格上基于盆景树模型的环签名

王凤和[①②] 胡予濮[①] 王春晓[③]
[①](西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)
[②](泰山学院数学与系统科学学院 泰安 271021)
[③](山东建筑大学理学院 济南 250101)

摘 要：基于格上 SIS(Short Integral Solution)问题的困难性假设，在盆景树模型下，利用盆景树签名构造了一个格上的环签名。环签名的安全性是基于格上 SIS 问题的困难性。方案实现了签名者身份的完全匿名性，在标准模型下(无随机预言机)证明环签名方案满足存在性不可伪造。

关键词：密码学；环签名；格；盆景树；基向量
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2010)10-2400-04
DOI: 10.3724/SP.J.1146.2009.01491

A Lattice-based Ring Signature Scheme from Bonsai Trees

Wang Feng-he[①②] Hu Yu-pu[①] Wang Chun-xiao[③]
[①](*Key Laboratory of Computer Networks & Information Security of Ministry of Education, Xidian University, Xi'an* 710071, *China*)
[②](*Dept. of Mathematics, Taishan Collage., Taian* 271021, *China*)
[③](*Dept. of Mathematic and physics. Shandong Jianzhu University, Jinan* 250101, *China*)

Abstract: Under the hard assumption of SIS (Short Integral Solution), a lattice-based ring signature scheme in bonsai tree model is proposed, which based on the bonsai tree signature scheme. Security of proposed ring signature is based on the hardness of SIS. The privacy of signer is guaranteed in proposed ring signature. This ring signature is also unforgeability, which is proved in the standard model (without random oracle).

Key words: Cryptography; Ring signature; Lattice; Bonsai trees; Basis vectors

1 引言

2001 年，Rivest, Shamir 和 Tauman[1]提出了环签名的概念。环签名允许成员完全匿名地实现签名，验证者可以验证该签名来自群组的成员，但无法确定签名者的身份。环签名提出后引起了广泛关注，提出了各种基于数论假设或者利用双线性对设计的标准环签名方案[2−5]及其变形的环签名方案如可控环签名[6]，代理环签名[7,8]等。环签名及其变形方案可以被广泛的应用于电子选举、电子现金、Ad hoc groups 的匿名身份(认证)等领域。然而已有工作说明著名的大整数分解与离散对数问题在量子计算机上都可以在多项式时间内解决[9]，从而使得基于它们设计的密码系统在量子环境下都将不再安全。因此设计在后量子时代依然确保安全的环签名方案成为环签名领域一个有意义的研究方向。

格上的困难问题具有在量子计算环境下依然安全的特点，因此基于格设计密码算法具有后量子安全的优势。格上设计的密码系统除具有量子安全的特点之外还有其他的优点，例如格上算法的结构简单，运算快捷(主要使用模乘和模加运算而且仅仅涉及小整数运算)、格上困难问题在最坏和一般状态下的困难性等价等等。近几年来，越来越多的密码学家开始关注在一般格上设计可证明安全的密码系统，取得一系列的重要成果[10−16]。但与利用大数分解、离散对数设计的大量带有特殊安全性能的方案、协议比较，基于一般格建立的密码系统才刚刚起步，在格上设计的具有特殊功能的密码系统还很少，尤其注意到还没有在格上实现环签名的设计(尽笔者所知)。因此基于格设计环签名方案作为格理论在环签名领域中的有效应用也成为格基密码一个有价值的研究课题。

2009 年 E-Print 上公开 Peikert[13]的最新研究成果，Peikert 在格上利用格和基的扩充技术和原象

2009-11-20 收到，2010-03-02 改回
国家自然科学基金(60970119，60803149)和国家 973 计划项目(2007CB311201)资助课题
通信作者：王凤和 fenghe2166@163.com

抽样函数[16]在盆景树模型(Bonsai Trees)下设计了一个标准模型下的数字签名方案和一个分级身份加密方案，其核心工作是盆景树模型下的格扩充技术，即从一个母格及其一组小的基向量(好基或小基)出发构造更高维数的格和它上面的小基。本文利用盆景树签名构造了一个格上的环签名方案。本文的环签名方案中每一位环成员掌握着一个格矩阵作为公钥，对应格上的一组小基作为成员的签名密钥。在每次签名时，签名者以自己公钥对应的格作为盆景树的根节点(母格)利用其他成员的公开钥和签名消息将自己的格扩展，得到一个更大维数的格并以此格作为盆景树的下一级节点(子格)，建立一个盆景树模型，在此过程中同时把母格上的小基扩展得到子格上的一组小基。利用子格上的小基通过盆景树签名完成自己的环签名。方案的安全性分析中说明方案允许成员实现完全匿名签名，验证者可以验证签名的合法性，并判断签名者确实来自群组，但是任何人不能发现签名者的身份。在标准模型下，证明方案的安全性是基于格上 SIS 问题的困难性。而格上 SIS 问题是量子计算环境下的困难问题，所以我们的格基环签名具有量子安全的特性。

2　基础知识

2.1 格

设 $\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_n$ 是 R^n 上一组线性无关的向量，格 Λ 定义为所有这些向量的整数线性组合构成的集合，即 $\Lambda=\left\{\sum_{i=1}^{n}a_i v_i \mid a_i\in Z\right\}$，$\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_n$ 构成格 Λ 的一组基。设 $\boldsymbol{\omega}$ 是一个向量，将 $\|\boldsymbol{\omega}\|_p=\left(\sum_{i=1}^{n}|\omega_i|^p\right)^{1/p}$ 定义为向量 $\boldsymbol{\omega}$ 的 l_p-范数，当 p=2 时，称作欧几里得范数。

2.2 格上的几个困难问题

以 SVP 和 CVP 问题为核心的格上困难问题，是格基密码安全性的保障，SVP 和 CVP 存在很多近似问题，本节仅仅介绍本文相关的 SVP 和 CVP 和其近似问题-SIS 问题。

(1)SVP 问题　设 $\boldsymbol{A}$ 是格的一组基，SVP 问题就是在格上寻找一个非零向量 $\boldsymbol{u}$ 满足任意格上的向量 $\boldsymbol{v}$,有 $\|\boldsymbol{u}\|\le\|\boldsymbol{v}\|$ 成立。其中 $\|\cdot\|$ 为给定的范数。

(2)CVP 问题　设 $\boldsymbol{A}$ 是格的一组基，$\boldsymbol{\omega}$ 是一个向量，CVP 问题就是要在格上寻找 $\boldsymbol{u}$，使得任意格上的向量 $\boldsymbol{v}$ 有：$\|\boldsymbol{u}-\boldsymbol{\omega}\|\le\|\boldsymbol{v}-\boldsymbol{\omega}\|$。其中 $\|\cdot\|$ 为给定的范数。

(3)SIS 问题(小整数解问题)参数 $q(\cdot),m(n),\beta(\cdot)$，给定 n 和 $\boldsymbol{A}\in Z_{q(n)}^{n\times m}$，寻找一个非零向量 $\boldsymbol{e}$，满足：$\boldsymbol{A}\boldsymbol{e}=0\bmod q(n),\|\boldsymbol{e}\|\le\beta(n)$。

2.3 盆景树原理

Peikert 引入的盆景树模型事实上是一个分级陷门函数，在盆景树模型下以某个格(一组基)作为根节点可以生成一个更大维数的格作为下一级的枝节点，同时得到格的一组基。这种由“根”到“枝”的“生长”可以是无陷门的即无指导生长(undirected growth)，此时“盆景师”在分级过程中没有使用陷门因此没有任何特权；也可以是有陷门时由“盆景师”控制盆景树的“生长”过程，包括控制生长(controlled growth)、扩展控制(extending control)和随机控制(randoming control)。本文主要使用盆景树的扩展控制方法，细节及其他原理参照文献[13]。格上的扩展控制(extending control)算法是一个由较小维数的格和基向量构造更大维数的格和基向量的算法。设任意一个格 $\Lambda(\boldsymbol{A})$ 以及它的一组基 $\boldsymbol{S}$，由 $(\boldsymbol{A},\boldsymbol{S})$ 得到一个更大维数的格 $\Lambda(\boldsymbol{A}')=\Lambda(\boldsymbol{A}\|\bar{\boldsymbol{A}})$ 及其基向量 $\boldsymbol{S}'$。我们将扩展控制记为 ExBasis$(\boldsymbol{S},\boldsymbol{A}'=\boldsymbol{A}\|\bar{\boldsymbol{A}})$，算法描述如下：

(1) $i=1,2\cdots m,\ \boldsymbol{s}_i'=\boldsymbol{s}_i\|\boldsymbol{0}\in\boldsymbol{Z}^{m'}$,

(2) $i=1,2,\cdots,\bar{m},\ \boldsymbol{s}_{m+i}'=\boldsymbol{t}_i\|\boldsymbol{e}_i$, 其中 $\boldsymbol{A}\boldsymbol{t}_i=-\bar{\boldsymbol{a}}_i=\boldsymbol{a}_{i+m}'$，$\boldsymbol{e}_i$ 是 i 个标准基向量。

文献[13]说明在盆景树模型下可以利用上述扩展控制算法构造盆景树签名。

2.4 盆景树签名

本节简要介绍文献[13]给出的盆景树签名方案。

注：签名的各个参数都是 n 的函数。

2.4.1 密钥生成　$\boldsymbol{A}\in Z_q^{n\times m_1}$ 是一个格 Λ 对应的格矩阵，$\boldsymbol{S}$ 是格 Λ 上的一组小基，设 $h(\cdot):\{0,1\}^*\to\{0,1\}^k$ 为一个安全的 hash 函数。按照同一分布随机、独立的生成 $2k$ 个矩阵 $\boldsymbol{A}_j^e\in Z_q^{n\times m_2}$，$j$=1,2,$\cdots$,$k$, e=0 或 1。则公钥为 $(\boldsymbol{A},\boldsymbol{A}_j^e)$，签名密钥为 $\boldsymbol{S}$，$m=m_1+km_2$，s 为安全参数。

2.4.2 签名　设签名消息 M 的 hash 值为 $\mu\in(0,1)$，根据 μ 各个位置的值选择对应公钥 $\boldsymbol{A}_j^e\in Z_q^{n\times m_2}$，令：$\boldsymbol{A}_\mu=\boldsymbol{A}\|\boldsymbol{A}_1^e\|\boldsymbol{A}_2^e\|\boldsymbol{A}_3^e\|\cdots\boldsymbol{A}_k^e\in Z_q^{n\times m}$，利用扩展控制算法[13]得到格 $\boldsymbol{A}_\mu$ 上的一组小基，进而利用原象抽样函数[16]生成格 $\boldsymbol{A}_\mu$ 上的一个小向量：$\boldsymbol{v}=\text{Sample}D(\text{Exbasis}(\boldsymbol{S},\boldsymbol{A}_\mu),s)$。如果取样得到 $\boldsymbol{0}$ 向量或者 $\|\boldsymbol{v}\|\ge s\sqrt{m}$，则重新取样。向量 $\boldsymbol{v}$ 作为消息 M 的签名。

2.4.3 验证　首先计算消息 M 的 hash 值 $\mu\in(0,1)$，根据 μ 各个位置的值选择对应公钥 $A_j^e\in Z_q^{n\times m_2}$，并与签名者的公钥级联得到矩阵 $\boldsymbol{A}_\mu=\boldsymbol{A}\|\boldsymbol{A}_1^e\|\boldsymbol{A}_2^e\|\boldsymbol{A}_3^e\|\cdots\boldsymbol{A}_k^e\in Z_q^{n\times m}$，然后验证：(1) $\boldsymbol{v}\ne\boldsymbol{0}$，$\|\boldsymbol{v}\|\le s\sqrt{m}$；(2) $\boldsymbol{A}_\mu\boldsymbol{v}=\boldsymbol{0}$。通过则接受签名，否则拒绝签名。

3 本文提出的环签名方案

3.1 系统生成

n 为整个方案的安全参数，其他参数都是 n 的函数。设 $U_1 \cdots U_l$ 是 l 个用户分别掌握一个格矩阵 $\boldsymbol{A}_1, \boldsymbol{A}_2 \cdots \boldsymbol{A}_l \in Z_q^{n \times m_1}$，以及对应格上的一组小基 $\boldsymbol{S}_i$。密钥分配中心随机、独立地生成 $2k$ 个矩阵 $\boldsymbol{A}_j^e \in Z_q^{n \times m_2}$，$j$=1,2,$\cdots$,$k$，$e$=0 或 1。同时密钥分配中心也要将环成员的公钥级联成一个新的矩阵 $\boldsymbol{A} = \boldsymbol{A}_1 \| \boldsymbol{A}_2 \| \boldsymbol{A}_3 \| \cdots \| \boldsymbol{A}_{l-1} \| \boldsymbol{A}_l$。设 $h(\cdot): \{0,1\}^* \to \{0,1\}^k$ 为一个输出为 k-bit 的安全 hash 函数。则环公钥为 $(\boldsymbol{A}_j^e, \boldsymbol{A})$，$j$=1,2,$\cdots$,$k$，$e$=0 或 1，对应格上的 $\boldsymbol{S}_i$ 作为用户 U_i 的签名密钥。其它安全参数定义为：$m_1 = O(n \cdot \log n)$，$m_2 = O(n \cdot \log n)$，$m' = lm_1 + km_2$，$q = O(n^2)$，$s > L\omega(\sqrt{\log n}), L = O(\sqrt{n \log q})$。

3.2 签名

设用户 U_i 要生成签名消息 M 的签名，消息的 hash 值 $\mu = h(M) \in (0,1)^k$。U_i 首先利用对应 $\mu \in (0,1)^k$ 的各个分值选择公开参数矩阵 $\boldsymbol{A}_j^e \in Z_q^{n \times m_2}$，然后建立盆景树：利用秘密钥 $\boldsymbol{S}_i$ 将格 $\boldsymbol{A}_i$ 扩展为更大维数的格 $\boldsymbol{A}' = \boldsymbol{A}_i \| \boldsymbol{A}_1 \| \boldsymbol{A}_2 \| \cdots \| \boldsymbol{A}_{i-1} \| \boldsymbol{A}_{i+1} \| \cdots \| \boldsymbol{A}_k \| \boldsymbol{A}_1^{\mu_1} \| \cdots \| \boldsymbol{A}_k^{\mu_k}$，并生成此格上的一组小基 $\boldsymbol{S}'_\mu$。然后用户 U_i 改变 $\boldsymbol{A}'$ 中各个子阵 $\boldsymbol{A}_i$ 的位置使之与环公钥 $\boldsymbol{A}$ 一致并相应得改变基 $\boldsymbol{S}'_\mu$ 中各分量的位置，得到 $\boldsymbol{A}_\mu$ 和 $\boldsymbol{S}_\mu$。通过 $\boldsymbol{A}_\mu, \boldsymbol{S}_\mu$，利用盆景树签名得到向量 $\boldsymbol{v}$：$\boldsymbol{v} = \text{Sample}D(\text{Exbasis}(\boldsymbol{S}_i, \boldsymbol{A}_\mu), s)$。$\boldsymbol{v}$ 作为消息 M 的签名。

3.3 验证

验证者得到消息 M 的签名 $\boldsymbol{v}$ 后，首先计算 hash 函数值 $\mu = h(M) \in (0,1)^k$，利用 μ 的各个分量值选取环参数矩阵 $\boldsymbol{A}_j^e$，并与环公钥 $\boldsymbol{A}$ 级联得到 $\boldsymbol{A}_\mu$，然后验证：(1) $\boldsymbol{v} \neq \boldsymbol{0}$，$\| \boldsymbol{v} \| \leq s\sqrt{m}$；(2) $\boldsymbol{A}_\mu \boldsymbol{v} = \boldsymbol{0}$。通过以上验证则接受签名，否则拒绝签名。

说明 该环签名的主要基于盆景树签名格完成签名，完备性验证参照文献[13]，本文略。

4 环签名的性能分析

4.1 匿名性

定理 1 本文的方案实现了签名者身份的完全匿名性。

证明 消息的环签名是大维数格上的一个范数较小的向量，而大维数格矩阵 $\boldsymbol{A}_\mu$ 中子阵 $\boldsymbol{A}$ 包含所有环成员的公钥信息，注意到这些公钥的位置是完全平等的，因此从任何一个成员的公钥出发都可能得到该消息的签名 $\boldsymbol{v}$，即每一个成员都可能生成此签名，因此验证者不能从 $\boldsymbol{v}$ 中分解出签名者公钥的任何信息，他只能以 $1/l$ 的概率推测签名人的身份，l 是成员的个数；而要通过大维数格上的一个小向量得到小维数格上的一组小基(签名密钥)来对应签名人的身份更是不可行的。进一步地，消息的环签名 $\boldsymbol{v}$ 服从格上的正态分布[13]，因此任意两个环成员的签名或者一个环成员对两个消息的签名服从的概率分布对验证者而言是不可区分的。所以环签名实现了无条件匿名性。 证毕

4.2 存在性不可伪造性

定义 1 存在性不可伪造：一个签名方案称作是存在性不可伪造的，如果对于任意多项式时间的伪造者在掌握签名公钥的条件下通过与签名者的多项式有限次的交互得到有限个消息对应的签名，如果伪造者能够输出一个新消息的合法签名的概率是可以忽略的。

定理 2 假设存在不是任何环成员的概率多项式时间敌手 F 能够至多通过 Q 次 hash 询问，Q_1 次环签名询问以不可忽略的概率 ε 伪造新的消息 μ (假设 μ 是一个 hash 值)的合法环签名，其中消息 μ 从未在签名询问中被询问过。则可以构造算法 S 以近似 ε / kQ_1 的概率来解大维数格上的 SIS 问题。

证明 设算法 S 得到一个大维数格上 SIS 问题的实例 $(q, m', s\sqrt{m'}, \boldsymbol{A})$，其中矩阵 $\boldsymbol{A} = \boldsymbol{A}_0 \| \boldsymbol{U}_1^0 \| \boldsymbol{U}_1^1 \| \boldsymbol{U}_2^0 \| \boldsymbol{U}_2^1 \| \cdots \| \boldsymbol{U}_k^0 \| \boldsymbol{U}_k^1$，$\boldsymbol{A}_0 \in Z_q^{n \times lm_1}, \boldsymbol{U}_i^b \in Z_q^{n \times m_2}$，$l$ 为正整数，b 取 0 或 1，$m' = 2km_2 + lm_1$。算法 S 希望利用敌手 $\mathcal{F}$ 作为子程序得到一个范数小于 $s\sqrt{m'}$ 的向量，满足 $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{0}$ 成立。为此算法 S 充当挑战者与敌手 $\mathcal{F}$ 进行以下询问应答的游戏，鼓励敌手攻击环签名方案。首先算法 S 维护两张列表 L_1 和 L_2 以保持询问回应的一致性。L_1 用于跟踪记录敌手 $\mathcal{F}$ 的 hash 询问，L_2 用于跟踪敌手 $\mathcal{F}$ 的环签名询问。不失一般性，假设敌手 $\mathcal{F}$ 在做签名询问前已经经过了 Q 次正确的 hash 询问并得到了消息的正确 hash 函数值。设待签名的消息为 $\mu_1 \cdots \mu_Q$ (hash 值)，则算法 S 计算比特串 p 的集合 T，p 取不是任何 $\mu_1 \cdots \mu_Q$ 前缀的最小的比特串，于是 $|p| < k$(注：由文献[13]集合 T 可以在多项式时间内计算得到)。算法 S 在集合 T 中任意取一个 p，设 $t = |p|$，算法 S 生成环签名的公钥如下：

(1) $i \leq t, \boldsymbol{A}_i^{(p_i)} = \boldsymbol{U}_i^0, t < i < k, b \in \{0,1\}: \boldsymbol{A}_i^b = \boldsymbol{U}_i^0$；

(2) $i \leq t$，生成矩阵 $\boldsymbol{A}_i^{1-p_i}$ 及小基 $\boldsymbol{S}_i$。

将矩阵 $\boldsymbol{A}_0$ 作为环签名方案中环成员公钥级联得到矩阵，矩阵 $\boldsymbol{A}_i^b$ 对应一个环签名方案中的环公开参数矩阵 $\boldsymbol{A}_j^e$。以 $(\boldsymbol{A}_0, \boldsymbol{A}_i^b)$ 来初始化敌手 $\mathcal{F}$，让敌手 $\mathcal{F}$ 来攻击以上环签名。

签名询问：设算法 S 开始为敌手 $\mathcal{F}$ 发送消息 μ_J 的签名询问生成环签名：在列表 L_2 中寻找此消息的

签名记录 $\boldsymbol{v}_J$，若找到此消息则返回列表中相应的 $\boldsymbol{v}_J$ 作为签名。若消息 μ_J 不在 L_2 中，设 i 为第一个满足 $\mu_{j_i} \neq p_i$ 的位置，算法 S 通过格 $\boldsymbol{A}_i^{(1-p_i)}$ 及其好基 $\boldsymbol{S}_i$ 利用盆景树下的扩展控制算法得到格 $\boldsymbol{A}_{\mu_J} = \boldsymbol{A}_0 \,||\, \boldsymbol{A}_1^{(p_1)} \,||\, \boldsymbol{A}_2^{(p_2)} \,||\cdots||\, \boldsymbol{A}_{i-1}^{(p_{i-1})} \,||\, \boldsymbol{A}_i^{(p_i)}$ 及其好基 $\boldsymbol{S}_{\mu_J}$，然后利用原象抽样算法得到消息 μ_J 的签名 $\boldsymbol{v}_J$，将消息 μ_J 的签名 $\boldsymbol{v}_J$ 发送给敌手 $\mathcal{F}$，同时在列表 L_2 中存储消息 μ_J 及其签名 $\boldsymbol{v}_J$。在敌手 $\mathcal{F}$ 对所有签名询问满意后，敌手 $\mathcal{F}$ 以概率 ε 生成第 Q_1+1 个消息 μ_{Q_1+1} 的伪造签名 $\boldsymbol{v}_{Q+1}$。算法 S 检查 p 是否是消息 μ_{Q+1} 的前缀，如果不是 μ_{Q_1+1} 的前缀，算法 S 终止游戏，宣布失败。否则 p 是 μ_{Q_1+1} 的前缀，则矩阵 $\boldsymbol{A}_{\mu_{Q+1}}$ 是由矩阵 $\boldsymbol{A}_0$ 和 k 个 $\boldsymbol{U}_i^{(b)}$ 级联得到。所以算法 S 可以通过添加子阵并调整子阵的顺序同时在 $\boldsymbol{v}_{Q_1+1}$ 上添加相应的 0 并调整顺序，得到一个向量 $\boldsymbol{v}$，满足：$\boldsymbol{A}\boldsymbol{v} = \boldsymbol{0} (\bmod q)$，由模拟过程知 $||\boldsymbol{v}|| \leqslant s\sqrt{m'}$。从而算法 S 成功得到 $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{0}$ 的一个小整数解。

分析算法 S 成功的优势：算法 S 成功的关键是随机选取的集合 T 中的比特串 p 应该是第 Q_1+1 个消息 μ_{Q_1+1} 的前缀，此概率接近 $1/kQ_1$，从而算法 S 成功的概率近似为 ε / kQ_1。　　证毕

4.3 效率分析

方案的一个不足之处是在签名时要将盆景树模型下的母格扩充为一个比原始盆景树签名更大维数的格，原因是环成员需要联合其他成员的公钥。这使得环签名中签名格的维数要大于原始的盆景树签名。设 $m_1 = c_1 n \lg q$, $m_2 = c_2 n \lg q$，其中 c_1,c_2 为常数，本文的方案中签名格矩阵的列数和签名长度为 $kc_1 n \lg q + lc_2 n \lg q$，$l$ 为环成员的个数。所以本文签名效率要低于盆景树签名，事实上一般的特殊签名的效率总要比原始签名要低。本文环签名方案中用户的密钥长度都为 $m_1 \lg q$，与盆景树签名相同。公钥长度为 $2km_2 n \lg q + lm_1 n \lg q$，其中 l 是环成员个数，k 是 hash 函数的输出长度。由于方案设计中仅仅使用到了小整数的模加和模乘运算，所以计算效率较高。但是方案密钥长度较大，所以存储代价较高，这也是当前格基密码普遍存在的效率瓶颈。如何设计效率更高的格基环签名方案值得进一步研究。

5　结论

利用盆景树模型，借助盆景树签名，在格上构造了一个环签名方案。实现了环签名的完全匿名性和签名的存在性不可伪造性，在标准模型下证明方案的不可伪造性是基于格上 SIS 问题的困难性，因此方案具有在量子计算环境下依然安全的优点。

参 考 文 献

[1] Rivest R, Shamir A, and Tauman Y. How to leak a secret [C]. AsiaCrypt2001. Berlin, Springer-Verlag, 2001, Vol. 2248: 552–565.

[2] Zhang Fang-guo and Kim K. ID-based blind signature and ring signature from pairings[C]. ASIACRYPT 2002, Queenstown, New Zealand, 2002: 533–547.

[3] Chow S. M, Yiu S-M, and Hui L C K. Efficient identity based ring signature[C]. ACNS 2005, LNCS, 2005, Vol. 3531: 499–512.

[4] Herranz J and S′ aez G. New identity-based ring signature schemes[C]. ICICS2004, LNCS, 2004, Vol. 3269: 27–39.

[5] Dodis Y, Kiayias A, Nicolosi A, and Shoup V. Anonymous identification in Ad Hoc groups[C]. Eurocrypt'2004, LNCS, 2004, Vol.3027: 609–626.

[6] Wei Gao, Wang Gui-lin, Wang Xue-li, and Xie Dong-qing. Controllable ring signatures[C]. WISA 2006, LNCS, 2007, Vol. 4298: 1–14.

[7] Li Jin, Chen Xiao-feng, Yuen Tsz-hon, and Wang Yan-ming. Proxy ring signature: formal definitions, efficient construction and new variant[C]. CIS2006, LNAI, 2007, Vol.4456: 545–555.

[8] 鲍皖苏, 隗云, 钟普查. 原始签名人匿名的代理环签名研究[J]. 电子与信息学报, 2009, 31(10): 2392–2396.
Bao Wan-su, Wei Yun, and Zhong Pu-cha. Research on proxy ring signature with anonymity of the original signer. *Journal of Electronics & Information Technology*, 2009, 31(10): 2392–2396.

[9] Shor P W. Polynomial-time algorithm for prime factorizeation and discrete logarithm on a quantum computer[J]. *SIAM Journal on Computing*, 1997, 26(5): 1484–1509.

[10] Lyubashevsky V and Micciancio D. Asymptotically Efficient Lattice-Based Digital Signature[C]. TCC2008, LNCS, 2008, Vol. 4948: 37–54.

[11] Regev O. On Lattice, learning with errors, random linear codes, and cryptography[C]. STOC'05, Baltimore, MD 2005: 84–93.

[12] Lyubashevsky V. Lattice-based identification schemes secure under active attacks[C]. PKC' 2008, LNCS, 2008, Vol. 4939: 162–179.

[13] Peikert C. Bonsai Trees [EB/OL]. http:// eprint.iacr.org /2009/359.

[14] Alwen J and Peikert C. Generating shorter bases for hard random lattices[C]. In STACS'2009, Freiburg-Germany, 2009: 75–86.

[15] Micciancio D and Regev O. Worst-case to average-case reductions based on gaussian measures[J]. *SIAM J. Compututer*, 2007, 37(1): 267–302.

[16] Gentry C, Peikert C, and Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions[C]. STOC'2008, Victoria, BC- Canada, 2008: 197–206.

王凤和：　男，1979 年生，博士，讲师，研究方向为格密码、数字签名.

胡予濮：　男，1955 年生，博士生导师，教授，研究方向为信息安全、网络安全.

王春晓：　女，1979 年生，硕士，讲师，研究方向为数字签名.