可抵御唯密文攻击的基于格的公钥加密

李 君
(华东师范大学 计算机科学与技术系, 上海 200241)

摘 要: 针对最新提出的对 Cai-Cusick 公钥加密方案的唯密文攻击进行研究,提出了一个可抵御该攻击的新的公钥加密方案。通过对原始加密方案中某些参数的修改,改变了公钥中向量长度,从而实现对原始方案攻击的有效抵御,并且通过程序模拟出新的加密方案。从数据分析可得,随着实验次数的增加,该方案抵御唯密文攻击的成功概率近似为百分之百。这说明了新的加密方案能有效抵御最新提出的唯密文攻击,且由于该方案延续了原始加密方案的加密步骤,其也具备了更少密文扩展的特性。今后将进一步研究语义安全的可抵御唯密文攻击的有效加密方案。

关键词: 唯密文攻击; 格; 公钥加密; 最短向量问题; 格密码
中图分类号: TP309.7 **文献标志码**: A **文章编号**: 1001-3695(2014)01-0196-03
doi:10.3969/j.issn.1001-3695.2014.1.045

Lattice-based public-key encryption with resistance of ciphertext-only attack

LI Jun
(*Dept. of Computer Science & Technology, East China Normal University, Shanghai* 200241, *China*)

Abstract: This paper proposed a new lattice-based public-key encryption which could resist the chosen ciphertext attack against Cai-Cusick encryption scheme. A small modification on parameters of the original scheme yielded this new scheme. This paper made a program to simulate this new scheme and found that with growth of the number of experiences, the probability of resisting chosen ciphertext was approximate to one. Hence, this new scheme could resist the attack efficiently. On the other hand, this improved encryption scheme also inherited the benefits from the original scheme, of less ciphertext expansion. It draw a conclusion that this scheme has less ciphertext expansion and can prevent the ciphertext-only attack.

Key words: ciphertext-only attack; lattice; public-key encryption; SVP; lattice-based cryptography

格通常被定义为 R^n 的子集,并被广泛应用于密码学和密码分析中。格是一些线性无关向量的整数线性组合。随着量子计算的发展,在量子的攻击下传统的理论密码系统越来越脆弱[1]。因此密码学家越来越多地致力于设计基于格的新型加密方案。主要原因是因为基于格的加密系统不仅具有简单和快速计算的特性,同时也可以抵御能分解大整数和计算离散对数的量子算法。格蕴藏着丰富的组合结构,该结构在过去的两个世纪中,已经吸引了许多伟大的数学家们的注意。因此,格在数学和计算机科学中被广泛应用,包括数论、组合优化以及密码学。1996 年,Ajtai[2] 构建了一个单向函数,其平均情况的安全性被证明与格中困难问题的最坏情况的安全性相关。后来 Ajtai 等人[3,4] 基于这一突破性的成果,提出了第一个基于唯一最短向量问题(u-SVP)安全性的加密方案。之后,利用该格的困难问题的加密方案相继被提出[5~10]。

随着格密码的逐渐发展,格被应用于密码学的众多领域。2007 年 Kawachi 等人[11] 给出了一个将基于格的单比特加密方案转换为多比特加密方案的通用方法。2010 年 Agrawal 等人[12] 提出了第一个基于格的有效基于身份加密方案。2011 年 Alwen 等人[13] 给出了一个计算格中短基的方法。目前,Cai 等人[14] 提出了一个基于格的加密方案来提高 Ajtai-Dwork 加密方案的加密。Cai-Cusick 基于格的公钥加密方案的主要思路是将 Ajtai-Dwork 加密技术和背包问题相结合,从而得到更少的密文扩展。不幸的是,由于 Pan 等人[15] 在 2011 年发现了一个该加密方案的唯密文攻击,使得该想法最终没能成功。事实上,Pan 等人表明了存在一个攻击者,其通过计算公钥的 Gram-Schmidt 正交化向量,可以恢复 Cai-Cusick 加密方案加密的整条消息,且该攻击成功的概率非常接近于 1。

据笔者所知,Pan 等人提出的对 Cai-Cusick 基于格的公钥加密方案的攻击是现存唯一对该方案的攻击。在本文中,进一步研究了文献[15]中提出的唯密文攻击,并且指出 Pan 等人的攻击使用了公钥的 Gram-Schmidt 正交化向量,其可以通过对原始加密方案参数的修改达到预防的效果。因此,该改进的版本不仅继承了 Cai-Cusick 加密方案的优点,还可以有效抵御目前发现的 Pan-Deng 攻击。本文方法将攻击成功的概率绑定为一个可忽略的数值,笔者相信该改进的 Cai-Cusick 基于格的公钥加密方案是目前为止最有效的。

1 准备工作

本文需要用到如下一些记号,这些记号在文献[14,15]中也有用到:

$S^{n-1}=\{x\in R^n:\|x\|=1\}$ 称为单位范围(unit sphere);

v 表示一个 n 维的向量;

$\|v\|=\langle v,v\rangle^{1/2}$ 称为欧几里德范数;

$H_i(u)=\{x\in R^n:\langle x,u\rangle=i\}$ 是垂直于 u 的平行多面体,

收稿日期: 2013-03-04; **修回日期**: 2013-04-24

作者简介:李君(1989-),女,浙江宁波人,硕士研究生,主要研究方向为信息安全、格密码(jungleli@126.com).

其中 $i \in \mathbf{Z}^+$, $u \in S^{n-1}$;

A 是 $\mathbf{R}^n$ 的一个子空间,且满足

$$A^{\perp} = \{x \in \mathbf{R}^n : \langle x, v \rangle = 0, \forall v \in A\}$$

假设 $\{v_1, v_2, \cdots, v_m\}$ 是一组格的基向量,这组基向量的跨度(span)定义如下:

$$\text{span}(v_1, v_2, \cdots, v_m) = \{[v_1, v_2, \cdots, v_m]x : x \in \mathbf{R}^n\}$$

定义 1　对于任意一组向量 $v_1, v_2, \cdots, v_m$,对应的 Gram-Schmidt 正交化向量 $v_1^*, v_2^*, \cdots, v_m^*$ 定义如下:

$$v_i^* = v_i - \sum_{j=1}^{i-1} \mu_{i,j} v_j^* \tag{1}$$

$$v_1^* = v_1 \tag{2}$$

其中:$i = 1, \cdots, m$;$\mu_{i,j} = \dfrac{\langle v_i, v_j^* \rangle}{\langle v_j^*, v_j^* \rangle}$。

2　Cai-Cusick 公钥加密方案和 Pan-Deng 攻击的回顾

2.1　回顾 Cai-Cusick 公钥加密方案

以下是 Cai-Cusick 公钥加密方案密钥生成、加密、解密过程。n 和 m 是安全参数。

1)密钥生成　加密者从单位范围 S^{n-1} 内随机选择一个向量 u。b 是一个正的实数, N_0 也是一个正数,且大于 b。选择 m 个满足如下特征的数 $N_1, \cdots, N_m$:

$$N_k > \sum_{i=0}^{k-1} N_i + b \quad \text{for } k = 1, 2, \cdots, m$$

接着,从各自的平行多面体 $H_{N_i}(u)$ $(i = 0, 1, \cdots, m)$ 中随机选择 $m+1$ 个向量 $v_0, \cdots, v_m$,以及一个对 $m+1$ 字母进行排列的随机置换 σ。最后,公钥被设置为 $pk = ((v_{\sigma(0)}, v_{\sigma(1)}, \cdots, v_{\sigma(m)}), b)$,私钥被设置为 $sk = ((u, N_0, N_1, \cdots, N_m), \sigma)$ 并且秘密保存。

2)加密　假设 $M = (a_0, a_1, \cdots, a_m)$ 是明文块,其中 $a_i \in \{0, 1\}$。对明文块 M 进行加密,首先选择一个随机向量 r 满足 $\| r \| \leqslant b/2$。之后用如下方程计算密文:

$$C = \sum_{i=0}^{m} a_i v_{\sigma(i)} + r \tag{3}$$

3)解密　要解密密文,首先计算如下内积:

$$S = \langle u, C \rangle = \sum_{i=0}^{m} a_{\sigma^{-1}(i)} N_i + \langle u, r \rangle \tag{4}$$

如果 $S \geqslant N_m - b/2$,那么返回 $a_{\sigma^{-1}(m)} = 1$;否则,返回 $a_{\sigma^{-1}(m)} = 0$。接着用 $S - a_{\sigma^{-1}(m)} N_m$ 代替 S,用同样的步骤可以恢复 $a_{\sigma^{-1}(m-1)}$,如此循环迭代直到将所有 $m+1$ bit $\{a_{\sigma^{-1}(i)}\}$ 都恢复为止。最后,使用 σ 恢复原来的明文块 M。

2.2　对 Cai-Cusick 公钥加密方案的唯密文攻击

Pan 等人[15]提出了对 Cai-Cusick 加密方案的唯密文攻击,他们指出 Cai-Cusick 加密方案被破解的概率大于如下式子:

$$1 - \frac{4bm(n-3)}{\pi} \sqrt{B^2 - N_m^2} \tag{5}$$

这个概率非常接近于 1。事实上,要想破解 Cai-Cusick 加密方案,攻击者首先要知道公钥 $v_{\sigma(0)}, v_{\sigma(1)}, \cdots, v_{\sigma(m)}, b$ 以及任意的一个密文 C。接着执行如下步骤:

a)攻击者计算 Gram-Schmidt 正交化向量 $v_{\sigma(0)}^*, \cdots, v_{\sigma(m)}^*$;

b)如果 $\min_{0 \leqslant i \leqslant m} \| v_{\sigma(i)}^* \| \leqslant b$,那么攻击者失败了;

c)否则攻击者重复如下两个步骤,直到 $i < 0$;

d)计算离 $\dfrac{\langle v_{\sigma(i)}^*, C \rangle}{\| v_{\sigma(i)}^* \|^2}$ 最近的整数,并将其记为 a_i;

e)$C := C - a_i v_{\sigma(i)}$, $i := i - 1$。

最后,攻击者可以得到原始明文 $(a_0, \cdots, a_m)$。读者可以参考文献[15]对该攻击的细节进行了解。

3　如何抵御攻击:本文的改进

据笔者所知,Pan-Deng 唯密文攻击是对 Cai-Cusick 基于格的公钥加密方案的现存唯一攻击。通过进一步的研究发现,一个小小的改善可以使该公钥加密方案有效抵御 Pan-Deng 唯密文攻击。

3.1　本文改进的公钥加密方案

Pan-Deng 攻击关键部分是向量 $v_{\sigma(i)}$ 的长度。因此,要想 Cai-Cusic 公钥加密方案抵御该唯密文攻击,需要改变 $v_{\sigma(i)}$ 的长度。具体改进的方案如下:

1)密钥生成　m 和 n 是系统参数,其中 $m = \lfloor cn \rfloor$, c 是一个大于 1 的正整数;n 和 m 分别是格的维和秩。假设 κ 是给出的安全参数,运行如下步骤来产生公私钥:

a)从单位范围 $S^{n-1} = \{x \in \mathbf{R}^n : \| x \| = 1\}$ 中随机选择一个向量 u;

b)选择一个实数 $b > 0$;

c)选择一个实数 $d > 2^{\kappa}$;

d)分别从 $H_{N_0}(u), \cdots, H_{N_m}(u)$ 中随机选择向量 $v_0, v_1, \cdots, v_m$,其中 $N_k > \sum_{i=0}^{k-1} N_i + bd$, $k = 1, 2, \cdots, m$ 且 $N_0 > bd$;

e)随机选择对 $m+1$ 个字母的一个置换 σ;

f)设置一组向量 $V_0', \cdots, V_m'$,每个 V_i' 等于 $\dfrac{1}{d} v_{\sigma(i)}$;

g)输出公钥 $pk = ((V_0', V_1', \cdots, V_m'), b)$ 和私钥 $sk = ((u, N_0, N_1, \cdots, N_m, d), \sigma)$。

2)加密　给出要加密的明文块 $M = (a_0, a_1, \cdots, a_m)$,其中 $a_i \in \{0, 1\}$。加密者首先从 $\{x \in \mathbf{R}^n : \| x \| \leqslant b/2\}$ 中随机选择一个 n 维的向量 r,之后用如下方程计算密文:

$$C = \sum_{i=0}^{m} a_i V_i' + r \tag{6}$$

3)解密　要想解密密文 C,解密者首先计算如下内积:

$$S = \langle u, C \rangle = \sum_{i=0}^{m} a_i \langle u, V_i' \rangle + \langle u, r \rangle = \frac{1}{d} \sum_{i=0}^{m} a_{\sigma^{-1}(i)} N_i + \langle u, r \rangle \tag{7}$$

之后执行如下步骤:

a)如果 $i \geqslant 0$,计算

$$a_{\sigma^{-1}(i)} = \begin{cases} 1 & \text{if } S \geqslant \dfrac{1}{d} N_i - b/2 \\ 0 & \text{otherwise} \end{cases} \tag{8}$$

b)用 $S - \dfrac{1}{d} a_{\sigma^{-1}(i)} N_i$ 代替 S;

c)$i = i - 1$。

在获得所有 $\{a_{\sigma^{-1}(i)}\}$ $(0 \leqslant i \leqslant m)$ 之后,使用 σ 来恢复明文块 $M = (a_0, \cdots, a_m)$。

4)正确性验证　由于 $|\langle u, r \rangle| \leqslant \| u \| \| r \| = \| r \| \leqslant b/2$,得到

$$\frac{1}{d} \sum_{i=0}^{m} a_{\sigma^{-1}(i)} N_i - \frac{b}{2} \leqslant S \leqslant \frac{1}{d} \sum_{i=0}^{m} a_{\sigma^{-1}(i)} N_i + \frac{b}{2}$$

因此,如果 $a_{\sigma^{-1}(m)} = 1$,那么满足 $S \geqslant \dfrac{1}{d} N_m - b/2$;否则,由于 $\langle u, r \rangle \leqslant b/2$ 和 $N_m > \sum_{i=0}^{m-1} N_i + bd$。$S$ 范围如下:

$$S \leqslant \frac{1}{d} \sum_{i=0}^{m-1} N_i + b/2 < \frac{1}{d} N_m - b/2$$

对于另外的比特也是如此。

3.2 关于参数

以下参数被所有参与者认可。由 $b' > b$ 定义：

$$v_i = (2^i b'/P)\,u + \sqrt{1-(2^{2i}b'^2/P^2)}\,\rho_i$$

其中：$0 \leqslant i \leqslant m$，$P >> 2^n$，并且 ρ_i 独立且均匀分布在垂直于 u 的 $n-2$ 维单位范围内。

v_i 的分布区分于 $m+1$ 个范围的独立均匀采样，并且可以抵御通过计算与 $v_{\sigma(0)}, \cdots, v_{\sigma(m)}$ 向量有关得到的统计信息方面的攻击。举例说明，如 $\sum_{i=0}^{m} v_i = \sum_{i=0}^{m} v_{\sigma(i)}$ 可能会泄露关于秘钥的一些信息。

秘钥 d 应该大于 2^κ，其中 κ 是一个整数（在这里假设 $\kappa \geqslant 80$，其可以保证本文方案可以抵御 Pan-Deng 唯密文攻击）。

3.3 安全性分析

正如在 Pan-Deng 唯密文攻击中看到的，a_i 成立的概率非常接近于 1，这个等式是其攻击中关键部分。然而，在本文的方案中这个情况不会发生，因为通过改变向量 $v_{\sigma(i)}$ 的长度改变了函数 $\frac{\langle v^*_{\sigma(i)}, C\rangle}{\| v^*_{\sigma(i)} \|^2}$ 的范围。原因解释如下：

不失一般性，假设 $(a_0, a_1, \cdots, a_m)$ 是想要从密文 C 中恢复的消息，r 是随机选择的一个向量，长度满足 $\| r \| \leqslant b/2$。将 r 重新表示为

$$r = \sum_{i=0}^{m} r_i v^*_{\sigma(i)} + w \tag{9}$$

其中：$r_i \in \mathrm{R}$ 并且 $w \in \mathrm{span}(v^*_{\sigma(0)}, v^*_{\sigma(1)}, \cdots, v^*_{\sigma(m)})^{\perp}$，之后得到

$$\| r \| = \sqrt{\sum_{i=0}^{m} r_i^2 \| v^*_{\sigma(i)} \|^2 + \| w \|^2} \geqslant | r_m | \| v^*_{\sigma(m)} \| \tag{10}$$

由于

$$| r_m | \| v^*_{\sigma(m)} \| \leqslant \| r \| \leqslant b/2,$$

$$\| v^*_{\sigma(m)} \| \geqslant \min_{0 \leqslant i \leqslant m} \{ \| v^*_{\sigma(i)} \| \} > b > 0 \tag{11}$$

得到 r_m 的范围如下：

$$| r_m | \leqslant \frac{b}{2 \| v^*_{\sigma(m)} \|} < 1/2 \tag{12}$$

通过相同的分析，可得到 $| r_i | < 1/2 (0 \leqslant i \leqslant m)$。

另一方面，在改进的加密方案中

$$\langle v^*_{\sigma(m)}, C\rangle = \frac{1}{d} a_m \| v^*_{\sigma(m)} \|^2 + r_m \| v^*_{\sigma(m)} \|^2 \tag{13}$$

其中：$| r_m | < 1/2$，$d > 2^\kappa$。那么

$$\frac{\langle v^*_{\sigma(m)}, C\rangle}{\| v^*_{\sigma(m)} \|^2} = \begin{cases} r_m & \text{if } a_m = 0 \\ \frac{1}{d} + r_m & \text{else } a_m = 1 \end{cases} \tag{14}$$

因此，无论 $a_m = 1$ 或者不为 1，离 $\frac{\langle v^*_{\sigma(i)}, C\rangle}{\| v^*_{\sigma(i)} \|^2}$ 最近的整数对于任何随机选择的向量 r 总是等于 0 。

最后，发现离 $\frac{\langle v^*_{\sigma(i)}, C\rangle}{\| v^*_{\sigma(i)} \|^2}$ 最近的整数等于 1 的情况仅当 $| r_m | \geqslant \frac{1}{2} - \frac{1}{d}$ 时成立。

由于向量 r 是随机选择的，根据本文方案中的加密算法，$| r_m |$ 也应该随机分布于区间 $[0, \frac{1}{2})$ 中。因此对于任何通过本文方案的加密算法随机选择的向量 r，式(12)成立的概率为

$$\Pr\left[\frac{\langle v^*_{\sigma(m)}, C\rangle}{\| v^*_{\sigma(m)} \|^2} = 1 \right] = \frac{\frac{1}{2} - (\frac{1}{2} - \frac{1}{d})}{\frac{1}{2} - 0} = \frac{2}{d} \leqslant \frac{1}{2^{\kappa-1}} \tag{15}$$

因此了解到，一个采用 Pan-Deng 唯密文方案进行攻击的攻击者成功的概率最多为 $\frac{1}{2^{\kappa-1}}$，这是一个可以忽略的可能性。通过以上对 a_m 的分析可以发现，该分析对于 $a_i (0 \leqslant i \leqslant m-1)$ 同样成立。用如下的定理来陈述本文改进的方案可以有效抵御 Pan-Deng 的唯密文攻击。

定理 1 对于 $d > 2^{\kappa+1}$，改进的公钥加密方案可以成功抵御 Pan-Deng 唯密文攻击，除了一个可忽略的失败概率 $\frac{1}{2^\kappa}$ 外。

3.4 实验及其结果

对本文中的改进方案进行了代码实现，并且通过反复实验发现，该方案抵御 Pan-Deng 唯密文攻击的概率接近 100%。首先给出了测试抵御成功概率的实验步骤：

a) 初始化参数 m、n 和 κ；

b) % 该步实现密钥生成

$u \leftarrow \{ x \in \mathrm{R}^n : \| x \| = 1 \}$

$b \leftarrow \{ x \in \mathrm{R} \}$

$d \leftarrow \{ x > 2^\kappa : x \in \mathrm{R} \}$

$N_0 \leftarrow bd + 1$

$v_0 \leftarrow \{ v : \langle v, u \rangle = N_0 \}$

for $i = 1 : m$

$N_i = \sum_{j=0}^{i-1} N_j + bd + 1$

$v_i \leftarrow \{ v : \langle v, u \rangle = N_i \}$

end

c) % 该步实现 Pan-Deng 攻击成功条件判定

$V = \frac{1}{d} [v_0 \mid v_1 \mid \cdots \mid v_m]$

$V^* = G - S(V)$

min = min $\| v_i^* \|$

%1 表示抵御成功，0 表示抵御失败

if min $\leqslant b$

output 1

else output 0

end

以上给出的步骤是一次测试所需要的步骤，通过对该过程反复实验，对抵御成功的次数进行统计，得到如表 1 所示的实验结果。通过表 1 的结果发现，提出的新方案可以有效抵御 Pan-Deng 唯密文攻击，并且该抵御成功的概率几乎接近于 100%。

表 1 实验结果

运行次数	安全参数	抵御成功的概率/%	运行次数	安全参数	抵御成功的概率/%
10	10	80	100	60	88
10	20	90	1 000	70	89.2
10	30	90	1 000	80	92.1
100	40	92	1 000	90	91.5
100	50	91			

4 结束语

本文改进了 Cai-Cusick 公钥加密方案来抵御 Pan-Deng 唯密文攻击。由于 Pan-Deng 攻击是目前所知对于 Cai-Cusick 公钥加密方案的唯一攻击，本文提出的新方案可以抵御所有目前已知的攻击方案。未来笔者将致力于构建该方案的安全性证明。

参考文献：

[1] SHOR P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proc of the 35th Annual Symposium on Foundations of Computer Science. Washington DC: IEEE Computer Society, 1994: 124-134.

（下转第 209 页）

n_m 表示明文长度,n_u 表示用户身份长度,本方案与 Zhang 方案[11]具体比较如表 1 所示。

表 1　方案间公、私钥和签名长度的比较

方案	公钥长度	私钥长度	签名长度
文献[11]	$Z_q^* + \|G_q\| + (n_u + k + 5 + n_m)\|G\|$	$(2n+1)\|G\| + \|G_q\|$	$(n+3)\|G\| + 2n_u\|G_q\|$
本方案	$Z_q^* + \|G_q\| + (n_u + k + 5)\|G\|$	$2n\|G\|$	$(2n+1)\|G\| + 2n_u\|G_q\|$

由表 1 可知,本文方案与文献[11]相比,公钥长度和私钥长度明显减少,这在当今网络资源带宽受限的情况下具有明显的优势,非常适合当今社交网络和车载网络等环境下使用。

由表 2 可知,本文方案与文献[11]相比,验证运算量虽然有所增加,但签名运算量降低了,在当今无线网络等小型网络快速发展的情况下,该方案有着明显的优势。

表 2　运算效率的比较

方案	签名运算量	验证运算量
文献[11]	$(5n_u + 2n + 9/2)e$	$(k+3)e + (n+4)p$
本方案	$(5n_u + n + 1)e$	$(k+3+3n)e + (3n+1)p$

5　结束语

本文在文献[11]的基础上,提出了一个新的可追踪身份的门限属性签名方案。方案的安全性基于一般的计算性 Diffie-Hellman 问题,由 PKG 产生的追踪密钥,实现对属性签名中签名者身份的可追踪性和不可联系性。方案的验证运算效率有所降低,但方案的公钥、私钥有明显的减少,签名效率很大提高,在通信带宽受限的情况下,有明显的优势。

参考文献:

[1] SAHAI A, WATERS B. Fuzzy identify-based encryption[C]//Proc of the 24th Annual International Conference on Theory and APPlications of Cryptographic Techniques. 2005: 457-473.

[2] GOYAL V, PANDEY O, SAHAI A, *et al*. Attribute-based encryption for fine-grained access control of encrypted data[C]// Proc of the 13th ACM Conference on Computer and Communications Security. New York: ACM Press, 2006: 89-98.

[3] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext policy attribute-based encryption[C]// Proc of IEEE Symposium on Security and Privacy. [S. l.]: IEEE Computer Society, 2007: 321-334.

[4] OSTROVSKY R, SAHAI A, WATERS B. Attribute-based encryption with non-monotonic access structures[C]// Proc of the 14th ACM Conference on Computer and Communications Security. New York: ACM Press, 2007: 195-203.

[5] CHEUNG L, NEWPORT C. Provably secure ciphertext policy ABE[C]// Proc of the 14th ACM Conference on Computer and Communications Security. New York: ACM Press, 2007: 456-465.

[6] YANG pi-yi, CAO Zhen-fu, DONG Xiao-lei. Fuzzy identify based signature with applications to biometric authen tication[J]. Computer and Electrical Engineering, 2011, 37(4): 532-540.

[7] EMURA K, MIYAJI A, OMOTE K. A dynamic attribute- based group signature scheme and its application in an anonymous survey for the collection of attribute statistics[C]// Proc of International Conference on Availability, Reliability and Security. 2009: 487-492.

[8] LI J, AU M H, SUSILO W, *et al*. Attribute-based signature and its applications[C]// Proc of the 5th ACM Symposium on Information, Computer and Communications Security. Beijing: ACM Press, 2010: 60-69.

[9] ESCALA A, HERRANZ J, MORILLO P. Revocable attribute-based signatures with adaptive security in the standard model[C]// Proc of Progress in Cryptogy-Africacrypt. Berlin: Springer-Verlag, 2011: 224-241.

[10] DESMEDT Y, FRANKEL Y. Shared gengration of authenticators and signatures[C]//Proc of Advances in Crypto. Berlin: Springer- Verlag, 1992.

[11] 张秋璞,徐震,叶顶锋. 一个可追踪身份的基于属性签名方案[J]. 软件学报, 2012, 23(9): 2449-2464.

[12] GROTH J, OSTROVSKY R, SAHAAI A. Perfect noninteractive zero knowledge for NP[C]// Proc of Advances in Cryptology Eurocrypt. Berlin: Springer- Verlag, 2006: 339-358.

(上接第 198 页)

[2] 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.

[3] AJTAI M, DWORK C. A public-key cryptosystem with worst-case/ave rage-case equivalence [C]//Proc of the 29th Annual ACM Symposium on Theory of Computing. New York: ACM Press, 1997: 284-293.

[4] AJTAI M, DWORK C. The first and fourth public-key cryptosystems with worst-case/average-case equivalence [C]//Proc of Electronic Colloquium on Computational Complexity. 2007: 97-134.

[5] GOLDREICH O, GOLDWASSER S, HALEVI S. Public-key cryptosystems from lattice reduction problems[C]//Advances in Cryptology. Berlin: Springer, 1997: 112-131.

[6] HOFFSTEIN J, HOWGRAVE-GRAHAM N, PIPHER J, *et al*. NTRUS: digital signatures using the NTRU lattice[C]//Topics in Cryptology. Berlin: Springer, 2003: 122-140.

[7] PEIKERT C. Public-key cryptosystems from the worst-case shortest vector problem[C]//Proc of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 333-342.

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

[9] MICCIANCIO D, REGEV O. Lattice-based cryptography[M]//Post-Quantum Cryptography. Berlin: Springer, 2009: 147-191.

[10] REGEV O. Lattice-based cryptography[C]//Advances in Cryptology. Berlin: Springer, 2006: 131-141.

[11] KAWACHI A, TANAKA K, XAGAWA K. Multi-bit cryptosystems based on lattice problems[C]//Public Key Cryptography. Berlin: Springer, 2007: 315-329.

[12] AGRAWAL S, BONEH D, BOYEN X. Efficient lattice (H) IBE in the standard model[C]//Advances in Cryptology. Berlin: Springer, 2010: 553-572.

[13] ALWEN J, PEIKERT C. Generating shorter bases for hard random lattices[J]. Theory of Computing Systems, 2011, 48(3): 535-553.

[14] CAI Jin-yi, CUSICK T W. A lattice-based public-key cryptosystem [C]//Selected Areas in Cryptography. Berlin: Springer, 1999: 219-233.

[15] PAN Yan-bin, DENG Ying-pu. A ciphertext-only attack against the Cai-Cusick lattice-based public-key cryptosystem[J]. IEEE Trans on Information Theory, 2011, 57(3): 1780-1785.