软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2016,27(11):2884−2897 [doi: 10.13328/j.cnki.jos.004884]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

有效的格上无证书加密方案*

陈 虎[1,2], 胡予濮[1], 连至助[1], 贾惠文[1]

[1](综合业务网理论及关键技术国家重点实验室(西安电子科技大学),陕西 西安 710071)

[2](江苏省教育大数据科学与工程重点实验室(江苏师范大学),江苏 徐州 221116)

通讯作者: 陈虎, E-mail: chenhuchh@163.com

摘 要: 利用原像抽样算法抽取部分私钥和带误差的学习问题生成秘密值及公钥来构造格上无证书加密方案.在随机预言模型下,借助可抵抗拥有询问秘密值能力的两类攻击者形式化地证明了该方案在自适应选择身份攻击下(甚至是量子的)密文是不可区分的.通过分析方案的正确性、安全性和效率来说明如何选择参数.使用两种不同的扩大明文空间的方法来进一步提高方案的效率.这体现出该方案具有很强的灵活性.特别地,给出了逐步定比特填充法.它是一种由固定长度比特串去确定多个更长比特串的有效方法.该方法在构建多比特无证书加密过程中起到重要作用.鉴于内蕴了格和无证书密码系统的优势,该方案具有灵活、有效、抗量子攻击和不涉及证书管理等优点.

关键词: 格公钥密码;无证书密码系统;原像抽样算法;带误差的学习问题

中图法分类号: TP309

中文引用格式: 陈虎,胡予濮,连至助,贾惠文.有效的格上无证书加密方案.软件学报,2016,27(11):2884−2897. http://www.jos.org.cn/1000-9825/4884.htm

英文引用格式: Chen H, Hu YP, Lian ZZ, Jia HW. Efficient certificateless encryption schemes from lattices. Ruan Jian Xue Bao/ Journal of Software, 2016,27(11):2884−2897 (in Chinese). http://www.jos.org.cn/1000-9825/4884.htm

Efficient Certificateless Encryption Schemes from Lattices

CHEN Hu[1,2], HU Yu-Pu[1], LIAN Zhi-Zhu[1], JIA Hui-Wen[1]

[1](State Key Laboratory of Integrated Service Networks (Xidian University), Xi'an 710071, China)

[2](Jiangsu Key Laboratory of Education Big Data Science and Engineering (Jiangsu Normal University), Xuzhou 221116, China)

Abstract: A certificateless encryption scheme from lattices is put forward by using preimage sampleable algorithm to extract partial private keys and learning with errors to generate secret values and public keys. The new scheme is indistinguishably secure against adaptive chosen-identity attacks, even against quantum-computing attacks. This is achieved in the random oracle model by formally demonstrating that this construction can fight against two types of adversaries who can request secret values. Proper parameter setting for the scheme is obtained specifically by performing an analysis of its correctness, security, and efficiency. Two methods for further improving its efficiency are used by enlarging its plaintext space according to both distinct approaches, which also shows that the given scheme is flexible. Specially, an efficient method of successive padding with fixed bit is presented for obtaining multiple longer bit strings determined by a fixed-size bit string, which provides a valuable contribution towards building the multi-bit certificateless encryption scheme. Due to advantages inheriting from lattices and certificateless cryptosystem, the proposed schemes are flexible, efficient, resistant to quantum-computing attacks and free from certificate management.

Key words: lattice-based cryptography; certificateless cryptosystem; preimage sampleable algorithm; learning with errors

* 基金项目: 国家自然科学基金(61472309, 61672412, 61373171); 安徽省高校自然科学基金(KJ2016A626, KJ2016A627)

Foundation item: National Natural Science Foundation of China (61472309, 61672412, 61373171); Natural Science Foundation of Anhui Higher Education Institutions (KJ2016A626, KJ2016A627)

收稿时间: 2015-03-15; 修改时间: 2015-06-16, 2016-07-30; 采用时间: 2015-08-12; jos 在线出版时间: 2015-12-21

CNKI 网络优先出版: 2015-12-22 14:59:16, http://www.cnki.net/kcms/detail/11.2560.TP.20151222.1459.001.html

© 中国科学院软件研究所 http://www.jos.org.cn

近年来,作为关注焦点和研究热点的格公钥密码获得快速蓬勃地发展[1−11],突出体现在格上实现了全同态加密[3,12−15]和全同态签名[16].与传统的以大整数分解或离散对数等困难问题为基础的公钥密码相比,格公钥密码具有显著的优势[6]:首先,格具有良好的抗量子计算攻击特性,这种特性使得在格上构造的密码方案呈现高安全性;其次,格上困难问题存在从最差情况到平均情况归约的特性,该特性可以保证解决一个格上随机困难问题实例的困难性不低于最差情况下的格中困难问题的困难性,这使得格上构造的密码方案可避免任何不可预见的结构上的弱点且具有良好的可证安全性.另外,格上密码系统涉及到的运算是环$\mathbb{Z}_q$(其中,$q=poly(n)$,n为安全参数)上矩阵和向量之间的运算(十分简单且可并行),这使得在格上构造的密码方案具有高效性.然而,格公钥密码也存在空间开销大的缺陷,如文献[2]中签名方案的公/私钥尺寸均为$\tilde{O}(n^2)$,这样,基于传统证书的格密码方案必然带来巨大的存储开销和通信代价.而基于身份的格密码方案[2,4,10,13]虽然避免了证书管理带来的额外开销,但其固有的密钥托管问题又使其上的方案含有潜在的安全风险.然而,无证书公钥系统[17]既解决了基于身份的公钥系统中密钥托管问题,又保持其不需要使用公钥证书的优点,从而使其成为持续的热点,并在无证书加密[18,19]、签名[20−22]和认证[23]等方面取得丰硕的成果[24].但是,上述成果都不是以格为基础构造的.然而,构造无证书体制下格密码方案可实现二者优势互补,这对构造高效安全的方案有特别的意义.

2014 年,文献[25,26]在这方面做了有益的工作.文献[25]给出了一个标准模型下可证安全的无证书加密的一般性构造方法,并在格上给出实例化的方案.为实现无证书加密在选择密文攻击(chosen-ciphertext attack, CCA2)下安全,文中巧妙地组合分级加密、基于身份的加密、密钥封装和消息认证码这 4 个密码原型.如此密集的密码原型和它们的参数之间的制约关系导致整体方案的效率受损并在一定程度上抵消了无证书密码系统所带来的优势,如用户公钥应包含 4 个$\mathbb{Z}_q^{n\times m}$上的矩阵,这些矩阵分别为基于身份的加密和密钥封装方案的公钥,尤其是密钥封装方案所对应的那一个矩阵,要求 $m>10n\log q$(密钥封装以一个承诺方案作为构件使然).此外,条$m>10n\log q$ 也加剧恶化了该方案的密文长度及密文扩展比,从而弱化了方案的实用性.根据方案的设计,加密的明文$x\in\{0,1\}^{\ell}$需要先用解承诺串$dec\in\{0,1\}^m$去级联变为$(x\,|\,dec)\in\{0,1\}^{\ell+m}$,再对比特串$s_1$和$s_2$分别使用多比特版本的分级方案和基于身份的方案进行加密,其中,$s_2=s_1\oplus(x||dec)$,s_1均匀随机地从$\{0,1\}^{\ell+m}$中选择.若使密文长度最短,则要用$(\ell+m)$-比特版本的方案.此时,仅加密比特串 s_1 和 s_2 即可导致密文至少含有 $2(\ell+m)+30n|\log q|$个$\mathbb{Z}_q$中元素且明文的比特长度ℓ不能远大于 m,否则,系统和用户的公钥就过于庞大.与文献[18]中方案的效率相比,文献[25]中方案的优势体现在构造 CCA2 安全的无证书加密方案是利用两个在选择明文攻击(chosen-plaintext attack,简称 CPA)下安全的加密方案来实现.这不仅体现了该方案的理论价值,而且彰显了构造高效 CPA 安全的加密方案(甚至是在随机预言模型下)具有重要的理论和实际应用价值.文献[26]就是基于格密码提出了一个随机预言模型下 CPA 安全的无证书加密方案.然而,分析发现,该方案的效率尚需提高,且安全性证明存在问题.在效率方面,系统公钥$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$和私钥$\boldsymbol{T}\in\mathbb{Z}_q^{m\times m}$中参数$m>6n\log q$导致方案的存储和计算代价以及密文尺寸都偏大;其次,用户生成自己秘密值的过程耗时太多,因为需要大量反复地进行高斯抽样以获取一个$\mathbb{Z}_q^{m\times m}$上的可逆矩阵作为秘密值.在攻击者为$\mathcal{A}_{\mathrm{I}}$的安全性证明过程中,游戏中的挑战者$\mathcal{B}$是无证书加密方案的挑战者,又是基于身份的加密方案 IBE[2]的攻击者.为方便叙述,不妨设$\mathcal{C}$为 IBE 的挑战者.$\mathcal{C}$传递 IBE 的系统公钥$\boldsymbol{A}$和用户公钥$\boldsymbol{u}^*$给$\mathcal{B}$.$\mathcal{B}$将获得的 $\boldsymbol{A}$ 作为无证书加密的系统公钥,$\boldsymbol{u}^*$设定为其秘密地随机均匀选取的目标身份 ID_i 的哈希值$Hash(ID_i)$.注意到,证明中,$\mathcal{B}$同时设置了目标身份 ID_i 的部分私钥 $\boldsymbol{t}_i$ 并在其他询问中用到这个值,这是不合理的.因为$\mathcal{B}$作为 IBE 的攻击者,不知道 $\boldsymbol{A}$ 的陷门信息(否则不攻自破),所以$\mathcal{B}$给出 $\boldsymbol{u}^*$所对应的有效的部分私钥 $\boldsymbol{t}_i$ 的概率可忽略或者给出的是无效的部分私钥 $\boldsymbol{t}_i$(即大尺寸的).若 $\boldsymbol{t}_i$ 是前种情况,则此归约证明是毫无意义的;若 $\boldsymbol{t}_i$ 是后种情况,则$\mathcal{B}$提供的模拟场景与真实攻击场景是容易区分的.总之,在安全证明中,上述两种情况都必须避免.其次,在部分私钥询问中,$\mathcal{B}$在回答目标身份的部分私钥时是依据$\mathcal{A}_{\mathrm{I}}$将来是否替换目标身份的公钥而做出不同的回应(若不替换,则给予 $\boldsymbol{t}_i$;否则,终止协议).这也是不合理的,因为$\mathcal{B}$是无法预测或控制$\mathcal{A}_{\mathrm{I}}$未来的公钥替换行为.最后,因为$\mathcal{B}$准备挑战密文的过程没有具体给出,以至于无法搞清$\mathcal{B}$究竟是如何把从$\mathcal{C}$那里获得的挑战密文嵌入到为$\mathcal{A}_{\mathrm{I}}$生成的挑战密文之中,进而无法判断$\mathcal{A}_{\mathrm{I}}$的猜测值和$\mathcal{B}$的猜测值之间的对应关系.所以,简单地把$\mathcal{A}_{\mathrm{I}}$的猜

© 中国科学院软件研究所 http://www.jos.org.cn

测值作为$\mathcal{B}$的猜测值就存在问题了.这个问题同样存在于$\mathcal{B}$与攻击者$\mathcal{A}_{\mathrm{II}}$的游戏中.此外,在攻击者为$\mathcal{A}_{\mathrm{II}}$的安全性证明过程中,根据其对攻击者能力的规定,$\mathcal{A}_{\mathrm{II}}$应拥有系统私钥,故$\mathcal{B}$应该把系统私钥给$\mathcal{A}_{\mathrm{II}}$,但没有任何地方能体现出$\mathcal{A}_{\mathrm{II}}$获知了系统私钥.其实,从$\mathcal{B}$对目标身份的选取和嵌入他自己欲解决的困难问题的相关信息到目标身份等方面来看,两种情况(即$\mathcal{B}$分别与$\mathcal{A}_{\mathrm{I}}$和$\mathcal{A}_{\mathrm{II}}$的游戏)下的设置完全相同.这意味着$\mathcal{B}$完全不知道系统私钥,更别说$\mathcal{A}_{\mathrm{II}}$了,这背离了他们的安全模型.

本文在格上构造了一个单比特的无证书加密方案,并在随机预言模型下给出形式化的安全证明.我们借鉴文献[20,21]的做法,适当地强化了攻击者的攻击能力[24]:允许第2类攻击者$\mathcal{A}_{\mathrm{II}}$可替换除目标用户之外的任何用户的公钥,允许两类攻击者询问用户的秘密值.为达到更高的效率,我们采用文献[6]中的新型陷门生成方法以降低所生成格的维数、陷门尺寸和密文尺寸,并充分利用该陷门下并行的原像抽样算法.注意到,秘密值和公钥生成方法不仅决定其尺寸的大小,而且直接影响方案的安全性,所以设计基于格的无证书加密方案的难点在于如何生成用户秘密值和公钥.与文献[26]中的方案相比,我们用户的秘密值和公钥生成算法更加简单、有效——用户的秘密值就作为带误差的学习(learning with errors,简称LWE)问题的秘密向量来生成公钥.这样不仅避免了抽取$\mathbb{Z}_q^{m\times m}$上可逆矩阵[26],而且大幅缩短了密文长度.此外,我们的方案中生成用户的公钥无需部分私钥的信息,所以它具有"将来解密"特色[18],即,用户可在尚未获得部分私钥之前就公布其公钥来接收发送给他的密文,待将来获取部分私钥后再解密.表1中的数据显示,我们的方案在系统公/私钥尺寸,用户公/私钥尺寸和解密平均计算量等方面都明显优于文献[25,26]中的方案,特别地,我们的密文尺寸约为文献[26]中的20%.随后,我们通过两种扩大明文空间的方法来降低密文扩展比或节省计算量来提高方案的效率:第1种方法把明文空间由$\mathbb{Z}_2$变为$\mathbb{Z}_P$,在几乎不增加用户公/私钥存储代价的情况下,有效地降低密文扩展比;第2种方法把明文空间由$\mathbb{Z}_2$变为$\mathbb{Z}_2^t$,在无需增大原方案参数的情况下,通过加密时共享了一些随机值、解密时共用了一些密文分量,既节省了计算量又缩短了密文长度,所付出的代价却是可接受的,即用户公/私钥的尺寸随t的增大而仿线性增大.这样,允许选择适当的t保证不增加方案的渐进复杂度.我们通过引入逐步定比特填充法,给出了多比特的无证书加密方案.

本文第1节说明有关的符号约定、LWE问题、格的陷门生成和原像抽样算法等必要的知识.第2节给出无证书加密的概念和安全模型.第3节提出单比特和多比特的无证书加密方案.第4节分析方案的正确性、安全性、参数设置和效率等.最后总结全文.

1 预备知识

1.1 符号说明

设$n,m\in\mathbb{Z}$且$n>0$,素数$q>0$,记$[n]=\{1,2,\ldots,n\}$,$[m]_q=m \bmod q\in(-q/2,q/2]$,$poly(n)$表示关于$n$的任意多项式函数,$negl(n)=o(1/poly(n))$是一个可忽略的函数(当$n\to+\infty$时).符号$x\leftarrow X$在不同的环境中有不同的含义,具体来说,若$X$为一个集合,则$x\leftarrow X$表示$x$是从$X$中均匀随机抽取;若$X$为随机变量的概率分布,则$x\leftarrow X$表示$x$是以概率分布$X$抽取;若$X$为一个多项式时间的算法,则$x\leftarrow X$表示$x$是算法$X$的输出结果.对正数$B$和数集上的分布列$\{\mathcal{Y}_n\}_{n\in\mathbb{N}}$,若满足$P_{x\leftarrow\mathcal{Y}_n}(|x|<B)=1-negl(n)$,则称$\mathcal{Y}$以$B$为界的分布并记为$\mathcal{Y}_B$.用小写/小写斜黑体/大写斜黑体拉丁字母表示标量/列向量/矩阵,如$a/\boldsymbol{a}/\boldsymbol{A}$,而用符号$\boldsymbol{A}^T$表示矩阵的转置,用符号$\mathcal{S}_1(\boldsymbol{A})$表示矩阵$\boldsymbol{A}$的最大奇异值.符号$(a|\boldsymbol{b}^T)$为标量$a$和向量$\boldsymbol{b}$的级联,该符号可自然地推广到向量和矩阵间的级联.运算$\boldsymbol{A}\otimes\boldsymbol{B}$表示两个矩阵的张量积.除非特别说明,文中的对数$\log x$均以2为底,总是用$\boldsymbol{I}_n$表示$n$阶单位矩阵,$\boldsymbol{g}^T=(1,2,4,\ldots,2^{k-1})\in\mathbb{Z}_q^k$表示$k=\lceil\log q\rceil$维本原向量,$\boldsymbol{G}$表示矩阵$\boldsymbol{I}_n\otimes\boldsymbol{g}^T$,$D_{\Lambda,s}$表示中心在原点、偏差为$s$的格$\Lambda$上的离散高斯分布.

1.2 LWE问题及误差分布

LWE问题[1],尤其是判定LWE问题,是保证格上加密方案[1,2,5,12]安全的基石.判定LWE问题就是区分两种在$\mathbb{Z}_q^n\times\mathbb{Z}_q$上的概率分布.

© 中国科学院软件研究所 http://www.jos.org.cn

- 一种是均匀分布 $\mathcal{U}:(\boldsymbol{a},b)\leftarrow\mathbb{Z}_q^n\times\mathbb{Z}_q$;
- 另一种定义如下:

$$A_{\boldsymbol{s},\chi}:(\boldsymbol{a},\boldsymbol{a}^T\boldsymbol{s}+e)\in\mathbb{Z}_q^n\times\mathbb{Z}_q,\text{其中},\boldsymbol{s}\leftarrow\mathbb{Z}_q^n,e\leftarrow\chi \tag{1}$$

给定上述两种分布和任意的正整数 $m=poly(n)$,构造分布 $\mathcal{G}_m:\{0,1\}\rightarrow\{\mathcal{U}^m,A_{s,\chi}^m\}$,即

$$\mathcal{G}_m(b)=\begin{cases}\mathcal{U}^m, & b=0\\ A_{s,\chi}^m, & b=1\end{cases}.$$

定义 1(平均情况). 判定 LWE 问题 $DLWE_{n,m,q,\chi}$就是要求区分器$\mathcal{D}$在未知 b 的条件下,给定$(\boldsymbol{A},\boldsymbol{b})\leftarrow\mathcal{G}_m(b)$,以不可忽略的概率输出 $b'\in\{0,1\}$,并满足 $b'=b$.这里,$(\boldsymbol{A},\boldsymbol{b})\in\mathbb{Z}_q^{n\times m}\times\mathbb{Z}_q^m$.

判定 LWE 问题是困难的,并存在从最差到平均情况的困难性归约.

引理 1[1]. 设 n 是安全参数,对素数 $q=q(n)$和$\alpha\in(0,1)$,满足 $q\alpha>2\sqrt{n}$, 存在一个有效的误差分布χ,满足:若存在一个有效的算法(可能是量子的)能够解决 $DLWE_{n,m,q,\chi}$,则存在有效的量子算法解决最差情况下近似因子为 $\tilde{O}(n/\alpha)$ 的 SIVP 和 GapSVP 问题.

根据现有结果[8,27,28],公式(1)可作如下修改:

$$A_{\boldsymbol{s},\chi}:(\boldsymbol{a},\boldsymbol{a}^T\boldsymbol{s}+pe)\in\mathbb{Z}_q^n\times\mathbb{Z}_q,\text{其中},p\in\mathbb{Z}_q^*,\boldsymbol{s}\leftarrow\chi^n,e\leftarrow\chi \tag{2}$$

对引理 1 中的误差分布,本文取 $\chi=D_{\mathbb{Z},q\alpha}$, 则有如下重要不等式:

引理 2[2]. 设 $\boldsymbol{x}\leftarrow D_{\mathbb{Z}^n,s},x\leftarrow D_{\mathbb{Z},s}$, 若 $s\geqslant\omega\left(\sqrt{\log n}\right)$, 则不等式 $\|\boldsymbol{x}\|\leqslant s\sqrt{n}$ 和 $|x|\leqslant s\omega\left(\sqrt{\log n}\right)$ 以概率 $1-negl(n)$成立.

我们设计的无证书加密方案安全性归约到文献[2]第 7.1 节中对偶加密方案的简单变形和文献[12]第 3.1 节中的基本加密方案,分别记为 GPV-I 和 BGV-II.它们在判定 LWE 问题困难性假设下是语义安全的(indistinguishable CPA,简称 IND-CPA).这里只给出 GPV-I 的描述.

- 密钥生成算法:先选择 $\boldsymbol{A}\leftarrow\mathbb{Z}_q^{n\times m}$, 其中,$m\geqslant 2n\log q,n$ 为安全参数,$(2,q)=1$.再抽取私钥 $\boldsymbol{e}\leftarrow D_{\mathbb{Z}^m,r}$, 其中, $r>\omega\left(\sqrt{\log m}\right)$. 最后,计算公钥 $\boldsymbol{u}=\boldsymbol{A}\boldsymbol{e}\bmod q$.
- 加密算法:设明文 $b\in\{0,1\}$,选择 $\boldsymbol{s}\leftarrow\chi^n,\boldsymbol{x}\leftarrow\chi^m$ 和 $x\leftarrow\chi$,计算 $\boldsymbol{P}=\boldsymbol{A}^T\boldsymbol{s}+2\boldsymbol{x}\in\mathbb{Z}_q^m,c=\boldsymbol{u}^T\boldsymbol{s}+2x+b\in\mathbb{Z}_q$. 输出密文$(c,\boldsymbol{p})$.
- 解密算法:$b'=[(c-\boldsymbol{e}^T\boldsymbol{p})\bmod q]\bmod 2$.

1.3 剩余哈希引理(letfover Hash lemma)

Letfover Hash lemma 是本文设置参数的重要依据之一,它的简化版本[28]与双通函数族(a family of 2-universal functions)密切相关.

定义 2. 我们称函数族 $\mathcal{H}=\{h:X\rightarrow Y\}$ 是双通的(2-universal),如果对于任意相异的 $x_1,x_2\in X$,总有 $P_{h\leftarrow\mathcal{H}}(h(x_1)=h(x_2))=1/|Y|$成立.

一个重要的结论[28]:若 G 是一个有限的阿贝尔加法群,对于任意的整数 $m\geqslant 1$,向量 $\boldsymbol{a}\in G^m$,则有函数族$\mathcal{H}=\{h_{\boldsymbol{a}}:\{0,1\}^m\rightarrow G;\boldsymbol{x}\mapsto h_{\boldsymbol{a}}(\boldsymbol{x})=\boldsymbol{a}^T\boldsymbol{x}\}$是 2-universal.

特别地,取群 $G=\mathbb{Z}_q^n$, 向量 $\boldsymbol{A}\in G^m=\mathbb{Z}_q^{n\times m}$, 则有 $\mathcal{H}=\{h_A:\{0,1\}^m\rightarrow\mathbb{Z}_q^n;\boldsymbol{x}\mapsto h_A(\boldsymbol{x})=\boldsymbol{A}\boldsymbol{x}\}$ 也是 2-universal.

引理 3[28]. 若$\mathcal{H}=\{h:X\rightarrow Y\}$是 2-universal 哈希函数族,$h\leftarrow\mathcal{H},x\leftarrow X$ 均匀独立地选取,则$(h,h(x))$的分布与$\mathcal{H}\times Y$上的均匀分布的距离至多为 $\frac{1}{2}\sqrt{|Y|/|X|}$.

1.4 格的陷门生成和原像抽样算法

本文采用文献[6]中格的陷门生成及原像抽样算法,其部分结果由引理 4 给出.

引理 4[6]. 若给定整数 $n>0,q>1$ 和 $m=O(n\log q)$(足够大),则存在一个有效的随机算法 $GenTrap(1^n,1^m,q)$满足

© 中国科学院软件研究所 http://www.jos.org.cn

$(\boldsymbol{A},\boldsymbol{R})\leftarrow GenTrap(1^n,1^m,q)$,其中,$\boldsymbol{R}$ 为陷门,输出矩阵 $\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$ 的分布与集合 $\mathbb{Z}_q^{n\times m}$ 上的均匀分布以不高于 $negl(n)$ 的概率可区分.此外,还存在有效的随机原像抽样算法 $SampleD(\cdot)$,对任何的向量 $\boldsymbol{u}\in\mathbb{Z}_q^n$ 和足够大的正实数 $s=O\left(\sqrt{n\log q}\right)\cdot\omega\left(\sqrt{\log n}\right)$,若以 $\boldsymbol{A},\boldsymbol{R},\boldsymbol{u},s$ 作为输入,则有 $\boldsymbol{x}\leftarrow SampleD(\boldsymbol{A},\boldsymbol{R},\boldsymbol{u},s)$满足输出向量 $\boldsymbol{x}\in\mathbb{Z}_q^m$ 的分布与格 $\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A})$ 上的高斯分布 $D_{\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A}),s\cdot\omega\left(\sqrt{\log n}\right)}$ 以不高于 $negl(n)$的概率可区分.

2 无证书加密的概念和安全模型

无证书加密方案涉及到一个密钥生成中心(KGC)、发送方和接收方.它由系统参数生成(*Setup*)、部分私钥提取(*ExtractPPK*)、设置公/私钥(*Setkey*)、加密(*Enc*)和解密(*Dec*)这 5 种算法组成.各算法的定义请参考文献[18,24].为方便,用符号 *params*,*MPK*,*MSK*,*ID*,*PK*,*SK*,*PPK*,*SV* 分别表示公开参数、系统公钥、系统私钥、用户身份、用户公钥、用户私钥、用户部分私钥、用户秘密值.

无证书加密方案中攻击者按能力分为第 1 类攻击者$\mathcal{A}_{\mathrm{I}}$和第 2 类攻击者$\mathcal{A}_{\mathrm{II}}$.$\mathcal{A}_{\mathrm{I}}$不能获知 *MSK*,但可在公钥空间随意取值以替代任何用户的 *PK*.$\mathcal{A}_{\mathrm{II}}$可知 *MSK*,可如$\mathcal{A}_{\mathrm{I}}$那样替换除了目标身份之外任何用户的 *PK*.

无证书加密的 IND-CPA 安全是通过区分困难问题的挑战者$\mathcal{B}$和攻击者$\mathcal{A}\in\{\mathcal{A}_{\mathrm{I}},\mathcal{A}_{\mathrm{II}}\}$之间的游戏来定义.

设置系统参数:挑战者$\mathcal{B}$输入安全参数 n,运行$(params,MSK,MPK)\leftarrow Setup(1^n)$.$\mathcal{B}$将$(params,MPK)$发送给$\mathcal{A}$.若$\mathcal{A}$是$\mathcal{A}_{\mathrm{II}}$,则还需同时把 *MSK* 给$\mathcal{A}_{\mathrm{II}}$.这样,$\mathcal{A}_{\mathrm{II}}$无需进行部分私钥询问.

询问回应:$\mathcal{A}$可以有限次地访问受控于$\mathcal{B}$的预言器(以及可能存在的 *hash* 函数随机预言器).为此,$\mathcal{B}$以列表的方式记录与$\mathcal{A}$交互过程中产生的数据,初始为空表.我们的安全模型允许攻击者询问用户的秘密值以强化其攻击能力[24].同时,$\mathcal{A}$具有获知部分私钥和秘密值的能力就可自己生成用户私钥,从而也无需用户私钥询问.

- 生成用户询问:$\mathcal{A}$提供一个身份 *ID*,$\mathcal{B}$运行 $PPK\leftarrow ExtractPPK(ID,params)$ 和 $(SV,PK)\leftarrow Setkey(ID,params)$.$\mathcal{B}$把上述数据加入列表并返回相应的 *PK*.特别地,如果涉及到计算 *hash*(*ID*),且该 *hash* 函数被作为随机预言器,则$\mathcal{B}$需要把 *hash*(*ID*)值也加入列表并连同相应的 *PK* 一起返给$\mathcal{A}$.
- 部分私钥询问:$\mathcal{A}_{\mathrm{I}}$ 给出一个身份 *ID*,若该身份已生成,则$\mathcal{B}$查表获取 *PPK*;否则,$\mathcal{B}$运行 $PPK\leftarrow ExtractPPK(ID,params)$获取 *PPK*.$\mathcal{B}$把上述数据加入列表并返回相应的 *PPK*.
- 公钥替换询问:$\mathcal{A}$给出一个身份 *ID* 和新公钥 *PK*′,$\mathcal{B}$重置其公钥为 *PK*′.
- 秘密值询问:$\mathcal{A}$给出一个身份 *ID*,若该身份已生成,$\mathcal{B}$查表获取 *SV*;否则,$\mathcal{B}$运行$(SV,PK)\leftarrow Setkey(ID,params)$.$\mathcal{B}$把上述数据加入列表并返回相应的 *SV*.

挑战:一旦$\mathcal{A}$决定结束询问并输出两个挑战明文 $m_0,m_1\in\mathcal{M}$和一个挑战身份 ID^*给$\mathcal{B}$.$\mathcal{B}$执行以下步骤:

(1) 当$\mathcal{A}=\mathcal{A}_{\mathrm{I}}$时,若 ID^*当前所对应的公钥未被替换,或者 ID^*当前所对应的公钥被替换为有效的公钥(即公钥取自公钥空间且具有合法公钥的结构),且其部分私钥未被询问过,则转入步骤(3);若 ID^*当前所对应的公钥被替换成有效的公钥且其部分私钥已被询问过,则终止游戏;若 ID^*当前所对应的公钥被替换成无效的公钥,则以$\mathcal{A}$失败而结束游戏.

(2) 当$\mathcal{A}=\mathcal{A}_{\mathrm{II}}$时,检查 ID^*应满足其公钥没被替换且曾未询问其秘密值;否则,终止游戏.

(3) 随机选择 $b\in\{0,1\}$,计算 $c^*\leftarrow Enc(params,ID^*,PK_{ID^*},m_b)$,把 c^*返回给$\mathcal{A}$.

猜测:最后,$\mathcal{A}$输出其猜测值 $b'\in\{0,1\}$给$\mathcal{B}$.

$\mathcal{A}$获胜,当且仅当 $b=b'$.$\mathcal{A}$在游戏中获胜的优势记为$\varepsilon=2|P(b=b')-1/2|$.

定义 3. 若不存在任何多项式有界的攻击者$\mathcal{A}\in\{\mathcal{A}_{\mathrm{I}},\mathcal{A}_{\mathrm{II}}\}$,以一个不可忽视的优势在上述游戏中胜出,则称该无证书加密方案是自适应选择消息和身份攻击下语义安全的.

© 中国科学院软件研究所 http://www.jos.org.cn

3 无证书加密

本节首先设计明文空间为$\mathbb{Z}_2$的单比特无证书加密方案,然后再扩展为大明文空间上的方案.

3.1 单比特的无证书加密

我们方案涉及到 KGC 和用户,KGC 利用文献[6]的陷门生成算法为用户生成部分私钥,而用户利用带误差的学习问题来生成自己的秘密值和公钥.具体算法如下:

- *Setup*(1^n):设正整数 n 为安全参数,素数 $q=ploy(n)$,$\alpha\in(0,1)$,$k=\lceil \log q \rceil$,$N=2nk$ 和正整数 $M=O(n\log q)$,误差分布 $\chi_B = D_{\mathbb{Z},q\alpha}$. 根据引理2,取 $B=q\alpha\cdot\omega\left(\sqrt{\log n}\right)$.$H:\{0,1\}^*\to\mathbb{Z}_q^n$ 是一个安全的密码哈希函数.根据引理4,密钥生成中心 KGC 运行 $(\boldsymbol{A},\boldsymbol{R})\leftarrow Gentrap(1^n,1^N,q)$,其中,$\bar{\boldsymbol{A}}\leftarrow\mathbb{Z}_q^{n\times nk}$,$\boldsymbol{R}\leftarrow D_{\mathbb{Z},s_1}^{nk\times nk}$,$\boldsymbol{A}=(\bar{\boldsymbol{A}}\,|\,\boldsymbol{G}-\bar{\boldsymbol{A}}\boldsymbol{R})\in\mathbb{Z}_q^{n\times N}$,$s_1=4\omega\left(\sqrt{\log n}\right)>4\eta_\varepsilon(\mathbb{Z})$. 设置 $(MPK,MSK)=(\boldsymbol{A},\boldsymbol{R})\in\mathbb{Z}_q^{n\times N}\times\mathbb{Z}_B^{nk\times nk}$,$s_2=\sqrt{7(s_1(\boldsymbol{R})^2+1)}$ 为原像抽样算法的参数,消息空间$\mathbb{Z}_2$.公开参数 $params=\{n,k,N,M,q,\alpha,s_2,\chi_B,\mathbb{Z}_2,H,\boldsymbol{A}\}$.
- *ExtractPPK*(ID,$params$):KGC 对用户提交的身份 $ID\in\{0,1\}^*$认证后,计算部分私钥 $\boldsymbol{d}\in\mathbb{Z}_q^N$,并利用安全信道传 $\boldsymbol{d}$ 给该用户.用户验证应满足 $\boldsymbol{A}\boldsymbol{d}=\boldsymbol{u}$ 且 $\|\boldsymbol{d}\|\leqslant s_2\sqrt{N}\cdot\omega\left(\sqrt{\log n}\right)$:
  (1) 计算 $\boldsymbol{u}=H(ID)$,并从矩阵 $\boldsymbol{A}=(\bar{\boldsymbol{A}}\,|\,\boldsymbol{G}-\bar{\boldsymbol{A}}\boldsymbol{R})\in\mathbb{Z}_q^{n\times N}$ 中截取前 nk 列子矩阵 $\bar{\boldsymbol{A}}$;
  (2) 抽取 $\boldsymbol{d}\leftarrow SampleD(\bar{\boldsymbol{A}},\boldsymbol{R},\boldsymbol{u},s_2)$, 其中, $\boldsymbol{d}\in\mathbb{Z}_q^N$.
- *Setkey*(ID,$params$):身份为 ID 的用户选取自己的秘密值 $\boldsymbol{x}\leftarrow\chi_B^n$, 设置私钥 $SK=(\boldsymbol{x},\boldsymbol{d})\in\mathbb{Z}_q^n\times\mathbb{Z}_q^N$, 并按如下步骤设置公钥 PK:
  (1) 任选矩阵 $\boldsymbol{B}\leftarrow\mathbb{Z}_q^{n\times M}$, 向量 $\boldsymbol{e}_1\leftarrow\chi_B^M$;
  (2) 计算 $\boldsymbol{b}=\boldsymbol{B}^T\boldsymbol{x}+2\boldsymbol{e}_1 \bmod q\in\mathbb{Z}_q^M$;
  (3) 设置公钥 $PK=(\boldsymbol{b}\,|\,\boldsymbol{B}^T)\in\mathbb{Z}_q^{M\times(1+n)}$.
- *Enc*(m,ID,PK,$params$):欲对消息 $m\in\mathbb{Z}_2$ 加密后发送给身份为 ID、公钥为 $PK=(\boldsymbol{b}|\boldsymbol{B}^T)$的接收方,发送方执行如下步骤:
  (1) 任选向量 $\boldsymbol{r}\leftarrow\{0,1\}^M$, $\boldsymbol{s}\leftarrow\chi_B^n$,$\boldsymbol{e}_2\leftarrow\chi_B^N$ 和 $e\leftarrow\chi_B$;
  (2) 计算 $\boldsymbol{v}_1=\boldsymbol{B}\boldsymbol{r}\in\mathbb{Z}_q^n$,$\boldsymbol{v}_2=\boldsymbol{A}^T\boldsymbol{s}+2\boldsymbol{e}_2\in\mathbb{Z}_q^N$;
  (3) 计算 $v=m+\langle\boldsymbol{b},\boldsymbol{r}\rangle+\langle\boldsymbol{s},H(ID)\rangle+2e \bmod q$;
  (4) 输出密文 $\boldsymbol{c}=(v\,|\,\boldsymbol{v}_1\,|\,\boldsymbol{v}_2)\in\mathbb{Z}_q^{1+n+N}$.
- *Dec*($\boldsymbol{c}$,SK,$params$):接收方获得密文 $\boldsymbol{c}=(v|\boldsymbol{v}_1|\boldsymbol{v}_2)$后,用其私钥 $SK=(\boldsymbol{x},\boldsymbol{d})$进行解密:

$$m=[v-\langle\boldsymbol{v}_1,\boldsymbol{x}\rangle-\langle\boldsymbol{v}_2,\boldsymbol{d}\rangle]_q \bmod 2.$$

3.2 多比特的无证书加密

把第 3.1 节方案的明文空间由$\mathbb{Z}_2$ 扩大到$\mathbb{Z}_p$(由公式(2)可知,只要满足 $p<<q$ 且$(p,q)=1$,并相应修改方案中 LWE 的计算公式,把解密公式中 mod 2 改为 mod p 即可)以有效地降低密文扩展比.另外,我们还可以如文献[2,29]的做法,把它由单比特加密扩展成多比特加密(即,把$\mathbb{Z}_2$ 变为 $\mathbb{Z}_2^t$).为此,取定 $b\in\{0,1\}$,设身份 $ID\in\{0,1\}^\ell$,则对身份 ID 做第 1 次扩充得到身份 $ID_1=(ID|b)$,从第 2 次扩充起,第 i 次扩充的身份为 $ID_i=(ID_{i-1}|b)$,其中,$2\leqslant i\leqslant t$.为避免不同用户之间一个用户的身份是另一个的前缀,用参数ℓ规定了所有用户申请认证的身份为定长比特串;否则,会存在安全漏洞.例如,假设 $t=2$,合法用户 U 的身份为 1001,攻击者选择 100 和 10011 这两个身份就可从 KGC 合法地获得与用户 U 等效的部分私钥.我们把上述对一个定长身份逐比特地填充固定比特来确定多个身份的方法称为逐步定比特填充法.下面给出该种扩展方法对应的加密方案,具体算法如下:

- *Setup*(1^n,1^t,1^ℓ):同第 3.1 节 *Setup*(1^n)算法,只是多了输入参数 t 和ℓ,其中,t 是明文向量的维数,ℓ为系统

© 中国科学院软件研究所 http://www.jos.org.cn

中用户身份向量的维数且身份用定长比特串表示.为保证用户公钥安全和不增加方案的渐进复杂度,这里限定正整数 $t=\Theta(n)$.这样,$(MPK,MSK)=(\boldsymbol{A},\boldsymbol{R})$,公开参数 $params=\{n,k,N,M,q,\alpha,s_2,\chi_B,\ell,\mathbb{Z}_2^t,H,\boldsymbol{A}\}$.

- *ExtractPPK*(*ID*,*params*):KGC 对用户所提交的定长身份 $ID\in\{0,1\}^{\ell}$ 认证后,计算部分私钥 $\boldsymbol{D}$,并用安全信道传给该用户.用户验证应有 $\boldsymbol{A}\boldsymbol{d}_i=\boldsymbol{u}_i$ 且 $\|\boldsymbol{d}_i\|\leqslant s_2\sqrt{N}\cdot\omega\left(\sqrt{\log n}\right)$, $i\in[t]$:
  (1) 计算 $(H(ID),H(ID|1),H(ID|11),...,H(ID|\underbrace{11...1}_{t-1}))=(\boldsymbol{u}_1,\boldsymbol{u}_2,\boldsymbol{u}_3,...,\boldsymbol{u}_t)=\boldsymbol{U}\in\mathbb{Z}_q^{n\times t}$,并从矩阵 $\boldsymbol{A}=(\bar{\boldsymbol{A}}|\boldsymbol{G}-\bar{\boldsymbol{A}}\boldsymbol{R})\in\mathbb{Z}_q^{n\times N}$ 中截取前 *nk* 列子矩阵 $\bar{\boldsymbol{A}}$;
  (2) 抽取 $\boldsymbol{d}_i\leftarrow SampleD(\bar{\boldsymbol{A}},\boldsymbol{R},\boldsymbol{u}_i,s_2)$,其中,$\boldsymbol{d}_i\in\mathbb{Z}_q^N$,$i\in[t]$.令 $(\boldsymbol{d}_1,\boldsymbol{d}_2,...,\boldsymbol{d}_t)=\boldsymbol{D}\in\mathbb{Z}_q^{N\times t}$.
- *Setkey*(*ID*,*params*):身份为 *ID* 的用户选取自己的秘密值 $\boldsymbol{x}_i\leftarrow\chi_B^n$,其中,$i\in[t]$.令$(\boldsymbol{x}_1,\boldsymbol{x}_2,\ldots,\boldsymbol{x}_t)=\boldsymbol{X}\in\mathbb{Z}_q^{n\times t}$,置私钥 $SK=(\boldsymbol{X}^T|\boldsymbol{D}^T)\in\mathbb{Z}_q^{t\times(n+N)}$,并设置其公钥 *PK* 如下:
  (1) 任选矩阵 $\boldsymbol{B}\leftarrow\mathbb{Z}_q^{n\times M}$,向量 $\boldsymbol{e}_{1i}\leftarrow\chi_B^M$,其中,$i\in[t]$;
  (2) 计算 $\boldsymbol{b}_i=\boldsymbol{B}^T\boldsymbol{x}_i+2\boldsymbol{e}_{1i}\bmod q\in\mathbb{Z}_q^M$;
  (3) 设置 $\bar{\boldsymbol{B}}=(\boldsymbol{b}_1,\boldsymbol{b}_2,...,\boldsymbol{b}_t)\in\mathbb{Z}_q^{M\times t}$、公钥 $PK=(\bar{\boldsymbol{B}}|\boldsymbol{B}^T)\in\mathbb{Z}_q^{M\times(t+n)}$.
- *Enc*(**m**,*ID*,*PK*,*params*):欲对消息 $\boldsymbol{m}\in\mathbb{Z}_2^t$ 加密后发送给身份为 *ID*、公钥为 $PK=(\bar{\boldsymbol{B}}|\boldsymbol{B}^T)$ 的接收方,发送方执行:
  (1) 任选向量 $\boldsymbol{r}\leftarrow\{0,1\}^M$,$\boldsymbol{s}\leftarrow\chi_B^n$,$\boldsymbol{e}_2\leftarrow\chi_B^N$ 和 $\boldsymbol{e}\leftarrow\chi_B^t$;
  (2) 计算 $\boldsymbol{v}_1=\boldsymbol{B}\boldsymbol{r}\in\mathbb{Z}_q^n$,$\boldsymbol{v}_2=\boldsymbol{A}^T\boldsymbol{s}+2\boldsymbol{e}_2\in\mathbb{Z}_q^N$;
  (3) 计算 $\boldsymbol{U}=(H(ID),H(ID|1),...,H(ID|11...1))\in\mathbb{Z}_q^{n\times t}$;
  (4) 计算 $\boldsymbol{v}=\boldsymbol{m}+\bar{\boldsymbol{B}}^T\boldsymbol{r}+\boldsymbol{U}^T\boldsymbol{s}+2\boldsymbol{e}\bmod q$;
  (5) 输出密文 $\boldsymbol{c}=(\boldsymbol{v}|\boldsymbol{v}_1|\boldsymbol{v}_2)\in\mathbb{Z}_q^{t+n+N}$.
- *Dec*(**c**,*SK*,*params*):接收方获得密文 $\boldsymbol{c}=(\boldsymbol{v}|\boldsymbol{v}_1|\boldsymbol{v}_2)$后,使用其私钥 $SK=(\boldsymbol{X}^T|\boldsymbol{D}^T)$进行解密:

$$\boldsymbol{m}=[\boldsymbol{v}-\boldsymbol{X}^T\boldsymbol{v}_1-\boldsymbol{D}^T\boldsymbol{v}_2]_q \bmod 2.$$

4 方案分析

本节先从所给方案的正确性、安全性入手,然后根据前面二者的要求去设置参数并讨论其效率.容易看出,只要单比特方案是正确和安全的,必然可推出多比特方案的相应性质.因此,下面只讨论单比特方案的性质,并把它简记为 CLPKE.

4.1 正确性

定理 1. 我们称上述的 CLPKE 是正确的,若对任意的消息 $m\in\{0,1\}$、任意的身份 $ID=\{0,1\}^*$、公/私钥对 $(PK,SK)\leftarrow Setkey(ID,params)$和密文 $\boldsymbol{c}\leftarrow Enc(m,ID,PK,params)$,则 $m\leftarrow Dec(\boldsymbol{c},SK,params)$以 $1-negl(n)$概率成立.具体来说,对密文 $\boldsymbol{c}\leftarrow Enc(m,ID,PK,params)$,则有 $v-\langle\boldsymbol{v}_1,\boldsymbol{x}\rangle-\langle\boldsymbol{v}_2,\boldsymbol{d}\rangle=m+2error \bmod 2$.进一步地,若$|2error|<q/2$,则总有:

$$m=[v-\langle\boldsymbol{v}_1,\boldsymbol{x}\rangle-\langle\boldsymbol{v}_2,\boldsymbol{d}\rangle]_q \bmod 2.$$

证明:

$$v-\langle\boldsymbol{v}_1,\boldsymbol{x}\rangle-\langle\boldsymbol{v}_2,\boldsymbol{d}\rangle=m+\boldsymbol{x}^T\boldsymbol{B}\boldsymbol{r}+2\boldsymbol{e}_1^T\boldsymbol{r}+\boldsymbol{s}^T\boldsymbol{A}\boldsymbol{d}+2e-\boldsymbol{x}^T\boldsymbol{B}\boldsymbol{r}-\boldsymbol{d}^T\boldsymbol{A}^T\boldsymbol{s}-2\boldsymbol{d}^T\boldsymbol{e}_2=m+\underbrace{2e+2\boldsymbol{e}_1^T\boldsymbol{r}-2\boldsymbol{d}^T\boldsymbol{e}_2}_{2error} \bmod q.$$

当$|2error|=|2e+2\boldsymbol{e}_1^T\boldsymbol{r}-2\boldsymbol{d}^T\boldsymbol{e}_2|<q/2$时,则有 $m=[v-\langle\boldsymbol{v}_1,\boldsymbol{x}\rangle-\langle\boldsymbol{v}_2,\boldsymbol{d}\rangle]_q \bmod 2$ 成立. □

4.2 安全性

下面两个定理证明了 CLPKE 在两类自适应选择消息和身份攻击下是语义安全的.

定理 2. 在随机预言模型下,设$\mathcal{A}_1$是自适应选择消息和身份攻击下第 1 类攻击者,若在时间 *T* 内至多进行

© 中国科学院软件研究所 http://www.jos.org.cn

q_1次生成用户询问、q_2次部分私钥询问、q_3次公钥替换询问和q_4次秘密值询问后,以不可忽略的区分优势ε攻破 CLPKE,则存在一个概率多项式算法$\mathcal{B}$以区分优势$\varepsilon_{\mathcal{B}} \geqslant (1-1/q_1)^{q_2}\cdot 1/q_1\cdot\varepsilon - negl(n)$,在不超过 $T+q_1t_1+q_2t_2+q_3t_3+q_4t_4$时间间隔内攻破 GPV-I 的 CPA 安全性,其中,$t_1(t_2,t_3,t_4)$表示一次生成用户(部分私钥、公钥替换、秘密值)询问所需的时间.

证明:假定概率多项式算法$\mathcal{F}$是 GPV-I 的挑战者;而算法$\mathcal{B}$在攻击 GPV-I 的游戏中充当 CPA 攻击者,同时又是攻击 CLPKE 的游戏中的挑战者.下面论述如何根据算法$\mathcal{A}_1$和$\mathcal{F}$去构造算法$\mathcal{B}$.

$\mathcal{B}$不仅需要把他攻击 GPV-I 的任务嵌入到攻击 CLPKE 的游戏中并借助$\mathcal{A}_1$来完成该任务,而且要为$\mathcal{A}_1$提供与真实攻击不可区分的场景.为此,我们通过游戏序列 Game 0,Game 1 和 Game 2 来完成.设 $Game_i$=1 表示 Game i 中$\mathcal{A}_1$获胜,则 $2|P[Game_i=1]-1/2|$就是 Game i 中$\mathcal{A}_1$的区分优势,$i\in\{0,1,2\}$.

Game 0:它就是第 2 节描述的关于无证书加密 IND-CPA 安全的真实攻击过程,涉及$\mathcal{A}_1$和$\mathcal{B}$间的交互.故有:

$$2|P[Game_0=1]-1/2|=\varepsilon.$$

Game 1:它只是把 Game 0 的生成用户询问中提取用户部分私钥的算法改变为:选 $\boldsymbol{d}_i \leftarrow D_{\mathbb{Z}^N,s_2\cdot\omega(\sqrt{\log n})}$,计算 $\boldsymbol{u}_i=\boldsymbol{A}\boldsymbol{d}_i$ 满足(*,$\boldsymbol{u}_i$,*,*,*,*,*)以前未出现在$\mathcal{H}$列表中,并令 $H(ID_i)=\boldsymbol{u}_i$;否则,重新抽取 $\boldsymbol{d}_i$.这样,Game 1 提取用户部分私钥的算法不再使用系统私钥 $\boldsymbol{R}$.根据文献[2]中原像抽样函数的性质,Game 0 和 Game 1 所得到的部分私钥的分布是不可区分的.即 Game 0 和 Game 1 对$\mathcal{A}_1$是不可区分的.因此,$|P[Game_1=1]-P[Game_0=1]|=negl(n)$.

Game 2:它只是把 Game 1 的系统公钥 $\boldsymbol{A}$ 的生成方式改变为 $\boldsymbol{A}\leftarrow\mathbb{Z}_q^{n\times m}$,其余同 Game 1.因为 Game 1 抽取用户部分私钥已经不再使用矩阵 $\boldsymbol{A}$ 的陷门 $\boldsymbol{R}$,根据引理 4,$(\boldsymbol{A},\boldsymbol{R})\leftarrow GenTrap(1^n,1^m,q)$和 $\boldsymbol{A}\leftarrow\mathbb{Z}_q^{n\times m}$ 输出 $\boldsymbol{A}$ 的分布是不可区分的.即,Game 1 和 Game 2 对$\mathcal{A}_1$是不可区分的.故有$|P[Game_2=1]-P[Game_1=1]|=negl(n)$.这样,我们有:

$$\begin{aligned}\varepsilon-2\,|\,P[Game_2=1]-1/2\,|&=2\,|\,P[Game_0=1]-1/2\,|-2\,|\,P[Game_2=1]-1/2\,|\\&\leqslant 2\,|\,P[Game_0=1]-P[Game_1=1]\,|+2\,|\,P[Game_1=1]-P[Game_2=1]\,|\\&\leqslant negl(n).\end{aligned}$$

进一步地,有 $2|P[Game_2=1]-1/2|\geqslant\varepsilon-negl(n)$.

既然 Game 2 中系统公钥 $\boldsymbol{A}$ 是随机均匀选取的,这为$\mathcal{B}$嵌入他所解决的问题提供了可能,具体过程如下:

系统参数的设置:$\mathcal{F}$设置并传给算法$\mathcal{B}$关于 GPV-I 的公开参数 $(n,q,\boldsymbol{A}\in\mathbb{Z}_q^{n\times N},\alpha,r,\chi_B,N=2n\lceil\log q\rceil)$和公钥 $\boldsymbol{u}^*\in\mathbb{Z}_q^n$.$\mathcal{B}$根据上述公开参数去设置 CLPKE 的系统参数 $params=\{n,k,N,M,q,\alpha,s_2,\chi_B,\mathbb{Z}_2,H,\boldsymbol{A}\}$,使两个加密方案的公共参数取值一致.$\mathcal{B}$把系统参数 $params$ 传送$\mathcal{A}_1$.

询问应答:$\mathcal{B}$控制并把哈希函数 H 作为随机预言器.$\mathcal{A}_1$可以自适应地做生成用户、部分私钥、公钥替换、秘密值等询问.简单起见,假设$\mathcal{A}_1$的询问都是不同的.$\mathcal{B}$维护$\mathcal{H}$列表,初始为空.列表中每一项的格式为

$$(ID,\boldsymbol{u},\boldsymbol{d},\boldsymbol{x},\boldsymbol{b},\boldsymbol{B},\boldsymbol{e}).$$

- 生成用户询问($Create(\cdot)$):$\mathcal{B}$随机选择 $t\in[q_1]$.当$\mathcal{A}_1$询问 $Create(ID_i)$时,$\mathcal{B}$执行:
  (1) 若 $i=t$,则置 $H(ID_t)=\boldsymbol{u}^*$,$\boldsymbol{d}_t=\perp$($\perp$表示该值未知,下同);否则,选 $\boldsymbol{d}_i\leftarrow D_{\mathbb{Z}^N,s_2\cdot\omega(\sqrt{\log n})}$,计算 $\boldsymbol{u}_i=\boldsymbol{A}\boldsymbol{d}_i$ 满足(*,$\boldsymbol{u}_i$,*,*,*,*,*)以前未出现在$\mathcal{H}$列表中;否则,重新抽取 $\boldsymbol{d}_i$.
  (2) 选择 $\boldsymbol{B}_i\leftarrow\mathbb{Z}_q^{n\times M}$,$\boldsymbol{x}_i\leftarrow\chi_B^n$,$\boldsymbol{e}_i\leftarrow\chi_B^M$,计算 $\boldsymbol{b}_i=\boldsymbol{B}_i^T\boldsymbol{x}_i+2\boldsymbol{e}_i \bmod q$.
  (3) 把元组$(ID_i,\boldsymbol{u}_i,\boldsymbol{d}_i,\boldsymbol{x}_i,\boldsymbol{b}_i,\boldsymbol{B}_i,\boldsymbol{e}_i)$添加到$\mathcal{H}$列表中,并把$(ID_i,\boldsymbol{u}_i,\boldsymbol{b}_i,\boldsymbol{B}_i)$给$\mathcal{A}_1$.

不失一般性地假设$\mathcal{A}_1$下面询问所涉及的身份 ID_i 均已生成:

- 部分私钥询问($PPkey(\cdot)$):当$\mathcal{A}_1$询问 $PPkey(ID_i)$时,$\mathcal{B}$执行:当 $i=t$ 时,终止协议;否则,在$\mathcal{H}$列表中按身份 ID_i 查找元组$(ID_i,\boldsymbol{u}_i,\boldsymbol{d}_i,\boldsymbol{x}_i,\boldsymbol{b}_i,\boldsymbol{B}_i,\boldsymbol{e}_i)$,将 $\boldsymbol{d}_i$ 返给$\mathcal{A}_1$.
- 公钥替换询问($Replace(\cdot,\cdot)$):当$\mathcal{A}_1$做 $Replace(ID_i,(\boldsymbol{b}_i',\boldsymbol{B}_i'))$询问时,$\mathcal{B}$根据 ID_i 检查$\mathcal{H}$列表,把元组$(ID_i,\boldsymbol{u}_i,\boldsymbol{d}_i,\boldsymbol{x}_i,\boldsymbol{b}_i,\boldsymbol{B}_i,\boldsymbol{e}_i)$替换为$(ID_i,\boldsymbol{u}_i,\boldsymbol{d}_i,\perp,\boldsymbol{b}_i',\boldsymbol{B}_i',\perp)$.
- 秘密值询问($Value(\cdot)$):收到$\mathcal{A}_1$询问 $Value(ID_i)$后,$\mathcal{B}$根据 ID_i 检查$\mathcal{H}$列表并执行:若 $\boldsymbol{x}_i\neq\perp$,则返回 $\boldsymbol{x}_i$ 给$\mathcal{A}_1$;

© 中国科学院软件研究所 http://www.jos.org.cn

否则,输出⊥.

挑战:一旦$\mathcal{A}_{\mathrm{I}}$决定结束询问,他输出两个不同的挑战明文 $m_0,m_1\in\{0,1\}$和一个挑战身份 ID^*给$\mathcal{B}$.$\mathcal{B}$做出如下回应:

(1) 若$ID^*\neq ID_t$,则$\mathcal{B}$终止协议;否则,$\mathcal{B}$根据ID^*检查$\mathcal{H}$列表获取元组$(ID^*,\boldsymbol{u}^*,\perp,\boldsymbol{x}_t,\boldsymbol{b}_t,\boldsymbol{B}_t,\boldsymbol{e}_t)$或$(ID^*,\boldsymbol{u}^*,\perp,\perp,\boldsymbol{b}'_t,\boldsymbol{B}'_t,\perp)$,其中,前者对应于$ID^*$的公钥没有被替换,后者则是其公钥被替换了.

(2) 若ID^*的公钥没有被替换,则令$(\boldsymbol{b}^*,\boldsymbol{B}^*)=(\boldsymbol{b}_t,\boldsymbol{B}_t)$并转入步骤(4);否则,执行步骤(3).

(3) 对替换后的公钥$(\boldsymbol{b}'_t,\boldsymbol{B}'_t)$进行有效性测试,若不是有效的公钥,则以$\mathcal{A}_{\mathrm{I}}$失败而结束游戏;否则,$\mathcal{B}$设置$(\boldsymbol{b}^*,\boldsymbol{B}^*)=(\boldsymbol{b}'_t,\boldsymbol{B}'_t)$并转入步骤(4).公钥$(\boldsymbol{b}'_t,\boldsymbol{B}'_t)$有效性测试在$\mathcal{A}_{\mathrm{I}}$和$\mathcal{B}$之间进行:$\mathcal{B}$选择$\boldsymbol{y}\leftarrow\mathbb{Z}_q^{1+n}$和$\boldsymbol{r}\leftarrow\{0,1\}^M$,再传递$(\boldsymbol{b}'_t,\boldsymbol{B}'_t,\boldsymbol{y})$和$(\boldsymbol{b}'_t,\boldsymbol{B}'_t,(\boldsymbol{r}^T\boldsymbol{b}'_t\,|\,\boldsymbol{B}'_t\boldsymbol{r}))$给$\mathcal{A}_{\mathrm{I}}$.若$\mathcal{A}_{\mathrm{I}}$能够以$1-negl(n)$概率区分它们,则称公钥$(\boldsymbol{b}'_t,\boldsymbol{B}'_t)$为有效的公钥.

(4) $\mathcal{B}$把$\mathcal{A}_{\mathrm{I}}$所给的(m_0,m_1)作为自己的挑战消息传递给$\mathcal{F}$,并从$\mathcal{F}$处获得挑战密文$(v',\boldsymbol{v}_2)$.于是,$\mathcal{B}$为$\mathcal{A}_{\mathrm{I}}$设置的挑战密文为$(v^*,\boldsymbol{v}_1^*,\boldsymbol{v}_2^*)=(v'+\boldsymbol{r}^T\boldsymbol{b}^*,\boldsymbol{B}^*\boldsymbol{r},\boldsymbol{v}_2)$,其中,$\boldsymbol{r}\leftarrow\{0,1\}^M$.

猜测:最后,$\mathcal{A}_{\mathrm{I}}$输出其猜测的结果 b 给$\mathcal{B}$.$\mathcal{B}$把该 b 传送给$\mathcal{F}$作为回应.

区分优势分析:在挑战密文生成过程中,$\mathcal{A}_{\mathrm{I}}$按公/私钥生成算法可非常容易获得有效公钥;反之,若提供无效公钥,则$\mathcal{A}_{\mathrm{I}}$会以$1-negl(n)$概率失败.因为$\mathcal{A}_{\mathrm{I}}$所有的努力都是为了在游戏中获胜,所以可以合理地假定$\mathcal{A}_{\mathrm{I}}$以概率1提供有效的公钥.

$\mathcal{B}$攻击 GPV-I 的区分优势$\varepsilon_{\mathcal{B}}$等于如下 3 个事件同时发生的概率:

- S_1:在部分私钥询问时,协议未终止.
- S_2:满足$ID^*=ID_t$.
- S_3:$\mathcal{A}_{\mathrm{I}}$成功区分挑战密文.

在协议没有终止的条件下,$\mathcal{A}_{\mathrm{I}}$在 Game 2 条件下的区分优势为$2|P[Game_2=1]-1/2|\geqslant\varepsilon-negl(n)$,即

$$P(S_3|S_2\cap S_1)\geqslant\varepsilon-negl(n).$$

又因为$P(S_1)\geqslant(1-1/q_1)^{q_2}$,$P(S_2\,|\,S_1)\geqslant 1/q_1$,所以有:

$$\varepsilon_{\mathcal{B}}=P(S_1\cap S_2\cap S_3)=P(S_1)P(S_2\,|\,S_1)P(S_3\,|\,S_2\cap S_1)\geqslant(1-1/q_1)^{q_2}\cdot 1/q_1\cdot\varepsilon-negl(n).$$

这样,若$\mathcal{A}_{\mathrm{I}}$能够在时间 T 内以不可忽略的区分优势ε攻破 CLPKE,则$\mathcal{B}$可以在不超过$T+q_1t_1+q_2t_2+q_3t_3+q_4t_4$时间间隔内以区分优势$\varepsilon_{\mathcal{B}}\geqslant(1-1/q_1)^{q_2}\cdot 1/q_1\cdot\varepsilon-negl(n)$攻破 GPV-I. □

定理 3. 在随机预言模型下,设$\mathcal{A}_{\mathrm{II}}$是自适应选择消息和身份攻击下第 2 类攻击者,若在时间 T 内至多进行q_1次生成用户询问、q_2次公钥替换询问和q_3次秘密值询问后,以不可忽略的区分优势ε攻破 CLPKE,则存在一个概率多项式算法$\mathcal{B}$,以区分优势$\varepsilon_{\mathcal{B}}\geqslant(1-1/q_1)^{q_2+q_3}\cdot 1/q_1\cdot\varepsilon-negl(n)$,在不超过 $T+q_1t_1+q_2t_2+q_3t_3$ 时间间隔内攻破 BGV-II 的 CPA 安全性,其中,$t_1(t_2,t_3)$表示一次生成用户(公钥替换、秘密值)询问所需的时间.

证明:假定概率多项式算法$\mathcal{F}$是 BGV-II 的挑战者;而算法$\mathcal{B}$在攻击 BGV-II 的游戏中充当 CPA 攻击者,又是攻击 CLPKE 游戏中的挑战者.下面说明如何根据算法$\mathcal{A}_{\mathrm{II}}$和$\mathcal{F}$去构造出算法$\mathcal{B}$.

系统参数的设置:$\mathcal{F}$设置并传给算法$\mathcal{B}$关于 BGV-II 的公开参数$(n,M=O(n\log q),\alpha,q,\chi_B)$和公钥$(\boldsymbol{b}^*,\boldsymbol{B}^*)\in\mathbb{Z}_q^M\times\mathbb{Z}_q^{n\times M}$.$\mathcal{B}$根据上述公开参数运行 $Setup(1^n)$算法来设置 CLPKE 的系统公/私钥$(\boldsymbol{A},\boldsymbol{R})$,系统参数$params=\{n,k,N,M,q,\alpha,s_2,\chi_B,\mathbb{Z}_2,H,\boldsymbol{A}\}$,使两个加密方案的公共参数取值一致.$\mathcal{B}$把系统参数 $params$ 和系统私钥 $\boldsymbol{R}$送给$\mathcal{A}_{\mathrm{II}}$.

询问应答:因为哈希函数 H 不再视为随机预言器,$\mathcal{B}$和$\mathcal{A}_{\mathrm{II}}$均可以独立自由地访问它,所以$\mathcal{A}_{\mathrm{II}}$可独立计算任何用户的部分私钥,无需部分私钥询问.$\mathcal{A}_{\mathrm{II}}$可以自适应地做生成用户、公钥替换、秘密值等询问.为简单起见,假设$\mathcal{A}_{\mathrm{II}}$的询问都是不同的.$\mathcal{B}$维护格式为$(ID,\boldsymbol{x},\boldsymbol{b},\boldsymbol{B},\boldsymbol{e})$且初始为空的$\mathcal{H}$列表.

- 生成用户询问($Create(\cdot)$):$\mathcal{B}$随机选择$t\in[q_1]$.当$\mathcal{A}_{\mathrm{II}}$询问 $Create(ID_i)$时,$\mathcal{B}$执行:

© 中国科学院软件研究所 http://www.jos.org.cn

(1) 若 $i=t$,则设置 $\boldsymbol{b}_t=\boldsymbol{b}^*,\boldsymbol{B}_t=\boldsymbol{B}^*,\boldsymbol{x}_t=\perp,\boldsymbol{e}_t=\perp$;否则,选择 $\boldsymbol{B}_i \leftarrow \mathbb{Z}_q^{n\times M},\boldsymbol{x}_i \leftarrow \chi_B^n,\boldsymbol{e}_i \leftarrow \chi_B^M$,计算:

$$\boldsymbol{b}_i = \boldsymbol{B}_i^T\boldsymbol{x}_i + 2\boldsymbol{e}_i \bmod q.$$

(2) 把元组$(ID_i,\boldsymbol{x}_i,\boldsymbol{b}_i,\boldsymbol{B}_i,\boldsymbol{e}_i)$添加到$\mathcal{H}$列表中,并把$(ID_i,\boldsymbol{b}_i,\boldsymbol{B}_i)$给$\mathcal{A}_{\mathrm{II}}$.

不失一般性地假设$\mathcal{A}_{\mathrm{II}}$下面询问所涉及的身份 ID_i 均已生成:

- 公钥替换询问($Replace(\cdot,\cdot)$):当$\mathcal{A}_{\mathrm{II}}$做 $Replace(ID_i,(\boldsymbol{b}_i',\boldsymbol{B}_i'))$ 询问时,$\mathcal{B}$执行:当 $i=t$ 时,终止协议;否则,据 ID_i 检查$\mathcal{H}$列表,把元组$(ID_i,\boldsymbol{x}_i,\boldsymbol{b}_i,\boldsymbol{B}_i,\boldsymbol{e}_i)$替换为 $(ID_i,\perp,\boldsymbol{b}_i',\boldsymbol{B}_i',\perp)$.
- 秘密值询问($Value(\cdot)$):收到$\mathcal{A}_{\mathrm{II}}$询问 $Value(ID_i)$后,$\mathcal{B}$执行:
  - 当 $i=t$ 时,终止协议.
  - 否则,在$\mathcal{H}$列表中按身份 ID_i 查找元组$(ID_i,\boldsymbol{x}_i,\boldsymbol{b}_i,\boldsymbol{B}_i,\boldsymbol{e}_i)$并执行:若 $\boldsymbol{x}_i\neq\perp$,则返回 $\boldsymbol{x}_i$ 给$\mathcal{A}_{\mathrm{II}}$;否则,输出$\perp$.

挑战:一旦$\mathcal{A}_{\mathrm{II}}$决定结束询问,他输出两个不同的挑战明文 $m_0,m_1\in\{0,1\}$和一个挑战身份 ID^*给$\mathcal{B}$.$\mathcal{B}$做出如下回应:

(1) 若 $ID^*\neq ID_t$,则$\mathcal{B}$终止协议;否则,$\mathcal{B}$根据 ID^*检查$\mathcal{H}$列表获取元组$(ID^*,\perp,\boldsymbol{b}^*,\boldsymbol{B}^*,\perp)$并计算出 $\boldsymbol{u}_t=H(ID_t)$和 $\boldsymbol{d}_t\leftarrow ExtractPPK(ID_t,params)$.

(2) $\mathcal{B}$把获取的(m_0,m_1)作为挑战消息传递给$\mathcal{F}$,并从$\mathcal{F}$处获得挑战密文$(v',\boldsymbol{v}_1)$.于是,$\mathcal{B}$为$\mathcal{A}_{\mathrm{II}}$ 设置的挑战密文为 $(v^*,\boldsymbol{v}_1^*,\boldsymbol{v}_2^*)=(v'+\boldsymbol{s}^T\boldsymbol{u}_t,\boldsymbol{v}_1,\boldsymbol{A}^T\boldsymbol{s}+2\boldsymbol{e})$,其中,$\boldsymbol{s}\leftarrow\chi_B^n,\boldsymbol{e}\leftarrow\chi_B^N$.

猜测:最后,$\mathcal{A}_{\mathrm{II}}$输出其猜测的结果 b 给$\mathcal{B}$.$\mathcal{B}$把 b 传送给$\mathcal{F}$作为回应.

区分优势分析:类似于定理 2 中分析,不再赘述. □

4.3 参数设置

设正整数 n 为安全参数,其余的量如 N,M,q,α,s_2 等都是 n 的函数.据系统参数生成算法,我们有:

$$\bar{\boldsymbol{A}}\leftarrow\mathbb{Z}_q^{n\times nk},\boldsymbol{R}\leftarrow D_{\mathbb{Z},s_1}^{nk\times nk},\boldsymbol{A}=(\bar{\boldsymbol{A}}\,|\,\boldsymbol{G}-\bar{\boldsymbol{A}}\boldsymbol{R})\in\mathbb{Z}_q^{n\times N},s_1=4\omega\left(\sqrt{\log n}\right)>4\eta_\varepsilon(\mathbb{Z}) \tag{3}$$

事实上,公式(3)中 $\bar{\boldsymbol{A}}$ 的列数=nk 满足陷门安全要求.根据文献[6],当 $q=p^e$ 且 p 为素数时,矩阵 $\bar{\boldsymbol{A}}$ 的列数 $\geqslant\left(n\log q+\log\left(2+\frac{2}{\varepsilon}\right)\right)\Big/\log(s_1/\eta_\varepsilon)$ 来保证 $(\bar{\boldsymbol{A}},\bar{\boldsymbol{A}}\boldsymbol{R})$ 分布与均匀分布统计不可区分.若取 $s_1=4\eta_\varepsilon(\mathbb{Z})$,则有 $\bar{\boldsymbol{A}}$ 的列数 $=\frac{1}{2}[n\log q+\omega(\log n)]$. 保守地取 $\bar{\boldsymbol{A}}$ 的列数 $=\frac{1}{2}[n\log q+n]$, 随着 s_1 的增大,满足不可区分性条件的 $\bar{\boldsymbol{A}}$ 的列数下限不增甚至减小,因此,当 $s_1=4\omega\left(\sqrt{\log n}\right)>4\eta_\varepsilon(\mathbb{Z})$ 时,取 $\bar{\boldsymbol{A}}$ 的列数 $=n\lceil\log q\rceil\geqslant\frac{1}{2}[n\log q+n\log q]>\frac{1}{2}[n\log q+n]$ 足以满足条件.这样,我们有:

$$N=2n\lceil\log q\rceil \tag{4}$$

再从方案的安全性方面考虑:

(1) $DLWE_{n,N,q,\chi}$问题的困难性假设

因为用户公钥生成和加密等操作都要满足 DLWE 问题的困难性假设,所以根据引理 1 有:

$$\begin{cases} q=poly(n)=n^{O(1)} \\ q\alpha>2\sqrt{n} \end{cases} \tag{5}$$

(2) Leftover Hash lemma 导出的统计不可区分性

加密和公钥有效性测试都需要满足$(\boldsymbol{b},\boldsymbol{B},\boldsymbol{b}^T\boldsymbol{r},\boldsymbol{B}\boldsymbol{r})$分布与 $\mathbb{Z}_q^N\times\mathbb{Z}_q^{n\times M}\times\mathbb{Z}_q\times\mathbb{Z}_q^n$ 上的均匀分布统计不可区分.为此,构造双通的哈希函数族:

$$\mathcal{H}=\left\{h_{\boldsymbol{B}'}:\{0,1\}^M\to\mathbb{Z}_q^{n+1};\boldsymbol{r}\mapsto h_{\boldsymbol{B}'}(\boldsymbol{r})=\boldsymbol{B}'\boldsymbol{r}=\begin{pmatrix}\boldsymbol{b}^T\\ \boldsymbol{B}\end{pmatrix}\boldsymbol{r} \bmod q\right\}.$$

根据引理 3,$(h_{\boldsymbol{B}'},h_{\boldsymbol{B}'}(\boldsymbol{r}))$的分布与 $\mathcal{H}\times\mathbb{Z}_q^{n+1}$ 上的均匀分布的距离至多为

© 中国科学院软件研究所 http://www.jos.org.cn

$$\Delta=\frac{1}{2}\sqrt{|Y|/|X|}=\frac{1}{2}\sqrt{q^{(n+1)}/2^{M}}.$$

欲使$\Delta\leqslant 1/2^{n}=negl(n)$成立,则充分条件是:

$$M=(n+1)\lceil\log q\rceil+2n \tag{6}$$

最后,从方案的正确性考虑:

$$|error|=|e+\boldsymbol{e}_1^T\boldsymbol{r}-\boldsymbol{d}^T\boldsymbol{e}_2|\leqslant|e|+|\boldsymbol{e}_1^T\boldsymbol{r}|+|\boldsymbol{d}^T\boldsymbol{e}_2| \tag{7}$$

因为 $e\leftarrow\chi_B$,根据引理 2:

$$|e|\leqslant B=q\alpha\cdot\omega\left(\sqrt{\log n}\right) \tag{8}$$

由 $\boldsymbol{r}\leftarrow\{0,1\}^{M}$, $\boldsymbol{e}_1\leftarrow\chi_B^{M}$, $M=(n+1)\lceil\log q\rceil+2n$ 和文献[15]中命题 2.3 可知:

$$|\boldsymbol{e}_1^T\boldsymbol{r}|\leqslant\sqrt{M}q\alpha\cdot\omega\left(\sqrt{\log n}\right)=q\alpha\cdot O\left(\sqrt{n\log q}\right)\cdot\omega\left(\sqrt{\log n}\right) \tag{9}$$

由 $\boldsymbol{d}\leftarrow SampleD(\boldsymbol{R},\overline{\boldsymbol{A}},\boldsymbol{u},s_2),s_2=\sqrt{7(\mathcal{S}_1(\boldsymbol{R})^2+1)},\mathcal{S}_1(\boldsymbol{R})\leqslant O\left(\sqrt{n\log q}\right)\cdot\omega\left(\sqrt{\log n}\right)$ 可知:

$$s_2=O\left(\sqrt{n\log q}\right)\cdot\omega\left(\sqrt{\log n}\right) \tag{10}$$

根据引理 4,等价地有 $\boldsymbol{d}\leftarrow D_{\Lambda_{\boldsymbol{u}}^{\perp}(\boldsymbol{A}),s_2\cdot\omega\left(\sqrt{\log n}\right)}$. 又 $\boldsymbol{e}_2\leftarrow\chi_B^{N}$, 根据事实 1[29]、引理 2 和公式(5):

$$\begin{aligned}|\boldsymbol{e}_2^T\boldsymbol{d}|&\leqslant\|\boldsymbol{d}\|q\alpha\cdot\omega\left(\sqrt{\log n}\right)\\&\leqslant\sqrt{N}s_2\cdot\omega\left(\sqrt{\log n}\right)\cdot q\alpha\cdot\omega\left(\sqrt{\log n}\right)\\&=\sqrt{2n\lceil\log q\rceil}\cdot s_2q\alpha\cdot\omega\left(\sqrt{\log n}\right)^2\\&=q\alpha O(n\log q)\cdot\omega\left(\sqrt{\log n}\right)^3\\&=q\alpha O(n\cdot\log n)\cdot\omega\left(\sqrt{\log n}\right)^3\end{aligned} \tag{11}$$

由公式(7)~公式(9)和公式(11)可知:

$$\begin{aligned}|error|&\leqslant|e|+|\boldsymbol{e}_1^T\boldsymbol{r}|+|\boldsymbol{d}^T\boldsymbol{e}_2|\\&\leqslant q\alpha\left(\omega\left(\sqrt{\log n}\right)+O\left(\sqrt{n\log q}\right)\cdot\omega\left(\sqrt{\log n}\right)+O(n\log n)\cdot\omega\left(\sqrt{\log n}\right)^3\right)\\&=q\alpha O(n\log n)\cdot\omega\left(\sqrt{\log n}\right)^3.\end{aligned}$$

取 $\alpha=1\Big/\left(O(n\log n)\cdot\omega\left(\sqrt{\log n}\right)^3\right)$, 可满足 $2|error|<q/2$.又因为 $\sqrt{n}\geqslant\log n\geqslant 4$ 和 $q\alpha>2\sqrt{n}$, 所以可取素数:

$$q=O(n^2)\omega\left(\sqrt{\log n}\right)^3 \tag{12}$$

由公式(4)、公式(6)、公式(10)和公式(12),我们有如下定理:

定理 4(存在性). 设安全参数 $n\geqslant 16$,若取:

$q=O(n^2)\omega\left(\sqrt{\log n}\right)^3$, $M=(n+1)\lceil\log q\rceil+2n$,$N=2n\lceil\log q\rceil$, $\alpha=1\Big/\left(O(n\log n)\cdot\omega\left(\sqrt{\log n}\right)^3\right)$,$s_2=O\left(\sqrt{n\log q}\right)\omega\left(\sqrt{\log n}\right)$,

则存在一个语义安全的无证书加密方案.

4.4 效 率

下面把本文的 CLPKE 与目前现存的格上无证书加密方案[25,26]作效率比较.为此,设 n 为安全参数,q 为模数,m 为系统所生成格的维数,$k=\lceil\log q\rceil$,尺寸以数据的比特长度来计.为方便比较,典型地取 $\omega\left(\sqrt{\log n}\right)=\log n$, 如文献[2,30].考虑到文献[25]可能为多比特加密方案,故比较密文尺寸和加(解)密计算量时,我们采用每比特真正消息的平均密文尺寸和加(解)密平均计算量,如平均密文尺寸等于 ℓ 比特消息被加密为密文的总长度除以消息的比特个数 ℓ.类似地定义加(解)密平均计算量.这样,我们选择了 13 项指标.

首先,文献[25]中方案的参数 $m,q,\tilde{O}(n/\alpha)$ 的取值同文献[26],分别大于我们方案对应的参数取值(见表 1).引入参数 ℓ 和 d,其中,ℓ 表示真正被加密的消息长度 $x\in\{0,1\}^{\ell}$,d 表示多比特版本的 HIBE 和 IBE 加密方案每次可处

© 中国科学院软件研究所 http://www.jos.org.cn

理的最大比特串长度.当使用 d 比特版本的 HIBE 和 IBE 方案加密 $\{0,1\}^{\ell+\bar{m}}$ 时,不妨假定这 $\ell+\bar{m}$ 个比特恰好分成 t 组,每组含 d 个比特,即 $dt=\ell+\bar{m}$.系统私钥 $\boldsymbol{T}_0\in\mathbb{Z}^{m\times m}$ 满足 $\|\boldsymbol{T}_0\|\leqslant\sigma_0\sqrt{m}\leqslant O(n\log q)$ 且 $m=O(n\log q)$,故取 $\sigma_0=\sqrt{n\log q}$ 为矩阵 $\boldsymbol{T}_0$ 中元素绝对值的上界.用户的部分私钥 $\boldsymbol{T}_{id}\in\mathbb{Z}^{2m\times 2m}$ 矩阵是利用 $\boldsymbol{T}_0\in\mathbb{Z}^{m\times m}$ 为陷门基抽样后再随机化所得,所以 $\boldsymbol{T}_{id}$ 中元素绝对值的上界不小于 $\boldsymbol{T}_0$ 中元素绝对值的上界,所以用户私钥的尺寸至少为 $180n^2k^2\log\sqrt{n\log q}$. 生成用户部分私钥需要 $O((2m)^2)$次格上离散高斯抽样,每次抽样的复杂度[2]为 $O((2m)^2)$,所以生成用户部分私钥需要计算量为 $O((2m^2))\cdot O((2m^2))=O(n^4k^4)$.

Table 1 Efficiency comparison

表 1 效率对比

方案	Ref.[25]	Ref.[26]	本文
维数m	$6nk$	$6nk$	$2nk$
模数q	$O(n^4k^{3.5})\omega(\log n)^3$	$O(n^4k^{3.5})\omega(\log n)^3$	$O(n^2)\omega\left(\sqrt{\log n}\right)^3$
近似因子 $\tilde{O}(n/\alpha)$	$\tilde{O}(n^{4.5})$	$\tilde{O}(n^{4.5})$	$\tilde{O}(n^2)$
系统公钥尺寸	$24n^2k\log q+dn\log q$	$6n^2k\log q$	$2n^2k\log q$
系统私钥尺寸	$36n^2k^2\log\left(\sqrt{n\log q}\right)$	$36n^2k^2\log\left(\sqrt{n\log q}\right)$	$n^2k^2\log\left(4\sqrt{n}\right)$
用户公钥尺寸	$28nk\log q+dn\log q$	$(6n^2k+n)\log q$	$(n^2k+2nk+k+2n^2+2n)\log q$
用户私钥尺寸	$\geqslant 180n^2k^2\log\sqrt{n\log q}$	$\geqslant 15nk\log(6nk)$	$\leqslant(1.5n+5.5nk)\log n$
平均密文尺寸	$\left(2+\frac{30nk(\ell+10nk)}{\ell d}+\frac{20nk+n}{\ell}\right)\log q$	$(12nk+1)\log q$	$(2nk+n+1)\log q$
生成用户公钥计算量	不需要计算	$O(n^2\log^2 q\log n)$	$O(n^2\log^2 q\log n)$
生成用户部分私钥计算量	$O(n^4k^4)$	$O(n^2k^2)$	$O(n\log n)$
生成用户私钥计算量	不需要计算	$O(n^2\log^2 q\log^2 n)$	不需要计算
加密平均计算量	$\frac{1}{\ell}[O(n^3k\log^2 q)+O(tn^2k\log q\log n)+O(tdn\log q\log n)]$	$O(n^2\log^3 q)$	$O(n^2\log^2 q\log n)$
解密平均计算量	$\frac{1}{\ell}[O(n^3k\log^2 q)+O(dn^2k^2)+O(tdnk\log q\log n))]$	$O(n\log^2 q\log n)$	$O(n\log^2 q\log n)$

在文献[26]中,用户私钥$(\boldsymbol{t},\boldsymbol{e})\in\mathbb{Z}^m\times\mathbb{Z}^m$ 且 $\boldsymbol{t}\leftarrow D_{\mathbb{Z}^m,\sigma_1}$,$\boldsymbol{e}\leftarrow D_{\mathbb{Z}^m,\sigma_2}$,其中,

$$\sigma_1=m\omega(\log m),\sigma_2=\|\boldsymbol{t}\|\sigma_s,\sigma_s=\sqrt{m}O\left(\sqrt{n\log q}\right)\omega(\log m).$$

这样,$\sigma_1>m,\sigma_2=\|\boldsymbol{t}\|\sigma_s>\sqrt{m}\sigma_s=mO\left(\sqrt{n\log q}\right)\omega(\log m)>\sqrt{m^3}$.

所以,用户私钥尺寸至少为 $2.5m\log m=15nk\log(6nk)$.生成用户的部分私钥需要做一次 m 维格上的离散高斯抽样,所以生成用户部分私钥需要计算量为 $O(m^2)=O(n^2k^2)$.

在本文中,系统私钥 $\boldsymbol{R}\leftarrow D_{\mathbb{Z},s_1}^{nk\times nk}$,$s_1=4\omega\left(\sqrt{\log n}\right)\leqslant 4\sqrt{n}$,系统私钥尺寸不大于 $n^2k^2\log\left(4\sqrt{n}\right)$.用户私钥$(\boldsymbol{x},\boldsymbol{d})\in\mathbb{Z}^n\times\mathbb{Z}^N$ 且 $\boldsymbol{x}\leftarrow D_{\mathbb{Z}^m,q\alpha}$,$\boldsymbol{d}\leftarrow SampleD(\boldsymbol{R},\bar{\boldsymbol{A}},\boldsymbol{u},s_2)$. 根据参数设置,可以 $1-negl(n)$概率保证 $0<q<n^{2.5}\omega\left(\sqrt{\log n}\right)^2$,$0<\alpha<1\Big/\left(n\omega\left(\sqrt{\log n}\right)^3\right)$,则有 $2\sqrt{n}<q\alpha\cdot\omega\left(\sqrt{\log n}\right)<n^{1.5}$,即$\|\boldsymbol{x}\|_\infty<n^{1.5}$.

又根据引理 2 和引理 4,$\|\boldsymbol{d}\|_\infty\leqslant s_2\cdot\omega\left(\sqrt{\log n}\right)^2=O\left(\sqrt{n\log q}\right)\omega\left(\sqrt{\log n}\right)^3<n^{2.75}$.这样,用户私钥的尺寸至多为 $n\log n^{1.5}+N\log n^{2.75}=(1.5n+5.5nk)\log n$.因为采用文献[6]中陷门生成算法,所以本文生成用户部分私钥需要计算量为 $O(n\log n)$.

表 1 给出了 3 个方案在相同安全参数 n 下的比较结果.结果显示:

(1) 与文献[25]中单比特版本方案相比(即 $d=1$),除了生成用户公/私钥计算量这两项指标(其中,在生成用户私钥计算量上二者持平)以外,本文方案在表 1 中所列的其他各项指标上均有明显优势.

(2) 与文献[25]中多比特版本方案相比(即 $d>1$ 且 $d|(\ell+10nk)$),在生成用户公钥计算量上我们的方案处于劣

© 中国科学院软件研究所 http://www.jos.org.cn

势.在平均密文尺寸上,当 $1<d\leqslant 15$ 且ℓ为满足 $d|(\ell+10nk)$条件的任意正整数,或者当 $15<d\leqslant \ell+10nk$ 且ℓ为满足 $d|(\ell+10nk)$和 $1\leqslant \ell<25$ 的正整数时,我们的方案占优势;但是当 $k\leqslant d\leqslant \ell+10nk$ 且ℓ为满足 $d|(\ell+10nk)$和$\ell\geqslant 30nk$ 的正整数时,文献[25]中的方案占优势(这里给出各个方案占优的充分条件,下同).在加密平均计算量方面,当$\ell\leqslant O(n)$且 d 为满足 $d|\ell+10nk,d>1$ 的任意正整数,或者当$\ell>O(n)$且 d 为满足 $d|\ell+10nk,1<d\leqslant 1+10nk/\ell$的任意正整数时,都是我们的方案占优;当$\ell>O(n)$且 d 为满足 $d|\ell+10nk,d\geqslant O(nk)$的任意正整数时,文献[25]中的方案占优势.另外,在生成用户私钥计算量上二者持平.因此,除了上述 4 个指标以外,本文方案在所列的其余 9 项指标上均有显著的优势(与参数ℓ和 d 的取值无关).

(3) 与文献[26]相比,本文方案在表 1 中所列的各项指标上均有明显优势.

5 结 论

本文在格上借助于文献[6]中陷门生成方法提出一个单比特的无证书加密方案.该方案在随机预言模型下被证明是语义安全的.与文献[25,26]中的方案相比,我们的方案具有更短的公/私钥和更低的解密平均计算量,尤其是比文献[26]有更短的密文及更简单、自然的用户公/私钥生成算法.这种简单的算法也有力地促成了把单比特变为多比特的无证书加密方案,而且在单比特方案安全情况下选择的参数,如 m,q,N,M,α,s_2,可以不变地直接应用到后者,并使后者具有与前者同样的安全性.另外,我们的方案可根据实际情况对明文空间做 $\mathbb{Z}_2\to\mathbb{Z}_2^t\to\mathbb{Z}_p^t$ 的扩展,还可以方便地把它移植到多项式环上,以获得更小的参数和更好的效率.

致谢 我们向给予支持和提出宝贵建议的评审专家深表感谢.

References:

[1] Regev O. On lattices, learning with errors, random linear codes, and cryptography. In: Proc. of the STOC. New York, ACM, 2005. 84−93. [doi: 10.1145/1060590.1060603]

[2] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. In: Proc. of the STOC. New York, ACM, 2008. 197−206. [doi: 10.1145/1374376.1374407]

[3] Gentry C. Fully homomorphic encryption using ideal lattices. In: Mitzenmacher M, ed. Proc. of the STOC. New York, ACM, 2009. 169−178. [doi: 10.1145/1536414.1536440]

[4] Agrawal S, Boneh D, Boyen X. Efficient lattice (H)IBE in the standard model. In: Gilbert H, ed. Proc. of the EUROCRYPT 2010. LNCS 6110, Berlin, Heidelberg: Springer-Verlag, 2010. 553−572. [doi: 10.1007/978-3-642-13190-5_28]

[5] Brakerski Z, Vaikuntanathan V. Fully homomorphic encryption from ring-LWE and security for key dependent messages. In: Rogaway P, ed. Proc. of the CRYPTO 2011. LNCS 6841, Berlin, Heidelberg: Springer-Verlag, 2011. 505−524. [doi: 10.1007/978-3-642-22792-9_29]

[6] Micciancio D, Peikert C. Trapdoor for lattices: Simpler, tighter, faster, smaller. In: Pointcheval D, Johansson T, eds. Proc. of the EUROCRYPT 2012. LNCS 6223, Berlin, Heidelberg: Springer-Verlag, 2012. 191−208. [doi: 10.1007/978-3-642-29011-4_41]

[7] Micciancio M, Peikert C. Hardness of SIS and LWE with small parameters. In: Canetti R, Garay JA, eds. Proc. of the CRYPTO 2013. Part I. LNCS 8042, Berlin, Heidelberg: Springer-Verlag, 2013. 21−39. [doi: 10.1007/978-3-642-40041-4_2]

[8] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings. Journal of the ACM, 2013,60(6): 1−35. [doi: 10.1145/2535925]

[9] Boneh D, Gentry C, Gorbunov S, Halevi S, Nikolaenko V, Segev G, Vaikuntanathan V, Vinavagamurthy D. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits. In: Nguyen PQ, Oswald EE, eds. Proc. of EUROCRYPT 2014. LNCS 8441, Berlin, Heidelberg: Springer-Verlag, 2014. 533−556. [doi: 10.1007/978-3-642-55220-5_30]

[10] Ducas L, Lyubashevsky V, Prest T. Efficient identity-based encryption over NTRU lattices. In: Sarkar P, Iwata T, eds. Proc. of ASIACRYPT 2014. Part II. LNCS 8874, Berlin, Heidelberg: Springer-Verlag, 2014. 22−41. [doi: 10.1007/978-3-662-45608-8_2]

[11] Nguyen PQ, Zhang J, Zhang ZF. Simpler efficient group signatures from lattices. In: Kate J, ed. Proc. of the PKC 2015. LNCS 9020, Berlin, Heidelberg: Springer-Verlag, 2015. 401−426. [doi: 10.1007/978-3-662-46447-2_18]

[12] Brakerski Z, Gentry C, Vaikuntanathan V. Fully homomorphic encryption without Bootstrapping. In: Goldwasser S, ed. Proc. of the Innovations in Theoretical Computer Science. 2012. 309−325. [doi: 10.1145/2090236.2090262]

[13] Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: Conceptually-Simpler, asymptotically-faster, attribute-based. In: Canetti R, Garay JA, eds. Proc. of the CRYPTO 2013. Part I. LNCS 8042, Berlin, Heidelberg: Springer-Verlag, 2013. 75−92. [doi: 10.1007/978-3- 642-40041-4_5]

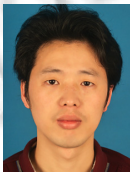
© 中国科学院软件研究所 http://www.jos.org.cn

[14] Alperin-Sheriff J, Peikert C. Faster bootstrapping with polynomial error. In: Garay JA, Gennaro R, eds. Proc. of the CRYPTO 2014. LNCS 8616, Berlin, Heidelberg: Springer-Verlag, 2014. 297−314. [doi: 10.1007/978-3-662-44371-2_17]
[15] Brakerski Z, Vaikuntanathan V. Lattice-Based FHE as secure as PKE. In: Proc. of the ITCS. 2014. 1−12. http://eprint.iacr.org/2013/541
[16] Gorbunov S, Vaikuntanathan V, Wichs D. Leveled fully homomorphic signatures from standard lattices. In: Proc. of the STOC. New York, ACM, 2015. 469−477. http://eprint.iacr.org/2014/897 [doi: 10.1145/2746539.2746576]
[17] Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: Laih CS, ed. Proc. of the ASIACRYPT 2003. LNCS 2894, Berlin, Heidelberg: Springer-Verlag, 2003. 452−473. [doi: 10.1007/978-3-540-40061-5_29]
[18] Dent A. A survey of certificateless encryption schemes and security models. Int'l Journal of Information Security, 2008,7(5): 347−377. [doi: 10.1007/s10207-008-0055-0]
[19] Zhou CX, Zhou W, Dong XW. Provable certificateless generalized signcryption scheme. Designs, Codes and Cryptography, 2014, 71(2):331−346. [doi: 10.1007/s10623-012-9734-y]
[20] Chen H, Zhang FT, Song RS. Certificateless proxy signature scheme with provable security. Ruan Jian Xue Bao/Journal of Software, 2009,20(3):692−701 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/574.htm [doi: 10.3724/SP.J.1001.2009.00574]
[21] Chen H, Zhu CJ, Song RS. Efficient certificateless signature and group signature schemes. Journal of Computer Research and Development, 2010,47(2):231−237 (in Chinese with English abstract).
[22] Zhang L, Wu QH, Domingo-Fener J, Qin B, Zeng P. Signatures in hierarchical certificateless cryptography: Efficient constructions and provable security. Information Sciences, 2014,272:223−237. [doi: 10.1016/j.ins.2014.02.085]
[23] Chin JJ, Behnia R, Heng SH, Phan RCW. Cryptanalysis of a certificateless identification scheme. Security and Communication Networks, 2015,8(2):122−125. [doi: 10.1002/sec.963]
[24] Zhang FT, Sun YX, Zhang L, Geng MM, Li SJ. Research on certificateless public key cryptography. Ruan Jian Xue Bao/Journal of Software, 2011,22(6):1316−1332 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4007.htm [doi: 10.3724/SP.J.1001.2011.04007]
[25] Sepahi R, Steinfeld R, Pieprzyk J. Lattice-Based certificateless public-key encryption in the standard model. Int'l Journal of Information Security, 2014,13(4):315−333. [doi: 10.1007/s10207-013-0215-8]
[26] Jiang MM, Hu YP, Lei H, Wang BC, Lai QQ. Lattice-Based certificateless encryption scheme. Frontiers of Computer Science, 2014,8(5):828−836. [doi: 10.1007/s11704-014-3187-6]
[27] Lindner R, Peikert C. Better key sizes (and attacks) for LWE-based encryption. In: Kiayias A, ed. Proc. of the CT-RSA 2011. LNCS 6558, Berlin, Heidelberg: Springer-Verlag, 2011. 319−339. [doi: 10.1007/978-3-642-19074-2_21]
[28] Alwen J, Peikert C. Generating shorter bases for hard random lattices. In: Proc. of the Symp. on Theoretical Aspects of Computer Science. 2009. 75−86. [doi: 10.1007/s00224-010-9278-3]
[29] Peikert C, Vaikuntanathan V, Waters B. A framework for efficient and composable oblivious transfer. In: Wagner D, ed. Proc. of the CRYPTO 2008. LNCS 5157, Berlin, Heidelberg: Springer-Verlag, 2008. 554−571. [doi: 10.1007/978-3-540-85174-5_31]
[30] Gentry C, Halevi S, Vaikuntanathan V. A simple BGN-type cryptosystem from LWE. In: Gilbert H, ed. Proc. of the EUROCRYPT 2010. LNCS 6110, Berlin, Heidelberg: Springer-Verlag, 2010. 506−522. [doi: 10.1007/978-3-642-13190-5_26]

附中文参考文献:

[20] 陈虎,张福泰,宋如顺.可证安全的无证书代理签名方案.软件学报,2009,20(3):692−701. http://www.jos.org.cn/1000-9825/574.htm [doi: 10.3724/SP.J.1001.2009.00574]
[21] 陈虎,朱昌杰,宋如顺.高效的无证书签名和群签名方案.计算机研究与发展,2010,47(2):231−237.
[24] 张福泰,孙银霞,张磊,耿曼曼,李素娟.无证书公钥密码体制研究.软件学报,2011,22(6):1316−1332. http://www.jos.org.cn/1000-9825/4007.htm [doi: 10.3724/SP.J.1001.2011.04007]

陈虎(1975－),男,江苏睢宁人,博士,副教授,主要研究领域为密码学.



连至助(1986－),男,博士生,主要研究领域为密码学.

胡予濮(1955－),男,博士,教授,博士生导师,主要研究领域为密码学.

贾惠文(1990－),男,博士生,主要研究领域为密码学.

© 中国科学院软件研究所 http://www.jos.org.cn