# 无陷门格基签密方案

路秀华*①② 温巧燕② 王励成③ 杜 蛟④
①(廊坊师范学院数学与信息科学学院 廊坊 065000)
②(北京邮电大学网络与交换技术国家重点实验室 北京 100876)
③(北京邮电大学信息安全中心 北京 100876)
④(河南师范大学数学与信息科学学院 新乡 453007)

**摘 要**：现有的格基签密方案以陷门产生算法和原像取样算法为核心算法。但是，这两个算法都很复杂，运算量较大，严重影响格基签密方案的执行效率。该文运用无陷门格基签名及其签名压缩技术，结合基于带错学习问题的加密方法，提出第 1 个基于格理论的、不依赖于陷门产生算法和原像取样算法的签密方案。方案在带错学习问题和小整数解问题的难解性假设下，达到了自适应选择密文攻击下的不可区分性和自适应选择消息攻击下的不可伪造性。方案在抗量子攻击的同时，保证了较高的执行效率。

**关键词**：基于格的密码学；签密；无陷门格基签名；带错学习问题；小整数解问题
**中图分类号**：TP309 **文献标识码**：A **文章编号**：1009-5896(2016)09-2287-07
**DOI**: 10.11999/JEIT151044

# A Lattice-based Signcryption Scheme Without Trapdoors

LU Xiuhua①② WEN Qiaoyan② WANG Licheng③ DU Jiao④
①(*Faculty of Mathematics and Information Science*, *Langfang Teachers University*, *Langfang* 065000, *China*)
②(*State Key Laboratory of Networking and Switching Technology*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)
③(*Information Security Center*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)
④(*College of Mathematics and Information Science*, *Henan Normal University*, *Xinxiang* 453007, *China*)

**Abstract**: The existing lattice-based signcryption schemes are based on trapdoor generation algorithm and preimage sample algorithm. However, both algorithms are complex, require a lot of time to run, and affect the efficiency of latticed-based signcryption schemes deeply. To solve this problem, the first lattice-based signcryption scheme without trapdoor generation algorithm and preimage sample algorithm is proposed, with the help of the technique of lattice signatures without trapdoors and the associated signature compression technique, as well as the encryption method based on the learning with errors assumption. The scheme achieves indistinguishability against adaptive chosen ciphertext attacks under the learning with errors assumption. It also achieves existential unforgeability against adaptive chosen message attacks under the small integer solution assumption. The proposed scheme is not only quantum resistant, but also efficient.

**Key words**: Lattice-based cryptography; Signcryption; Lattice signatures without trapdoors; Learning with errors problem; Small integer solution problem

## 1 引言

签密是由文献[1]提出的基本密码学原语，可以同时实现信息的机密性和认证性，为信息的安全传输，提供最基本的安全保障。在大整数因子分解问题和离散对数问题等传统数论问题的难解性假设下，已有大量的签密方案被提出[2–4]。但是伴随着文献[5]提出分解大整数和解决离散对数问题的量子多项式时间算法，以及量子计算机这些年来的飞速发展，我们不得不去探寻能够抵抗量子算法攻击的密码体制。

基于格的密码学是新兴的抗量子密码，由于其独特的理论优势，近二十年来发展迅速。格基密码目前可以实现绝大部分的密码学功能，比如认证密钥交换方案[6]，可撤销的加密方案[7]等。至于签密方案，格上的实现已有文献[8–11]，这些方案都以格中

收稿日期：2015-09-14；改回日期：2016-06-27；网络出版：2016-08-09
*通信作者：路秀华 luxiuhua2014@sina.cn
基金项目：国家自然科学基金(61300181, 61502044, 61402015, U1404601, 11471104)，中央高校基本科研业务费专项资金(2015RC23)，河北省教育厅青年基金(QN2015084)，廊坊市科技局项目(2015011063)，廊坊师范学院博士基金(LSLB201408)
Foundation Items: The National Natural Science Foundation of China (61300181, 61502044, 61402015, U1404601, 11471104), The Fundamental Research Funds for the Central Universities (2015RC23), Hebei Province Education Funds for Youth Project (QN2015084), Langfang Municipal Science and Technology Support Program (2015011063), Langfang Teachers University Doctor Funds (LSLB201408)

的陷门产生算法和原像取样算法为基础，算法的计算复杂度较大。文献[12]在 2012 年提出了格中无陷门签名方案的构造方法，文献[13]在 2014 年对其进行了改进，缩短了签名的长度。本文在文献[13]的基础上，构建了一个不需要陷门产生算法和原像取样算法的格基签密方案，并以带错学习问题和小整数解问题的难解性假设为基础，结合文献[14]的转化方法，证明了方案的自适应选择密文攻击下的不可区分性和自适应选择消息攻击下的不可伪造性。最后，给出了方案的效率分析，验证了所构造方案的高效性。

## 2 签密的形式化定义

一个签密方案由 3 个算法组成：密钥生成算法，签密算法，解签密算法。

(1) 密钥生成算法：该算法输入安全参数 $n$，输出每个用户的公私钥对 $(\mathrm{pk},\mathrm{sk})$。

(2) 签密算法：不妨设发送者持有的公私钥对为 $(\mathrm{pk}_s,\mathrm{sk}_s)$，接收者持有的公私钥对为 $(\mathrm{pk}_r,\mathrm{sk}_r)$。

发送者要发送消息 $\varpi$ 给接收者，他将用 $\mathrm{sk}_s$ 和 $\mathrm{pk}_r$ 对 $\varpi$ 同时执行签名和加密操作，得到密文 $\boldsymbol{C}=$ $=\mathrm{Signcrypt}(\mathrm{sk}_s,\mathrm{pk}_r,\varpi)$。

(3) 解签密算法：接收者收到密文 $\boldsymbol{C}$，他将用 $\mathrm{sk}_r$ 和 $\mathrm{pk}_s$ 对 $\boldsymbol{C}$ 执行解密和签名验证操作。如果解密成功且签名验证通过，输出消息 $\varpi$，即 $\varpi=\mathrm{Unsigncrypt}(\mathrm{sk}_r,\mathrm{pk}_s,\boldsymbol{C})$；否则，输出错误符号“$\perp$”。

签密方案的正确性如下：对持有 $(\mathrm{pk}_s,\mathrm{sk}_s)$ 的发送者和持有 $(\mathrm{pk}_r,\mathrm{sk}_r)$ 的接收者，若 $\boldsymbol{C}=\mathrm{Signcrypt}(\mathrm{sk}_s,\mathrm{pk}_r,\varpi)$ 成立，则 $\varpi=\mathrm{Unsigncrypt}(\mathrm{sk}_r,\mathrm{pk}_s,\boldsymbol{C})$ 以接近 1 的概率成立。

## 3 签密的安全模型

一个签密方案必须同时实现信息的机密性和认证性，因此方案的安全性包含两个方面：(1)自适应选择密文攻击下的不可区分性(INDistinguishability against adaptive Chosen Ciphertext Attacks, IND-CCA2)；(2)自适应选择消息攻击下的不可伪造性(Existential UnForgeability against adaptive Chosen Message Attacks, EUF-CMA)。

### 3.1 IND-CCA2 安全性

签密方案的IND-CCA2安全性由下面的游戏来描述，游戏由挑战者CH和敌手AD交互完成。

**初始阶段** CH执行密钥生成算法，生成接收者的公私钥对 $(\mathrm{pk}_r^*,\mathrm{sk}_r^*)$。 CH将 $\mathrm{pk}_r^*$ 发送给AD，保密 $\mathrm{sk}_r^*$。

**阶段 1** AD自适应地执行多项式有界次数的解签密查询。 解签密查询中，AD提供密文 $\boldsymbol{C}$ 和对应发送者的公私钥对 $(\mathrm{pk}_s,\mathrm{sk}_s)$ 给CH。 CH执行解签密算法。如果密文 $\boldsymbol{C}$ 是合法的，CH返回对应的明文 $\varpi$ 给AD；如果密文 $\boldsymbol{C}$ 是不合法的，CH返回错误符号“$\perp$”。

**挑战阶段** 敌手AD给出两个长度相同的明文 $\varpi_0$，$\varpi_1$ 和发送者的公私钥对 $(\mathrm{pk}_s^*,\mathrm{sk}_s^*)$，一起发送给挑战者CH。CH随机选择 $b\in\{0,1\}$，执行签密算法，将 $\boldsymbol{C}^*=\mathrm{Signcrypt}(\mathrm{sk}_s^*,\mathrm{pk}_r^*,\varpi_b)$ 返回给敌手AD。

**阶段 2** 敌手AD重复阶段1的操作，但他不能对 $\boldsymbol{C}^*$ 和 $(\mathrm{pk}_s^*,\mathrm{sk}_s^*)$ 进行解签密查询。

**猜测阶段** 敌手AD给出他对 $b$ 的猜测 $b'$。 如果 $b'=b$，则敌手AD赢得了这个游戏。

在这个游戏中，令 $\Pr(b'=b)$ 为 $b'=b$ 的概率，则敌手AD的优势定义为 $\mathrm{adv}(\mathrm{AD})=\left|2\Pr(b'=b)-1\right|$。

**定义 1** 一个签密方案是IND-CCA2安全的，如果每个多项式有界的敌手在上述游戏中的优势都是可忽略的。特别地，如果在上述游戏中不允许敌手进行解签密查询，则签密方案具有选择明文攻击下的不可区分性(INDistinguishability against Chosen Plaintext Attacks, IND-CPA)。

### 3.2 EUF-CMA 安全性

签密方案的 EUF-CMA 安全性由挑战者CH和敌手FG之间的如下交互来描述。

**初始阶段** CH执行密钥生成算法，生成发送者的公私钥对 $(\mathrm{pk}_s^*,\mathrm{sk}_s^*)$。 CH将 $\mathrm{pk}_s^*$ 发送给FG，保密 $\mathrm{sk}_s^*$。

**攻击阶段** FG自适应地执行多项式有界次数的签密查询。FG发送消息 $\varpi$ 和接收者的公私钥对 $(\mathrm{pk}_r,\mathrm{sk}_r)$ 给CH。CH执行签密算法，返回密文 $\boldsymbol{C}=\mathrm{Signcrypt}(\mathrm{sk}_s^*,\mathrm{pk}_r,\varpi)$ 给敌手FG。

**伪造阶段** FG选定接收者的公私钥对 $(\mathrm{pk}_r^*,\mathrm{sk}_r^*)$ 和消息 $\varpi^*$，创建初始阶段指定发送者的密文 $\boldsymbol{C}^*$。如果 $\boldsymbol{C}^*$ 不是之前签密查询的结果，而且 $\boldsymbol{C}^*$ 在解签密算法中的输出不是错误符号“$\perp$”，则称敌手FG赢得了这个游戏。FG赢得游戏的概率就是他在这个游戏中的优势。

**定义 2** 签密方案是 EUF-CMA 安全的，如果每个多项式有界的敌手在上述游戏中的优势都是可忽略的。

## 4 无陷门格基签密方案 1

(1) 系统设置：

(a) $n$ 为系统安全参数，$\omega$ 满足 $2^{\omega}\binom{n}{\omega}\geq 2^{128}$，$m=2n$，$M$ 是一个小的正整数(比如 8)，$d$ 是一个小的正整数(比如 24)，$0<\alpha<1$，$q>2^d$，$\sigma=\alpha q$，$\upsilon=7\sigma\sqrt{n\omega}$，$B=14\sigma\sqrt{\omega}(n-1)$。

(b) $\mathbb{D}_\sigma = \mathbb{D}_{\sigma,0}$ 是均值为 0，标准差为 $\sigma$ 的高斯分布。$\mathbb{D}_\upsilon = \mathbb{D}_{\upsilon,0}$ 是均值为 0，标准差为 $\upsilon$ 的高斯分布。

(c)随机选取 $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{m\times n}$，这里 $\mathbb{Z}$ 是整数集合。

(d) $H:\{0,1\}^* \rightarrow \Upsilon=\{\boldsymbol{v}:\boldsymbol{v}\in\{-1,0,1\}^n,\ \|\boldsymbol{v}\|_1 \le \omega\}$ 是抗碰撞的 Hash 函数。

(e) $(E_k, D_k)$ 是一个安全的理想对称加密算法，密钥空间为 $\{k \mid k \in \{0,1\}^n\}$。

(2)密钥生成算法：

(a)随机抽取矩阵 $\boldsymbol{S} \leftarrow \mathbb{D}_\sigma^{n\times n}$，$\boldsymbol{E} \leftarrow \mathbb{D}_\sigma^{m\times n}$。这里要求矩阵 $\boldsymbol{S}$ 和 $\boldsymbol{E}$ 的所有分量都不超过 $7\sigma$。如果某个分量不满足要求，重新抽取。

(b)令 $\boldsymbol{T} = \boldsymbol{AS} + \boldsymbol{E} (\mathrm{mod}\ q)$。则 $\boldsymbol{T}$ 为用户公钥，$\boldsymbol{S}$ 为用户私钥。

(3)签密算法：设消息 $\varpi$ 的发送者持有公私钥对 $(\boldsymbol{T}_s, \boldsymbol{S}_s)$，接收者持有公私钥对 $(\boldsymbol{T}_r, \boldsymbol{S}_r)$，消息发送者对消息 $\varpi$ 执行如下操作：

(a)随机抽取 $\boldsymbol{y} \leftarrow \mathbb{D}_\upsilon^n$。

(b)令 $\boldsymbol{c} = H\left(\lfloor \boldsymbol{Ay} (\mathrm{mod}\ q) \rceil_d, \varpi\right)$，$\boldsymbol{z} = \boldsymbol{S}_s\boldsymbol{c} + \boldsymbol{y}$。这里 $\lfloor x \rceil_d = (x - [x]_{2^d})/2^d$，$[x]_{2^d}$ 表示在区间 $(-2^{d-1}, 2^{d-1}]$ 中满足 $x \equiv [x]_{2^d} \left(\mathrm{mod}\ 2^d\right)$ 的惟一整数。

(c)令 $\boldsymbol{w} = \boldsymbol{Az} - \boldsymbol{T}_s\boldsymbol{c}\left(\mathrm{mod}\ q\right)$。若 $\boldsymbol{w}$ 的某个分量 $w_i$ 满足 $\left|[w_i]_{2^d}\right| > 2^{d-1} - 7\omega\sigma$，返回步骤(a)重新抽取 $\boldsymbol{y}$。

(d)以概率 $\min\left(\frac{\mathbb{D}_\upsilon^n(\boldsymbol{z})}{M\mathbb{D}_{\upsilon,\boldsymbol{S}_s\boldsymbol{c}}^n(\boldsymbol{z})}, 1\right)$ 保留 $(\boldsymbol{z}, \boldsymbol{c})$。

(e)取 $\boldsymbol{c}$ 的前 $n$ 个比特记为 $\bar{c}$，其余比特记为 $\tilde{c}$，则 $\boldsymbol{c}$ 的二进制表示为 $\bar{c} \,||\, \tilde{c}$，这里 $||$ 表示串的连接。令 $\mu = E_{\bar{c}}(\varpi, \boldsymbol{z}, \tilde{c})$。

(f)随机抽取噪声向量 $\boldsymbol{e}_1 \leftarrow \mathbb{D}_\sigma^m$，$\boldsymbol{e}_2, \boldsymbol{e}_3 \leftarrow \mathbb{D}_\sigma^n$，令 $\boldsymbol{\nu}_1^{\mathrm{T}} = -\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_2^{\mathrm{T}}$，$\boldsymbol{\nu}_2^{\mathrm{T}} = \boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{T}_r + \boldsymbol{e}_3^{\mathrm{T}} + \bar{c}\cdot\lfloor q/2 \rfloor$。这里 $\boldsymbol{\nu}_1^{\mathrm{T}}$ 表示向量 $\boldsymbol{\nu}_1$ 的转置。

则密文 $\boldsymbol{C} = (\mu, \boldsymbol{\nu}_1, \boldsymbol{\nu}_2)$。

(4)解签密算法：接收者收到密文 $\boldsymbol{C} = (\mu, \boldsymbol{\nu}_1, \boldsymbol{\nu}_2)$，他如下操作：

(a)计算 $\hat{\boldsymbol{c}} = \boldsymbol{\nu}_1^{\mathrm{T}} \cdot \boldsymbol{S}_r + \boldsymbol{\nu}_2^{\mathrm{T}}$，则 $\hat{\boldsymbol{c}} \in \mathbb{Z}_q^{1\times n}$。不妨设 $\hat{\boldsymbol{c}} = (c_1', c_2', \cdots, c_n')$。对 $i = 1,2,\cdots,n$，如果 $c_i' \in [-\lfloor q/4 \rfloor, \lfloor q/4 \rfloor)$，令 $c_i = 0$；否则 $c_i = 1$。则 $\bar{c} = (c_1, c_2, \cdots, c_n)$。

(b) 计算 $D_{\bar{c}}(\mu) = (\varpi, \boldsymbol{z}, \tilde{c})$，设二进制串 $\bar{c} \,||\, \tilde{c}$ 对应的 $\{-1,0,1\}^n$ 中元素为 $\boldsymbol{c}$。

(c) 验证 $\boldsymbol{c} = H\left(\lfloor \boldsymbol{Az} - \boldsymbol{T}_s\boldsymbol{c}\left(\mathrm{mod}\ q\right)\rceil_d, \varpi\right)$ 和 $\|\boldsymbol{z}\|_2 \le B$ 是否成立。如果都成立，接受明文 $\varpi$；否则，输出错误符号“$\perp$”。

### 4.1 方案 1 的正确性

因为 $\boldsymbol{T}_r = \boldsymbol{AS}_r + \boldsymbol{E}_r (\mathrm{mod}\ q)$，所以

$$\begin{aligned}\hat{\boldsymbol{c}} &= (c_1', c_2', \cdots, c_n') = \boldsymbol{\nu}_1^{\mathrm{T}} \cdot \boldsymbol{S}_r + \boldsymbol{\nu}_2^{\mathrm{T}} \\ &= (-\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_2^{\mathrm{T}})\boldsymbol{S}_r + \boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{T}_r + \boldsymbol{e}_3^{\mathrm{T}} + \bar{c}\cdot\lfloor q/2 \rfloor \\ &= \left(-\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_2^{\mathrm{T}}\right)\boldsymbol{S}_r + \boldsymbol{e}_1^{\mathrm{T}}\left(\boldsymbol{AS}_r + \boldsymbol{E}_r\right) + \boldsymbol{e}_3^{\mathrm{T}} + \bar{c}\cdot\lfloor q/2 \rfloor \\ &= -\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{AS}_r + \boldsymbol{e}_2^{\mathrm{T}}\boldsymbol{S}_r + \boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{AS}_r + \boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{E}_r + \boldsymbol{e}_3^{\mathrm{T}} + \bar{c}\cdot\left\lfloor q/2 \right\rfloor \\ &= \boldsymbol{e}_2^{\mathrm{T}}\boldsymbol{S}_r + \boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{E}_r + \boldsymbol{e}_3^{\mathrm{T}} + \bar{c}\cdot\lfloor q/2 \rfloor\end{aligned}$$

$\boldsymbol{S}_r$，$\boldsymbol{E}_r$，$\boldsymbol{e}_1$，$\boldsymbol{e}_2$，$\boldsymbol{e}_3$ 的分量都来自分布 $\mathbb{D}_\sigma$，所以若 $c_i' \in \left[-\lfloor q/4 \rfloor, \lfloor q/4 \rfloor\right)$，$c_i = 0$；否则 $c_i = 1$。由此可还原 $\bar{c}$。

由对称加密算法 $(E_k, D_k)$ 的正确性，通过 $D_{\bar{c}}(\mu)$ 可正确还原 $(\varpi, \boldsymbol{z}, \tilde{c})$，从而可得 $\boldsymbol{c}$。

因为 $\boldsymbol{T}_s = \boldsymbol{AS}_s + \boldsymbol{E}_s \left(\mathrm{mod}\ q\right)$，所以

$\boldsymbol{w} = \boldsymbol{Az} - \boldsymbol{T}_s\boldsymbol{c}\left(\mathrm{mod}\ q\right) = \boldsymbol{A}\left(\boldsymbol{S}_s\boldsymbol{c} + \boldsymbol{y}\right) - \left(\boldsymbol{AS}_s + \boldsymbol{E}_s\right)\cdot\boldsymbol{c}\left(\mathrm{mod}\ q\right) = \boldsymbol{Ay} - \boldsymbol{E}_s\boldsymbol{c}\left(\mathrm{mod}\ q\right)$。

又 $\boldsymbol{w}$ 的所有分量 $w_i$，$i = 1,2,\cdots,m$，都满足 $\left|[w_i]_{2^d}\right| \le 2^{d-1} - 7\omega\sigma$，所以有

$\lfloor \boldsymbol{w} \rceil_d = \lfloor \boldsymbol{Ay} - \boldsymbol{E}_s\boldsymbol{c}\left(\mathrm{mod}\ q\right)\rceil_d = \lfloor \boldsymbol{Ay}\left(\mathrm{mod}\ q\right)\rceil_d$，由此 $\boldsymbol{c} = H(\lfloor \boldsymbol{Az} - \boldsymbol{T}_s\boldsymbol{c}\left(\mathrm{mod}\ q\right)\rceil_d, \varpi)$。

根据文献[12]中舍去取样算法和高斯分布 $\mathbb{D}_\upsilon^n$ 的性质，$\boldsymbol{z}$ 以至少 $1 - 2^{-128}$ 的概率满足 $\|\boldsymbol{z}\|_2 \le B$。

综上，只要算法被正确执行，$\boldsymbol{c} = H\left(\lfloor \boldsymbol{Az} - \boldsymbol{T}_s\boldsymbol{c}\left(\mathrm{mod}\ q\right)\rceil_d, \varpi\right)$ 和 $\|\boldsymbol{z}\|_2 \le B$ 将以接近于 1 的概率成立，得到的消息 $\varpi$ 就是被加密的明文。

### 4.2 方案 1 的 IND-CPA 安全性

**定义 3**　固定向量 $\boldsymbol{s} \in \mathbb{Z}_q^n$，给出若干个对 $(\boldsymbol{a}, b = \langle \boldsymbol{a}, \boldsymbol{s} \rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$，$e$ 服从高斯分布 $\mathbb{D}_\sigma$，带错学习(Learning With Errors, LWE)问题的目标是确定 $\boldsymbol{s}$。

在本文的方案中，LWE 问题具有形式 $(\boldsymbol{A}, \boldsymbol{T}) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^{m\times n}$，其中 $\boldsymbol{T} = \boldsymbol{AS} + \boldsymbol{E}\left(\mathrm{mod}\ q\right)$，$\boldsymbol{S} \leftarrow \mathbb{D}_\sigma^{n\times n}$，$\boldsymbol{E} \leftarrow \mathbb{D}_\sigma^{m\times n}$，且矩阵 $\boldsymbol{S}$ 和 $\boldsymbol{E}$ 的所有分量都不超过 $7\sigma$。依据文献[13]，$\boldsymbol{T}$ 不服从均匀分布，但它和均匀分布是计算不可区分的，由 $\boldsymbol{A}$ 和 $\boldsymbol{T}$ 无法获知 $\boldsymbol{S}$ 的任何信息，所以此 LWE 问题是难解问题。

**定理 1**　方案 1 以 LWE 问题的难解性为基础，达到了 IND-CPA 安全性。

**证明**　我们给出一个游戏序列。

$G_0$ 是 IND-CPA 安全性定义中的游戏。

$G_1$ 在 $G_0$ 的基础上，将挑战者 CH 生成的挑战密文 $\boldsymbol{C}^* = (\mu^*, \boldsymbol{\nu}_1^*, \boldsymbol{\nu}_2^*)$ 中的 $\mu^*$ 改为对称加密算法密文空间中一个均匀随机选取的 $\tilde{\mu}$。

由理想的对称加密算法的安全性，$\mu^*$ 和均匀随机选取的 $\tilde{\mu}$ 是计算不可区分的，因此 $(\mu^*, \boldsymbol{\nu}_1^*, \boldsymbol{\nu}_2^*)$ 和 $(\tilde{\mu}, \boldsymbol{\nu}_1^*, \boldsymbol{\nu}_2^*)$ 是计算不可区分的，所以 $G_1$ 和 $G_0$ 是计算不可区分的。

$G_2$ 在 $G_1$ 的基础上，将挑战者 CH 生成的挑战密文 $\boldsymbol{C}^*=(\tilde{\mu},\boldsymbol{\nu}_1^*,\boldsymbol{\nu}_2^*)$ 中的 $\boldsymbol{\nu}_1^*$ 改为 $\mathbb{Z}_q^n$ 中的随机值 $\tilde{\boldsymbol{\nu}}_1$。

由 LWE 问题的难解性，$\boldsymbol{\nu}_1^*=-\boldsymbol{A}^{\mathrm{T}}\boldsymbol{e}_1^*+\boldsymbol{e}_2^*$ 和随机值 $\tilde{\boldsymbol{\nu}}_1$ 是计算不可区分的，所以 $(\tilde{\mu},\boldsymbol{\nu}_1^*,\boldsymbol{\nu}_2^*)$ 和 $(\tilde{\mu},\tilde{\boldsymbol{\nu}}_1,\boldsymbol{\nu}_2^*)$ 是计算不可区分的，亦即，$G_2$ 和 $G_1$ 是计算不可区分的。进而，$G_2$ 和 $G_0$ 是计算不可区分的。

$G_3$ 在 $G_2$ 的基础上，将挑战者 CH 生成的挑战密文 $\boldsymbol{C}^*=(\tilde{\mu},\tilde{\boldsymbol{\nu}}_1,\boldsymbol{\nu}_2^*)$ 中的 $\boldsymbol{\nu}_2^*$ 改为 $\mathbb{Z}_q^n$ 中的随机值 $\tilde{\boldsymbol{\nu}}_2$。

由 LWE 问题可知，$\boldsymbol{T}_r^*=\boldsymbol{A}\boldsymbol{S}_r^*+\boldsymbol{E}_r^*(\mathrm{mod}\ q)$ 和 $\mathbb{Z}_q^{m\times n}$ 中均匀随机选取的矩阵是计算不可区分的，由此 $\boldsymbol{\nu}_2^*=\boldsymbol{T}_r^{*\mathrm{T}}\boldsymbol{e}_1^*+\boldsymbol{e}_3^*+\bar{c}^{\mathrm{T}}\cdot\lfloor q/2\rfloor$ 和 $\mathbb{Z}_q^n$ 中均匀随机选取的向量是计算不可区分的，所以 $(\tilde{\mu},\tilde{\boldsymbol{\nu}}_1,\boldsymbol{\nu}_2^*)$ 和 $(\tilde{\mu},\tilde{\boldsymbol{\nu}}_1,\tilde{\boldsymbol{\nu}}_2)$ 是计算不可区分的，亦即，$G_3$ 和 $G_2$ 是计算不可区分的。进而，$G_3$ 和 $G_0$ 是计算不可区分的。

在 $G_3$ 的挑战密文 $\boldsymbol{C}^*=(\tilde{\mu},\tilde{\boldsymbol{\nu}}_1,\tilde{\boldsymbol{\nu}}_2)$ 中，$\tilde{\mu}$，$\tilde{\boldsymbol{\nu}}_1$，$\tilde{\boldsymbol{\nu}}_2$ 都是各自取值空间中的随机值，此时挑战密文 $\boldsymbol{C}^*$ 中已经不再含有关于明文 $\varpi_b$ 的任何信息，因此敌手猜对 $b$ 的优势为零。

由 $G_3$ 和 $G_0$ 的计算不可区分性，在 $G_0$ 中，敌手猜对 $b$ 的优势是可以忽略的，所以方案 1 是 IND-CPA 安全的。 证毕

## 5 无陷门格基签密方案 2

为了使无陷门格基签密方案达到IND-CCA2安全性，我们采用文献[14]的转化方法，在方案 1 的基础上构建了无陷门格基签密方案 2。 由方案 1 的 IND-CPA 安全性和文献[14]的结论，方案 2 是 IND-CCA2 安全的。方案 2 描述如下：

(1)系统设置

(a) $n$ 为系统安全参数，$\omega$ 满足 $2^{\omega}\binom{n}{\omega}\geq 2^{128}$，$m=2n$，$M$ 是一个小的正整数(比如 8)，$d$ 是一个小的正整数(比如 24)，$0<\alpha<1$，$q>2^d$，$\sigma=\alpha q$，$\upsilon=7\sigma\sqrt{n\omega}$，$B=14\sigma\sqrt{\omega}(n-1)$。

(b) $\mathbb{D}_{\sigma}=\mathbb{D}_{\sigma,0}$ 是均值为 0，标准差为 $\sigma$ 的高斯分布。$\mathbb{D}_{\upsilon}=\mathbb{D}_{\upsilon,0}$ 是均值为 0，标准差为 $\upsilon$ 的高斯分布。

(c)随机选取 $\boldsymbol{A}\leftarrow\mathbb{Z}_q^{m\times n}$，这里 $\mathbb{Z}$ 是整数的集合。

(d) $(E_k,D_k)$ 是一个安全的理想对称加密算法，密钥 $k$ 来自于空间 $\Sigma$。

(e) $H_1:\{0,1\}^*\rightarrow\Upsilon=\{\boldsymbol{v}:\boldsymbol{v}\in\{-1,0,1\}^n,\ \|\boldsymbol{v}\|_1\leq\omega\}$，$H_2:\{0,1\}^n\rightarrow\Sigma$，$H_3:\{0,1\}^*\times\{0,1\}^*\rightarrow\Pi$ 是抗碰撞的 Hash 函数，这里 $\Pi$ 是一个多次掷币空间。

(2)密钥生成算法：

(a)随机抽取矩阵 $\boldsymbol{S}\leftarrow\mathbb{D}_{\sigma}^{n\times n}$，$\boldsymbol{E}\leftarrow\mathbb{D}_{\sigma}^{m\times n}$。这里要求矩阵 $\boldsymbol{S}$ 和 $\boldsymbol{E}$ 的所有分量都不超过 $7\sigma$。如果某个分量不满足要求，重新抽取。

(b)令 $\boldsymbol{T}=\boldsymbol{A}\boldsymbol{S}+\boldsymbol{E}(\mathrm{mod}\ q)$。则 $\boldsymbol{T}$ 为用户公钥，$\boldsymbol{S}$ 为用户私钥。

(3)签密算法：消息 $\varpi$ 的发送者持有公私钥对 $(\boldsymbol{T}_s,\boldsymbol{S}_s)$，接收者持有公私钥对 $(\boldsymbol{T}_r,\boldsymbol{S}_r)$，发送者对消息 $\varpi$ 执行如下操作：

(a)随机抽取 $\boldsymbol{y}\leftarrow\mathbb{D}_{\upsilon}^n$。

(b)令 $\boldsymbol{c}=H_1\left(\lfloor\boldsymbol{A}\boldsymbol{y}\left(\mathrm{mod}\ q\right)\rceil_d,\varpi\right)$，$\boldsymbol{z}=\boldsymbol{S}_s\boldsymbol{c}+\boldsymbol{y}$。

(c)令 $\boldsymbol{w}=\boldsymbol{A}\boldsymbol{z}-\boldsymbol{T}_s\boldsymbol{c}(\mathrm{mod}\ q)$。若 $\boldsymbol{w}$ 的某个分量 $w_i$ 满足 $\left|[w_i]_{2^d}\right|>2^{d-1}-7\omega\sigma$，返回步骤(a)重新抽取 $\boldsymbol{y}$。

(d)以概率 $\min\left(\frac{\mathbb{D}_{\upsilon}^n(\boldsymbol{z})}{M\mathbb{D}_{\upsilon,\boldsymbol{S}_s\boldsymbol{c}}^n(\boldsymbol{z})},1\right)$ 保留 $(\boldsymbol{z},\boldsymbol{c})$。

(e)随机选取 $\tau\in\{0,1\}^n$，令 $\mu=E_{H_2(\tau)}(\varpi,\boldsymbol{z},\boldsymbol{c})$。

(f)令 $\eta=H_3(\tau,\mu)$，由 $\eta$ 的随机性，抽取噪声向量 $\boldsymbol{e}_1\leftarrow\mathbb{D}_{\sigma}^m$，$\boldsymbol{e}_2,\boldsymbol{e}_3\leftarrow\mathbb{D}_{\sigma}^n$，令 $\boldsymbol{\nu}_1^{\mathrm{T}}=-\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{A}+\boldsymbol{e}_2^{\mathrm{T}}$，$\boldsymbol{\nu}_2^{\mathrm{T}}=\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{T}_r+\boldsymbol{e}_3^{\mathrm{T}}+\tau\cdot\lfloor q/2\rfloor$。

则密文 $\boldsymbol{C}=(\mu,\boldsymbol{\nu}_1,\boldsymbol{\nu}_2)$。

(4)解签密算法：接收者收到密文 $\boldsymbol{C}=(\mu,\boldsymbol{\nu}_1,\boldsymbol{\nu}_2)$，他如下操作：

(a)计算 $\hat{\tau}=\boldsymbol{\nu}_1^{\mathrm{T}}\cdot\boldsymbol{S}_r+\boldsymbol{\nu}_2^{\mathrm{T}}$，则 $\hat{\tau}\in\mathbb{Z}_q^{1\times n}$。不妨设 $\hat{\tau}=(\tau_1^{'},\tau_2^{'},\cdots,\tau_n^{'})$。对 $i=1,2,\cdots,n$，如果 $\tau_i^{'}\in[-\lfloor q/4\rfloor,\lfloor q/4\rfloor)$，令 $\tau_i=0$；否则 $\tau_i=1$。则 $\tau=(\tau_1,\tau_2,\cdots,\tau_n)$。

(b)计算 $D_{H_2(\tau)}(\mu)=(\varpi,\boldsymbol{z},\boldsymbol{c})$。

(c)验证 $\boldsymbol{c}=H_1\left(\lfloor\boldsymbol{A}\boldsymbol{z}-\boldsymbol{T}_s\boldsymbol{c}(\mathrm{mod}\ q)\rceil_d,\varpi\right)$ 和 $\|\boldsymbol{z}\|_2\leq B$ 是否成立。如果都成立，接受明文 $\varpi$；否则，输出错误符号“$\perp$”。

### 5.1 方案 2 的正确性

因为 $\boldsymbol{T}_r=\boldsymbol{A}\boldsymbol{S}_r+\boldsymbol{E}_r(\mathrm{mod}\ q)$，所以

$$\begin{aligned}\hat{\tau}=(\tau_1^{'},\tau_2^{'},\cdots,\tau_n^{'})&=\boldsymbol{\nu}_1^{\mathrm{T}}\cdot\boldsymbol{S}_r+\boldsymbol{\nu}_2^{\mathrm{T}}\\&=\left(-\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{A}+\boldsymbol{e}_2^{\mathrm{T}}\right)\boldsymbol{S}_r+\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{T}_r+\boldsymbol{e}_3^{\mathrm{T}}+\tau\cdot\lfloor q/2\rfloor\\&=\left(-\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{A}+\boldsymbol{e}_2^{\mathrm{T}}\right)\boldsymbol{S}_r+\boldsymbol{e}_1^{\mathrm{T}}\left(\boldsymbol{A}\boldsymbol{S}_r+\boldsymbol{E}_r\right)+\boldsymbol{e}_3^{\mathrm{T}}+\tau\cdot\lfloor q/2\rfloor\\&=-\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{A}\boldsymbol{S}_r+\boldsymbol{e}_2^{\mathrm{T}}\boldsymbol{S}_r+\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{A}\boldsymbol{S}_r+\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{E}_r+\boldsymbol{e}_3^{\mathrm{T}}+\tau\cdot\lfloor q/2\rfloor\\&=\boldsymbol{e}_2^{\mathrm{T}}\boldsymbol{S}_r+\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{E}_r+\boldsymbol{e}_3^{\mathrm{T}}+\tau\cdot\lfloor q/2\rfloor\end{aligned}$$

$\boldsymbol{S}_r,\boldsymbol{E}_r,\boldsymbol{e}_1,\boldsymbol{e}_2,\boldsymbol{e}_3$ 的分量都取自 $\mathbb{D}_{\sigma}$，所以若 $\tau_i^{'}\in[-\lfloor q/4\rfloor,\lfloor q/4\rfloor)$，则 $\tau_i=0$；否则 $\tau_i=1$。由此可还原 $\tau$。

由对称加密算法 $(E_k,D_k)$ 的正确性，通过 $D_{H_2(\tau)}(\mu)$ 可正确还原 $(\varpi,\boldsymbol{z},\boldsymbol{c})$。

因为 $\boldsymbol{T}_s=\boldsymbol{A}\boldsymbol{S}_s+\boldsymbol{E}_s(\mathrm{mod}\ q)$，所以

$\boldsymbol{w}=\boldsymbol{A}\boldsymbol{z}-\boldsymbol{T}_s\boldsymbol{c}(\mathrm{mod}\ q)=\boldsymbol{A}\left(\boldsymbol{S}_s\boldsymbol{c}+\boldsymbol{y}\right)-\left(\boldsymbol{A}\boldsymbol{S}_s+\boldsymbol{E}_s\right)\cdot\boldsymbol{c}(\mathrm{mod}\ q)=\boldsymbol{A}\boldsymbol{y}-\boldsymbol{E}_s\boldsymbol{c}(\mathrm{mod}\ q)$。

又 $\boldsymbol{w}$ 的所有分量 $w_i$，$i=1,2,\cdots,m$，都满足 $\left|[w_i]_{2^d}\right|\leq 2^{d-1}-7\omega\sigma$，所以有

$\lfloor \boldsymbol{w} \rceil_d = \lfloor \boldsymbol{Ay} - \boldsymbol{E}_s\boldsymbol{c} (\mathrm{mod}\ q) \rceil_d = \lfloor \boldsymbol{Ay} (\mathrm{mod}\ q) \rceil_d$

由此，$\boldsymbol{c} = H_1\left(\lfloor \boldsymbol{Az} - \boldsymbol{T}_s\boldsymbol{c} (\mathrm{mod}\ q) \rceil_d, \varpi\right)$。

根据文献[12]中舍去取样算法和高斯分布 $\mathbb{D}_v^n$ 的性质，$\boldsymbol{z}$ 以至少 $1-2^{-128}$ 的概率满足 $\|\boldsymbol{z}\|_2 \le B$。

综上，只要算法被正确执行，$\boldsymbol{c} = H_1\left(\lfloor \boldsymbol{Az} - \boldsymbol{T}_s\boldsymbol{c} (\mathrm{mod}\ q) \rceil_d, \varpi\right)$ 和 $\|\boldsymbol{z}\|_2 \le B$ 将以接近于 1 的概率成立，得到的消息 $\varpi$ 就是被加密的明文。

### 5.2 方案 2 的 IND-CCA2 安全性

**定义 4**　给出若干个对 $(\boldsymbol{a}, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$，判定性 LWE 问题判定 $b$ 是下列哪种情况：

(1)服从均匀分布。(2) $b = \langle \boldsymbol{a}, \boldsymbol{s} \rangle + e$，$\boldsymbol{s}$ 服从高斯分布 $\mathbb{D}_\sigma^n$，$e$ 服从高斯分布 $\mathbb{D}_\sigma$。

**定理 2**　方案 2 以判定性 LWE 问题的难解性为基础，达到了 IND-CCA2 安全性。

**证明**　挑战者 CH 随机选取 $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{m\times n}$，从预言机 $\boldsymbol{O}$ 处获得 $\boldsymbol{T}^* \in \mathbb{Z}_q^{m\times n}$，$\boldsymbol{T}^*$ 满足如下两种情况之一：

(1)服从均匀分布。

(2)存在 $\boldsymbol{S}^* \leftarrow \mathbb{D}_\sigma^{n\times n}$，$\boldsymbol{E}^* \leftarrow \mathbb{D}_\sigma^{m\times n}$，矩阵 $\boldsymbol{S}^*$ 和 $\boldsymbol{E}^*$ 的所有分量都不超过 $7\sigma$，$\boldsymbol{T}^* = \boldsymbol{AS}^* + \boldsymbol{E}^* (\mathrm{mod}\ q)$。

如果存在敌手 AD 能够攻破方案 2 的 IND-CCA2 安全性，则挑战者 CH 可以借助敌手 AD 的攻击能力，判断出 $\boldsymbol{T}^*$ 是上述情况(1)还是情况(2)，从而解决判定性 LWE 问题。

**初始阶段**　挑战者 CH 令 $\boldsymbol{T}^*$ 为接收者的公钥，发送给敌手 AD。

**阶段 1**　敌手 AD 自适应地执行多项式有界次数的如下查询。

(1)对 $(\varpi, \boldsymbol{T}_s, \boldsymbol{S}_s)$ 的 $H_1$ 查询：AD 发送消息 $\varpi$ 和公私钥为 $(\boldsymbol{T}_s, \boldsymbol{S}_s)$ 的消息发送者给 CH。CH 随机抽取 $\boldsymbol{z} \leftarrow \mathbb{D}_v^n$，$\boldsymbol{c} \in \Upsilon$。令 $\boldsymbol{w} = \boldsymbol{Az} - \boldsymbol{T}_s\boldsymbol{c} (\mathrm{mod}\ q)$。如果 $\boldsymbol{w}$ 的某个分量 $w_j$ 满足 $\left|[w_j]_{2^d}\right| > 2^{d-1} - 7\omega\sigma$，重新抽取 $(\boldsymbol{z}, \boldsymbol{c})$。否则，令 $\boldsymbol{c} = H_1\left(\lfloor \boldsymbol{Az} - \boldsymbol{T}_s\boldsymbol{c} (\mathrm{mod}\ q) \rceil_d, \varpi\right)$，在 $H_1$ 列表中保存记录 $(\varpi, \boldsymbol{T}_s, \boldsymbol{S}_s, \boldsymbol{z}, \boldsymbol{c})$，返回 $\boldsymbol{c}$ 给敌手 AD。

(2)对 $\tau$ 的 $H_2$ 查询：CH 随机抽取 $h_{2_\tau} \leftarrow \Sigma$，令 $h_{2_\tau} = H_2(\tau)$，在 $H_2$ 列表中保存记录 $(\tau, h_{2_\tau})$，返回 $h_{2_\tau}$ 给敌手 AD。

(3)对 $(\tau, \mu)$ 的 $H_3$ 查询：CH 随机抽取 $h_{\tau,\mu} \leftarrow \Pi$，令 $h_{\tau,\mu} = H_3(\tau, \mu)$，在 $H_3$ 列表中保存记录 $(\tau, \mu, h_{\tau,\mu})$，返回 $h_{\tau,\mu}$ 给敌手 AD。

(4)对 $(\boldsymbol{T}_s, \boldsymbol{S}_s, \mu, \boldsymbol{\nu}_1, \boldsymbol{\nu}_2)$ 的解签密查询：对公私钥对为 $(\boldsymbol{T}_s, \boldsymbol{S}_s)$ 的发送者和密文 $\boldsymbol{C} = (\mu, \boldsymbol{\nu}_1, \boldsymbol{\nu}_2)$，挑战者 CH 遍历 $H_1$，$H_2$ 和 $H_3$ 列表查找 $(\varpi, \boldsymbol{T}_s, \boldsymbol{S}_s, \boldsymbol{z}, \boldsymbol{c})$，$(\tau, h_{2_\tau})$ 和 $(\tau, \mu, h_{\tau,\mu})$，使之满足如下关系：

(a) $\mu = E_{h_{2_\tau}}(\varpi, \boldsymbol{z}, \boldsymbol{c})$。

(b)由 $h_{\tau,\mu}$ 的随机性，抽取噪声向量 $\boldsymbol{e}_1 \leftarrow \mathbb{D}_\sigma^m$，$\boldsymbol{e}_2, \boldsymbol{e}_3 \leftarrow \mathbb{D}_\sigma^n$ 后，$\boldsymbol{\nu}_1^{\mathrm{T}} = -\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_2^{\mathrm{T}}$，$\boldsymbol{\nu}_2^{\mathrm{T}} = \boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{T}^* + \boldsymbol{e}_3^{\mathrm{T}} + \tau \cdot \lfloor q/2 \rfloor$。

如果这样的元组存在，返回 $\varpi$。否则输出 $\perp$ 并拒绝。

**挑战阶段**　由敌手 AD 来决定阶段 1 何时结束，然后敌手 AD 选择两个相同长度的明文 $\varpi_0$ 和 $\varpi_1$，和公私钥对为 $(\boldsymbol{T}_s^*, \boldsymbol{S}_s^*)$ 的消息发送者给挑战者 CH。CH 随机选择 $b \in \{0,1\}$，执行如下操作：

(1)随机抽取 $\boldsymbol{y} \leftarrow \mathbb{D}_v^n$。

(2)令 $\boldsymbol{c} = H_1\left(\lfloor \boldsymbol{Ay} (\mathrm{mod}\ q) \rceil_d, \varpi_b\right)$，$\boldsymbol{z} = \boldsymbol{S}_s^*\boldsymbol{c} + \boldsymbol{y}$。

(3)令 $\boldsymbol{w} = \boldsymbol{Az} - \boldsymbol{T}_s^*\boldsymbol{c} (\mathrm{mod}\ q)$。若 $\boldsymbol{w}$ 的某个分量 $w_i$ 满足 $\left|[w_i]_{2^d}\right| > 2^{d-1} - 7\omega\sigma$，返回步骤(1)重新抽取 $\boldsymbol{y}$。

(4)以概率 $\min\left(\dfrac{\mathbb{D}_v^n(\boldsymbol{z})}{M\mathbb{D}_{v,\boldsymbol{S}_s^*\boldsymbol{c}}^n(\boldsymbol{z})}, 1\right)$ 保留 $(\boldsymbol{z}, \boldsymbol{c})$。

(5)随机选取 $\tau \in \{0,1\}^n$，令 $\mu^* = E_{H_2(\tau)}(\varpi_b, \boldsymbol{z}, \boldsymbol{c})$。

(6)令 $\eta = H_3(\tau, \mu^*)$，由 $\eta$ 的随机性，抽取噪声向量 $\boldsymbol{e}_1 \leftarrow \mathbb{D}_\sigma^m$，$\boldsymbol{e}_2, \boldsymbol{e}_3 \leftarrow \mathbb{D}_\sigma^n$，令 $\boldsymbol{\nu}_1^{*\mathrm{T}} = -\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{A} + \boldsymbol{e}_2^{\mathrm{T}}$，$\boldsymbol{\nu}_2^{*\mathrm{T}} = \boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{T}^* + \boldsymbol{e}_3^{\mathrm{T}} + \tau \cdot \lfloor q/2 \rfloor$。

最后，CH 将密文 $(\mu^*, \boldsymbol{\nu}_1^*, \boldsymbol{\nu}_2^*)$ 返回敌手 AD。

**阶段 2**　敌手 AD 重复阶段 1 的操作，但他不能对 $(\boldsymbol{T}_s^*, \boldsymbol{S}_s^*, \mu^*, \boldsymbol{\nu}_1^*, \boldsymbol{\nu}_2^*)$ 进行解签密查询。

**猜测阶段**　敌手 AD 给出他对 $b$ 的猜测 $b'$，返回给 CH。如果 $b = b'$，CH 获知存在 $\boldsymbol{S}^* \leftarrow \mathbb{D}_\sigma^{n\times n}$，$\boldsymbol{E}^* \leftarrow \mathbb{D}_\sigma^{m\times n}$，矩阵 $\boldsymbol{S}^*$ 和 $\boldsymbol{E}^*$ 的所有分量都不超过 $7\sigma$，使得 $\boldsymbol{T}^* = \boldsymbol{AS}^* + \boldsymbol{E}^* (\mathrm{mod}\ q)$。否则，CH 获知 $\boldsymbol{T}^*$ 服从均匀分布。从而判定性 LWE 问题实例 $(\boldsymbol{A}, \boldsymbol{T}^*)$ 获得求解。　　证毕

### 5.3 方案 2 的 EUF-CMA 安全性

**定理 3**　方案 2 以 SIS 问题的难解性为基础，达到了 EUF-CMA 安全性。

**证明**　令 $\boldsymbol{A}' = (\boldsymbol{A} | \boldsymbol{I}_m) \in \mathbb{Z}_q^{m\times(n+m)}$ 是一个 SIS 问题实例，如果存在敌手 FG 能够以不可忽略的概率攻击方案 2 的 EUF-CMA 安全性，则挑战者 CH 可以找到非零短向量 $\boldsymbol{e}' \in \mathbb{Z}^n$，$\boldsymbol{e}'' \in \mathbb{Z}^m$，使得 $\boldsymbol{Ae}' + \boldsymbol{e}'' = \boldsymbol{0} (\mathrm{mod}\ q)$。挑战者 CH 和敌手 FG 进行如下交互。

**初始阶段**　CH 随机抽取矩阵 $\boldsymbol{S}_s^* \leftarrow \mathbb{D}_\sigma^{n\times n}$，$\boldsymbol{E}_s^* \leftarrow \mathbb{D}_\sigma^{m\times n}$。这里矩阵 $\boldsymbol{S}_s^*$ 和 $\boldsymbol{E}_s^*$ 的所有分量都不超过 $7\sigma$。令 $\boldsymbol{T}_s^* = \boldsymbol{AS}_s^* + \boldsymbol{E}_s^* (\mathrm{mod}\ q)$，则 $\boldsymbol{T}_s^*$ 为用户公钥，$\boldsymbol{S}_s^*$ 为用户私钥。CH 将 $\boldsymbol{T}_s^*$ 发送给 FG，保密 $\boldsymbol{S}_s^*$。

**攻击阶段**　FG 自适应地执行多项式有界次数的如下查询。

(1)对 $\varpi_i$ 的 $H_1$ 查询：　FG 发送消息 $\varpi_i$ 给 CH。CH 随机选取 $\boldsymbol{z}_i \leftarrow \mathbb{D}_v^n$，$\boldsymbol{c}_i \in \Upsilon$，令 $\boldsymbol{w} = \boldsymbol{Az}_i -$

$\boldsymbol{T}_s^*\boldsymbol{c}_i \pmod q$。如果 $\boldsymbol{w}$ 的某个分量 $w_j$ 满足 $\left|\left[w_j\right]_{2^d}\right| > 2^{d-1}-7\omega\sigma$，重新抽取 $(\boldsymbol{z}_i,\boldsymbol{c}_i)$。否则，令 $\boldsymbol{c}_i = H_1\left(\lfloor \boldsymbol{A}\boldsymbol{z}_i - \boldsymbol{T}_s^*\boldsymbol{c}_i \pmod q \rceil_d, \varpi_i\right)$，在 $H_1$ 列表中保存记录 $(\varpi_i,\boldsymbol{z}_i,\boldsymbol{c}_i)$，返回 $\boldsymbol{c}_i$ 给敌手 FG。

(2)签密查询：FG 发送消息 $\varpi_i$ 和接收者的公私钥对 $(\boldsymbol{T}_r,\boldsymbol{S}_r)$ 给 CH。CH 首先对 $\varpi_i$ 执行 $H_1$ 查询，获得 $(\boldsymbol{z}_i,\boldsymbol{c}_i)$。然后随机选取 $\tau\in\{0,1\}^n$，令 $\mu=E_{H_2(\tau)}(\varpi_i,\boldsymbol{z}_i,\boldsymbol{c}_i)$，$\eta=H_3(\tau,\mu)$。由 $\eta$ 的随机性，抽取噪声向量 $\boldsymbol{e}_1\leftarrow\mathbb{D}_\sigma^m$，$\boldsymbol{e}_2,\boldsymbol{e}_3\leftarrow\mathbb{D}_\sigma^n$，令 $\boldsymbol{\nu}_1^{\mathrm{T}}=-\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{A}+\boldsymbol{e}_2^{\mathrm{T}}$，$\boldsymbol{\nu}_2^{\mathrm{T}}=\boldsymbol{e}_1^{\mathrm{T}}\boldsymbol{T}_r+\boldsymbol{e}_3^{\mathrm{T}}+\tau\cdot\lfloor q/2\rfloor$。CH 返回密文 $\boldsymbol{C}=(\mu,\boldsymbol{\nu}_1,\boldsymbol{\nu}_2)$ 给敌手 FG。

**伪造阶段** FG 选定接收者的公私钥对 $(\boldsymbol{T}_r^*,\boldsymbol{S}_r^*)$ 和消息 $\varpi^*$，创建初始阶段指定发送者的合法密文 $\boldsymbol{C}^*=(\mu^*,\boldsymbol{\nu}_1^*,\boldsymbol{\nu}_2^*)$。

CH 借助 $\boldsymbol{S}_r^*$ 解签密 $\boldsymbol{C}^*$ 获得 $(\varpi^*,\boldsymbol{z}^*,\boldsymbol{c}^*)$。CH 对 $\varpi^*$ 执行 $H_1$ 查询，由分叉引理[15]，获得 $(\varpi^*,\overline{\boldsymbol{z}},\overline{\boldsymbol{c}})$ 且 $\boldsymbol{c}^*\neq\overline{\boldsymbol{c}}$。此时，$\lfloor \boldsymbol{A}\boldsymbol{z}^*-\boldsymbol{T}_s^*\boldsymbol{c}^* \pmod q\rceil_d = \lfloor \boldsymbol{A}\overline{\boldsymbol{z}}-\boldsymbol{T}_s^*\overline{\boldsymbol{c}} \pmod q\rceil_d$，所以，$\boldsymbol{A}\boldsymbol{z}^*-\boldsymbol{T}_s^*\boldsymbol{c}^*+\boldsymbol{e}^*=\boldsymbol{A}\overline{\boldsymbol{z}}-\boldsymbol{T}_s^*\overline{\boldsymbol{c}} \pmod q$，这里 $\left\|\boldsymbol{e}^*\right\|_\infty\le 2^{d-1}$。因为 $\boldsymbol{T}_s^*=\boldsymbol{A}\boldsymbol{S}_s^*+\boldsymbol{E}_s^* \pmod q$，可得 $\boldsymbol{A}(\boldsymbol{z}^*-\overline{\boldsymbol{z}}+\boldsymbol{S}_s^*(\overline{\boldsymbol{c}}-\boldsymbol{c}^*))+\boldsymbol{e}^*+\boldsymbol{E}_s^*(\overline{\boldsymbol{c}}-\boldsymbol{c}^*)=\boldsymbol{0} \pmod q$。令 $\boldsymbol{e}'=\boldsymbol{z}^*-\overline{\boldsymbol{z}}+\boldsymbol{S}_s^*(\overline{\boldsymbol{c}}-\boldsymbol{c}^*)$，$\boldsymbol{e}''=\boldsymbol{e}^*+\boldsymbol{E}_s^*(\overline{\boldsymbol{c}}-\boldsymbol{c}^*)$，则 $\left\|\boldsymbol{e}'\right\|_\infty\le 2B+14\sigma\omega$，$\left\|\boldsymbol{e}''\right\|_\infty\le 2^{d-1}+14\sigma\omega$。

此外，由于 $\boldsymbol{S}_s^*$ 和 $\boldsymbol{E}_s^*$ 不唯一，敌手无法确定 $\boldsymbol{S}_s^*$ 和 $\boldsymbol{E}_s^*$。因此，至少以 1/2 的概率，$(\boldsymbol{e}',\boldsymbol{e}'')\neq(\boldsymbol{0},\boldsymbol{0})$。

证毕

### 5.4 方案 2 的效率分析

取定安全参数 $n$，$q=\mathrm{poly}(n)$，表 1 给出了文献[8–11]中效率最高的文献[10]中的方案和方案 2 的效率对比，比较项涵盖了方案的空间和时间需求。其中，参数 $m$ 以 1 为单位，公钥尺寸、私钥尺寸和密文增量以 bit 为单位，签密运算量、解签密运算量以基本运算次数计数。$S_p$ 表示原像取样算法，$S_d$ 表示高斯抽样算法，$M_v$ 表示矩阵向量乘法。在运算量的统计中，忽略了 Hash 函数运算、异或运算、加法运算等低能耗运算。因为对称加解密算法的运算量比公钥密码算法的运算量低很多，因此在运算量的统计中，我们也忽略了对称加解密算法的运算量。由表 1 的对比结果，方案 2 具有更小的空间需求和时间需求。

**表 1 与文献[10]的效率对比**

| | 文献[10] | 方案 2 |
|---|---|---|
| 参数 $m$ | $\lceil 2n\lg q\rceil$ | $2n$ |
| 公钥尺寸 | $2n^2\lg^2 q$ | $2n^2\lg q$ |
| 私钥尺寸 | $\frac{1}{2}n^2\lg^2 q\lg(\lg n)$ | $n^2\lg q$ |
| 密文增量 | $n(3\lg q+2\lg 2q+3)\lg q$ | $2n\lg q$ |
| 签密运算量 | $S_p+5S_d+3M_v$ | $4S_d+6M_v$ |
| 解签密运算量 | $6M_v$ | $3M_v$ |

## 6 结束语

陷门产生算法和原像取样算法的计算复杂度是影响格基密码实用性的重要因素。本文提出的格基签密方案，使用了无陷门签名技术和基于 LWE 问题的加密方法，避免了陷门产生算法和原像取样算法的使用，提高了方案的运算效率，高效地保证了量子计算机环境下信息传输的机密性和认证性。在本文方案的基础上研究代理签密，多接收者签密，聚合签密等具有特殊应用需求的高效签密方案的设计，将是下一步的研究内容。

## 参 考 文 献


[1] ZHENG Y. Digital signcryption or how to achieve cost (signature+encryption)<<cost(signature)+cost(encryption) [C]. CRYPTO 1997, California, USA, 1997: 165–179.

[2] MALONE-LEE J and MAO W. Two birds one stone: signcryption using rsa[C]. Proceedings of the 2003 RSA conference on The Cryptographers' track, San Francisco, USA, 2003: 211–226.

[3] LI Fagen and TAKAGI T. Secure identity-based signcryption in the standard model[J]. *Mathematical and Computer Modelling*, 2013, 57(11/12): 2685–2694.

[4] LU Y and LI J. Efficient certificate-based signcryption secure against public key replacement attacks and insider attacks[J]. *The Scientific World Journal*, 2014, Article ID 295419.

[5] Shor P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. *SIAM Journal on Computing*, 1997, 26(5): 1484–1509.

[6] 杨孝鹏, 马文平, 张成丽. 一种新型基于环上带误差学习问题的认证密钥交换方案[J]. 电子与信息学报, 2015, 37(8): 1984–1988.
YANG Xiaopeng, MA Wenping, and ZHANG Chengli. New authenticated key exchange scheme based on ring learning with errors problem[J]. *Journal of Electronics & Information Technology*, 2015, 37(8): 1984–1988.

[7] 张彦华, 胡予濮, 江明明, 等. 格上可撤销的基于身份的适应性安全的加密方案[J]. 电子与信息学报, 2015, 37(2): 423–428.
ZHANG Yanhua, HU Yupu, JIANG Mingming, *et al*. A lattice-based revocable adaptive-id secure encryption scheme [J]. *Journal of Electronics & Information Technology*, 2015,

37(2): 423–428.

[8] WANG Fenghe, HU Yupu, and WANG Chunxiao. Post-quantum secure hybrid signcryption from lattice assumption[J]. *Applied Mathematics & Information Sciences*, 2012, 6(1): 23–28.

[9] LI Fagen, BIN MUHAVA F T, KHAN M K, *et al*. Lattice-based signcryption[J]. *Concurrency and Computation: Practice and Experience*, 2013, 25(14): 2112–2122.

[10] YAN Jianhua, WANG Licheng, YANG Yixian, *et al*. Efficient lattice-based signcryption in standard model[J]. *Mathematical Problems in Engineering*, 2013, Article ID 702539.

[11] LU Xiuhua, WEN Qiaoyan, JIN Zhengping, *et al*. A lattice-based signcryption scheme without random oracles[J]. *Frontiers of Computer Science*, 2014, 8(4): 667–675.

[12] LYUBASHEVSKY V. Lattice signatures without trapdoors [C]. EUROCRYPT 2012, Cambridge, USA, 2012: 738–755.

[13] BAI Shi and GALBRAITH S D. An improved compression technique for signatures based on learning with errors[C]. CT-RSA 2014, San Francisco, USA, 2014: 28–47.

[14] FUJISAKI E and OKAMOTO T. Secure integration of asymmetric and symmetric encryption schemes[J]. *Journal of Cryptology*, 2013, 26(1): 80–101.

[15] BELLARE M and NEVEN G. Multi-signatures in the plain public-key model and a general forking lemma[C]. Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, USA, 2006: 390–399.

路秀华： 女，1979 年生，副教授，博士生，研究方向为基于格的公钥密码学.

温巧燕： 女，1959 年生，教授，研究方向为密码学和信息安全.

王励成： 男，1971 年生，副教授，研究方向为密码学和网络安全.

杜 蛟： 男，1978 年生，讲师，博士，研究方向为密码学与应用数学.