基于格密码理论的装备保障信息网络身份认证方案

张建航[1,2]，曹泽阳[1]，徐庆征[2]，贺　健[2]
(1.空军工程大学防空反导学院，西安，710051;2.国防科技大学信息通信学院，西安，710106)

摘要　针对当前装备保障信息网络身份认证方案无法抵抗正在崛起的量子计算机攻击及认证效率较低的问题,基于新的格密码理论,提出了装备保障信息网络在量子计算环境下安全且快速的身份认证方案。该方案采用理想格结构生成方案的主密钥,将装备身份信息输入到原像抽样函数中得出装备身份信息对应的认证密钥,利用无陷门的采样技术产生出装备的认证信息。结果表明:该方案在理想小整数解问题困难性假设的条件下,达到了适应性选择身份和选择消息攻击下的不可伪造性安全;在保证安全的前提下,该方案在达到相同的安全等级水平时在认证速率和验证速率方面均高于传统基于 RSA 和 ECC 的认证方案。

关键词　装备保障信息网络;量子计算机;格密码理论;身份认证
DOI　10.3969/j.issn.1009-3516.2019.01.013
中图分类号　TN918;E96　　**文献标志码**　A　　**文章编号**　1009-3516(2019)01-0079-05

Identity-Based Authentication Scheme for Equipment Support Information Network Using Latticed-Based Cryptography Theory

ZHANG Jianhang[1,2], CAO Zeyang[1], XU Qingzheng[2], HE Jian[2]
(1. Air and Missile Defense College, Air Force Engineering University, Xi'an 710051, China;
2. Information and Communication College, National University of Defense Technology, Xi'an 710106, China)

Abstract: The current equipment support information network is threatened by the quantum computer. The current identity authentication schemes for equipment support information network cannot resistant quantum computer attack, and the efficiency of these schemes is low. The first identity authentication scheme which is secure under the quantum computer environment for equipment support information network from lattice-based new cryptographic assumption is presented. Firstly, the master keys are generated from ideal lattice. Secondly, the authentication key is generated using preimage sampleable functions with the equipment identity information. Thirdly, the authentication information of the equipment is produced by non-trap door sampling technique. The scheme achieves existential unforgeability against adaptive chosen identity and message under the small integer solution assumption. Compared with the traditional schemes such as RSA and ECC authentication schemes, our scheme has higher authentication and verify efficiency at the same level of security.

收稿日期: 2018-07-14
基金项目: 国家自然科学基金(61305083)
作者简介: 张建航(1979—),男,陕西礼泉人,讲师,博士,主要从事装备保障信息网络安全问题研究。E-mail:hzjh2006@126.com

引用格式: *张建航，曹泽阳，徐庆征，等. 基于格密码理论的装备保障信息网络身份认证方案[J]. 空军工程大学学报(自然科学版)，2019，20(1)：79-83. ZHANG Jianhang, CAO Zeyang, XU Qingzheng, et al. Identity-Based Authentication Scheme for Equipment Support Information Network Using Latticed-Based Cryptography Theory[J]. Journal of Air Force Engineering University (Natural Science Edition), 2019, 20(1): 79-83.*

Key words: equipment support information network; quantum computer; latticed-based cryptography theory; identity authentication

量子计算技术的快速发展和量子计算机的崛起给基于传统密码理论的装备保障信息网络带来极大的威胁。装备保障信息网络是军用信息网络的重要组成部分,主要依托国防通信网等军用信息网络[1]。特别是战时装备保障信息网络具有动态变化的拓扑结构和较小的传输宽带,节点计算能力和存储资源易受限,节点之间快速切换变化,信道较脆弱,这都使得装备保障信息网络的认证对象之间的信任关系不断变化,加大了认证过程的复杂度和难度。目前,针对装备保障信息网络安全认证问题的研究结果很少,已有研究均是基于传统的密码理论设计的方案[2-3],还没有针对装备保障信息网络安全认证问题的量子计算环境下安全的相关文献。设计新的量子计算环境下装备保障信息网络安全且快速的认证方案是一项迫切需要解决的新问题,也是满足未来信息化战争装备作战使用与保障、发挥装备协同作战的客观需求。

1 装备保障信息网络认证面临的新挑战

1.1 现有装备保障信息网络认证方案的缺点

随着量子计算机的出现以及信息化战争进程的加快,现有装备保障信息网络认证越来越表现出许多的缺点,突出表现在以下 2 个方面:

1)当前装备保障信息网络的认证方案在量子计算环境下将变得不再安全。量子计算机之所以能对装备保障信息网络的认证方法构成严重威胁,主要是基于 2 种量子算法:①Grover 量子搜索算法[4]。该算法的计算复杂度是 N 的平方根,这个算法攻击方案相当于把密钥的长度减少到原来的一半;②Shor 量子算法[5]。该算法是可在多项式时间内破解所有可以转化为广义傅里叶变换的公钥密码算法,这个算法对正在广泛使用的基于 RSA 和 ECC 的装备保障信息网络认证方案构成致命的威胁。

2)现有装备保障信息网络认证方案效率比较低下,难以满足信息化战争快速认证的需求。众所周知,战时的装备保障信息网络由于传输宽带资源较小、节点计算资源受限等固有因素,加之基于传统公钥认证方法都需要进行模大指数、双线性对等非常复杂的数学运算,这些都造成装备保障信息网络中的认证方案实际运行速度相对缓慢,认证效率较低。

1.2 抵抗量子计算机攻击的认证方法

目前,能够抵抗量子计算机攻击的认证系统主要有 3 类[6]:①基于量子物理学的量子密码体制;②基于生物学的 DNA 密码体制;③基于量子计算机不擅长的数学困难问题构建的密码体制。

格理论已经成为前沿密码设计与分析新理论的典型代表,基于格理论设计的安全认证方案具有显著的优势[7]:

1)能够抵抗量子计算机攻击。格中新的小整数解 SIS(Small Integer Solution)问题[8]和差错学习 LWE(Learning With Errors)问题[9]都是量子计算机并不擅长计算的数学困难问题,已经被证明了在量子计算环境下仍然是安全的。

2)基于格理论的密码结构是线性的,且涉及的运算都是小整数的矩阵和向量的乘积以及向量之间的加法运算,便于系统的软、硬件实现。

3)基于格理论设计的算法和方案已经被证明了在最坏情况下和平均情况下具有同等的安全性。

2 基于格密码理论的新方法

2.1 格的概念

格是定义在 n 维欧式空间 R^n 上的离散加法子群,具体定义如下:

定义 1(格) 设给定的向量集合为 $\boldsymbol{B}=\{\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m\}\subset\mathrm{R}^n$,且 $\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m$ 为 m 个线性无关的向量,则:

$$\Lambda=\Lambda(\boldsymbol{B})=\{\sum_{i=1}^{m}x_i\boldsymbol{b}_i,x_i\in\mathrm{Z}\}$$

这样的集合 Λ 或者 $\Lambda(\boldsymbol{B})$称为格。

定义 2(理想格) 选取环 $\mathrm{Z}[x]/(x^n+1)$的理想作为本文的理想格,其中 $n=2^\lambda,\lambda\in\mathrm{Z}^+,q$ 为素数,$q=1 \bmod 2n,m=kn,k\in\mathrm{Z}^+$。理想格对应的矩阵 $\boldsymbol{A}_q^{n\times m}$ 的具体构造方法详见文献[10]。按此构造的矩阵集合记为 $L(n,m,q)$。

定义 3(Ideal-SIS 问题) 给定一个素数 q,均匀随机选取矩阵 $\boldsymbol{A}\in L(n,m,q)$,一个小的正实数 $\beta>0$,则求解一个非零向量 $\boldsymbol{e}\in\mathrm{Z}^m$,使得 $\boldsymbol{A}\boldsymbol{e}=0 \bmod q$,且 $\|\boldsymbol{e}\|_2\leqslant\beta$。

2.2 基于格理论的原像抽样函数

定义 4(原像抽样函数) 设 n 为安全参数,$q=\mathrm{poly}(n),m\geqslant 5n\log q$。由陷门抽样算法[11],可知,输出集合 $\boldsymbol{A}\in\mathrm{Z}_q^{n\times m}$ 及对应格 $\Lambda_q^{\perp}(\boldsymbol{A})$上的陷门基 $\boldsymbol{T}$,并

且 $\|\boldsymbol{T}\| \leqslant O(n\log q)$。设定高斯分布的参数 $s > \|\tilde{\boldsymbol{T}}\|\omega(\sqrt{m})$,$\tilde{\boldsymbol{T}}$ 是陷门基 $\boldsymbol{T}$ 的按列向量施密特正交化矩阵。定义 $f(\boldsymbol{e}) = \boldsymbol{A}\boldsymbol{e} \bmod q$,$\boldsymbol{T}$ 为陷门基,定义域为:$D_n = \{\boldsymbol{e} \in \mathrm{Z}^m \mid \|\boldsymbol{e}\| \leqslant s\sqrt{m}\}$。对任意给定的向量 $\boldsymbol{u} \in \mathrm{Z}^m$,利用陷门基 $\boldsymbol{T}$ 可以求得 $\boldsymbol{u}$ 在 $f(\boldsymbol{e}) = \boldsymbol{A}\boldsymbol{e} \bmod q$ 下的原像。计算任意的 $\boldsymbol{t} \in \mathrm{Z}^m$ 满足 $\boldsymbol{A}\boldsymbol{t} = \boldsymbol{u} \bmod q$。由高斯抽样算法[12],计算得出 $\boldsymbol{v} \leftarrow \mathrm{SampleD}(\boldsymbol{T}, s, -\boldsymbol{t})$,则 $\boldsymbol{v} \sim D_{\Lambda_q^{\perp}, s, -t}$。输出 $\boldsymbol{e} = \boldsymbol{t} + \boldsymbol{v}$。原像抽样函数(Preimage Sampleable Functions)简记为 $\mathrm{PSF}(\boldsymbol{A}, \boldsymbol{T}, s, \boldsymbol{u})$。

3　基于格密码理论的装备保障信息网络身份认证设计

装备保障信息网络基于身份的认证避免了 PKI 系统开销庞大的证书管理和分发,直接将用户的身份或装备标识作为公钥。身份认证方案在装备保障信息网络中主要有 3 种运行模式:第 1 种是节点之间的身份认证。节点之间的身份认证是不同节点之间的双向身份认证,主要在骨干通信网络中运行(如图 1 中①);第 2 种是节点对用户的身份认证,包括装备保障指挥网用户接入骨干通信网节点,装备保障单位接入装备保障指挥车节点,还包括用户登录操作系统时系统对用户的认证等(如图 1 中②);第 3 种是射频识别系统中的身份认证,即射频识别系统中读写器以无线方式对装备标签进行的认证,(如图 1 中③)。

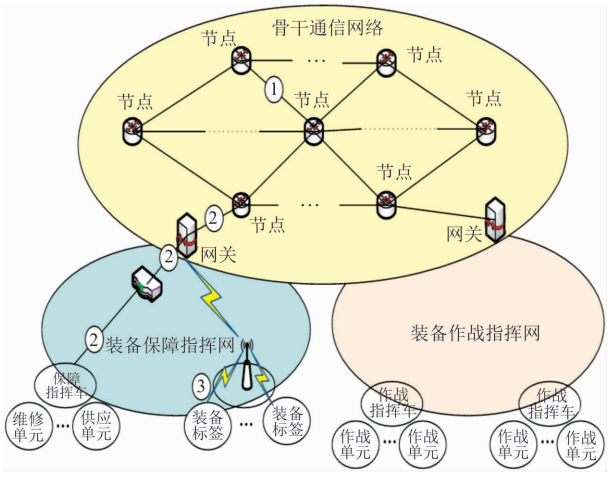

图 1　装备保障信息网络身份认证示意图

3.1　新方案参数的设定

设 n 为安全参数,q 为 2^{γ},γ 为某个正整数。运算 $\bmod q$ 的结果限制在 $[-\frac{q}{2}+1, \frac{q}{2}]$。在多项式环 $\mathrm{Z}[x]/(x^n+1)$ 中随机选择一个小系数的稀疏多项式 $f(x)$,记为 $\boldsymbol{f}$。若 $\boldsymbol{f}$ 可逆,则记为 $\boldsymbol{f}_q^{-1}$。否则,重新选择 $\boldsymbol{f}$,直到满足可逆条件。$\boldsymbol{f}$ 按照定义 3 生成环 $\mathrm{Z}[x]/(x^n+1)$ 的一个理想,理想格矩阵记为 $\boldsymbol{T}$,在此理想格中随机选择小系数多项式 $g(x)$,记为 $\boldsymbol{g}$,然后计算 $\boldsymbol{h} = \boldsymbol{f}_q^{-1}\boldsymbol{g}$,$\boldsymbol{h}$ 按照定义 3 生成环 $\mathrm{Z}[x]/(x^n+1)$ 的一个理想,该理想格矩阵记为 $\boldsymbol{A}_q^{n\times m}$,则 $\boldsymbol{f}$,$\boldsymbol{g}$ 作为私钥(陷门),$\boldsymbol{h}$ 作为公钥。设新方案中用户的身份标识 $\mathrm{id}_i (i = 1, 2, \cdots, k)$ 和待认证消息 $\boldsymbol{u}$ 均来自空间 $\{0,1\}^*$。

3.2　认证密钥生成

设高斯分布的参数 $s > \|\tilde{\boldsymbol{T}}\|\omega(\sqrt{m})$,矩阵 $\tilde{\boldsymbol{T}}$ 为矩阵 $\boldsymbol{T}$ 的列向量施密特密特正交化后得到的矩阵。我们设置一个哈希函数 $H_1: \{0,1\}^* \rightarrow \mathrm{Z}_q^{n\times m}$。然后计算哈希函数 $H_1(\mathrm{id}_i) = (\boldsymbol{h}_1, \boldsymbol{h}_2, \cdots, \boldsymbol{h}_m)$,其中 $\boldsymbol{h}_j \in \mathrm{Z}_q^n, j = 1, \cdots, m$。利用原像抽样函数进行计算,$\boldsymbol{s}_j \leftarrow \mathrm{PSF}(\boldsymbol{A}, \boldsymbol{T}, s, \boldsymbol{h}_j)$,若得到的向量组 $\boldsymbol{s}_1, \boldsymbol{s}_2, \cdots, \boldsymbol{s}_{m-1}, \boldsymbol{s}_m$ 线性无关,则输出向量组 $\boldsymbol{s}_j (j = 1, 2, \cdots, m)$。否则,重新抽取向量组 $\boldsymbol{s}_j$ 直到满足线性无关为止。设 $\boldsymbol{S}_j = (\boldsymbol{s}_1 \| \boldsymbol{s}_2 \| \cdots \| \boldsymbol{s}_m)$,那么,身份标识 id_i 的认证密钥为 $\boldsymbol{S}_i$。

3.3　身份认证过程

令 $\boldsymbol{u} \in \{0,1\}^*$ 表示一个待认证的消息,一个哈希函数 $H_2: \mathrm{Z}^n \times \{0,1\}^* \rightarrow \{-1,0,1\}^m$。则对该消息在身份 id_i 下进行如下认证:①由离散高斯分布 D_s^m 中选择一个向量 $\boldsymbol{y} \leftarrow D_s^m$;②计算 $\boldsymbol{c} = H_2(\boldsymbol{A}\boldsymbol{y} \bmod q, \boldsymbol{u})$,$\boldsymbol{z} = \boldsymbol{T}\boldsymbol{c} + \boldsymbol{y}$;③以概率 $\min\left(\frac{D_s^m(z)}{MD_{\boldsymbol{c},s}^m}\right)$ 输出 $(\boldsymbol{z}, \boldsymbol{c})$ 作为消息 $\boldsymbol{u}$ 的认证信息,M 为某个常数。

3.4　认证验证过程

对给定消息 $\boldsymbol{u}$ 和认证身份标识为 id_i 的认证消息 $(\boldsymbol{z}, \boldsymbol{c})$。验证 2 个条件是否成立:① $\|\boldsymbol{z}\| \leqslant 2s\sqrt{m}$;② $\boldsymbol{c} = H_2(\boldsymbol{A}\boldsymbol{z} - H_1(\mathrm{id}_i)\boldsymbol{c}, \boldsymbol{u})$

若以上 2 个条件都满足时,则接受认证消息,否则拒绝。

4　装备保障信息网络身份认证的性能分析

4.1　正确性证明

结论 1　在 3.1 节所述选择的安全参数下,该新方案满足正确性要求。

证明

1) $\boldsymbol{A}\boldsymbol{z} - H_1(\mathrm{id}_i)\boldsymbol{c} = \boldsymbol{A}\boldsymbol{S}_i\boldsymbol{c} + \boldsymbol{A}\boldsymbol{y} - H_1(\mathrm{id}_i)\boldsymbol{c} = \boldsymbol{A}\boldsymbol{S}_i\boldsymbol{c} + \boldsymbol{A}\boldsymbol{y} - H_1(\mathrm{id}_i)\boldsymbol{c} = \boldsymbol{A}\boldsymbol{y}$。

2)选取 $s \approx \sqrt{d(d+1)/3}$,由文献[13],则 $\|\boldsymbol{z}\|$ 以极大的概率 $1 - 2^{-m}$ 满足 $\|\boldsymbol{z}\| \leqslant 2s\sqrt{m}$。

因此,给定的新方案满足正确性要求。

4.2 安全性证明

结论 2 对于给定的参数 n,m,q,s,如果 Ideal-SIS 问题是困难的,那么本文给出的新方案在适应性选择身份和选择消息攻击下是不可伪造的。

证明 该证明的过程是构造一个攻击者 A(attacker)和挑战者 C(challenger)之间的交互式协议过程。

1)C 发送给 A 安全参数 n,m,q,s 和系统公钥 $\boldsymbol{A}$。

2)A 进行 H_1 询问。A 发送身份标识 id'_i 给 C,C 检查身份标识列表 L_1,如果该身份标识已经在列表中,则返回相应的列表值。否则,计算 $H_1(\mathrm{id}'_i)$,然后将计算的结果返回给 A。然后,C 将本次询问记录到列表 L_1 里。

3)A 进行认证询问。A 发送身份标识 id'_i 和消息 $\boldsymbol{u}'$ 给 C,要求返回相应的身份认证信息。C 对于 A 发送的 id'_i,从列表 L_1 中找到 id'_i 相应的 $\boldsymbol{S}'_i$。然后 C 由离散高斯分布 $D_{s'}^m$ 中选择一个向量 $\boldsymbol{y}\leftarrow D_{s'}^m$,并计算 $\boldsymbol{c}=H_2(\boldsymbol{A}\boldsymbol{y}\bmod q,\boldsymbol{u}')$,$\boldsymbol{z}=\boldsymbol{T}\boldsymbol{c}+\boldsymbol{y}$,哈希函数 $H_2:Z_q^n\times\{0,1\}^*\rightarrow\{-1,0,1\}^m$,以概率 $\min\left(\frac{D_{s'}^m(\boldsymbol{z}')}{MD_{Sc,s'}^m}\right)$ 输出结果$(\boldsymbol{z}',\boldsymbol{c}')$发送给 A 作为认证询问的返回值。最后 C 将$(\mathrm{id}'_i,\boldsymbol{u}',\boldsymbol{A},\boldsymbol{S}'_i,\boldsymbol{z}',\boldsymbol{c}')$保存到列表 L_2 里。

A 可以不断向 C 发起以上的询问过程,直到 A 感到满意为止。然后 A 根据询问的结果和自己掌握的信息进行身份标识和消息的伪造。对于真实的身份标识 id_i 和消息 $\boldsymbol{u}A$ 以概率 θ 输出一个伪造的认证信息$(\tilde{\boldsymbol{z}},\tilde{\boldsymbol{c}})$。接下来,$C$ 根据以上交互式协议的过程,构造一个求解 Ideal-SIS 问题的算法:①C 从列表 L_2 中查询到$(\mathrm{id}'_i,\boldsymbol{u}',\boldsymbol{A},\boldsymbol{S}'_i,\boldsymbol{z}',\boldsymbol{c}',\boldsymbol{y}')$。②$C$ 计算 $\boldsymbol{A}\tilde{\boldsymbol{z}}-H_1(\mathrm{id}'_i)\tilde{\boldsymbol{c}}$,并且检验 $\boldsymbol{A}\tilde{\boldsymbol{z}}-H_1(\mathrm{id}'_i)\tilde{\boldsymbol{c}}=\boldsymbol{A}\boldsymbol{y}'$ 是否成立。如果成立,那么 C 得到哈希函数 H_2 的一对碰撞。③如果 $\tilde{\boldsymbol{z}}\neq\boldsymbol{z}'$ 成立,那么 C 得到 Ideal-SIS 问题的一个解 $\tilde{\boldsymbol{z}}-\boldsymbol{z}'$。

根据文献[14],函数 $\boldsymbol{y}=\boldsymbol{A}\boldsymbol{s}\bmod q$ 的原像的最小熵不小于 $\omega(\log n)$。如果 A 成功地伪造了认证消息,并且有 $\tilde{\boldsymbol{z}}\neq\boldsymbol{z}'$,那么,$C$ 求解 Ideal-SIS 问题的概率不小于 $\theta(1-2^{-\omega(\log n)})$。如果 A 以不可忽略的优势概率 θ 能成功伪造一个合法认证信息,那么 C 就以极大的概率成功破解了 Ideal-SIS 问题。这与 Ideal-SIS 问题困难性假设矛盾。

综上所述,该方案在 Ideal-SIS 问题困难性假设的条件下,达到了适应性选择身份和选择消息攻击下的不可伪造性安全。

4.3 运行效率分析

本方案中,我们采用理想格结构,使得方案的空间复杂度和计算复杂度均有效降低。本方案的密钥选取算法避免了已有文献[12,15]中较复杂的陷门生成算法,类似于文献[16]的密钥生成算法,因此具有密钥生成过程简单、密钥量较小的优点。使用配置为 Intel Core i7-3770 3.4 GHz,32 GB RAM 的计算机运行程序,在达到几种不同安全级别的条件下,本方案的运行情况与传统的 RSA 和 ECC 认证方案[17]效率的比较见表 1。可以看出,在安全等级相同的条件下(128 bits),本方案的认证速率和验证速率均要高于传统的基于 RSA 和 ECC 认证方案的效率,本方案在运行过程中占用的存储空间 2.3 kb 与 RSA 运行所占存储空间 4 kb 基本持平,但是本方案运行所占存储空间 2.3 kb 与 ECC 方案所占的空间 0.5 kb 相比扩大了 3.6 倍。

表 1 本方案与 RSA 和 ECC 认证方案效率比较

	安全级别/bits	认证尺寸/kb	认证速率/(kb·s^{-1})	验证速率/(kb·s^{-1})
本方案	120	2.3	16	66
	160	2.5	10	64
RSA	103~112	2	0.8	27
	≥128	4	0.1	7.5
ECC	128	0.5	9.5	2.5
	192	0.75	5	1

5 结语

本文针对装备保障信息网络的军事特点,分析了装备保障信息网络在量子计算和信息化时代面临的新问题,基于新的格密码理论,提出了一个面向装备保障信息网络量子安全的快速身份认证方案。该方案紧密结合装备保障信息网络战争环境特点以及前沿格密码理论,以面向装备实际应用为目标,对方案进行了精心设计,从理论上证明了新方案的正确性和安全性,并对方案的运行效率进行了分析。这对于后量子时代提高我军装备保障信息网络的安全保障能力具有很重要的现实意义和应用价值。

参考文献(References):

[1] 杨学强,黄俊. 装备保障信息化建设概论[M]. 北京:国防工业出版社,2011:145-146.
YANG X Q, HUANG J. Introduction of Equipment Support Informatization Construction[M]. Beijing: National Defense Industry Press, 2011:145-146. (in Chinese)

[2] 卢昱，晏杰，陈立云，等. 装备保障信息网络身份认证体系研究[J]. 指挥与控制学报，2016，2(2)：134-138.
LU Y，YAN J，CHEN L Y. et al. The Identity Authentication Architecture for Equipment Support Information Network[J]. Journal of Command and Control，2016，2(2)：134-138. (in Chinese)

[3] 晏杰，卢昱，陈立云，等. 基于“北斗”的战场移动装备域间身份认证方法[J]. 电讯技术，2014，54(12)：1683-1687.
YAN J，LU Y，CHEN L Y. et al. Beidou-Based Inter-Domain Identity Authentication for Mobile Equipment in Battlefield[J]. Telecommunication Engineering，2014，54(12)：1683-1687. (in Chinese)

[4] GROVER L K. Quantum Mechanics Helps in Searching for a Needle in a Haystack[J]. Physical Review Letters，1997，79(2)：325-328.

[5] SHOR P W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer[J]. SIAM Journal on Computing，1997，26(5)：1484-1509.

[6] 张焕国，毛少武，吴万青，等. 量子计算复杂性理论综述[J]. 计算机学报，2016，12(29)：2404-2428.
ZHANG H G，MAO S W，WU W Q，et al. Overview of Quantum Computation Complexity Theory[J]. Chinese Journal of Computers，2016，12(29)：2404-2428. (in Chinese)

[7] PEIKERT C. A Decade of Lattice Cryptography [J]. Foundations and Trends in Theoretical Computer Science，2016，10(4)：283-424.

[8] ATTAI M. Generating Hard Instances of Lattice Problems (Extended Abstract) [C]//In 28th ACM STOC，ACM Press，1996：99-108.

[9] ODED R，On Lattices，Learning with Errors，Random Linear Codes，and Cryptography[C]//Proceedings of the 37th Annual ACM Symposium on Theory of Computing，STOC 2005. ACM Press，2005：84-93.

[10] 张建航. 快速格公钥密码方案的研究[D]. 西安：西安电子科技大学，2012：50-51.
ZHANG J H. Research on Efficient Lattice-Based Public Key Cryptosystems[D]. Xi'an：Xidian University，2012：50-51. (in Chinese)

[11] ALWEN J. PEIKERT C. Generating Shorter Bases for Hard Random Lattices. Theory of Computing Systems[C]//In STACS 2009. 48(3)：535-553.

[12] GENTRY C，PEIKERT C，VAIKUNTANATHAN V. Trapdoors for Hard Lattices and New Cryptographic Constructions[C]//In STOC 2008：197-206.

[13] LYUBASHEVSKY V. Lattice Signatures without Trapdoors[C]//EUROCRYPT2012：735-755.

[14] PEIKERT C，ROSEN A. Efficient Collision-resistant Hashing from Worst-Case Assumptions Cyclic Lattices [R]. ECCC Report TR05-158，2006：145-166.

[15] ATTAI M. Generating Hard Instances of the Short Basis Problem[C]//In ICALP，1999：1-9.

[16] HOFFSTEIN J，PIPHER J，SILVERMAN J H，NTRU：A Ring-Based Public Key Cryptosystem[M]//Proceedings of the 3rd International Symposium (ANTS-III)，LNCS 1423，1998：267-288.

[17] 陈鲁生. 现代密码学[M]. 北京：科学出版社，2000：69-71.
CHEN L S. Modern Cryptography[M]. Beijing：Science Press，2000：69-71. (in Chinese)

(编辑：徐敏)