

基于格的数字多签名体制

彭春燕, 杜秀娟, 李梅菊, 刘雪珂
(青海师范大学 计算机学院, 青海 西宁 810008)

摘 要: 传统的数字多签名体制大多基于大整数与离散对数困难问题, 这一多签名方案在量子计算机环境下已不再安全. 利用格理论上的小整数解问题(SIS)的困难性问题构造的数字多签名方案, 能够抵抗量子计算机攻击. 该数字多签名体制, 可以分为同时签名和顺序签名两种类型. 分别描述了格理论上的这两种数字多签名体制的密钥生成、签名步骤及签名验证过程, 证明了基于格的数字多签名的有效性及安全性.

关键词: 格; 多签名; 同时签名; 顺序签名

中图分类号: TP309

文献标识码: A

文章编号: 1000—7180(2016)08—0050—04

Digital Multi-signature Scheme Based on Lattice

PENG Chun-yan, DU Xiu-juan, LI Mei-ju, LIU Xue-ke

(Department of Computer, Qinghai Normal University, Xining 810008, China)

Abstract: The traditional digital multi-signature scheme mostly based on large integer factorization and the discrete logarithm problems, which has not been secure in quantum environment. The paper presents a new lattice-based multi-signature scheme that can resist the quantum attack using the hardness of average-case short integer solution problem (SIS). Multi-signature includes two types: simultaneous signature and sequential signature. The paper describes respectively the key generation, multi-signature generation and multi-signature verification of the two multi-signature schemes, and then has proved the digital multi-signature scheme based on lattice is especially efficient and secure to multi-signature generation.

Key words: lattice; multi-signature; simultaneous signature; sequential signature

1 引言

数字签名技术在安全领域中有着非常广泛的应用. 应用需求不同, 数字签名的方式也相应产生了许多变种. 多个用户在网络环境下的电子交易等活动中一起对相同的消息进行签名, 就是我们常说的数字多签名. 最早有关多签名的定义是由 Itakura 和 Nakamura^[1]在 1983 年提出, 并在其文中定义: 当 N 个用户共同对相同的消息一一进行签名将会获得一个签名, 此签名的长度是一个确定的常数, 那么这种签名方式称之为数字多签名. 这种数字签名方式如按照签名者的合作方式或者签名时机不同, 可以划

分为同时多签名及顺序多签名两种类型. 在验证该多签名时, 无论哪种方式都需要得到此 N 个用户的公钥进行验证, 并且要求验证的计算量不会随着用户数量的增长而有所增长. 近些年来密码学家也曾使用离散对数、大整数分解等相关数学理论构造了多种著名的数字多签名方案, Bellare 和 Nover^[2]两位学者曾在 CCS2006 会议上提出了一种工作在平凡公钥模型下的三轮交互的多人签名方案; Ji^[3]等人提出了基于 Schnorr 体制的新数字多签名体制, 并且证明了顺序签名类型的多签名体制的安全性. 然而, 这些签名方案大多是基于大整数分解和离散对数困难问题的, 随着量子计算机的不断发展, 这些

收稿日期: 2015—11—01; **修回日期:** 2015—12—12

基金项目: 国家自然科学基金资助项目(61162003); 国家社会科学基金项目(N15XMZ057); 青海科技厅项目(2015-ZJ-904, 2012-Z-902, 2015-ZJ-718)

能在多项式时间内解决的问题显然已经不能满足数字安全签名技术的需要. 因此, 如何设计一种基于公钥密码体制上的多签名方案且有能力抵抗量子计算机下的各种攻击, 是后量子时代的密码安全研究领域中的一个亟待解决的问题.

Ajtai^[4]在1996年就利用格理论问题的困难性, 提出了基于格上NP问题的密码构造方案, 这一机制的提出开辟了基于格的公钥密码体制的新方向. 其次, 由于格理论上的最短向量问题(Shortest Vector Problem, SVP)、最近向量问题(Closest Vector Problem, CVP)及各种衍生形式的基本问题, 从理论分析上都被证明都是NP困难问题, 并且到目前为止, 还没有发现可以使用量子计算机破译它们的算法, 因此研究基于格难题构造的密码体制, 并且使其能够抵抗量子计算机攻击的这一问题的研究逐渐成为后量子时代国内外众多专家学者的研究热点. 基于格难题的公钥密码作为后量子密码的典型加密机制, 也受到了很多专家学者的关注. Gentry, Peikert 和 Vaikuntanathan^[5]于2008年曾利用原像可抽样门限函数, 构造了第一个可验证安全性的基于格难题的签名机制, 以及基于身份的公钥加密方案, 这对于格理论在密码学的应用是一个具有里程碑意义的研究成果, 同时也使得基于格公钥密码体制的研究出现了一个前所未有的高峰期. 在2010年, Cash^[6]等人利用格基扩展的技术实现了“盆景树”模型下的数字签名方案, 该签名机制无需随机预言机技术的支持. 本文中首次将格理论用于多签名体制, 设计了两种新的基于格难题的多签名方案: 一个是同时签名类型. 另一个是顺序签名类型, 由于格被证明在量子环境下是安全的, 因而此方案具有更高的安全性和抗攻击能力. 与基于传统的多项式数论难题相比, 利用小整数模加和模乘等简单运算以及原像采样算法, 可以使得多签名体制减少签名生成的计算量, 同时具有计算简单、效率更高的特点.

2 相关的数学概念和原理

2.1 格

格是一种线性结构, 它是建立在偏序集合上的代数系统, 格上的运算大多是线性运算. 由于使用格理论研究的对象不同, 通常会采用不同的形式对它进行定义分析. 在计算机信息安全及工程领域中, 大多使用如下的方式定义格.

定义1 设 $v_1, \dots, v_n \in \mathbb{R}^m$ 为一组线性无关向量. 由 $v_1, \dots, v_n$ 生成的格 L 指的是向量 $v_1, \dots, v_n$ 的

线性组合所构成的向量集合, 且所使用的系数均在 $\mathbb{Z}$ 中, 即 $L = \{n_1 v_1 + n_2 v_2 + \dots + n_i v_i \mid n_1, n_2, \dots, n_i \in \mathbb{Z}\} = \left\{ \sum_{i=1}^d n_i v_i \mid n_i \in \mathbb{Z} \right\}$, 这样的集合 L 称为格. 任何一组可以生成格的线性无关的向量都称为格的基, 集合中向量个数称为格的维度, 记作 $\dim(L) = n$.

定义2 已知 $q, m, n \in \mathbb{Z}$, 矩阵 $A \in \mathbb{Z}_q^{n \times m}$, 且 $u \in \mathbb{Z}_q^n$, 则针对 q 模格有如下定义:

$$\Lambda_q(A^T) = \{x \in \mathbb{Z}^m : x = A^T s \bmod q, s \in \mathbb{Z}^n\},$$

$$\Lambda_q^\perp(A) = \{x \in \mathbb{Z}^m : Ax = 0 \bmod q\},$$

$$\Lambda_q^u(A) = \{x \in \mathbb{Z}^m : Ax = u \bmod q\}.$$

2.2 格上的难题

在格中寻找最短的非零向量问题, 即最短向量问题 SVP, 以及在格中寻找与指定非格向量最为接近的向量, 即最近向量问题 CVP, 都是格理论中最基本的困难问题.

定义3 在格 L 中寻找一个最短的非零向量 $v \in L$, 以使其欧几里得范数 $\|v\|$ 最小称为最短向量问题.

定义4 给定一个不在格 L 中的向量 $w \in \mathbb{R}^m$, 寻找一个向量 $v \in L$, 使它最接近 w , 即寻找一个向量 $v \in L$, 使得欧几里得范数 $\|w - v\|$ 最小称为最短向量问题.

可以使用格基约减的方法求出格的一组优质基, 以上两个格中基本困难问题通过一定的格基约减算法可转化为某些困难程度近似的问题, 常见的近似问题解决方法是小整数解问题 SIS, 其定义如下:

定义5 给定任意一个整数 q , 矩阵 $A \in \mathbb{Z}_q^{n \times m}$, 任意一个实数 β , 找到一个非零向量 $e \in \mathbb{Z}^m$, 满足 $Ae = 0 \bmod q$, 且 $\|e\| \leq \beta$. 其中, q, m, β 都可以表示由 n 的生成多项式, 并且 A 是随机均匀分布的.

由文献[7]可知, 由于 A 是随机均匀选取的, 在选择合适参数的情况下, 小整数问题 SIS 问题是一个NP困难问题, 理论的证明已由 Micciancio, Regev 两位学者在该文献中给出.

2.3 格上原像抽样函数

定理1^[4] 设 n 为一个安全参数, q 为任一素数, 令 $m \geq 2n \log q$, 对所有满足 $A \in \mathbb{Z}_q^{n \times m}$, $s \geq \omega \sqrt{\log m}$ 和 $e \leftarrow D_s^n$, s 则以极大的概率使得 $u = Ae \bmod q$ 在 $\mathbb{Z}_q^n$ 上的统计是均匀分布的.

该定理表明若输入的是格上利用离散高斯分布采样以后所得的点, 那么由随机均匀选取的这一矩

阵向量积在该矩阵所生产的向量空间上也应当是均匀分布的。

定理 2 ^[5,9] 设 n 为算法的一个参数,对任意一个素数 $q = \text{poly}(n)$,整数 $m \geq 5n \log q$,存在一个概率多项式时间算法 $\text{TrapGen}(1^n)$,以 1^n 为输入值,则可以输出一个统计,且该统计是接近均匀分布的矩阵 $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ 以及相应 $\Lambda^\perp(\mathbf{A})$ 上的一组满秩向量集合 $\mathbf{T}$,满足: $\|\mathbf{T}\| \leq L \approx m^{1+\epsilon}, \epsilon > 0$.

在文献[5]中,作者给出了原像采样门陷函数的构造过程,对于门限函数的构造描述如下:

(1) 根据定理 2 可以得到矩阵 $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ 及向量集合 $\mathbf{T}, \mathbf{A}$ 作为公钥, $\mathbf{T}$ 作为私钥,同时作为下文 $f_A(\cdot)$ 函数中的门陷;

(2) 先定义一个单向门陷函数: $f_A(x) = \mathbf{A}x \pmod{q}$, 其中: $x \in D_n = \{x \in \mathbb{Z}_q^m, \|x\| \leq \sqrt{m}\}$, 且向量 x 满足 D_n^m, s 分布的条件。

(3) 再给定一个向量 $\mathbf{u} \in \mathbb{Z}_q^m$, 采用线性代数的方法选择向量 $\mathbf{t} \in \mathbb{Z}_q^m$, 满足 $\mathbf{A}\mathbf{t} = \mathbf{u} \pmod{q}$, 然后利用门陷 $\mathbf{T}$, 中心 $\mathbf{t}$, 偏移量 s , 输出一个统计在格 $\Lambda^\perp(\mathbf{A})$ 上的离散高斯分布的格向量 $\mathbf{v}$, 可以求出原像值 $\sigma = \mathbf{t} + \mathbf{v}$, 进而使得 $\mathbf{A}\sigma = \mathbf{u} \pmod{q}$ 。

在上述的原像采样函数中,其陷门基 $\mathbf{T}$ 的范数直接决定了输出向量 σ 的范数,只有得知陷门基 $\mathbf{T}$ 也就是陷门基 $\mathbf{T}$ 的拥有者才能得到向量 $\mathbf{u} \in \mathbb{Z}_q^m$ 在 $f_A(x) = \mathbf{A}x \pmod{q}$ 的一个满足 $\sigma \in D_n$ 的原像。本文中利用这一原理构造出同时多签名体制和顺序多签名体制。

3 同时多签名体制

同时多签名有时也被称为广播多重数字签名体制,它是指消息的发送者同时将这一消息发送给每一位签名者进行签名,然后由共同选取的签名收集者收集签名消息,由收集者对签名消息进行归并整理并发送给签名验证者,最后由签名验证者再验证这一签名消息有效与否。设 N 个签名者分别是 $U_1, U_2, \dots, U_N$, 一起对相同的消息 m 进行同时签名。

3.1 密钥生成

输入一个安全参数 n, q, m, s 均为 n 的函数, c 为常数, 设 $q = \text{poly}(n), m \geq cn \log q$, 参数 $s \geq m^{1+\epsilon} \cdot \omega(\log m)^{1/2}$. 设有 $U_i (1 \leq i \leq N)$ 个用户, 使用 $\text{TrapGen}(1^n)$ 生成 N 个随机均匀矩阵 $\mathbf{A}_i \in \mathbb{Z}_q^{n \times m} (1 \leq i \leq N)$ 及格 $\Lambda_q^\perp(\mathbf{A}_i)$ 上的一组陷门基 $\mathbf{S}_i \in \mathbb{Z}_q^{n \times m}$. 利用矩阵 $\mathbf{A}_i$ 短基抽样算法生成另一个矩阵 $\mathbf{B}_i \in \mathbb{Z}_q^{n \times m} (1 \leq i \leq N)$ 及其格 $\Lambda_q^\perp(\mathbf{B}_i)$ 上的一组短基 $\mathbf{T}_i$

$\in \mathbb{Z}_q^{n \times m}$, 满足 $\mathbf{B}_i \mathbf{A}_i^\perp = 0, (\mathbf{A}_i, \mathbf{B}_i)_{i=1}^N$ 作为签名者的公开密钥, $\mathbf{T}_i$ 作为签名者 $U_i (1 \leq i \leq N)$ 的私钥。

3.2 同时多签名

假设 $U_i (1 \leq i \leq N)$ 个签名者同时对一个消息 m 进行签名, 执行如下步骤:

(1) 用户 $U_i (1 \leq i \leq N)$ 随机选择一个向量 $\mathbf{r} \leftarrow \{0, 1\}^n$, 利用随机预言机 $H_1: \{0, 1\}^* \rightarrow \mathbb{Z}_q^{n \times k}$, 计算: $h_i = H_1(m; \mathbf{r}) \in \mathbb{Z}_q^{n \times k}$;

(2) 随机均匀选择向量 $\mathbf{t}_i \in \mathbb{Z}_q^m$, 同时满足 $\mathbf{B}_i \mathbf{t}_i = h_i \pmod{q}$;

(3) 对于每个 $U_i (1 \leq i \leq N)$ 以 $-\mathbf{t}_i$ 为中心, 在参数 s 下利用原像抽样算法抽取向量 $\mathbf{v}_i \leftarrow D_{\Lambda^\perp, s, -\mathbf{t}_i}$, 可以求出 $\sigma_i = \mathbf{t}_i + \mathbf{v}_i$. 检查是否满足 $\|\sigma_i\| \leq s\sqrt{m}$, 若不足, 重新抽取向量 $\mathbf{v}_i$, 使得 $\mathbf{B}_i \sigma_i = h_i \pmod{q}$ 成立;

(4) 计算 $\mathbf{z}_i = \mathbf{A}_i^\perp \sigma_i + \sigma_i \pmod{q}$, 再构造一个 NIWI 证明 $\pi^{[8]}$, 输出签名 $e = (\mathbf{r}, \mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_N, \pi)$;

最后由收集者将得到的结果 e 发送给验证者, e 即是 $U_1, U_2, \dots, U_N$ 的同时多签名后所生成的消息。

3.3 多签名验证

当验证者接收到多签名结果 $e = (\mathbf{r}, \mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_N, \pi)$ 之后, 先验证 π 是否正确, 如果 π 是正确的, 且 N 作为公钥的个数恰好与签名消息 e 中 $\mathbf{z}_i$ 的个数恰好相等, 同时对于每个用户 $U_i (1 \leq i \leq N)$, 都能够满足等式 $\mathbf{A}_i \mathbf{z}_i = h_i \pmod{q}$, 则验证成功输出 1, 否则验证失败输出 0。

4 顺序多签名体制

在顺序的多数字签名体制中, 先由消息发送者共同协商出消息签名顺序。其次, 按照顺序将消息发送给首个签名参与者, 当此签名者签名后, 按预先的顺序发送给第二个签名者, 以此类推, 直到最后一个签名者完成签名并交付给验证者。在顺序签名过程中, 除了第一个签名者外, 其余每一位签名者在收到签名消息后, 先来验证上一签名的有效性, 如果签名有效, 继续签名, 然后将签名消息发送给下一个签名者; 如果签名无效, 拒绝再对消息签名, 自行终止整个签名, 当签名验证者收到签名消息后, 验证签名有效与否, 如果验证有效, 该多签名消息是有效的; 否则, 该多签名消息无效。与同时多签名机制相似, 我们设 N 个签名者 $U_1, U_2, \dots, U_N$ 对相同的一个消息 m 进行顺序签名。因为密钥生成过程和同时多签名体制是相同的, 直接讨论顺序多签名的详细过程。

4.1 顺序多签名

假设 $U_i (1 \leq i \leq N)$ 个签名者按预先的约定好

的顺序对一个消息 m 进行签名,则执行以下步骤。

第一位签名者 U_1 的签名过程:

(1) 随机选择一个向量 $\mathbf{r} \leftarrow \{0,1\}^n$, 利用随机预言机 $H_1: \{0,1\}^* \rightarrow \mathbb{Z}_q^{n \times k}$, 计算: $h_1 = H_1(m; \mathbf{r}) \in \mathbb{Z}_q^{n \times k}$;

(2) 随机均匀选择向量 $\mathbf{t}_1 \in \mathbb{Z}_q^m$, 同时满足 $B_1 \mathbf{t}_1 = h_1 \pmod{q}$;

(3) 以 $-\mathbf{t}_1$ 为中心, 在参数 s 下利用原像抽样算法抽取向量 $\mathbf{v}_1 \leftarrow D_{\Lambda^\perp, s, -\mathbf{t}_1}$, 可以求出 $\sigma_1 = \mathbf{t}_1 + \mathbf{v}_1$. 检查是否满足不等式 $\|\sigma_1\| \leq s\sqrt{m}$, 使得等式 $B_1 \sigma_1 = h_1 \pmod{q}$ 成立;

(4) 计算 $z_1 = A_1^\perp s_1 + \sigma_1 \pmod{q}$, U_1 把 $\mathbf{r}, z_1, \sigma_1$ 作为签名结果传给第二位签名者 U_2 .

第 i 位签名者 $U_i (i > 1)$ 的签名过程:

(1) 先由 U_i 计算验证上一个签名者 U_{i-1} 的 $B_i z_i = h_i \pmod{q} (i \geq 1)$ 是否成立, 若不成立, 终止签名; 若等式成立则继续执行以下步骤;

(2) 随机选择一个向量 $\mathbf{r} \leftarrow \{0,1\}^n$, 利用随机预言机 $H_1: \{0,1\}^* \rightarrow \mathbb{Z}_q^{n \times k}$, 计算: $h_i = H_1(m; \mathbf{r}) \in \mathbb{Z}_q^{n \times k}$;

(3) 随机均匀选择向量 $\mathbf{t}_i \in \mathbb{Z}_q^m$, 同时满足 $B_i \mathbf{t}_i = h_i \pmod{q}$;

(4) 以 $-\mathbf{t}_i$ 为中心, 在参数 s 下利用原像抽样算法抽取向量 $\mathbf{v}_i \leftarrow D_{\Lambda^\perp, s, -\mathbf{t}_i}$, 可以求出 $\sigma_i = \mathbf{t}_i + \mathbf{v}_i$. 检查是否满足 $\|\sigma_i\| \leq s\sqrt{m}$, 使得 $B_i \sigma_i = h_i \pmod{q}$ 成立;

(5) 计算 $z_i = A_i^\perp s_i + \sigma_i \pmod{q}$, 把 $\mathbf{r}, z_1, \dots, z_i, \sigma_1, \dots, \sigma_i$ 作为签名结果传给下一位签名者, 如果是 $U_i (i = N)$, 再构造一个 NIWI 证明 π , 则把 $(\mathbf{r}, z_1, \dots, z_N, \sigma_1, \dots, \sigma_N, \pi)$ 传送给验证者。

4.2 多签名验证

当验证者接收到多签名 $(\mathbf{r}, z_1, z_2, \dots, z_N, \sigma_1, \sigma_2, \dots, \sigma_N, \pi)$ 之后, 验证公钥的个数 N 与签名 e 中 z_i 的个数是否相符, 同时对于每个 $U_i (1 \leq i \leq N)$, 都有 $B_i z_i = h_i \pmod{q}$ 成立, 则输出 1, 表示签名有效, 否则输出 0, 表示该签名无效。

5 安全性分析

5.1 正确性

如果签名者 $U_i (1 \leq i \leq N)$ 及验证者遵守签名规则, 则验证者将总认为上述产生的多签名是正确的。设 $(\mathbf{r}, z_1, z_2, \dots, z_N, \sigma_1, \sigma_2, \dots, \sigma_N, \pi)$ 是一个合法的群成员的签名, 那么 π 是一个正确的证明, 其次,

对于任意的 $1 \leq i \leq N$, 都有:

$$B_i z_i = B_i (A_i^\perp s_i + \sigma_i) = B_i \sigma_i = h_i \pmod{q}.$$

验证成功, 因此可证明该签名方案是有效的。

5.2 安全性

该多签名机制是在格理论的基础上提出的, 能够成功抵制量子计算机下的安全主动攻击。理论分析表明该方案在对抗被动攻击下也是安全的, 其安全性主要取决于两个因素: 一是从所有消息签名者的公开密钥 $(A_i, B_i)_{i=1}^N$ 和多签名获取私钥 NP 问题的困难性; 二是敌手伪造部分多签名使得全体多签名满足验证等式的困难性。在任何情况下, 任何敌手要获取部分或全部签名者的私钥是不可行的, 当计算 $z_i = A_i^\perp s_i + \sigma_i \pmod{q}$ 时, 要想通过 z_i 求解 σ_i 就会面临求解格上的 SIS 困难问题, 这是做不到的。另外, 多签名的密钥是由各个成员的签名密钥共同生成的, 其他成员若想伪造最终签名消息的前提条件须要得知签名密钥。这与 G. KeyGen 中提出的零知识证明^[7] 是相违背的, 也就意味着必须要解决最近向量这一困难问题, 这显然在计算上是不可行的。

6 结束语

本文首次基于格理论的知识构造了两种不同类型的数字多签名方案, 并且这两种多签名方案是能够抗量子攻击的。与以往的传统多签名体制相比, 基于格的多签名体制在多签名生成速度上有了一些改进, 同时, 也讨论了多签名体制的有效性和安全性。后续的工作可以在优化签名长度, 存储、计算开销上再做一些优化。

参考文献:

- [1] K Itakura, K Nakamura. A public-key cryptosystem suitable for digital multisignatures[J]. NEC research and development, 1983, 71(1): 1-8.
- [2] M Bellare, G Neven. Multi-signatures in the plain public-key model and a general forking lemma[C] // 13th ACM conference on Computer and communications security (CCS ' 06). Alexandria, USA: IEEE, 2006.
- [3] 纪家慧, 赵仁杰. 新的数字多签名体制[J]. 计算机学报, 1997, 20(6): 533-538.
- [4] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for Hard Lattices and New Cryptographic Constructions [C] // Proc of STOC ' 2008. Victoria: ACM, 2008: 197-206.

- [3] Abdoa A, Awad H, Paredes S, et al. OC-48 configurable IP traffic generator with DWDM capability [C] // Proc Canadian Conference on Electrical and Computer Engineering. Ottawa, Canada: IEEE, 2006: 1842-1845.
- [4] Covington G A, Gibb G, Lockwood J W, et al. A packet generator on the NetFPGA platform [C] // Proc IEEE Field-Programmable Custom Computing Machines. Napa, California: IEEE, 2009: 235-238.
- [5] Leland W, Taqqu M, Willinger W, et al. On the self-similar nature of ethernet traffic (extended version) [J]. IEEE/ACM Transactions on Networking, 1994, 2(1): 1-15.
- [6] Willinger W, Taqqu M, Sherman R, et al. Self-similarity through high-variability: statistical analysis of ethernet LAN traffic at the source level [J]. IEEE ACM Transactions on Networking, 1997, 5(1): 71-86.
- [7] Crovella M E, Bestavros A. Self-similarity in World Wide Web traffic: evidence and possible causes [J]. IEEE/ACM Transactions on Networking, 1997, 5(6): 835-846.
- [8] Jeong H D. Modelling of self-similar teletraffic for simulation [D]. Christchurch: University of Canterbury, 2002.

作者简介:

王晓婷 女, (1987-), 博士研究生. 研究方向为高性能交换机结构与算法设计、SOC 实现.

E-mail: wangxiaoting12409@163.com.

王忆文 男, (1966-), 博士, 教授. 研究方向为高性能交换机技术、可重构 SOC 架构、指纹识别.

李平 男, (1957-), 教授, 博士生导师. 研究方向为 FPGA 设计与测试、SOC 设计与验证.

(上接第 53 页)

- [5] Cash D, Hofheinz D, Kiltz E, et al. Bonsai trees, or how to delegate a lattice basis [C] // Proc of Eurocrypt 2010 LNCS6110. Berlin: Springer, 2010: 523-552.
- [6] Micciancio D, Regev O. Worst-case to average-case reductions based on gaussian measures [J]. SIAM Journal on Computing, 2007, 37(1): 267-302.
- [7] Micciancio D, Vadhan S P. Statistical zero-knowledge proofs with efficient provers: Lattice Problems and more [C] // Proceedings of the Advances in Cryptology-CryPTP'03. Berlin: Springer-Verlag, 2003: 282-298.
- [8] Ajtai M. Generating hard instances of the short basis problem [C]. ICALP 1999. Berlin: Springer Verlag, 1999: 1-9.
- [9] 谢璇, 喻建平, 王廷, 等. 基于格的变色龙签名方案 [J]. 计算机科学, 2013, 40(2): 117-119.

作者简介:

彭春燕 女, (1980-), 博士研究生, 副教授. 研究方向为无线网络与安全研究. E-mail: 7456911@qq.com.

杜秀娟 女, (1970-), 教授, 博士生导师. 研究方向为水下通信协议、无线网络安全.