基于格的变色龙签名方案

谢 璇 喻建平 王 廷 张 鹏
(深圳大学ATR国防科技重点实验室 深圳 518060)

摘 要 与普通数字签名相比,变色龙签名不仅满足不可否认性,而且具有非交互式、不可传递的特点。然而,基于传统数学难题构造的变色龙签名方案不能抵抗量子计算机的攻击。为了设计在量子计算机环境下依然安全的变色龙签名,利用格上小整数解问题SIS(Small Integer Solution)和非齐次小整数解问题ISIS(Inhomogeneous Small Integer Solution)的困难性假设,构造了基于格的变色龙签名方案。在随机预言模型下,证明了该方案在适应性选择消息攻击下是安全的。

关键词 格,变色龙签名,变色龙哈希函数,SIS,ISIS
中图法分类号 TP309 **文献标识码** A

Chameleon Signature Scheme Based on Lattice

XIE Xuan YU Jian-ping WANG Ting ZHANG Peng
(ATR Key Lab of National Denfence Technology, Shenzhen University, Shenzhen 518060, China)

Abstract The chameleon signatures not only meet the characteristics of non-repudiable, but also are non-interactive and non-transferable compared with the traditional digital signatures. However, the scheme of chameleon signature based on traditional mathematic problem construction can not defense the attack of the quantum computers. In order to design a safe Chameleon signature in the environment of quantum computers, a lattice-based Chameleon signature was proposed, which is based on the hardness of average-case SIS(Small Integer Solution) and ISIS(Inhomogeneous Small Integer Solution). Further more, we proved that this scheme is unforgeability under adaptive chosen-message attack in the random oracle model.

Keywords Lattice, Chameleon signature, Chameleon hash function, SIS, ISIS

1 引言

H. Krawczyk 和 T. Rabin[1] 于2000年首次提出变色龙签名(Chameleon Signatures)的概念,并构造了第一个基于离散对数难题的变色龙签名方案。区别于普通数字签名,变色龙签名中采用变色龙哈希函数对消息散列。在没有陷门信息时,变色龙哈希函数与普通哈希函数具有相同的性质;当拥有陷门信息时,很容易找到另一输入具有相同的哈希值。变色龙签名中指定签名验证者,且该验证者能对已知签名伪造消息,使得验证等式依然成立。因此,变色龙签名和不可否认签名类似,同样具有不可传递性,但是它的优势在于,其不需要交互协议。由于变色龙签名具有这些特点,因此它特别适合应用于电子投票和电子拍卖等领域[2,3]。

近年来,随着量子计算机的发展,传统密码体制中的困难性问题如大整数分解和离散对数问题都可以使用量子计算机在多项式时间内解决。作为传统密码体制基石的困难性问题一旦得到破解,在其上构造的各种加密算法、数字签名算法的安全性将遭到致命的威胁。因此,设计一种能抵抗量子计算机攻击的变色龙签名方案在后量子时代数字签名研究中是十分必要的。由于格上一些困难问题如:最短向量问题SVP(Shortest Vector Problem)、最近向量问题CVP(Closest Vector Problem)等都被证明是NP困难的,并且没有发现量子多项式破译算法,因此基于格理论构造能够抵抗量子计算机攻击的密码体制[4-8]成为了后量子时代国内外众多专家学者的研究热点。

Gentry, Peikert 和 Vaikuntanathan 在文献[4]中给出了原像采样陷门函数组的定义,并以此原像采样陷门函数组为基础构造了普通数字签名方案。本文以此普通签名方案为基础,运用D. Cash等在文献[5]设计的基于格的变色龙哈希函数构造了基于格的变色龙签名方案。最后,证明了该变色龙签名方案不仅满足不可传递性,在基于平均情况 $SIS_{q,m,2s\sqrt{m}}$ 问题是困难的假设下还满足在适应性选择消息攻击下是不可伪造的。

2 基础知识

2.1 格

定义1(格) $b_1, b_2, \cdots, b_k$ 为 $\mathbf{R}^n$ 中 k 个线性无关的向量,由它们的整数线性组合构成的集合:

到稿日期:2012-04-21 返修日期:2012-06-15 本文受国家自然科学基金(61171072,61001058)资助。
谢 璇(1987—),男,硕士,主要研究领域为密码学与信息安全,E-mail:xiexuan200308@126.com;喻建平(1968—),男,博士,教授,博士生导师,主要研究领域为密码学与信息安全。

$$L(b_1,b_2,\cdots,b_k)=\{\sum_{i=1}^{k}x_ib_i \mid x_i\in\mathbf{Z}\}$$

即为格。其中 k 为格 L 的秩，n 为格 L 的维数，一般 $k\leqslant n$，当 $k=n$ 时，称 L 为满秩格。格 L 中最短距离 $\lambda_1(L(\mathbf{B}))$ 指格中最短非零向量的长度。

在基于格的密码体制中最常用的是以下 3 类整数格，因格中向量的元素均取自 $\mathbf{Z}_q$，故称之为 q 模格。

定义 2(q 模格)　已知整数 q,m,n 和矩阵 $\mathbf{A}\in\mathbf{Z}_q^{n\times m}$，且 $\mathbf{u}\in\mathbf{Z}_q^n$，有

$$\mathbf{\Lambda}_q(\mathbf{A})=\{\mathbf{x}\in\mathbf{Z}^m:\mathbf{x}=\mathbf{A}^{\mathrm{T}}\mathbf{s} \bmod q \text{ for some } \mathbf{s}\in\mathbf{Z}^n\}$$

$$\mathbf{\Lambda}_q^{\perp}(\mathbf{A})=\{\mathbf{x}\in\mathbf{Z}^m:\mathbf{Ax}=0 \bmod q\}$$

$$\mathbf{\Lambda}_q^{\mathbf{u}}(\mathbf{A})=\{\mathbf{x}\in\mathbf{Z}^m:\mathbf{Ax}=\mathbf{u} \bmod q\}$$

2.2　格上困难问题

格上最核心的困难问题是著名的最短向量问题 SVP (Shortest Vector Problem) 和最近向量问题 CVP (Closest Vector Problem)。

定义 3(SVP)　给定格基 $\mathbf{B}$，找出格 $L(\mathbf{B})$ 中的最短非零向量。

定义 4(CVP)　给定格基 $\mathbf{B}$ 和一目标向量 $\mathbf{t}$，找出格 $L(\mathbf{B})$ 中离 $\mathbf{t}$ 最近的向量。

为了便于构造密码算法，通常将格上一些最基本的困难性问题作一定的规约转化成某些困难程度近似的问题。其中最常见的是小整数解问题 SIS 和非齐次小整数解问题 ISIS。

定义 5(小整数解问题 SIS)　给定整数 q，矩阵 $\mathbf{A}\in\mathbf{Z}_q^{n\times m}$ 和实数 β，求解满足 $\mathbf{Ae}=0 \bmod q$ 的整数向量 $\mathbf{e}\in\mathbf{Z}^m$，且 $\|\mathbf{e}\|\leqslant\beta$。其中 q,m,β 都可以由 n 的多项式表示，$\mathbf{A}$ 是随机均匀的，$\|\cdot\|$ 表示欧几里德范数。

定义 6(非齐次小整数解问题 ISIS)　给定整数 q，矩阵 $\mathbf{A}\in\mathbf{Z}_q^{n\times m}$ 和实数 β，求解满足 $\mathbf{Ae}=\mathbf{u} \bmod q$ 的整数向量 $\mathbf{e}\in\mathbf{Z}^m$，且 $\|\mathbf{e}\|\leqslant\beta$。其中 $\mathbf{u}\in\mathbf{Z}_q^n,q,m,\beta$ 都可以由 n 的多项式表示，$\mathbf{A}$ 是随机均匀的，$\|\cdot\|$ 表示欧几里德范数。

如果 $\mathbf{A},\mathbf{u}$ 是均匀选取的，则称 SIS 和 ISIS 是一般情况困难(Hard-on-Average)问题。SIS 问题等同于在 q 模格 $\mathbf{\Lambda}_q^{\perp}(\mathbf{A})$ 上寻找短的非零向量问题。D. Micciancio 和 O. Regev 在文献[9]中证明了在选择合适参数的情况下 SIS 和 ISIS 问题是 NP 困难的。

2.3　原像采样陷门函数

定理 1[4]　设 n 为安全参数，q 为素数，令 $m\geqslant 2n\log q$，对所有的 $\mathbf{A}\in\mathbf{Z}_q^{n\times m}$，$s\geqslant\omega(\sqrt{\log m})$ 和 $\mathbf{e}\leftarrow D_s^m$，$s$ 则以压倒性概率使得 $\mathbf{u}=\mathbf{Ae} \bmod q$ 在 $\mathbf{Z}_q^n$ 上是统计均匀分布的。

定理 1 表明了若输入为格的离散高斯分布上采样所得的点，那么随机均匀选取的矩阵向量积在该矩阵所生成的向量空间上也是均匀分布的。

定理 2[4,10]　给定素数 $q=poly(n)$，整数 $m\geqslant 5n\log q$，存在一概率多项式算法 TrapGen(1^n) 输入 1^n，输出矩阵 $\mathbf{A}\in\mathbf{Z}_q^{n\times m}$ 和满秩集合 $\mathbf{S}\subset\mathbf{\Lambda}_q^{\perp}(\mathbf{A})$，其中 $\mathbf{A}$ 在 $\mathbf{Z}_q^{n\times m}$ 上是统计均匀分布的，并且 $\|\mathbf{S}\|\leqslant L\approx m^{1+\varepsilon},\varepsilon>0$。

基于平均情况下 SIS 和 ISIS 问题，Gentry 等在文献[4]中给出了原像采样陷门函数的具体构造。简单描述如下：

(1)根据定理 2 生成$(\mathbf{A},\mathbf{S})$。其中 $\mathbf{A}$ 为公钥，$\mathbf{S}$ 为私钥。

(2)定义函数 f_{A} 为 $f_{\mathrm{A}}(\mathbf{e})=\mathbf{Ae} \bmod q$，定义域为 $\mathbf{D}_n=\{\mathbf{e}\in\mathbf{Z}^m:\|\mathbf{e}\|\leqslant s\sqrt{m}\}$，值域为 $\mathbf{R}_n=\mathbf{Z}_q^n$，向量 $\mathbf{e}$ 服从 $D\mathbf{Z}^m,s$ 分布。

(3)单向陷门求逆算法 SamplePre($\mathbf{A},\mathbf{S},s,\mathbf{u}$)：采用线性代数的方法找任意向量 $\mathbf{t}\in\mathbf{Z}^m$ 满足 $\mathbf{At}=\mathbf{u} \bmod q$，然后输入陷门 $\mathbf{S}$、中心 $\mathbf{t}$、偏移量 s，利用高斯采样算法在格 $\mathbf{\Lambda}_q^{\perp}(\mathbf{A})$ 的离散高斯分布中取向量 $\mathbf{v}$，求得原像值 $\boldsymbol{\sigma}=\mathbf{t}+\mathbf{v}$。

事实上，$\boldsymbol{\sigma}$ 满足函数：$f_{\mathrm{A}}(\boldsymbol{\sigma})=\mathbf{A}\boldsymbol{\sigma}=\mathbf{u} \bmod q$。下文中将 SamplePre($\mathbf{A},\mathbf{S},s,\mathbf{u}$)简写成 SamplePre($\mathbf{S},\mathbf{u}$)。

定理 3[4]　如果没有陷门，基于平均情况下 $\mathbf{ISIS}_{q,m,s\sqrt{m}}$ 问题是困难的假设，以上构造的原像采样陷门函数 f_{A} 是单向的。基于平均情况下 $\mathbf{SIS}_{q,m,2s\sqrt{m}}$ 问题是困难的假设，此函数是抗碰撞的。

3　变色龙签名方案

3.1　方案设计

本文以文献[4]提出的格上基本签名方案为基础，结合文献[5]设计的基于格的变色哈希函数构造了格上变色龙签名方案。该签名方案分为参数设置(Setup)，密钥生成(KeyGen)，签名(Sign)，验证(Verify) 4 个部分。

(1)Setup

约定　Alice 为签名者，Bob 为签名接收者(拥有变色龙哈希函数陷门)，n 为安全参数，设 $q=poly(n)$，$m\geqslant 5n\log q$，$L=m^{1+\varepsilon}$，其中 $\varepsilon>0$，高斯参数 $s\geqslant L\cdot\omega(\sqrt{\log m})$，消息空间 $M=\{0,1\}^k$，随机空间 $R=\{\mathbf{r}\in\mathbf{Z}^m:\|\mathbf{r}\|\leqslant s\cdot\sqrt{m}\}$ 服从 $D\mathbf{Z}^m,s$ 分布。上述参数设置既满足了 $\mathbf{SIS}_{q,m,2s\sqrt{m}}$ 和 $\mathbf{ISIS}_{q,m,s\sqrt{m}}$ 问题的困难性假设，也满足了构造变色龙哈希函数的参数要求[4,5]。

(2)KeyGen(1^n)

输入安全参数 n，两次调用 TrapGen(1^n) 分别生成随机均匀矩阵 $\mathbf{A}_1,\mathbf{A}_2\in\mathbf{Z}_q^{n\times m}$ 和满秩集合(陷门)$\mathbf{S}_1,\mathbf{S}_2$，其中 $\mathbf{S}_1\subset\mathbf{\Lambda}_q^{\perp}(\mathbf{A}_1)$，$\mathbf{S}_2\subset\mathbf{\Lambda}_q^{\perp}(\mathbf{A}_2)$。定义原像采样陷门函数 $f_{\mathrm{A}_2}(\mathbf{s})=\mathbf{A}_2\mathbf{s} \bmod q$。$\mathbf{A}_1$ 用于构造变色龙哈希函数，$\mathbf{A}_2$ 为变色龙签名验证密钥，$\mathbf{S}_1$ 为变色龙哈希函数陷门，$\mathbf{S}_2$ 为变色龙签名私钥。Bob 秘密持有 $\mathbf{S}_1$，Alice 秘密持有 $\mathbf{S}_2$。

(3)Sign($\mathbf{m},\mathbf{A}_1,\mathbf{S}_2$)

输入待签名消息 $\mathbf{m}\in M$、随机均匀矩阵 $\mathbf{A}_1$、变色龙签名私钥 $\mathbf{S}_2$，签名算法输出变色龙签名 $\boldsymbol{\sigma}$。具体步骤如下：

①Alice 随机均匀选取 $\mathbf{A}_0\in\mathbf{Z}_q^{n\times k}$，$\mathbf{r}\in R$(其中 $\mathbf{A}_0$ 公开，$\mathbf{r}$ 不公开)，令 $\mathbf{A}=\mathbf{A}_0\|\mathbf{A}_1$，待签名消息 $\mathbf{m}\in M$，构造从消息空间 M 和随机空间 R 映射到值域 $Y=\mathbf{Z}_q^n$ 的哈希函数：

$$h_A(\mathbf{m};\mathbf{r})=\mathbf{A}\cdot(\mathbf{m}\|\mathbf{r})=\mathbf{A}_0\mathbf{m}+\mathbf{A}_1\mathbf{r}$$

(Cash 等在文献[5]中证明了假设 $\mathbf{SIS}_{q,m,2s\sqrt{m}}$ 问题是困难的，那么哈希函数 h_{A} 满足变色龙哈希函数的性质)

然后，Alice 将待签名消息 $\mathbf{m}$ 经变色龙哈希函数 h_{A} 处理后输出为 $\mathbf{y}=h_{\mathrm{A}}(\mathbf{m};\mathbf{r})$；最后，Alice 对 $\mathbf{y}$ 进行签名。

②Alice 对计算得到的每个待签名消息 $\mathbf{m}$ 的变色龙哈希值 $\mathbf{y}$，先查询本地消息签名库，如果$(\mathbf{y},\boldsymbol{\sigma})$已经存在，则输出 $\boldsymbol{\sigma}$ 作为对待签名消息 $\mathbf{m}$ 的变色龙签名；否则 Alice 调用 SamplePre($\mathbf{S}_2,\mathbf{y}$)，输入变色龙签名私钥 $\mathbf{S}_2$ 和消息散列值 $\mathbf{y}$，利用陷门 $\mathbf{S}_2$ 求 $\mathbf{y}$ 对应 f_{A_2} 的原像 $\boldsymbol{\sigma}$，输出 $\boldsymbol{\sigma}$ 作为对消息 $\mathbf{m}$ 的变色龙签名，并将$(\mathbf{y},\boldsymbol{\sigma})$存储到本地。最后，Alice 将$(\mathbf{m},\mathbf{r},\boldsymbol{\sigma})$发送给 Bob 进行签名验证。

(4)Verify($\mathbf{A}_0,\mathbf{A}_1,\mathbf{A}_2,\mathbf{m},\mathbf{r},\boldsymbol{\sigma}$)

输入消息 $\mathbf{m}$、随机向量 $\mathbf{r}$、Alice 的签名 $\boldsymbol{\sigma}$、随机均匀矩阵

$\mathbf{A}_0$ 和 $\mathbf{A}_1$、变色龙签名验证密钥 $\mathbf{A}_2$，Bob 验证签名的过程如下：如果 $\boldsymbol{\sigma}\in\mathbf{Z}^m$ 且 $\mathbf{A}_2\boldsymbol{\sigma}=\mathbf{A}_0\mathbf{m}+\mathbf{A}_1\mathbf{r}$，则验证通过，否则拒绝。

事实上，$\mathbf{y}$ 是待签名消息 $\mathbf{m}$ 经变色龙哈希函数 $h_{\mathrm{A}}(\mathbf{m};\mathbf{r})$ 哈希后的输出，即 $\mathbf{y}=h_{\mathrm{A}}(\mathbf{m};\mathbf{r})=\mathbf{A}_0\mathbf{m}+\mathbf{A}_1\mathbf{r}$；$\boldsymbol{\sigma}$ 是利用陷门 $\mathbf{S}_2$ 求得 $\mathbf{y}$ 对应原像采样陷门函数 $f_{\mathbf{A}_2}$ 的原像，即：$\mathbf{y}=f_{\mathbf{A}_2}(\boldsymbol{\sigma})=\mathbf{A}_2\boldsymbol{\sigma} \bmod q$。于是，一个合法签名 $\boldsymbol{\sigma}$ 应满足 $\mathbf{A}_2\boldsymbol{\sigma}=\mathbf{A}_0\mathbf{m}+\mathbf{A}_1\mathbf{r}$。

3.2 安全性分析

结论 1　基于平均情况 $\mathbf{SIS}_{q,m,2s\sqrt{m}}$ 问题是困难的假设下，本文构造的变色龙签名方案在适应性选择消息攻击下是不可伪造的。

证明：对本定理的证明可转化为证明在不知道签名者私钥和变色龙哈希函数陷门的情况下，任何第三方都无法伪造一个合法的变色龙签名。本文借鉴文献[4]中的证明方法，结合变色龙哈希函数的特殊性质进行证明，如下：

假设存在一敌手 $\mathcal{A}$ 能够以不可忽略的概率 ε 伪造变色龙签名方案的一个签名，那么，存在一概率多项式时间算法 $\mathcal{S}$，能够在不需要陷门的情况下以接近 ε 的概率找到原像采样陷门函数的一个碰撞。矩阵 $\mathbf{A}$ 为原像采样陷门函数 f_{A} 的索引，$\mathcal{S}$ 以 $\mathbf{A}$ 为公钥运行 $\mathcal{A}$，$\mathcal{A}$ 询问变色龙哈希函数 h_{A} 和签名预言机如下（不失一般性，假设 $\mathcal{A}$ 在询问签名预言机之前都要先对变色龙哈希函数 h_{A} 进行询问）：

对变色龙哈希 h_{A} 的询问：$\mathcal{A}$ 对每次输入不同的消息 $\mathbf{m}\in\{0,1\}^*$，$\mathcal{S}$ 先查询本地存储是否有 $(\mathbf{m},\boldsymbol{\sigma})$，如果有，则返回 $f_{\mathbf{A}_2}(\boldsymbol{\sigma})$，如果没有，则调用定义域采样均匀输出算法 SampleDom(1^n)[4] 生成 $\boldsymbol{\sigma}$ 并存储到本地，最后返回 $f_{\mathbf{A}_2}(\boldsymbol{\sigma})$ 给 $\mathcal{A}$。

对签名预言机的询问：当 $\mathcal{A}$ 询问消息的散列值 $\mathbf{y}$ 的签名时，$\mathcal{S}$ 将查询本地存储的消息散列签名表 $(\mathbf{y},\boldsymbol{\sigma})$，如果已存在，则将 $\boldsymbol{\sigma}$ 作为签名值返回。

最后，在试图输出伪造的消息散列签名值对 $(\mathbf{y}',\boldsymbol{\sigma}')$ 之前，$\mathcal{A}$ 已经对 h_{A} 进行了询问，当 $\mathbf{A}$ 输出 $(\mathbf{y}',\boldsymbol{\sigma}')$ 时，$\mathcal{S}$ 查找本地存储中的 $(\mathbf{y}',\boldsymbol{\sigma}_{\mathbf{y}'})$ 并输出，从而能得到函数 f_{A} 的一对碰撞 $(\boldsymbol{\sigma}',\boldsymbol{\sigma}_{\mathbf{y}'})$。由定理 1 可知：SampleDom$(1^n)$ 具有输出均匀的性质，故 $\mathcal{S}$ 的输出和值域同为 $\mathbf{Z}_q^n$ 的变色龙哈希 h_{A} 的均匀随机输出是相同的。因此，当 $\mathcal{A}$ 以概率 ε 输出一个合法的伪造变色龙签名 $(\mathbf{y}',\boldsymbol{\sigma}')$ 时，可知 $f_{\mathbf{A}_2}(\boldsymbol{\sigma}')=\mathbf{y}'=f_{\mathbf{A}_2}(\boldsymbol{\sigma}_{\mathbf{y}'})$，并且 $\boldsymbol{\sigma}'\neq\boldsymbol{\sigma}_{\mathbf{y}'}$。这是因为 $\mathcal{A}$ 如果曾经对 $\mathbf{y}'$ 做过签名询问，$\mathcal{A}$ 再次询问时会直接得到签名值 $\boldsymbol{\sigma}_{\mathbf{y}'}$，又因为 $(\mathbf{y}',\boldsymbol{\sigma}')$ 是一个合法的伪造，所以 $\boldsymbol{\sigma}'\neq\boldsymbol{\sigma}_{\mathbf{y}'}$。如果 $\mathcal{A}$ 是第一次对 $\mathbf{y}'$ 做签名询问，则 $\mathcal{S}$ 调用 SampleDom(1^n) 生成 $\boldsymbol{\sigma}_{\mathbf{y}'}$，返回 $f_{\mathbf{A}_2}(\boldsymbol{\sigma}_{\mathbf{y}'})$ 给 $\mathcal{A}$。最终，在没有陷门的条件下，对给定的消息散列值 $\mathbf{y}'$，能够得到一个概率多项式时间算法 $\mathcal{S}$ 以不可忽略的概率 ε 找到原像采样陷门函数 f_{A} 的一对碰撞 $(\boldsymbol{\sigma}',\boldsymbol{\sigma}_{\mathbf{y}'})$，这与定理 3 中在没有陷门的条件下，基于平均情况 $\mathbf{SIS}_{q,m,2s\sqrt{m}}$ 是困难的假设，该原像采样陷门函数是抗碰撞的相矛盾。

因此，在没有签名者私钥的情况下，任何第三方能够伪造一个合法变色龙签名的概率是可忽略的。

结论 2　签名接收者利用变色龙哈希函数陷门能够很容易地伪造变色龙签名。

证明：对消息 $\mathbf{m}$ 的一个合法变色龙签名对 $(\mathbf{m},\mathbf{r},\boldsymbol{\sigma})$，签名接收者 Bob 能够很容易地伪造对另一个消息 $\mathbf{m}'$ 的变色龙签名对 $(\mathbf{m}',\mathbf{r}',\boldsymbol{\sigma})$。其具体过程如下：首先，计算原消息 $\mathbf{m}$ 的变色龙哈希值 $\mathbf{y}=h_{\mathrm{A}}(\mathbf{m};\mathbf{r})=\mathbf{A}_0\mathbf{m}+\mathbf{A}_1\mathbf{r}$。然后，利用陷门 $\mathbf{S}_1$，对计算得到的哈希值 $\mathbf{y}\in\mathbf{Z}_q^n$，新消息 $\mathbf{m}'\in M$，从离散高斯分布 $D\Lambda_{\mathbf{u}}^{\perp}(\mathbf{A}_1)$，$s$ 中采样得到 $\mathbf{r}'\in R$ 使得 $\mathbf{u}=\mathbf{A}_1\mathbf{r}'=\mathbf{y}-\mathbf{A}_0\mathbf{m}'$[5]。于是 $\mathbf{A}_0\mathbf{m}+\mathbf{A}_1\mathbf{r}=\mathbf{y}=\mathbf{A}_0\mathbf{m}'+\mathbf{A}_1\mathbf{r}'$，也就是说，Bob 很容易求得 $(\mathbf{m}',\mathbf{r}')\neq(\mathbf{m},\mathbf{r})$，但是其变色龙哈希值相同。所以，$(\mathbf{m},\mathbf{r})$ 的合法变色龙签名 $\boldsymbol{\sigma}$ 对于 $(\mathbf{m}',\mathbf{r}')$ 从原理上同样是合法的。因此，签名接收者利用变色龙哈希函数陷门能够很容易地伪造变色龙签名。

结论 3　上述变色龙签名具有不可传递性。

证明：由结论 2 可知：因为变色龙哈希函数的陷门 $\mathbf{S}_1$ 为签名接收者私有，所以签名接收者可以利用陷门求得另一消息 $\mathbf{m}'(\mathbf{m}'\neq\mathbf{m})$ 使得 $h_{\mathrm{A}}(\mathbf{m}')=h_{\mathrm{A}}(\mathbf{m})$。从而，签名接收者可以将对消息 $\mathbf{m}$ 的合法签名伪造成对新消息 $\mathbf{m}'$ 的签名，使其与原消息 $\mathbf{m}$ 的签名不可区分。因此签名接收者不可能把签名出示给第三方使第三方相信签名的真实性。

3.3 效率分析

本文提出的基于格的变色龙签名方案中，签名的私钥长度为 $2m\log q$，公钥长度为 $nm\log q$，签名的长度为 $m\log q$，验证计算复杂度为 $nm^2(\log q)^2$。该签名方案适应于对任意长度的消息进行签名。

结束语　随着量子计算机的发展，传统的变色龙签名方案被证明是不安全的，而格上难题 SIS 和 ISIS 还没有发现量子计算机破译算法，因此本文构造的变色龙签名方案是抗量子计算机攻击的。并且，该方案只利用到了小整数模加和模乘等简单的线性运算以及文献[4]中的高效采样算法，与基于传统数论难题的变色龙签名方案相比，具有计算简单、效率更高的特点。

由于变色龙签名不仅具有签名者不可否认性，还具有签名接收者不可传递性等特点。因此它在电子投票和电子拍卖中具有良好的应用前景。

参 考 文 献

[1] Krawczyk H, Rabin T. Chameleon signatures[C]// Proceeding of NDSS'00. 2000:143-154

[2] 马晓静，王尚平，等. 一种新的基于身份的变色龙数字签名方案[J]. 计算机工程，2006，32(18)：175-177

[3] 詹阳，田海博，等. 基于身份的无密钥托管的变色龙 hash 函数和签名[J]. 北京工业大学学报，2010，36(5)：685-688

[4] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions[C]// Proc 40th ACM Symp on Theory of Computing(STOC). New York, 2008: 197-206

[5] Cash D, Hofheinz D, Kiltz E, et al. Bonsai Trees, or How to delegate a Lattice Basis[C]// Advances in Cryptology EUROCRYPT 2010. Berlin: Springer Verlag, 2010: 523-552

[6] Ajtai M. Generating hard instances of lattice problems [C]// STOC. Philadelphia Pennysylvania. USA, 1996: 99-108

[7] Ajtai M, Dwork C. A public-key cryptosystem with Worst-case/average-case equivalence[C]// STOC. 1997: 284-293

[8] Regev O. On lattices, learning with errors, random linear codes, and Cryptography[J]. Journal of the ACM, 2009, 56(2): 1-40

[9] Micciancio D, Regev O. Worst-case to average-case reductions based on Gaussian measures[J]. SIAM Journal on Computing, 2007, 37(1): 267-302

[10] Ajtai M. Generating hard instances of the short basis problem [C]// ICALP 1999. Berlin: Springer Verlag, 1999: 1-9