一种基于格的认证加密方案*

张祥火[a]，杨晓元[a,b]，王绪安[a]

（武警工程大学 a. 电子技术系 网络与信息安全武警部队重点实验室；b. 信息安全研究所，西安 710086）

摘　要：基于格上困难问题的密码体制成为当前研究的热点。基于 R-LWE（ring-learning with errors）困难问题和广义压缩背包问题的哈希函数，构造了一种基于格的认证加密方案。方案在加密过程中利用了 R-LWE 困难问题，其加解密速度快、密文扩展率低等特性；认证过程使用的是广义压缩背包问题，其效率高，安全性能够达到 IND-CPA（indistinguishability under chosen plaintext attack）。

关键词：格；R-LWE；认证加密

中图分类号：TP391　　**文献标志码**：A　　**文章编号**：1001-3695(2013)09-2788-03

doi:10.3969/j.issn.1001-3695.2013.09.057

Authentication encryption scheme based on lattice

ZHANG Xiang-huo[a], YANG Xiao-yuan[a,b], WANG Xu-an[a]

(*a. Key Laboratory of Network & Information Security under the Chinese Armed Police Force, Dept. of Electronic, b. Institute of Information Security, Engineering College of Chinese Armed Police Force, Xi'an* 710086, *China*)

Abstract: Based on the R-LWE difficult problem and generalized compression knapsack problem hash function, this paper constructed a lattice-based authenticated encryption scheme. The new scheme made use of R-LWE difficult problem in the encryption and decryption, and had the good characteristic that the encryption and decryption speed was quick, the expansion ratio of the ciphertext was low. The authentication process was realized by using generalized compression knapsack problem, the efficiency, of which was very high, and its security could achieve IND-CPA.

Key words: lattice; R-LWE; authentication encryption

0　引言

计算机与网络技术的迅猛发展和普及给现代人的生活提供了越来越多的便利，但同时也出现了一个非常现实的问题，那就是如何来保证人们的信息安全（包括保密性、完整性与真实性等）。尤其是量子计算的深入研究，导致了现行的包括基于离散对数和大整数分数的许多密码体制的安全性都受到了威胁，国内外也因此掀起了研究抗量子计算密码的高潮。而基于格上困难问题设计的加密方案，作为后量子时代的典型代表，能够很好地解决保密性问题。但是在一些现实应用中，不但要保证通信的安全保密性，还要达到通信消息的不可否认性等，这就需要引入认证算法。安全高效的认证加密算法能够很好地满足现实需求，认证加密就是通过加密算法和认证算法共同完成消息的保密性和真实性。文献[1]提出了一个认证加密方案，该方案执行时，计算量较少，通信上占用带宽较少，所以效率较高。文献[2]基于 RSA 公钥密码体制和 Diffie-Hellman 密钥交换协议设计了一个认证加密方案。文献[3]根据 RSA 加密系统和中国剩余定理，提出了一种新的基于多密钥的 RSA 认证加密方案，该方案与通常的 RSA 加密系统不同，每个用户只有一个加密密钥，但解密密钥由两个以上的短密钥组成，大大地加快了解密的速度。黄益栓等人[4]将传统的对称加密方法与基于身份的公钥加密系统相结合，设计了一种基于身份的认证加密方案，该方案是椭圆曲线上的双线性映射构造的。文献[5]针对文献[4]中接收者可以假冒其他的用户发送消息给自己这一缺陷，提出了基于 Diffie-Hellman 问题的一种改进的认证加密方案。上述方案主要都是基于 RSA、ECC 等问题设计的，其安全性随着量子计算的深入研究而受到威胁，效率也有待改善。因此，本文基于以上问题和应用需求提出了一种基于格的认证加密方案。

1　预备知识

格（lattice）是一类定义在有限域上的、离散的几何结构，是线性空间中 n 维向量构成的一个子集。其定义如下：

定义 1[6]　设向量 $b_1, b_2, \cdots, b_m \in \mathrm{R}^n$ 线性无关，$b_1, b_2, \cdots, b_m$ 的所有整数线性组合构成 m 维的格 $L(b_1, b_2, \cdots, b_m)$，记为

$$L(b_1, b_2, \cdots, b_m) = \{ v \in R^n \mid v = \sum_{i=1}^{m} t_i b_i, t_i \in Z \}$$

称 $[b_1, b_2, \cdots, b_m]$ 是格 L 的一组基，并记 $\mathrm{Dim}(L) = m$ 为格的维数，n 称为格的阶。如果 $m = n$，则称格 L 是满维的（full dimension）或满秩的（full rank）。格的基也可以用矩阵的形式表示，设 $B = [b_1, b_2, \cdots, b_m]$，那么以 B 为基生成的格记做 $L(B) = \{ Bt \mid t \in Z^m \}$，这里的 Bt 表示普通的矩阵与向量乘法。

1.1　LWE 问题的困难性及其扩展

1）LWE 问题的定义

收稿日期：2012-12-04；**修回日期**：2013-02-01　　**基金项目**：国家自然科学基金资助项目（61272492，61103231，61103230）

作者简介：张祥火（1988-），男，硕士研究生，主要研究方向为信息安全、密码学（781984554@qq.com）；杨晓元（1959-），男，教授，硕士，主要研究方向为信息安全、密码学；王绪安（1981-），男，讲师，硕士，主要研究方向为信息安全、密码学.

定义 2[7]　公开选取一个安全参数 $n>1$,一个模数 $q\geqslant 2$,实数 $\alpha>0$ 和定义在 Z_q 上的错误(噪声)概率分布 $\bar{\Psi}_{\alpha q}=\{\lceil qx\rfloor \bmod q \mid x\sim N(0,\alpha^2)\}$,秘密选取均匀分布的向量 $\boldsymbol{s}\in Z_q^n$。设 $\chi_a=\bar{\Psi}_{\alpha q}$,保持向量 $\boldsymbol{s}$ 不变,多次随机选取均匀分布的向量 $\boldsymbol{a}\in Z_q^n$,选取 $e\in\chi_\alpha$,输出 $(\boldsymbol{a},b=\langle \boldsymbol{a},\boldsymbol{s}\rangle+e)\in Z_q^n\times Z_q$,并将其分布记做 A_{s,χ_a}(也称 LWE 分布),加运算是在 Z_q 上操作的(模 q)。如果存在一个算法,对于任何的 $\boldsymbol{s}\in Z_q^n$,能够利用给定的任意 m 个独立取自 A_{s,χ_a} 的采样,以很大的概率输出 $\boldsymbol{s}\in Z_q^n$,就说该算法能够解决模数为 q、错误分布为 χ_a 的计算性 LWE 问题。

LWE 问题可以看做随机线性码的解码问题,或者格上的有限距离解码问题(bounded distance decoding problem,BDD)。特别地,当 $q=2$ 时 LWE 问题就转换为 LPN(learning parity with noise)问题。

2)LWE 问题的困难性

如果没有附加错误的干扰,求解上述问题是非常容易的,对得到的 m 个等式使用高斯消元法(Gaussian elimination)就可以在多项式时间内求出 $\boldsymbol{s}$。但引入错误后使得这个问题变得异常困难,如果使用高斯消元,m 个等式在进行线性组合之后,会将错误放大到一个无法控制的级别,从而使得到的等式不含任何信息。目前解决 LWE 问题的主要算法及效率分析如表 1 所示。

表 1　目前解决 LWE 问题的主要算法及效率分析

算法	需要的采样数 m	时间复杂度
最大似然算法	$O(n)$	$q^n=2^{O(n\log n)}$
单'1'算法	$2^{O(n\log n)}$	$2^{O(n\log n)}$
BKW'03 算法[8]	$2^{O(n)}$	$2^{O(n)}$
AroraGe'10 算法[9]	$2^{O((\alpha q)^2)}$	$2^{O((\alpha q)^2)}$

目前研究表明 LWE 问题是困难的,原因如下:

a)已知求解 LWE 问题的算法都运行在指数时间内,即使量子算法也难以奏效。

b)LWE 问题是 LPN 问题的一个自然扩展,LPN 问题在学习论中已被认为是困难的。另外,LPN 问题可以形式化为随机线性二进制码的解码问题,因此,任何成功解决 LPN 问题的算法都会导致编码理论的重大突破。

c)最重要的是,LWE 问题的困难性可以归约到标准格上困难性问题(如 gap-SVP 和 SIVP)的最困难情况[7]。更为准确地讲,若 $q=2^n$,那么 LWE 的困难性等价于近似因子为 $f(n)$ 的 gap-SVP 问题;若 $q=\mathrm{poly}(n)$,LWE 的困难性满足这样的假设:在以一个短基作为帮助的情况下 gap-SVP 仍然是困难的,或者即使给出一个量子计算机作为辅助,解决近似因子为多项式的 gap-SVP 和 SIVP 仍然是困难的。

定理 1[10]　设 n,q 是整数,$\alpha\in(0,1)$ 且 $\alpha q>2\sqrt{n}$,如果存在一个有效的算法能够解决 $\mathrm{LWE}_{q,\chi}$ 问题,那么也存在一个有效的量子算法能够在近似因子 $\tilde{O}(n/\alpha)$ 内解决格上 gap-SVP 和 SIVP 的判定性问题。

实际上,从某种程度上讲,SIVP 要比 gap-SVP 困难。获得的解决格上最困难实例的近似因子典型形式为 $\tilde{O}(n/\alpha)$,因此在 LWE 困难假设中,必须要求 $\alpha\geqslant 1/\mathrm{poly}(n)$。

3)R-LWE 问题

定义 3[11]　R-LWE 问题。设 $f(x)=x^n+1\in Z[x]$,安全参数 $n=2^k(k\in Z)$(保证 $f(x)$ 不可逆),离散错误分布 $\chi=\bar{\Psi}_{aq}$。设秘密环多项式 $\boldsymbol{s}\in R_q$ 均匀分布,随机均匀选取 $\boldsymbol{a}\in R_q$ 和噪声 $e\in R$(e 的系数服从 χ 分布),计算 $(\boldsymbol{a},b=\boldsymbol{a}\boldsymbol{s}+e)\in R_q\times R_q$,并将其分布记为 $A_{s,\bar{\Psi}_{\alpha q}}$(也称 R-LWE 分布)。计算性 R-LWE 问题就是通过 m 个取自 $A_{s,\bar{\Psi}_{\alpha q}}$ 的样本以很大概率正确解出 $\boldsymbol{s}\in R_q$。判定性 R-LWE 问题描述如下:存在一个攻击者 A 和一个 R-LWE 预言机 O,O 包含两个采样算法 $O_\$$(随机选取 $(\boldsymbol{a},b)\in \cup(R_q\times R_q)$)和 O_s(设定秘密 $\boldsymbol{s}\in R_q$ 和选择均匀分布的 $\boldsymbol{a}\in R_q$,计算 $(\boldsymbol{a},b=\boldsymbol{a}\boldsymbol{s}+e)\in A_{s,\bar{\Psi}_{\alpha q}}$,其中 e 的系数服从 χ 分布);攻击者 A 向预言机 O 询问,O 随机利用 $O_\$$ 或者 O_s 产生 m 个实例 $(\boldsymbol{a},b)\in R_q\times R_q$ 返回给攻击者 A。如果 A 能够准确分辨出实例取自 $O_\$$ 或 O_s 的优势

$$\mathrm{adv}(A)=\left|\Pr[A^{O_\$}=1]-\Pr[A^{O_s}=1]\right|$$

是不可忽略的,那么就说 A 能够解决判定性 R-LWE 问题。

定理 2[11]　对于一个多项式(甚至量子)时间的攻击者,如果不存在一个多项式时间内的量子算法来解决理想格中近似 SVP 问题(近似因子为 $\tilde{O}(n)$)的最难实例,那么取自 R-LWE 分布的 $\tilde{O}(n)$ 个采样是伪随机的。

在定理 2 归约过程中,当参数 q 为素数且 $f(x)=x^n+1\in Z[x]$ 能够在 Z_q 上分解为 n 个不同线性因子时,判定性 R-LWE 是困难的。

1.2　广义压缩背包问题及哈希函数

广义压缩背包问题(generalized compact knapsack problem)[12]。给定环 $R=Z[x]/f(x)$ 和它的一个子集 D(其中元素系数较小),$m\in Z$,已知环多项式向量 $\hat{\boldsymbol{a}}=(\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_m)^{\mathrm{T}}\in R^m$ 和一个目标多项式 $t\in R$,求解环多项式向量 $\hat{\boldsymbol{z}}=(z_1,z_2,\cdots,z_m)^{\mathrm{T}}\in D^m$,使得 $\hat{\boldsymbol{a}}\otimes\hat{\boldsymbol{z}}=t$。适当地选择 R 和 D,即使 m 为常数,解决广义背包问题的一般实例等价于求解理想格中一个 SIS 困难问题的最难实例。因此,容易构造出一个安全性建立在格上困难假设的单向函数。

基于广义压缩背包问题的哈希函数 H[13]。给定一个环 $R_q=Z_q[x]/f(x)$ 和其子集 D,其中 $f\in Z[x]$ 是一个次数为 n 的首一、不可约多项式,$p\geqslant n^2\in Z$,m 是一个常数,随机均匀产生 $\hat{\boldsymbol{a}}=(\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_m)^{\mathrm{T}}\in R_q^m$,定义有序的 m 元组 $\hat{\boldsymbol{a}}=(\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_m)^{\mathrm{T}}$ 为哈希函数 H。对于消息 $\hat{\boldsymbol{z}}=(z_1,z_2,\cdots,z_m)^{\mathrm{T}}\in D^m$,其哈希值为 $H(\hat{\boldsymbol{z}})=\hat{\boldsymbol{a}}\otimes\hat{\boldsymbol{z}}\in R_q$,显然哈希函数 H 是从 D^m 到 R_q 上的一个映射。

定理 3[13]　对于参数满足要求的上述哈希函数 H,若存在一个多项式时间内的算法可找到不同的 $\hat{\boldsymbol{b}}$ 和 $\hat{\boldsymbol{b}}'$,使得 $H(\hat{\boldsymbol{b}})=H(\hat{\boldsymbol{b}}')$,即找到 H 的一个碰撞,那么存在一个多项式算法解决环上的最短多项式问题 SPP(shortest polynomial problem)。

已经证明,环上 SPP 的复杂性与格中 SVP 问题相当。

2　方案描述

1)参数说明　设 $m=O(\log q)$,$f(x)=x^n+1\in Z[x]$,$q>2n^2$,$R_q=Z_q[x]/\langle f(x)\rangle$,$r\in Z$。

2)密钥生成算法 Gen　随机选取环多项式向量 $\hat{\boldsymbol{s}}=(\boldsymbol{s}_1,\boldsymbol{s}_2,\cdots,\boldsymbol{s}_m)^{\mathrm{T}}\in R^m$,其系数均匀取自 $\{-r,-r+1,\cdots,r\}$,$\hat{\boldsymbol{s}}$ 为私钥,随机选取均匀分布的 $\hat{\boldsymbol{a}}\in R_q^m$,公钥为 $(\hat{\boldsymbol{a}},p=\hat{\boldsymbol{a}}\otimes\hat{\boldsymbol{s}})\in R_q^m\times R_q$,$H$ 为广义压缩背包问题的哈希函数。

3)加密算法 Enc　Alice 随机选取均匀分布的多项式 $x\in R_q$,选择噪声分布 $e_0\in R$ 和 $\hat{\boldsymbol{e}}_0=(e_1,e_2,\cdots,e_m)^{\mathrm{T}}$,$\hat{\boldsymbol{e}}_0\in R^m$,$e_0$,

$e_1,\cdots,e_m$ 的系数服从 χ 分布。将加密消息编码为环多项式 $m \in R_2$,进行如下计算:

$$(u=\hat{a}x+\hat{e}_0)\in R_q^m,(c=px+e_0+m\lfloor q/2\rfloor)\in R_q$$

令 $T=m\times u$,再将 T 映射到 D^m 上的某个元素 V,$C=H(V)$。其中三元组(u,c,C)为密文,并发送给 Bob。

4)解密算法 Bob 对(u,c,C)进行如下计算:由于$(u,c)\in R_q^m\times R_q$,计算 $m=c-\hat{u}\otimes\hat{s}\in R$。如果这个多项式的每个系数到 0 的距离比到$\lfloor q/2\rfloor$的距离近,那么相应为 0,否则为 1。由此恢复出明文消息。

5)认证算法 VEK 计算 $T'=m'\times u=m\times u$,再将 T 映射到 D^m 上的某个元素 V,检验是否有 $C=H(V)$ 成立,若成立则说明消息来自 Alice。

3 方案分析

3.1 正确性分析

a)设 $q>2n^2$,$\alpha\leqslant 1/(rt\sqrt{m})$,$t\geqslant 20$,利用上述方案产生密钥加密消息 m,那么解密算法以趋近于 1 的概率正确恢复出明文。

证明 计算

$$m'=c-\hat{u}\otimes\hat{s}=px+e_0+m\lfloor q/2\rfloor-\hat{u}\otimes\hat{s}=$$
$$(\hat{a}\otimes\hat{s})x+e_0+m\lfloor q/2\rfloor-x\hat{a}\otimes\hat{s}-\hat{e}_0\otimes\hat{s}=$$
$$e_0-\hat{e}_0\otimes\hat{s}+m\lfloor q/2\rfloor=e_0-\sum_{i=1}^{m}e_i s_i+m\lfloor q/2\rfloor$$

密文要正确解密,必须要求环多项式 $e_0-\sum_{i=1}^{m}e_i s_i$ 的每一个系数的绝对值不超过$\lfloor q/4\rfloor$。环多项式 $\hat{s}$ 的系数在$\{-r,-r+1,\cdots,r\}$上均匀分布。设噪声 $e_0,e_1,\cdots,e_m$ 的分布取自 $E_i=\lceil qX_i\rfloor \bmod q$ $(0\leqslant i\leqslant m)$,其中 $X_i\sim N(0,\alpha^2)$,下面用 $q\sum_{i=1}^{m}s_iX_i$ 代替 $\hat{e}_0\otimes\hat{s}$ 来进行讨论。

概率论中,如果存在 n 个互不相关的正态分布样本 $X_i\sim N(\mu,\sigma^2)(1\leqslant i\leqslant n)$,那么样本之和$\sum_{i=1}^{n}X_i\sim N(n\mu,n\sigma^2)$。同样,本文中 X_i 之间互不相关,故 s_iX_i 的每个系数服从均值为 0、标准差为 $\|s_i\|\times\alpha\leqslant r\times\alpha$ 正态分布。类似地,$\sum_{k=1}^{m}s_kX_k$服从均值为 0、标准差小于等于$\sqrt{\sum_{k=1}^{m}(r\alpha)^2}=\sqrt{m}r\alpha=\sqrt{m}r/(rt\sqrt{m})=1/t$的正态分布。

下面是一个正态分布的截尾不等式。设 $z\sim N(0,1)$,那么

$$\Pr(|z|>x)=2\int_x^{+\infty}\frac{1}{\sqrt{2\pi}}e^{-\frac{1}{2}z^2}dz\leqslant\frac{1}{x}\sqrt{\frac{2}{\pi}}e^{-\frac{1}{2}x^2}\quad x>0$$

类似地,$\sum_{i=1}^{m}s_iX_i$ 中每个系数 z 大于 1/4 的概率为

$$\Pr(|z|>1/4)\leqslant\frac{4}{t}\sqrt{\frac{2}{\pi}}e^{-\frac{t^2}{32}}\quad t\geqslant 20$$

显然,这个数值是可忽略不计的,所以能够正确解出 m' 且等于 m。

b)$T'=m'\times u=m\times u$,从 T' 映射到 D^m 上的某个元素 V',$C'=H(V')$。由于$T'=T$,所以 $C'=C$。因此能够通过验证。

综上,正确性验证完毕。

3.2 安全性分析

a)分析方案的加密。该加密算法是基于 R-LWE 问题,而 R-LWE 问题可以归约到格上的困难问题上。R-LWE 是 LWE 困难问题的一个扩展,其中 LWE 问题的困难性可以归约到标准格上困难性问题(如 gap-SVP 和 SIVP)的最困难情况。更为准确地讲,若 $q=2^n$,那么 LWE 的困难性等价于近似因子为 $f(n)$的 gap-SVP 问题;若 $q=\text{poly}(n)$,LWE 的困难性满足这样的假设:在以一个短基作为帮助的情况下 gap-SVP 仍然是困难的,或者即使给出一个量子计算机作为辅助,解决近似因子为多项式的 gap-SVP 和 SIVP 仍然是困难的。

b)分析方案的签名。由于广义压缩背包问题的哈希函数 H[13] 是抗碰撞,即在一个多项式时间内的算法找不到不同的 $\hat{b}$ 和 $\hat{b}'$,使得 $H(\hat{b})=H(\hat{b}')$。如果找到 H 的一个碰撞,那么就存在一个多项式算法解决环上的最短多项式问题(shortest polynomial problem,SPP)。但已经证明,环上 SPP 的复杂性与格中 SVP 问题相当。

c)方案在假设 R-LWE 问题是困难的情况下,可以达到 IND-CPA 安全。

(a)挑战者执行密钥生成算法生成一对密钥对 pk、sk,并将加密公钥公布给攻击者,挑战者保留私钥。

(b)攻击者可以进行任意次的加密操作和其他需要的操作。

(c)最后攻击者选择不同的明文 M_0、M_1 提交给挑战者。

(d)挑战者任意挑选一 $M_b(b\in\{0,1\})$,对 M_b 使用公钥 pk 执行加密操作 $E(M_b,pk)$,得挑战密文 C,将挑战密文返还给攻击者。

(e)攻击者在接收到挑战密文后可以再执行任意次的计算或加密。最后,攻击者输出对 b 的猜测 b'。

$\varepsilon=\text{adv}_A^{\text{R-LWE}}=|\Pr[b]-1/2|$,若攻击者要在相当的优势概率 ε 下取得挑战—攻击游戏,则意味着攻击都能够以一个相当优势的概率解决 $\text{LWE}_{q,\chi}$ 问题,而 $\text{LWE}_{q,\chi}$ 是一个困难问题,所以方案能够达到 IND-CPA 安全。

3.3 效率分析

上述方案只包括模 q 的加法运算和乘法运算,效率非常高。根据分析,可以将文中操作和数据量化如下:

a)公钥大小 $=(m+1)n\log(q)$ bit;

b)私钥大小 $=mn\log(r+1)$ bit;

c)明文大小 $=n$ bit;

d)密文大小 $=(m+2)n\log q$ bit;

e)密文扩展率 $=(m+2)\log q$;

f)加密操作量 $=\tilde{O}((m+1)n)$;

g)解密操作量 $=\tilde{O}((m+1)n)$。

表 2 是本文方案与其他方案的效率比较。

表 2 类似方案效率比较

方案	明文/bit	密文扩展率	加密操作/bit	解密操作/bit
本文方案	n	$(m+2)\log q$	$O((m+1)n)$	$O((m+1)n)$
Regev's LWE	$k(k<n)$	$(n/k+1)\log q$	$O((m+k)n)$	$O(nk)$
Dual LWE	$k(k<n)$	$(m/k+1)\log q$	$O((m+k)n)$	$O(mk)$

当上述方案达到相同安全等级时,另外两种方案中 m 的取值大约是本文方案的 n 倍。由此可以看出,本文方案加解密操作少,速度也就快,密文扩展率较低。本文方案基于 R-LWE 问题进行操作,有着消息容量大的优势;加解密运算都是在多项式环上进行,从而可以通过快速傅里叶变换大幅度提高加解密速度;认证过程简单、高效。 (下转第 2794 页)

有效。因此本文算法综合性能仍然较好,具有实用价值。

表 1 本文算法与文献[7]算法比较

算法	兴趣点数	匹配点	误匹配点数	检测时间/s
文献[7]算法($\omega=0.5$)	1 328	21	0	95.87
本文算法($T_d=16, T_f=2$)	993	24	0	9.46

3 结束语

针对图像窜改操作中最常见的复制粘贴窜改方式,本文提出了一种基于 Harris 兴趣点和空域均值信息的窜改检测方法。算法通过检测具有视觉意义的 Harris 角点作为兴趣点,并且提取其邻域内空域的五个具有均值意义的特征对兴趣点进行特征描述,大大降低了算法的时间复杂度。实验结果表明,算法不仅能够有效检测多区域复制粘贴窜改操作,并且能够有效抵抗高斯白噪声,JPEG 压缩,对比度、亮度和曝光度调整以及 JPEG 压缩和加噪的混合操作。然而,本文算法也有需要进一步研究和改进的地方,通过仿真实验观察,Harris 算子对于高斯模糊的后处理操作比较敏感,即高斯模糊会使 Harris 算子检测到的兴趣点数量大大减少,从而影响算法的检测结果。因此,在保持算法检测性能的同时,如何使算法对于更多的窜改后处理操作具有更强的鲁棒性是今后研究工作的方向。

参考文献:

[1] FRIDRICH J, SOUKAL D, LUKAS J. Detection of copy-move forgery in digital images[C]//Proc of Digital Forensic Research Workshop. Washington DC: IEEE Computer Society, 2003: 55-61.

[2] CAO Yan-jun, GAO Tie-gang, FAN Li, *et al*. A robust detection algorithm for region duplication in digital images [J]. International Journal of Digital Content Technology and its Applications, 2011, 5(6): 95-103.

[3] HUANG Yan-ping, LU Wei, SUN Wei, *et al*. Improved DCT-based detection of copy-move forgery in images[J]. Forensic Science International, 2011, 206(1-3): 178-184.

[4] LI Guo-hui, WU Qiong, TU Dan, *et al*. A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD[C]//Proc of IEEE International Conference on Multimedia and Expo. 2007: 1750-1753.

[5] KANG Xiao-bing, WEI Sheng-min. Identifying tampered regions using singular value decomposition in digital image forensics[C]// Proc of International Conference on Computer Science and Software Engineering. Washington DC: IEEE Computer Society, 2008: 926-930.

[6] LUO Wei-qi, HUANG Ji-wu, QIU Guo-ping. Robust detection of region-duplication forgery in digital images[C]//Proc of the 18th International Conference on Pattern Recognition. 2006: 746-749.

[7] HUANG Hai-ling, GUO Wei-qiang, ZHANG Yu. Detection of copy-move forgery in digital images using sift algorithm[C]//Proc of Pacific-Asia Workshop on Computational Intelligence and Industrial Application. Washington DC: IEEE Computer Society, 2008: 272-276.

[8] AMERINI I, BALLAN L, CALDELLI R, *et al*. A SIFT-based forensic method for copy-move attack detection and transformation recovery [J]. IEEE Trans on Information Forensics and Security, 2011, 6(3): 1099-1110.

[9] LOWE D G. Distinctive image features from scale-invariant keypoints [J]. International Journal of Computer Vision, 2004, 60(2): 91-110.

[10] XU Bo, WANG Jun-wen, LIU Guang-jie, *et al*. Image copy-move forgery detection based on SURF[C]//Proc of International Conference on Multimedia Information Networking and Security. Washington DC: IEEE Computer Society, 2010: 889-892.

[11] SHIVAKUMAR B, SANTHOSH B. Detection of region duplication forgery in digital images using SURF[J]. International Journal of Computer Science Issues, 2011, 8(4): 199-205.

[12] BAY H, ESS A, TUYTELAARS T, *et al*. SURF: speeded up robust features[J]. Computer Vision and Image Understanding, 2008, 110(3): 346-359.

[13] HARRIS C, STEPHENS M. A combined corner and edge detector [C]//Proc of the 4th Alvey Vision Conference. 1988: 147-151.

(上接第 2790 页)

4 结束语

本文从安全性考虑,基于现实的需要提出了一个基于格的认证加密方案。该方案具有加解密速度快、密文扩展率低、安全性高等优势;提出的方案还存在许多需要改进之处,如提出一个格上可公开验证的认证加密方案,构造一个格上 CCA 安全性的认证加密方案,设计一个格上基于身份的认证加密方案,将其改进为一个效率更高的基于格的签密方案等。

参考文献:

[1] 李树栋. 一个新的可公开验证的认证加密方案[J]. 烟台职业学院学报, 2007, 13(2): 55 - 57.

[2] 林飞. 一种基于 RSA 的认证加密方案[D]. 广州: 暨南大学, 2000.

[3] 章磊, 卢建朱, 凌捷, 等. 一种新的基于多素数 RSA 认证加密方案[J]. 计算机应用研究, 2005, 22(5): 105-107.

[4] 黄益栓, 卢建朱. 一种基于身份的认证加密新方案[J]. 计算机工程, 2007, 33(7): 149-150.

[5] 蔡艳桃. 一种基于身份的认证加密方案的改进[J]. 计算机工程与应用, 2011, 47(15): 119-122.

[6] AJTAI M. Generating hard instances of lattice problems[C]//Proc of the 28th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 1996: 99-108.

[7] REGEV O. The learning with errors problem[EB/OL]. http:// www.cs. tau. ac. il/ ~ odedr/papers/lwesurvey. pdf.

[8] BLUM A, KALAI A, WASSERMAN H. Noise-tolerant learning, the parity problem, and the statistical query model [J]. Journal of the ACM, 2003, 50(4): 506-519.

[9] ARORA S, GE Rong. New algorithms for learning in presence of errors[C]//Proc of the 38th International Colloquim Conference on Automata, Languages and Programming, Volume Part I. 2011: 403-415.

[10] REGEV O. On lattices, learning with errors, random linear codes and cryptography [J]. Journal of the ACM, 2009, 56(6): 34.

[11] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings[C]//Proc of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2010: 1-23.

[12] MICCIANCIO D. Generalized compact knapsacks, cyclic lattices, and efficient one way functions [J]. Computational Complexity, 2007, 16(4): 411.

[13] LYUBASHEVSKY V, MICCIANCIO D. Generalized compact knapsacks are collision resistant[C]//Lecture Notes in Computer Science, vol 4052. Berlin: Springer-Verlag, 2006: 144-155.