一种新型基于环上带误差学习问题的认证密钥交换方案

杨孝鹏* 马文平 张成丽
(西安电子科技大学综合业务网及关键技术国家重点实验室 西安 710071)

摘 要：利用格上判定带误差学习问题(Ring-DLWE)困难假设，该文基于Peikert的调和技术构造认证密钥交换方案。在标准模型下，该方案是CK模型中可证明安全的，并达到弱前向安全性(wPFS)。与现有的基于LWE的密钥交换方案相比，该方案使用平衡的密钥提取函数，因而保护共享会话密钥，同时因其基于格中困难问题，所以能抵抗量子攻击。

关键词：密码学；格；认证密钥交换；CK模型；环上判定带误差学习问题(Ring-DLWE)

中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2015)08-1984-05
DOI: 10.11999/JEIT141506

New Authenticated Key Exchange Scheme Based on Ring Learning with Errors Problem

Yang Xiao-peng Ma Wen-ping Zhang Cheng-li
(*State Key Laboratory of Integrated Service Networks*, *Xidian University, Xi'an* 710071, *China*)

Abstract: Using the hard assumption of Ring-Decision Learning With Errors (Ring-DLWE) in the lattice, a new Authenticated Key Exchange (AKE) scheme is proposed, which is based on the Peikert's reconciliation technique. Under the standard model, the proposed scheme is provably secure in the CK model, which is additionally achieves weak Perfect Forward Secrecy (wPFS). Compared with the current Key Exchange (KE) schemes based on the LWE, the proposed scheme not only protects the shared session key with balanced key derivation function but also resists quantum attacks because of the hard assumption on lattice problem.

Key words: Cryptography; Lattice; Authenticated Key Exchange (AKE); CK model; Ring-Decision Learning With Errors (Ring-DLWE)

1 引言

认证密钥交换是密码学中的基本原型。它不仅允许通信双方协商出共享密钥而且为双方提供认证。每个通信方拥有一对静态公私钥，其中静态公钥由可信第三方颁发。在协议执行过程中，每个通信方首先生成自己的短暂公私钥，再计算会话状态，最后利用密钥提取函数计算共享密钥。

近年来，基于格的密码体制因其具有较高的渐进效率、可并行计算、抗量子攻击等优点，迅速成为密码学研究新热点，并取得了一系列成果[1–12]。其中，基于带误差学习(Learning With Errors, LWE)问题的困难性在建立秘密共享方案方面应用广泛[6–12]。文献[6]基于LWE提出了认证密钥交换协议，并证明协议是强安全的。文献[7]指出文献[6]的协议难以抵抗不知道任何秘密信息的外部攻击者实施的假冒攻击。文献[8]提出基于LWE的秘密共享方案。该方案借助符号函数来降噪，但符号函数泄露了密钥的一些信息。文献[9]提出基于LWE的认证密钥交换方案，并构造了特征函数和符号函数。为了使符号函数输出分布与均匀分布不可区分，要求模数很大。针对现有文献的不足，该文基于环上带误差学习问题(RLWE)问题[10]提出新的认证密钥交换方案，使用较小的模数，并利用平衡密钥提取器，所以不会泄露共享密钥的信息，而且所有计算可以采用分圆域上快速傅里叶变换(FFT)[10]加速。

2 预备知识

2.1 符号说明

用$\mathbb{C}$，$\mathbb{R}$，$\mathbb{Z}$和$\mathbb{Q}$分别表示复数集、实数集、整数集和有理数集。对于$x\in\mathbb{R}$，定义$[x]_2=\lfloor x+1/2\rfloor\in\mathbb{Z}$。对于$q\geq 1$，定义$\mathbb{Z}_q=\mathbb{Z}/q\mathbb{Z}$。一个$n$维格表示为$\Lambda=L(\boldsymbol{B})=\{\boldsymbol{Bc}:\boldsymbol{c}\in\mathbb{Z}^k\}$, $\boldsymbol{B}\in\mathbb{R}^{n\times k}$

2014-11-27收到，2015-02-19改回，2015-06-08网络优先出版
国家自然科学基金(61072140, 61373171)，高等学校博士学科点专项科研基金(20100203110003)，高等学校创新引智计划项目(B08038)，“十二五”国家密码发展基金(MMJJ201401003)和华为技术有限公司合作项目(YB2013120005)资助课题
*通信作者：杨孝鹏 xp_yang89xidian@126.com

是格的基。高斯函数为 $\rho_r(\boldsymbol{x})=\exp\left(\frac{-\pi\|\boldsymbol{x}\|^2}{r^2}\right)$，其中 $\boldsymbol{x}\in H=\{\boldsymbol{x}: x_i=x_{m-i},\ \forall i\in\mathbb{Z}_m^*\}$。格的陪集 $\Lambda+\boldsymbol{c}$ 上的离散高斯概率分布为 $D_{\Lambda+\boldsymbol{c},r}(\boldsymbol{x})=\frac{\rho_r(\boldsymbol{x})}{\rho_r(\Lambda+\boldsymbol{c})}$，$\forall\boldsymbol{x}\in\Lambda+\boldsymbol{c}$。对于正整数 m，ζ_m 是本原 m 阶单位根。$\mathrm{K}=\mathbb{Q}(\zeta_m)$ 表示 m 次分圆域，$\mathrm{R}=\mathbb{Z}[\zeta_m]$ 表示 m 次分圆环。$\{\zeta_m^j:\gcd(j,m)=1\}_{j=0}^{m-1}$ 是 R 的幂基 $\boldsymbol{P}$。设 τ 是 K 的自同构，$\mathrm{R}^\vee$ 的解码基为 $\boldsymbol{d}=\tau(\boldsymbol{P})^\vee$。设 p 为奇素数，记 $g=\prod_{p|m}(1-\zeta_p)$。设 $\mathcal{R}$ 为可换环，$\mathcal{R}$ 上离散傅里叶变换 DFT_m 为矩阵 $(\omega_m^{ij})_{(i\times j)\in(\mathbb{Z}_m\times\mathbb{Z}_m)}$，中国剩余变换 CRT_m 为 DFT_m 的亚矩阵，阶为 $\mathbb{Z}_m^*\times[\varphi(m)]$。

2.2 格上亚高斯变量

定义 1[10] 对于 $\delta>0$，$\forall t\in\mathbb{R}$，若满足 $\mathrm{E}[\exp(2\pi tX)]\le\exp(\delta+\pi r^2t^2)$，则称 $\mathbb{R}$ 上随机变量 X 是标准偏差为 r 的 δ-亚高斯变量。由马尔科夫不等式得：$\forall t\ge0$，有

$$\Pr[|X|\ge t]\le 2\exp\left(\delta-\pi t^2/r^2\right)\tag{1}$$

事实 1[10] 若 X_1 是 δ_1-亚高斯变量，标准偏差为 r_1，X_2 是 δ_2-亚高斯变量，标准偏差为 r_2。X_1 与 X_2 相互独立，则 X_1+X_2 是 $(\delta_1+\delta_2)$-亚高斯变量，标准偏差为 $\sqrt{r_1^2+r_2^2}$。

引理 1[10] 设 $g\cdot e$ 是 δ-亚高斯变量，标准偏差为 $\widehat{m}\cdot r$。$\forall e'\in Q(\zeta_m)$，则对于 $e\cdot e'\in\mathbb{Q}(\zeta_m)$，用 $\mathrm{R}^\vee$ 的每个解码基表示时，系数均是 δ-亚高斯变量，标准偏差为 $r\cdot\|e\|_2$。

引理 2[10] 设 $e\leftarrow\chi$，其中 $\chi=[\varphi_r]$，$\varphi_r=(\widehat{m}/g)\cdot D_r$。则 $g\cdot e$ 是 δ-亚高斯变量，标准偏差为 $\widehat{m}\cdot\sqrt{r^2+2\pi\cdot\mathrm{rad}(m)/m}$，且 $\|g\cdot e\|_2\le\widehat{m}\cdot(r+\sqrt{\mathrm{rad}(m)/m})\cdot\sqrt{n}$ 以至少 $1-2^{-n}$ 的概率成立。

2.3 代数整数环上格的抽样

设 $a\in\mathrm{K}\otimes\mathbb{R}$，用 R 的解码基表示为 $a=(\widehat{m}/g)\cdot\langle\boldsymbol{d},\boldsymbol{a}\rangle$。代数整数环上格的高斯抽样简述如下：(1)利用典范嵌入计算 $\sigma\left(\left\{\zeta_m^t\right\}_{t=0}^{\varphi(m)}\right)=\mathrm{CRT}_m$；(2)从空间 H 上的连续高斯分布中抽样 $\sigma(a)$，左乘 CRT_m，计算 $\boldsymbol{a}=\mathrm{CRT}_m\cdot\sigma(a)$；(3)计算 $a=(\widehat{m}/g)\cdot\langle\boldsymbol{d},\boldsymbol{a}\rangle$；(4)对 a 的解码基的每个系数凑整为最近整数，输出 $[a]$。

2.4 困难问题

定义 2[4,10] 对于 $\boldsymbol{s}\in\mathrm{R}_q^\vee$，$\mathrm{K}\otimes\mathbb{R}$ 上的分布 χ，随机均匀选取 $\boldsymbol{a}\in\mathrm{R}_q$，$\boldsymbol{e}$ 是服从 χ 的噪声。计算 $\boldsymbol{b}=\boldsymbol{a}\cdot\boldsymbol{s}+\boldsymbol{e}\bmod q\mathrm{R}^\vee$。记 $(\boldsymbol{a},\boldsymbol{b}=\boldsymbol{a}\cdot\boldsymbol{s}+\boldsymbol{e}\bmod q\mathrm{R}^\vee)$ 的分布为 $A_{\boldsymbol{s},\chi}$。以不可忽略的概率区分 $A_{\boldsymbol{s},\chi}$ 与 $\mathrm{R}_q^\vee\times(\mathrm{K}\otimes\mathbb{R}/q\mathrm{R}^\vee)$ 上的均匀分布问题就是判定 Ring-LWE 问题，记作 $\mathrm{RDLWE}_{q,\chi}$。

引理 3[4] 设 $\alpha=\omega(\sqrt{\log_2 n})$，向量 $\boldsymbol{x}\in\mathbb{Z}^n$，分布 χ_α 与分布 $\chi_\alpha+\boldsymbol{x}$ 统计距离至多为 $\|\boldsymbol{x}\|/\alpha$。

2.5 安全模型

安全模型定义请参见文献[13]。

2.6 调和技术

调和函数定义请参见文献[11]。

引理 4[11] 对于偶数模 q，若 $x\in\mathbb{Z}_q$ 是随机均匀的，则 $[x]_2$ 是随机均匀的。

引理 5[11] 对于偶数模 q，若 $w=x+e\bmod q$，$v\in\mathbb{Z}_q$，$e\in E$，则 $\mathrm{rec}(w,\langle x\rangle_2)=[x]_2=\mathrm{rec}(x,\langle x\rangle_2)$。

引理 6[11] 对于奇数模 q，若 $x\in\mathbb{Z}_q$ 是随机均匀的，$\overline{x}\leftarrow\mathrm{dbl}(x)\in\mathbb{Z}_{2q}$，给定 $\langle\overline{x}\rangle_2$ 条件下，$[x]_2$ 的分布是一致分布。

3　方案

3.1 方案描述

设 $\mathrm{R}_q=\mathbb{Z}_q[X]/(\Phi_m(X))$，$q$ 为奇素数且满足 $q\equiv1\bmod m$，$\alpha q\ge\omega(\sqrt{\log_2 n})$。A 抽样 $\boldsymbol{s}_\mathrm{A},\boldsymbol{e}_\mathrm{A}\in\chi$，将 $\boldsymbol{s}_\mathrm{A}$ 作为静态私钥，计算静态公钥 $\boldsymbol{P}_\mathrm{A}=\boldsymbol{a}\cdot\boldsymbol{s}_\mathrm{A}+\boldsymbol{e}_\mathrm{A}\in\mathrm{R}_q$。B 抽样 $\boldsymbol{s}_\mathrm{B},\boldsymbol{e}_\mathrm{B}\in\chi$，将 $\boldsymbol{s}_\mathrm{B}$ 作为静态私钥，计算静态公钥 $\boldsymbol{P}_\mathrm{B}=\boldsymbol{a}\cdot\boldsymbol{s}_\mathrm{B}+\boldsymbol{e}_\mathrm{B}\in\mathrm{R}_q$。方案如图1所示。

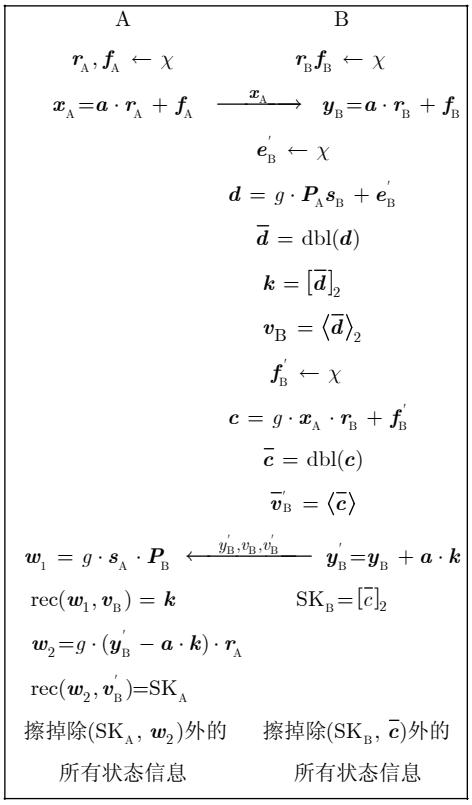

图 1　基于 Ring-LWE 的认证密钥交换方案

3.2 正确性

引理 7 假设$\|g\cdot\boldsymbol{s}_i\|_2\le\ell$，$\|g\cdot\boldsymbol{r}_i\|_2\le\ell$。令$\boldsymbol{e}_1=g\cdot(\boldsymbol{s}_{\mathrm{A}}\cdot\boldsymbol{e}_{\mathrm{B}}-\boldsymbol{s}_{\mathrm{B}}\cdot\boldsymbol{e}_{\mathrm{A}})-\boldsymbol{e}_{\mathrm{B}}^{'}\in\mathrm{R}$，$\bar{\boldsymbol{e}}_1\in\mathrm{R}$为在$\bar{\boldsymbol{d}}\leftarrow\mathrm{dbl}(\boldsymbol{d})$中选取的随机元。对于$\mu>0$，若A能恢复$\boldsymbol{k}$的真实值，则要求

$$\left(\frac{q}{8}\right)^2\ge\left[r'\cdot\left(2\ell^2+n\right)+\frac{\pi}{2}\right]\cdot\mu^2 \tag{2}$$

进一步，在A恢复$\boldsymbol{k}$的真实值条件下，$\mathrm{SK}_{\mathrm{A}}=\mathrm{SK}_{\mathrm{B}}$以至少$n(1-2\cdot\exp(3\delta-\pi\mu^2))$的概率成立。

证明 因为$\boldsymbol{w}_1=\boldsymbol{d}+g\cdot(\boldsymbol{s}_{\mathrm{A}}\cdot\boldsymbol{e}_{\mathrm{B}}+\boldsymbol{s}_{\mathrm{B}}\cdot\boldsymbol{e}_{\mathrm{A}})-\boldsymbol{e}_{\mathrm{B}}^{'}\in\mathrm{R}_q$。由引理2可知$g\cdot\boldsymbol{e}_{\mathrm{A}}$和$g\cdot\boldsymbol{e}_{\mathrm{B}}$都是$\delta$-亚高斯变量，标准偏差为$\widehat{m}\cdot r'$，其中$r'=(r^2+2\pi\cdot\mathrm{rad}(m)/m)^{1/2}$。因为$\|g\cdot\boldsymbol{s}_i\|_2\le\ell$，$\|g\cdot\boldsymbol{r}_i\|_2\le\ell$，由引理1可知$g\cdot\boldsymbol{e}_{\mathrm{A}}\cdot\boldsymbol{s}_{\mathrm{B}}$和$g\cdot\boldsymbol{e}_{\mathrm{B}}\cdot\boldsymbol{s}_{\mathrm{A}}$的解码基的每个系数都是$\delta$-亚高斯变量，标准偏差为$r'\cdot\ell$。由引理1可知$\boldsymbol{e}_{\mathrm{B}}'$的解码基的每个系数都是$\delta$-亚高斯变量，标准偏差为$r'\cdot\sqrt{n}$。另外，$\bar{\boldsymbol{e}}_1$的解码基的每个系数都是0-亚高斯变量，标准偏差为$\sqrt{2\pi}$。

由事实1可知$2\boldsymbol{e}_1+\bar{\boldsymbol{e}}_1$的解码基的每个系数都是$3\delta$-亚高斯变量，标准偏差为$2[r'^2(2\lambda^2+n)+\pi/2]^{1/2}$。此时，$2\boldsymbol{e}_1+\bar{\boldsymbol{e}}_1$的解码基的每个系数落在区间$[-q/4,q/4)$上。由引理5可知A能恢复$\boldsymbol{k}$的真实值。由式(1)得出式(2)。$2\boldsymbol{e}_1+\bar{\boldsymbol{e}}_1$的解码基的每个系数以至少$1-2\cdot\exp(3\delta-\pi\mu^2)$的概率落在区间$[-q/4,q/4)$上。由引理5得A以至少$n(1-2\cdot\exp(3\delta-\pi\mu^2))$的概率恢复出$\boldsymbol{k}$的真实值。同理可证在A恢复$\boldsymbol{k}$的真实值条件下，$\mathrm{SK}_{\mathrm{A}}=\mathrm{SK}_{\mathrm{B}}$以至少$n(1-2\cdot\exp(3\delta-\pi\mu^2))$的概率成立。 证毕

3.3 参数选取

由引理7可知只需取$q=\widetilde{O}(n^2)$。为保证$\alpha\cdot q\ge\omega(\sqrt{\log_2 n})$，设$r=(2n/\log_2(2n))^{1/4}\cdot\omega(\sqrt{\log_2 n})$。

3.4 效率比较

方案效率由计算复杂度和通信复杂度组成。计算复杂度主要考虑向量乘法和抽样。通信复杂度考虑发送比特总数。表1对现有的基于Ring-LWE的密钥交换方案做比较(密钥为n bit)。

4 安全分析

定理 1 设n是安全参数，$\alpha<(\log_2 n/n)^{1/2}$，$q=1\bmod m$是一个多项式有界的素数且$\alpha q\ge\omega(\sqrt{\log_2 n})$。若$\mathrm{RDLWE}_{q,\chi}$是困难问题，则上述方案在标准模型下是带wFS的SK安全的。

证明 在下述证明中，设sid^*表示测试会话标示符，$\mathcal{A}$表示敌手，Suc表示敌手赢得游戏。根据测试会话是否有匹配会话，分为以下两种情形进行分析：

情形 1 sid^*有匹配会话，并且$\mathcal{A}$可以得到sid^*的静态私钥。这部分证明要利用混合游戏$G_{1,x}$。记$\mathrm{Adv}(\mathcal{A},G_{1,x})$表示$\mathcal{A}$赢得游戏$G_{1,x}$的优势，其中$x=0,1,2,3,4$。

$G_{1,0}$ 这个游戏是敌手和协议之间的真实交互。$\mathcal{A}$按照模型规定的能力向模拟器$\mathcal{S}$发出询问，并得到相应的回答。特别地，当$\mathcal{A}$向一个未完成的会话发出Test询问时，$\mathcal{S}$选取$b\in_{\mathcal{R}}\{0,1\}$。若$b=0$，则$\mathcal{S}$返回一个随机密钥给$\mathcal{A}$。否则，$\mathcal{S}$返回sid的真实密钥给$\mathcal{A}$。

$G_{1,1}$ 这个游戏和$G_{1,0}$基本相同，下述情况除外：$\mathcal{S}$抽取$\boldsymbol{r}_{\mathrm{B}}^{'},\boldsymbol{f}_{\mathrm{B}}^{'}\in\chi$，计算$\boldsymbol{y}_{\mathrm{B}}^{''}=\boldsymbol{a}\cdot\boldsymbol{r}_{\mathrm{B}}^{'}+\boldsymbol{f}_{\mathrm{B}}^{'}$，选取$\boldsymbol{k}\in_{\mathcal{R}}\{0,1\}^n$，计算$\boldsymbol{y}_{\mathrm{B}}^{'}=\boldsymbol{y}_{\mathrm{B}}^{''}+\boldsymbol{a}\cdot\boldsymbol{k}$，选取$\boldsymbol{r}_{\mathrm{B}}^{'}\in_{\mathcal{R}}\mathrm{R}_q$，计算$\boldsymbol{v}_{\mathrm{B}}=\left\langle\mathrm{dbl}(\boldsymbol{r}_{\mathrm{B}}^{'})\right\rangle_2$，$\boldsymbol{c}=g\cdot\boldsymbol{x}_{\mathrm{A}}\cdot\boldsymbol{r}_{\mathrm{B}}+\boldsymbol{f}_{\mathrm{B}}^{'}$，依据协议规范地计算$\bar{\boldsymbol{c}},\boldsymbol{v}_{\mathrm{B}}^{'},\mathrm{SK}_{\mathrm{B}}$，并发送$(\boldsymbol{y}_{\mathrm{B}}^{'},\boldsymbol{v}_{\mathrm{B}},\boldsymbol{v}_{\mathrm{B}}^{'})$给$\mathcal{A}$。

因为$\boldsymbol{y}_{\mathrm{B}}^{''}$的分布与一致分布计算不可区分，所以$\mathcal{A}$猜测出$\boldsymbol{y}_{\mathrm{B}}^{'}=\boldsymbol{y}_{\mathrm{B}}^{''}+\boldsymbol{a}\cdot\boldsymbol{k}$的概率可忽略。因为$\boldsymbol{y}_{\mathrm{B}}^{'}=\boldsymbol{a}\cdot(\boldsymbol{r}_{\mathrm{B}}^{'}+\boldsymbol{k})+\boldsymbol{f}_{\mathrm{B}}^{'}$，由引理3可知$\boldsymbol{r}_{\mathrm{B}}^{'}+\boldsymbol{k}$的分布统计接近$\chi$，则$G_{1,1}$中的$\boldsymbol{y}_{\mathrm{B}}^{'}$的分布统计接近$G_{1,0}$中的$\boldsymbol{y}_{\mathrm{B}}^{'}$的分布。构造一个规约$\mathcal{R}_1$，它的两对输入为$(\boldsymbol{a},\boldsymbol{y}_{\mathrm{B}}^{'})$和$(\boldsymbol{b}',\boldsymbol{r}_{\mathrm{B}}^{'})\in_{\mathcal{R}}\mathrm{R}_q\times\mathrm{R}_q$。设$\bar{\boldsymbol{v}}=\mathrm{dbl}(\boldsymbol{c})$，输出$(\boldsymbol{a},\boldsymbol{P}_{\mathrm{B}}=\boldsymbol{s}_{\mathrm{A}}^{-1}\cdot\boldsymbol{b}',\boldsymbol{y}_{\mathrm{B}}^{'},\boldsymbol{v}_{\mathrm{B}},\boldsymbol{k})$。若$\mathcal{R}_1$的输入取自$A_{\boldsymbol{e}_0,\chi}$，则$\mathcal{R}_1$的输出和$G_{1,0}$的输出相同。否则，$\mathcal{R}_1$的输出和$G_{1,1}$输出相同。由引理6可知这两对输入计算不可区分。若$\mathrm{RDLWE}_{q,\chi}$是困难问题，则

$$\left|\mathrm{Adv}\left(\mathcal{A},G_{1,1}\right)-\mathrm{Adv}\left(\mathcal{A},G_{1,0}\right)\right|\le\mathrm{negl}(n) \tag{3}$$

表 1 基于 Ring-LWE 的密钥交换方案的性能比较(密钥为 n bit)

方案	认证	q的尺寸	困难假设	安全模型	计算复杂度	ROM	发送比特总数
文献[8]	×	n^4	$\text{Ideal-SIVP}_{\widetilde{O}(n^{9/2})}$	×	$O(2^{2n-2})$	×	$n+2n\log_2 q$
文献[9]	√	$2^{\omega(\log_2 n)}$	$\text{Ideal-SIVP}_{\widetilde{O}(n^{9/2})}$	BR	$O(2^{2n-2})$	√	$n+2n\log_2 q$
本文	√	$\widetilde{O}(n^2)$	$\text{Ideal-SIVP}_{\widetilde{O}(n^{5/2})}$	CK	$O(2^{n+1})$	×	$2n+2n\log_2 q$

$G_{1,2}$ 这个游戏和 $G_{1,1}$ 基本相同，下述情况除外：$\mathcal{S}$ 选取 $\boldsymbol{P}_{\mathrm{B}}^{'} \in_{\mathcal{R}} \mathrm{R}_q$，计算 $\boldsymbol{w}_1 = g \cdot \boldsymbol{s}_{\mathrm{A}} \cdot \boldsymbol{P}_{\mathrm{B}}^{'}$，选取 $\boldsymbol{k} \in_{\mathcal{R}} \mathrm{R}_q$，设置 $\mathrm{rec}(\boldsymbol{w}_1, \boldsymbol{v}_{\mathrm{B}}) = \boldsymbol{k}$，依据协议规范地计算 $\boldsymbol{w}_2$ 和 SK_{A}。

因为 $\boldsymbol{P}_{\mathrm{B}}$ 的分布与一致分布计算不可区分，则由引理 6 可知给定 $\boldsymbol{v}_{\mathrm{B}}$ 条件下，$\boldsymbol{k}$ 是一致分布的。且

$$\left|\mathrm{Adv}\left(\mathcal{A}, G_{1,2}\right) - \mathrm{Adv}\left(\mathcal{A}, G_{1,1}\right)\right| \le \mathrm{negl}(n) \tag{4}$$

$G_{1,3}$ 这个游戏和 $G_{1,2}$ 基本相同，下述情况除外：$\mathcal{S}$ 选取 $\boldsymbol{y}_{\mathrm{B}}^{''} \in_{\mathcal{R}} \mathrm{R}_q$，$\boldsymbol{k} \in_{\mathcal{R}} \{0,1\}^n$，计算 $\boldsymbol{y}_{\mathrm{B}}^{'} = \boldsymbol{y}_{\mathrm{B}}^{''} + \boldsymbol{a} \cdot \boldsymbol{k}$，选取 $\boldsymbol{c} \in_{\mathcal{R}} \mathrm{R}_q$，计算 $\bar{\boldsymbol{c}}, \boldsymbol{v}_{\mathrm{B}}, \boldsymbol{v}_{\mathrm{B}}^{'}$，选取 $\mathrm{SK}_{\mathrm{B}} \in_{\mathcal{R}} \{0,1\}^n$，并设置 $[\bar{\boldsymbol{c}}]_2 = \mathrm{SK}_{\mathrm{B}}$，发送 $(\boldsymbol{y}_{\mathrm{B}}^{'}, \boldsymbol{v}_{\mathrm{B}}, \boldsymbol{v}_{\mathrm{B}}^{'})$ 给 $\mathcal{A}$。

$G_{1,2}$ 中 SK_{B} 替换为 $G_{1,3}$ 中的随机值。设 $(\boldsymbol{u}_1, \boldsymbol{v}_1)$ 和 $(\boldsymbol{u}_2, \boldsymbol{v}_2)$ 是两个 Ring-LWE 挑战组。构造求解 Ring-LWE 问题的区分器 $\mathcal{D}$，$\mathcal{D}$ 设置 $\boldsymbol{s}_{\mathrm{A}} = \boldsymbol{u}_1$，$\boldsymbol{x}_{\mathrm{A}} = \boldsymbol{u}_2$，$\boldsymbol{y}_{\mathrm{B}}^{'} = \boldsymbol{v}_1$，选取 $\boldsymbol{k} \in_{\mathcal{R}} \{0,1\}^n$，计算 $\boldsymbol{y}_{\mathrm{B}}^{'} = \boldsymbol{y}_{\mathrm{B}}^{''} + \boldsymbol{a} \cdot \boldsymbol{k}$，设置 $\boldsymbol{c} = \boldsymbol{v}_2$，依据协议规范计算 $\bar{\boldsymbol{c}}, \mathrm{SK}_{\mathrm{B}}, \boldsymbol{v}_{\mathrm{B}}^{'}$。另外，$\mathcal{D}$ 选取 $\mathrm{SK}_{\mathrm{B}} \in_{\mathcal{R}} \{0,1\}^n$，设置 $[\bar{\boldsymbol{c}}]_2 = \mathrm{SK}_{\mathrm{B}}$，发送 $(\boldsymbol{y}_{\mathrm{B}}^{'}, \boldsymbol{v}_{\mathrm{B}}, \boldsymbol{v}_{\mathrm{B}}^{'})$ 给 $\mathcal{A}$。若 $\mathrm{RDLWE}_{q,\chi}$ 是困难问题，则

$$\left|\mathrm{Adv}\left(\mathcal{A}, G_{1,3}\right) - \mathrm{Adv}\left(\mathcal{A}, G_{1,2}\right)\right| \le \mathrm{negl}(n) \tag{5}$$

$G_{1,4}$ 这个游戏和 $G_{1,3}$ 基本相同，下述情况除外：$\mathcal{S}$ 选取 $\boldsymbol{x}_{\mathrm{A}}^{'} \in_{\mathcal{R}} \mathrm{R}_q$，设置 $\mathrm{SK}_{\mathrm{A}} \in_{\mathcal{R}} \{0,1\}^n$ 作为共享密钥。在 $G_{1,4}$ 中，SK_{A} 是均匀随机的。给定 $\boldsymbol{w}_2$ 条件下，$\mathrm{rec}(\boldsymbol{w}_2, \boldsymbol{v}_{\mathrm{B}}^{'})$ 的输出分布统计接近均匀分布。$G_{1,3}$ 与 $G_{1,4}$ 计算不可区分，且有

$$\left|\mathrm{Adv}\left(\mathcal{A}, G_{1,4}\right) - \mathrm{Adv}\left(\mathcal{A}, G_{1,3}\right)\right| \le \mathrm{negl}(n) \tag{6}$$

在 $G_{1,4}$ 中，会话状态完全随机化，则敌手不能通过 Test 问询获得任何优势。结合式(3)～式(6)可知 $\mathcal{A}$ 的优势是可忽略的量。

情形 2　sid^* 没有匹配会话，且 $\mathcal{A}$ 可以得到 sid^* 的静态私钥。这部分证明要利用混合游戏 $G_{2,x}$。

$G_{2,0}$ 这个游戏与情形 1 中游戏 $G_{1,0}$ 相同。

$G_{2,1}$ 这个游戏和 $G_{2,0}$ 基本相同，下述情况除外：$\mathcal{S}$ 抽取 $\boldsymbol{r}_{\mathrm{A}}^{'}, \boldsymbol{f}_{\mathrm{A}}^{'} \in \chi$，计算 $\boldsymbol{x}_{\mathrm{A}}^{'} = \boldsymbol{a} \cdot \boldsymbol{r}_{\mathrm{A}}^{'} + \boldsymbol{f}_{\mathrm{A}}^{'}$，抽取 $\boldsymbol{r}_{\mathrm{B}}^{'}, \boldsymbol{f}_{\mathrm{B}}^{'} \in \chi$，计算 $\boldsymbol{y}_{\mathrm{B}}^{''} = \boldsymbol{a} \cdot \boldsymbol{r}_{\mathrm{B}}^{'} + \boldsymbol{f}_{\mathrm{B}}^{'}$，选取 $\boldsymbol{k} \in_{\mathcal{R}} \{0,1\}^n$，计算 $\boldsymbol{y}_{\mathrm{B}}^{'} = \boldsymbol{y}_{\mathrm{B}}^{''} + \boldsymbol{a} \cdot \boldsymbol{k}$，选取 $\boldsymbol{r}_{\mathrm{B}}^{'} \in_{\mathcal{R}} \mathrm{R}_q$，计算 $\boldsymbol{v}_{\mathrm{B}} = \left\langle \mathrm{dbl}(\boldsymbol{r}_{\mathrm{B}}^{'}) \right\rangle_2$，并发送 $(\boldsymbol{y}_{\mathrm{B}}^{'}, \boldsymbol{v}_{\mathrm{B}}, \boldsymbol{v}_{\mathrm{B}}^{'})$ 给 $\mathcal{A}$。类似分析 $G_{1,1}$ 与 $G_{1,0}$ 的不可区分性，可以得到

$$\left|\mathrm{Adv}\left(\mathcal{A}, G_{2,1}\right) - \mathrm{Adv}\left(\mathcal{A}, G_{2,0}\right)\right| \le \mathrm{negl}(n) \tag{7}$$

$G_{2,2}$ 这个游戏和 $G_{2,1}$ 基本相同，下述情况除外：$\mathcal{S}$ 用 $\boldsymbol{P}_{\mathrm{B}^*} \in_{\mathcal{R}} \mathrm{R}_q$ 替换 $G_{2,1}$ 中的 $\boldsymbol{P}_{\mathrm{B}}^*$。类似分析 $G_{1,2}$ 与 $G_{1,1}$ 的不可区分性，可以得到

$$\left|\mathrm{Adv}\left(\mathcal{A}, G_{2,2}\right) - \mathrm{Adv}\left(\mathcal{A}, G_{2,1}\right)\right| \le \mathrm{negl}(n) \tag{8}$$

$G_{2,3}$ 这个游戏和 $G_{2,2}$ 基本相同，下述情况除外：$\mathcal{S}$ 抽取 $\boldsymbol{r}_{\mathrm{A}}^{'}, \boldsymbol{f}_{\mathrm{A}}^{'} \in \chi$，计算 $\boldsymbol{x}_{\mathrm{A}}^{'} = \boldsymbol{a} \cdot \boldsymbol{r}_{\mathrm{A}}^{'} + \boldsymbol{f}_{\mathrm{A}}^{'}$，选取 $\boldsymbol{P}_{\mathrm{B}}^{'} \in_{\mathcal{R}} \mathrm{R}_q$，计算 $\boldsymbol{w}_1 = g \cdot \boldsymbol{s}_{\mathrm{A}} \cdot \boldsymbol{P}_{\mathrm{B}}^{'}$，依据协议规范地计算 SK_{A}。类似分析 $G_{1,3}$ 与 $G_{1,2}$ 的不可区分性，可以得到

$$\left|\mathrm{Adv}\left(\mathcal{A}, G_{2,3}\right) - \mathrm{Adv}\left(\mathcal{A}, G_{2,2}\right)\right| \le \mathrm{negl}(n) \tag{9}$$

$G_{2,4}$ 这个游戏和 $G_{2,3}$ 基本相同，下述情况除外：$\mathcal{S}$ 抽取 $\boldsymbol{r}_{\mathrm{A}}^{'}, \tilde{\boldsymbol{f}}_{\mathrm{A}}^{'} \in \chi$，计算 $\boldsymbol{z}_1 = \boldsymbol{a} \cdot \boldsymbol{r}_{\mathrm{A}}^{'} + \tilde{\boldsymbol{f}}_{\mathrm{A}}^{'}$，计算 $\boldsymbol{x}_{\mathrm{A}}^{'} = \boldsymbol{z}_1 + \boldsymbol{f}_{\mathrm{A}}^{'} = \boldsymbol{a} \cdot \boldsymbol{r}_{\mathrm{A}}^{'} + (\boldsymbol{f}_{\mathrm{A}}^{'} + \tilde{\boldsymbol{f}}_{\mathrm{A}}^{'})$，计算 $\boldsymbol{c} = g \cdot \boldsymbol{x}_{\mathrm{A}}^{'} \cdot \boldsymbol{r}_{\mathrm{B}} + \boldsymbol{f}_{\mathrm{B}}^{'}$，依据协议规范地计算 $\bar{\boldsymbol{c}}, \mathrm{SK}_{\mathrm{B}}, \boldsymbol{v}_{\mathrm{B}}^{'}, \boldsymbol{y}_{\mathrm{B}}^{'}$。由引理 3 可知 $\mathcal{A}$ 不能区分 $G_{2,4}$ 与 $G_{2,3}$。则有

$$\left|\mathrm{Adv}\left(\mathcal{A}, G_{2,4}\right) - \mathrm{Adv}\left(\mathcal{A}, G_{2,3}\right)\right| \le \mathrm{negl}(n) \tag{10}$$

$G_{2,5}$ 这个游戏和 $G_{2,4}$ 基本相同，下述情况除外：$\mathcal{S}$ 选取 $\boldsymbol{v}_{\mathrm{B}}^{'} \in_{\mathcal{R}} \{0,1\}^n$，依据协议规范地计算 SK_{A}。因为在 $\boldsymbol{v}_{\mathrm{B}}^{'}$ 随机均匀条件下，SK_{A} 的分布是一致分布。由引理 5 可知 $\mathcal{A}$ 猜测成功的优势可忽略，则有

$$\left|\mathrm{Adv}\left(\mathcal{A}, G_{2,5}\right) - \mathrm{Adv}\left(\mathcal{A}, G_{2,4}\right)\right| \le \mathrm{negl}(n) \tag{11}$$

$G_{2,6}$ 这个游戏和 $G_{2,5}$ 基本相同，下述情况除外：$\mathcal{S}$ 选取 $\boldsymbol{z}_1 \in_{\mathcal{R}} \mathrm{R}_q$。在 $G_{2,6}$ 中会话密钥完全随机化，则敌手不能通过 Test 问询获得任何优势。结合式(7)～式(11)可知 $\mathcal{A}$ 的优势是可忽略的量。　　证毕

5　结束语

本文利用 Ring-DLWE 困难假设，基于调和技术构造出一种新型认证密钥交换方案。相对于现有的基于 LWE 的认证密钥交换方案来说，本文使用较小的模数，并利用平衡函数提取共享密钥。下一步工作可以考虑基于 LWE 构造强安全的认证密钥交换方案。

参 考 文 献

[1] Gentry C, Peikert C, and Vaikuntanathan V. Trapdoor for hard lattices and new cryptographic constructions[C]. Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, BC, Canada, 2008: 197–206.

[2] Regev O. On lattices, learning with errors, random linear codes, and cryptography[J]. *Journal of the ACM*, 2009, DOI:10.1145/1568318.1568324.

[3] Peikert C. Public-key cryptosystems for the worst-case shortest vector problem[C]. Proceedings of the 41th Annual ACM Symposium on Theory of Computing, Bethesda, MD, USA, 2009: 333–342.

[4] Lyubashevsky V, Peikert C, and Regev O. On ideal lattices and learning with errors over rings[C]. Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Riviera, France, 2010: 1–23.

[5] Benny A, David C, and Peikert C. Fast cryptographic primitives and circular-secure encryption based on hard learning problems[C]. Proceedings of the 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, 2009: 595–618.

[6] Fujioka A, Suzuki K, Xagawa K, *et al*.. Practical and post-quantum authenticated key exchange from one-way secure key encapsulation mechanism[C]. Proceedings of the 8th ACM Symposium on Information, Computer, and Communication Security, Hangzhou, China, 2013: 83–94.

[7] 胡学先, 魏江宏, 叶茂, 等. 对一个强安全的认证密钥交换协议的分析[J]. 电子与信息学报, 2013, 35(9): 2278–2282.
Hu Xue-xian, Wei Jiang-hong, Ye Mao, *et al*.. Cryptanalysis of a strongly secure authenticated key exchange protocol[J]. *Journal of Electronics & Information Technology*, 2013, 35(9): 2278–2282.

[8] Ding Jin-tai. A simple provably secure key exchange scheme based on the learning with errors problems[OL]. http://eprint.iacr.org/2012/688, 2014, 6.

[9] Zhang Jiang, Zhang Zhen-feng, Ding Jin-tai, *et al*.. Authenticated key exchange from ideal lattices[OL]. http://eprint.iacr.org/2014/589, 2014, 7.

[10] Lyubashevsky V, Peikert C, and Regev O. A toolkit for ring-LWE cryptography[C]. Proceedings of the 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, 2013: 35–54.

[11] Peikert C. Lattice cryptography for the Internet[C]. Proceedings of the 6th International Workshop, Post-Quantum Cryptography, Waterloo, Canada, 2014: 197–219.

[12] Peikert C. An efficient and parallel gaussian sampler for lattices[C]. Proceedings of the 30th Annual International Cryptology Conference, Santa Barbara, CA, USA, 2010: 80–97.

[13] Canetti R and Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels[C]. Proceedings of the 20th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Innsbruck, Austria, 2001: 453–474.

杨孝鹏： 男，1986 年生，博士生，研究方向为格密码.

马文平： 男，1965 年生，博士，教授，博士生导师，研究方向为通信理论、纠错码和信息安全等.

张成丽： 女，1985 年生，博士生，研究方向为格密码.