.org/10.1145/1536414.1536440

[5] Chen, L., Jordan, S., *et al.* (2016) Report on Post-Quantum Cryptography. US Department of Commerce, National Institute of Standards and Technology, Gaithersburg.

[6] Micciancio, D. and Regev, O. (2009) Lattice-Based Cryptography. In: Bernstein, D.J., Buchmann, J. and Dahmen, E., Eds., *Post-Quantum Cryptography*, Springer, Heidelberg, Berlin, New York, 147-191. https://doi.org/10.1007/978-3-540-88702-7_5

[7] Wang, X.Y. and Liu, M.J. (2014) Survey of Lattice-Based Cryptography. *Journal of Cryptologic Research*, **1**, 13-27.

[8] 李子臣, 谢婷, 张卷美, 等. 基于 RLWE 的后量子认证密钥交换协议[J]. 计算机研究与发展, 2019, 56(12): 2694-2701.

[9] 中国密码协会. 全国密码算法设计竞赛公钥参赛算法[EB/OL]. http://sfjs.cacrnet.org.cn/site/term/list_72_1.html

[10] 高昕炜. 基于 RLWE 的后量子密钥交换协议构造和应用[D]: [硕士/博士学位论文]. 北京: 北京交通大学, 2019.

[11] Zhang, J., Yu, Y., Fan, S., *et al.* (2020) Tweaking the Asymmetry of Asymmetric-Key Cryptography on Lattices: Kems and Signatures of Smaller Sizes. *IACR International Conference on Public-Key Cryptography*, Vol. 12111, 37-65. https://doi.org/10.1007/978-3-030-45388-6_2

[12] Bos, J., Ducas, E., Kiltz, E., *et al.* (2018) CRYSTALS—Kyber: A CCA-Secure Module-Lattice-Based KEM. 2018 *IEEE European Symposium on Security and Privacy* (*EuroS&P*), London, UK, 353-367. https://doi.org/10.1109/EuroSP.2018.00032

[13] Ding, J., Gao, X., Takagi, T. and Wang, Y. (2019) One Sample Ring-LWE with Rounding and Its Application to Key Exchange. *International Conference on Applied Cryptography and Network Security*, Colombia, 5-7 June 2019, 323-343. https://doi.org/10.1007/978-3-030-21568-2_16

[14] Jin, Z. and Zhao, Y. (2019) Generic and Practical Key Establishment from Lattice. *International Conference on Applied Cryptography and Network Security*, Colombia, 5-7 June 2019, 302-322. https://doi.org/10.1007/978-3-030-21568-2_15

[15] Regev, O. (2009) On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *Journal of the ACM*, **56**, Article No. 34. https://doi.org/10.1145/1568318.1568324

[16] Lyubashevsky, V., Peikert, C. and Regev, O. (2013) On Ideal Lattices and Learning with Errors over Rings. *Journal of the ACM*, **60**, Article No. 43. https://doi.org/10.1145/2535925

[17] Bos, J.W., Lauter, K., Loftus, J. and Naehrig, M. (2013) Improved Security for a Ring-Based Fully Homomorphic Encryption Scheme. *IMA International Conference on Cryptography and Coding*, Vol. 8308, 45-64. https://doi.org/10.1007/978-3-642-45239-0_4

[18] Brakerski, Z., Gentry, C. and Vaikuntanathan, V. (2012) (Leveled) Fully Homomorphic Encryption without Bootstrapping. *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, Cambridge, MA, January 2012, 309-325. https://doi.org/10.1145/2090236.2090262

[19] Castryck, W., Iliashenko, I. and Vercauteren, F. (2016) On Error Distributions in Ring-Based LWE. *LMS Journal of Computation and Mathematics*, **19**, 130-145. https://doi.org/10.1112/S1461157016000280

[20] Feng, C. and Zhao, Y. (2017) Ideal Lattice Based Justifiable Secure Digital Signature Scheme. *Computer Engineering*,

43, 103-107.

[21] Lyubashevsky, V. (2009) Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures. *International Conference on the Theory and Application of Cryptology and Information Security* Springer, Vol. 5912, 598-616. https://doi.org/10.1007/978-3-642-10366-7_35