

文章编号:1001-9081(2016)04-0956-06

DOI:10.11772/j.issn.1001-9081.2016.04.0956

格上基于身份的广播加密方案

黄文真*, 杨晓元, 王绪安, 吴立强

(武警工程大学 电子技术系, 西安 710086)

(*通信作者电子邮箱 450814714@qq.com)

摘要:针对 Wang 等(WANG J, BI J. Lattice-based identity-based broadcast encryption. <https://eprint.iacr.org/2010/288.pdf>)在随机预言机下提出的格基广播加密方案安全性较低且实用性较差的问题,利用盆景树扩展控制算法和一次签名算法构造了一个标准模型下基于格上错误学习(LWE)问题的身份基广播加密方案。首先利用一个编码函数替换随机预言机,将方案置于标准模型下;然后运行盆景树扩展控制算法生成用户的私钥和广播公钥;最后在加密阶段加入一次签名算法,提高方案的安全性。分析表明,相对于已有同类方案,新方案安全性较高达到了适应性攻击下选择密文安全(IND-ID-CCA)且方案具有动态扩展特性,能够通过用户身份矩阵的伸缩来实现用户的添加或删除,因此实用性较强。

关键词:身份基广播加密; 错误学习; 盆景树扩展控制算法; 一次签名算法; 适应性攻击下选择密文安全

中图分类号:TP309.7 文献标志码:A

Identity-based broadcast encryption based on lattice

HUANG Wenzhen*, YANG Xiaoyuan, WANG Xu'an, WU Liqiang

(Department of Electronic Technology, Engineering University of CAPF, Xi'an Shaanxi 710086, China)

Abstract: Focusing on the issue of low security and poor practicability in the lattice-based broadcast encryption scheme proposed by Wang et al. (WANG J, BI J. Lattice-based identity-based broadcast encryption. <https://eprint.iacr.org/2010/288.pdf>) in the random oracle, an identity-based broadcast encryption scheme based on Learning With Errors (LWE) in the standard model was constructed by expanding control algorithm of bonsai tree and one-time signature algorithm. Firstly, the random oracle was replaced by a coding function to make the scheme be in the standard model. Then, the bonsai tree expanding control algorithm was used to generate the private keys of users and public key. Finally, the one-time signature algorithm was added to improve the security. Analysis shows that compared with existed similar schemes, the scheme gets stronger security, achieves adaptively indistinguishable-chosen ciphertext attack security with dynamic extension, which means the users can be added or deleted by expanding or contracting the identity matrix. Hence it has strong practicability.

Key words: identity-based broadcast encryption; Learning With Error (LWE); bonsai tree expanding control algorithm; one-time signature algorithm; adaptively indistinguishable-chosen ciphertext attack security

0 引言

有别于一对一的加密通信方式,广播加密(Broadcast Encryption, BE)^[1]实现的是在公共信道中进行一对多的加密通信。加密方对消息进行加密后,通过公共信道传输给一组接收方,接收方中只有经过授权的用户才能够对密文进行解密从而还原出消息。在实际应用中,广播加密已经被应用到许多领域,例如付费电视节目、版权保护、流媒体等。自 Amos 等^[1]提出广播加密的概念后,很多密码学者开始致力于广播加密的研究中。近十年以来,关于广播加密的优秀理论研究成果有很多,其中比较具有代表性的是:BGW(Boneh-Gentry-Waters)方案^[2],该方案使用双线性对实现了固定的密文长度以及固定的私钥长度,保证了较低的存储代价以及传输代价,但公钥的尺寸比较大,与用户的数量之间呈线性关系递

增。

基于身份的加密(Identity-Based Encryption, IBE)体制最早由 Adi^[3]提出,目的是为了简化电子邮件的传输。IBE 体制以其较为简便的密钥管理优势,克服了传统公钥基础设施(Public Key Infrastructure, PKI)密钥管理复杂的问题,逐步地走向实际应用中。

基于身份的加密体制与广播加密体制的结合形成了基于身份的广播加密体制,也称身份基广播加密(Identity-Based Broadcast Encryption, IBBE)。Cécile^[4]最早给出身份基广播加密的形式化定义并提出一个具有动态特性的方案,克服了 BGW 方案的弱点降低了公钥的存储代价。IBBE 与 IBE 密切相关,当广播群组的用户数目 $N=1$ 时,IBBE 就退化成 IBE。

随着量子计算机的出现,传统密码体制受到了严重的威胁,格密码^[5]以其高效的运算速度且具有抗量子攻击的优良

收稿日期:2015-09-15;修回日期:2015-11-10。

基金项目:国家自然科学基金资助项目(61272492);陕西省自然科学基础研究计划项目(2015JM6353, 2014JM8300)。

作者简介:黄文真(1991—),男,福建漳州人,硕士研究生,主要研究方向:广播加密、格密码、多线性映射、基于身份密码; 杨晓元(1959—),男,湖南湘潭人,教授,硕士,主要研究方向:椭圆曲线密码、格密码、代理重加密; 王绪安(1981—),男,湖北荆州人,副教授,博士研究生,主要研究方向:代理重加密、基于身份密码; 吴立强(1986—),男,陕西商洛人,讲师,硕士,主要研究方向:格密码、基于身份密码。

特性为公钥密码注入了活力,引起了学者的广泛关注,成为近几年密码学的研究热点之一。特别是2005年以后,关于格的新方法、新思想、新理论层出不穷。2010年,Wang等^[6]在格上构造了一个IBBE方案,该方案在密钥的构造上方法灵活,使用用户身份的扩展格作为公钥,密钥的代价较小。2011年,Li等^[7]基于错误学习(Learn With Errors, LWE)问题设计了一个格上可证明安全的基于群组的广播加密方案,但效率并不高。2012年,张伟仁等^[8]构造了一个格上新的身份类广播加密方案,该方案具有动态特性,计算效率较高,但公钥尺寸较大。2013年,Adela^[9]将Benoit等^[10]构造的匿名广播加密方案置于格的环境下设计了一个具有匿名性质的格基广播加密方案。为了实现匿名性,该方案使用两种密码学原语来构建密码方案:一种是安全性基于R-LWE的基于标签的提示系统,另一种是基于LWE的具有不可区分选择密文攻击(Indistinguishable-Chosen Ciphertext Attack, IND-CCA)安全的公钥加密系统。2015年,Zhang等^[11]将前向安全机制应用到广播加密中,提出了一个具有前向安全的基于格的身份类广播加密方案。

本文基于Wang等^[6]构造的适应性攻击下选择明文安全的方案,结合盆景树扩展控制算法和一次签名算法构造了一个可证明安全且具有动态特性的身份基广播加密方案。新方案利用盆景树扩展控制算法生成用户私钥,使得系统能够通过控制用户身份矩阵的伸缩来实现对用户的动态管理,且加入一次签名算法,提高了安全性,达到适应性攻击下选择密文安全。

1 预备知识

1.1 格

1.1.1 格的定义

格^[5]是一种特殊的代数结构,是由一系列的点构成的网状结构。它的定义如下:

定义1 一个n维的格A,是指由n个线性独立的向量**b₁, b₂, …, b_n**和整数的线性组合所形成的点的集合A(**b₁, b₂, …, b_n**) = { $\sum_{i \in [n]} \alpha_i b_i | \alpha_i \in \mathbb{Z}$ },其中向量**b₁, b₂, …, b_n**称作格A的一组基,记为B = [b₁, b₂, …, b_n]。

1.1.2 格上几个困难问题

基于格的密码方案是基于格上困难问题设计的,下面介绍了几个著名的格上困难问题^[12]:

1) 最短向量问题(Shortest Vector Problem, SVP)。

输入 任意一个向量a ∈ ℝⁿ和n维格A的任意一组基B。

输出 格A中的一个向量v,并且v与a之间的距离||a - v|| = λ(A, a)最短。

2) 近似最短向量问题(approximate SVP, app-SVP)。

输入 任意一个向量a ∈ ℝⁿ和n维格A的任意一组基B。

输出 格A中的一个向量v,并且v与a之间的距离||a - v|| = f(n)λ(A, a)最短,其中f(n)是关于n的多项式。

3) 最近向量问题(Closest Vector Problem, CVP)。

输入 n维格A的任意一组基B。

输出 一个非零的短向量v ∈ A,并且||v|| = λ₁(A)找到格上一点使得与给定的点在空间上距离最近。

4) 近似最短向量问题(approximate CVP, app-CVP)

输入 n维格A的任意一组基B。

输出 一个非零的短向量v ∈ A,并且||v|| = f(n)λ₁(A),其中f(n)是关于n的多项式,称为近似因子。

1.2 LWE 困难性假设

定义2 计算性LWE问题^[12]:给定参数m,n ∈ ℤ,整数q = q(n) > 2和Z上的一个高斯错误分布χ^m。(A, A^Ts + e) ∈ Z^{n × m} × Z^m,其中:A ← Z^{n × m}, s ← Zⁿ, e ← χ^m。计算性LWE问题的任务是由b = A^Ts + e还原出秘密信息s的值。

1.3 盆景树扩展控制算法

盆景树原理是由Chris^[13]提出的,主要包括未受控制生长算法、控制生长算法、扩展控制算法和随机控制,其中扩展控制算法能够实现从一个格到更高维数格的扩展。算法具体如下:

ExtBasis(S, A' = A || Ā)

1) 输入矩阵A ∈ Z^{n × m}, S ∈ Z^{n × m}, Ā ∈ Z^{n × m̄};

2) 求解AW = -Ā,并从中选取一个解W ∈ Z^{n × m̄};

3) 输出S' = [S W] ∈ Z^{m' × m'},其中I_{m × m}为单位矩阵。

定理1 存在多项式时间算法ExtBasis满足:给定一个任意的矩阵A ∈ Z^{n × m},格A[⊥](A)的任意一组基S ∈ Z^{n × n}和任意一个矩阵Ā ∈ Z^{n × m̄},算法ExtBasis(S, A' = A || Ā)输出格A[⊥](A) ⊆ Z^{m+n}的一组基S',且满足||S'|| = ||S||。

1.4 原像抽样函数

原像抽样函数(Preimage Sampleable Function, PSF)^[14]是进行格基密码方案设计强有力的工具之一。它的定义如下:

定义3 原像抽样函数PSF由以下四个多项式时间算法组成:

1) TrapGen(1ⁿ):陷门生成算法。输入安全参数1ⁿ,输出一个陷门t和f_a:D_n → ℝ_n。

2) Eval(a, x):估值算法。输入a和元素x ∈ D_n,返回一个值y = f_a(x)。

3) SampleDom(1ⁿ):具有均匀输出的域抽样算法。输入安全参数1ⁿ,从D_n分布中抽样出x。

4) SamplePre(t, y):带陷门的原像抽样算法。输入与a相关的陷门t和像y,从D_n分布中抽样出x,满足y = f_a(x)。

在此基础上,介绍通用的原像抽样算法GenSamplePre^[6],如下所示:

在不失一般性的前提下,设S = [k] = {1, 2, …, k},其中k ∈ [l]。令k₁, k₂, k₃, k₄为正整数且k = k₁ + k₂ + k₃ + k₄。记A_S = [A_{S₁} || A_{S₂} || A_{S₃} || A_{S₄}] ∈ Z^{n × km},其中:A_{S₁} ∈ Z^{n × k₁m}, A_{S₂} ∈ Z^{n × k₂m}, A_{S₃} ∈ Z^{n × k₃m}, A_{S₄} ∈ Z^{n × k₄m}, A_R = [A_{S₁} || A_{S₃}] ∈ Z^{n × (k₁+k₃)m}。给定格A[⊥](A_R)上的一个短基B_R和整数r ≥ ||B_R|| · ω(√lb(km)),算法GenSamplePre能够抽样出函数f_{A_S}(e) = A_Se mod q的原像,具体过程如下:

1) 分别从分布D_{Z^{k₂m}}和D_{Z^{k₄m}}中抽样出e_{S₂} ∈ Z^{k₂m}和e_{S₄} ∈ Z^{k₄m}。令e_{S₂} = [e_{k₁+1}, e_{k₁+2}, …, e_{k₁+k₂}] ∈ (Z^m)^{k₂}, e_{S₄} = [e_{k-k₄+1}, e_{k-k₄+2}, …, e_k] ∈ (Z^m)^{k₄}。

2) 令 $\mathbf{z} = \mathbf{y} - \mathbf{A}_{S_2}\mathbf{e}_{S_2} - \mathbf{A}_{S_4}\mathbf{e}_{S_4}$, 运行 $\mathbf{e}_R \leftarrow \text{SamplePre}(\mathbf{A}_R, \mathbf{B}_R, \mathbf{z}, r)$, 从分布 $D_{\mathbf{A}_y^\perp(\mathbf{A}_s, r)}$ 中抽样出一个向量 $\mathbf{e}_R \in \mathbf{Z}^{(k_1+k_3)m}$, 令:

$$\mathbf{e}_R = [\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_{k_1}, \mathbf{e}_{k_1+k_2+1}, \dots, \mathbf{e}_{k-k_4}] \in (\mathbf{Z}^m)^{k_1+k_3}$$

$$\mathbf{e}_{S_1} = [\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_{k_1}] \in (\mathbf{Z}^m)^{k_1}$$

$$\mathbf{e}_{S_3} = [\mathbf{e}_{k_1+k_2+1}, \mathbf{e}_{k_1+k_2+2}, \dots, \mathbf{e}_{k-k_4}] \in (\mathbf{Z}^m)^{k_3}$$

$$3) \text{ 输出 } \mathbf{e} \in \mathbf{Z}^{km}, \mathbf{e} = [\mathbf{e}, \mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_k].$$

定理 2 令 n, q, m, k 为正整数, 且 $q \geq 2, m \geq 2n \ln q$ 。存在一个算法 GenSamplePre, 输入 $\mathbf{A}_s \in \mathbf{Z}_q^{n \times km}, R \subseteq [k]$, 格 $\Lambda^\perp(\mathbf{A}_R)$ 的一组基 \mathbf{B}_R , 向量 $\mathbf{y} \in \mathbf{Z}_q^n$ 和整数 $r \geq \|\mathbf{B}_R\| \cdot \omega(\sqrt{\ln(km)})$, 得 $\mathbf{e} \leftarrow \text{GenSamplePre}(\mathbf{B}_R, \mathbf{A}_s, \mathbf{A}_R, \mathbf{y}, r)$ 。对于绝大多数满足条件的 $\mathbf{A}_s \in \mathbf{Z}^{n \times km}$ 而言, \mathbf{e} 的采样与分布 $D_{\mathbf{A}_y^\perp(\mathbf{A}_s, r)}$ 在统计距离上是不可区分的。

1.5 强不可伪造一次签名算法

一个签名算法 $\text{SS} = (\text{KG}, \text{Sign}, \text{Vrfy})$ 通常包括公私钥生成算法、签名算法和验证算法, 如下所示:

1) $\text{KG}(1^k)$: 公私钥生成算法。输入系统的安全参数 1^k , 输出公私钥对 $(\text{sign}_k, \text{vk}), \text{vk}$ 用于验证, sign_k 用于签名。

2) $\text{Sign}(\text{sign}_k, m)$: 签名算法。输入签名的消息 m 和签名私钥 sign_k , 输出签名 σ 。

3) $\text{Vrfy}(m, \sigma, \text{vk})$: 验证算法。输入消息 m 、签名 σ 和验证公钥 vk , 输出 $b \in \{0, 1\}$ 。若验证成功, 则输出 1; 否则输出 0。

下面定义强不可伪造一次签名算法 OTS($\text{KG}, \text{Sign}, \text{Vrfy}$), 它是通过攻击者 \mathcal{A} 与挑战者 \mathcal{C} 直接的游戏来定义的:

1) 初始化阶段: 挑战者 \mathcal{C} 运行 $\text{KG}(1^k)$ 来获取验证公钥 vk 和签名私钥 sign_k , \mathcal{A} 获得验证公钥 vk 。

2) 询问阶段: 攻击者 \mathcal{A} 至多获得一次对 m 的签名询问, 挑战者 \mathcal{C} 返回 $\sigma \leftarrow \text{Sign}(\text{sign}_k, m)$ 。

3) 伪造阶段: 攻击者 \mathcal{A} 输出 (m^*, σ^*) , 其中 $(m^*, \sigma^*) \neq (m, \sigma)$ 。

以上攻击者伪造成功, 即 $\text{Vrfy}(m^*, \sigma^*, \text{vk}) = 1$ 的概率记为 $\text{AdvOTS}_{\mathcal{A}}$, 若对于所有 τ 时间的攻击者 \mathcal{A} , 满足 $\text{AdvOTS}_{\mathcal{A}} < \varepsilon$, 则称该签名体制 (τ, ε) 为强不可伪造一次签名。

2 基于身份广播加密定义及安全模型

2.1 基于身份广播加密定义

身份基广播加密(IBE)是基于身份加密(IBE)体制的一种延伸。特别地, 当 IBE 体制中的一次加密的最大用户数 $m=1$ 时, IBE 就变成了 IBE。

通常, 一个 IBE 方案由四个算法构成:

1) $\text{Setup}(\lambda, m)$: 输入安全参数 λ 和一次加密的最大用户数目 m , 输出主密钥 MSK 以及公钥 PK 。其中主密钥 MSK 由私钥生成器(Private Key Generator, PKG)掌握, 公钥 PK 公开。

2) $\text{Extract}(ID_i, \text{MSK})$: 输入主密钥 MSK 和用户的身份 ID_i , 私钥生成中心 PKG 运行私钥提取算法, 生成与用户身份相相应的私钥 sk_{ID_i} 。

3) $\text{Encrypt}(S, \text{PK}, M)$: 给定一组接收者身份集合 S , 输入公钥 PK , 广播者运行加密算法, 首先利用加密密钥 K 对消息 M 进行加密形成密文主体 C_M ; 然后对加密密钥 K 进行封装,

形成密文头部 Hdr , 最终的密文 C 由两部分组成即 (Hdr, C_M) ; 最后将密文 C 发送给接收用户。

4) $\text{Decrypt}(S, ID_i, sk_{ID_i}, Hdr, PK)$: 经过授权的用户在接到密文后, 利用私钥 sk_{ID_i} 对密文的头部 Hdr 进行解密, 得到加密密钥 K , 然后利用 K 对密文主体 C_M 解密, 得到消息 M 。

2.2 安全模型

安全性方面, 通过攻击者和挑战者之间的游戏定义了适应性攻击下选择密文安全(adaptively Indistinguishable Chosen Ciphertext Attack, IND-ID-CCA)^[15]。在适应性攻击模型下, 攻击者能够适应性地选择想要攻击的身份, 如下所示:

1) 初始化阶段: 挑战者 \mathcal{C} 运行系统初始化程序 $\text{Setup}(\lambda, l)$, 生成公钥 PK , 并将其公布给攻击者 \mathcal{A} 。

2) 密钥询问阶段: 攻击者 \mathcal{A} 适应性地发起 ID_i ($1 \leq i \leq l$, l 表示一次加密的最大用户数) 的私钥提取询问, 挑战者运行私钥提取算法 Extract 生成与身份 ID_i 相对应的私钥, 并把结果返回给攻击者 \mathcal{A} 。

3) 挑战阶段: 询问阶段结束后, 攻击者 \mathcal{A} 指定一个挑战身份集合 $S^* = \{ID_1^*, ID_2^*, \dots, ID_k^*\}$ ($k \leq l$), 满足密钥询问阶段中的身份 $ID_i \notin S^*$ 。挑战者令 $(Hdr^*, K_0) = \text{Encrypt}(S^*, PK)$, 且 K_1 是密钥空间 K 中的一个随机值。挑战者随机选择一个随机值 $b \leftarrow \{0, 1\}$, 并返回 (Hdr^*, K_b) 给攻击者 \mathcal{A} 。

4) 猜测阶段: 攻击者 \mathcal{A} 输出一个猜测 $b' \in \{0, 1\}$, 如果 $b' = b$, 则攻击者赢得游戏。

本文用 q_E 表示密钥提取询问的次数, 将 q_E 和 l 视为攻击参数, 则攻击者 \mathcal{A} 的优势为:

$$\text{Adv}_{\text{IBBE}}^{IBBE} = |\Pr(b = b') - 1|$$

定义 4 如果攻击者 \mathcal{A} 在上述的游戏过程中获得的优势 $\text{Adv}_{\text{IBBE}}(l, q_E)$ 是可以忽略的, 称该 IBBE 方案是 (l, q_E) 适应性攻击下安全的。

3 Wang 等提出的广播加密方案

2010 年, Wang 等^[6] 利用格委托技术, 最先构造了格上具备适应性攻击下选择明文安全的身份类广播加密方案, 具体如下:

1) 参数设置。令 k, l, m, n, q, t 为正整数, 且 $q \geq 2, m \geq 2n \ln q, k \leq l$, 其中 l 表示一次加密的最大用户数, IBBE 方案共享的参数函数 $L(k), r(k), \alpha(k)$ 定义如下。

用户的私钥基尺寸:

$$L \geq m \cdot \omega(\sqrt{\ln n})$$

$$L(k) \geq L \cdot m^{\frac{k}{2}} \cdot \omega(\ln^{\frac{k}{2}} m)$$

生成短基的高斯参数:

$$r(k) \geq L(k-1) \cdot \omega(\sqrt{\ln m})$$

噪声的高斯参数:

$$\alpha(k) \leq \frac{1}{r(k) \sqrt{km+1} \cdot \omega(\sqrt{\ln n})}$$

2) 系统建立。

选择一个哈希函数(在安全性证明的过程中, H 被视为随机预言机), 随机均匀地选取 $V \in \mathbf{Z}_q^{n \times t}$, 其中 t 是加密消息的密钥长度; 运行陷门生成函数 TrapGen 生成格 $\Lambda_q^\perp(A_0)$ 和格上的一个短基 $T_0 \in \mathbf{Z}_q^{m \times m}$ ($\|T_0\| \leq L$), 输出系统的主密钥 $\text{MSK} = T_0 \in \mathbf{Z}_q^{m \times m}$, 公钥 $\text{PK} = (A_0, H, V)$ 。

3) 私钥提取。

对任意的 $ID_i \in \{0,1\}^*$, 分配相关的矩阵如下:

$$\mathbf{A}_i = [\mathbf{A}_0 \parallel \mathbf{A}_{ID_i}] \in \mathbf{Z}_q^{n \times 2m}$$

运行格基授权算法生成用户私钥 \mathbf{T}_{ID_i} , 即格 $A^\perp(\mathbf{A}_i)$ 的一个基:

$$\mathbf{T}_{ID_i} \leftarrow \text{SampleBasis}(\mathbf{T}_0, \mathbf{A}_i, S_0 = \{1\}, L(1)); \|\bar{\mathbf{T}}_{ID_i}\| \leqslant L \quad (1)$$

4) 加密。

设接收方为 $S = \{ID_1, ID_2, \dots, ID_k\}, k \leq l$, 则广播者作如下操作:

① 令 $\mathbf{A}_S = [\mathbf{A}_0 \parallel \mathbf{A}_{ID_1} \parallel \dots \parallel \mathbf{A}_{ID_k}] \in \mathbf{Z}_q^{n \times (k+1)m}$, 定义一个标签 lab_S 用来记录矩阵 \mathbf{A}_S 与用户身份 $\{ID_1, ID_2, \dots, ID_k\}$ 的相关信息。

② 随机选择一个向量 $\mathbf{u} \in \mathbf{Z}_q^n$, 计算 $\mathbf{p} = \mathbf{A}_S^T \mathbf{u} + \mathbf{x}_1 \in \mathbf{Z}_q^{(k+1)m}$, 其中 $\mathbf{x}_1 \leftarrow \chi^{(k+1)m}, \chi = \varphi_{\alpha(k+1)}$ 。

③ 选取一个消息加密密钥 $K \in \{0,1\}^t$, 对于 $1 \leq j \leq t$, 令 $b_j = bit_j(K)$ 表示 K 的第 j 比特, 计算

$$\mathbf{c} = \mathbf{V}^T \mathbf{u} + \mathbf{x}_2 + K \cdot \lfloor q/2 \rfloor \in \mathbf{Z}_q^t$$

其中: $\mathbf{x}_2 \leftarrow \chi^t$, 输出 $Hdr = (\mathbf{p}, \mathbf{c}, lab_S)$ 。

5) 解密。

授权 $ID_i \in S$ 在得到密文后, 按照以下步骤操作:

① 通过 lab_S 信息得到 $\mathbf{A}_S = [\mathbf{A}_0 \parallel \mathbf{A}_{ID_1} \parallel \dots \parallel \mathbf{A}_{ID_k}] \in \mathbf{Z}_q^{n \times (k+1)m}$ 。

② 令 $\mathbf{V} = [\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_t] \in (\mathbf{Z}_q^n)^t$, 对于 $1 \leq j \leq t$, 运行广义原像抽样算法生成:

$\mathbf{e}_j \leftarrow \text{GenSamplePre}(\mathbf{T}_{ID_i}, \mathbf{A}_{ID_i}, \mathbf{A}_S, \mathbf{v}_j, r(k+1)) \in \mathbf{Z}^{(k+1)m}$
其中: \mathbf{e}_j 服从 $D_{A_{\mathbf{v}_j}^\perp(\mathbf{A}_S), r(k+1)}$ 分布。

③ 令 $\mathbf{c} = [\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_t] \in \mathbf{Z}_q^t$, 对于 $1 \leq j \leq t$, 计算 $b'_j = \mathbf{c}_j - \mathbf{e}_j^T \mathbf{p} \in \mathbf{Z}_q$ 。在 0 和 $\lfloor q/2 \rfloor$ 之间判断, 若 b'_j 更接近 0 , 则输出 $b_j = 0$; 否则输出 $b_j = 1$ 。

④ 最后输出 $K = [b_1, b_2, \dots, b_t]$, 并利用 K 作为输入运行相应算法, 输出明文 M 。

4 方案

本章使用盆景树扩展控制算法、强不可伪造一次签名算法 OTS(KG, Sign, Vrfy) 和原像抽样算法, 在标准模型下构造了一个适应性攻击模型下可证明安全的基于身份广播加密方案, 记为 LIBBE。方案具体如下:

设一次加密的最大用户数为 l , 系统中第 i 个用户的身份记为 ID_i 。

1) 系统建立。

输入系统的安全参数 λ , 运行陷门生成函数 TrapGen 生成一个格 $A_q^\perp(\mathbf{A}_0)$ 以及对应的基 \mathbf{T}_0 , 其中: $MSK = \mathbf{T}_0$ 作为系统的主密钥, 由私钥生成器(PKG)掌握; $\mathbf{A}_0 \in \mathbf{Z}_q^{n \times m}$ 为公共参数。随机选择两个矩阵 $\mathbf{E}_0, \mathbf{E}_1 \in \mathbf{Z}_q^{n \times m}$ 和 $\mathbf{V} \in \mathbf{Z}_q^{n \times t}$, 其中: t 是消息加密密钥的长度; 建立编码函数 $H: \mathbf{Z}_q^n \rightarrow \mathbf{Z}_q^{m \times m}$ 。

2) 私钥提取。

对任意的一个用户 $ID_i \in \{0,1\}^*$, 私钥生成器 PKG 首先为用户 ID_i 生成相应的身份矩阵 $\mathbf{A}_i = [\mathbf{A}_0 \parallel (\mathbf{E}_0 + \mathbf{E}_1 \cdot H(ID_i))] \in \mathbf{Z}_q^{n \times 2m}$; 然后, 运行盆景树扩展控制算法, 输入

$(\mathbf{T}_0, \mathbf{A}_i)$, 输出用户的私钥 $\mathbf{T}_i \leftarrow \text{ExtBasis}(\mathbf{T}_0, \mathbf{A}_i, \mathbf{u}_i)$ 。

3) 加密。

假设接收用户集合为 $S = \{ID_1, ID_2, \dots, ID_k\}, D_S = \{\mathbf{e} \in \mathbf{Z}^{(2k+1)m}: \|\mathbf{e}\| \leqslant r(2k+1)\}$, 广播者生成接收用户集合的身份矩阵 $\mathbf{A}_S = [\mathbf{A}_0 \parallel \mathbf{A}_{ID_1} \parallel \dots \parallel \mathbf{A}_{ID_k}] \in \mathbf{Z}_q^{n \times (2k+1)m}$, 广播者作如下操作:

① 运行强不可伪造一次签名算法的密钥生成算法 OTS.KG, 生成签名密钥 $signk$ 和验证密钥 vk 。

② 选择一个向量 $\mathbf{u} \in \mathbf{Z}_q^n$, 计算 $\mathbf{p} = \mathbf{A}_S^T \mathbf{u} + \mathbf{x}_1 \in \mathbf{Z}_q^{(2k+1)m}$, 其中: $\mathbf{x}_1 \leftarrow \chi^{(2k+1)m}, \chi = \varphi_{\alpha(2k+1)}$ 。

③ 随机选取一个消息加密密钥 $K \in \{0,1\}^t$, 对于 $1 \leq j \leq t$, 令 $b_j = bit_j(K)$ 表示 K 的第 j 比特, 计算 $\mathbf{c} = \mathbf{V}^T \mathbf{u} + \mathbf{x}_2 + K \cdot \lfloor q/2 \rfloor \in \mathbf{Z}_q^t$, 其中 $\mathbf{x}_2 \leftarrow \chi^t$, 输出 $Hdr = (\mathbf{p}, \mathbf{c})$ 。

④ 利用密钥 K 对消息 M 进行加密形成密文主体部分 C_b ; 令 $C_1 = (Hdr, C_b)$, 运行一次签名算法 $\sigma \leftarrow \text{OTS.Sign}(C_1, signk)$, 形成最终的密文为 $C = (vk, \sigma, C_1)$ 。

4) 解密。

合法用户 $ID_i \in S$ 在收到密文后, 首先利用验证密钥 vk , 验证 $\text{OTS.Vrfy}(C, \sigma, vk) = 1$ 是否成立, 若成立, 则接收用户输出 $C_1 = (Hdr, C_b)$ 。

然后, 作如下操作:

① 令 $\mathbf{V} = [\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_t] \in (\mathbf{Z}_q^n)^t$, 对于 $1 \leq j \leq k$, 用户 ID_i 运行盆景树扩展控制算法, 生成接收用户集合对应格的基 $\mathbf{T}_S \leftarrow \text{ExtBasis}(\mathbf{T}_i, \mathbf{A}_{ID_i}, \mathbf{A}_S)$ 。

② 输入 \mathbf{T}_S , 运行原像抽样算法生成 $\mathbf{e}_j \leftarrow \text{GenSamplePre}(\mathbf{T}_S, \mathbf{A}_{ID_i}, \mathbf{A}_S, \mathbf{v}_j, r(2k+1))$, 且 \mathbf{e}_j 服从 $D_{A_{\mathbf{v}_j}^\perp(\mathbf{A}_S), r(2k+1)}$ 分布。

③ 然后令 $\mathbf{c} = [\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_t] \in \mathbf{Z}_q^t$, 对于 $1 \leq j \leq t$, 计算 $b'_j = \mathbf{c}_j - \mathbf{e}_j^T \mathbf{p} \in \mathbf{Z}_q$, 如果 b'_j 比 $\lfloor q/2 \rfloor$ 更接近 0 , 则输出 $b_j = 0$; 否则, $b_j = 1$ 。

④ 最后输出 $K = [b_1, b_2, \dots, b_t]$, 并利用 K 运行对称加密算法, 输出明文 M 。

5 方案分析

5.1 正确性分析

方案的正确性依赖于 LWE 以及陷门函数的特性。在加密阶段, 集合 S 中的合法用户构建一个单向函数, $f_{A_S}: D_S \rightarrow \mathbf{Z}_q^n$, $f_{A_S}(\mathbf{e}) = \mathbf{A}_S \mathbf{e} \bmod q$, 其中 $D_S = \{\mathbf{e} \in \mathbf{Z}^{(2k+1)m}: \|\mathbf{e}\| \leqslant r(k+1)\}$ 具有以下特性:

1) 正确分布: 通过文献[14]引理 5.1 可知, $\mathbf{v}_j = \mathbf{A}_S \mathbf{e} \bmod q$ 的分布满足 \mathbf{Z}_q^n 上均匀分布; 通过定理 2, 算法 GenSamplePre($\mathbf{T}_S, \mathbf{A}_{ID_i}, \mathbf{A}_S, \mathbf{v}_j, r(k+1)$) 取样一个元素 $\mathbf{e}_j \in D_S$ 满足 $D_{A_{\mathbf{v}_j}^\perp(\mathbf{A}_S), r(2k+1)}$ 上可忽略的统计距离。

2) 不带陷门的单向函数: 通过文献[14]定理 5.9 可知, 求逆一个均匀输出的函数 f_{A_S} 等价于解决不同类的非齐次最小整数解问题。

因此, 合法用户 $ID_i \in S$ 收到密文 $C = (vk, \sigma, C_1)$ 后, 首先利用签名的验证密钥 vk 验证 $\text{OTS.Vrfy}(C_1, \sigma, vk) = 1$ 是否成立, 若成立, 输出 $C_1 = (Hdr, C_b)$ 。

然后, 作如下操作:

$\text{ExtBasis}(\mathbf{T}_i, \mathbf{A}_{ID_i}, \mathbf{A}_s) \rightarrow \mathbf{T}_s \Rightarrow$

$\text{GenSamplePre}(\mathbf{T}_s, \mathbf{A}_{ID_i}, \mathbf{A}_s, \mathbf{v}_j, r(2k+1)) \rightarrow \mathbf{e}_j$

其中: \mathbf{e}_j 服从 $D_{\mathbf{A}_{ID_i}^{-1}(\mathbf{A}_s), r(2k+1)}$ 分布

$$\begin{aligned} b'_j &= \mathbf{c}_j - \mathbf{e}_j^T \mathbf{p} = \\ &\mathbf{v}_j^T \mathbf{u} + \mathbf{x}_2 + b_j \cdot \lfloor q/2 \rfloor - \mathbf{e}_j^T \cdot (\mathbf{A}_s^T \mathbf{u} + \mathbf{x}_1) = \\ &\mathbf{v}_j^T \mathbf{u} + \mathbf{x}_2 + b_j \cdot \lfloor q/2 \rfloor - [(\mathbf{A}_s \mathbf{e}_j)^T \mathbf{u} + \mathbf{e}_j^T \mathbf{x}_1] = \\ &\mathbf{x}_2 + b_j \cdot \lfloor q/2 \rfloor - \mathbf{e}_j^T \mathbf{x}_1 \end{aligned}$$

若 $b_j = 0$, 则 b'_j 接近 0; 若 $b_j = 1$, b'_j 接近 $\lfloor q/2 \rfloor$ 。因此通过 b'_j 的值, 接收用户可以正确地推出 b_j 的值。

5.2 安全性分析

设 LIBBE' 为不加入一次签名的方案, 本节首先证明了 LIBBE' 是标准模型下适应性不可区分选择明文攻击安全 (Indistinguishable-Chosen Plaintext Attack, IND-CPA); 然后在此基础上加入一次签名算法, 证明 LIBBE 是选择密文攻击 (Chosen Ciphertext Attack, CCA) 安全的。

定理 3 令 $q \geq 2r(l)(m+1)$, $\chi = \psi_{\alpha(l+1)}$, $m \geq 2n \lg q$ 。如果 LWE _{q, χ} 是困难的, 则上述的 LIBBE' 方案是 IND-ID-CPA 安全的。

证明 为了方便分析, 本文只考虑在方案中加密 1 比特消息密钥的情况。假设存在适应性攻击者 \mathcal{A}_1 能够以不可区分的优势 $Adv_{L_{q,E}}^{\text{LIBBE}'}(\mathcal{A}_1)$ 攻破本文方案, q_E 为私钥提取询问的次数, 本文现在构造一个攻击者 \mathcal{B} , 攻击 LWE 问题的优势为 $Adv_{q,\chi}^{\text{LWE}}(\mathcal{B})$ 且满足

$$Adv_{q,\chi}^{\text{LWE}}(\mathcal{B}) \geq Adv_{\text{LIBBE}'}^{\text{IND-CPA}}(\mathcal{A}_1) - negl(n)$$

\mathcal{B} 和 \mathcal{A}_1 的交互如下:

初始化 \mathcal{B} 均匀地选取 $k^* \in [l]$ (k^* 是挑战的用户集合长度), 从 LWE 预言机中得到 $(k^* + 1)m + 1$ 个取样 $(\mathbf{a}_j, b_j) \in \mathbf{Z}_q^n \times \mathbf{Z}_q$ ($1 \leq j \leq (k^* + 1)m + 1$), 其中 $\mathbf{a}_j \in \mathbf{Z}_q^n$ 是随机的, $b_j = \mathbf{a}_j^T \mathbf{s} + \mathbf{x}_j$ 也是随机的, $\mathbf{s} \in \mathbf{Z}_q^n$ 和高斯噪声 \mathbf{x}_j 服从 χ 。然后, \mathcal{B} 解析这些 LWE 取样 $(\mathbf{a}_j, b_j) \in \mathbf{Z}_q^n \times \mathbf{Z}_q$ ($1 \leq j \leq (k^* + 1)m + 1$) 为 $(\mathbf{A}_i^*, \mathbf{p}_i^*) \in (\mathbf{Z}_q^{n \times m} \times \mathbf{Z}_q^m)$ ($0 \leq i \leq k^*$) 和 $(\mathbf{y}^*, \mathbf{c}^*) = (\mathbf{a}_{(k^*+1)m+1}, b_{(k^*+1)m+1}) \in \mathbf{Z}_q^n \times \mathbf{Z}_q^m$ 。

1) 询问阶段。

\mathcal{A}_1 发起以下询问:

攻击者 \mathcal{A}_1 适应性地发出私钥询问, \mathcal{B} 运行盆景树扩展控制算法 $\text{ExtBasis}(\mathbf{T}_0, \mathbf{A}_i, \mathbf{u}_i)$, 并按照下面的规则将私钥告知攻击者:

① 如果攻击者 \mathcal{A}_1 第一次询问 ID_i 的私钥, 则 \mathcal{B} 维护一张表 L_f , 计算与身份 ID_i 公钥 $\mathbf{A}_i = [\mathbf{A}_0 \parallel \mathbf{A}_{ID_i}]$ 相对应的私钥 \mathbf{T}_i , 并将 (ID_i, \mathbf{T}_i) 添加到列表 L_f 中。

$$\mathbf{T}_i = \text{ExtBasis}(\mathbf{T}_0, \mathbf{A}_i, \mathbf{u}_i)$$

② 如果攻击者 \mathcal{A}_1 已经询问过 ID_i 的私钥, \mathcal{B} 就从列表 L_f 中选出相应的私钥 \mathbf{T}_i 回答攻击者的询问。

2) 挑战阶段。

攻击者 \mathcal{A}_1 决定询问阶段一结束时, 挑战者 \mathcal{B} 选取一个消息加密密钥 $K \in \{0,1\}^t$, 计算 $\mathbf{c}^* = \mathbf{v}^T \mathbf{u} + \mathbf{x}_2 + K \cdot \lfloor q/2 \rfloor$, $\mathbf{x}_2 \leftarrow \chi^t$ 。攻击者随机选择明文 M_0, M_1 发送给挑战者, 挑战者利用 K 加密, 得到 C_b , 然后将 $C_1 = (\mathbf{c}^*, C_b)$ 发送给攻击者。

3) 询问阶段二。

攻击者继续适应性地发出与阶段一相同方式的私钥提取

询问 $q_{s_0+1}, q_{s_0+2}, \dots, q_{s_0+s}$ 。

4) 猜测阶段。

最后, 攻击者 \mathcal{A}_1 输出一个猜想 $b' \in \{0,1\}$ 。如果 $b' = b^*$, \mathcal{B} 返回一个真值; 否则 $b' \neq b^*$, 返回一个随机值。

在 \mathcal{A}_1 看来, \mathcal{B} 的行为是接近于一个被提供真实的、适应性安全的实验。特别地, \mathbf{A}_{s^*} 是使用 LWE 实例构造出来的, 且具有均匀分布的特点, 不管 LWE 实例是否真实, 很容易可看出一个挑战询问停止的概率为:

$$1 - \frac{1}{lq_{H_1}^{k^*-1}}$$

如果 \mathcal{B} 无法在询问阶段停止, 那么他的回答分布是统计接近于一个真实的适应性安全的环境。对于挑战密文, 如果 LWE 实例是真实的, 则 \mathbf{c}^* 的组成将和 LWE 游戏的分布是一致的, 然而, 如果 LWE 实例是随机的, 那么 \mathbf{c}^* 的组成同样是随机的。如果 \mathcal{A}_1 给出一个不同的成功概率, 那么, \mathcal{B} 将能够成功地在 $(k^* + 1)m + 1$ 个真实和随机 LWE 问题实例进行区分。

因为每一个 \mathbf{c}^* 是独立的且为均匀分布, 所以证明可以推广到多比特。

综上, 由 LWE 问题的困难性假设可知, 方案 LIBBE' 在标准模型下是 IND-ID-CPA 安全的。

定理 4 若方案 LIBBE' 是标准模型下 IND-ID-CPA 安全的, 那么加入一次签名的方案 LIBBE 是标准模型下 CCA 安全。

证明 游戏是在攻击者 \mathcal{A}_1 与攻击者 \mathcal{A}_2 之间展开的, 其中是 \mathcal{A}_1 以选择明文攻击方式攻击方案 LIBBE' 的攻击者, \mathcal{A}_2 是以选择密文攻击方式攻击方案 LIBBE 的攻击者。令 (vk^*, σ^*, C_1) 为 \mathcal{A}_2 生成的挑战密文。

令事件 Forge 表示攻击者 \mathcal{A}_2 发送密文 $C = (vk, \sigma, c)$ 给解密预言机进行解密询问, 满足 $(\sigma^*, C_1^*) \neq (\sigma, C_1)$, $Vrfy_{vk^*}(C_1, \sigma) = 1$ 。

攻击者 \mathcal{A}_2 可以以 $Pr_{\sigma_2}[\text{Forge}]$ 的优势攻破一次签名体制, 又一次签名密钥是随机选取的, 所以, $Pr_{\sigma_2}[\text{Forge}]$ 的值是可忽略的。

构造 σ_2 如下:

1) 系统运行初始化算法, 生成 (PK, MSK) , 将 PK 发送给 σ_1 , 这里 σ_1 充当解密预言机。

2) 攻击者 σ_2 对 (vk, σ, c) 进行解密预言询问时, σ_1 进行以下操作:

① 如果 $Vrfy_{vk}(\sigma, c) = 1$ 不成立, σ_1 输出 \perp 。

② 如果 $Vrfy_{vk}(\sigma, c) = 1, vk = vk^*$ 即 Forge 事件发生, σ_1 停止运算, 并输出一随机数。

③ 如果 $Vrfy_{vk}(\sigma, c) = 1$, 且 $vk \neq vk^*$, 则 σ_1 进行预言询问, 使用 vk 解签名, 输出对询问密文 c 的解密明文 m , 并返回 m 。

3) σ_2 选择两个明文 m_0, m_1, σ_1 对 $m_b, b \in \{0,1\}$ 进行加密得到一个密文 c^* , σ_1 计算 $\sigma^* = \text{Sign}_{vk^*}(c^*)$, 并将 (c^*, σ^*, vk^*) 返回给 σ_2 。

4) σ_2 继续发出询问, σ_1 按照前面的应答方式进行应答, 值得注意的是, σ_2 不能对 (c^*, σ^*, vk^*) 进行解密询问。

5) σ_2 输出对 b 的猜测。

因为 $LWE_{q,\chi}$ 问题是困难的,且一次签名密钥是随机选取的,因此 $Pr_{\alpha_1, \text{LIBBE}}[\text{Succ}]$ 和 $Pr_{\alpha_2}[\text{Forge}]$ 可以忽略不计,又

$$Pr_{\alpha_1, \text{LIBBE}}[\text{Succ}] \geq Pr_{\alpha_2, \text{LIBBE}}[\text{Succ}] - 0.5Pr_{\alpha_2}[\text{Forge}]$$

$$Pr_{\alpha_2, \text{LIBBE}}[\text{Succ}] \leq \xi + 0.5Pr_{\alpha_2}[\text{Forge}]$$

综上所述,本文构造的方案 LIBBE 是标准模型下 IND-ID-CCA 安全的。

5.3 性能分析

本文方案与其他基于身份广播加密方案相比,实现了固定长度的公私钥,而且由于基于格构造的方案,运算只涉及模数的加法和乘法运算,因此计算开销较小。表 1 为本文方案与一些现有方案之间效率及安全性的对比。

表 1 方案比较

方案	密文头部	公钥长度	私钥长度	模型	安全性
DE ^[4]	$O(1)$	$O(l)$	$O(l)$	随机预言机	IND-sID-CPA
GW ^[6]	$O(S)$	$O(l)$	$O(1)$	标准模型	IND-ID-CPA
LIBBE	$O(S)$	$O(1)$	$O(1)$	标准模型	IND-ID-CCA

注:IND-sID-CPA 表示选择身份和选择明文攻击安全的不可区分性。

另外,本文方案还具有动态特性,方案中使用盆景树扩展控制算法生成用户的身份矩阵,通过对身份矩阵的伸缩来控制系统中用户的数量,能够方便地实现用户的动态增加或删除。例如在广播系统中,设广播者对用户 $\{ID_1, ID_2, \dots, ID_k\}$ 进行传输(接收用户矩阵为 $A_s = [A_0 \parallel A_1 \parallel \dots \parallel A_k]$),若系统中新增用户 ID_{k+1} ,则只需要将身份 ID_{k+1} 对应的矩阵 A_{k+1} 级联到 A_s 中;若用户 ID_i 被撤销,则只需将矩阵中的 A_i 移除。

6 结语

本文基于格上困难问题构造了一个可证明安全的基于身份广播加密方案。首先,利用盆景树扩展控制算法生成用户的私钥,同时也使得方案具有动态特性,能够实现用户的增加或删除;然后,加入一次签名算法,并在标准模型下,证明方案是适应性攻击下选择密文安全。

参考文献:

- [1] AMOS F, MONI N. Broadcast encryption [C] // CRYPTO 1993: Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer, 1994: 480 – 491.
- [2] DAN B, CRAIG G, BRENT W. Collusion resistant broadcast encryption with short ciphertexts and private keys [C] // CRYPTO 2005: Proceedings of the 25th Annual International Cryptology Conference on Advances in Cryptology, LNCS 3621. Berlin: Springer, 2005: 258 – 275.
- [3] ADI S. Identity-based cryptosystems and signature schemes[C] // Proceedings of CRYPTO 1984 on Advances in Cryptology, LNCS 196. Piscataway, NJ: IEEE, 1984: 47 – 53.
- [4] CÉCILE D. Identity-based broadcast encryption with constant size ciphertexts and private keys [C] // ASIACRYPT 2007: Proceedings of the 13th International Conference on the Theory and Application of Cryptology and Information Security, LNCS 4833. Piscataway, NJ: IEEE, 2007: 200 – 215.
- [5] DANIELE M, ODED R. Lattice-based cryptography[M] // BERNSTEIN D J, BUCHMANN J, DAHMEN E. Post Quantum Cryptography. Berlin: Springer, 2009: 47 – 91.
- [6] WANG J, BI J. Lattice-based identity-based broadcast encryption [EB/OL]. [2015-02-10]. <https://eprint.iacr.org/2010/288.pdf>.
- [7] LI X, YANG B, GUO Y, et al. Provably secure group based broadcast encryption on lattice [J]. Journal of Information & Computational Science, 2011, 8(2): 179 – 193.
- [8] 张伟仁,胡予濮,杨晓元.格上新的身份类广播加密方案[J].北京邮电大学学报 2012, 35(6): 112 – 115. (ZHANG W R, HU Y P, YANG X Y. New identity-based broadcast encryption scheme based on lattice [J]. Journal on Beijing University of Posts and Telecommunications, 2012, 35(6): 112 – 115.)
- [9] ADELA G. Anonymous lattice-based broadcast encryption [C] // ICT-EurAsia 2013: Proceedings of the 2013 International Conference on Information and Communication Technology, LNCS 7804. Berlin: Springer, 2013: 353 – 362.
- [10] BENOIT L, PATERSON K G, QUAGLIA E A. Anonymous broadcast encryption: adaptive security and efficient constructions in the standard model [C] // PKC 2012: Proceedings of the 15th International Conference on Practice and Theory in Public Key Cryptography, LNCS 7293. Berlin: Springer, 2012: 206 – 224.
- [11] ZHANG X, WANG S, ZHANG W. Forward-secure identity-based broadcast encryption scheme from lattice [J]. Applied Mathematics & Information Sciences, 2015, 9(4): 1993 – 2000.
- [12] MICCIANCIO D, GOLDWASSER S. Complexity of Lattice Problems: a Cryptographic Perspective [M]. Berlin: Springer, 2002.
- [13] CHRIS P. Bonsai trees (or, arboriculture in lattice-based cryptography) [EB/OL]. [2015-02-10]. <https://eprint.iacr.org/2009/359.pdf>.
- [14] GENTRY C, PEIKERT C, VAIKUNTANATHAN V. Trapdoors for hard lattices and new cryptographic constructions [C] // STOC 2008: Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing. New York: ACM, 2008: 197 – 206.
- [15] GENTRY C, WATERS B. Adaptive security in broadcast encryption systems (with short ciphertexts) [C] // EUROCRYPT 2009: Proceedings of the 28th Annual International Conference on Advances in Cryptology: the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2009: 171 – 188.
- [16] DAVID C, DENNIS H, EIKE K, et al. Bonsai trees, or how to delegate a lattice basis [C] // EUROCRYPT 2010: Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 6110. Berlin: Springer, 2010: 523 – 552.

Background

This work is partially supported by the National Natural Science Foundation of China (61272492), the Basic Research Project of Natural Science in Shaanxi Province(2015JM6353, 2014JM8300)

HUANG Wenzhen, born in 1991, M. S. candidate. His research interests include broadcast encryption, lattice cryptography, multilinear maps, identity-based cryptography.

YANG Xiaoyuan, born in 1959, M. S., professor. His research interests include elliptic curve cryptography, lattice cryptography, proxy re-encryption.

WANG Xu'an, born in 1981, M. S., associate professor. His research interests include proxy re-encryption, identity-based cryptography.

WU Liqiang, born in 1986, M. S., lecturer. His research interests include lattice cryptography, identity-based cryptography.