软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, 2023,34(2):802−817 [doi: 10.13328/j.cnki.jos.006694]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于 *k*-Lin 假设的同态加密方案*

赖俊祚[1], 黄正安[2], 翁 健[1], 吴永东[1]

[1](暨南大学 网络空间安全学院, 广东 广州 510632)

[2](鹏城实验室, 广东 深圳 518055)

通信作者: 黄正安, E-mail: huangzha@pcl.ac.cn

摘 要: 作为数字货币的底层核心技术之一, 区块链随着数字货币的快速发展而受到了广泛关注. 由于区块链具有去中心化、防篡改、可追溯等性质, 如今越来越多的企业和个人用户选择利用区块链技术来实现数据的传输和记录. 区块链公开透明的特性, 一方面充分保证了数据的可用性; 但另一方面, 又给用户的隐私信息带来了严重威胁. 为了同时兼顾用户数据的机密性和可用性, 同态加密常常被用到区块链的安全解决方案之中. 然而, 现实应用对于所部署的同态加密方案的安全强度要求也很可能会随着时间推移而有所变化. 考虑到区块链应用场景的复杂多样性和分布式特点, 同态加密方案一旦部署下去, 之后, 当随着时间推移需要调整安全性强度时, 相应的工作量将会非常繁重. 此外, 在区块链的现实应用中, 考虑到监管方面的需求, 很多情况下(尤其是针对某些群组成员发布和传输的数据)需要允许某可信第三方(如监管方)能够对链上的相应密文数据进行解密. 若采用传统的同态加密方案对数据进行加密, 可信第三方需要存储所有用户的私钥, 这将给密钥管理和存储带来巨大压力. 针对当前的区块链应用场景和安全需求, 提出了一个基于 $\mathbb{Z}_{N^2}^*$ ($N=pq$)上的判定性 *k*-Lin 假设的加法同态加密方案. 该方案不仅在标准模型下能够满足 IND-CCA1 安全性, 还具有 3 个特殊优势: (i) 可以通过对参数 *k* 的调控细粒度地调节加密方案的安全性强度; (ii) 加密方案具有双解密机制: 存在两种私钥, 一种由用户本人持有, 另一种由可信第三方持有, 其中, 可信第三方的私钥可用于该加密体制所有用户的密文解密; (iii) 加密方案可以极为便利地退化为 IND-CPA 安全的公钥加密方案, 退化后的方案不仅其公私钥长度和密文长度变得更短, 而且同样具有加法同态性和双解密机制.

关键词: 区块链; 同态加密; 安全性调控; 监管; 双解密机制

中图法分类号: TP309

中文引用格式: 赖俊祚, 黄正安, 翁健, 吴永东. 基于 *k*-Lin 假设的同态加密方案. 软件学报, 2023, 34(2): 802–817. http://www.jos.org.cn/1000-9825/6694.htm

英文引用格式: Lai JZ, Huang ZA, Weng J, Wu YD. *k*-Lin-based Homomorphic Encryption Schemes. Ruan Jian Xue Bao/Journal of Software, 2023, 34(2): 802−817 (in Chinese). http://www.jos.org.cn/1000-9825/6694.htm

k-Lin-based Homomorphic Encryption Schemes

LAI Jun-Zuo[1], HUANG Zheng-An[2], WENG Jian[1], WU Yong-Dong[1]

[1](College of Cyber Security, Ji'nan University, Guangzhou 510632, China)

[2](PengCheng Laboratory, Shenzhen 518055, China)

Abstract: Blockchain, as one of the underlying key technologies of digital currency, has received extensive attention with the rapid development of digital currency. Due to the decentralization, tamper resistance, traceability, and other properties of blockchain, more and more enterprise/individual users now choose to use blockchain technology to achieve data transmission and recording. On the one hand, the openness and transparency of the blockchain can fully guarantee the availability of data, but on the other hand, it brings high risks to users' privacy. In order to balance the confidentiality and availability of data, homomorphic encryption is usually employed in security

* 基金项目: 国家自然科学基金(61922036, U2001205); 广东省基础与应用基础研究重大项目(2019B030302008)
收稿时间: 2021-06-10; 修改时间: 2022-04-12; 采用时间: 2022-04-29; jos 在线出版时间: 2022-07-22

solutions of blockchain. However, in practice, the security strength of the deployed homomorphic encryption schemes is likely to change over time. Considering the complex diversity and distributed characteristics of blockchain application scenarios, once a homomorphic encryption scheme is deployed, the corresponding workload will be very heavy when its security strength needs to be adjusted over time. To make things worse, in practice of blockchain, when considering the regulation requirements in many cases (especially for the data published and transmitted by certain group members), a trusted third party (TTP) such as a regulator, which is able to decrypt all the corresponding ciphertexts on the chain, is needed. If a traditional homomorphic encryption scheme is deployed, the TTP needs to store all users' secret keys, which introduces lots of practical problems to key management and storage of the TTP. According to the current application scenarios and security requirements of blockchain, an additive homomorphic encryption scheme is proposed, whose security is based on the decisional *k*-Lin assumption over $\mathbb{Z}_{N^2}^*$ where $N=pq$. The proposed scheme can be proved IND-CCA1 secure in the standard model, and has the following three advantages: (i) fine-grained adjustment of the security strength of the proposed scheme can achieved via adjusting the parameter *k*; (ii) it is a double decryption scheme (i.e., it has two kinds of secret keys, where one of them is held by a certain user, and the other is kept by the TTP, so the TTP can use this key to decrypt all the ciphertexts encrypted by the users under their own public keys); (iii) it can easily degenerate into an IND-CPA secure homomorphic encryption scheme, such that the obtaining scheme, with shorter public-secret key pair and shorter ciphertexts, is also an additively homomorphic, double decryption scheme.

Key words: blockchain; homomorphic encryption; security adjustment; regulation; double decryption mechanism

1 引 言

1.1 背 景

自 2009 年以来, 数字货币与日俱增, 而区块链作为数字货币的底层核心技术之一[1], 也因此受到广泛关注. 区块链本质上是一个由 P2P 网络通信、密码学技术、共识机制等多种技术方法组合而成的分布式数据库, 具有去中心化、公开透明、不可篡改和可追溯等特性. 区块链的多重优良特性, 使其不仅能够应用于密码货币领域, 还在社会管理、医疗健康、产品溯源等方面有着广泛的应用. 随着区块链相关应用的大量涌现, 通过区块链实现存储和传输的数据量越来越庞大, 其中不乏涉及用户隐私的数据信息. 由于区块链公开透明的特性, 链上存储的用户数据面临着隐私泄露的风险, 这也给区块链的应用和发展带来了巨大挑战.

为了解决区块链上数据隐私泄露的问题, 一种很直接的解决方案就是对链上的数据进行加密. 但是传统的加密方案只能保证数据的机密性, 降低了数据的可用性. 1978 年, Rivest 等人[2]首次提出了同态加密的概念. 同态加密支持密文数据上的运算, 允许在不知道明文的情况下, 通过对密文直接进行操作来实现对明文数据的运算. 早期的同态加密方案[3−6]或者只支持对密文的加法运算, 或者只支持对密文的乘法运算, 或者只支持对密文的加法运算和一次乘法运算. 2009 年, Gentry[7]构造了第一个全同态加密方案, 实现了同时支持对密文进行任意加法和乘法运算的设想, 是密码学研究的一个重大突破. 自此以后, 全同态加密获得了蓬勃的发展, 国内外研究学者提出了一系列全同态加密方案[8−19]. 与全同态加密相比, 加法同态加密虽然在功能上具有一定的缺陷, 但在安全计算方面具有巨大的效率优势. 因此, 在当前的实际应用中, 加法同态加密具有广泛的应用价值: 结合区块链应用来考虑, 如果利用同态加密方案对数据进行加密, 再把密文传到链上, 就可以在保持链上数据机密性的同时, 也保证数据一定程度上的可用性.

考虑到区块链应用场景的复杂多样性, 现实应用对于所部署同态加密方案的安全强度要求也很可能会随着时间推移而有所变化. 如果最初部署的加密方案安全强度较低, 则随着时间的推移, 该方案可能不再足以保证数据的安全性; 如果所部署的加密方案安全强度较高, 则又会造成计算成本和时间成本的极大浪费. 而且, 考虑到区块链场景的分布式特点, 一旦同态加密方案部署下去, 之后, 如果为了调整安全性强度而对方案进行重新部署, 这将给系统和各用户带来繁重的工作量和极大的不便.

此外, 从目前区块链应用的需求角度来看, 监管是区块链相关业务必不可少的一个重要环节. 如果采用传统的加法同态加密算法对上链数据进行处理, 虽然可以同时兼顾数据的机密性和可用性, 但是由于只有持解密私钥的用户才能对密文进行解密, 这就给监管方增加了监管难度. 对于这种情况, 最直接的解决方案是: 每个用户都将各自的解密私钥发送给监管方, 以便于监管方对密文进行解密和审查. 但这样一来, 在密钥传输、管理和存储等方面的成本都会大幅度增加.

1.2 本文贡献

针对这一问题, 我们提出一个基于 $\mathbb{Z}_{N^2}^*$ ($N=pq$)上的判定性 k-Lin 假设的公钥加密方案. 我们的方案(即第 3 节的方案 PKE_{add})不仅具有加法同态性, 而且在 $\mathbb{Z}_{N^2}^*$ 上的判定性 k-Lin 假设下还能证明 IND-CCA1 安全性. 此外, 我们的方案 PKE_{add} 还具有以下 3 个重要优势.

(i) 可以通过对参数 k 的调控细粒度地调节 PKE_{add} 的 IND-CCA1 安全性强度. 简单而言, 针对 PKE_{add}, 我们设计了相应的转化算法. 该转化算法可以把现有的(关于 PKE_{add} 的)公共参数、公私钥对和密文转化为安全性强度更高(即 k 值更大)的加法同态加密方案(记为 PKE'_{add})的公共参数、公私钥对和密文, 从而实现对 PKE_{add} 的更新升级;

(ii) PKE_{add} 具有“双解密机制”[20]. 确切地说, 双解密机制是指存在两种不同的私钥: 一种是与特定用户公钥 pk 绑定的私钥 sk, 由用户(接收方)保存, 使得该用户可以对所有用 pk 加密而得的密文进行解密; 另一种是通用性更强的私钥(称为陷门), 可以对任意公钥加密而得的密文进行解密. 在区块链应用场景中, 如果采用具有双解密机制的同态加密方案, 则用户公私钥可以由用户保管(公钥可以公开, 私钥由用户自己安全存储, 不公开), 而通用性更强的陷门则由监管方持有. 这样一来, 不仅链上数据的可用性在一定程度上得到了保证, 而且监管方也可以通过固定的单一密钥来对其他用户的链上密文数据进行解密和监管. 由于双解密机制这个性质, PKE_{add} 在现实部署中能够有效减轻监管方的密钥管理成本和压力. 与当前具有双解密机制的同态加密方案[20,21]相比, PKE_{add} 依赖于更弱的计算困难性假设, 而且满足更强的安全性(即 IND-CCA1 安全性);

(iii) PKE_{add} 还可以极为便利地退化为 IND-CPA 安全的公钥加密方案, 以适应某些对传输数据长度和计算效率要求较高而安全性要求相对不那么高的应用场景. 退化后的加密方案不仅其公私钥长度和密文长度变得更短, 而且同样具有加法同态性和双解密机制.

2 预备知识

2.1 基本符号

本文中, 我们统一用 κ 表示安全参数. 对于一个概率算法 A, 我们用 $y\leftarrow A(x)$ 表示“以 x 为输入、调用算法 A、最后输出结果 y”这一过程; 如果 A 的运行时间是关于 κ 的多项式, 则称 A 为概率多项式时间(probabilistic polynomial time, PPT)算法.

我们用 $\mathbb{N}$ 表示自然数集. 对任意 $n\in\mathbb{N}$, 符号 $[n]$ 表示集合 $\{1,\ldots,n\}$. 对任意有限集 S, $s\leftarrow S$ 表示从 S 中均匀随机地选取出 s. 若 $\mathcal{D}$ 是定义在 S 上的概率分布, 则 $s\leftarrow\mathcal{D}$ 表示从 S 中按概率分布 $\mathcal{D}$ 选取元素 s. 对于一个集合 S(或群 G), 我们用 $|S|$(或 $|G|$)表示该集合 S(或该群 G)的元素个数. 对于一个字符串 m, 我们用 $|m|$ 表示该字符串的比特长度. 对任意群元素 $a\in G$, $ord(a)$ 表示 a 的阶.

对于一个素数 p, 如果 $p'=\dfrac{p-1}{2}$ 也是素数, 则称 p 为安全素数. 记 $\mathcal{SP}(\kappa)$ 为所有长度为 κ 比特的安全素数组成的集合.

2.2 计算困难性假设

我们回顾 $\mathbb{Z}_{N^2}^*$ 上的 DDH 假设[20], 具体如下: 令 $N=pq$, 其中, p 和 q 均为安全素数(即 $p'=\dfrac{p-1}{2}$ 和 $q'=\dfrac{q-1}{2}$ 都是素数). 我们用 $\phi(\cdot)$ 来表示 Euler’s totient function, 即 $\phi(N)=(p-1)(q-1)=4p'q'$, 用 $\lambda(N)$ 来表示 Carmichael’s function, 即 $\lambda(N)=lcm(p-1,q-1)$. 对任意 $y\in\mathbb{Z}_{N^2}^*$, 若存在 $x\in\mathbb{Z}_{N^2}^*$ 使得 $y=x^2 \bmod N^2$, 则称 y 是模 N^2 的二次剩余(quadratic residue). 记 $\mathcal{QR}_{N^2}$ 为所有模 N^2 的二次剩余组成的循环群, 则有 $|\mathrm{QR}_{N^2}|=\dfrac{N\phi(N)}{4}=pp'qq'$, 而且 $\mathcal{QR}_{N^2}$ 中每个阶为 N 的元素均为 $1+kN(k\in\mathbb{N})$ 的形式[4,20].

定义 1($\mathbb{Z}_{N^2}^*$ **上的 DDH 假设)**[20]. $\mathbb{Z}_{N^2}^*$ 上的 *k*-Lin 假设是指对任意 PPT 算法 *A*:

$$\boldsymbol{Adv}_A^{DDH}(\kappa) := |\Pr[\boldsymbol{Exp}_A^{DDH}(\kappa)=1 \mid b=0] - \Pr[\boldsymbol{Exp}_A^{DDH}(\kappa)=1 \mid b=1]|$$

都是可忽略的. 其中, 实验 $\boldsymbol{Exp}_A^{DDH}(\kappa)$ 定义如下:

Experiment $\boldsymbol{Exp}_A^{DDH}(\kappa)$:

$p,q \leftarrow \mathcal{SP}\left(\frac{\kappa}{2}\right)$; $N=pq$; $g \leftarrow \mathcal{QR}_{N^2}$; $x,y,z \leftarrow [|\mathcal{QR}_{N^2}|]$; $b \leftarrow \{0,1\}$

$X=g^x \bmod N^2$; $Y=g^y \bmod N^2$; $Z_0=g^{xy} \bmod N^2$; $Z_1=g^z \bmod N^2$

$b' \leftarrow A(N,g,X,Y,Z_b)$

Return b'.

2.3 公钥加密

一个公钥加密方案 PKE 由(*Setup*,*Gen*,*Enc*,*Dec*)这 4 个 PPT 算法组成, 其中: 设置算法 *Setup* 以安全参数 1^κ作为输入, 输出一个公共参数 *pp*; 密钥生成算法 *Gen* 以公共参数 *pp* 作为输入, 输出一对公私钥对(*pk*,*sk*); 加密算法 *Enc* 以公共参数 *pp*、公钥 *pk* 和明文 *m* 作为输入, 输出一个密文 *c*; 解密算法 *Dec* 是确定性算法, 以公共参数 *pp*、私钥 *sk* 和密文 *c* 作为输入, 输出一个明文 *m* 或符号⊥(表示 *c* 不是合法密文).

记 PKE 的明文空间为$\mathcal{M}$. PKE 的正确性要求如下: 对任意由 *Setup* 生成的 *pp*, 对任意由 *Gen*(*pp*)生成的(*pk*,*sk*)和任意合法明文 $m \in \mathcal{M}$, 有 *Dec*(*pp*,*sk*,*Enc*(*pp*,*pk*,*m*))=*m*.

安全性方面, 我们考虑标准的公钥加密安全模型: 抗选择明文攻击的密文不可区分性(indistinguishability under chosen-plaintext attack, IND-CPA 安全性)和抗非自适应选择密文攻击的密文不可区分性(indistinguishability under non-adaptive chosen-ciphertext attack, IND-CCA1 安全性). 其中, IND-CCA1 的安全性强于 IND-CPA 的安全性.

定义 2(IND-CPA 安全性). 如果对任意 PPT 敌手 $A=(A_1,A_2)$, *A* 在 $\boldsymbol{Exp}_{PKE,A}^{IND\text{-}CPA}(\kappa)$ 中的优势为

$$\boldsymbol{Adv}_{PKE,A}^{IND\text{-}CPA}(\kappa) := \left|\Pr[\boldsymbol{Exp}_{PKE,A}^{IND\text{-}CPA}(\kappa)=1]-\frac{1}{2}\right|$$

都是可忽略的, 则称 PKE 是 IND-CPA 安全的. 其中, 实验 $\boldsymbol{Exp}_{PKE,A}^{IND\text{-}CPA}(\kappa)$ 定义如下.

Experiment $\boldsymbol{Exp}_{PKE,A}^{IND\text{-}CPA}(\kappa)$:

$pp \leftarrow Setup(1^\kappa)$; $(pk,sk) \leftarrow Gen(pp)$; $b \leftarrow \{0,1\}$

$(m_0^*,m_1^*,st) \leftarrow A_1(pp,pk)$; $c^* \leftarrow Enc(pp,pk,m_b^*)$; $b' \leftarrow A_2(c^*,st)$

Return ($b'=b$)

在上述实验中, 我们要求 $m_0^*,m_1^* \in \mathcal{M}$ 且 $|m_0^*|=|m_1^*|$.

定义 3(IND-CPA 安全性). 如果对任意 PPT 敌手 $A=(A_1,A_2)$, *A* 在 $\boldsymbol{Exp}_{PKE,A}^{IND\text{-}CCA1}(\kappa)$ 中的优势为

$$\boldsymbol{Adv}_{PKE,A}^{IND\text{-}CCA1}(\kappa) := \left|\Pr[\boldsymbol{Exp}_{PKE,A}^{IND\text{-}CCA1}(\kappa)=1]-\frac{1}{2}\right|$$

都是可忽略的, 则称 PKE 是 IND-CCA1 安全的. 其中, 实验 $\boldsymbol{Exp}_{PKE,A}^{IND\text{-}CCA1}(\kappa)$ 定义如下.

Experiment $\boldsymbol{Exp}_{PKE,A}^{IND\text{-}CCA1}(\kappa)$:

$pp \leftarrow Setup(1^\kappa)$; $(pk,sk) \leftarrow Gen(pp)$; $b \leftarrow \{0,1\}$

$(m_0^*,m_1^*,st) \leftarrow A_1^{Dec(pp,sk,\cdot)}(pp,pk)$; $c^* \leftarrow Enc(pp,pk,m_b^*)$; $b' \leftarrow A_2(c^*,st)$

Return ($b'=b$)

在上述实验中, 我们要求 $m_0^*,m_1^* \in \mathcal{M}$ 且 $|m_0^*|=|m_1^*|$. A_1 可以向解密预言机 *Dec*(*pp*,*sk*,·)询问任意密文 *c*′, 将会收到 *Dec*(*pp*,*sk*,*c*′)作为回答.

3 基于判定性 *k*-Lin 假设的加法同态加密方案

本节中, 我们提出一个基于 $\mathbb{Z}_{N^2}^*$ 上的判定性 *k*-Lin 假设的公钥加密方案. 该方案的优势在于: (1) 具有加法同态性, 从而能够在一定程度上保证数据的可用性; (2) 安全性可细粒度调节, 即可根据现实场景中的安全需求(根据所需的安全性强度)对方案进行具体调节, 比如从 IND-CCA1 安全性降为 IND-CPA 安全性, 或者把方案安全性所依赖的困难性假设逐步减弱等等.

本节结构如下: 首先, 我们引入新的计算困难性假设($\mathbb{Z}_{N^2}^*$ 上的判定性 *k*-Lin 假设); 接着, 我们基于这一假设构造 IND-CCA1 安全的加法同态加密方案; 最后, 进一步介绍该方案所具有的特性.

3.1 $\mathbb{Z}_{N^2}^*$ 上的判定性*k*-Lin假设

本节中, 我们给出 $\mathbb{Z}_{N^2}^*$ 上判定性 *k*-Lin 假设(简记为 *k*-Lin 假设)的正式定义.

定义 4($\mathbb{Z}_{N^2}^*$ 上的 *k*-Lin 假设). 对任意 $k\in\mathbb{N}$, $\mathbb{Z}_{N^2}^*$ 上的 *k*-Lin 假设是指对任意 PPT 算法 *A*:

$$\boldsymbol{Adv}_A^{k\text{-}Lin}(\kappa):=|\Pr[\boldsymbol{Exp}_A^{k\text{-}Lin}(\kappa)=1\,|\,b=0]-\Pr[\boldsymbol{Exp}_A^{k\text{-}Lin}(\kappa)=1\,|\,b=1]|$$

都是可忽略的. 其中, 实验 $\boldsymbol{Exp}_A^{k\text{-}Lin}(\kappa)$ 如下所示.

Experiment $\boldsymbol{Exp}_A^{k\text{-}Lin}(\kappa)$:

$p,q\leftarrow\mathcal{SP}\left(\frac{\kappa}{2}\right)$; $N=pq$; $g\leftarrow\mathcal{QR}_{N^2}$; $x_1,...,x_k$, $y_1,...,y_k$, $z\leftarrow[|\mathcal{QR}_{N^2}|]$; $b\leftarrow\{0,1\}$

$X_1=g^{x_1} \bmod N^2;...;X_k=g^{x_k} \bmod N^2;...;T_1=g^{x_1y_1} \bmod N^2;...;T_k=g^{x_ky_k} \bmod N^2$

$Z_0=g^{y_1+...+y_k} \bmod N^2$; $Z_1=g^z \bmod N^2$; $b'\leftarrow A(N,g,X_1,...,X_k,T_1,...,T_k,Z_b)$

Return b'.

$\mathbb{Z}_{N^2}^*$ 上的 *k*-Lin 假设相当于 Hofheinz 和 Kiltz 在[22]中定义的 *k*-Linear 假设的一种特殊形式(即其循环群取定为 $\mathcal{QR}_{N^2}$), 也可视为文献[20]中的 $\mathbb{Z}_{N^2}^*$ 上 DDH 假设的一个推广版本. 而且, $\mathbb{Z}_{N^2}^*$ 上的 *k*-Lin 假设弱于 DDH 假设. 正式地, 我们有如下定理.

定理 1. 若 $\mathbb{Z}_{N^2}^*$ 上的 DDH 假设成立, 则对任意 $k\in\mathbb{N}$, $\mathbb{Z}_{N^2}^*$ 上的 *k*-Lin 假设也成立. 而且, *k* 越大, $\mathbb{Z}_{N^2}^*$ 上的 *k*-Lin 假设就越弱.

该定理证明比较简单. 出于完整性考虑, 我们在本文附录 A 中附上该定理的证明.

3.2 方案构造

本节中, 我们提出一个基于 $\mathbb{Z}_{N^2}^*$ 上 *k*-Lin 假设的加法同态公钥加密方案.

令明文空间为 $\mathcal{M}=\mathbb{Z}_N$, 密文空间为 $(\mathbb{Z}_{N^2}^*)^{k+3}$, 其中, $k\in\mathbb{N}$. 我们的加密方案 PKE_{add} 如图 1 所示.

- PKE_{add} 的正确性分析如下.

由于:

$$\prod_{i=1}^{k+1}c_i^{a_i} \bmod N^2=\prod_{i=1}^{k}(X_i^{r_i})^{a_i}\cdot\left(\prod_{i=1}^{k}g^{r_i}\right)^{a_{k+1}} \bmod N^2=\prod_{i=1}^{k}(X_i^{a_i}g^{a_{k+1}})^{r_i} \bmod N^2=\prod_{i=1}^{k}d_i^{r_i} \bmod N^2=c_{k+3},$$

所以解密算法 *Dec* 不会返回⊥. 又因为:

$$\prod_{i=1}^{k+1}c_i^{b_i} \bmod N^2=\prod_{i=1}^{k}(X_i^{r_i})^{b_i}\cdot\left(\prod_{i=1}^{k}g^{r_i}\right)^{b_{k+1}} \bmod N^2=\prod_{i=1}^{k}(X_i^{b_i}g^{b_{k+1}})^{r_i} \bmod N^2=\prod_{i=1}^{k}h_i^{r_i} \bmod N^2,$$

于是有:

$$u=\frac{c_{k+2}}{\prod_{i=1}^{k+1}c_i^{b_i}} \bmod N^2=\frac{\prod_{i=1}^{k}h_i^{r_i}(1+mN) \bmod N^2}{\prod_{i=1}^{k}h_i^{r_i} \bmod N^2} \bmod N^2=1+mN \bmod N^2.$$

考虑到 $m\in\mathcal{M}=\mathbb{Z}_N$, 所以:

$$\tilde{m}=\frac{u-1 \bmod N^2}{N}=\frac{mN \bmod N^2}{N}=m.$$

由此, 正确性得证.

- 加法同态性.

下面, 我们验证 PKE_{add} 的加法同态性. 对任意 $m_1,m_2\in\mathcal{M}=\mathbb{Z}_N$, 记 $Enc(pp,pk,m_1)$所使用的随机数为 $(r_1^{(1)},...,r_k^{(1)})$, $Enc(pp,pk,m_2)$所使用的随机数为 $(r_1^{(2)},...,r_k^{(2)})$. 于是, 有:

$$Enc(pp,pk,m_1)=\left(X_1^{r_1^{(1)}} \bmod N^2,...,X_k^{r_k^{(1)}} \bmod N^2,\prod_{i=1}^{k}g^{r_i^{(1)}} \bmod N^2,\prod_{i=1}^{k}h_i^{r_i^{(1)}}(1+m_1N) \bmod N^2,\prod_{i=1}^{k}d_i^{r_i^{(1)}} \bmod N^2\right),$$

$$Enc(pp,pk,m_2)=\left(X_1^{r_1^{(2)}} \bmod N^2,...,X_k^{r_k^{(2)}} \bmod N^2,\prod_{i=1}^{k}g^{r_i^{(2)}} \bmod N^2,\prod_{i=1}^{k}h_i^{r_i^{(2)}}(1+m_2N) \bmod N^2,\prod_{i=1}^{k}d_i^{r_i^{(2)}} \bmod N^2\right).$$

从而可得:

$$\begin{aligned}Enc(pp,pk,m_1)\cdot Enc(pp,pk,m_2)=&\left(X_1^{r_1^{(1)}+r_1^{(2)}} \bmod N^2,...,X_k^{r_k^{(1)}+r_k^{(2)}} \bmod N^2,\prod_{i=1}^{k}g^{r_i^{(1)}+r_i^{(2)}} \bmod N^2,\right.\\&\left.\prod_{i=1}^{k}h_i^{r_i^{(1)}+r_i^{(2)}}(1+m_1N)(1+m_2N) \bmod N^2,\prod_{i=1}^{k}d_i^{r_i^{(1)}+r_i^{(2)}} \bmod N^2\right)\\=&\left(X_1^{r_1^{(1)}+r_1^{(2)}} \bmod N^2,...,X_k^{r_k^{(1)}+r_k^{(2)}} \bmod N^2,\prod_{i=1}^{k}g^{r_i^{(1)}+r_i^{(2)}} \bmod N^2,\right.\\&\left.\prod_{i=1}^{k}h_i^{r_i^{(1)}+r_i^{(2)}}(1+(m_1+m_2)N) \bmod N^2,\prod_{i=1}^{k}d_i^{r_i^{(1)}+r_i^{(2)}} \bmod N^2\right)\\=&Enc(pp,pk,m_1+m_2).\end{aligned}$$

Setup(1^κ):

$p,q\leftarrow\mathcal{SP}\left(\frac{\kappa}{2}\right)$; $N=pq$; $p'=\frac{p-1}{2}$; $q'=\frac{q-1}{2}$; $\alpha\leftarrow\mathbb{Z}_{N^2}^*$; $g=\alpha^2 \bmod N^2$

If $ord(g)\neq|\mathcal{QR}_{N^2}|$ (i.e., one of $g^{p'qq'}$, $g^{pqq'}$, $g^{pp'q'}$, $g^{pp'q}$ equals 1 mod N^2):

repeat the process of $\alpha\leftarrow\mathbb{Z}_{N^2}^*$, until $ord(g)=|\mathcal{QR}_{N^2}|$

For $1\leqslant i\leqslant k$:

$x_i\leftarrow[|\mathcal{QR}_{N^2}|]$

If $\gcd(x_i,|\mathcal{QR}_{N^2}|)\neq 1$:

repeat the process of $x_i\leftarrow[|\mathcal{QR}_{N^2}|]$, until $\gcd(x_i,|\mathcal{QR}_{N^2}|)=1$

$X_i=g^{x_i} \bmod N^2$

$pp=(N,g,(X_i)_{i\in[k]})$

Return pp

Gen(pp):

$a_1,...,a_{k+1},b_1,...,b_{k+1}\leftarrow[|\mathcal{QR}_{N^2}|]$

For $1\leqslant i\leqslant k$:

$d_i=X_i^{a_i}g^{a_{k+1}} \bmod N^2$; $h_i=X_i^{b_i}g^{b_{k+1}} \bmod N^2$

$pk=((d_i)_{i\in[k]},(h_i)_{i\in[k]})$; $sk=(a_1,\ldots,a_{k+1},b_1,\ldots,b_{k+1})$

Return (pk,sk)

图 1 公钥加密方案 PKE_{add}

Enc(*pp*,*pk*,*m*):

$r_1,...,r_k \leftarrow \mathbb{Z}_{N^2}$; $c_1 = X_1^{r_1} \bmod N^2$;...; $c_k = X_k^{r_k} \bmod N^2$

$c_{k+1} = \prod_{i=1}^{k} g^{r_i} \bmod N^2$; $c_{k+2} = \prod_{i=1}^{k} h_i^{r_i}(1+mN) \bmod N^2$; $c_{k+3} = \prod_{i=1}^{k} d_i^{r_i} \bmod N^2$

Return $c=(c_1,\ldots,c_{k+3})$

Dec(*pp*,*sk*,$c=(c_1,\ldots,c_{k+3})$):

If $c_{k+3} \neq \prod_{i=1}^{k+1} c_i^{a_i}$: Return $\perp$

$u = \dfrac{c_{k+2}}{\prod_{i=1}^{k+1} c_i^{b_i}} \bmod N^2$; $\tilde{m} = \dfrac{u-1 \bmod N^2}{N}$

Return $\tilde{m}$

图 1 公钥加密方案 PKE_{add} (续)

3.3 安全性证明

本节中, 我们证明加密方案 PKE_{add} 满足 IND-CCA1 安全性. 具体而言, 我们有下述定理.

定理 2. 对任意 $k\in\mathbb{N}$, 当 $\mathbb{Z}_{N^2}^*$ 上的 k-Lin 假设成立时, PKE_{add} 满足 IND-CCA1 安全性.

证明: 假设 PKE_{add} 不满足 IND-CCA1 安全性, 则必然存在一个 IND-CCA1 敌手 A, 使得 $\boldsymbol{Adv}_{PKE_{add},A}^{IND\text{-}CCA1}(\kappa)$ 不可忽略. 记 A_1 的解密询问次数为 Q_d. 我们构造一个针对 $\mathbb{Z}_{N^2}^*$ 上 k-Lin 问题的敌手 B 如下所示.

B 收到$(N,g,X_1,\ldots,X_k,T_1,\ldots,T_k,Z)$以后, 随机选取 $a_1,...,a_{k+1},b_1,...,b_{k+1} \leftarrow \left[\dfrac{N^2}{4}\right]$, 并计算:

$$d_1 = X_1^{a_1} g^{a_{k+1}} \bmod N^2;...;\ d_k = X_k^{a_k} g^{a_{k+1}} \bmod N^2,$$
$$h_1 = X_1^{b_1} g^{b_{k+1}} \bmod N^2;...;\ h_k = X_k^{b_k} g^{b_{k+1}} \bmod N^2.$$

B 令 $pk=(N,g,(X_i)_{i\in[k]},(d_i)_{i\in[k]},(h_i)_{i\in[k]})$, $sk=(a_1,\ldots,a_{k+1},b_1,\ldots,b_{k+1})$, 并将 pk 发给 A_1.

由于 B 持有 sk, 所以 B 可以正确回答 A_1 的解密询问.

B 从 A_1 处收到 (m_0^*,m_1^*) 之后, 随机选取 $b\leftarrow\{0,1\}$, 计算:

$$c_1^* = T_1 \bmod N^2,...,c_k^* = T_k \bmod N^2,$$
$$c_{k+1}^* = Z \bmod N^2;\ c_{k+2}^* = \prod_{i=1}^{k+1}(c_i^*)^{b_i}(1+m_b^*N) \bmod N^2;\ c_{k+3}^* = \prod_{i=1}^{k+1}(c_i^*)^{a_i} \bmod N^2.$$

然后, B 将挑战密文 $c^* = (c_1^*,...,c_{k+3}^*)$ 发给 A_2.

最后, B 从 A_2 处收到一个比特 b', 将 $b''=(b'=b)$作为自己的最终输出值.

以上就是关于敌手 B 的描述. 下面我们考虑 B 的优势.

首先, 我们记事件 Event 为"存在某个 $i'\in[k+1]$, 使得 $a_{i'} > \dfrac{N\phi(N)}{4}$ 或 $b_{i'} > \dfrac{N\phi(N)}{4}$". 由于 $a_1,\ldots,a_{k+1}$, $b_1,\ldots,b_{k+1}$ 都是从 $\left[\dfrac{N^2}{4}\right]$ 中均匀随机采样的, 而 $\dfrac{N\phi(N)}{4} = pp'qq' = N\cdot\dfrac{p-1}{2}\dfrac{q-1}{2} = \dfrac{N^2}{4} - \dfrac{(p+q)N-1}{4}$, 从而有:

$$\Pr[Event] \leqslant 2(k+1)\frac{(p+q)N-1}{N^2}$$

仍是一个可忽略的量.

当 $Z = g^{y_1+\ldots+y_k}$ 时, 若事件 Event 不发生, 则 B 完美地为 A 提供了 $\boldsymbol{Exp}_{PKE_{add},A}^{IND\text{-}CCA1}(\kappa)$ 的环境. 所以:

$$\begin{aligned}\Pr[\boldsymbol{Exp}_B^{k\text{-}Lin}(\kappa)=1\mid Z=g^{y_1+\ldots+y_k}] &\geqslant \Pr[\boldsymbol{Exp}_B^{k\text{-}Lin}(\kappa)=1\mid (Z=g^{y_1+\ldots+y_k})\wedge\neg Event]\cdot\Pr[\neg Event\mid Z=g^{y_1+\ldots+y_k}]\\ &=\Pr[\boldsymbol{Exp}_B^{k\text{-}Lin}(\kappa)=1\mid (Z=g^{y_1+\ldots+y_k})\wedge\neg Event]\cdot\Pr[\neg Event]\\ &\geqslant \Pr[\boldsymbol{Exp}_{PKE_{add},A}^{IND\text{-}CCA1}(\kappa)=1]\cdot\left(1-2(k+1)\frac{(p+q)N-1}{N^2}\right)\\ &\geqslant \Pr[\boldsymbol{Exp}_{PKE_{add},A}^{IND\text{-}CCA1}(\kappa)=1]-2(k+1)\frac{(p+q)N-1}{N^2}.\end{aligned}$$

接下来, 我们考虑 $Z=g^z \bmod N^2 (z\leftarrow|\mathcal{QR}_{N^2}|)$时的情况. 记 $\Delta z=z-(y_1+\ldots+y_k) \bmod |\mathcal{QR}_{N^2}|$. 由于 z 是从$|\mathcal{QR}_{N^2}|$中均匀选取的, 以压倒性的概率(准确地说, 概率是$1-\frac{1}{pp'qq'}$)有$\Delta z\neq 0$.

为简单起见, 我们用"log(·)"表示"$\log_g(\cdot)$". 敌手 A 从公钥 pk 中所能得到的所有关于$(b_1,\ldots,b_{k+1})$的信息最多只有:

$$\log(h_1)=b_1x_1+b_{k+1},\ldots,\log(h_k)=b_kx_k+b_{k+1}.$$

又因为

$$\begin{bmatrix}\log(h_1)\\ \vdots\\ \log(h_k)\\ b_{k+1}\end{bmatrix}=\begin{bmatrix}x_1 & 0 & \cdots & 0 & 1\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & \cdots & x_k & 1\\ 0 & 0 & \cdots & 0 & 1\end{bmatrix}\begin{bmatrix}b_1\\ \vdots\\ b_k\\ b_{k+1}\end{bmatrix}$$

将系数矩阵记为 M_{k+1}, 则显然有 $\det M_{k+1}\neq 0$. 所以即使给定公钥 pk, 当 A_1 没有进行解密询问时, 从 A_1 的角度来看, b_{k+1} 的分布仍是均匀随机的.

另一方面, 挑战密文 $c^*=(c_1^*,\ldots,c_{k+3}^*)$ 中与$(b_1,\ldots,b_{k+1})$相关的部分只有 c_{k+2}^*, 而 c_{k+2}^* 中用于掩盖明文的部分为 $\prod_{i=1}^{k+1}(c_i^*)^{b_i}=\prod_{i=1}^{k}T_i^{b_i}Z^{b_{k+1}}=g^{(b_1x_1y_1+\ldots+b_kx_ky_k)+b_{k+1}z}$. 我们注意到:

$$\begin{aligned}\log\left(\prod_{i=1}^{k}T_i^{b_i}Z^{b_{k+1}}\right)&=(b_1x_1y_1+\ldots+b_kx_ky_k)+b_{k+1}z\\ &=(b_1x_1y_1+\ldots+b_kx_ky_k)+b_{k+1}(y_1+\ldots+y_k+\Delta z)\\ &=\log(h_1)y_1+\ldots+\log(h_k)y_k+b_{k+1}\Delta z.\end{aligned}$$

所以, 如果不考虑解密询问(即假设敌手 A 只能看到公钥和挑战密文), 那么当$\Delta z\neq 0$ 时, 从 A 的角度来看, 挑战密文服从均匀分布(即: 无论 B 选取的挑战明文是 m_0^* 还是 m_1^*, 从 A 的角度来看, 挑战密文的分布都是一样的). □

接下来, 我们进一步分析 A_1 能够进行解密询问时的成功概率.

记事件 Bad 为"A_1 提出某个解密询问 $c'=(c_1',\ldots,c_{k+3}')$, 使得: (i) $r_{k+1}'\neq r_1'+\ldots+r_k'$, 其中, $c_1'=X_1^{r_1'} \bmod N^2,\ldots$, $c_k'=X_k^{r_k'} \bmod N^2$, $c_{k+1}'=g^{r_{k+1}'} \bmod N^2$ 且 (ii) 解密算法 Dec 不返回$\perp$". 关于事件 Bad 发生的概率, 我们有如下引理.

引理 1. $\Pr[Bad]\leqslant\frac{Q_d}{pp'qq'-(Q_d-1)}$.

若事件 Bad 不发生, 那么对于 A_1 提出的任意解密询问 $c'=(c_1',\ldots,c_{k+3}')$ (记 $c_1'=X_1^{r_1'} \bmod N^2,\ldots, c_k'=X_k^{r_k'}$, $\bmod N^2$, $c_{k+1}'=g^{r_{k+1}'} \bmod N^2$), 要么该密文满足 $r_{k+1}'=r_1'+\ldots+r_k'$, 要么解密预言机返回$\perp$. 如果解密预言机返回$\perp$, A_1 不会得到任何关于$(b_1,\ldots,b_{k+1})$的信息; 如果解密预言机返回 m', 则 A_1 可自行计算出 $\prod_{i=1}^{k+1}(c_i')^{b_i}=\frac{c_{k+2}'}{1+m'N}$ $\bmod N^2$. 同时, 我们留意到:

$$\begin{aligned}\log\left(\prod_{i=1}^{k+1}(c_i')^{b_i}\right)&=b_1\log(c_1')+...+b_{k+1}\log(c_{k+1}')\\&=b_1x_1r_1'+...+b_kx_kr_k'+b_{k+1}r_{k+1}'\\&=b_1x_1r_1'+...+b_kx_kr_k'+b_{k+1}(r_1'+...+r_k')\\&=\log(h_1)r_1'+...+\log(h_k)r_k'.\end{aligned}$$

所以, 若事件 Bad 不发生, A_1 没有从解密询问中得到(除了公钥 pk 以外的)任何关于$(b_1,\ldots,b_{k+1})$的信息. 于是:

$$\begin{aligned}\Pr[\boldsymbol{Exp}_B^{k\text{-}Lin}(\kappa)=1\mid Z=g^z\wedge\Delta z\neq 0]&=\Pr[\boldsymbol{Exp}_B^{k\text{-}Lin}(\kappa)=1\mid Z=g^z\wedge\Delta z\neq 0\wedge\neg Bad]\cdot\Pr[\neg Bad\mid Z=g^z\wedge\Delta z\neq 0]+\\&\quad\Pr[\boldsymbol{Exp}_B^{k\text{-}Lin}(\kappa)=1\mid Z=g^z\wedge\Delta z\neq 0\wedge Bad]\cdot\Pr[Bad\mid Z=g^z\wedge\Delta z\neq 0]\\&=\Pr[\boldsymbol{Exp}_B^{k\text{-}Lin}(\kappa)=1\mid Z=g^z\wedge\Delta z\neq 0\wedge\neg Bad]\cdot\Pr[\neg Bad]\\&\leqslant\Pr[\boldsymbol{Exp}_B^{k\text{-}Lin}(\kappa)=1\mid Z=g^z\wedge\Delta z\neq 0\wedge\neg Bad]\cdot\Pr[\neg Bad]+\Pr[Bad]\\&=\frac{1}{2}\Pr[\neg Bad]+\Pr[Bad]\\&=\frac{1}{2}+\frac{1}{2}\Pr[Bad].\end{aligned}$$

上述第 2 个等号是因为只有 A_1 能提出解密询问, 而与 Z 有关的信息都是在挑战密文时才提供给 A. 也就是说, Z 的值对于 A_1 的解密询问没有任何影响.

综合起来, 有:

$$\begin{aligned}\boldsymbol{Adv}_B^{k\text{-}Lin}(\kappa)&=|\Pr[\boldsymbol{Exp}_B^{k\text{-}Lin}(\kappa)=1\mid Z=g^{y_1+...+y_k}]-\Pr[\boldsymbol{Exp}_B^{k\text{-}Lin}(\kappa)=1\mid Z=g^z]|\\&=\left(1-\frac{1}{pp'qq'}\right)|\Pr[\boldsymbol{Exp}_B^{k\text{-}Lin}(\kappa)=1\mid Z=g^{y_1+...+y_k}]-\Pr[\boldsymbol{Exp}_B^{k\text{-}Lin}(\kappa)=1\mid Z=g^z\wedge\Delta z\neq 0]|\\&\geqslant|\Pr[\boldsymbol{Exp}_B^{k\text{-}Lin}(\kappa)=1\mid Z=g^{y_1+...+y_k}]-\Pr[\boldsymbol{Exp}_B^{k\text{-}Lin}(\kappa)=1\mid Z=g^z\wedge\Delta z\neq 0]|-\frac{1}{pp'qq'}\\&\geqslant\Pr[\boldsymbol{Exp}_{PKE_{add},A}^{IND\text{-}CCA1}(\kappa)=1]-2(k+1)\frac{(p+q)N-1}{N^2}-\frac{1}{2}-\frac{1}{2}\Pr[Bad]-\frac{1}{pp'qq'}\\&\geqslant\boldsymbol{Adv}_{PKE_{add},A}^{IND\text{-}CCA1}(\kappa)-2(k+1)\frac{(p+q)N-1}{N^2}-\frac{Q_d}{2(pp'qq'-(Q_d-1))}-\frac{1}{pp'qq'}.\end{aligned}$$

由于 $\boldsymbol{Adv}_{PKE_{add},A}^{IND\text{-}CCA1}(\kappa)$ 不可忽略, 所以 $\boldsymbol{Adv}_B^{k\text{-}Lin}(\kappa)$ 也不可忽略, 与 $\mathbb{Z}_{N^2}^*$ 上的 k-Lin 假设矛盾.

最后, 我们补上引理 1 的证明.

证明(引理 1): 对任意 $j\in[Q_d]$, 记事件 Bad_j 为: A_1 的第 j 次解密询问使得 Bad 首次发生. 于是:

$$\Pr[Bad]\leqslant\sum_{j=1}^{Q_d}\Pr[Bad_j].$$

事件 Bad_j 发生, 即意味着 A_1 的第 j 次解密询问 $c'=(c_1',...,c_{k+3}')$ (记 $c_1'=X_1^{r_1'} \bmod N^2$,..., $c_k'=X_k^{r_k'} \bmod N^2$, $c_{k+1}'=g^{r_{k+1}'} \bmod N^2$)满足 $r_{k+1}'\neq r_1'+...+r_k'$ 且 $c_{k+3}'=\prod_{i=1}^{k+1}(c_i')^{a_i}$.

由于 A_1 还没有收到挑战密文, A_1 所知道的所有关于$(a_1,\ldots,a_{k+1})$的信息都是通过公钥 pk 而得. 也就是说, A_1 最多只知道$(\log(d_1)=a_1x_1+a_{k+1},\ldots,\log(d_k)=a_kx_k+a_{k+1})$. 由与前面类似的分析可知: 如果仅给定公钥 pk, 从 A_1 的角度来看, a_{k+1} 的分布仍是均匀随机的.

而另一方面, $r_{k+1}'\neq r_1'+...+r_k'$ 当且仅当 $\Delta r'=r_{k+1}'-(r_1'+...+r_k')\neq 0 \bmod |\mathcal{QR}_{N^2}|$, 而 $c_{k+3}'=\prod_{i=1}^{k+1}(c_i')^{a_i}$ 则意味着:

$$\begin{aligned}\log(c'_{k+3}) &= a_1\log(c'_1)+\ldots+a_k\log(c'_k)+a_{k+1}\log(c'_{k+1})\\ &= a_1x_1r'_1+\ldots+a_kx_kr'_k+a_{k+1}r'_{k+1}\\ &= a_1x_1r'_1+\ldots+a_kx_kr'_k+a_{k+1}(r'_1+\ldots+r'_k+\Delta r')\\ &= \log(d_1)r'_1+\ldots+\log(d_k)r'_k+a_{k+1}\Delta r'.\end{aligned}$$

由于$\Delta r'\neq 0$, 且 A_1 从公钥中没有得到任何关于 a_{k+1} 的信息, 所以对于第 j 次解密询问, A_1 能生成满足"$c'_{k+3}=\prod_{i=1}^{k+1}(c'_i)^{a_i}$"的 c'_{k+3} 的概率最多只有 $\frac{1}{pp'qq'-(j-1)}$.

所以, 综合起来有:

$$\Pr[Bad]\leqslant\sum_{j=1}^{Q_d}\Pr[Bad_j]\leqslant\sum_{j=1}^{Q_d}\frac{1}{pp'qq'-(j-1)}\leqslant\frac{Q_d}{pp'qq'-(Q_d-1)}.$$ □

3.4 方案的优势

在上一节, 我们已证明 PKE_{add} 是一个 IND-CCA1 安全的加法同态加密方案, 从而能在满足 IND-CCA1 安全性的前提下(一定程度上)保证数据的可用性. 本节中, 我们将进一步说明方案 PKE_{add} 额外具有的 3 个重要优势.

(1) 可以通过对参数 k 的调控, 来细粒度地调节 PKE_{add} 的 IND-CCA1 安全性强度;

(2) PKE_{add} 具有双解密机制, 在现实部署中, 能够有效减轻监管方的密钥管理成本和压力;

(3) PKE_{add} 能便利地退化为 IND-CPA 安全的加法同态加密方案, 以适应某些对传输数据长度和计算效率要求较高而安全性要求相对不那么高的应用场景.

3.4.1 细粒度调节 IND-CCA1 安全性强度

正如上一节分析所指出的, PKE_{add} 在 $\mathbb{Z}^*_{N^2}$ 上的 k-Lin 假设下能满足 IND-CCA1 安全性. 根据定理 1, k 越大, $\mathbb{Z}^*_{N^2}$ 上的 k-Lin 假设就越弱, PKE_{add} 的 IND-CCA1 安全性所依赖的困难假设也就越弱, 亦即 PKE_{add} 的 IND-CCA1 安全性就更能够得到保证. 因此, 可以通过对参数 k 的调控, 来调整 PKE_{add} 的 IND-CCA1 安全性强度.

为了便于区分, 对于 $k\in\mathbb{N}$, 若 PKE_{add} 的 IND-CCA1 安全性依赖于 $\mathbb{Z}^*_{N^2}$ 上的 k-Lin 假设, 我们就称 PKE_{add} 达到 k-级别的 IND-CCA1 安全性强度.

我们强调: 对任意 $0\leqslant k_0\leqslant k_1$, PKE_{add} 都能够很便利地由 k_0-级别的 IND-CCA1 安全性强度提升为 k_1-级别的 IND-CCA1 安全性强度.

具体转化方式如下.

假设当前在应用中部署的 $PKE_{add}=(Setup,Gen,Enc,Dec)$ 满足 k_0-级别的 IND-CCA1 安全性强度, 由于现实的信息安全环境变化, 需要将其 IND-CCA1 安全性强度提升到 k_1 级别(相应地, 将这一级别的方案简记为 $PKE'_{add}=(Setup',Gen',Enc',Dec')$). 记 pp 是当前阶段 $Setup$ 所生成的公共参数和陷门, (pk,sk) 是当前阶段 Gen 所生成的公私钥对, $c=(c_1,\ldots,c_{k_0+3})$ 是当前阶段的任意一个由 Enc 生成的密文. 我们提出 3 个转化算法 $(TransfmSetup,TransfmGen,TransfmEnc)$, 如图 2 所示.

具体而言: 算法 $TransfmSetup$ 以 pp 为输入, 生成新的公共参数 pp'; 算法 $TransfmGen$ 以 (pk,sk) 为输入, 生成新的公私钥对 (pk',sk'); 算法 $TransfmEnc$ 以 $(c_1,\ldots,c_{k_0+3})$ 为输入, 生成新的密文 $c'=(c'_1,\ldots,c'_{k_1+3})$. 通过各元素的结构对比, 可以看出:

(i) pp' 可作为 PKE'_{add} 的公共参数;

(ii) (pk',sk') 可分别作为 PKE'_{add} 的公钥和私钥;

(iii) $c'=(c'_1,\ldots,c'_{k_1+3})$ 可作为 PKE'_{add} 的密文, 且其用 Dec' 解密所得明文与 $(c_1,\ldots,c_{k_0+3})$ 用 Dec 解密所得明文完全相同.

而且, 转化后得到的 pp'、(pk',sk') 和 c' 也几乎最大限度地保留了原来 pp、(pk,sk) 和 c 中的元素. 换句话说, 图 2 的转化方法可看作是在最大限度地保留现有参数、公私钥对和密文等各要素的基础上, 将满足 k_0-级别

IND-CCA1 安全性强度的 PKE_{add} 转化为满足 k_1-级别 IND-CCA1 安全性强度的 PKE'_{add}.

TransfmSetup(pp):
Parse $pp=(N,g,(X_i)_{i\in[k_0]})$
For $k_0+1\leqslant i\leqslant k_1$:
$x_i\leftarrow[|\mathcal{QR}_{N^2}|]$
If $\gcd(x_i,|\mathcal{QR}_{N^2}|)\neq 1$:
repeat the process of $x_i\leftarrow[|\mathcal{QR}_{N^2}|]$, until $\gcd(x_i,|\mathcal{QR}_{N^2}|)=1$
$X_i=g^{x_i} \bmod N^2$
$pp'=(N,g,(X_i)_{i\in[k_1]})$
Return pp'

TransfmGen(pp',(pk,sk)):
Parse $pk=((d_i)_{i\in[k_0]},(h_i)_{i\in[k_0]})$, $sk=(a_1,...,a_{k_0+1},b_1,...,b_{k_0+1})$
$a'_{k_0+1},...,a'_{k_1},b'_{k_0+1},...,b'_{k_1}\leftarrow[|\mathcal{QR}_{N^2}|]$
$a'_{k_1+1}=a_{k_0+1}$; $b'_{k_1+1}=b_{k_0+1}$
For $k_0+1\leqslant i\leqslant k_1$:
$d_i=X_i^{a'_i}g^{a'_{k_1+1}} \bmod N^2$; $h_i=X_i^{b'_i}g^{b'_{k_1+1}} \bmod N^2$
$pk'=((d_i)_{i\in[k_1]},(h_i)_{i\in[k_1]})$; $sk'=(a_1,...,a_{k_0},a'_{k_0+1},...,a'_{k_1+1},b_1,...,b_{k_0},b'_{k_0+1},...,b'_{k_1+1})$
Return (pk',sk')

TransfmEnc(pp', pk',(c_1,...,c_{k_0+3})):
$r_{k_0+1},...,r_{k_1}\leftarrow\mathbb{Z}_{N^2}$; $c'_{k_0+1}=X_{k_0+1}^{r_{k_0+1}} \bmod N^2$;...; $c'_{k_1}=X_{k_1}^{r_{k_1}} \bmod N^2$
$c'_{k_1+1}=c_{k_0+1}\cdot\prod_{i=k_0+1}^{k_1}g^{r_i} \bmod N^2$; $c'_{k_1+2}=c_{k_0+2}\cdot\prod_{i=k_0+1}^{k_1}h_i^{r_i} \bmod N^2$
$c'_{k_1+3}=c_{k_0+3}\cdot\prod_{i=k_0+1}^{k_1}d_i^{r_i} \bmod N^2$
Return $c'=(c_1,...,c_{k_0},c'_{k_0+1},...,c'_{k_1+3})$

图 2 转化算法 *TransfmSetup*、*TransfmGen* 和 *TransfmEnc*

3.4.2 双解密机制

按照图 1 所示, PKE_{add} 的 *Setup* 算法在运行过程中生成了两个素数 p 和 q. 记陷门 $td=(p,q)$. 我们可以在 PKE_{add} 现有的 4 个算法(即 *Setup*、*Gen*、*Enc* 和 *Dec*)之外再构造一个新的解密算法 *MDec*: 该算法以公共参数 pp、陷门 td、用户公钥 pk 和密文 c 作为输入, 输出一个明文 m 或符号⊥(表示 c 不是合法密文). 具体来说, *MDec* 的构造方法如下.

首先, 对任意 $p,q\leftarrow\mathcal{SP}\left(\frac{\kappa}{2}\right)$, $N=pq$, 记 g 为 $\mathcal{QR}_{N^2}$ 中的任意一个生成元, 令 $a\in[|\mathcal{QR}_{N^2}|]$, $h=g^a \bmod N^2$. 考虑下述算法 $Comp_{DL}$.

$Comp_{DL}(N,g,h)$:

$$u=\frac{h^{\lambda(N)}-1 \bmod N^2}{N};\ v=\frac{g^{\lambda(N)}-1 \bmod N^2}{N};\ \tilde{a}=\frac{u}{v} \bmod N$$

Return $\tilde{a}$

由于 $\mathcal{QR}_{N^2}$ 是阶为 $\frac{N\phi(N)}{4}$ 的循环群, g 是 $\mathcal{QR}_{N^2}$ 的生成元, 从而 $g^{\lambda(N)}$的阶是 N, 所以 $g^{\lambda(N)}$可以写成 $1+kN(k\in\mathbb{N})$的形式[4,20]. 于是, $\frac{g^{\lambda(N)}-1 \bmod N^2}{N}=k \bmod N$, $\frac{h^{\lambda(N)}-1 \bmod N^2}{N}=ak \bmod N$.

所以, $Comp_{DL}(N,g,h)$的输出 $\tilde{a}=a \bmod N$.

因此, 有下述定理.

定理 3. 对 $\mathcal{QR}_{N^2}$ 的任意生成元 g 和任意 $a\in[|\mathcal{QR}_{N^2}|]$, 均有 $\tilde{a}=a \bmod N$.

以算法 $Comp_{DL}$ 为基本构件, 我们设计了算法 *MDec*, 如图 3 所示. 其中, 该算法所调用的 $Comp_{DL}$ 见第 3.4.2 节.

MDec(pp,td,pk,c=(c_1,…,c_{k+3})):

Parse $pp=(N,g,(X_i)_{i\in[k]})$, $td=(p,q)$, $pk=((d_i)_{i\in[k]},(h_i)_{i\in[k]})$

$p'=\frac{p-1}{2}$; $q'=\frac{q-1}{2}$; $\omega=(2p'q')^{-1} \bmod N$

For $1\leqslant i\leqslant k$:

$\hat{r}_i=Comp_{DL}(N,X_i,c_i)$

$u=\left(\frac{c_{k+2}}{\prod_{i=1}^{k}h_i^{\hat{r}_i}}\right)^{2p'q'} \bmod N^2$

Return $\tilde{m}=\frac{u-1 \bmod N^2}{N}\omega \bmod N$

图 3 PKE_{add} 的另一个解密算法 *MDec*

下面我们分析 *MDec* 的解密正确性.

由于 g 是 $\mathcal{QR}_{N^2}$ 的生成元, 且对任意 $i\in[k]$, 均有 $\gcd(x_i,|\mathcal{QR}_{N^2}|)=1$, 所以对任意 $i\in[k]$, X_i 也是 $\mathcal{QR}_{N^2}$ 的生成元. 从而根据定理 3, 对任意 $i\in[k]$, 有:

$$\hat{r}_i=Comp_{DL}(N,X_i,c_i)=r_i \bmod N.$$

又因为 g 的阶为 $pp'qq'=Np'q'$, 所以对任意 $i\in[k]$, 有:

$$(h_i^{r_i})^{p'q'}=((g^{b_ix_i+b_{k+1}})^{r_i})^{p'q'}=((g^{b_ix_i+b_{k+1}})^{\hat{r}_i})^{p'q'}=(h_i^{\hat{r}_i})^{p'q'} \bmod N^2.$$

从而有:

$$c_{k+2}^{2p'q'}=\left(\prod_{i=1}^{k}h_i^{r_i}(1+mN)\right)^{2p'q'}=\prod_{i=1}^{k}h_i^{2p'q'\hat{r}_i}(1+mN)^{2p'q'}.$$

于是:

$$u=\left(\frac{c_{k+2}}{\prod_{i=1}^{k}h_i^{\hat{r}_i}}\right)^{2p'q'}=(1+mN)^{2p'q'}=1+2p'q'mN \bmod N^2.$$

所以有:

$$\tilde{m}=\frac{u-1 \bmod N^2}{N}\omega \bmod N=\frac{2p'q'mN \bmod N^2}{N}\omega \bmod N=m.$$

由此, *MDec* 的解密正确性得证.

- 讨论

综上所述, 当知道陷门 td=(p,q)时, *MDec* 也可以作为方案 PKE_{add} 的又一个解密算法. 而且, *MDec* 不需要以私钥 sk 作为输入, 所以在现实应用中, 可以让各用户保存自己的公私钥, 而监管方持有陷门 td, 这样一来, 监管方就可以通过 *MDec* 算法对用户的密文数据进行解密和监管, 而不需要存储所有用户的私钥信息, 极大地减轻了监管方在密钥管理方面的成本和压力.

3.4.3 IND-CPA 安全性

我们的方案 PKE_{add} 也可以极为便利地退化成 IND-CPA 安全的加密方案(简记为 PKE_{add}^{cpa}), 以适应某些效率要求更高而安全性要求相对不那么高的应用场景.

具体来说, IND-CPA 安全的加密方案 PKE_{add}^{cpa} 如图 4 所示.

PKE_{add}^{cpa} 的正确性分析、加法同态性分析和 IND-CPA 安全性证明均与 PKE_{add} 的分析类似, 这里不再重复.

与 PKE_{add} 相比, PKE_{add}^{cpa} 的安全性退化为 IND-CPA, 但相应地公私钥长度也减小了一半, 密文也减少了一个群元素.

$Setup^{cpa}(1^{\kappa})$:

$p,q \leftarrow \mathcal{SP}\left(\frac{\kappa}{2}\right)$; $N=pq$; $p'=\frac{p-1}{2}$; $q'=\frac{q-1}{2}$; $\alpha \leftarrow \mathbb{Z}^*_{N^2}$; $g=\alpha^2 \bmod N^2$

If $ord(g) \neq |\mathcal{QR}_{N^2}|$ (i.e., one of $g^{p'qq'}$, $g^{pqq'}$, $g^{pp'q'}$, $g^{pp'q}$ equals 1 mod N^2):

repeat the process of $\alpha \leftarrow \mathbb{Z}^*_{N^2}$, until $ord(g)=|\mathcal{QR}_{N^2}|$

For $1 \leqslant i \leqslant k$:

$x_i \leftarrow [|\mathcal{QR}_{N^2}|]$

If $\gcd(x_i,|\mathcal{QR}_{N^2}|) \neq 1$:

repeat the process of $x_i \leftarrow [|\mathcal{QR}_{N^2}|]$, until $\gcd(x_i,|\mathcal{QR}_{N^2}|)=1$

$X_i = g^{x_i} \bmod N^2$

$pp=(N,g,(X_i)_{i\in[k]})$

Return pp

$Gen^{cpa}(pp)$:

$b_1,...,b_{k+1} \leftarrow [|\mathcal{QR}_{N^2}|]$

For $1 \leqslant i \leqslant k: h_i = X_i^{b_i} g^{b_{k+1}} \bmod N^2$

$pk=(h_1,\ldots,h_k)$; $sk=(b_1,\ldots,b_{k+1})$

Return (pk,sk)

$Enc^{cpa}(pp,pk,m)$:

$r_1,...,r_k \leftarrow \mathbb{Z}_{N^2}$; $c_1 = X_1^{r_1} \bmod N^2$;...;$c_k = X_k^{r_k} \bmod N^2$

$c_{k+1} = \prod_{i=1}^{k} g^{r_i} \bmod N^2$; $c_{k+2} = \prod_{i=1}^{k} h_i^{r_i}(1+mN) \bmod N^2$

Return $c=(c_1,\ldots,c_{k+2})$

$Dec^{cpa}(pp,sk,c=(c_1,\ldots,c_{k+2}))$:

$u = \frac{c_{k+2}}{\prod_{i=1}^{k+1} c_i^{b_i}} \bmod N^2$; $\tilde{m} = \frac{u-1 \bmod N^2}{N}$

Return $\tilde{m}$

图 4 公钥加密方案 PKE_{add}^{cpa}

PKE_{add}^{cpa} 是在 $\mathbb{Z}^*_{N^2}$ 上的 k-Lin 假设下证明的 IND-CPA 安全性, 所以与第 3.4.1 节的分析类似, 可以通过对参数 k 的调控来调整 PKE_{add}^{cpa} 的 IND-CPA 安全性强度. 而且对任意 $0<k_0<k_1$, PKE_{add}^{cpa} 也都能够很便利地由 k_0-级别的 IND-CPA 安全性强度提升为 k_1-级别的 IND-CPA 安全性强度, 即可以仿照图 2 提出类似的转化算法. 具体细节这里也不再重复.

此外, PKE_{add}^{cpa} 同样也具有双解密机制. 具体来说, PKE_{add}^{cpa} 的 $Setup^{cpa}$ 算法在运行过程中也生成了两个素数 p 和 q. 于是, 记陷门 $td=(p,q)$, 我们可以构造关于 PKE_{add}^{cpa} 的一个新的解密算法 $MDec^{cpa}$ 如图 5 所示(其中, 该算法所调用的 $Comp_{DL}$ 见第 3.4.2 节).

$MDec^{cpa}(pp,td,pk,c=(c_1,\ldots,c_{k+2}))$:

Parse $pp=(N,g,(X_i)_{i\in[k]})$, $td=(p,q)$, $pk=(h_1,\ldots,h_k)$

$p'=\frac{p-1}{2}$; $q'=\frac{q-1}{2}$; $\omega=(2p'q')^{-1} \bmod N$

For $0 \leqslant i \leqslant k$:

$\hat{r}_i = Comp_{DL}(N,X_i,c_i)$

$u = \left(\frac{c_{k+2}}{\prod_{i=1}^{k} h_i^{\hat{r}_i}}\right)^{2p'q'} \bmod N^2$

Return $\tilde{m} = \frac{u-1 \bmod N^2}{N}\omega \bmod N$

图 5 PKE_{add}^{cpa} 的另一个解密算法 $MDec^{cpa}$

4 总 结

我们从区块链的数据隐私安全需求和现实应用需求角度出发, 提出了一个在 $\mathbb{Z}_{N^2}^*$ 上的判定性 k-Lin 假设下满足 IND-CCA1 安全性的加法同态加密方案. 我们的方案具有 3 个重要优势: (1) 可以通过对参数 k 的调控, 细粒度地调节其 IND-CCA1 安全性强度; (2) 具有双解密机制, 所以该方案部署在区块链应用场景中, 能够有效减轻监管方的密钥管理成本和压力; (3) 能够便利地退化为 IND-CPA 安全的加法同态加密方案, 以适应某些对传输数据长度和计算效率要求较高而安全性要求相对不那么高的应用场景, 而且退化后的方案依然具有双解密机制.

References:

[1] Satoshi N. Bitcoin: A peer-to-peer electronic cash system. 2008. https://bitcoin.org/bitcoin.pdf

[2] Ronald LR, Len A, Michael LD. On data banks and privacy homomorphisms. Foundations of Secure Computation, 1978, 4(11): 169−180.

[3] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978, 21(2): 120−126.

[4] Paillier P. Public-key cryptosystems based on composite degree residuosity classes. In: Stern J, ed. Proc. of the Advances in Cryptology (EUROCRYPT'99). Berlin: Springer, 1999. 223−238.

[5] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. on Information Theory, 1985, 31(4): 469−472.

[6] Boneh D, Goh EJ, Nissim K. Evaluating 2-DNF formulas on ciphertexts. In: Kilian J, ed. Proc. of the Theory of Cryptography (TCC 2005). Berlin: Springer, 2005. 325−341.

[7] Gentry C. Fully homomorphic encryption using ideal lattices. In: Proc. of the 41st Annual ACM Symp. on Theory of Computing (STOC 2009). New York: ACM, 2009. 169−178.

[8] Smart NP, Vercauteren F. Fully homomorphic encryption with relatively small key and ciphertext sizes. In: Nguyen PQ, Pointcheval D, eds. Proc. of the Public Key Cryptography (PKC 2010). Berlin: Springer, 2010. 420−443.

[9] Brakerski Z, Vaikuntanathan V. Fully homomorphic encryption from ring-LWE and security for key dependent messages. In: Rogaway P, ed. Proc. of the Advances in Cryptology (CRYPTO 2011). Berlin: Springer, 2011. 505−524.

[10] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping. ACM Trans. on Computation Theory (TOCT), 2014, 6(3): 1−36.

[11] Gentry C, Halevi S, Smart NP. Better bootstrapping in fully homomorphic encryption. In: Fischlin M, Buchmann J, Manulis M, eds. Proc. of the Public Key Cryptography (PKC 2012). Berlin: Springer, 2012. 1−16.

[12] Nuida K, Kurosawa K. (Batch) fully homomorphic encryption over integers for non-binary message spaces. In: Oswald E, Fischlin M, eds. Proc. of the Advances in Cryptology (EUROCRYPT 2015). Berlin: Springer, 2015. 537−555.

[13] Lai J, Deng RH, Ma C, Sakurai K, Weng J. CCA-secure keyed-fully homomorphic encryption. In: Cheng CM, Chung KM, Persiano G, Yang BY, eds. Proc. of the Public-key Cryptography (PKC 2016). Berlin: Springer, 2016. 70−98.

[14] Canetti R, Raghuraman S, Richelson S, Vaikuntanathan V. Chosen-ciphertext secure fully homomorphic encryption. In: Fehr S, ed. Proc. of the Public-key Cryptography (PKC 2017). Berlin: Springer, 2017. 213−240.

[15] Yu QF, Tu GS, Li NB, Zhou TP. Multi-hop multi-policy attributed-based fully homomorphic encryption scheme. Journal of Computer Applications, 2019, 39(8): 2326−2332 (in Chinese with English abstract).

[16] Brakerski Z, Dttling N, Garg S, Malavolta G. Leveraging linear decryption: Rate-1 fully-homomorphic encryption and time-lock puzzles. In: Hofheinz D, Rosen A, eds. Proc. of the Theory of Cryptography (TCC 2019). Berlin: Springer, 2019. 407−437.

[17] Li NB, Zhou TP, Che XL, Yang XY, Han YL. Overview on multi-key fully homomorphic encryption. Journal of Cryptologic Research, 2020, 7(6): 713−734 (in Chinese with English abstract).

[18] Tang CM, Hu YZ, Li XX. Three round secure multiparty computation based on multi-key full-homomorphic encryption without CRS. Journal of Cryptologic Research, 2021, 8(2): 273−281 (in Chinese with English abstract).

[19] Chillotti I, Gama N, Georgieva M, Izabachène M. TFHE: Fast fully homomorphic encryption over the torus. Journal of Cryptology, 2020, 33: 34−91.

[20] Bresson E, Catalano D, Pointcheval D. A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications. In: Laih CS, ed. Proc. of the Advances in Cryptology (ASIACRYPT 2003). Berlin: Springer, 2003. 37−54.

[21] Youn TY, Park YH, Kim CH, Lim J. An efficient public key cryptosystem with a privacy enhanced double decryption mechanism. In: Preneel B, Tavares S, eds. Proc. of the Selected Areas in Cryptography (SAC 2005). Berlin: Springer, 2005. 144−158.

[22] Hofheinz D, Kiltz E. Secure hybrid encryption from weakened key encapsulation. In: Menezes A, ed. Proc. of the Advances in Cryptology (CRYPTO 2007). Berlin: Springer, 2007. 553−571.

[23] Shacham H. A cramer-shoup encryption scheme from the linear assumption and from progressively weaker linear variants. Cryptology ePrint Archive: Report 2007/074, 2007.

[24] Boneh D, Silverberg A. Applications of multilinear forms to cryptography. In: Melles CG, Brasselet JP, Kennedy G, Lauter K, McEwan L, eds. Proc. of the Topics in Algebraic and Noncommutative Geometry: Proc. in Memory of Ruth Michler, Vol.324 of Contemporary Mathematics. American Mathematical Society, 2003. 71−90.

附中文参考文献:

[15] 余卿斐, 涂广升, 李宁波, 周潭平. 多跳多策略属性基全同态加密方案. 计算机应用, 2019, 39(8): 2326−2332.

[17] 李宁波, 周潭平, 车小亮, 杨晓元, 韩益亮. 多密钥全同态加密研究. 密码学报, 2020, 7(6): 713−734.

[18] 唐春明, 胡业周, 李习习. 基于多密钥全同态加密方案的无 CRS 模型安全多方计算. 密码学报, 2021, 8(2): 273−281.

附录 A: 定理 1 的证明

在给出定理 1 的正式证明之前, 我们考虑如下两个引理. 这两个引理可视为 Lemma B.1&B.2[23]的变体.

记 G_T 是一个阶为 $|\mathcal{QR}_{N^2}|=pp'qq'$ 的循环群. $e_k:\mathcal{QR}_{N^2}^k\to G_T$ 称为 $\mathcal{QR}_{N^2}^k$ 上的一个 k 级多线性映射[24], 当且仅当其满足以下两个条件.

(1) 对任意 $u_1,...,u_k\in\mathcal{QR}_{N^2}$ 和任意 $a_1,...,a_k\in[|\mathcal{QR}_{N^2}|]$, 有 $e_k(u_1^{a_1},...,u_k^{a_k})=e_k(u_1,...,u_k)^{\prod_{i=1}^k a_i}$;

(2) 映射 e_k 非退化, 即当 $u_1,\ldots,u_k$ 均为 $\mathcal{QR}_{N^2}$ 的生成元时, $e_k(u_1,\ldots,u_k)$是 G_T 的生成元.

引理 2. 假设存在 $\mathcal{QR}_{N^2}^k$ 上的一个 k+1 级多线性映射 e_{k+1}, 则 $\mathbb{Z}_{N^2}^*$ 上的 k-Lin 假设不成立.

引理 3. 在通用群模型(generic group model)下, 对于一个攻击 $\mathbb{Z}_{N^2}^*$ 上的 k+1-Lin 假设的敌手 A, 如果 A 最多只能询问 q 次预言机, 则 A 的成功概率最多只有 $\frac{(k+1)(q+2k+6)^2}{pp'qq'}$.

引理 2、引理 3 的证明分别与文献[23]的 Lemma B.1、Lemma B.2 的证明类似, 所以这里就不再重复了.

下面我们给出定理 1 的正式证明.

证明: 首先, 我们证明当 $\mathbb{Z}_{N^2}^*$ 上的 DDH 假设成立时, $\mathbb{Z}_{N^2}^*$ 上的 1-Lin 假设(即 k=1)也成立.

对任意一个针对 $\mathbb{Z}_{N^2}^*$ 上 1-Lin 问题的敌手 A, 我们构造一个针对 $\mathbb{Z}_{N^2}^*$ 上的 DDH 问题的敌手 B 如下: B 收到(N,g,X,Y,Z)后, 令 $\tilde{g}=X$, $\tilde{X}_1=g$, $\tilde{T}_1=Y$, $\tilde{Z}=Z$; 然后, B 将 $(N,\tilde{g},\tilde{X}_1,\tilde{T}_1,\tilde{Z})$ 发给 A; 最后, B 把 A 的返回值 b'作为自己的最终输出值.

下面我们计算 B 的优势.

对于 B 的输入(N,g,X,Y,Z), 记 $X=g^x \bmod N^2$, $Y=g^y \bmod N^2$. 由于 x 是从 $[|\mathcal{QR}_{N^2}|]$ 中均匀随机选取的, 所以至少以 $1-\left(\frac{1}{p}+\frac{1}{p'}+\frac{1}{q}+\frac{1}{q'}\right)$ 的概率有 $\gcd(x,|\mathcal{QR}_{N^2}|)=1$(即 $x^{-1} \bmod |\mathcal{QR}_{N^2}|$存在).

当 $x^{-1} \bmod |\mathcal{QR}_{N^2}|$存在时, 有 $\tilde{X}_1=g=X^{x^{-1}}=\tilde{g}^{x^{-1}} \bmod N^2$, $\tilde{T}_1=Y=g^y=(\tilde{g}^{x^{-1}})^y=\tilde{g}^{x^{-1}y} \bmod N^2$.

记 $\tilde{X}_1=\tilde{g}^{\tilde{x}_1} \bmod N^2$, $\tilde{T}_1=\tilde{g}^{\tilde{x}_1\tilde{y}_1} \bmod N^2$, 则默认有 $\tilde{x}_1=x^{-1} \bmod |\mathcal{QR}_{N^2}|$, $\tilde{y}_1=y \bmod |\mathcal{QR}_{N^2}|$. 这种情况

下，若 $Z=g^{xy} \bmod N^2$，则 $\tilde{Z}=Z=(g^x)^y=\tilde{g}^{\tilde{y}_1} \bmod N^2$；若 $Z=g^z \bmod N^2$，则 $\tilde{Z}=Z=g^z=\tilde{g}^{\tilde{z}} \bmod N^2$，其中，$\tilde{z}=x^{-1}z \bmod |\mathcal{QR}_{N^2}|$服从均匀分布.

所以，当 $x^{-1} \bmod |\mathcal{QR}_{N^2}|$存在时，$B$ 完美地给 A 模拟了 $\boldsymbol{Exp}_A^{1\text{-}Lin}(\kappa)$ 的环境，B 攻击成功当且仅当 A 攻击成功. 于是:

$$\boldsymbol{Adv}_B^{DDH}(\kappa) \geqslant \left(1-\left(\frac{1}{p}+\frac{1}{p'}+\frac{1}{q}+\frac{1}{q'}\right)\right)\boldsymbol{Adv}_A^{1\text{-}Lin}(\kappa).$$

接着，我们证明: 当 $\mathbb{Z}_{N^2}^*$ 上的 k-Lin 假设成立时，$\mathbb{Z}_{N^2}^*$ 上的$(k+1)$-Lin 假设也成立.

对任意一个针对 $\mathbb{Z}_{N^2}^*$ 上$(k+1)$-Lin 问题的敌手 B_{k+1}，我们构造一个针对 $\mathbb{Z}_{N^2}^*$ 上的 k-Lin 问题的敌手 B_k 如下.

- B_k 收到$(N,g,X_1,\ldots,X_k,T_1,\ldots,T_k,Z)$后，自行选取 $x_{k+1},y_{k+1} \leftarrow [|\mathcal{QR}_{N^2}|]$，并计算:

$$X_{k+1}=g^{x_{k+1}} \bmod N^2,\ T_{k+1}=g^{x_{k+1}y_{k+1}} \bmod N^2 \text{和} \tilde{Z}=Z\cdot g^{y_{k+1}} \bmod N^2;$$

- 接着，B_k 把 $(N,g,X_1,\ldots,X_k,X_{k+1},T_1,\ldots,T_k,T_{k+1},\tilde{Z})$ 发给 B_{k+1};
- 最后，B_k 从 B_{k+1} 处收到 b'，便将 b'作为自己的最终输出值.

显然，B_k 完美地为 B_{k+1} 模拟了 $\boldsymbol{Exp}_{B_{k+1}}^{(k+1)\text{-}Lin}(\kappa)$ 的环境，而且 B_k 攻击成功当且仅当 B_{k+1} 攻击成功. 所以:

$$\boldsymbol{Adv}_{B_k}^{k\text{-}Lin}(\kappa)=\boldsymbol{Adv}_{B_{k+1}}^{(k+1)\text{-}Lin}(\kappa).$$

最后，由引理 2 和引理 3 可知: 在通用群模型下，即使 $\mathbb{Z}_{N^2}^*$ 上的$(k+1)$-Lin 假设成立，$\mathbb{Z}_{N^2}^*$ 上的 k-Lin 假设也不一定成立. 由此可知: k 越大，$\mathbb{Z}_{N^2}^*$ 上的 k-Lin 假设就越弱. □

赖俊祚(1981－)，男，博士，教授，主要研究领域为密码学，信息安全.

翁健(1976－)，男，博士，教授，CCF 专业会员，主要研究领域为密码学，信息安全.

黄正安(1986－)，男，博士，助理研究员，主要研究领域为密码学，信息安全.

吴永东(1970－)，男，博士，教授，CCF 专业会员，主要研究领域为区块链，网络系统安全，物联网安全，信息安全.