

基于新“0”测试参数的理想格上多线性映射

古春生^{1),2)} 景征骏¹⁾ 史培中¹⁾ 于志敏¹⁾

¹⁾(江苏理工学院计算机工程学院 江苏 常州 213001)

²⁾(中国科学院信息工程研究所信息安全国家重点实验室 北京 100093)

摘要 密码学中的多线性映射具有广泛应用,包括多方密钥交换、广播加密、基于身份的加密、基于属性的加密、不可区分模糊器和函数加密等.虽然多线性映射存在无限应用的可能,但目前多线性映射构造方案仅有三个——GGH13、CLT13 和 GGH15,且它们都存在“0”化攻击、新的难度假设和可信安装的安全问题.针对第一个多线性映射候选构造方案 GGH13, Hu 和 Jia 最近基于“0”化攻击提出了攻击 GGH13 构造的多项式时间算法,完全破解了基于 GGH13 映射的两个重要应用——多方密钥交换协议(MPKE)和使用 3-精确覆盖问题的证据加密方案(WE).本文主要改进理想格上的 GGH13 构造方案,以解决其存在的“0”化攻击和可信安装的安全问题.首先,为避免“0”化攻击问题,作者通过设计新的“0”测试参数提出基于新随机化方法的多线性映射构造,其安全性基于新的困难问题假设——ext-GDDH/ext-GCDH;其次,为去除可信安装问题,作者使用中国剩余定理提出无可信安装的理想格上多线性映射构造,其安全性基于新的困难问题假设——wots-ext-GCDH/wots-ext-GDDH;最后,作者给出基于改进多线性映射构造的多方密钥交换协议 nr-MPKE 和 wots-MPKE.

关键词 多线性映射;“0”化攻击;可信安装;多方密钥交换;证据加密

中图法分类号 TP309 **DOI号** 10.11897/SP.J.1016.2018.01068

New Zero-Test Parameter Based Multilinear Maps from Ideal Lattices

GU Chun-Sheng^{1),2)} JING Zheng-Jun¹⁾ SHI Pei-Zhong¹⁾ YU Zhi-Min¹⁾

¹⁾(School of Computer Engineering, Jiangsu University of Technology, Changzhou, Jiangsu 213001)

²⁾(State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093)

Abstract Cryptographic multilinear maps have found many applications, including multipartite key exchange, broadcast encryption, identity-based encryption, attribute-based encryption, indistinguishability obfuscation and function encryption. Although the multilinear map has unlimited possibilities of applications, currently only the GGH13, CLT13 and GGH15 constructions are known, and all have zeroizing attacks, new hardness assumptions and trusted setup. For the first candidate construction GGH13 of multilinear maps, Hu and Jia recently extended the zeroizing attack in GGH13 introduced by Garg, Gentry and Halevi, and presented a polynomial time algorithm, which completely breaks two important GGH13-based applications, i. e. multipartite key exchange and witness encryption using 3-exact cover problem. This paper mainly improves the GGH13 construction from ideal lattices to solve its security issues of zeroizing attacks and trusted setup. First, in order to avoid the zeroizing attacks, we describe a new randomization construction of multilinear maps by designing new zero-test parameter. Different from the GGH13 construction, the public parameters in our construction do not contain encodings of zero, and only consists of some level-1 encodings of non-zero elements and their corresponding zero-test

收稿日期:2016-08-18;在线出版日期:2017-07-04. 本课题得到国家自然科学基金(61672270, 61602216)、教育部人文社会科学研究项目(14YJAZH023, 15YJCZH129)、中国科学院信息安全国家重点实验室开放课题面上项目(2015-MSB-10)、江苏省“青蓝工程”中青年学术带头人项目(KYQ14004)、江苏省高校优秀中青年教师和校长境外研修计划、常州市应用基础研究指导性项目(2016365)资助. 古春生,男,1971年生,博士,教授,中国计算机学会(CCF)会员,主要研究领域为基于格的密码学和密码分析. E-mail: chunsheng_gu@163.com. 景征骏,男,1978年生,博士,副教授,主要研究方向为公钥密码学和密码分析. 史培中,男,1982年生,博士,讲师,主要研究方向为网络安全和协议安全分析. 于志敏,男,1973年生,硕士,讲师,主要研究方向为公钥密码学和密码分析.

parameters. That is, essentially the new zero-test parameters are the product of the level-0 encoding of non-zero elements with the zero-test parameter in the origin GGH13 scheme. At present, the security of our construction only depends upon the new hardness assumptions ext-GDDH/ext-GCDH, and cannot reduce to other classical hardness problems. Furthermore, to analyze the security of our construction, we have proved that it can prevent the currently known attacks, i. e. the attacks of easily computable quantities, the attacks based on the low-level encodings of zeros or non-zeros. To further enhance the security and avoid potential attacks, we use the Kilian randomized matrix method and the NTRU prime field as the countermeasures, respectively. In addition, we theoretically prove that any noise-based construction of multilinear maps cannot completely avoid the zeroizing attacks. Second, in order to remove the trusted setup, we describe a construction without trusted setup of multilinear maps using ideal lattices by applying Chinese remainder theorem. In this construction, each participant first uses the new randomization construction as the basic building block to generate and publish her/his own public parameters. Then, each participant combines the public parameters of all parties by applying Chinese remainder theorem to generate the common public parameters shared by the parties. Finally, each participant adaptively generates all other algorithms of a graded encoding scheme under the common public parameters to obtain the construction without trusted setup. Similarly, the security of our construction without trusted setup only relies on the new hardness assumptions wots-ext-GCDH/wots-ext-GDDH, and cannot reduce to other classic hardness problems. Moreover, to analyze the security of the construction without trusted setup, we have proved that it can resist the currently known attacks, including the attacks against the new randomization construction and the extension of Cheon et al.'s zeroizing attacks. Third, we present the multipartite key exchange protocols nr-MPKE and wots-MPKE based on our improvement constructions of multilinear maps, respectively. The security of the nr-MPKE (resp. wots-MPKE) protocol relies on the hardness assumptions ext-GCDH/ext-GDDH (resp. wots-ext-GCDH/wots-ext-GDDH).

Keywords multilinear maps; zeroizing attack; trusted setup; multipartite key exchange; witness encryption

1 引言

1.1 问题提出

多线性映射^[1]是一种新的密码原语,在密码学中有大量应用.最简单的双线性映射能够用于构造非交互式密钥交换协议(Non-interactive Key Exchange Protocol)^[2]、三方 Diffie-Hellman 密钥交换协议(Tripartite Key Exchange Protocol)^[3]、基于身份加密(Identity-based Encryption)^[4-5]和基于属性加密(Attribute-based Encryption)^[6]、广播加密(Broadcast Encryption)^[7]等.对于多线性映射,在其构造方案出现前,人们已经开始研究其在密码学中的应用^[1,8-10].在多线性映射构造方案^[11-12]研究取得突破后,多线性映射的应用范围进一步扩大,如证据加密(Witness Encryption, WE)、不可区分模糊器(Indistinguishability Obfuscation, IO)和函数加

密(Function Encryption, FE)等^[13-18].因此,随着多线性映射在密码学中的应用范围不断扩大,作为应用基础的构造方案将越来越重要.

目前多线性映射构造方案仅有三个——基于理想格的 GGH13 构造、基于中国剩余定理的整数上 CLT13 构造和基于图导出的格上 GGH15 构造.但是,这些构造都存在安全问题.

(1) GGH13 构造

Garg, Gentry 和 Halevi^[11]提出了第一个基于理想格的近似多线性映射 GGH13 构造,其安全性依赖于新的问题难度假设 GDDH/GCDH (Graded Decisional/Computational Diffie-Hellman),目前并不能将其安全归约到经典困难问题 Ring-LWE^[19]或 NTRU^[20].这是由于 GGH13 构造的公共参数中包含的“0”测试参数实际上是有缺陷的私钥.同时,GGH13 构造在生成公共参数时使用了秘密元素,导致该构造需要可信安装;而且 GGH13 构造产生

编码时需要对编码进行再随机化,故公共参数中需要包含一些“0”元素的 1-级编码,导致该构造方案存在“0”化攻击问题.最近,Langlois,Stehlé 和 Steinfeld^[21]给出了 GGH13 构造的变种 GGHLite.虽然 GGHLite 改进了 GGH13 的再随机化过程的安全分析,提高了 GGH13 的效率,但该变种仅减少了 GGH13 的公共参数大小,并没有改变 GGH13 的构造结构.因此,变种 GGHLite 仍然存在 GGH13 构造同样的安全问题.

目前,攻击 GGH13 构造的方法主要有两类:

① 需要“0”元素的低级编码的攻击^[11,22-24].

Garg,Gentry 和 Halevi^[11]首先给出基于“0”化攻击(也称为弱离散对数攻击,Weak-DL Attack)计算求解 GGH13 构造的秘密理想元素的格基.随后,Hu 和 Jia^[22]通过扩展“0”化攻击,提出了针对 GGH13 构造的多项式时间攻击算法,完全破解了基于 GGH13 构造的两个重要应用——多方密钥交换协议 MPKE(MultiPartite Key Exchange)^[11]和使用 3-精确覆盖问题的证据加密方案 WE^[13].同时,Hu 和 Jia 还证明了安全难度假设 κ -GMDDH (κ -Graded Multilinear Decisional Diffie-Hellman Assumption) 为假,而该难度假设是 Garg 等人^[14]构造的属性基电路加密方案的安全基础.最近,为避免“0”化攻击问题,Halevi^[25]构造了 GGH13 的一个新变种(简记为 GHL15),该变种使用二次(或更高次数)的“0”测试参数多项式替换原方案中的线性“0”测试参数多项式.然而,Brakerski 等人^[24]通过对变种 GHL15 的高次“0”测试参数多项式“求导”,计算得到线性“0”测试参数多项式,并将其转换为 GGH13 构造的“0”测试参数,结果导致该变种仍然存在 GGH13 构造同样的“0”化攻击问题.

② 不需要“0”元素的低级编码的攻击^[26-29].其一,子域格攻击.由于两个非“0”的 1-级编码的商会产生一个 NTRU 型问题实例,Albrecht,Bai 和 Ducas^[26]通过使用数域中范数的方法将 NTRU 型实例从全域映射到子域,从而产生更易求解的 NTRU 型格问题.而 Cheon,Jeong 和 Lee^[27]则通过数域中迹的方法将 NTRU 型实例从全域映射到子域.对于无“0”编码的 GGH13 构造,这两种子域格攻击方法都产生了一个量子多项式时间破解算法和一个经典的次指数时间攻击算法.其二,Cheon 等人的“0”化攻击方法扩展.虽然 GGH13 变种^[30]的公共参数中并没有直接包含“0”的低级编码,但其公共参数中每个非“0”元素的编码出现在每条不同路径上.这导致 Coron 等人^[28]基于 Cheon 等人的“0”化攻击方法^[31]扩展,提出了计算秘密理想元素格基

的多项式时间攻击算法.其三,零化多项式攻击(Annihilation Polynomial Attack):Miles,Sahai 和 Zhandry^[29]使用零化多项式方法攻击了基于 GGH13 的不可区分模糊器 IO^[32-33].Miles,Sahai 和 Zhandry 利用模糊器 IO 变换后的分支程序(Branching Program,BP),在计算结果为“0”时返回的元素集上构造出零化多项式,并进而计算获得秘密理想元素的格基,从而破解了基于 GGH13 的模糊器 IO.最近,Chen,Gentry 和 Halevi^[34]利用分支程序的特殊结构——输入可分性,扩展了零化多项式攻击到基于 GGH13 的 GGHRSW 模糊器 IO^[15].

(2) CLT13 构造

跟随 GGH13 构造的框架,Coron,Lepoint 和 Tibouchi^[12]使用中国剩余定理构造了整数上多线性映射 CLT13,其安全性依赖于新的问题难度假设 GDDH/GCDH.虽然 CLT13 的编码在形式上与整数环中近似 GCD 问题(Approximate Greatest Common Divisor, AGCD)类似,但目前并不能将 CLT13 的安全归约到近似 GCD 问题.这是因为 CLT13 的公共参数中不仅包含了整数近似 GCD 的抽样、0-级编码和许多特殊的近似 GCD 的抽样以及 1-级编码(即在整数模上近似 GCD 的抽样除以随机整数),而且也包含了有缺陷的私钥,即“0”测试参数.同时,CLT13 构造在产生公共参数时使用的素数因子需要保密,导致该构造同样需要可信安装.虽然 Coron,Lepoint 和 Tibouchi^[12]在对 CLT13 进行安全分析时认为 CLT13 不存在“0”化攻击问题,但是 Cheon 等人^[31]使用扩展的“0”化攻击已经完全破解了 CLT13 构造.为了修复 CLT13 构造,Garg 等人^[35]和 Boneh,Wu 和 Zimmerman^[36]分别提出了 CLT13 构造的改进方案.然而,Coron 等人^[23]证明使用 Cheon 等人的“0”化攻击方法^[31]扩展同样能够破解这些改进方案.随后,Coron,Lepoint 和 Tibouchi^[37]通过设计新的“0”测试参数方法提供了 CLT13 构造的一个新变种(简记为 CLT15).但是,最近 Cheon 等人^[38]使用攻击 CLT13 构造^[31]的类似方法,完全破解了 CLT15 构造,即该变种仍然存在“0”化攻击问题.

(3) GGH15 构造

Gentry,Gorbunov 和 Halevi^[39]使用近似特征向量方法^[40]提出了基于图导出的格上多线性映射 GGH15 构造.虽然 GGH15 构造的安全性依赖于 LWE(Learning with Error)困难问题^[41],但目前并不能将其归约到 LWE 问题难度.这是因为格上 GGH15 构造的公共参数不仅包含了 LWE 问题的实例,而且还包含了图,并由图中结点和路径决定了

公共参数中的LWE实例. 类似地, 格上GGH15构造的公共参数产生时使用的陷门也需要保密, 导致该构造也需要可信安装; 而且该构造中“0”的编码是弱陷门, 导致其公共参数中不能提供“0”的编码. 格上GGH15构造的优点是其安全性相关于LWE问题的计算难度, 即与格问题的计算难度相关; 缺点是构造由图导出, 其安全性不易分析和证明, 并且即使格上GGH15构造工作在多项式环上, 其效率也比理想格上GGH13构造的效率更低. 不幸的是, GGH15构造同样存在安全问题, 最近基于GGH15构造的多方密钥交换协议MPKE已经被破解^[28]. GGH15构造被破解的原因在于其公共参数中图的每个路径上都包含相同明文元素的编码, 只是相同明文编码在每个路径上的结点次序不同.

综上所述, 现有多线性映射构造都被破解, 特别是基于这些构造的多方密钥交换协议MPKE. 这就提出了下面的公开问题:

- (1) 现有多线性映射构造能否改造成抗“0”化攻击的安全方案?
- (2) 现有构造方案能否改造成无可信安装的多线性映射?

本文研究肯定地回答了上述问题. 由于本文主要改进理想格上的GGH13构造, 下面先概述GGH13构造, 然后给出本文主要贡献.

1.2 GGH13构造概述

GGH13构造工作在多项式环 $R = \mathbb{Z}[x]/\langle x^n + 1 \rangle$ 和 $R_q = R/qR$ 上. GGH13构造首先选择秘密的“短”元素 $\mathbf{g} \in R$ (例如 $\mathbf{g}$ 的无穷大范数 $\|\mathbf{g}\|_\infty \leq n^{1.5}$) 和秘密随机元素 $\mathbf{z} \in R_q$. 明文编码是 R/I 的陪集, 其中 $I = \langle \mathbf{g} \rangle$ 为元素 $\mathbf{g}$ 生成的主理想格. 为产生陪集 $e_I = \mathbf{e} + I$ 的编码, 使用该陪集的任一“短”的代表元素 $\mathbf{c}$ (例如 $\mathbf{c}$ 的无穷大范数 $\|\mathbf{c}\|_\infty \leq n^2$), 在 R_q 中计算产生元素 $[\mathbf{c}/\mathbf{z}]_q$ 作为陪集 e_I 的编码. 由于GGH13构造中元素 $\mathbf{g}, \mathbf{z}$ 是隐藏的秘密元素, 导致构造的使用者无法直接产生上述形式的编码. 为解决编码产生问题, GGH13构造在其公共参数中提供了元素“1” (即陪集 $1 + I$ 的编码 $\mathbf{y} = [(1 + \mathbf{a} \cdot \mathbf{g})/\mathbf{z}]_q$). 因此, 陪集 e_I 的编码计算为 $[\mathbf{e} \cdot \mathbf{y}]_q$. 又因为编码中使用了秘密元素 $\mathbf{z}$, 所以GGH13构造是一个分级编码方案. GGH13构造以分母 $\mathbf{z}$ 的次数作为编码级数, 即明文元素 $\mathbf{e}$ 是陪集 e_I 的0-级编码, 元素 $[\mathbf{e} \cdot \mathbf{y}]_q$ 为陪集 e_I 的1-级编码, 元素 $[\mathbf{e} \cdot \mathbf{y}^i]_q$ 是陪集 e_I 的*i*-级编码. 易于验证, 这些分级编码能够进行限定次数的加法和乘法的同态计算. 实际上, 两个*i*-级编码的和仍为一个*i*-级编码; *i*个1-级编码的乘积将产生一个*i*-级编码, 并且一个 κ -级编码方案能够将不大于 κ 的任

意数量的编码进行相乘. 为判定一个 κ -级编码是否为“0”元素的编码, GGH13构造的公共参数中提供了“0”测试参数 $\mathbf{p}_{zt} = [\mathbf{h}\mathbf{z}^\kappa/\mathbf{g}]_q$. 如果给定一个 κ -级编码 $\mathbf{u} = [\mathbf{c}/\mathbf{z}^\kappa]_q$, 则由 $\mathbf{v} = [\mathbf{p}_{zt} \cdot \mathbf{u}]_q$ 的无穷大范数大小能够判定 $\mathbf{u}$ 是否为“0”元素的 κ -级编码. 如果 $\mathbf{v}$ 的无穷大范数 $\|\mathbf{v}\|_\infty$ 远小于 q , 则 $\mathbf{u}$ 是“0”元素的 κ -级编码, 否则 $\mathbf{u}$ 是非“0”元素的 κ -级编码. 因此, 对于非“0”元素的编码, $\mathbf{v}$ 中每个系数的最有意义的比特位仅依赖于陪集 e_I , 而与陪集中的具体代表元素无关. 所以, 对于一个 κ -级编码, 这就实现了仅依赖于陪集 e_I 的比特提取函数. 上述即定义了理想格上分级编码的GGH13构造.

GGH13构造需要再随机化. 如果给定元素 $\mathbf{e}$ 的1-级编码 $\mathbf{u}' = [\mathbf{e} \cdot \mathbf{y}]_q$, 则攻击者通过将 $\mathbf{u}'$ 除以 $\mathbf{y}$ 能够有效恢复 $\mathbf{u}'$ 中包含的0-级编码元素 $\mathbf{e}$. 为防止这种简单除法攻击, GGH13构造引入了编码的再随机化方法. 所谓再随机化方法, 是指在公共参数中包含一些“0”元素 (即陪集 $0 + I$) 的1-级编码 $\mathbf{x}_j = [\mathbf{s}_j \mathbf{g}/\mathbf{z}]_q$, 并且通过使用1-级编码 $\mathbf{x}_j$ 的线性组合来实现1-级编码的再随机化. 例如对编码 $\mathbf{u}'$ 使用再随机化方法, 则将 $\mathbf{u}'$ 变换为1-级编码 $\mathbf{u} = [\mathbf{u}' + \sum_j \beta_j \mathbf{x}_j]_q$, 其中 β_j 是 $\mathbb{Z}$ 上的标准差为 $\sigma_1^* = 2^\lambda$ 的离散高斯抽样, λ 为安全参数. 虽然这种再随机化方法产生的编码 $\mathbf{u}$ 的分布与原始编码 $\mathbf{u}'$ 的分布具有统计相关性 (因为分布 $\sum_j \beta_j \mathbf{s}_j$ 是以0为中心的), 但通过设置较大的再随机化参数 σ_1^* 可以阻止这种统计相关性攻击^[14], 然而增大 σ_1^* 将降低构造方案的效率. 为提高GGH13构造的效率, Langlois, Stehlé和Steinfeld^[21]使用Rényi扩散 (Rényi Divergence, RD) 和多项式环上剩余Hash引理, 将GGH13的公共参数大小从 $O(\kappa^3 \lambda^5 \log(\kappa \lambda))$ 减少到 $O(\kappa^3 \lambda \log^2(\kappa \lambda))$, 其中 λ 为安全参数, κ 为多线性映射次数. 虽然GGH13构造使用再随机化方法避免了简单除法攻击, 但在公共参数中包含“0”元素的1-级编码却导致GGH13构造产生了“0”化攻击问题^[11, 22]. 因此, GGH13构造需要再随机化方法既是其低效的一个主要因素, 也是导致基于GGH13构造的应用MPKE和WE被破解的主要原因.

GGH13构造需要可信安装. 由于GGH13构造存在需要保密的秘密元素, 所以GGH13构造的初始化阶段需要存在可信中心以产生方案的初始化参数, 可信中心对初始化算法中选择和使用的秘密参数保密 (例如元素 $\mathbf{g}, \mathbf{z}$ 和产生公共参数时所使用的其它随机参数等), 仅仅发布构造方案初始化算法产生的公共参数. 这种可信安装要求不仅损害

GGH13 构造的安全性,而且在网络环境下有时无法获得一个可信中心.

1.3 本文贡献

本文主要研究理想格上 GGH13 构造方案中存在的安全问题——“0”化攻击和可信安装问题. 针对“0”化攻击问题,本文通过设计新的“0”测试参数构造无“0”编码的多线性映射;针对可信安装问题,本文使用中国剩余定理构造无可信安装的多线性映射. 因此,本文将通过改进理想格上 GGH13 构造,以解决其存在的两个安全问题.

本文贡献主要有以下 3 点:

(1) 基于新随机化方法构造了无“0”编码的多线性映射. 在构造 GGH13 时, Garg, Gentry 和 Halevi^[11] 将构造无“0”的 1-级编码的再随机化方法提出作为一个公开问题. 本文工作的出发点是公共参数中只提供非“0”元素的 1-级编码,关键是如何使用这些非“0”编码的线性组合产生的编码. 为此,我们通过重新设计 GGH13 构造中的“0”测试参数,使得新的“0”测试参数不仅用于“0”测试函数计算,而且也用于编码特殊的 0-级编码元素. 改进 GGH13 构造的基本思想是:公共参数中仅包含一些非“0”元素的 1-级编码和与其对应的新的“0”测试参数,即将该非“0”元素的 0-级编码与 GGH13 构造中的“0”测试参数乘积作为新的“0”测试参数. 新随机化的多线性映射构造的安全性依赖于新的难度假设问题——GCDH/GDDH 的提取变种 ext-GCDH/ext-GDDH 问题. 由于在新随机化构造中,公共参数中不再包含“0”元素的 1-级编码,从而避免了 GGH13 构造中的“0”化攻击问题.

(2) 基于中国剩余定理构造了无可信安装的多线性映射. 由于上述无“0”编码的 GGH13 改进仍然存在秘密元素需要保密,即上述改进构造还是需要可信中心产生公共参数. 本文研究的出发点是:如果使用多线性映射的所有参与方各自保存一部分秘密信息,使得参与方的任何子集都不能获得构造的全部秘密信息,则通过这种秘密信息分散保存的方式能够构造出无可信安装的多线性映射. 为此,我们通过中国剩余定理将各方使用上述新随机化构造产生的公共参数组合,以计算得到无可信安装构造的公共参数. 从构造方法角度看, CLT13 构造^[12]本质上是将多项式环上理想的 GGH13 构造扩展到整数环上理想的构造,并且为使构造安全,使用中国剩余定理将 n 个整数环上理想的构造组合在一起;而本文则是将中国剩余定理从整数环上直接扩展到多项式环上(具体扩展方法将在第 7.1 节给出),以构造无可信安装的多线性映射. 这种扩展不仅实现了无可

信安装构造,而且本文构造方案中模的素因子不再需要保密(具体构造方案将在第 7.2 节给出),解决了 CLT13 构造中模的素因子需要保密的问题. 无可信安装构造的基本思想是:首先,每个参与方使用新随机化构造的初始化算法产生各自的公共参数并发布;然后,每个参与方使用中国剩余定理将各方的公共参数组合在一起以产生所有方共用的公共参数;最后,各方自适应地产生无可信安装构造中的其它算法,以正确实现共用的公共参数环境下无可信安装的分级编码方案. 本文无可信安装构造的安全性也依赖于新的难度假设问题——GCDH/GDDH 的提取变种 wots-ext-GCDH/wots-ext-GDDH 问题. 由于构造方案产生公共参数时不再需要可信中心,从而去除了 GGH13 构造中的可信安装问题.

(3) 给出了基于新的多线性映射构造的多方密钥交换协议 nr-MPKE 和 wots-MPKE. 虽然 Hu 和 Jia^[22] 已经完全破解了基于 GGH13 的两个重要应用——MPKE 和 WE,但目前我们仅能构造出抗 Hu-Jia 攻击的 MPKE 协议. 这是因为 Hu 和 Jia^[22] 不仅破解了公开编码工具的 WE 方案,而且也破解了隐藏编码工具的 WE 方案. 所以,我们将构造避免 Hu-Jia 攻击的 WE 改进方案作为公开问题.

1.4 本文结构

第 2 节介绍本文研究相关的预备知识;第 3 节构造新随机化方法的多线性映射;第 4 节分析新随机化构造的已知攻击;第 5 节给出新随机化构造的安全假设;第 6 节构造无可信安装的多线性映射;第 7 节给出基于新的多线性映射的多方密钥交换协议 MPKE;第 8 节是结束语和公开问题. 附录 1 给出 GGH13 构造及其安全假设.

2 预备知识

2.1 符号

设 λ 为安全参数,符号 $\mathbb{Z}$ 、 $\mathbb{Q}$ 和 $\mathbb{R}$ 分别表示整数集、有理数集和实数集, q 为正整数, $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ 为整数环,符号 $[q]$ 表示元素集合 $\{1, 2, \dots, q\}$, 符号 $|q|$ 除表示 q 的绝对值外,也重载表示 q 的比特长度.

设 $n = 2^k$, k 为正整数. 设 $R = \mathbb{Z}[x]/\langle x^n + 1 \rangle$ 和 $R_q = R/qR$ 为多项式环, $\mathbb{K} = \mathbb{Q}[x]/\langle x^n + 1 \rangle$ 为数域.

我们使用小写黑体字母表示列向量(如 $\mathbf{a}$),大写黑体字母表示矩阵(如 $\mathbf{A}$). 向量或矩阵的转置使用上标符号 $\mathbf{T}$ 表示(如 $\mathbf{a}^{\mathbf{T}}$, $\mathbf{A}^{\mathbf{T}}$). 向量 $\mathbf{a}$ 的第 i 个坐标表示为 a_i . 多项式环 R 和 R_q 中的元素也用小写黑体字母. 向量 $\mathbf{a} \in \mathbb{R}^n$ 的欧几里德范数(也称为 l_2 范数)表示为 $\|\mathbf{a}\|_2$ (简记为 $\|\mathbf{a}\|$), 其无穷大范数表

示为 $\|a\|_\infty$.

设 $A \in \mathbb{R}^{m \times n}$ 是秩为 n 的矩阵, $U_A = \{\|Au\|_2 : u \in \mathbb{R}^n, \|u\|_2 = 1\}$, 则 A 的最小奇异值 (Least Singular Value) 为 $\sigma_n(A) = \inf(U_A)$, 最大奇异值 (Largest Singular Value) 为 $\sigma_1(A) = \sup(U_A)$.

符号 $[a]_q$ (或 $a \bmod q$) 表示整数 a 在模 q 下的值, 并且 $[a]_q \in (-q/2, q/2]$, 即本文使用模的绝对最小剩余系. 类似地, 符号 $[a]_q$ (或 $a \bmod q$) 表示向量 (或多项式环中的元素) 的每个分量 (或每个系数) 取值为 $[a_i]_q, i \in [n]$.

给定任意元素 $a \in R$, 符号 $MSB_l(a) \in \{0, 1\}^{l \times n}$ 表示从 a 的每个系数中提取 l 个最有意义的比特位 (Most Significant Bits, MSB).

本文使用标准渐近符号 $O(\cdot), \Omega(\cdot), \Theta(\cdot), \omega(\cdot), o(\cdot)$.

可忽略量 (Negligible Amount) 是指对于任意正常数 c , 其渐近小于 λ^{-c} , 通常记为 $\text{negl}(\lambda)$. 如果对任意 $c > 0, \lim_{\lambda \rightarrow \infty} \lambda^c f(\lambda) = 0$, 则函数 $f(\lambda)$ 为 λ 上一个可忽略的函数. 不可忽略量是指存在某个正常数 c , 其渐近不小于 λ^{-c} . 一个函数为指数小的函数 (或称为几乎为 0), 是指其渐近小于 $2^{-\Omega(\lambda)}$; 一个函数为指数上接近于 1 的函数 (或称为几乎为 1), 是指它渐近为 $1 - 2^{-\Omega(\lambda)}$.

2.2 数域和子域

冯克勤^[42]介绍了代数数论的基本理论, 本小节仅简要叙述子域格攻击^[26]中使用的数域方面一些相关定义.

设 $\mathbb{K}$ 是 $\mathbb{Q}$ 上一个度为 $n = [\mathbb{K} : \mathbb{Q}]$ 的数域, 并假定 $\mathbb{K}$ 是 $\mathbb{Q}$ 的 Galois 扩展, 即 Galois 群 $G = \text{Gal}(\mathbb{K}/\mathbb{Q})$ 是 $\mathbb{K}$ 的 $\mathbb{Q}$ 线性自同构群.

设 $\mathbb{L}$ 是 $\mathbb{K}$ 的子域, 根据 Galois 理论基本定理, G 的子群 G' 与 $\mathbb{K}$ 的子域 $\mathbb{L}$ 之间一一对应, 即 G' 是固定子域 $\mathbb{L}$ 时 G 的子群, $G' = \text{Gal}(\mathbb{K}/\mathbb{L})$. 设 $n' = [\mathbb{L} : \mathbb{Q}], r = [\mathbb{K} : \mathbb{L}]$, 其中 $n = r \cdot n'$.

数域中的经典包含映射 $\mathbb{L} \subset \mathbb{K}$ 将具体表示为映射 $\vartheta : \mathbb{L} \rightarrow \mathbb{K}$. 我们使用符号 $O_{\mathbb{K}}$ 和 $O_{\mathbb{L}}$ 分别表示数域 $\mathbb{K}$ 和 $\mathbb{L}$ 的整数环.

对于数域中相对范数 $N_{\mathbb{K}/\mathbb{L}} : \mathbb{K} \rightarrow \mathbb{L}$ 和相对迹 $Tr_{\mathbb{K}/\mathbb{L}} : \mathbb{K} \rightarrow \mathbb{L}$, 我们定义乘法和加法映射如下:

$$N_{\mathbb{K}/\mathbb{L}} : \alpha \rightarrow \prod_{\theta \in G'} \theta(\alpha),$$

$$Tr_{\mathbb{K}/\mathbb{L}} : \alpha \rightarrow \sum_{\theta \in G'} \theta(\alpha).$$

为简单起见, 下面简称为范数和迹. 给定 $\alpha, \beta \in \mathbb{K}$ 和 $a \in \mathbb{L}$, 则易于验证范数和迹的下列性质:

- (1) $N_{\mathbb{K}/\mathbb{L}}(\alpha \cdot \beta) = N_{\mathbb{K}/\mathbb{L}}(\alpha) \cdot N_{\mathbb{K}/\mathbb{L}}(\beta),$
- $Tr_{\mathbb{K}/\mathbb{L}}(\alpha + \beta) = Tr_{\mathbb{K}/\mathbb{L}}(\alpha) + Tr_{\mathbb{K}/\mathbb{L}}(\beta);$

$$(2) N_{\mathbb{K}/\mathbb{L}}(a \cdot \beta) = a^r \cdot N_{\mathbb{K}/\mathbb{L}}(\beta),$$

$$Tr_{\mathbb{K}/\mathbb{L}}(a \cdot \beta) = a \cdot Tr_{\mathbb{K}/\mathbb{L}}(\beta).$$

分圆数域 (Cyclotomic Field): 设 ζ_m 为任一 m -次的单位原根, 即 $(\zeta_m)^m = 1$, 且当 $1 \leq i < m$ 时 $(\zeta_m)^i \neq 1$, 则称数域 $\mathbb{K} = \mathbb{Q}(\zeta_m)$ 为 m -次分圆数域. 数域 $\mathbb{K} = \mathbb{Q}(\zeta_m)$ 的度为 $n = \varphi(m)$, 并且存在一个与 $\mathbb{Z}_m^*$ 同构的 Galois 群, 即 $i \in \mathbb{Z}_m^*$ 对应到自同构 $\theta_i : \zeta_m \rightarrow \zeta_m^i$, 这里 $\varphi(m)$ 为高斯函数, 表示在 $1, \dots, m$ 中与 m 互素的整数个数. 对于任意 $m' | m$, 数域 $\mathbb{Q}(\zeta_{m'})$ 是 $\mathbb{Q}(\zeta_m)$ 的一个子域, 且存在其它真子域. 如实子域 $\mathbb{Q}(\zeta_m + \bar{\zeta}_m)$ 是 $\mathbb{K}$ 中一个度为 $n/2$ 的真子域, 而且对于任意除子 $n' | n, \mathbb{K} = \mathbb{Q}(\zeta_m)$ 存在一个度为 n' 的子域.

根据分圆数域理论^[43] 知, $\mathbb{K}$ 的整数环 $O_{\mathbb{K}} = \mathbb{Z}[\zeta_m]$.

为便于理解基于子域的格攻击方法, 下面通过实例给出数域中上述相关定义的具体计算过程.

例 1. 设 $m=8, n=4$, 则多项式环定义为 $R = \mathbb{Z}[x]/\langle x^4 + 1 \rangle$, 数域 $\mathbb{K}$ 和子域 $\mathbb{L}$ 分别为

$$\mathbb{K} = \mathbb{Q}[x]/\langle x^4 + 1 \rangle = \mathbb{Q}(\zeta_m),$$

$$\mathbb{L} = \mathbb{Q}[x]/\langle x^2 + 1 \rangle = \mathbb{Q}(\zeta_n).$$

不失一般性, 假定 $f = -9x^3 + 2x^2 + x + 3 \in R$. 则 f 映射到整数环 $O_{\mathbb{K}} = \mathbb{Z}[\zeta_m]$ 中的元素 f 为

$$f = -9\zeta_m^3 + 2\zeta_m^2 + \zeta_m^1 + 3.$$

根据定义, $f \in O_{\mathbb{K}}$ 的范数和迹可分别计算为

$$\begin{aligned} N_{\mathbb{K}/\mathbb{L}}(f) &= ((-9\zeta_m^2 + 1)\zeta_m^1 + (2\zeta_m^2 + 3)) \times \\ &\quad ((-9\zeta_m^2 + 1)(-\zeta_m^1) + (2\zeta_m^2 + 3)) \\ &= 92\zeta_m^2 - 13 \\ &= 92\zeta_n - 13, \\ Tr_{\mathbb{K}/\mathbb{L}}(f) &= ((-9\zeta_m^2 + 1)\zeta_m^1 + (2\zeta_m^2 + 3)) + \\ &\quad ((-9\zeta_m^2 + 1)(-\zeta_m^1) + (2\zeta_m^2 + 3)) \\ &= 2(2\zeta_m^2 + 3) \\ &= 4\zeta_n + 6. \end{aligned}$$

给定元素 $f' = 92\zeta_n - 13 \in \mathbb{L}$, 则经典包含映射 $\vartheta : \mathbb{L} \rightarrow \mathbb{K}$ 将 f' 映射为 $f'' = \vartheta(f') = 92\zeta_m^2 - 13$.

注意: 这种经典映射 ϑ 将使用在子域格攻击中, 以提升子域 $\mathbb{L}$ 中的解到全域 $\mathbb{K}$ 中.

2.3 概率分布度量

目前, 概率分布之间接近程度的度量方法主要有两种——基于分布差的统计距离 (Statistical Distance, SD)^[44] 和基于分布比的 Rényi 扩散 RD ^[45].

设 D_1, D_2 为有限集 (或可测集) X 上两个概率分布, 则 D_1, D_2 之间的统计距离定义为

$$SD(D_1, D_2) = \frac{1}{2} \sum_{x \in X} |D_1(x) - D_2(x)|.$$

设 D_1, D_2 为有限集 (或可测集) X 上两个概率分布和 $\alpha > 1$, 则 D_1, D_2 之间的 Rényi 扩散定义为

$$RD_a(D_1 \parallel D_2) = \left(\sum_{x \in X} \frac{D_1(x)^a}{D_2(x)^{a-1}} \right)^{\frac{1}{a-1}}.$$

给定有限集 X , 符号 $x \leftarrow U(X)$ 表示使用均匀分布从集合 X 中抽样元素 x .

两个分布 D_1, D_2 是统计上不可区分的, 如果它们的统计距离 $SD(D_1(\lambda), D_2(\lambda))$ 是关于 λ 的一个可忽略函数.

有限集 X 上分布 D 是 ϵ -均匀的 (ϵ -uniform), 如果它与均匀分布的统计距离至多为 ϵ .

2.4 高斯函数

给定任意 $s > 0$ 和向量 $\mathbf{c} \in \mathbb{R}^n$, 则以 $\mathbf{c}$ 为中心, s 为参数的 $\mathbb{R}^n$ 上(球形)高斯函数(Spherical Gaussian Function)定义为

$$\rho_{s,c}(\mathbf{x}) = \exp(-\pi \|\mathbf{x} - \mathbf{c}\|^2 / s^2).$$

因为 $\int_{\mathbf{x} \in \mathbb{R}^n} \rho_{s,c}(\mathbf{x}) d\mathbf{x} = s^n$, 所以, $\rho_{s,c}(\mathbf{x}) / s^n$ 是一个概率密度函数, 并且能使用标准方法对函数 $\rho_{s,c}(\mathbf{x}) / s^n$ 进行有效近似^[46]. 因此, 以 $\mathbf{c}$ 为中心, s 为参数的高斯分布定义为

$$\forall \mathbf{x} \in \mathbb{R}^n, D_{s,c}(\mathbf{x}) = \rho_{s,c}(\mathbf{x}) / s^n.$$

给定秩为 n 的矩阵 $\mathbf{S} \in \mathbb{R}^{m \times n}$ 和向量 $\mathbf{c} \in \mathbb{R}^n$, 则以 $\mathbf{c}$ 为中心, $\mathbf{S}$ 为参数的 $\mathbb{R}^n$ 上椭圆形高斯函数(Ellipsoid Gaussian Function)定义为

$$\rho_s(\mathbf{x}) = \exp(-\pi(\mathbf{x} - \mathbf{c})^T (\mathbf{S}^T \mathbf{S})^{-1} (\mathbf{x} - \mathbf{c})).$$

显然, 椭圆形高斯函数只依赖于协方差矩阵(Covariance Matrix) $\mathbf{A} = \mathbf{S}^T \mathbf{S}$, 与 $\mathbf{S}$ 的选择无关. 而且, 如果设置 $\mathbf{S} = s \mathbf{I}_n$, 其中 $\mathbf{I}_n$ 为 $n \times n$ 单位矩阵, 则椭圆形高斯函数变成为球形高斯函数.

2.5 格和理想格

2.5.1 格

一个 n -维满秩的格 $L \subset \mathbb{R}^n$ 是由 n 个线性独立向量 $\mathbf{b}_j \in \mathbb{R}^n$ 的所有整数线性组合 $\sum_{j=1}^n y_j \mathbf{b}_j$ 产生的集合. 如果将向量 $\mathbf{b}_j$ 当作矩阵 $\mathbf{B}$ 的列, 那么格 $L(\mathbf{B}) = \{\mathbf{B}\mathbf{y} : \mathbf{y} \in \mathbb{Z}^n\}$. 格 L 的平行体(Parallelepiped)定义为 $P(\mathbf{B}) = \{\mathbf{B}\mathbf{y} : \mathbf{y} \in [-1/2, 1/2)^n \cap \mathbb{R}^n\}$; 格 L 的生成空间是由 $\mathbf{B}$ 的向量生成的线性空间, 即 $\text{span}(L) = \{\mathbf{B}\mathbf{y} : \mathbf{y} \in \mathbb{R}^n\}$.

对于格 L , 它的对偶格 L^* 定义为在模 1 下 $\text{span}(L)$ 中所有与 L 正交的点集, 即 $L^* = \{\mathbf{y} \in \text{span}(L) : \forall \mathbf{x} \in L, \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}\}$.

给定格 $L(\mathbf{B})$, 其行列式为 $\det(L) = |\det(\mathbf{B})|$. 对于任何 $i \leq n$, 格 L 的第 i 个最小值 $\lambda_i(L)$ 定义为最小的 r , 满足格 L 包含 i 个线性独立的向量, 且它们的范数都不大于 r .

引理 1(推论 2^①, Minkowski's First Theorem).

对于任何 n -维满秩的格 L ,

$$\lambda_1(L) \leq \sqrt{n} (\det(L))^{1/n}.$$

引理 2(定理 3^①, Minkowski's Second Theorem).

对于任何 n -维满秩的格 L ,

$$\left(\prod_{i=1}^n \lambda_i(L) \right)^{1/n} \leq \sqrt{n} (\det(L))^{1/n}.$$

为定界 $\lambda_n(L)$, 我们还需要 Hadamard 不等式.

引理 3(定理 16.6^[47], Hadamard's Inequality).

设矩阵 $\mathbf{B} \in \mathbb{R}^{n \times n}$ 的列向量为 $\mathbf{b}_1, \dots, \mathbf{b}_n$, 那么

$$|\det(\mathbf{B})| \leq \prod_{j=1}^n \|\mathbf{b}_j\|.$$

2.5.2 理想格

设元素 $\mathbf{g} \in R$, 由元素 $\mathbf{g}$ 生成的主理想格记为 $I = \langle \mathbf{g} \rangle$, 其在 R 上的理想格记为 $Rot(\mathbf{g}) = (\mathbf{g}, \mathbf{x} \cdot \mathbf{g}, \dots, \mathbf{x}^{n-1} \cdot \mathbf{g})$. 给定任意元素 $\mathbf{a} \in R$, 符号 $[\mathbf{a}]_g = \mathbf{a} \bmod \mathbf{g} \in P(Rot(\mathbf{g}))$ 是指将元素 $\mathbf{a}$ 映射到理想格 I 的平行体 $P(Rot(\mathbf{g}))$ 内的唯一代表元素, 即 $[\mathbf{a}]_g = Rot(\mathbf{g})\mathbf{y}$, 其中 $\mathbf{y} \in [-1/2, 1/2)^n \cap \mathbb{R}^n$.

2.5.3 离散高斯分布

对于任意 $s > 0, \mathbf{c} \in \mathbb{R}^n$, 格 L 上离散高斯分布定义为

$$\forall \mathbf{x} \in L, D_{L,s,c}(\mathbf{x}) = \rho_{s,c}(\mathbf{x}) / \rho_s(L),$$

其中 $\rho_{s,c}(L) = \sum_{\mathbf{x} \in L} \rho_{s,c}(\mathbf{x})$.

对于秩为 n 的矩阵 $\mathbf{S} \in \mathbb{R}^{m \times n}$, 向量 $\mathbf{c} \in \mathbb{R}^n$, 集合 $L \perp \mathbf{c}$ 上的椭圆高斯分布定义为

$$\forall \mathbf{x} \in L \perp \mathbf{c}, D_{L+\mathbf{c},s}(\mathbf{x}) = \rho_s(\mathbf{x}) / \rho_s(L + \mathbf{c}),$$

其中 $\rho_s(L + \mathbf{c}) = \sum_{\mathbf{x} \in L + \mathbf{c}} \rho_s(\mathbf{x})$.

当向量 $\mathbf{c} = 0$ 时, 符号 $D_{L,s,0}$ 简写为 $D_{L,s}$, 而且格 L (或理想格 I) 上的随机高斯抽样表示为 $\mathbf{x} \leftarrow D_{L,s}$ (或 $\mathbf{d} \leftarrow D_{I,s}$).

由 Micciancio 和 Regev^[46] 引入的平滑参数(Smoothing Parameter)记作 $\eta_\epsilon(L)$, 是指给定格 L 和实数 $0 < \epsilon < 1$, $\eta_\epsilon(L)$ 定义为最小的 s , 满足条件 $\rho_{1/s}(L^* \setminus \{0\}) \leq \epsilon$.

下面以引理形式给出平滑参数的一些性质.

引理 4(引理 4.4^[46]). 给定任意一个 n -维的格 L , $0 < \epsilon < 1, s \geq \eta_\epsilon(L)$, 则有

$$\Pr_{\mathbf{x} \leftarrow D_{L,s}} [\|\mathbf{x}\| \geq s\sqrt{n}] \leq \frac{1+\epsilon}{1-\epsilon} \cdot 2^{-n}.$$

引理 5(引理 3^[48]). 给定秩为 n 的格 L , 常数 $0 < \epsilon < 1$, 向量 $\mathbf{c} \in \mathbb{R}^n$ 和矩阵 $\mathbf{S} \in \mathbb{R}^{m \times n}$, 满足 $\sigma_n(\mathbf{S}) \geq \eta_\epsilon(L)$, 则有

① Regev O. Lattices in Computer Science, Lecture 1, 2009 Fall: 1-10. http://www.cims.nyu.edu/~regev/teaching/lattices_fall_2009/index.html

$$\Pr_{x \leftarrow D_{L,S,\epsilon}} [\|x\| \geq \sigma_1(S)\sqrt{n}] \leq \frac{1+\epsilon}{1-\epsilon} \cdot 2^{-n}.$$

引理 6(引理 3.3^[46]). 设 L 是一个 n -维的格, $\epsilon > 0$, 则有

$$\eta_\epsilon(L) \leq \sqrt{\ln(2n(1+1/\epsilon))/\pi} \cdot \lambda_n(L).$$

引理 7(推论 2.8^[49]). 设 L, L' 为两个 n -维的格, 满足 $L' \subseteq L$, 且 $\epsilon \in (0, 1/2)$. 则对于任意 $c \in \mathbb{R}^n$, $s \geq \eta_\epsilon(L')$, 我们有

$$\text{SD}(D_{L',s,\epsilon} \bmod L', U(L \bmod L')) \leq 2\epsilon.$$

实际上, 上述引理 7 也可以看作引理 4.1^[46] 的一个推论.

引理 8(引理 4.1^[50]). 对于任何理想 $I \subseteq R$, $\epsilon \in (0, 1)$, $t \geq \sqrt{2\pi}$ 和 $\sigma \geq t/\sqrt{2\pi} \cdot \eta_\epsilon(I)$, 我们有

$$\Pr_{b \leftarrow D_{I,\sigma}} \left[\|b^{-1}\| \geq \frac{t}{\sigma \sqrt{n/2}} \right] \leq \frac{1+\epsilon}{1-\epsilon} \frac{n \sqrt{2\pi e}}{t}.$$

为符号简单, 本文对从分布 $D_{L,\sigma}$ 中抽样的向量将直接被用作多项式环 R (或 R_q) 中的元素, 且向量的每个分量对应于 R (或 R_q) 中元素的相应系数; 反之亦然.

2.6 素理想

理想 $p \subset O_{\mathbb{K}}$ 称为素理想, 如果当 $a, b \in O_{\mathbb{K}}$, 且 $a \cdot b \in p$, 那么 $a \in p$ 或 $b \in p$. 如果素理想 p 仅由一个元素 $a \in O_{\mathbb{K}}$ 生成, 即 $p = \langle a \rangle$, 则 p 称为素主理想.

对于任一理想 $a \subset O_{\mathbb{K}}$, 其范数定义为 $N(a) = |O_{\mathbb{K}}/a|$, 这里 $|O_{\mathbb{K}}/a|$ 表示商环 $O_{\mathbb{K}}/a$ 的大小. 如果理想 $p \subset O_{\mathbb{K}}$ 的范数 $p = N(p)$ 为素数, 则 p 一定是素理想(引理 1.6.7^①). 注意: 素理想的范数并不一定是素数.

数域的整数环中素理想的分布非常类似于整数中素数的分布. 类似于素数定理, 我们有 Landau 的素理想定理. 下面以引理形式给出这两个定理.

引理 9(定理 1.5.1^[51], 素数定理). 设 $\pi(x)$ 表示不大于 x 的素数个数, 则 $\pi(x)$ 渐近为 $x/\ln x$, 即

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x} = 1.$$

引理 10(定理 5.17^[52], Landau 的素理想定理). 设 $\mathbb{K}$ 是度为 n 的代数数域, $\pi_{\mathbb{K}}(x)$ 表示 $O_{\mathbb{K}}$ 中范数不大于 x 的素理想个数, 则 $\pi_{\mathbb{K}}(x)$ 渐近为 $x/\ln x$.

然而, 在 GGH13 构造中, 抽样的秘密理想元素需要为素主理想元素. 为此, 当限定 Landau 的素理想定理到素主理想时, Garg^[52] 给出如下启发式猜测:

引理 11(猜测 5.18^[52]). 设 $m = 2n$, n 为 2 的幂, $\mathbb{K}$ 为 m -次分圆数域. 对于任一 $\sigma = \text{poly}(n)$, 存在常数 $c > 1$, 对于足够大 n , 我们有

$$\Pr_{f \leftarrow D_{\mathbb{Z}^n, \sigma}} [N(f) \geq 2^{O(n)} \text{ and is prime}] \geq \frac{1}{n^c}.$$

Smart 和 Vercauteren^[53] 的计算实验结果支持上述引理 11.

2.7 多线性映射

本节定义多线性映射和分级编码系统.

定义 1(多线性映射^[1]). 给定 $\kappa + 1$ 个阶为 q 的循环群 $G_1, \dots, G_\kappa, G_T$, 则由它们产生的 κ -级多线性映射 $e: G_1 \times \dots \times G_\kappa \rightarrow G_T$ 具有下列性质:

- (1) 对于元素 $\{g_j \in G_j\}_{j=1, \dots, \kappa}$ 和 $a \in \mathbb{Z}_q$, 映射 e 满足条件 $e(g_1, \dots, a \cdot g_j, \dots, g_\kappa) = a \cdot e(g_1, \dots, g_\kappa)$;
- (2) 映射 e 在下列情形是非退化的: 如果元素 $\{g_j \in G_j\}_{j=1, \dots, \kappa}$ 分别是所在群 G_j 的生成元素, 那么 $e(g_1, \dots, g_\kappa)$ 是 G_T 的生成元素.
- (3) 映射 e 能够有效计算, 但没有有效算法计算群 G_j, G_T 中的离散对数.

定义 2(κ -级编码系统^[11]). 环 R 上的一个 κ -级编码系统是一个集合 $S = \{S_j^{(\alpha)} \subset R; \alpha \in R, j \in [\kappa]\}$, 具有下列性质:

- (1) 任意 $j \in [\kappa]$, 集合 $\{S_j^{(\alpha)}; \alpha \in R\}$ 不相交;
- (2) 对于任意 $\alpha_1, \alpha_2 \in R$ 和 $j \in [\kappa]$, 编码 $u_1 \in S_j^{(\alpha_1)}$ 和 $u_2 \in S_j^{(\alpha_2)}$ 具有二元操作 ‘+’ 和 ‘-’, 满足 $u_1 + u_2 \in S_j^{(\alpha_1 + \alpha_2)}$, $u_1 - u_2 \in S_j^{(\alpha_1 - \alpha_2)}$, 其中 $\alpha_1 + \alpha_2$, $\alpha_1 - \alpha_2$ 均为环 R 中的加法和减法运算;
- (3) 对于任意 $\alpha_1, \alpha_2 \in R$ 和 $j_1, j_2 \in [\kappa]$, 且 $j_1 + j_2 \leq \kappa$, 编码 $u_1 \in S_{j_1}^{(\alpha_1)}$ 和 $u_2 \in S_{j_2}^{(\alpha_2)}$ 满足 $u_1 \times u_2 \in S_{j_1 + j_2}^{(\alpha_1 \times \alpha_2)}$, 其中 $\alpha_1 \times \alpha_2$ 为 R 中的乘法运算, 而 $j_1 + j_2$ 为整数标量加法.

2.8 剩余 Hash 引理 (Leftover Hash Lemma)

从有限集 X 到有限集 Y 的 Hash 函数族 H 是两两独立的 (Pairwise Independent), 如果对于所有不同的 $x, x' \in X$, $\Pr_{h \leftarrow U(H)} [h(x) = h(x')] = 1/|Y|$.

定义 3. 从 X 到 Y 的 Hash 函数族 H 是 ϵ -两两独立的, 如果

$$\sum_{x \neq x'} (\Pr_{h \leftarrow U(H)} [h(x) = h(x')] - 1/|Y|) \leq \frac{|X|^2}{|Y|} \epsilon.$$

引理 12(Leftover Hash Lemma, LHL^[54]). 设 H 是从 X 到 Y 两两独立的 Hash 函数族. 假定 $h \leftarrow U(H)$ 和 $x \leftarrow U(X)$ 是独立均匀选择的, 则 $(h, h(x))$ 是 $H \times Y$ 上 $\frac{1}{2} \sqrt{|Y|/|X|}$ 均匀的.

在 GGH13 构造中, Garg 等人使用了整数上的离散高斯 LHL(定理 2^[48]). 为优化 GGH13 构造,

① Osserman B. Algebraic Number Theory. Lecture Notes, 2008. <https://www.math.ucdavis.edu/~osserman/class/numthy/numthybook.pdf>

Langlois, Stehlé 和 Steinfeld^[21] 将整数上的离散高斯 LHL 自适应扩展到代数环上的离散高斯 LHL.

给定 $\mathbf{X} = (\mathbf{x}_1, \mathbf{x}_2) \in R^2$, 我们定义由抽样 $(\mathbf{u}_1, \mathbf{u}_2) \leftarrow (D_{R,s})^2$ 和输出 $\mathbf{y} = \mathbf{x}_1 \mathbf{u}_1 + \mathbf{x}_2 \mathbf{u}_2$ 导出的分布为 $E_{\mathbf{X},s} = \mathbf{x}_1 D_{R,s} + \mathbf{x}_2 D_{R,s}$. 代数环上的离散高斯 LHL^[21] 是指分布 $E_{\mathbf{X},s}$, 统计上接近于椭圆高斯分布 $D_{R,s\mathbf{X}^T}$, 即统计距离 $\text{SD}(E_{\mathbf{X},s}, D_{R,s\mathbf{X}^T})$ 可任意小.

对于高斯抽样产生的 $\mathbf{X}$, Stehlé 和 Steinfeld^[50] 证明以高概率 $\mathbf{X}$ 能够生成整个环 R .

引理 13 (引理 4.4^[50]). 设 $s' \geq 7n^{1.5} (\ln n)^{1.5}$, 则对于足够大的 $n = 2^k$ 有

$$\Pr_{\mathbf{x}_1, \mathbf{x}_2 \leftarrow D_{R,s'}} [\mathbf{X} \cdot R^2 = R] \geq \Omega(1).$$

设 $A_{\mathbf{X}} \subseteq \{(\mathbf{v}_1, \mathbf{v}_2) \in R^2 : \mathbf{x}_1 \mathbf{v}_1 + \mathbf{x}_2 \mathbf{v}_2 = 0\}$ 为正交于 $\mathbf{X}$ 的 1-维 R 模向量. 通过多项式到系数向量的映射, 我们将 $A_{\mathbf{X}}$ 当作 $\mathbb{Z}^{2n}$ 中一个 n -维的格.

引理 14 (引理 5.5^[21]). 设 $\mathbf{X}$ 和 $A_{\mathbf{X}}$ 定义如上, 则 $\eta_e(A_{\mathbf{X}}) \leq \delta n \cdot \sqrt{2 \log(2n(1+1/\epsilon))} / \pi$, 其中 $\delta = \max(\|\mathbf{x}_1\|_{\infty}, \|\mathbf{x}_2\|_{\infty})$.

引理 15 (引理 5.3^[21]). 给定满足 $\mathbf{X} \cdot R^2 = R$ 的 $\mathbf{X}$ 和上述定义的 $A_{\mathbf{X}}$, $\epsilon \in (0, 1/3)$, 如果 $s \geq \eta_e(A_{\mathbf{X}})$, 则 $\text{SD}(E_{\mathbf{X},s}, D_{R,s\mathbf{X}^T}) \leq 2\epsilon$.

3 新随机化的多线性映射

本节构造基于新随机化方法的多线性映射. 由于理想格上 GGH13 构造^[11] 需要再随机化, 使得公共参数中需要包含许多明文“0”的 1-级编码. GGH13 构造的安全分析^[11] 显示通过这些“0”的 1-级编码易于计算得到构造中使用的秘密理想元素的格基, 即所谓“0”化攻击问题. 而且, 这种“0”化攻击已经导致基于 GGH13 构造的两个重要应用 MPKE 和 WE 被破解^[22].

为避免“0”化攻击问题, 在新随机化构造中, 公共参数只提供非“0”元素的 1-级编码, 不再包含“0”元素的 1-级编码, 也不包含“1”的 1-级编码. 为此, 本节通过设计新的“0”测试参数, 使其不仅用于“0”测试参数功能, 还用于编码与其对应的 1-级编码中的非“0”元素.

本节先构造对称多线性映射方案, 然后将其自适应扩展到非对称变种方案.

3.1 对称多线性映射

3.1.1 参数符号约定

为便于描述, 构造中参数符号约定如下:

λ : 安全参数;

κ : 多线性映射的次数;

q : 构造中编码的模;

n : 多项式环 R, R_q 中元素的向量维数;

σ : 产生秘密理想元素 (如 $\mathbf{g}$) 的高斯抽样参数;

σ' : 产生公共参数中 k -级编码的高斯抽样参数;

σ_k^* : 产生 k -级编码算法中的高斯抽样参数;

σ^* : 产生“0”测试参数的高斯抽样参数;

τ : 公共参数中 k -级编码的个数;

l_{-1} : 抽样理想元素 $\mathbf{g}$ 满足条件 $\|\mathbf{g}\| \leq l_{-1}$;

l : 从提取编码的每个系数中提取 l 个最有意义的比特位.

3.1.2 构造

对于构造中参数的大小设置, 我们将在第 3.1.3 节中具体给出.

公共参数产生算法 $par \leftarrow \text{InstGen}(1^\lambda, 1^\epsilon)$:

(1) 选择足够大素数 q ;

(2) 随机抽样 $\mathbf{z} \leftarrow U(R_q)$, 满足条件 $\mathbf{z}^{-1} \in R_q$;

(3) 抽样选择素理想元素 $\mathbf{g} \leftarrow D_{\mathbb{Z}^n, \sigma}$, 满足条件 $\beta = |R/\langle \mathbf{g} \rangle| = |\det(\text{Rot}(\mathbf{g}))| > 2^\lambda$, $\|\mathbf{g}\| \leq \sqrt{n}\sigma$, 并且 $\mathbf{g}^{-1} \in \mathbb{K}$ 和 $\|\mathbf{g}^{-1}\| < l_{-1}$, 记其生成的主理想格为 $I = \langle \mathbf{g} \rangle \subset R$;

(4) 抽样选择素理想元素 $\mathbf{f} \leftarrow D_{\mathbb{Z}^n, \sigma}$, 满足条件 $\|\mathbf{f}\| \leq \sqrt{n}\sigma$, 并且 $\mathbf{f}^{-1} \in \mathbb{K}$ 和 $\|\mathbf{f}^{-1}\| < l_{-1}$;

(5) 对于 $j \in [\tau]$:

(5.1) 抽样选择元素 $\mathbf{x}_j \leftarrow D_{\mathbb{Z}^n, \sigma'}$;

(5.2) 计算 $\mathbf{e}_j = [\mathbf{x}_j]_{\mathbf{g}}$ 和 $\mathbf{a}_j = (\mathbf{x}_j - \mathbf{e}_j)/\mathbf{g}$;

(5.3) 计算产生明文元素 $\mathbf{e}_j$ 的 1-级编码 $\mathbf{y}_j = [\mathbf{x}_j/\mathbf{z}]_q$;

(6) 对于 $j \in [\tau]$:

(6.1) 抽样选择元素 $\mathbf{b}_j \leftarrow D_{\mathbb{Z}^n, \sigma^*}$;

(6.2) 计算 $\mathbf{h}_j = \mathbf{e}_j \mathbf{f} + \mathbf{b}_j \mathbf{g}$;

(6.3) 产生新的“0”测试参数 $\mathbf{p}_{z,j} = [\mathbf{h}_j \mathbf{z}^{\kappa}/\mathbf{g}]_q$;
 // $\mathbf{p}_{z,j}$ 不仅是“0”测试参数, 也是明文元素 $\mathbf{e}_j$ 的特殊编码, 与 $\mathbf{y}_j$ 中的明文元素 $\mathbf{e}_j$ 一一对应.

(7) 输出公共参数 $par = \{n, q, \{\mathbf{y}_j, \mathbf{p}_{z,j}\}_{j \in [\tau]}\}$.

1-级编码算法 $\mathbf{u} \leftarrow \text{Enc}(par, 1, \{\mathbf{d}_j\}_{j \in [\tau]})$:

(1) 高斯抽样选择元素 $\mathbf{d}_j \leftarrow D_{\mathbb{Z}^n, \sigma_1^*}$, $j \in [\tau]$;

(2) 计算产生 1-级编码 $\mathbf{u} = \left[\sum_{j \in [\tau]} \mathbf{d}_j \mathbf{y}_j \right]_q$;

// 编码 $\mathbf{u}$ 中的明文 $\mathbf{d} = \sum_{j \in [\tau]} \mathbf{d}_j \mathbf{e}_j$ 是隐藏的.

编码加法算法 $\mathbf{u} \leftarrow \text{Add}(par, k, \mathbf{u}_1, \dots, \mathbf{u}_m)$:

给定 m 个 k -级编码 $\mathbf{u}_r$, 则它们的和 $\mathbf{u} = \left[\sum_{r=1}^m \mathbf{u}_r \right]_q$

是一个 k -级编码.

编码乘法算法 $\mathbf{u} \leftarrow \text{Mul}(par, 1, \mathbf{u}_1, \dots, \mathbf{u}_k)$:

给定 k 个 1-级编码 u_r , 则它们的积 $u = \left[\prod_{r=1}^k u_r \right]_q$

是一个 k -级编码.

“0”测试算法 $\text{isZero}(\text{par}, \{d_j\}_{j \in [\tau]}, u)$:

(1) 给定 $d_j \leftarrow D_{\mathbb{Z}^n, \sigma_1^*}$, $j \in [\tau]$, 计算产生“0”测试

参数 $p_{zt} = \left[\sum_{j \in [\tau]} d_j p_{zt,j} \right]_q$;

(2) 给定一个 κ -级编码 u , 计算“0”测试函数 isZero 以判定 u 中明文元素是否为“0”, 即

$$\text{isZero}(\text{par}, \{d_j\}_{j \in [\tau]}, u) = \begin{cases} 1, & \text{如果 } \| [u \cdot p_{zt}]_q \|_{\infty} < q^{7/8} \\ 0, & \text{否则} \end{cases}.$$

提取算法 $w \leftarrow \text{Ext}(\text{par}, \{d_j\}_{j \in [\tau]}, u)$:

(1) 给定 $d_j \leftarrow D_{\mathbb{Z}^n, \sigma_1^*}$, $j \in [\tau]$, 计算产生“0”测试

参数 $p_{zt} = \left[\sum_{j \in [\tau]} d_j p_{zt,j} \right]_q$;

(2) 给定一个 κ -级编码 u , 计算产生提取编码 $v = [u \cdot p_{zt}]_q$;

(3) 从 v 的每个系数中提取 $l = (\log q)/8 - \lambda$ 个最有意义的比特位, 输出提取比特串 w , 即

$$w = \text{Ext}(\text{par}, \{d_j\}_{j \in [\tau]}, u) = \text{MSB}_l(v).$$

评论 1. (1) 上述构造不能直接产生任意给定明文元素的 1-级编码, 只能产生隐藏明文的 1-级编码 $u = \left[\sum_{j \in [\tau]} d_j y_j \right]_q$. 这是因为构造的公共参数中没有明文“0”的 1-级编码, 也没有明文“1”的 1-级编码, 只提供了隐藏明文元素 e_j 的 1-级编码 y_j .

(2) 在上述构造中, 新产生 1-级编码 u 中隐藏的明文元素, 并不能直接使用, 必须通过与 u 对应的“0”测试参数间接使用. 这是因为新的“0”测试参数 $p_{zt,j}$ 不仅是“0”测试参数, 也是隐藏了明文元素 e_j 的特殊编码, 而且 $p_{zt,j}$ 与 y_j 一一对应, 它们编码的隐藏明文元素 e_j 相同. 因此, 如果基于新随机化多线性映射构造 MPKE 协议, 则必须使用与 1-级编码 $u = \left[\sum_{j \in [\tau]} d_j y_j \right]_q$ 对应的“0”测试参数, 即 $p_{zt} = \left[\sum_{j \in [\tau]} d_j p_{zt,j} \right]_q$.

(3) 上述构造的公共参数中, 仅包含了非“0”元素 e_j 的 1-级编码 y_j 和对应的“0”测试参数 $p_{zt,j}$, 所以构造中仅能产生可用的隐藏明文元素的 1-级编码. 如果需要产生可用的隐藏明文元素的 μ -级编码, 则需要在公共参数中, 包含非“0”的 μ -级编码 $y_{\mu,j} = [(e_{\mu,j} + a_{\mu,j} \mathbf{g})/\mathbf{z}^{\mu}]_q$ 和对应的“0”测试参数 $p_{zt,\mu,j} = [(e_{\mu,j} \mathbf{f} + b_{\mu,j} \mathbf{g})\mathbf{z}^{\kappa}/\mathbf{g}]_q$, 这里 $\mu \in [\kappa]$. 在这种情况下, 算法 $u \leftarrow \text{Enc}(\text{par}, \mu, d_j)$ 将产生一个 μ -级编码, 即给定 $d_j \leftarrow D_{\mathbb{Z}^n, \sigma_1^*}$, $j \in [\tau]$, 计算产生隐藏的明文元素 $d_{(\mu)} = \sum_{j \in [\tau]} d_j e_{\mu,j}$ 的 μ -级编码 $u = \left[\sum_{j \in [\tau]} d_j y_{\mu,j} \right]_q$. 注意: 此时给定 $d_j \leftarrow D_{\mathbb{Z}^n, \sigma_1^*}$, $j \in [\tau]$, 算法 $\text{Enc}(\text{par},$

$\mu, d_j)$ 产生的不同级数上的可用隐藏明文元素 $d_{(\mu)} = \sum_{j \in [\tau]} d_j e_{\mu,j}$ 并不相同. 这是由于不同级数编码包含的明文元素并不相同所造成. 本文构造方案中仅考虑 1-级编码 y_j 和对应的“0”测试参数 $p_{zt,j}$ 情况.

(4) 在上述构造中, GGH13 构造的“0”测试参数 $p_{zt} = [h\mathbf{z}^{\kappa}/\mathbf{g}]_q$ 中 h 已经被新的“0”测试参数 $p_{zt,j}$ 中 b_j 吸收替代, 即 $p_{zt,j} = [(e_j \mathbf{f} + b_j \mathbf{g})\mathbf{z}^{\kappa}/\mathbf{g}]_q$.

(5) 在新的“0”测试参数中, 隐藏明文部分引入了因子 f . 虽然因子 f 并不能避免第 4.1 节交叉乘积产生的容易计算量问题, 但是可能增加攻击者基于容易计算量的攻击难度. 而且, 构造中将因子 f 放在“0”测试参数中, 是为了使得模 q 保持尽可能小. 当然, 构造也可以在编码 y_j 中引入另一个因子 $f_1 \leftarrow D_{\mathbb{Z}^n, \sigma}$, 即设置 $y_j = [x_j/\mathbf{z}]_q = [(e_j f_1 + a_j \mathbf{g})/\mathbf{z}]_q$.

(6) 新的“0”测试参数 $p_{zt,j}$ 或它们组合产生的 p_{zt} 都能用作“0”测试参数. 而且, 使用 $p_{zt,j}$ 的随机组合也能保证“0”测试参数安全, 使得攻击者产生的无效编码能够通过 p_{zt} 测试的概率几乎为 0.

3.1.3 参数设置

设 λ 为安全参数, 其它参数具体设置如下:

(1) 设多线性映射的次数为 $\kappa = \text{poly}(\lambda)$.

(2) 设置 $n = O(\kappa \lambda \log \lambda)$.

根据 BKZ 算法^[55], 为计算 γ -近似因子的最短向量问题 γ -SVP, 则需要计算维数为 $n/\log \gamma$ 的子格块的最短向量. 因此, 为阻止格归约算法攻击, 我们设置 $\gamma = q^{1/2}$ 和 $n = O(\lambda \log q) = O(\kappa \lambda \log \lambda)$, 从而使得攻击复杂性达到 $O(2^{\lambda})$.

(3) 设置 $\sigma = O(n \log n)$.

根据引理 6 知, 当 $\epsilon = 1/3$ 时

$$\begin{aligned} \eta_{\epsilon}(\mathbb{Z}^n) &\leq \sqrt{\ln(2n(1+1/\epsilon))}/\pi \cdot \lambda_n(\mathbb{Z}^n) \\ &\leq O(\sqrt{\log n}). \end{aligned}$$

根据引理 8, 为使选择元素 $\mathbf{g}$ 的拒绝概率 $p_g \leq$

$\frac{1+\epsilon}{1-\epsilon} \frac{n \sqrt{2\pi e}}{t} < 1$, 需要设置 $t > n \sqrt{2\pi e}$. 我们跟随 GGHlite 构造^[21], 设置 $t = 2n \sqrt{2\pi e}/p_g$.

因此, 可以验证 $\sigma = O(n \log n)$ 满足引理 8 的条件 $\sigma \geq t/\sqrt{2\pi} \cdot \eta_{\epsilon}(\mathbb{Z}^n)$.

根据引理 4 知, 高斯抽样时以高概率有 $\|\mathbf{g}\| \leq \sqrt{n}\sigma$, $\|\mathbf{f}\| \leq \sqrt{n}\sigma$.

(4) 设置 $l_{-1} = n$.

根据引理 8, Langlois, Stehlé 和 Steinfeld^[21] 设置 $l_{-1} = O(1/\sqrt{n \log n})$, 但是在设置 $\|\mathbf{g}^{-1}\|$ 的这种上界时并没有考虑 $\mathbf{g}$ 为素理想这一条件.

因为 l_{-1} 越大, 拒绝接受 $\mathbf{g}$ 的概率就越小. 所以, 为增加选中素理想 $\mathbf{g}$ 的概率, 我们设置 $l_{-1} = n$.

(5) 由引理 13 和引理 15, 设置 $\tau=2$.

(6) 设置 $\sigma'=O(n^3)$.

首先, 根据引理 13 知, 为使得公共参数产生时抽样的 $\mathbf{x}_1, \mathbf{x}_2$ 能够以高概率生成环 R , 我们需要设置 $\sigma' \geq 7n^{1.5}(\ln n)^{1.5}$.

其次, 由引理 7 知, 为使分布 $D_{\mathbb{Z}^n, \sigma'} \bmod \langle \mathbf{g} \rangle$ 与均匀分布 $U(\mathbb{Z}^n / \langle \mathbf{g} \rangle)$ 的统计距离 SD 小于 2ε , 我们需要设置 $\sigma' \geq \eta_\varepsilon(\langle \mathbf{g} \rangle)$.

因为环 R 上理想格 $\langle \mathbf{g} \rangle$ 的连续 Minkowski 最小值相等, 即 $\lambda_1(\langle \mathbf{g} \rangle) = \dots = \lambda_n(\langle \mathbf{g} \rangle)$. 所以, 由引理 2 和引理 3 可得

$$\begin{aligned}\lambda_n(\langle \mathbf{g} \rangle) &= \left(\prod_{i=1}^n \lambda_i(\langle \mathbf{g} \rangle) \right)^{1/n} \\ &\leq \sqrt{n}(\det(\langle \mathbf{g} \rangle))^{1/n} \\ &= \sqrt{n}(\det(\text{Rot}(\mathbf{g})))^{1/n} \\ &\leq \sqrt{n} \|\mathbf{g}\|.\end{aligned}$$

因此, 由引理 6 (取 $\varepsilon=2^{-n}$) 可得

$$\begin{aligned}\eta_\varepsilon(\langle \mathbf{g} \rangle) &\leq O(\sqrt{n \log n}) \cdot \lambda_n(\langle \mathbf{g} \rangle) \\ &\leq O(n^2 \log n \sqrt{n \log n}) \\ &\leq O(n^3).\end{aligned}$$

又因为 $7n^{1.5}(\ln n)^{1.5} \leq O(n^3)$, 所以设置 $\sigma' = O(n^3)$ 能够满足上述所有条件.

(7) 设置 $\sigma_1^* = O(n^{5.5})$.

虽然新随机化构造并不需要再随机化过程, 即产生 1-级编码时不再需要使用“淹没”方法^[11, 21]去除其包含的 0-级编码的统计相关性, 但是我们需要新产生的 1-级编码中包含的 0-级编码尽可能接近均匀分布 $U(R/\langle \mathbf{g} \rangle)$.

由引理 15 知, 当 $\sigma_1^* \geq \eta_\varepsilon(A_X)$ 时, $\text{SD}(E_{X, \sigma_1^*}, D_{R, \sigma_1^*}^{\mathbf{x}^T}) \leq 2\varepsilon$.

又引理 14 (取 $\varepsilon=2^{-n}$) 知,

$$\begin{aligned}\eta_\varepsilon(A_X) &\leq \delta n \cdot \sqrt{2 \log(2n(1+1/\varepsilon))} / \pi \\ &\leq \sqrt{n \sigma'} \cdot n \cdot O(\sqrt{n \log n}) \\ &\leq \sqrt{n \sigma'} \cdot n \cdot O(\sqrt{n \log n}) \\ &\leq O(n^{5.5}),\end{aligned}$$

其中 $\delta = \max(\|\mathbf{x}_1\|_\infty, \|\mathbf{x}_2\|_\infty)$.

(8) 设置 $\sigma^* = q^{5/8}$.

在 GGH13 构造^[11] 和变种 GGHlite^[21] 中, 设置 $\sigma^* = q^{1/2}$. 虽然当 $\sigma^* = q^{1/2}$ 时, 目前没有发现基于迹的子域格攻击 (第 4.5 节) 能够攻击“0”测试参数, 但是为增强新随机化构造抗基于迹的子域格攻击, 本文将 σ^* 增大到 $q^{5/8}$.

(9) 设置素数 $q = O(n^{92\kappa})$.

设 $\mathbf{u}_r = [\mathbf{c}_r / \mathbf{z}]_q$ 为 1-级编码算法 Enc 产生的编码, 则根据上述参数选择可得

$$\begin{aligned}\|\mathbf{c}_r\| &= \|\mathbf{d}_1 \mathbf{x}_1 + \mathbf{d}_2 \mathbf{x}_2\| \\ &\leq \|\mathbf{d}_1 \mathbf{x}_1\| + \|\mathbf{d}_2 \mathbf{x}_2\| \\ &\leq 2 \cdot n \cdot \sqrt{n \sigma_1^*} \cdot \sqrt{n \sigma'} \\ &\leq O(n^{10.5}).\end{aligned}$$

又因为 κ -级编码 $\mathbf{u} = [\mathbf{c} / \mathbf{z}^\kappa]_q$ 是由 κ 个 1-级编码相乘得到, 所以 $\|\mathbf{c}\| = \left\| \prod_{r=1}^{\kappa} \mathbf{c}_r \right\| \leq O(n^{11.5})^\kappa$. 因此, 为保证“0”测试算法和提取算法的正确性, 要求 $\|\mathbf{c}\| < q^{1/8}$. 因此, 选择设置素数 $q = O(n^{11.5})^{8\kappa}$ 能够满足算法所有条件.

(10) 设置 $l = (\log q) / 8 - \lambda$.

减去 λ 是为保证提取编码的错误容余量, 使得提取算法提取比特串时发生错误的概率约为 $2^{-\lambda}$.

所以, 根据上述参数设置, 构造中编码大小约为 $n|q| \approx 92\kappa n \log n$, 公共参数大小约为 $4n|q|$, 其中 $|q|$ 为 q 的比特长度.

3.1.4 正确性

新随机化构造改进了 GGH13 构造中的“0”测试参数, 并且新构造的公共参数中仅包含非“0”的 1-级编码和与其对应的“0”测试参数, 因此需要证明新的构造方案中算法正确性.

在证明新随机化构造中算法的正确性之前, 首先给出证明过程中需要的两个引理.

引理 16 (引理 3^[11]). 设 $\mathbf{v} = [\mathbf{c} \cdot \mathbf{h} / \mathbf{g}]_q$. 假设 $\|\mathbf{v} \cdot \mathbf{g}\|$ 和 $\|\mathbf{c} \cdot \mathbf{h}\|$ 每个至多 $q/2$, $\langle \mathbf{g} \rangle$ 是素理想, 则 $\mathbf{c}$ 或 $\mathbf{h}$ 属于理想 $\langle \mathbf{g} \rangle$.

引理 17 (引理 4^[11]). 给定 $\sigma = O(n \log n)$, $\sigma^* = q^{5/8}$, 设高斯抽样 $\mathbf{g} \leftarrow D_{\mathbb{Z}^n, \sigma}$ 满足 $I = \langle \mathbf{g} \rangle$ 为素理想, $\mathbf{h} \leftarrow D_{\mathbb{Z}^n, \sigma^*}$ 不属于理想 $\langle \mathbf{g} \rangle$, 则不存在 $0 < \varepsilon < 1/8$ 和 I 的非“0”陪集中元素 $\mathbf{c}$, 满足 $\|\mathbf{c}\| < q^{1/8}$ 且 $\|[\mathbf{c} \cdot \mathbf{h} / \mathbf{g}]_q\| < q^{1-\varepsilon}$.

引理 18. 公共参数产生算法 $\text{par} \leftarrow \text{InstGen}(1^\lambda, 1^\kappa)$ 是一个概率多项式时间算法.

证明. (1) 根据引理 9 中的素数定理知, 不大于 m 的整数中大约有 $m / \ln m$ 个素数. 所以, 随机选择不大于 m 的整数为素数的概率约为 $1 / \ln m$. 因此, 算法能在概率多项式时间产生素数 $q = O(n^{92\kappa})$.

(2) 因为随机元素 $\mathbf{z} \leftarrow U(R_q)$ 不可逆的概率约为 $O(1/q)$, 故易于选择元素 $\mathbf{z}$.

(3) 根据引理 11, 抽样元素 $\mathbf{g} \leftarrow D_{\mathbb{Z}^n, \sigma}$ 为素理想且 $|R/\langle \mathbf{g} \rangle| > 2^\lambda$ 的概率约为 $1/n^c$, 而且当 $l_{-1} = n$ 时, 条件 $\|\mathbf{g}^{-1}\| < l_{-1}$ 以高概率成立. 故算法能在概率多项式时间产生元素 $\mathbf{g}$.

(4) 同理, 可以在概率多项式时间产生元素 $\mathbf{f} \leftarrow D_{\mathbb{Z}^n, \sigma}$.

(5) 易证算法的第 (5)、(6) 两步能够在多项式时间完成. 证毕.

注意: 当维数 n 很大时, 产生素主理想元素 g 是非常耗时的. 然而, 这不会导致新随机化构造实现困难, 因为构造可以选择非素的主理想元素 g . 实际上, Albrecht 等人^[56] 已经优化实现了非素的主理想元素 g 的分级编码方案.

引理 19. 假设 $u \leftarrow \text{Enc}(par, 1, \{d_j\}_{j \in [\tau]})$, 则 u 为隐藏的明文元素 $d = \sum_{j \in [\tau]} d_j e_j$ 的 1-级编码.

证明. 因为 $u \leftarrow \text{Enc}(par, 1, \{d_j\}_{j \in [\tau]})$, 则

$$\begin{aligned} u &= \left[\sum_{j \in [\tau]} d_j y_j \right]_q \\ &= \left[\sum_{j \in [\tau]} d_j (e_j + a_j g) / z \right]_q \\ &= \left[\left(\sum_{j \in [\tau]} d_j e_j + g \sum_{j \in [\tau]} d_j a_j \right) / z \right]_q \\ &= \left[(d + ag) / z \right]_q, \end{aligned}$$

这里 $d = \sum_{j \in [\tau]} d_j e_j$, $a = \sum_{j \in [\tau]} d_j a_j$. 证毕.

引理 20. 假设 $u \leftarrow \text{Add}(par, k, u_1, \dots, u_m)$, 则 u 为 k -级编码; 假设 $u \leftarrow \text{Mul}(par, 1, u_1, \dots, u_k)$, 则 u 为 k -级编码.

证明. 设 m 个 k -级编码 $u_r = \left[\frac{c_r}{z^k} \right]_q$, 则它们和

$$u = \left[\sum_{r=1}^m u_r \right]_q = \left[\frac{\sum_{r=1}^m c_r}{z^k} \right]_q \text{ 是一个 } k\text{-级编码.}$$

设 k 个 1-级编码 $u_r = \left[\frac{c_r}{z} \right]_q$, 则它们积 $u =$

$$\left[\prod_{r=1}^k u_r \right]_q = \left[\frac{\prod_{r=1}^k c_r}{z^k} \right]_q \text{ 是一个 } k\text{-级编码.} \quad \text{证毕.}$$

引理 21. 设 $u = [c/z^\kappa]_q$ 为上述新随机化构造产生的一个 κ -级编码, 则 $\|c\| < q^{1/8}$.

证明. 因为一个 κ -级编码是由 κ 个 1-级编码的乘积产生, 所以可设 u 为 κ 个 1-级编码 $u_r =$

$$[c_r/z]_q \text{ 的乘积 } u = \left[\prod_{r=1}^{\kappa} u_r \right]_q = \left[\prod_{r=1}^{\kappa} c_r / z^\kappa \right].$$

因为 u_r 都是由 1-级编码算法 Enc 产生, 故可设

$$u_r = \text{Enc}(par, 1, \{d_{r,j}\}_{j \in [\tau]}), \quad r \in [\kappa],$$

其中 $d_{r,j} \leftarrow D_{\mathbb{Z}^n, \sigma_1^*}, j \in [\tau]$.

通过整理 u_r 可得, $c_r = \sum_{j \in [\tau]} d_{r,j} x_j$.

由第 3.1.3 节参数设置知, 以概率几乎为 1 有

$$\begin{aligned} \|c_r\| &= \left\| \sum_{j \in [\tau]} d_{r,j} x_j \right\| \\ &\leq 2 \cdot n \cdot \|d_{r,j}\| \cdot \|x_j\| \\ &\leq 2n \cdot \sqrt{n} \sigma_1^* \cdot \sqrt{n} \sigma' \\ &\leq 2n^2 \cdot O(n^{5.5}) \cdot O(n^3) \\ &= O(n^{10.5}). \end{aligned}$$

因此,

$$\begin{aligned} \|c\| &= \left\| \prod_{r=1}^{\kappa} c_r \right\| \\ &\leq n^{\kappa-1} \cdot \prod_{r=1}^{\kappa} \|c_r\| \\ &\leq n^{\kappa-1} \cdot (O(n^{10.5}))^\kappa \\ &< O(n^{11.5})^\kappa \\ &\leq q^{1/8}. \end{aligned}$$

证毕.

引理 22. 设参数设置如第 3.1.3 节定义, 则“0”测试算法 $\text{isZero}(par, \{d_j\}_{j \in [\tau]}, u)$ 能正确判定 κ -级编码 u 中的明文元素是否为“0”.

证明. 给定 $d_j \leftarrow D_{\mathbb{Z}^n, \sigma_1^*}, j \in [\tau]$, 则

$$p_{zt} = \left[\sum_{j \in [\tau]} d_j p_{zt,j} \right]_q = [z^\kappa h / g]_q,$$

其中 $h = \sum_{j \in [\tau]} d_j (e_j f + b_j g)$.

因为 κ -级编码 $u = [c/z^\kappa]_q$, 所以

$$[u \cdot p_{zt}]_q = \left[\frac{c}{z^\kappa} \cdot \frac{z^\kappa h}{g} \right]_q = [h \cdot c / g]_q.$$

现根据 u 中明文元素是否为“0”分别分析如下:

(1) 如果 κ -级编码 u 中明文元素为“0”, 则

$$\|u \cdot p_{zt}\|_q \leq q^{7/8}.$$

因为 u 中的明文元素为“0”, 故 c 属于理想 I , 即

c 能够被 g 整除. 所以, $(c/g) \in R_q$ 与 $(c \cdot g^{-1}) \in \mathbb{K}$ 相同, 即 $[c/g]_q = c \cdot g^{-1}$. 故由 g 抽样选取条件可得

$$\|c \cdot g^{-1}\| \leq n \cdot \|c\| \cdot \|g^{-1}\| < n^2 \cdot \|c\|.$$

又因为

$$\begin{aligned} \|h\| &= \left\| \sum_{j \in [\tau]} d_j (e_j f + b_j g) \right\| \\ &\leq \sum_{j \in [\tau]} \|d_j (e_j f + b_j g)\| \\ &\leq \tau n \cdot \|d_j\| \cdot \|e_j f + b_j g\| \\ &\leq 2n \cdot \sqrt{n} \sigma_1^* \cdot (2 \cdot n \cdot \|b_j\| \cdot \|g\|) \\ &< O(n^7) \cdot (2n \cdot \sqrt{n} \sigma^* \cdot \sqrt{n} \sigma) \\ &= O(q^{5/8} n^{10} \log n), \end{aligned}$$

又由引理 21 知 $\|c\| < q^{1/8}$, 所以

$$\begin{aligned} \|h \cdot c \cdot g^{-1}\| &\leq n \cdot \|h\| \cdot \|c \cdot g^{-1}\| \\ &< n^3 \cdot \|h\| \cdot \|c\| \\ &< q^{7/8}. \end{aligned}$$

因此, $[h \cdot c / g]_q = [h \cdot c \cdot g^{-1}]_q = h \cdot c \cdot g^{-1}$, 即

$$\|u \cdot p_{zt}\|_q = \|h \cdot c / g\|_q \leq \|h \cdot c \cdot g^{-1}\|_q < q^{7/8}.$$

(2) 如果 κ -级编码 u 中明文元素为非“0”, 则

$$\|u \cdot p_{zt}\|_q > q^{7/8}.$$

因为以概率几乎为 1, $h = \sum_{j \in [\tau]} d_j (e_j f + b_j g)$ 不属于理想格 $\langle g \rangle$, 并由引理 21 知 $\|c\| < q^{1/8}$, 故由引理 17 可得 $\|h \cdot c / g\|_q > q^{1-\epsilon}$, 其中 $0 < \epsilon < 1/8$.

所以,

$$\begin{aligned}
\| [u \cdot p_{zt}]_q \|_{\infty} &= \| [h \cdot c/g]_q \|_{\infty} \\
&\geq 1/\sqrt{n} \cdot \| [h \cdot c/g]_q \| \\
&> 1/\sqrt{n} \cdot q^{1-\epsilon} \\
&> q^{7/8}.
\end{aligned}$$

因此,“0”测试算法 isZero 能够正确判断 κ -级编码 u 中明文元素是否为“0”。证毕。

引理 23. 如果两个 κ -级编码 u, u' 中明文元素的陪集相同,则以概率几乎为 1 有

$$\text{Ext}(par, \{d_j\}_{j \in [\tau]}, u) = \text{Ext}(par, \{d_j\}_{j \in [\tau]}, u').$$

证明. 因为同级编码满足加法同态,所以如果两个 κ -级编码 u, u' 中编码的明文元素陪集相同,则 $u - u'$ 将是明文元素“0”的 κ -级编码。

故由引理 22 知 $\| [(u - u') \cdot p_{zt}]_q \|_{\infty} < q^{7/8}$, 其中

$$\begin{aligned}
p_{zt} &= \left[\sum_{j \in [\tau]} d_j p_{zt,j} \right]_q = \left[\frac{hz^{\kappa}}{g} \right]_q, d_j \leftarrow D_{Z^n, \sigma_1^*}, j \in [\tau] \text{ 和} \\
h &= \sum_{j \in [\tau]} d_j (e_j f + b_j g).
\end{aligned}$$

由此可得,提取编码 $v = [u \cdot p_{zt}]_q$ 中每个系数的最有意义的 $(\log q)/8$ 个比特位只与 u 中明文元素的陪集相关,而与具体使用的明文元素代表无关。

所以, $v = [u \cdot p_{zt}]_q$ 和 $v' = [u' \cdot p_{zt}]_q$ 中每个系数的最有意义的 $(\log q)/8$ 个比特位相同。然而,提取编码 v 和 v' 中每个系数的最少意义的 $7(\log q)/8$ 个比特位 (Least Significant Bits, LSB) 并不相同,这些低位不同的元素可能会由于进位不同造成提取比特串不相等。为此,提取算法预留 λ 位错误冗余量,即每个系数中仅提取 l 个比特,以保证提取比特串不相等的概率约为 $O(2^{-\lambda})$ 。

因此,如果 κ -级编码 u, u' 中的明文元素陪集相同,则对于 u, u' , 提取算法产生的提取比特串相等的概率为 $1 - O(2^{-\lambda})$ 。证毕。

3.2 非对称变种

本节给出新随机化构造的非对称变种。不同于 GGH13 的非对称变种^[11], 本文非对称变种重新设计了“0”测试参数,使得其不仅是“0”测试参数,也是与其对应的 1-级编码中的隐藏 0-级编码(即明文元素)的特殊编码。而且,在某种意义上,本文非对称构造也是多线性锯齿谜 (Multilinear Jigsaw Puzzles, MJP)^[15] 的一种变种。然而,本文非对称构造也不同于 MJP 构造,即 MJP 构造中的“0”测试参数仅具有“0”测试参数功能,而本文中的“0”测试参数还具有隐藏明文的编码功能。因此,使用本文非对称构造能够产生隐藏明文的 1-级编码,并且由 1-级编码 y_j 与“0”测试参数 $p_{zt,j}$ 的对应关系,可以计算获得与新产生 1-级编码对应的“0”测试参数,使其是隐藏明文与“0”测试参数的乘积,进而使得该隐藏明文可以使

用,而在 MJP 构造中无法产生这种可用隐藏明文的 1-级编码。

在非对称变种构造中,编码级数将使用索引集表示。如果索引集中仅有一个元素,则称其为基本索引集。

同样,本文非对称构造变种也使用参数符号 $\lambda, \kappa, q, n, \sigma, \sigma', \sigma_1^*, \sigma^*, \tau, l_{-1}, l$ 。

非对称变种具体构造如下:

公共参数产生算法 $vpar \leftarrow \text{vInstGen}(1^\lambda, 1^\kappa)$:

(1) 设置 $N = \kappa + 1$;

(2) 选择足够大的素数 q ;

(3) 抽样选择素理想元素 $g \leftarrow D_{Z^n, \sigma}$, 满足在 $\mathbb{K}$ 上有 $\|g\| \leq \sqrt{n}\sigma$ 和 $\|g^{-1}\| < l_{-1}$, 记 g 生成的主理想 $I = \langle g \rangle \subset R$;

(4) 抽样选择素理想元素 $f \leftarrow D_{Z^n, \sigma}$, 满足在 $\mathbb{K}$ 上有 $\|f\| \leq \sqrt{n}\sigma$ 和 $\|f^{-1}\| \leq n^2$;

(5) 对于 $i \in [N], j \in [\tau]$:

(5.1) 抽样选择 $x_{i,j} \leftarrow D_{Z^n, \sigma'}$;

(5.2) 计算 $e_{i,j} = [x_{i,j}]_g, a_{i,j} = (x_{i,j} - e_{i,j})/g$;

(5.3) 抽样选择 $b_{i,j} \leftarrow D_{Z^n, \sigma^*}$;

(6) 随机抽样 $z_i \leftarrow U(R_q), i \in [N]$, 满足条件 $z_i^{-1} \in R_q$;

(7) 设置 $z_i^* = \frac{\prod_{t=1}^N z_t}{z_i}, i \in [N]$;

(8) 对于 $i \in [N], j \in [\tau]$, 设置

$$y_{(i),j} = \left[\frac{x_{i,j}}{z_i} \right]_q, p_{(i),j} = \left[\frac{z_i^* (e_{i,j} f + b_{i,j} g)}{g} \right]_q;$$

(9) 输出公共参数 $vpar = \{vpar_i, i \in [N]\}$, 其中 $vpar_i = \{q, \{y_{(i),j}, p_{(i),j}\}, j \in [\tau]\}$ 。

索引集 $\{i\}$ -编码算法 $u_{(i)} \leftarrow \text{vEnc}(vpar, i, \{d_j\}_{j \in [\tau]})$:

给定 $d_j \leftarrow D_{Z^n, \sigma_1^*}, j \in [\tau]$, 索引集 $\{i\}$ -编码为

$$u_{(i)} = \left[\sum_{j=1}^{\tau} (d_j \cdot y_{(i),j}) \right]_q = \left[\frac{d_{(i)} + a_{(i)} g}{z_i} \right]_q,$$

其中 $d_{(i)} = \sum_{j=1}^{\tau} (d_j \cdot e_{i,j}), a_{(i)} = \sum_{j=1}^{\tau} (d_j \cdot a_{i,j})$ 。

编码加法算法 $u_S \leftarrow \text{vAdd}(vpar, u_{S_1}, \dots, u_{S_m})$:

给定 m 个索引集 S -编码 $u_{S,r}, r \in [m], S \subset [N]$,

则它们的和 $u_S = \left[\sum_{r=1}^m u_{S,r} \right]_q$ 是索引集 S -编码。

编码乘法算法 $u_{S_1 \cup S_2} \leftarrow \text{vMul}(vpar, u_{S_1}, u_{S_2})$:

给定索引集 S_1 -编码 u_{S_1} 和索引集 S_2 -编码 u_{S_2} , 满足 $S_1, S_2 \subset [N]$ 且 $S_1 \cap S_2 = \emptyset$, 则它们的积 $u_S = [u_{S_1} \cdot u_{S_2}]_q$ 是索引集 S -编码, 其中 $S = S_1 \cup S_2$ 。

对于 $i \in [N]$, 设索引集 $S_i^* = [N] - \{i\}$ 。

“0”测试算法 $\text{visZero}(vpar, \{d_j\}_{j \in [\tau]}, u_{S_i^*})$:

(1) 给定 $d_j \leftarrow D_{\mathbb{Z}^n, \sigma_1^*}, j \in [\tau]$, 计算产生索引集

$$\{i\} \text{ 对应的“0”测试参数 } p_{(i)} = \left[\sum_{j=1}^{\tau} d_j \cdot p_{(i), j} \right]_q.$$

(2) 给定索引集 S_i^* -编码 $u_{S_i^*}$, 计算“0”测试函数

visZero 以判定索引集 S_i^* -编码 $u_{S_i^*}$ 中明文元素是否为“0”, 即

$$\text{visZero}(vpar, \{d_j\}_{j \in [\tau]}, u_{S_i^*}) = \begin{cases} 1, & \text{如果 } \|[u_{S_i^*} \cdot p_{(i)}]_q\| \leq q^{7/8} \\ 0, & \text{否则} \end{cases}.$$

提取算法 $w \leftarrow \text{vExt}(vpar, i, \{d_j\}_{j \in [\tau]}, u_{S_i^*})$:

(1) 给定 $d_j \leftarrow D_{\mathbb{Z}^n, \sigma_1^*}, j \in [\tau]$, 计算产生索引集

$$\{i\} \text{ 对应的“0”测试参数 } p_{(i)} = \left[\sum_{j=1}^{\tau} d_j \cdot p_{(i), j} \right]_q.$$

(2) 给定索引集 S_i^* -编码 $u_{S_i^*}$, 计算提取编码 $v_{(i)} =$

$$[u_{S_i^*} \cdot p_{(i)}]_q.$$

(3) 从 $v_{(i)}$ 的每个系数中提取 $l = (\log q)/8 - \lambda$ 个最有意义的比特位, 输出提取比特串 w , 即

$$w = \text{vExt}(vpar, i, \{d_j\}_{j \in [\tau]}, u_{S_i^*}) = \text{MSB}_l(v_{(i)}).$$

评论 2. (1) 我们将非对称变种构造的公共参数 $vpar$ 写成 $vpar_i$ 形式, 这是为了证明非对称变种构造完全避免“0”化攻击的可能性.

(2) 在非对称构造变种中公共参数仅包含了基本索引集的编码和与其对应的“0”测试参数, 故仅能产生对应于基本索引集的可用隐藏明文元素的编码. 如果需要产生索引集 $S \subseteq [N]$ 的编码, 则需要提供索引集 S 的编码和与其对应的“0”测试参数, 这种情况与评论 1(3) 类似.

(3) 非对称构造变种的参数大小设置与第 3.1.3 节相同. 因为除了使用不同随机元素 z_i 以表示不同基本索引集的编码外, 非对称变种与新随机化对称构造完全相同.

(4) 类似于第 3.1.4 节, 易于证明非对称变种构造的正确性.

4 已知攻击分析

由于目前我们还不能从理论上证明本文提出的新随机化构造的安全性, 也不能将其归约到其它经典困难问题. 因此, 本节将从研究多线性映射的现有攻击方法入手, 分析现有已知攻击都不能用于攻击新随机化构造.

下面第 4.1 节给出容易计算量攻击分析; 第 4.2~4.3 节分析基于“0”的低级编码攻击方法不能用于攻击新随机化构造; 第 4.4~4.7 节分析基于非“0”的低级编码攻击方法也不能用于攻击新随机化构造.

4.1 容易计算量攻击分析

本节根据构造的公共参数产生一些容易计算量, 并且提出基于容易计算量的可能攻击以及相应的反制措施.

4.1.1 容易计算量

与 GGH13 构造类似, 新随机化构造同样存在易于计算的量, 但是不同于 GGH13, 攻击者通过这些计算量无法得到构造中秘密理想元素的格基.

给定新随机化构造的公共参数 par , 攻击者能够通过 1-级编码与“0”测试参数的交叉乘积 $(y_1 \cdot p_{zt,2} - y_2 \cdot p_{zt,1})$ 计算产生元素 v 如下:

$$v = [(d_1 y_1 + d_2 y_2)^{\kappa-1} (y_1 p_{zt,2} - y_2 p_{zt,1})]_q \\ = [(d_1 (e_1 + a_1 g) + d_2 (e_2 + a_2 g))^{\kappa-1} \cdot w]_q,$$

其中 $w = e_1 b_2 + e_2 a_1 f + a_1 b_2 g - e_2 b_1 - e_1 a_2 f - a_2 b_1 g$.

根据第 3.1.3 节的参数设置, 易于验证元素 v 并不是模 q 归约的 (即 $[v]_q = v$).

利用这种非模 q 归约的元素 v , 目前没有发现攻击者能够在经典计算机上使用多项式时间攻击新随机化构造. 这是因为: (1) 虽然攻击者通过 y_1, y_2 的不同组合 (d_1, d_2) 能够计算获得主理想元素 $e_j + a_j g, j \in [\tau]$ 的格基, 但是目前在经典计算机上并不存在有效算法^[11] 计算求解理想元素 $e_j + a_j g$; (2) 目前没有发现攻击者能够通过公共参数计算获得秘密理想元素 g 的格基. 由于现有攻击 GGH13 构造的方法^[22,24] 都需要能够获得理想格 $\langle g \rangle$ 的基或 $\langle g \rangle$ 中一些范数较小的元素, 所以这些攻击方法都不适用于新随机化构造.

4.1.2 基于容易计算量的攻击分析

对于新随机化构造, 我们提出基于容易计算量的量子多项式时间算法^[57-58] 或经典次指数时间算法^[59] 的可能攻击. 据我们所知, 本节的可能攻击方法是新的.

根据 4.1.1 节分析, 攻击者能够使用不同组合 (d_1, d_2) 产生非模 q 归约的一系列元素 v_i , 并通过量子多项式时间算法或经典次指数时间算法计算得到理想格 $\langle e_j + a_j g \rangle, j \in [\tau]$ 的“短”的生成元. 然而, 目前这些算法^[57-59] 并不能保证计算得到元素 $e_j + a_j g$, 而是以高概率为形如 $\delta \cdot (e_j + a_j g)$ 的元素, 其中 δ 为环 R 中的单位元, 且其系数向量的范数也较小.

为实施攻击, 我们需要假设单位元 δ 的逆元 δ^{-1} 的范数 $\|\delta^{-1}\|$ 较小, 如为 $n^{O(1)}$ 或 $O(q^{3/8})$. 因为现有算法^[58-60] 仅能保证主理想的生成元的范数 $\|\delta \cdot (e_j + a_j g)\|$ 和单位元 δ 的范数 $\|\delta\|$ 较小, 而对于其逆元 δ^{-1} 的范数大小则没有任何保证. 虽然由 δ 为 R 的单位元可得元素 $\delta^{-1} \in R$, 但目前并不知道估算范数 $\|\delta^{-1}\|$ 大小的方法. 我们注意到如果范数

$\|\delta^{-1}\|$ 较大, 则本节攻击方法并不可行。

给定公共参数 par , 不失一般性, 假设攻击者使用算法^[57-59] 计算得到理想格 $\langle e_j + a_j g \rangle, j \in [\tau]$ 的“短”的生成元为 $q_j = \delta_j \cdot (e_j + a_j g)$, 其中 δ_j 为环 R 中单位元。而且, 我们假设范数 $\|q_j\|$ 、 $\|\delta_j\|$ 和 $\|\delta_j^{-1}\|$ 都较小, 为符号简单, 我们记 $\delta = \delta_1, \beta = \delta^{-1}$ 。

根据上述假设条件, 攻击的具体步骤如下:

(1) 计算等价随机元素 z'

由 $y_j = [x_j/z]_q = [(e_j + a_j g)/z]_q$, 计算可得

$$z' = p_1/y_1 = [z\delta]_q.$$

(2) 产生新的公共参数 par'

由公共参数 par , 计算可得

$$y'_j = [y_j \cdot z']_q = x_j \delta,$$

$$p'_{zt,j} = [p_{zt,j} / (z')^\kappa]_q = [y'_j \cdot s + b'_j]_q,$$

其中 $s = f/g \cdot \beta^{\kappa+1}$, $b'_j = (b_j - a_j f) \cdot \beta^\kappa$ 。

(3) 产生等价提取元素 s'

由参数设置和假设条件知, y'_j 为非模 q 的元素, 因为范数 $\|x_j\|$ 和 $\|\delta\|$ 都较小。

同理, b'_j 也为非模 q 的元素, 因为范数 $\|b_j - a_j f\|$ 和 $\|\beta\|$ 也较小。

所以, 通过交叉乘积可得

$$c = [y'_1 \cdot p'_{zt,2} - y'_2 \cdot p'_{zt,1}]_q = y'_1 \cdot b'_2 - y'_2 \cdot b'_1.$$

因为 $\|y'_j\|$ 和 $\|b'_j\|$ 较小, 可得 c 为非模 q 的元素。

注意: 这里假设条件成立是攻击成功关键。否则, 如果 $\|\beta\| > O(q^{3/8})$, 则 c 以高概率为模 q 归约的元素, 即 $\|c\| \approx q$ 。

又假设元素 y'_1, y'_2 互素, 则有

$$c' = (y'_1)^{-1} \bmod (y'_2) \cdot c = b'_2 \bmod (y'_2).$$

所以, $r = (b'_2 - c')/y'_2 \in R$, 并且范数 $\|r\|$ 较小。

因此, 我们可得

$$s' = [(p'_{zt,2} - c')/y'_2]_q = [s + r]_q.$$

(4) 计算产生提取比特串

给定 par 和 1-级编码 $u_i = [c_i/z]_q, i \in [\kappa+1]$,

则等价提取编码可计算如下:

$$\begin{aligned} v' &= [s' \cdot \prod_{i=1}^{\kappa+1} (u_i \cdot z')]_q \\ &= [(s+r) \cdot \delta^{\kappa+1} \cdot \prod_{i=1}^{\kappa+1} c_i]_q \\ &= [f/g \cdot \beta^{\kappa+1} \cdot \delta^{\kappa+1} \cdot \prod_{i=1}^{\kappa+1} c_i + r']_q \\ &= [f/g \cdot \prod_{i=1}^{\kappa+1} c_i + r']_q, \end{aligned}$$

其中 $r' = r \cdot \delta^{\kappa+1} \cdot \prod_{i=1}^{\kappa+1} c_i$, 并且 $\|r'\|$ 较小。同样, 这里使用假设条件 $\|\delta\|$ 较小。

另一方面, 如果设 p_{zt} 为对应于 1-级编码 $u_{\kappa+1}$ 的“0”测试参数, 则提取编码可计算为

$$v = [p_{zt} \cdot \prod_{i=1}^{\kappa} u_i]_q = [f/g \cdot \prod_{i=1}^{\kappa+1} c_i + e']_q,$$

其中元素 e' 的范数 $\|e'\|$ 较小。

所以, 提取编码 v 和 v' 的提取比特串 $MSB_l(v)$ 和 $MSB_l(v')$ 以高概率相同。

4.1.3 反制措施

虽然目前基于容易计算量的攻击依赖于假设条件, 但是上述攻击分析表明存在这种攻击的可能性。为避免这种潜在攻击, 本文提出如下二个反制措施。

(1) 基于 Kilian 随机矩阵方法^[60] 的反制措施

通过容易计算量的攻击分析可以看出, 攻击关键在于容易计算量中存在主理想格问题。而目前量子多项式时间算法^[57-58] 或次指数时间算法^[59] 能够计算“短”的主理想格的生成元。另一方面, 由下面第 5.2 节分析可知, 基于噪声的多线性映射又不可能完全避免“0”化攻击问题, 即基于噪声的构造中一定存在某种容易计算量。

因此, 为抗上述攻击, 改进构造中存在的容易计算量需要能够避免产生主理想格问题。所以, 本节通过使用 Kilian 随机矩阵, 使得攻击者基于改进构造的容易计算量不再能够直接产生上述主理想格问题, 从而避免上述攻击算法^[57-59]。

我们注意到第 4.4~4.5 节的基于子域格攻击也利用了主理想格问题来攻击新随机化构造。因此, 本节反制措施也能适用于抗子域格攻击。类似地, 基于 Kilian 随机矩阵反制措施能够直接用于第 6 节无可信安装的多线性映射构造。为叙述简单, 下面不再赘述。

首先使用公共参数产生算法 $\text{InstGen}(1^\lambda, 1^\kappa)$ 产生公共参数 $par = \{n, q, \{y_j, p_{zt,j}\}_{j \in [\tau]}\}$, 并将其重新标号为 $par = \{n, q, \{y_{i_1, i_2, j}, p_{zt, i_1, i_2, j}\}_{i_1 \in [2], i_2 \in [2], j \in [\tau]}\}$ 。

注意: 这里产生公共参数 par 时, 除了“0”测试参数中噪声抽样参数设置为 $\sigma^* = O(n^3)$, 其它参数设置与 3.1.3 节相同。

新随机化构造可以改进如下:

公共参数产生算法:

设 par 为新随机化构造产生的公共参数。

① 抽样选择向量 $s, t \in R^2$, 其分量 s_i, t_i 满足

$$s_i, t_i \leftarrow D_{\mathbb{Z}^n, q^{5/16}}, i \in [2];$$

//注意: 这里向量中分量为 R 中元素, 故其分量仍使用黑体表示。

② 选择随机可逆元素 $z_1, z_2 \in R_q$;

③ 选择随机可逆矩阵 $T \in R_q^{2 \times 2}$;

④ 对于 $j \in [\tau]$, 计算产生 1-级编码

$$Y_j = \left[T \begin{pmatrix} y_{1,1,j} & y_{1,2,j} \\ y_{2,1,j} & y_{2,2,j} \end{pmatrix} T^{-1} \right]_q = [T(X_j/z)T^{-1}]_q,$$

$$\text{其中 } \mathbf{X}_j = \begin{bmatrix} \mathbf{x}_{1,1,j} & \mathbf{x}_{1,2,j} \\ \mathbf{x}_{2,1,j} & \mathbf{x}_{2,2,j} \end{bmatrix}.$$

⑤ 计算产生编码 $\mathbf{Y}_j$ 对应的“0”测试参数

$$\mathbf{P}_{zt,j} = \left[\mathbf{T} \begin{bmatrix} \mathbf{p}_{zt,1,1,j} & \mathbf{p}_{zt,1,2,j} \\ \mathbf{p}_{zt,2,1,j} & \mathbf{p}_{zt,2,2,j} \end{bmatrix} \mathbf{T}^{-1} \cdot \mathbf{z}_2 \right]_q;$$

⑥ 计算产生两端标签向量

$$\bar{\mathbf{s}}^T = \mathbf{s}^T \mathbf{T}^{-1} \mathbf{z}_1, \bar{\mathbf{t}} = \mathbf{T} \mathbf{t} / (\mathbf{z}_1 \mathbf{z}_2);$$

⑦ 输出 $\text{par}' = \{n, q, \bar{\mathbf{s}}, \bar{\mathbf{t}}, \{\mathbf{Y}_j, \mathbf{P}_{zt,j}\}_{j \in [t]}\}$.

易于自适应给出改进的其它算法, 这里略去.

评论 3. (1) 由于矩阵不满足交换律, 所以在使用改进构造产生 MPKE 协议时, 需要根据所有方产生的 1-级编码 $\mathbf{U}_i, i \in [\kappa+1]$ 确定提取比特串的计算顺序, 或事先约定计算顺序. 不失一般性, 设 $1, 2, \dots, \kappa+1$ 为提取比特串的计算顺序, 则第 $i (i \in [\kappa+1])$ 方的提取比特串计算为

$$\omega_i = \text{MSB}_l \left(\left[\bar{\mathbf{s}}^T \left(\prod_{t=1}^{i-1} \mathbf{U}_t \cdot \mathbf{P}_{zt,(i)} \cdot \prod_{t=i+1}^{\kappa+1} \mathbf{U}_t \right) \bar{\mathbf{t}} \right]_q \right),$$

其中 $\mathbf{P}_{zt,(i)}$ 为对应于 1-级编码 $\mathbf{U}_i$ 的“0”测试参数. 易于验证, 所有方产生的提取比特串 $\omega_i, i \in [\kappa+1]$ 以高概率相同.

(2) 引入随机元素 $\mathbf{z}_1, \mathbf{z}_2$ 绑定了编码与“0”测试参数的乘积计算方式, 同时也限制了攻击者能够产生的容易计算量的计算方式.

(3) 通过交叉乘积得到的容易计算量不再直接包含构造中使用的主理想格作为乘积因子. 易于看出, 构造中交叉乘积得到的非模 q 归约的元素形为

$$\mathbf{v} = [\bar{\mathbf{s}}^T (\mathbf{Y}_1 \mathbf{P}_{zt,(2)} - \mathbf{P}_{zt,(1)} \mathbf{Y}_2) \mathbf{Y}_j^{\kappa-1} \bar{\mathbf{t}}]_q \\ = \mathbf{s}^T (\mathbf{X}_1 \mathbf{B}_{(2)} - \mathbf{B}_{(1)} \mathbf{X}_2) \mathbf{X}_j^{\kappa-1} \mathbf{t}.$$

因为矩阵 $\mathbf{X}_1, \mathbf{X}_2, \mathbf{B}_{(1)}, \mathbf{B}_{(2)}$ 和向量 $\mathbf{s}, \mathbf{t}$ 中每个分量都是使用高斯抽样算法产生的, 相互之间并没有直接可以利用的关系, 所以元素 $\mathbf{v}$ 不再直接包含构造中使用的主理想元素 $\mathbf{x}_j = \mathbf{e}_j + \mathbf{a}_j \mathbf{g}$ 作为乘积因子. 因此, 改进构造去除了基于容易计算量产生的主理想格问题, 也避免了基于容易计算量对构造的潜在攻击.

(4) 改进构造在产生公共参数 par' 时将抽样参数设置为 $\sigma^* = O(n^3)$, 而在新随机化构造中则为 $\sigma^* = q^{5/8}$. 实际上, 为避免第 4.4~4.5 节的子域格攻击^[26-27], 改进构造在抽样元素 $\mathbf{s}_i, \mathbf{t}_i \leftarrow D_{\mathbb{Z}^n, q^{5/16}}$ 时使用高斯参数 $q^{5/16}$ 能够起到新随机化构造的“0”测试参数中噪声抽样参数 σ^* 的相同作用, 因为去除随机矩阵 $\mathbf{T}$ 的任何运算所产生元素的范数至少为 $\|\mathbf{s}^T \cdot \mathbf{t}\| = O(q^{5/8})$. 注意: 子域格攻击实际上针对形如 $[\bar{\mathbf{s}}^T \mathbf{Y}_j \bar{\mathbf{t}}]_q = [\bar{\mathbf{s}}^T \mathbf{X}_j \mathbf{t} / (\mathbf{z}_1 \cdot \mathbf{z}_2)]_q$ 的元素展开攻击, 这一点不同于使用交叉乘积产生的容易计算量元素.

(2) 基于 NTRU 型素数域^[61]的反制措施

量子多项式时间攻击算法^[57-58]仅能计算分领域中主理想格的“短”的生成元, 目前该算法并不能扩展到一般域上. 因此, 本文也可使用 NTRU 型素数域^[61]作为改进的反制措施.

不失一般性, 选取域 $\mathbb{K} = \mathbb{Q}[x] / \langle x^n + x + 1 \rangle$, 满足条件 n 为素数, $x^n + x + 1$ 为 $\mathbb{Q}$ 上不可约多项式, Galois 群同构到置换群 S_n , 并且 $R = \mathbb{Z}_q[x] / \langle x^n + x + 1 \rangle$ 是有限域. 对于素数 $n = 3k + 1$ 和“随机”素数 q , Osada^[62]证明了选取参数满足上述条件的概率约为 $1/n$. 最近, Bernstein 等人^[61]通过引入 NTRU 型素数研究了这种有限域在密码学上的应用. 为简单, 这里略去改进方案在素数域 $\mathbb{K} = \mathbb{Q}[x] / \langle x^n + x + 1 \rangle$ 中的参数选取、计算优化等问题^[61-62].

4.2 Hu-Jia 攻击分析

本节分析证明 Hu-Jia 攻击方法^[22]并不能用于攻击新随机化的多线性映射构造.

4.2.1 Hu-Jia 攻击方法概述

对于 GGH13 构造, Hu-Jia 攻击方法包括 3 步: 第 1 步计算产生一个给定 1-级编码所对应的等价明文元素; 第 2 步使用多个等价明文元素, 计算产生它们积对应的等价密钥; 第 3 步修改 GGH13 的编码和解码算法, 计算产生基于 GGH13 的多方共享密钥协议 MPKE.

因为第一步是 Hu-Jia 攻击成功的关键, 本节将其细化为 4 小步, 具体工作原理如下:

(1) 产生特殊的解码元素

不失一般性, 设 $\text{par}_0 = \{q, \mathbf{y}, \{\mathbf{x}_i\}_{i=1,2}, \mathbf{p}_{zt}\}$ 为 GGH13 构造的公共参数, 其中 $\mathbf{y} = [(1 + \mathbf{s}\mathbf{g})/\mathbf{z}]_q$, $\mathbf{x}_i = [\mathbf{s}_i \mathbf{g} / \mathbf{z}]_q$, $\mathbf{p}_{zt} = [\mathbf{h}\mathbf{z}^\kappa / \mathbf{g}]_q$, $\mathbf{g} \leftarrow D_{\mathbb{Z}^n, \sigma}$, $\mathbf{s}, \mathbf{s}_i \leftarrow D_{\mathbb{Z}^n, \sigma'}$, $\mathbf{h} \leftarrow D_{\mathbb{Z}^n, \sqrt{q}}$ 和 $\mathbf{z} \leftarrow U(R_q)$.

给定公共参数 par_0 , 我们能够计算得到特殊的解码 $\{\mathbf{y}^{(1)}, \mathbf{x}^{(i)}, i=1, 2\}$, 其中

$$\mathbf{y}^{(1)} = [\mathbf{p}_{zt} \cdot \mathbf{y}^{\kappa-1} \cdot \mathbf{x}_1]_q = \mathbf{h}(1 + \mathbf{s}\mathbf{g})^{\kappa-1} \mathbf{s}_1,$$

$$\mathbf{x}^{(i)} = [\mathbf{p}_{zt} \cdot \mathbf{y}^{\kappa-2} \cdot \mathbf{x}_i \cdot \mathbf{x}_1]_q = \mathbf{h}(1 + \mathbf{s}\mathbf{g})^{\kappa-2} (\mathbf{s}_i \mathbf{g}) \mathbf{s}_1.$$

注意: ① 元素 $\mathbf{y}^{(1)}, \mathbf{x}^{(i)}$ 都没有发生模 q 操作, 即它们都是非模 q 的环元素; ② 虽然 GGH13 构造^[11]的公共参数中包含了 τ 个明文元素“0”的 1-级编码 $\mathbf{x}_i$, 但是根据引理 13, Langlois, Stehlé 和 Steinfeld 证明 GGH13 构造仅需要 2 个 $\mathbf{x}_i, i=1, 2$, 其它 $\mathbf{x}_i$ 都可以由 $\{\mathbf{x}_1, \mathbf{x}_2\}$ 生成.

(2) 转换 1-级编码到特殊解码方程形式

给定有噪声的 1-级编码

$$\mathbf{u} = [\mathbf{d} \cdot \mathbf{y} + \mathbf{r}_1 \cdot \mathbf{x}_1 + \mathbf{r}_2 \cdot \mathbf{x}_2]_q,$$

其中秘密明文元素 $\mathbf{d}$ 为私钥, $\mathbf{r}_1, \mathbf{r}_2$ 为随机噪声.

计算特殊的解码

$$\begin{aligned} v &= [p_{zt} \cdot y^{\kappa-2} \cdot u \cdot x_1]_q \\ &= d \cdot y^{(1)} + r_1 \cdot x^{(1)} + r_2 \cdot x^{(2)}. \end{aligned}$$

因为元素 v 没有发生模 q 操作, 计算可得

$$v \bmod y^{(1)} = (r_1 x^{(1)} \bmod y^{(1)} + r_2 x^{(2)} \bmod y^{(1)}) \bmod y^{(1)}.$$

(3) 求解特殊解码方程

因为 $v \bmod y^{(1)}$ 和 $\{x^{(1)} \bmod y^{(1)}, x^{(2)} \bmod y^{(1)}\}$ 已知, 计算可得 $v' \in \langle x^{(1)}, x^{(2)} \rangle$, 满足条件 $(v - v') \bmod y^{(1)} = 0$. 记 $v' = r'_1 x^{(1)} + r'_2 x^{(2)}$, 这里 v' 的具体计算方法可参考附录 A^[22].

注意上述元素 r'_1, r'_2 的范数 $\|r'_1\|, \|r'_2\|$ 大小无限制.

(4) 产生 1-级编码对应的等价密钥

在数域 $\mathbb{K}$ 中计算得到 $d^{(0)} = (v - v')/y^{(1)}$, 商 $d^{(0)}$ 为 R 中元素. 通过整理可得

$$\begin{aligned} d^{(0)} &= (v - v')/y^{(1)} \\ &= d + ((r_1 - r'_1)s_1 + (r_2 - r'_2)s_2)g/(1 + sg). \end{aligned}$$

又因 g 和 $1 + sg$ 互素, 故 $d - d^{(0)} \in \langle g \rangle$. 所以 $d^{(0)}$ 是 d 的一个等价密钥. 虽然 $\|d^{(0)}\|$ 并不是一个小整数, 但 Hu-Jia 攻击^[22]通过 $x^{(i)}$ 能够控制等价密钥积的大小, 因为 $x^{(i)}$ 属于理想 $\langle g \rangle$.

4.2.2 新构造抗 Hu-Jia 攻击

为分析新随机化构造避免了 Hu-Jia 攻击, 本节对新随机化构造实施上述 Hu-Jia 攻击.

(1) 产生特殊的解码元素

通过分析 Hu-Jia 攻击过程的第一步可以发现, 攻击关键是得到特殊解码 $\{y^{(1)}, x^{(i)}, i=1, 2\}$, 其中 $x^{(i)}$ 属于理想格 $\langle g \rangle$.

因为新随机化构造的公共参数 par 没有包含“0”的 1-级编码 x_i , 无法通过 Hu-Jia 攻击方法计算得到 $x^{(i)}$.

由第 4.1 节分析可知, 新随机化构造中只有非“0”的 1-级编码与“0”测试参数交叉乘积才能得到不是模 q 归约的量. 所以, 使用交叉乘积可得

$$v = (r_1 y_1 + r_2 y_2)^{\kappa-1} (y_1 p_{zt,2} - y_2 p_{zt,1}) \bmod q.$$

易于验证, 元素 v 并属于主理想 $\langle g \rangle$, 其中 r_1, r_2 为高斯抽样选择的范数较小的环元素.

不失一般性, 使用 par 计算特殊解码如下:

$$\begin{aligned} y^{(1)} &= [(y_1)^{\kappa-1} (y_1 p_{zt,2} - y_2 p_{zt,1})]_q, \\ y^{(2)} &= [(y_1)^{\kappa-2} y_2 (y_1 p_{zt,2} - y_2 p_{zt,1})]_q. \end{aligned}$$

这里元素 $y^{(1)}, y^{(2)}$ 都没有发生模 q 操作, 即它们都是非模 q 的环元素.

(2) 转换 1-级编码到特殊解码方程形式

假定使用 y_1, y_2 产生的 1-级编码为 u , 则

$$u = [d_1 \cdot y_1 + d_2 \cdot y_2]_q,$$

其中秘密明文元素 $d_j \leftarrow D_{z'', \sigma_1^*}, j \in [2]$ 为私钥.

计算产生特殊解码方程

$$\begin{aligned} v &= [(y_1)^{\kappa-2} \cdot u \cdot (y_1 p_{zt,2} - y_2 p_{zt,1})]_q \\ &= d_1 \cdot y^{(1)} + d_2 \cdot y^{(2)}. \end{aligned}$$

(3) 求解特殊解码方程

因为 v 并不是模 q 归约的, 计算可得

$$v \bmod y^{(1)} = (d_2 y^{(2)}) \bmod y^{(1)}.$$

但是 $(d_2 y^{(2)}) \bmod y^{(1)} \neq d_2 y^{(2)}$. 因此, 我们并不能直接由 $(v - (v \bmod y^{(1)}))/y^{(1)}$ 计算得到 d_1 , 同样也不能计算获得 d_2 .

虽然使用 Hu-Jia 攻击第 1 步中(3)能够计算得到 d'_1, d'_2 满足条件 $v = d'_1 y^{(1)} + d'_2 y^{(2)}$, 但是目前无法计算得到满足条件 $\|d'_1\| \ll q^{3/8}, \|d'_2\| \ll q^{3/8}$ 的 d'_1, d'_2 . 这是因为计算求解的 d'_1, d'_2 将用于产生对应于 1-级编码 u 的“0”测试参数 $p_{zt} = [d'_1 \cdot p_{zt,1} + d'_2 \cdot p_{zt,2}]_q$.

给定 $y^{(1)}, y^{(2)}$ 和 $v = d_1 y^{(1)} + d_2 y^{(2)}$, 目前无有效格归约方法能够计算求解元素 d_1 和 d_2 . 因为给定 $y^{(1)}, y^{(2)}$ 和 v , 可以产生格

$$L_1 = \begin{bmatrix} -v \\ Rot(y^{(1)}) \\ Rot(y^{(2)}) \end{bmatrix} \text{ 或 } L_2 = \begin{bmatrix} -v & & \\ Rot(y^{(1)}) & I_n & \\ Rot(y^{(2)}) & & I_n \end{bmatrix},$$

其中 I_n 为 $n \times n$ 维单位矩阵.

由 3.1.3 节参数设置知, 对于格 L_1, L_2 调用格归约算法^[55,63]并不能得到元素 d_1 和 d_2 . 而且目前也无有效格归约算法计算得到 $d'_j, j \in [2]$, 满足条件 $v = d'_1 y^{(1)} + d'_2 y^{(2)}$ 和 $\|d'_j\| \ll q^{3/8}$.

因此, 针对新随机化构造, 无法有效实施 Hu-Jia 攻击的第一步中(3)和(4), 即无法产生 1-级编码 u 对应的等价密钥. 所以, 使用 Hu-Jia 攻击方法无法得到基于新随机化构造的协议 MPKE 的等价密钥.

综上, Hu-Jia 攻击方法^[22]并不能用于攻击新随机化构造.

原因分析: Hu-Jia 攻击 GGH13 构造成功的原因在于: 通过公共参数中“0”元素的编码产生了对应于明文元素“0”的特殊解码 $x^{(i)}$. 然而, 在新随机化构造中, 攻击者无法通过公共参数计算得到对应于明文元素“0”的特殊解码 $x^{(i)}$.

4.3 Brakerski 等人的攻击分析

4.3.1 Brakerski 等人的攻击概述

GGH13 构造存在“0”化攻击问题^[11,22]. 这是因为 GGH13 构造的“0”测试函数是线性的, 且公共参数中包含“0”的 1-级编码.

为避免“0”化攻击, Halevi^[25]使用非线性“0”测试函数以替换 GGH13 构造中的线性“0”测试函数, 给出了 GGH13 构造的一个变种 GHL15. GHL15 构造除了使用非线性“0”测试函数外, 其它算法与 GGH13 构造一样.

GHL15 构造的二次“0”测试函数: 给定任何编码 $\mathbf{u} = \sum_{i=0}^{n-1} u_i x^i \in R_q$, 系数向量记为 $\vec{\mathbf{u}} = (u_0, \dots, u_{n-1}) \in \mathbb{Z}_q^n$, 则 GHL15 构造中“0”测试函数是二次多项式函数 $f: \mathbb{Z}_q^n \rightarrow \mathbb{Z}_q$, 满足 $|[f(\vec{\mathbf{u}})]_q| < q^{3/4}$ 当且仅当 $\mathbf{u}$ 是明文元素“0”的 κ -级编码。

定义 $f(\vec{\mathbf{u}}) = \left[\sum_{i,j} \alpha_{i,j} \cdot v_i(\vec{\mathbf{u}}) \cdot v_j(\vec{\mathbf{u}}) \right]_q$, 其中 $\alpha_{i,j} \in \mathbb{Z}$ 是小的 (如 $|\alpha_{i,j}| < q^{1/4}$), 多元多项式函数 v_i 是来自于 GGH13 构造的线性“0”测试函数^[25], 即来自于 $\mathbf{v} = [\mathbf{u} \cdot \mathbf{p}_{zt}]_q$ 的系数向量

$$\vec{\mathbf{v}} = (v_0(\vec{\mathbf{u}}), \dots, v_{n-1}(\vec{\mathbf{u}})) \text{ 且 } \|\vec{\mathbf{v}}\|_\infty < q^{1/4}.$$

更高次数“0”测试函数扩展: GHL15 构造中 d -次“0”测试函数定义为

$$f(\vec{\mathbf{u}}) = \sum_{i_1, i_2, \dots, i_d} \alpha_{i_1, i_2, \dots, i_d} \cdot v_{i_1}(\vec{\mathbf{u}}) \cdots v_{i_d}(\vec{\mathbf{u}}).$$

攻击关键思想是在“0”的 κ -级编码上计算高次多项式的“导数”, 以逐步减少多项式次数到线性多项式。

设多元多项式 $f(x_0, \dots, x_{n-1}) \in \mathbb{Z}_q[x_0, \dots, x_{n-1}]$. 对于向量 $\vec{\mathbf{a}} = (a_0, \dots, a_{n-1}) \in \mathbb{Z}_q^n$, 定义 f 在向量 $\vec{\mathbf{a}}$ 的导数 f'_a 为

$$f'_a(x_0, \dots, x_{n-1}) = [f(x_0 + a_0, \dots, x_{n-1} + a_{n-1}) - f(x_0, \dots, x_{n-1})]_q.$$

易于验证, 如果多项式 $f(\mathbf{x})$ 在 x_i 上的总度数为 $t \geq 1$, 那么多项式 $f'_a(\mathbf{x})$ 的总度数至多为 $t-1$.

对于变种 GHL15, Brakerski 等人攻击^[24] 组成 3 个步骤: (1) 计算给定度为 d 的“0”测试函数的 $d-1$ 次导数, 获得一个仿射“0”测试函数; (2) 由于这个仿射“0”测试函数的自由常数项一定是小的, 所以丢弃其常数项; (3) 从 (2) 中产生的线性“0”测试函数恢复产生 GGH13 构造的一个“0”测试函数。

由使用这个线性“0”测试函数和 GGH13^[11] 中容易量的计算方法, 可以计算产生 GHL15 构造中秘密元素 $\mathbf{g}$ 的基等相关量. 因而, GHL15 构造仍然存在“0”化攻击问题。

4.3.2 新构造抗 Brakerski 等人的攻击

因为 Brakerski 等人攻击^[24] 的关键是使用“导数”方法, 由 GHL15 构造的非线性“0”测试函数计算产生 GGH13 构造的线性“0”测试函数. 然而, 本文新随机化构造中新的“0”测试函数仍为线性函数, 即 $\mathbf{v} = [\mathbf{u} \cdot \mathbf{p}_{zt}]_q$, 并不能通过“导数”计算获得有用信息, 而且新随机化构造的公共参数中也没有包含“0”的 1-级编码, 即攻击者无法产生秘密理想元素 $\mathbf{g}$ 的格基. 所以, Brakerski 等人攻击方法^[24] 也不适用于本文新随机化构造。

原因分析: Brakerski 等人攻击 GHL15 构造成

功的原因在于: 在 GHL15 构造中, 非线性“0”测试函数在求其“导数”后仍然是“0”测试函数, 导致攻击者能够基于此产生 GGH13 构造的“0”测试函数. 然而, 在新随机化构造中, “0”测试函数仍为线性函数, 并不存在求“导数”问题。

4.4 基于范数的子域格攻击分析

目前针对无“0”的低级编码 GGH13 构造的子域格攻击主要有两种——基于范数和基于迹的子域格攻击方法^[26-27]. 它们主要区别在于攻击产生的 NTRU 问题实例的分子、分母增长方式不同. 这种增长方式不同导致攻击方法适用于不同的 NTRU 问题实例: 如果攻击的 NTRU 实例中分子、分母的范数大致相等, 则更适用于使用基于范数的子域格攻击方法; 反之, 如果 NTRU 实例中分子、分母的范数差异较大, 则更适用于使用基于迹的子域格攻击方法。

本节先给出基于范数的子域格攻击方法分析, 下一节将给出基于迹的子域格攻击方法分析。

4.4.1 基于范数的子域格攻击概述

子域格攻击方法主要是攻击 NTRU 问题难度假设^[20, 26-27, 64], 即将 NTRU 问题实例从高维归约到低维以使用格归约算法求解. 为便于描述, 下面先给出 NTRU 问题定义。

定义 4 (NTRU 问题^[26-27]). 在 NTRU 问题中, 设 $R = \mathbb{Z}[x]/\langle x^n + 1 \rangle$ 为多项式环, q 为模, D_1, D_2 为 R 中概率分布, β 为目标范数, 简记为 NTRU (R, q, D_1, D_2, β) . 问题是给定 $\mathbf{h} = [\mathbf{u}/\mathbf{w}]_q$, 其中 $\mathbf{u} \leftarrow D_1, \mathbf{w} \leftarrow D_2$, 要求计算求解向量 $(\mathbf{x}, \mathbf{y}) \in R^2$, 满足 $(\mathbf{x}, \mathbf{y}) \neq (\mathbf{0}, \mathbf{0}) \bmod q$, 且 $(\mathbf{x}, \mathbf{y})$ 在格 Λ_h^q 中欧几里德范数小于 $\beta \sqrt{2n}$, 这里

$$\Lambda_h^q = \{(\mathbf{x}, \mathbf{y}) \in R^2 \text{ s.t. } \mathbf{h}\mathbf{x} - \mathbf{y} = \mathbf{0} \bmod q\}.$$

我们也将问题 NTRU (R, q, D_1, D_2, β) 记为 NTRU $(R, q, \sigma_1, \sigma_2, \beta)$, 其中 D_1, D_2 分别是方差为 σ_1^2, σ_2^2 的同向性分布 (Isotropic Distribution). 由于在基于范数的子域格攻击^[26] 中 $\sigma_1 = \sigma_2$, 我们将这种 NTRU 问题简记为 NTRU (R, q, σ, β) .

NTRU 格 Λ_h^q : 由 $\mathbf{h}$ 定义的格 Λ_h^q 的维数为 $2n$, 格 Λ_h^q 的体积为 $\text{Vol}(R)^2 q^n$. 如果 $\mathbf{h}$ 是随机均匀元素, 则高斯启发式预测格 Λ_h^q 的最短向量的范数约为 $\text{Vol}(R)^{1/n} \sqrt{nq/\pi e}$. 因此, 当 $\sigma < \text{Vol}(R)^{1/n} \sqrt{q/2\pi e}$ 时, 格 Λ_h^q 有非常短的向量, 且这个向量并不是唯一的最短向量。

不失一般性, 设数域 $\mathbb{K} = \mathbb{Q}(\zeta_m)$, $\mathbb{K}$ 的整数环为 $R = O_{\mathbb{K}}$. 给定实例 $\mathbf{h} \leftarrow \text{NTRU}(O_{\mathbb{K}}, q, \sigma, \beta)$, 即 $\mathbf{h} = [\mathbf{u}/\mathbf{w}]_q$, 其中 $(\mathbf{w}, \mathbf{u}) \in O_{\mathbb{K}}$ 为秘密元素, 要求计算输出

格 Λ_h^q 的一个短向量。

给定 NTRU 问题实例, 基于范数的子域格攻击方法^[26] 组成 3 个步骤:

(1) 基于范数的维数压缩

将 NTRU 实例从全域映射到选择的子域上, 即给定 $h = [u/w]_q$, 定义

$$u' = N_{\mathbb{K}/\mathbb{L}}(u), w' = N_{\mathbb{K}/\mathbb{L}}(w) \text{ 和 } h' = N_{\mathbb{K}/\mathbb{L}}(h).$$

由范数性质知

$$h' = [N_{\mathbb{K}/\mathbb{L}}(u)/N_{\mathbb{K}/\mathbb{L}}(w)]_q = [u'/w']_q.$$

子域格攻击的关键观察是 (w', u') 为格 $\Lambda_{h'}^q$ 中的一个向量, 并且依赖于参数, 其很可能是非常短的向量。

(2) 在子域中实行格归约

使用格归约算法^[55, 63], 计算求解子域上 NTRU 实例以得到一个短向量 $(x', y') \in \Lambda_{h'}^q$.

引理 24 (定理 2^[26]). 设 $w', u' \in O_{\mathbb{L}}$, 满足 $\langle w' \rangle$ 和 $\langle u' \rangle$ 是互素理想, 且对于某个 $h' \in O_{\mathbb{L}}$ 有 $h'w' = u' \bmod (qO_{\mathbb{L}})$. 如果 $(x', y') \in \Lambda_{h'}^q$ 的范数满足 $\|(x', y')\| < \frac{q}{\|(w', u')\|}$, 则对于某个 $v' \in O_{\mathbb{L}}$ 有 $(x', y') = v' \cdot (w', u')$.

因此, 由引理 24 知, 向量 (x', y') 是 (w', u') 的 $O_{\mathbb{L}}$ 倍数, 即存在 $v' \in O_{\mathbb{L}}$ 满足 $(x', y') = v' \cdot (w', u')$.

(3) 提升计算解向量

通过第 2.2 节的经典映射 ϑ , 将解向量 (x', y') 从子环 $O_{\mathbb{L}}$ 提升到环 $O_{\mathbb{K}}$, 即

$$x = \vartheta(x') = [\vartheta(v') \cdot \tilde{w} \cdot w]_q = [v \cdot w]_q,$$

$$y = [\vartheta(y') \cdot h / \vartheta(h')]_q = [\vartheta(v') \cdot \tilde{w} \cdot u]_q = [v \cdot u]_q,$$

其中 $\tilde{w} = \vartheta(w')/w \in O_{\mathbb{K}}$, $v = \vartheta(v') \cdot \tilde{w} \in O_{\mathbb{K}}$.

因此, 基于范数的子域格攻击方法不仅获得格 Λ_h^q 的一个短向量, 而且该向量是秘密密钥 (w, u) 的一个 $O_{\mathbb{K}}$ 倍数, 即 $(x, y) = v \cdot (w, u)$.

4.4.2 基于范数的子域格攻击分析

给定新随机化构造的公共参数 par , 可以构造三种 NTRU 格 Λ_h^q . 下面依次分析这些格对新随机化构造安全的影响。

(1) 基于非“0”编码的攻击

① 产生 NTRU 格 $\Lambda_{h_1}^q$, 其中 $h_1 = [y_1/y_2]_q$.

② 对于格 $\Lambda_{h_1}^q$, 使用基于范数的子域格攻击, 则产生秘密元素的一个 $O_{\mathbb{K}}$ 倍数, 即 $(x, y) = v \cdot (e_2 + a_2g, e_1 + a_1g)$, 其中 $v \in O_{\mathbb{K}}$.

③ 重复使用②中方法可以得到一组不同 v_i 对应的 $x_i = v_i \cdot (e_2 + a_2g)$.

因此, 使用量子多项式时间算法或经典次指数时间算法^[57-59], 攻击者能够计算得到 $q = \delta(e_2 + a_2g)$ 和 $z' = [q/y_2]_q = [z\delta]_q$.

易于看出, 这种情况类似于第 4.1.2 节的攻击. 如果逆元 δ^{-1} 的范数较小, 则攻击可行, 否则不可行。

(2) 基于“0”测试参数的攻击

① 产生格 $\Lambda_{h_2}^q$, 其中 $h_2 = [p_{z',1}/p_{z',2}]_q$.

② 对于格 $\Lambda_{h_2}^q$, 基于范数的子域格攻击并不能

成功. 因为 $h_2 = \left[\frac{e_1 f + b_1 g}{e_2 f + b_2 g} \right]_q$, 且 $\sigma^* = \|e_j f + b_j g\| = \Omega(q^{5/8})$, 然而根据 Albrecht, Bai 和 Ducas^[26] 的分析, 避免基于范数的子域格攻击只需参数 $\sigma^* \approx \Theta(q^{1/4})$. 而且, 当 $\sigma^* = \Omega(q^{1/2})$ 时, 元素 h_2 是在统计上接近均匀分布^[50].

(3) 基于新的“0”测试参数攻击

① 给定上述(1)中计算获得的元素 z' , 计算

$$h_3 = \frac{p_{z',1}}{(z')^c} = \left[\frac{e_1 f + b_1 g}{g \cdot \delta^c} \right]_q, \text{ 并产生格 } \Lambda_{h_3}^q.$$

② 对于格 $\Lambda_{h_3}^q$, 基于范数的子域格攻击也不能成功, 因为 $\sigma^* = \|e_1 f + b_1 g\| = \Omega(q^{5/8})$.

从上述攻击分析可知, 仅第(1)种情形存在攻击可能性. 这种攻击能否成功依赖于 δ^{-1} 的范数较小的假设是否成立。

为抗这种潜在攻击, 可以使用第 4.1.3 节的反制措施. (1) 基于 Kilian 随机矩阵的改进能够抗基于范数的子域格攻击. 因为通过改进构造的公共参数可计算产生元素 $y'_j = [\bar{s}^T Y_j \bar{t}]_q = [s^T X_j t / (z \cdot z_q)]_q$, 所以 $h'_1 = [y'_1/y'_2]_q = [s^T X_1 t / s^T X_2 t]_q$. 由参数设置可知 $\|s^T X_j t\| \geq O(q^{5/8})$, 故元素 h'_1 是在统计上接近均匀分布^[50]. 而且, 易于证明通过编码 Y_j 的其它组合形式产生的元素可获得同样结论; (2) 基于 NTRU 型素数域也能够抗基于范数的子域格攻击, 这是因为在 NTRU 型素数域中没有适合于子域格攻击使用的子域。

4.5 基于迹的子域格攻击分析

4.5.1 基于迹的子域格攻击概述

基于迹的子域格攻击方法^[27] 与上述基于范数的子域格攻击方法类似, 也是将全域上 NTRU 实例归约到子域上 NTRU 实例, 使得子域上 NTRU 实例的维数较低. 而且当 $2\sigma_2 < \sigma_1$ 时, 基于迹的子域格攻击更适合于攻击问题 $\text{NTRU}(R, q, \sigma_1, \sigma_2, \beta)$.

为描述 Cheon, Jeong 和 Lee^[27] 的攻击方法, 我们设 $n = 2^k$, $R' = \mathbb{Z}[x^{2^k}]/\langle x^n + 1 \rangle$, $\mathbb{K}' = \mathbb{Q}[x^{2^k}]/\langle x^n + 1 \rangle$, $0 \leq t \leq k$. 因此, 数域 $\mathbb{K}^0$ 是度为 2^t 的子域 $\mathbb{K}'$ 的 Galois 扩展域, 其 Galois 群 $G' = \text{Gal}(\mathbb{K}^0/\mathbb{K}') = \{\theta_0 = id, \theta_1, \dots, \theta_{2^t-1}\}$.

针对问题 $\text{NTRU}(R, q, \sigma_1, \sigma_2, \beta)$ 实例, 基于迹的子域格攻击方法^[27] 组成 3 个步骤:

(1) 基于迹的维数压缩

使用基于迹的方法, 将 NTRU 实例从全域 $\mathbb{K}^0$ 映射到选择的子域 $\mathbb{K}^t$, 即给定 $\mathbf{h} = [\mathbf{u}/\mathbf{w}]_q$, 定义

$$\begin{aligned} Tr_{\mathbb{K}^0/\mathbb{K}^t}\left(\frac{\mathbf{u}}{\mathbf{w}}\right) &= \sum_{i=0}^{2^t-1} \theta_i\left(\frac{\mathbf{u}}{\mathbf{w}}\right) \\ &= \frac{Tr_{\mathbb{K}^0/\mathbb{K}^t}(\mathbf{u}\theta_1(\mathbf{w})\theta_2(\mathbf{w})\cdots\theta_{2^t-1}(\mathbf{w}))}{\prod_{i=0}^{2^t-1} \theta_i(\mathbf{w})}. \end{aligned}$$

由第 2.2 节迹和范数的性质可知:

$$\mathbf{w}_t = N_{\mathbb{K}^0/\mathbb{K}^t}(\mathbf{w}) = \prod_{i=0}^{2^t-1} \theta_i(\mathbf{w}) \in R^t,$$

$$\mathbf{u}_t = Tr_{\mathbb{K}^0/\mathbb{K}^t}(\mathbf{u}\theta_1(\mathbf{w})\theta_2(\mathbf{w})\cdots\theta_{2^t-1}(\mathbf{w}))/2^t \in R^t.$$

因此, $\left[\frac{\mathbf{u}_t}{\mathbf{w}_t}\right]_q$ 是问题 $\text{NTRU}(R^t, q, \sigma_{1,t}, \sigma_{2,t}, \beta_t)$ 的一个新实例, 其中

$$\begin{aligned} \sigma_{1,t} &= \sigma_1 \sigma_2^{2^t-1} \prod_{i=1}^t \sqrt{n/2^i}, \quad \sigma_{2,t} = \sigma_2 \prod_{i=1}^t \sqrt{n/2^i}, \\ \beta_t &= \min\left\{\frac{q}{2\sigma_{1,t}\sqrt{n}}, \frac{q}{2\sigma_{2,t}\sqrt{n}}, \frac{q}{2n\sigma_1^2\|\mathbf{g}^{-1}\|\sqrt{n}}\right\}. \end{aligned}$$

$$\text{所以, } \mathbf{h}' = \left[\frac{\mathbf{u}_t}{\mathbf{w}_t}\right]_q = \left[\sum_{i=0}^{2^t-1} \theta_i(\mathbf{h})/2^t\right]_q.$$

攻击成功关键是 $(\mathbf{w}_t, \mathbf{u}_t)$ 为格 $\Lambda_{\mathbf{h}'}^q$ 中的一个向量, 并且根据方案参数设置, 其长度一般是非常短的向量。

(2) 在子域中实行格归约

使用格归约算法^[55, 63], 计算求解子域上 NTRU 实例以得到一个短向量 $(\mathbf{x}', \mathbf{y}') \in \Lambda_{\mathbf{h}'}^q$.

由引理 24 可知, 向量 $(\mathbf{x}', \mathbf{y}')$ 一定是 $(\mathbf{w}_t, \mathbf{u}_t)$ 的 R' 倍数, 即存在 $\mathbf{v}' \in R'$ 满足 $(\mathbf{x}', \mathbf{y}') = \mathbf{v}' \cdot (\mathbf{w}_t, \mathbf{u}_t)$.

(3) 提升计算解向量

将解向量 $(\mathbf{x}', \mathbf{y}')$ 从子环 R' 提升到环 $R^0 = R$.

由 $(\mathbf{x}', \mathbf{y}') = \mathbf{v}' \cdot (\mathbf{w}_t, \mathbf{u}_t)$ 可得,

$$\mathbf{x} = \mathbf{x}' = \mathbf{v}' \cdot \mathbf{w}_t = \mathbf{v}' \cdot \prod_{i=0}^{2^t-1} \theta_i(\mathbf{w}) = \mathbf{v} \cdot \mathbf{w},$$

$$\mathbf{y} = [\mathbf{x} \cdot \mathbf{h}]_q = \left[\mathbf{v}' \cdot \prod_{i=0}^{2^t-1} \theta_i(\mathbf{w}) \cdot \mathbf{u}/\mathbf{w}\right]_q = \mathbf{v} \cdot \mathbf{u},$$

其中 $\mathbf{v} = \mathbf{v}' \cdot \prod_{i=1}^{2^t-1} \theta_i(\mathbf{w}) \in R^0$.

因此, 基于迹的子域格攻击方法不仅获得格 $\Lambda_{\mathbf{h}'}^q$ 的一个短向量, 而且该向量是秘密密钥 $(\mathbf{w}, \mathbf{u})$ 的一个 R^0 倍数, 即 $(\mathbf{x}, \mathbf{y}) = \mathbf{v} \cdot (\mathbf{w}, \mathbf{u})$.

4.5.2 基于迹的子域格攻击分析

类似于第 4.4.2 节, 我们同样使用公共参数 par 构造三种 NTRU 格 $\Lambda_{\mathbf{h}'}^q$. 虽然前两种 NTRU 格对构造安全的分析方法和结论与第 4.4.2 节完全类似, 但是第三种 NTRU 格更适合于使用基于迹的子域

格攻击. 下面将重点分析第三种情况.

(1) 基于非“0”编码的攻击

① 产生 NTRU 格 $\Lambda_{\mathbf{h}_1}^q$, 其中 $\mathbf{h}_1 = [\mathbf{y}_1/\mathbf{y}_2]_q$.

② 使用基于迹的子域格攻击产生格 $\Lambda_{\mathbf{h}_1}^q$ 中秘密元素的一个倍数, 即 $(\mathbf{x}, \mathbf{y}) = \mathbf{v} \cdot (\mathbf{e}_2 + \mathbf{a}_2 \mathbf{g}, \mathbf{e}_1 + \mathbf{a}_1 \mathbf{g})$, 其中 $\mathbf{v} \in R$.

③ 重复使用②中方法可以得到不同 $\mathbf{v}_i$ 对应的 $\mathbf{x}_i = \mathbf{v}_i \cdot (\mathbf{e}_2 + \mathbf{a}_2 \mathbf{g})$, 并使用量子多项式时间算法或经典次指数时间算法^[57-59], 攻击者能够计算得到 $\mathbf{q} = \delta(\mathbf{e}_2 + \mathbf{a}_2 \mathbf{g})$ 和 $\mathbf{z}' = [\mathbf{q}/\mathbf{y}_2]_q = [\mathbf{z}\delta]_q$.

同样, 这种情况也类似于第 4.1.2 节的攻击. 如果逆元 δ^{-1} 的范数较小, 则攻击可行, 否则不可行.

(2) 基于“0”测试参数的攻击

① 产生格 $\Lambda_{\mathbf{h}_2}^q$, 其中 $\mathbf{h}_2 = [\mathbf{p}_{z,t,1}/\mathbf{p}_{z,t,2}]_q$.

② 对于格 $\Lambda_{\mathbf{h}_2}^q$, 基于迹的子域格攻击方法并不能成功. 这是因为 $\mathbf{h}_2 = \left[\frac{\mathbf{e}_1 \mathbf{f} + \mathbf{b}_1 \mathbf{g}}{\mathbf{e}_2 \mathbf{f} + \mathbf{b}_2 \mathbf{g}}\right]_q$, 并且 $\sigma^* = \|\mathbf{e}_j + \mathbf{b}_j \mathbf{g}\| = \Omega(q^{5/8})$, 而当 $\sigma^* = \Omega(q^{1/2})$ 时, 元素 $\mathbf{h}_2$ 已经在统计上接近均匀分布^[50].

(3) 基于新的“0”测试参数攻击

① 给定上述(1)中计算产生的元素 $\mathbf{z}'$, 计算

$$\mathbf{h}_3 = \frac{\mathbf{p}_{z,t,1}}{(\mathbf{z}')^\kappa} = \left[\frac{\mathbf{e}_1 \mathbf{f} + \mathbf{b}_1 \mathbf{g}}{\mathbf{g} \cdot \delta^\kappa}\right]_q, \text{ 并产生格 } \Lambda_{\mathbf{h}_3}^q.$$

为分析简单假设 $\delta = 1$, 否则攻击不会更容易.

② 对于格 $\Lambda_{\mathbf{h}_3}^q$, 基于迹的子域格攻击也不能成功, 因为 $\sigma^* = \|\mathbf{e}_1 \mathbf{f} + \mathbf{b}_1 \mathbf{g}\| = \Omega(q^{5/8})$. 当然这也是将 σ^* 从 $q^{1/2}$ 提高到 $q^{5/8}$ 的主要原因. 具体分析如下:

设 $\mathbf{h}_3 = \left[\frac{\mathbf{e}_1 \mathbf{f} + \mathbf{b}_1 \mathbf{g}}{\mathbf{g}}\right]_q = \left[\frac{\mathbf{b}}{\mathbf{g}}\right]_q$, 基于迹的维数压

缩为 $\mathbf{h}'_3 = \left[\sum_{i=0}^{2^t-1} \theta_i(\mathbf{h}_3)/2^t\right]_q = \left[\frac{\mathbf{b}'}{\mathbf{g}'}\right]_q$.

构造维数为 2^{k-t+1} 的格 $L_1 = \begin{pmatrix} \mathbf{I} & [\mathbf{b}'/\mathbf{g}']_q \\ 0 & q\mathbf{I} \end{pmatrix}$.

由 $\det(L_1) = q^{2^{k-t}}$ 和引理 1 可知, 格 L_1 的最短向量长度至多为 $\sqrt{2^{k-t+1}} q^{1/2}$.

不失一般性, 设使用格归约算法^[55, 63] 计算获得格向量 $(\mathbf{x}', \mathbf{y}') \in L_1$ 满足 $\|(\mathbf{x}', \mathbf{y}')\| \approx \sqrt{2^{k-t+1}} q^{1/2}$, 即 $\|\mathbf{x}'\| \approx \sqrt{2^{k-t+1}} q^{1/2}$ 和 $\|\mathbf{y}'\| \approx \sqrt{2^{k-t+1}} q^{1/2}$.

又由格 L_1 的结构可知,

$$\mathbf{y}' = \left[\mathbf{x}' \cdot \left[\frac{\mathbf{b}'}{\mathbf{g}'}\right]_q\right]_q = \left[\frac{\mathbf{x}' \cdot \mathbf{b}'}{\mathbf{g}'}\right]_q.$$

因为 $\mathbf{b}$ 和 $\mathbf{g}$ 互素, 故在 R' 中 $\mathbf{b}'$ 不可能是 $\mathbf{g}'$ 的倍数, 即 $\mathbf{b}' \bmod \mathbf{g}' \neq 0$. 所以, 由引理 17 可得 $\|[\mathbf{b}'/\mathbf{g}']_q\| \approx q$.

注意: 为符号简单起见, 这里使用了 $\approx q$, 实际上应

为 $=q^{1-\epsilon}$, 其中 ϵ 为非常小的正数. 下面做类似处理.

下面, 我们证明以概率几乎为 1, 在 R' 中 x' 不是 g' 的倍数.

反证法. 设在 R' 中 $x' = g'x''$, 且 $x'' \in R'$, 则有

$$\|x''\| \geq \|x'\| / (n \cdot \|g'\|) \approx q^{1/2},$$

$$\|x''\| = \|x' \cdot (g')^{-1}\| \leq n \cdot \|x'\| \|(g')^{-1}\| \approx q^{1/2},$$

其中 $\|g'\|, \|(g')^{-1}\|$ 都较小, 否则攻击方法更不可行.

所以, $\|x''\| \approx q^{1/2}$.

由 $\|b'\| > q^{5/8}$ 可得, $\|x'' \cdot b'\| \approx q^{9/8}$.

所以, 以概率几乎为 1 有 $\|x'' \cdot b'\|_q \approx q$.

然而, 由 $\|y'\| = \left\| \left[\frac{x' \cdot b'}{g'} \right]_q \right\| = \|[x'' \cdot b']_q\|$ 知,

$$\|[x'' \cdot b']_q\| \approx \sqrt{2^{k-t+1}} q^{1/2}. \text{ 矛盾.}$$

因此, 在 R' 中 x' 不是 g' 的倍数的概率几乎为 1, 即攻击者使用格归约算法^[55, 63]时无法使得 x' 是 g' 的倍数, 也不能由此获得秘密理想 g 的倍数. 也就是说, 格归约算法在产生 x' 时, 以概率几乎为 1 将 $[b'/g']_q$ 作为整体进行归约, 而不是在模 q 下先约减除数因子 g' , 再根据 b' 在模 q 下产生 x'' , 使其满足条件 $\|[x'' \cdot b']_q\| \approx \sqrt{2^{k-t+1}} q^{1/2}$.

上述分析结果与实验结果^[26]相符, 也与理论证明结果^[50]相一致. 一方面, 根据实验结果(表 7^[26]), 当 $\sigma^* \approx \Theta(q^{1/4})$ 时, NTRU 问题已经能够完全避免子域格攻击. 由于 NTRU 问题^[26]的分子、分母的抽样参数都为 $\sigma^* \approx \Theta(q^{1/4})$, 所以分子分母乘积的范数约为 $\Theta(q^{1/2})$. 另一方面, Stehlé 和 Steinfeld^[50]从理论上证明了当 $\sigma^* = \Omega(q^{1/2})$ 时, NTRU 问题在统计上接近均匀分布. 在这种情况下, NTRU 问题的分子分母乘积的范数约为 $\Theta(q)$. 因此, 基于实验和理论结果^[26, 50], 本文设置 $\sigma^* = q^{5/8}$ 能够避免子域格攻击. 因为分子和分母乘积的范数约为 $\Theta(q^{5/8})$, 介于实验值 $\Theta(q^{1/2})$ 和理论值 $\Theta(q)$ 之间. 当然, 也可从熵(entropy)的角度分析上述抽样参数能够避免基于迹的子域格攻击.

从上述攻击分析可知, 只有第(1)种情形存在攻击可能性. 类似于第 4.4.2 节, 可以证明第 4.1.3 节的反制措施同样能够抗基于迹的子域格攻击.

4.6 Cheon 等人的攻击方法扩展分析

为避免“0”化攻击, Halevi^[30]基于 GGH15 构造了一个非对称 GGH13 变种(简记为 Hal15), 该变种能够实现多方密钥交换协议, 而且给出一个简单难度假设作为安全分析目标.

本节我们首先简要回顾变种 Hal15 (Section 7^[30]), 然后给出基于 Cheon 等人方法扩展攻击简单难度假设^[28], 最后证明这种扩展攻击方法不适用于新随机化构造.

4.6.1 变种 Hal15

由于针对变种 Hal15 的攻击仅与其公共参数相关, 所以我们仅给出 Hal15 的公共参数产生和简单难度假设攻击^[28, 30].

公共参数产生算法 $par_{\text{Hal15}} \leftarrow \text{vInstGen}(1^\lambda, 1^\kappa)$: 设 λ 为安全参数, κ 为多线性映射的次数.

(1) 抽样选择 $g \leftarrow D_{\mathbb{Z}^n, \sqrt{n \log n}}$ 和 $h \leftarrow D_{\mathbb{Z}^n, \sqrt{q}}$, 满足条件理想 $\langle g \rangle$ 和 $\langle h \rangle$ 是互素的.

(2) 随机抽样可逆元素 $z_{i,j} \leftarrow U(R_q)$, $i \in [\kappa]$, $j \in$

$[\kappa]$, 满足对于所有 $i \in [\kappa]$, $z = \prod_{j=1}^{\kappa} z_{i,j} \in R_q$.

(3) 计算“0”测试参数为 $p_{zt} = hz/g \in R_q$.

(4) 对于每个 $j \in [\kappa]$,

(4.1) 抽样 $t (t \geq 2)$ 个两两互素的元素 $e_{j,k} \leftarrow D_{\mathbb{Z}^n, \sqrt{n \log n}}$, $k \in [t]$;

//注意: 虽然在 Hal15^[30] 中 $t=2$, 但实际上需要选择 $t > \kappa$.

(4.2) 对于每个 $e_{j,k}$, 抽样 $e_{j,k}$ 的 κ 个 0-级编码 $e_{i,j,k} \leftarrow D_{\mathbb{Z}^n, \sqrt{n \log n}, e_{j,k}}$, $i \in [\kappa]$;

(4.3) 使用元素 $z_{i,j}$ 产生并输出编码 $u_{i,j,k} = [e_{i,j,k}/z_{i,j}]_q$.

(5) 输出公共参数

$$par_{\text{Hal15}} = \{n, q, p_{zt}, \{u_{i,j,k}\}_{i,j \in [\kappa], k \in [t]}\}.$$

由于攻击 GGH13 构造的关键是计算获得秘密理想格 $\langle g \rangle$ 的基, 所以明文空间 $R_g = R/I$ (或 I) 的格基是 GGH13 构造及其改进的安全核心. 因此, 当前研究安全的多线性映射构造时将计算理想格 $\langle g \rangle$ 的基作为简单难度假设, 并被当作攻击者的核心计算任务.

假设 1 (简单难度假设^[30]). 给定上述变种 Hal15 的公共参数 par_{Hal15} , 则求解理想格 $\langle g \rangle$ 的任何基在计算上是困难的.

4.6.2 Cheon 等人的攻击方法扩展^[28]

为易于叙述, 我们描述参数 $\kappa=3, t=3$ 时的攻击, 易于扩展攻击到 $\kappa > 3$ 的情况.

给定 par_{Hal15} , 则由公共参数产生算法可知,

$$e_{i,j,k} = e_{j,k} + r_{i,j,k} g, \quad i \in [\kappa], j \in [\kappa], k \in [t].$$

故可计算得到,

$$a_{i,k} = e_{i,1,k} e_{i,2,k} = e_{i,1,k} e_{i,2,k} + \epsilon_{i,k} g,$$

$$d_{i,k} = e_{i,3,k} = e_{i,3,k} + \delta_{i,k} g.$$

所以, 编码 $u_{i,1,s} u_{i,2,s} u_{i,3,r} \cdot s, r \in [t]$ 的分母为

$$z = \prod_{j=1}^{\kappa} z_{i,j}, \text{ 分子为元素 } e_{1,s} e_{2,s} e_{3,r} \text{ 的明文编码.}$$

不失一般性, 设 $s, r \in [t]$, 则

$$u_{(s,r)} = [u_{1,1,s} u_{1,2,s} u_{1,3,r} + u_{2,1,s} u_{2,2,s} u_{2,3,r} - 2u_{3,1,s} u_{3,2,s} u_{3,3,r}]_q.$$

所以, $u_{(s,r)}$ 为元素“0”的编码, 其分母为 z . 因此, $v_{s,r} = [u_{(s,r)} \cdot p_{zt}]_q$ 为非模 q 归约的环 R 中的元素.

一方面, 通过整理可将 $v_{s,r}$ 写成向量积形式

$$\begin{aligned} v_{s,r} &= (a_{1,s} d_{1,r} + a_{2,s} d_{2,r} - 2a_{3,s} d_{3,r}) \cdot \frac{h}{g} \\ &= (a_{1,s} \quad a_{2,s} \quad -2a_{3,s}) \cdot \begin{pmatrix} d_{1,r} \cdot h/g \\ d_{2,r} \cdot h/g \\ d_{3,r} \cdot h/g \end{pmatrix}. \end{aligned}$$

类似于扩展“0”化攻击^[23,31], 我们将元素 $v_{s,r}$, $s, r \in \llbracket t \rrbracket$ 写成矩阵 $V \in R^{3 \times 3}$, 并且 V 在 R 中以高概率为满秩矩阵.

另一方面, 将元素 $v_{s,r}$ 模 $\langle g \rangle$ 并整理, 则有

$$\begin{aligned} v_{s,r} &= \varepsilon_s \cdot he_{3,r} + he_{1,s} e_{2,s} \cdot \delta_r \bmod \langle g \rangle \\ &= (\varepsilon_s \quad he_{1,s} e_{2,s}) \begin{pmatrix} he_{3,r} \\ \delta_r \end{pmatrix} \bmod \langle g \rangle, \end{aligned}$$

其中 $\varepsilon_s = \varepsilon_{1,s} + \varepsilon_{2,s} - 2\varepsilon_{3,s}$, $\delta_r = \delta_{1,r} + \delta_{2,r} - 2\delta_{3,r}$.

所以, V 在模 $\langle g \rangle$ 下不可逆, 这是因为

$$V = \begin{pmatrix} \varepsilon_1 & he_{1,1} e_{2,1} \\ \varepsilon_2 & he_{1,2} e_{2,2} \\ \varepsilon_3 & he_{1,3} e_{2,3} \end{pmatrix} \begin{pmatrix} he_{3,1} & he_{3,2} & he_{3,3} \\ \delta_1 & \delta_2 & \delta_3 \end{pmatrix} \bmod \langle g \rangle.$$

因此, 在 R 中 V 的行列式 $\det(V)$ 一定是理想格 $\langle g \rangle$ 中非“0”元素. 由收集许多这样的非“0”元素, 我们能够通过计算这些元素的 GCD 或使用格归约算法获得理想格 $\langle g \rangle$ 的基. 所以, 在变种 Hal15 中简单难度假设并不成立, 即变种 Hal15 仍然存在“0”化攻击问题.

4.6.3 新构造抗 Cheon 等人的攻击方法扩展

由“0”化攻击^[23,28,38] 方法可知, 使用 Cheon 等人的攻击方法关键是产生元素“0”的 κ -级编码以构造上述矩阵 V .

由第 4.1 节分析可知, 攻击者使用新随机化构造的公共参数并不能直接计算得到“0”的 κ -级编码, 只能通过编码与“0”测试参数的交叉乘积方式获得隐藏元素“0”的 κ -级编码.

下面主要分析使用交叉乘积方法产生的非模 q 归约的环 R 中元素并不能计算获得理想格 $\langle g \rangle$ 的基, 即新随机化构造避免了 Cheon 等人方法扩展攻击^[28].

给定新随机化构造的公共参数 par , 设 $y = [c/z]_q$ 为任意一个 1-级编码, 则对于 $s, r \in \llbracket \tau \rrbracket$ 有

$$\begin{aligned} v_{s,r} &= [y^{\kappa-1} \cdot (y_s p_{zt,r} - y_r p_{zt,s})]_q \\ &= c^{\kappa-1} \cdot (c_s \cdot (e_r f + b_r g) / g - c_r \cdot (e_s f + b_s g) / g) \\ &= c^{\kappa-1} \cdot w_{s,r}, \end{aligned}$$

其中 $w_{s,r} = c_s \cdot (e_r f + b_r g) / g - c_r \cdot (e_s f + b_s g) / g$, $c_s = e_s + a_s g$ 和 $c_r = e_r + a_r g$.

下面我们将证明通过元素 $v_{s,r}$ 构造的矩阵 V , 满足如果 V 为 R 上满秩矩阵, 则 $V \in R^{2 \times 2}$, 并且 V 在模 $\langle g \rangle$ 下仍为满秩矩阵. 因此, Cheon 等人的攻击方法扩展并不能用于攻击新随机化构造.

(1) 将 $w_{s,r}$ 整理为 4 维向量积形式

$$\begin{aligned} w_{s,r} &= e_s \cdot b_r + a_s \cdot (e_r f + b_r g) - b_s \cdot e_r - (e_s f + b_s g) \cdot a_r \\ &= (e_s \quad a_s \quad b_s \quad e_s f + b_s g) \begin{pmatrix} b_r \\ e_r f + b_r g \\ -e_r \\ -a_r \end{pmatrix}. \end{aligned}$$

易于验证, 如果使用 $v_{s,r}$, $s, r \in \llbracket 4 \rrbracket$ 产生矩阵 $V = c^{\kappa-1} \cdot A \cdot B \in R^{4 \times 4}$, 则其行列式 $\det(V) = 0$. 因为矩阵 A 的第 1、3、4 列线性相关, 矩阵 B 的第 1、2、3 行线性相关.

类似地, 如果将 $w_{s,r}$ 整理为更高维向量积形式, 则 V 同样为非满秩矩阵, 即 $\det(V) = 0$.

(2) 将 $w_{s,r}$ 整理为 3 维向量积形式

$$\begin{aligned} w_{s,r} &= e_s \cdot (b_r - a_r f) + a_s \cdot (e_r f + b_r g) - b_s \cdot (e_r + a_r g) \\ &= (e_s \quad a_s \quad -b_s) \begin{pmatrix} b_r - a_r f \\ e_r f + b_r g \\ e_r + a_r g \end{pmatrix}. \end{aligned}$$

同样易于验证, 如果使用 $v_{s,r}$, $s, r \in \llbracket 3 \rrbracket$ 产生矩阵 $V = c^{\kappa-1} \cdot A \cdot B \in R^{3 \times 3}$, 则其行列式 $\det(V) = 0$. 因为矩阵 B 的第 1、2、3 行线性相关.

(3) 将 $w_{s,r}$ 整理为 2 维向量积形式

$$\begin{aligned} w_{s,r} &= c_s \cdot (e_r f + b_r g) / g - c_r \cdot (e_s f + b_s g) / g \\ &= (c_s \quad -c_r) \begin{pmatrix} (e_r f + b_r g) / g \\ (e_s f + b_s g) / g \end{pmatrix}. \end{aligned}$$

如果使用 $v_{s,r}$, $s, r \in \llbracket 2 \rrbracket$ 产生矩阵 $V = c^{\kappa-1} \cdot A \cdot B \in R^{2 \times 2}$, 则 V 在环 R 中以高概率为满秩矩阵.

现将 $w_{s,r}$ 在模 $\langle g \rangle$ 下整理为 2 维向量积形式

$$\begin{aligned} w_{s,r} &= (c_s \cdot (e_r f + b_r g) / g - c_r \cdot (e_s f + b_s g) / g) \bmod \langle g \rangle \\ &= e_s \cdot (b_r - a_r f) - (b_s - a_s f) \cdot e_r \\ &= (e_s \quad b_s - a_s f) \cdot \begin{pmatrix} b_r - a_r f \\ -e_r \end{pmatrix}. \end{aligned}$$

因此, 使用 $v_{s,r}$, $s, r \in \llbracket 2 \rrbracket$ 产生矩阵 $V = c^{\kappa-1} \cdot A \cdot B \in R^{2 \times 2}$, 则 V 在模 $\langle g \rangle$ 下以高概率为满秩矩阵. 所以, $\det(V) \bmod \langle g \rangle \neq 0$. 因此, 攻击者无法通过 Cheon 等人方法扩展攻击获得理想格 $\langle g \rangle$ 的基.

原因分析: Cheon 等人的方法扩展^[28] 攻击变种 Hal15^[30] 成功的原因在于: 对于 Hal15 构造, 隐藏的同明文出现在多个编码中, 但对于新随机化构造, 隐藏的同明文仅出现在一个编码中, 并仅在与该编码对应的“0”测试参数中包含了隐藏的明文元素. 这也是新随机化构造避免了 Cheon 等人方法扩展攻击的原因.

4.7 零化多项式攻击分析

本节分析证明,零化多项式攻击方法并不适用于新随机化构造. 针对基于 GGH13 的不可区分模糊器 IO^[32-33], Miles, Sahai 和 Zhandry^[29] 提出了零化多项式攻击方法. 由于该攻击无关对称或非对称多线性映射的 GGH13 构造,故下面仅分析对称多线性映射构造环境.

4.7.1 零化多项式攻击概述

设公共参数 $par_{10} = \{q, \{u_i\}_{i \in [m]}, p_{zt}\}$, 其中 $u_i = [(e_i + r_i g) / z^i]_q$ 为隐藏明文 e_i 的编码, $i \in [m]$, $j_i < \kappa$, 满足 $e_i \bmod g \neq 0$, r_i 为高斯抽样的元素, $p_{zt} = [hz^\kappa / g]_q$ 为“0”测试参数.

为实施零化多项式攻击,攻击者需要使用 par_{10} 产生“0”的 κ -级编码,并将其与 p_{zt} 相乘.

虽然 par_{10} 中并没有“0”元素的低级编码,但 IO 支持通过非“0”元素的低级编码的受限代数运算,计算得到“0”元素的 κ -级编码. 也就是说,给定一系列编码 $u_i, i \in [m]$, 攻击者^[29] 能够基于 IO 存取到一系列产生“0”元素的 κ -级编码的受限代数运算集.

Miles, Sahai 和 Zhandry^[29] 将由受限代数运算产生“0”元素的 κ -级编码 u , 按照 g 的幂进行分层表示如下:

$$u = \frac{g\gamma_1 + g^2\gamma_2 + \cdots + g^\kappa\gamma_\kappa}{z^\kappa}.$$

所以, $v = [u \cdot p_{zt}] = h \cdot (\gamma_1 + g\gamma_2 + \cdots + g^{\kappa-1}\gamma_\kappa)$, 其中每个 $\gamma_j, j \in [\kappa]$ 都是关于变量 $e_i, r_i, i \in [m]$ 的多项式.

零化多项式攻击关键在于能够使用多个不同受限代数运算产生的 γ_1 构造出零化多项式. 由于给定编码 $u_i, i \in [m]$ 和 p_{zt} , 攻击者只能得到隐含 γ_1 的元素 v , 所以构造基于多个不同隐含 γ_1 的零化多项式是攻击成功关键所在.

假设 $u^{(1)}, u^{(2)}, u^{(3)}$ 为不同代数运算产生的“0”的 κ -级编码, 它们与 p_{zt} 相乘计算产生的环 R 中元素为 $v^{(1)}, v^{(2)}, v^{(3)}$, 并且假定 $u^{(1)}, u^{(2)}, u^{(3)}$ 中包括的第一层多项式分别为 $\gamma_1^{(1)} = xr, \gamma_1^{(2)} = xr^2, \gamma_1^{(3)} = x$. 则存在一个有效可计算零化多项式 $Q(a, b, c) = a^2 - bc$, 满足 $Q(\gamma_1^{(1)}, \gamma_1^{(2)}, \gamma_1^{(3)})$ 是零多项式, 而且因为 Q 为齐次多项式, $Q(h\gamma_1^{(1)}, h\gamma_1^{(2)}, h\gamma_1^{(3)})$ 也是零多项式. 因此, 如果计算 $Q(v^{(1)}, v^{(2)}, v^{(3)})$, 则获得环 R 中理想 $\langle h^d g \rangle$ 中一个元素, 其中 $d = \deg(Q)$ 为多项式 Q 的度数.

注意: 零化多项式攻击^[29] 中将理想 $\langle h^d g \rangle$ 写作 $\langle hg \rangle$, 虽然元素 $h^d g \in \langle hg \rangle$, 但通过这种齐次多项式 Q 只能获得 $\langle h^d g \rangle$ 的基, 并不能得到断言的 $\langle hg \rangle$ 的基^[29]. 零化多项式攻击^[29] 中其它相关部分也存在类

似问题.

为了攻击基于 GGH13 的模糊器 IO^[32-33], Miles, Sahai 和 Zhandry^[29] 首先构造两个功能等价的函数, 即函数计算结果总是为 0、但作为分支程序时, 则是两个不同的简单分支程序 BP; 然后针对这种特殊的简单分支程序, 构造多个隐含变量 γ_1 上的零化多项式 $Q_{1,2,3}$. 虽然 Miles, Sahai 和 Zhandry 构造了这种简单分支程序关于隐含变量 γ_1 的零化多项式, 但是构造零化多项式在计算上一般非常困难^[65].

4.7.2 新构造抗零化多项式攻击

为证明新随机化构造能够避免零化多项式攻击^[29], 需要证明使用新构造的公共参数不能有效产生零化多项式.

给定新随机化构造的公共参数 par , 我们分析证明如下:

(1) 如果攻击者仅使用编码 $y_j, j \in [\tau]$ 支持的受限代数运算, 则其能够产生“0”元素的 k -级编码的概率约为 $O(1/\beta)$, 其中 $1 \leq k \leq \kappa, \beta = |R/\langle g \rangle| > 2^\lambda$.

不失一般性, 设编码支持的多项式 $Q(y_1, \dots, y_\tau)$ 计算产生“0”的 k -级编码, 即 $Q(y_1, \dots, y_\tau) = \frac{g\gamma_1 + g^2\gamma_2 + \cdots + g^k\gamma_k}{z^k}$. 所以, 由 $y_j = [(e_j + a_j g) / z]_q$ 可得 $Q(e_1, \dots, e_\tau) = 0 \bmod g$.

然而, 在 g 和 $e_j, j \in [\tau]$ 都未知的情况下, 目前并没有有效算法能够产生多项式 $Q(x_1, \dots, x_\tau)$, 满足 $Q(e_1, \dots, e_\tau) = 0 \bmod g$. 因此, 在这种情况下, 假设多项式 Q 产生的元素 $Q(e_1, \dots, e_\tau)$ 属于 $R/\langle g \rangle$ 中随机元素, 即 $Q(e_1, \dots, e_\tau) = 0 \bmod g$ 的概率约为 $O(1/\beta)$. 我们将证明这个假设或将其归约到更弱的安全假设作为一个公开问题.

(2) 如果攻击者仅使用 $p_{zt,j}, j \in [\tau]$ 支持的受限代数运算, 则其能够产生“0”元素的“0”测试参数的概率也约为 $O(1/\beta)$.

设多项式 $Q(p_{zt,1}, \dots, p_{zt,\tau})$ 产生“0”元素的“0”测试参数. 由于 $p_{zt,j} = [(e_j f + b_j g) z^\kappa / g]_q$ 中 $\|b_j\| > q^{5/8}$, 所以为得到隐藏“0”元素的“0”测试参数, 只能使用 $p_{zt,j}$ 的线性函数.

所以多元线性多项式 $Q(p_{zt,1}, \dots, p_{zt,\tau}) = bz^\kappa$, 即

$$Q(e_1 f + b_1 g, \dots, e_\tau f + b_\tau g) = bg,$$

$$Q(e_1 f, \dots, e_\tau f) = 0 \bmod g.$$

因为 f 与 g 互素, 所以 $e'_j = [e_j f]_g$ 为 $R/\langle g \rangle$ 中的随机元素.

因此, 在 g 和 $e'_j, j \in [\tau]$ 未知情况下, 多项式 $Q(e'_1, \dots, e'_\tau) = 0 \bmod g$ 的概率约为 $O(1/\beta)$. 所以, $Q(e_1 f, \dots, e_\tau f) = 0 \bmod g$ 的概率也约为 $O(1/\beta)$.

(3) 如果攻击者使用 $v_{s,r}$ 支持的代数运算, 则其能够产生 $\langle g \rangle$ 中非 0 元素 (即 rg) 的概率约为 $O(1/\beta)$, 其中 $v_{s,r}$ 为使用交叉乘积获得的非模 q 归约的元素.

由 4.1 节分析知, 1-级编码与“0”测试参数的交叉乘积可以计算得到隐含的明文元素“0”的编码. 所以, 对于 $s, r \in \llbracket \tau \rrbracket$, 可计算非模 q 归约的元素 $v_{s,r}$ 如下:

$$v_{s,r} = [(d_1 y_1 + d_2 y_2)^{\kappa-1} (y_s p_{zt,r} - y_r p_{zt,s})]_q \\ = [c \cdot w_{s,r}]_q,$$

其中

$$c = (d_1 (e_1 + a_1 g) + d_2 (e_2 + a_2 g))^{\kappa-1},$$

$$w_{s,r} = e_s b_r + e_r a_s f - e_r b_s - e_s a_r f + a_s b_r g - a_r b_s g.$$

因为 g 为素理想元素, c 为 $R/\langle g \rangle$ 中随机元素, 所以 c 与 g 互素的概率为 $O(1/\beta)$.

根据高斯抽样, $w'_{s,r} = [w_{s,r}]_g$ 为 $R/\langle g \rangle$ 中的随机元素, 所以 $v'_{s,r} = [v_{s,r}]_g$ 也为 $R/\langle g \rangle$ 中随机元素.

因此, 给定环 R 中一系列元素 $v_{s,r}, s, r \in \llbracket \tau \rrbracket$, 但 g 和 $a_j, b_j, e_j, j \in \llbracket \tau \rrbracket$ 未知, 攻击者能够产生多项式 $Q(\{v_{s,r}, s, r \in \llbracket \tau \rrbracket\})$ 满足 $Q(\{v_{s,r}, s, r \in \llbracket \tau \rrbracket\}) \neq 0$, $Q(\{v_{s,r}, s, r \in \llbracket \tau \rrbracket\}) = 0 \bmod g$ 的概率约为 $O(1/\beta)$.

综上, 给定公共参数 par , 攻击者能够计算得到秘密理想 g 的格基的概率约为 $O(1/\beta)$. 因此, 新随机化构造能够抗零化多项式攻击^[29].

原因分析: 零化多项式攻击^[29]成功的原因在于: 在基于 GGH13 的模糊器 $IO^{[32-33]}$ 中, (1) IO 本身支持一系列产生“0”元素的 κ -级编码的受限代数运算集; (2) 攻击者只要能给出一对功能相同的函数, 并能够区分使用 IO 模糊后的这对函数, 就算攻击 IO 成功. 但在新随机化构造中, 攻击者除了能够使用公共参数中固有的交叉乘积运算外, 并不能使用其它代数运算产生“0”元素的 κ -级编码.

5 安全性

为给出新随机化构造的安全性, 5.1 节给出新随机化构造的安全假设; 5.2 节证明构造完全无“0”编码方案的不可能性.

5.1 安全假设

与现有构造方案一样^[11-12, 37, 39], 本文新随机化构造的安全性只能基于新的难度问题安全假设, 也不能归约到经典困难问题假设.

新随机化构造安全基于 GCDH/GDDH 的提取变种——ext-GCDH/ext-GDDH. 由于难度问题 GCDH/GDDH 的安全实验 (见附录 1) 都使用了 GGH13 构造中的“0”元素的编码. 然而, 在新随机化构造中, 公共参数中并没有“0”元素的编码, 所

以对于新随机化构造的难度假设问题并不能直接使用难度假设问题 GCDH/GDDH. 但是, Langlois, Stehlé 和 Steinfeld^[21] 还定义了 GCDH 的提取变种——ext-GCDH, 这种难度问题并不依赖于“0”元素的编码. 因此, 本文将 ext-GCDH 自适应扩展到新随机化构造的难度假设.

为定义难度假设问题 ext-GCDH/ext-GDDH, 我们先给出新随机化构造的安全实验过程如下:

(1) 产生公共参数 $par \leftarrow \text{InstGen}(1^\lambda, 1^\kappa)$.

(2) 对于 $i = 0, 1, \dots, \kappa$:

(2.1) 抽样选择 $r_{i,j}, d_{i,j} \leftarrow D_{\mathbb{Z}^n, \sigma_1^*}, j \in \llbracket \tau \rrbracket$;

(2.2) 产生隐藏明文的 1-级编码

$$u_i = \left[\sum_{j \in \llbracket \tau \rrbracket} d_{i,j} y_j \right]_q.$$

(3) 产生 κ -级编码 $u^* = \left[\prod_{i=1}^{\kappa} u_i \right]_q$.

(4) 计算产生两个“0”测试参数.

(4.1) 计算与编码 u_0 对应的“0”测试参数

$$p_{zt} = \left[\sum_{j \in \llbracket \tau \rrbracket} d_{0,j} p_{zt,j} \right]_q;$$

(4.2) 计算随机的“0”测试参数

$$p_{zt_Rand} = \left[\sum_{j \in \llbracket \tau \rrbracket} r_{0,j} p_{zt,j} \right]_q.$$

(5) 计算提取比特串

$$w_C = w_D = \text{MSB}_l([u^* \cdot p_{zt}]_q).$$

(6) 计算随机提取比特串

$$w_{Rand} = \text{MSB}_l([u^* \cdot p_{zt_Rand}]_q).$$

定义 5 (提取问题 ext-GCDH/ext-GDDH). 根据上述安全实验, 提取问题 ext-GCDH/ext-GDDH 定义如下:

κ -级提取 CDH 问题 (ext-GCDH): 给定 $\{par, u_0, \dots, u_\kappa\}$, 输出提取比特串 w_C .

κ -级提取 DDH 问题 (ext-GDDH): 给定 $\{par, u_0, \dots, u_\kappa\}$, 区分 w_D 和 w_{Rand} , 即区分下面分布

$$D_{\text{ext-GDDH}} = \{par, u_0, \dots, u_\kappa, w_D\},$$

$$D_{\text{ext-Rand}} = \{par, u_0, \dots, u_\kappa, w_{Rand}\}.$$

假设 2. 假定任何概率多项式时间算法 A 攻击提取问题 ext-GCDH/ext-GDDH 的概率优势是可忽略的, 即

对于 ext-GCDH 问题, 我们有

$$\Pr[A(\{par, u_0, \dots, u_\kappa\}) = w_C] \leq \text{negl}(\lambda);$$

对于 ext-GDDH 问题, 我们有

$$|\Pr[A(w_D) = 1] - \Pr[A(w_{Rand}) = 1]| \leq \text{negl}(\lambda),$$

其中算法 A 中省略了 $\{par, u_0, \dots, u_\kappa\}$.

评论 4. (1) 上述安全假设类似形式已经隐含在 GGH13^[11] 和 GGH Lite^[21] 的难度假设中, 只是没有具体给出. Garg, Gentry 和 Halevi^[11] 假设判定问题 GDDH 在计算上是不可区分的, 而 Langlois,

Stehlé 和 Steinfeld^[21]则在证明 MPKE 协议安全时假设提取问题 ext-GCDH 是难的; (2) 本文给出安全假设是为了便于证明基于新随机化构造的应用安全性, 否则每个应用都要给出新的难度假设, 易于导致基于构造的应用安全性不具体, 也不明确; (3) 判定问题 ext-GDDH 能够归约到计算求解问题 ext-GCDH. 因为如果知道问题 ext-GCDH 的提取比特串 w_C , 则能够判定 w_D 和 w_{Rand} , 即判定问题 ext-GDDH. 然而, 目前还无法将求解问题 ext-GCDH 归约到判定问题 ext-GDDH.

5.2 完全无“0”编码的不可能性

虽然非对称变种构造中相同索引集的编码与“0”测试参数不再能够实行交叉乘积, 但是该变种中仍然存在不同索引集的编码与“0”测试参数之间的交叉乘积问题.

给定非对称变种构造的公共参数 $vpar = \{vpar_i, i \in \llbracket N \rrbracket\}$, 则对于 $j_1, j_2 \in \llbracket \tau \rrbracket$, 可计算不同索引集的交叉乘积如下:

$$v_{j_1, j_2} = \left[(y_{\{1\}, j_1} p_{\{2\}, j_2} - p_{\{1\}, j_1} y_{\{2\}, j_2}) \prod_{i=3}^N y_{\{i\}, j_1} \right]_q.$$

易于验证, 元素 v_{j_1, j_2} 并不是模 q 归约的. 因此, 一方面, 攻击者通过不同 v_{j_1, j_2} 能够计算获得主理想 $e_{i,j} + a_{i,j}g$ 的格基. 另一方面, 攻击者使用量子多项式时间算法^[57-58]或经典次指数时间算法^[59], 计算得到 $e_{i,j} + a_{i,j}g$ 和 $z_i = \left[\frac{e_{i,j} + a_{i,j}g}{y_{\{i\}, j}} \right]_q$, 并且进而可以计

算出 $y'_{\{i\}, j} = e_{i,j} + a_{i,j}g$, $p'_{\{i\}, j} = [(e_{i,j}f + b_{i,j}g)/g]_q$, $i \in \llbracket N \rrbracket, j \in \llbracket \tau \rrbracket$.

然而, 仅知道 $y'_{\{i\}, j}$ 和 $p'_{\{i\}, j}$, 攻击者还是无法计算秘密理想格 $\langle g \rangle$ 的基, 也无法攻击基于非对称变种构造的 MPKE 协议.

本文下面分别通过两个引理证明在基于噪声的分级多线性映射构造中完全避免“0”化攻击问题的不可能性和可能性. 不失一般性, 假设任意基于噪声的多线性映射能够应用于 MPKE 协议. 这是因为不仅 2.7 节的多线性映射定义体现了这一点, 而且多线性映射本身也来源于基于双线性映射的三方 Diffie-Hellman 密钥交换的扩展.

引理 25. (1) 任何基于噪声的 κ -级多线性映射对称构造一定存在“0”化攻击问题, 即攻击者一定能够计算得到“0”的 κ -级编码; (2) 如果任何基于噪声的多线性映射非对称构造的所有公共参数公开, 则该非对称变种构造也一定存在“0”化攻击问题.

证明. (1) 不失一般性, 设 par 为某个基于噪声的 κ -级多线性映射对称构造的公共参数.

首先, 攻击者使用 par 产生 $\kappa+1$ 个可以使用的

1-级编码 $u_i = e(d_i)$, $i \in \llbracket \kappa+1 \rrbracket$. 注意: 这里映射 $e(\cdot)$ 为某种基于噪声的 κ -级多线性映射, 将明文 d_i 通过映射 $e(\cdot)$ 产生 1-级编码 $u_i = e(d_i)$, 而且计算映射 $e(\cdot)$ 时也可能使用一些随机元素 (如 GGH13 构造). 为符号简单, 这里不标示可能使用的随机元素.

为便于陈述, 假定攻击者知道 1-级编码 u_i 中的 0-级编码 d_i (即明文元素). 当然, 攻击者知道隐藏了 0-级编码的其它可用元素也是可行的 (如新随机化构造中隐藏了明文元素的“0”测试参数).

其次, 攻击者计算产生编码 $u = d_1 \prod_{i=2}^{\kappa+1} u_i -$

$d_{\kappa+1} \prod_{i=1}^{\kappa} u_i$. 易于验证, u 是一个 κ -级编码, 并且 u 中的明文元素为“0”, 即 u 为一个“0”元素的 κ -级编码. 又因为 κ -级多线性映射 $e(\cdot)$ 为基于噪声的多线性映射, 故 κ -级编码 u 不等于 0 的概率几乎为 1.

因此, 给定构造的公共参数 par , 攻击者一定能够产生“0”元素的 κ -级编码, 即基于噪声的分级多线性映射对称构造一定存在“0”化攻击问题.

(2) 设 $vpar$ 为基于噪声的多线性映射非对称构造的公共参数.

首先, 攻击者使用 $vpar$ 能够计算产生基本索引集 $\{i\}$ 的编码 $u_{\{i\}} = e_{\{i\}}(d_i)$, $i \in \llbracket \kappa+1 \rrbracket$, 其中 $e_{\{i\}}(\cdot)$ 为某种基于噪声的多线性映射, 将明文 d_i 通过映射 $e_{\{i\}}(\cdot)$ 产生基本索引集 $\{i\}$ 的编码 $u_{\{i\}} = e_{\{i\}}(d_i)$.

其次, 攻击者能够计算最大索引集 S_1 -编码 $u_{S_1} = d_1 \prod_{i=2}^{\kappa+1} u_{\{i\}}$ 与最大索引集 S_2 -编码 $u_{S_2} = d_{\kappa+1} \prod_{i=1}^{\kappa} u_{\{i\}}$. 因为攻击者知道编码 $u_{\{i\}}$ 的明文编码 d_i (对于隐藏的明文编码 d_i , 可获得类似结果, 如本节给出的不同索引集交叉乘积).

最后, 攻击者能够计算产生编码 $u = u_{S_1} - u_{S_2}$. 因为假设非对称构造变种能够用于 MPKE 协议, 所以当 S_1, S_2 为最大索引集时, 即当 $|S_1| = |S_2| = \kappa$ 时, 非对称构造中索引集编码能够实行加法运算. 易于看出, u_{S_1} 和 u_{S_2} 编码了相同的明文元素, 故 u 是“0”元素的最大索引集编码.

注意: 这里基于噪声的非对称构造没有使用“0”测试参数. 如果构造中需要使用“0”测试参数以去除编码中索引集元素, 则需要将其与相应编码相乘以产生隐含的“0”元素的编码 (如本文非对称构造的不同索引集交叉乘积).

因此, 给定非对称构造的公共参数 $vpar$, 攻击者一定能够产生“0”元素的最大索引集编码, 即基于噪声的非对称多线性映射也一定存在“0”化攻击

问题.

证毕.

现在讨论完全避免“0”化攻击问题的可能性. 由非对称构造的安全分析可知, 攻击者能够通过不同索引集的交叉乘积计算得到非模 q 归约的非平凡量. 为了避免攻击者计算理想元素 $e_{i,j} + a_{i,j}g$ 的格基, 需要使得攻击者不能得到不同索引集下的公共参数. 因此, 假设在基于非对称变种构造的应用(如多方密钥交换 MPKE 协议)中, 各方之间不合谋交换各自的公共参数, 并且各方都通过某种安全方式获得自己的公共参数. 即: 假设第 $i(i \in \llbracket N \rrbracket)$ 方只能得到自己的公共参数 $vpar_i$, 并且不对外发布, 也不与其他方合谋交换各自拥有的公共参数. 注意: 这个假设条件非常强, 目的是为了证明在这样假设条件下非对称变种构造能够完全避免“0”化攻击问题.

对于第 $i(i \in \llbracket N \rrbracket)$ 方, 易于验证非对称构造中算法——索引集 $\{i\}$ -编码算法 $vEnc$ 、编码加法算法 $vAdd$ 、编码乘法算法 $vMul$ 、“0”测试算法 $visZero$ 和提取算法 $vExt$, 在仅知道参数 $vpar_i$ 时这些算法仍然能够正确计算.

引理 26. 如果在非对称变种构造中, 第 $i(i \in \llbracket N \rrbracket)$ 方只能得到自己的公共参数 $vpar_i$, 并且不对外发布, 则该变种构造没有“0”化攻击问题. 即: 如果攻击者仅使用非对称变种中某一方公共参数和其它方产生的索引集编码, 则其不能计算产生非模 q 归约的非平凡量.

证明. 因为第 $i(i \in \llbracket N \rrbracket)$ 方只有自己的公共参数 $vpar_i$, 即相同索引集 $\{i\}$ 的编码 $y_{\{i\},j}$ 和与其对应的“0”测试参数 $p_{\{i\},j}$. 由于它们编码了 R/I 中相同陪集元素 $e_{i,j} = e_{i,j} + I$, 则

$$\begin{aligned} u_{\{i\}} &= [y_{\{i\},j_1} p_{\{i\},j_2} - y_{\{i\},j_2} p_{\{i\},j_1}]_q \\ &= \left[\frac{e_{i,j_1} + a_{i,j_1}g}{z_i} \cdot \frac{z_i^*(e_{i,j_2}f + b_{i,j_2}g)}{g} - \frac{a_{i,j_2}g + e_{i,j_2}}{z_i} \cdot \frac{z_i^*(e_{i,j_1}f + b_{i,j_1}g)}{g} \right]_q \\ &= \left[\frac{z_i^*b_i}{z_i} \right]_q, \end{aligned}$$

其中,

$$b_i = a_{i,j_1}b_{i,j_2}g + a_{i,j_1}e_{i,j_2}f + e_{i,j_1}b_{i,j_2} - a_{i,j_2}b_{i,j_1}g - a_{i,j_2}e_{i,j_1}f - e_{i,j_2}b_{i,j_1}.$$

为消去 $u_{\{i\}}$ 的分母 z_i , $u_{\{i\}}$ 必须再乘以某个“0”测试参数 $p_{\{t\}} = \left[\frac{z_i^*b_t}{g} \right]_q$, $t \neq i$. 然而, 根据引理假设条件, 对于 $t \neq i$, 第 i 方并不知道第 $t(t \in \llbracket N \rrbracket)$ 方的“0”测试参数 $p_{\{t\},j}$. 因此, 第 i 方无法通过交叉乘积计算产生非模 q 归约的非平凡量.

又因为不同索引集的编码 $u_{\{i_1\}}$ 、 $u_{\{i_2\}}$ 编码了不同陪集 $e_{i_1} = e_{i_1} + I$ 、 $e_{i_2} = e_{i_2} + I$ 中的明文编码, 攻击

者使用四则算术运算并不能获得“0”的非空索引集编码.

当然, 如果需要非对称变种构造能够抗子域的格攻击^[26-27], 则非对称构造需要使用第 4.1.3 节中引入的反制措施. 否则, 攻击者能够使用量子多项式算法^[57-58]或经典次指数时间算法^[59], 由多个相同索引集 $\{i\}$ 的编码计算得到随机元素 z_i .

所以, 如果攻击者仅使用某个参与方的公共参数和其它方产生的索引集编码, 则攻击者不能计算得到非模 q 归约的非平凡量. 证毕.

从引理 25、26 可知, 如果基于噪声的多线性映射能够用于构造 MPKE 协议, 并且所有公共参数公开, 则攻击者能够使用该 MPKE 协议本身产生“0”元素的 κ -级(或最大索引集)编码. 因此, 基于噪声的多线性映射构造不可能完全避免“0”化攻击问题, 但是多线性映射构造存在“0”化攻击问题也并不意味着该构造不安全, 其安全性需要具体分析证明.

6 无可信安装的多线性映射

本节基于中国剩余定理(Chinese Remainder Theorem, CRT)构造无可信安装的多线性映射. 由于新随机化构造中, 初始化算法产生公共参数时使用的秘密元素需要保密, 使得构造方案需要可信安装. 通过分析发现, 秘密元素仅在公共参数产生时使用, 公共参数使用过程中不再需要使用秘密参数. 因此, 如果网络环境下每个参与方首先使用新随机化构造产生自己的公共参数, 并将秘密参数保密, 然后每个参与方使用中国剩余定理将所有参与方的公共参数组合起来以产生新的多线性映射构造, 则新构造将不需要可信中心安装.

在本节中, 第 6.1 节给出构造中使用的中国剩余定理 CRT 形式; 第 6.2 节基于多项式环 R 上 CRT 构造无可信安装的多线性映射; 第 6.3 节证明构造方案的正确性; 第 6.4 节给出构造的安全假设和已知攻击分析.

6.1 中国剩余定理 CRT 形式

本节首先描述整数环 $\mathbb{Z}$ 上 CRT, 然后将其扩展到多项式环 R 上.

6.1.1 整数环 $\mathbb{Z}$ 上 CRT

设 q 为 N 个不同素数的积, 即 $q = \prod_{i=1}^N q_i$. 由中国剩余定理 CRT 知, 环 $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ 同构于

$$\begin{aligned} \mathbb{Z}_q &= \mathbb{Z}/q\mathbb{Z} \\ &\cong \mathbb{Z}/q_1\mathbb{Z} \otimes \cdots \otimes \mathbb{Z}/q_N\mathbb{Z} \\ &\cong \mathbb{Z}_{q_1} \otimes \cdots \otimes \mathbb{Z}_{q_N}. \end{aligned}$$

给定任意 N 个数 $(a_1, \dots, a_N)$, 其中 $a_t \in \mathbb{Z}_{q_t}, t \in \llbracket N \rrbracket$, 则由 CRT 可以计算得到 $\mathbb{Z}_q$ 中唯一元素 a , 记为 $\text{CRT}_{(q_1, \dots, q_N)}(a_1, \dots, a_N)$, 满足 $a = a_t \bmod q_t, t \in \llbracket N \rrbracket$, 即

$$a = \text{CRT}_{(q_1, \dots, q_N)}(a_1, \dots, a_N) = \left[\sum_{t=1}^N a_t \cdot p_t \cdot w_t \right]_q \quad (1)$$

式中整数 p_t, w_t 是根据 CRT 原理计算得到, 即 $p_t = q/q_t, w_t = (p_t)^{-1} \bmod q_t$.

整数环 $\mathbb{Z}$ 上 CRT 是中国剩余定理的经典形式. Coron, Lepoint 和 Tibouchi^[12] 使用这种 CRT 形式构造了整数上多线性映射 CLT13.

6.1.2 多项式环 R 上 CRT

为将 CRT 从整数环 $\mathbb{Z}$ 扩展到多项式环 R , 我们将环 $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ 同构中的环 $\mathbb{Z}$ 替换为环 R .

$$\begin{aligned} \text{设 } q = \prod_{t=1}^N q_t, \text{ 则由 CRT 知 } R_q &\equiv R/qR \text{ 同构于} \\ R_q &= R/qR \\ &\cong R/q_1R \otimes \dots \otimes R/q_NR \\ &\cong R_{q_1} \otimes \dots \otimes R_{q_N} \\ &\cong \mathbb{Z}_{q_1}[x]/\langle x^n + 1 \rangle \otimes \dots \otimes \mathbb{Z}_{q_N}[x]/\langle x^n + 1 \rangle \\ &\cong \mathbb{Z}_{q_1^n} \otimes \dots \otimes \mathbb{Z}_{q_N^n}. \end{aligned}$$

类似地, 给定任意 N 个元素 $(a_1, \dots, a_N)$, 其中 $a_t \in R_{q_t}, t \in \llbracket N \rrbracket$, 则由 CRT 可以计算得到 R_q 中唯一元素 a , 记为 $\text{CRT}_{(q_1, \dots, q_N)}(a_1, \dots, a_N)$, 满足 $a = a_t \bmod q_t, t \in \llbracket N \rrbracket$, 即

$$a = \text{CRT}_{(q_1, \dots, q_N)}(a_1, \dots, a_N) = \left[\sum_{t=1}^N a_t \cdot p_t \cdot w_t \right]_q \quad (2)$$

其中整数 p_t, w_t 同样是根据 CRT 原理计算得到, 即 $p_t = q/q_t, w_t = (p_t)^{-1} \bmod q_t$.

因此, 根据多项式环 R 上 CRT, 我们能够使用类似于 CLT13^[12] 的方法构造出多项式环上无可信安装的多线性映射.

6.2 多线性映射构造

6.2.1 构造

为符号一致, 本节构造中参数符号意义约定与第 3.1.1 节相同, 即构造中仍然使用参数符号 $\lambda, \kappa, q, n, \sigma, \sigma', \sigma_1^*, \sigma^*, \tau, l_{-1}, l$. 这些参数大小设置将在第 6.2.2 节给出.

设 $N = \kappa + 1$ 为参与方个数.

为简单, 符号 $\text{CRT}_{(q_1, \dots, q_N)}(a_1, \dots, a_N)$ 简写为 $\text{CRT}(a_1, \dots, a_N)$. 除特殊说明外, 本文无可信安装构造中 CRT 都使用素数 $q_1, \dots, q_N$.

基于 CRT 的无可信安装的构造本身很简单. 构造的公共参数产生算法, 实际上就是每个参与方首先使用第 3.1.2 节新随机化构造产生各自的公开

参数, 然后每个参与方使用 CRT 将所有参与方的公开参数组合以产生构造的公共参数. 构造中所有其它算法都可以基于 CRT 自适应给出.

无可信安装构造的各个算法具体如下:

公共参数产生算法 $PAR \leftarrow \text{INSTGen}(1^\lambda, 1^\kappa)$:

对于每个参与方 $t \in \llbracket N \rrbracket$, 其计算如下:

(1) 第 t 方产生并发布公开参数 $\{par_t\}$.

(1.1) 选择足够大素数 q_t ;

(1.2) 随机抽样 $z_t \leftarrow U(R_{q_t})$, 满足 $z_t^{-1} \in R_{q_t}$;

(1.3) 抽样素理想元素 $g_t \leftarrow D_{\mathbb{Z}^n, \sigma}$, 满足条件 $\beta_t = |R/\langle g_t \rangle| = |\det(\text{Rot}(g_t))| > 2^\lambda$, 并且在 $\mathbb{K}$ 上有 $\|g_t\| \leq \sqrt{n}\sigma$ 和 $\|g_t^{-1}\| < l_{-1}$. 记 $g_t \in R$ 生成的主理想 $I_t = \langle g_t \rangle \subset R$.

(1.4) 抽样素理想元素 $f_t \leftarrow D_{\mathbb{Z}^n, \sigma}$, 满足条件在 $\mathbb{K}$ 上有 $\|f_t\| < \sqrt{n}\sigma$ 和 $\|f_t^{-1}\| < l_{-1}$;

(1.5) 对于 $j \in \llbracket \tau \rrbracket$:

(1.5.1) 抽样选取元素 $x_{j,t} \leftarrow D_{\mathbb{Z}^n, \sigma'}$;

(1.5.2) 计算 $e_{j,t} = [x_{j,t}]_{g_t}, a_{j,t} = (x_{j,t} - e_{j,t})/g_t$;

(1.5.3) 产生明文元素 $e_{j,t}$ 的 1-级编码

$$y_{j,t} = [x_{j,t}/z_t]_{q_t};$$

(1.6) 对于 $j \in \llbracket \tau \rrbracket$:

(1.6.1) 抽样选取元素 $b_{j,t} \leftarrow D_{\mathbb{Z}^n, \sigma^*}$;

(1.6.2) 计算 $h_{j,t} = e_{j,t} f_t + b_{j,t} g_t$;

(1.6.3) 产生“0”测试参数 $p_{z_t, j, t} = [h_{j,t} z_t^\kappa / g_t]_{q_t}$; $p_{z_t, j, t}$ 不仅是“0”测试参数, 也是明文 $e_{j,t}$ 的特殊 0-级编码, 与 $y_{j,t}$ 中的 0-级编码 $e_{j,t}$ 一一对应.

(1.7) 第 t 方发布公开参数

$$par_t = \{q_t, \{y_{j,t}, p_{z_t, j, t}\}_{j \in \llbracket \tau \rrbracket}\}.$$

//这里假定素数 q_t 两两互素. 实际上, 随机抽样的 N 个足够大的 q_t 两两互素的概率几乎为 1.

(2) 第 t 方使用 CRT 将所有方的公开参数 $\{par_1, \dots, par_N\}$ 进行组合, 以产生所有方共用的公共参数 PAR .

(2.1) 计算模 $q = \prod_{s=1}^N q_s$;

(2.2) 对于 $s \in \llbracket N \rrbracket$, 计算

$$p_s = q/q_s, w_s = (p_s)^{-1} \bmod q_s;$$

(2.3) 对于 $j \in \llbracket \tau \rrbracket$, 使用 CRT 计算产生 R_q 上 1-级编码:

$$y_j = \text{CRT}(y_{j,1}, \dots, y_{j,N});$$

(2.4) 对于 $j \in \llbracket \tau \rrbracket$, 使用 CRT 计算产生 R_q 上“0”测试参数:

$$p_{z_t, j} = \text{CRT}(p_1 p_{z_t, j, 1}, \dots, p_N p_{z_t, j, N}).$$

(3) 第 t 方输出所有方共用的公共参数

$$PAR = \{\{q_s, p_s, w_s\}_{s \in \llbracket N \rrbracket}, q, \{y_j, p_{z_t, j}\}_{j \in \llbracket \tau \rrbracket}\}.$$

高斯抽样 CRT 编码算法 $d_j \leftarrow \text{CRTSamp}(PAR)$:

(1) 使用高斯抽样算法选取 N 个元素

$$d_{j,1}, \dots, d_{j,N} \leftarrow D_{\mathbb{Z}^n, \sigma_1^*};$$

(2) 使用 CRT 计算产生 R_q 上 0-级编码元素

$$d_j = \text{CRT}(d_{j,1}, \dots, d_{j,N}).$$

1-级编码算法 $u \leftarrow \text{ENC}(PAR, 1, \{d_j\}_{j \in [t]}):$

(1) 使用高斯抽样 CRT 编码算法产生

$$d_j \leftarrow \text{CRTSamp}(PAR), j \in [t];$$

(2) 计算产生 R_q 上 1-级编码 $u = \left[\sum_{j \in [t]} d_j y_j \right]_q$.

加法编码算法 $u \leftarrow \text{ADD}(PAR, k, u_1, \dots, u_m):$

给定 m 个 k -级编码 u_l , 则它们和 $u = \left[\sum_{l=1}^m u_l \right]_q$

是一个 k -级编码.

乘法编码算法 $u \leftarrow \text{MUL}(PAR, 1, u_1, \dots, u_k):$

给定 k 个 1-级编码 u_l , 则它们积 $u = \left[\prod_{l=1}^k u_l \right]_q$

是一个 k -级编码.

“0”测试算法 $\text{ISZero}(PAR, \{d_j\}_{j \in [t]}, u):$

(1) 给定 $d_j \leftarrow \text{CRTSamp}(PAR), j \in [t]$, 计算

产生“0”测试参数 $p_{zt} = \left[\sum_{j \in [t]} d_j p_{zt,j} \right]_q$;

(2) 给定一个 κ -级编码 u , 计算“0”测试函数

ISZero 以判定 u 中明文元素是否为“0”, 即

$$\text{ISZero}(PAR, \{d_j\}_{j \in [t]}, u) =$$

$$\begin{cases} 1, & \text{如果 } \|[u \cdot p_{zt}]_q\|_{\infty} < q / (q_{\min})^{1/8} \\ 0, & \text{否则} \end{cases},$$

其中 $q_{\min} = \min\{q_s, s \in [N]\}$, 下文 $q_{\min}$ 与此相同.

提取算法 $w \leftarrow \text{EXT}(PAR, \{d_j\}_{j \in [t]}, u):$

(1) 给定 $d_j \leftarrow \text{CRTSamp}(PAR), j \in [t]$, 计算

产生“0”测试参数 $p_{zt} = \left[\sum_{j \in [t]} d_j p_{zt,j} \right]_q$;

(2) 给定一个 κ -级编码 u , 计算提取编码 $v =$

$$[u \cdot p_{zt}]_q;$$

(3) 从 v 的每个系数中提取 $l = (\log q_{\min}) / 8 - \lambda$

个最有意义的比特位, 输出提取比特串 w , 即

$$w = \text{EXT}(PAR, \{d_j\}_{j \in [t]}, u) = \text{MSB}_l(v).$$

6.2.2 参数设置

由于无可信安装构造使用新随机化构造作为基本构件, 因此在各方产生各自的公开参数 par_i 时, 所用参数的大小设置仍与第 3.1.3 节相同. 构造中其它参数大小则根据 CRT 计算产生.

参数大小具体设置如下:

λ : 安全参数.

$\kappa = \text{poly}(\lambda)$: 多线性映射的次数.

$n = O(\kappa \lambda \log \lambda)$: 多项式环的维数.

$\sigma = O(n \log n)$: 秘密素理想元素的抽样参数.

$\sigma' = O(n^3)$: 公开参数中 1-级编码的抽样参数.

$\sigma_1^* = O(n^{5.5})$: 1-级编码算法的高斯抽样参数;

产生 0-级编码的高斯抽样参数.

$\sigma^* = O(q_{\min}^{5/8})$: “0”测试参数的高斯抽样参数.

$q_t = O(n^{92\kappa})$: 第 t 方产生公开参数 par_t 时的模.

$q = \prod_{t=1}^N q_t = O(n^{92\kappa N})$: 构造中编码的模.

$q_{\min} = \min\{q_t, t \in [N]\}$: 参与方中最小的模 q_t .

$\tau = 2$: 公共参数中编码与“0”测试参数对的个数.

$l_{-1} = n$: 秘密素理想元素逆的范数上界.

$l = (\log q_{\min}) / 8 - \lambda$: 从提取编码的每个系数中提取 l 个最有意义的比特位.

所以, 根据上述参数设置, 构造中编码大小约为 $n|q| \approx 92\kappa N n \log n$, 公共参数大小约为 $2\tau n|q|$, 其中 $|q|$ 为 q 的比特长度.

6.3 正确性

6.3.1 证明思路

由 CRT 原理可知, 给定环 R_q 上任意两个 CRT 形式的元素, 加法是将它们的 CRT 形式中的对应分量相加; 乘法是将它们的 CRT 形式中的对应分量相乘.

因此, 证明基本思路就是使用 CRT 原理, 证明构造中的编码支持加法和乘法运算, 而且使用 CRT 形式的“0”测试参数能够判定编码是否为明文“0”的编码. 为此, 我们主要证明以下 3 点:

(1) 如果两个编码的级数相同, 则它们能够实行加法运算. 不失一般性, 设 u_1, u_2 为构造中 CRT 形式的 i -级编码, 即 $u_1 = \text{CRT}\left(\frac{a_1}{z_1^i}, \dots, \frac{a_N}{z_N^i}\right)$ 和 $u_2 =$

$\text{CRT}\left(\frac{b_1}{z_1^i}, \dots, \frac{b_N}{z_N^i}\right)$. 则根据 CRT 原理可知, 它们和 u

仍为 R_q 上 CRT 形式的 i -级编码, 即 $u = [u_1 + u_2]_q =$

$$\text{CRT}\left(\frac{a_1 + b_1}{z_1^i}, \dots, \frac{a_N + b_N}{z_N^i}\right).$$

(2) 如果两个编码级数和不大 κ , 则它们能够实行乘法运算. 不失一般性, 设 $u_1 = \text{CRT}\left(\frac{a_1}{z_1^i}, \dots, \frac{a_N}{z_N^i}\right)$,

$u_2 = \text{CRT}\left(\frac{b_1}{z_1^j}, \dots, \frac{b_N}{z_N^j}\right)$ 分别为 CRT 形式的 i -级编码

和 j -级编码, 且 $i+j \leq \kappa$. 则由 CRT 原理可知, 它们积 u 为环 R_q 上 CRT 形式的 $(i+j)$ -级编码, 即

$$u = [u_1 \cdot u_2]_q = \text{CRT}\left(\frac{a_1 \cdot b_1}{z_1^{i+j}}, \dots, \frac{a_N \cdot b_N}{z_N^{i+j}}\right).$$

(3) 如果一个 κ -级编码 u 是明文“0”的编码, 则该编码与“0”测试参数相乘产生的元素范数较小.

一方面, 因为 u 为环 R_q 上 CRT 形式的 κ -级编

码, 并且其包含的明文为“0”, 即

$$\mathbf{u} = \text{CRT}\left(\frac{\mathbf{c}_1}{\mathbf{z}_1^\kappa}, \dots, \frac{\mathbf{c}_N}{\mathbf{z}_N^\kappa}\right) = \text{CRT}\left(\frac{\mathbf{c}'_1 \mathbf{g}_1}{\mathbf{z}_1^\kappa}, \dots, \frac{\mathbf{c}'_N \mathbf{g}_N}{\mathbf{z}_N^\kappa}\right).$$

另一方面, “0”测试参数也是环 R_q 上 CRT 形式, 即 $\mathbf{p}_{zt} = \text{CRT}\left(p_1 \cdot \frac{\mathbf{h}_1 \mathbf{z}_1^\kappa}{\mathbf{g}_1}, \dots, p_N \cdot \frac{\mathbf{h}_N \mathbf{z}_N^\kappa}{\mathbf{g}_N}\right)$.

因此, $\mathbf{v} = [\mathbf{u} \cdot \mathbf{p}_{zt}]_q = \text{CRT}(p_1 \mathbf{h}_1 \mathbf{c}'_1, \dots, p_N \mathbf{h}_N \mathbf{c}'_N)$.

根据下面引理 29、30 可得

$$\begin{aligned} \mathbf{v} &= \text{CRT}(p_1 \mathbf{h}_1 \mathbf{c}'_1, \dots, p_N \mathbf{h}_N \mathbf{c}'_N) \\ &= \left[\sum_{t=1}^N p_t \mathbf{h}_t \mathbf{c}'_t \right]_q. \end{aligned}$$

由于 $\|p_t \mathbf{h}_t \mathbf{c}'_t\| \ll q$, 且 $N = \kappa + 1 = \text{poly}(\lambda)$, 所以 $\mathbf{v} = \sum_{t=1}^N p_t \mathbf{h}_t \mathbf{c}'_t$ 没有实行模 q 运算. 即“0”测试算法能够正确判定 κ -级编码 $\mathbf{u}$ 中的明文元素是否为“0”.

6.3.2 正确性证明

引理 27. 算法 $\text{PAR} \leftarrow \text{INSTGen}(1^\lambda, 1^\kappa)$ 运行在概率多项式时间, 并以几乎为 1 的概率输出公共参数 PAR .

证明. (1) 由引理 18 可得, 每一方都能够在概率多项式时间内产生参数 $\text{par}_t = \{q_t, \{y_{j,t}, p_{zt,j,t}\}_{j \in [r]}\}$, $t \in [N]$. 同时, 由于素数 $q_t = O(n^{92\kappa})$, 则根据引理 9 中的素数定理可证 $q_t, t \in [N]$ 两两互素的概率几乎为 1.

(2) 给定参数 $\{\text{par}_t, t \in [N]\}$, 根据 CRT 原理计算产生公共参数 PAR . 这一步显然能够在多项式时间内计算完成.

(3) 由于每一方都使用相同参数 $\{\text{par}_t, t \in [N]\}$ 产生公共参数 PAR , 故每一方使用 CRT 计算产生的公共参数 PAR 也相同. 证毕.

在证明构造中其它算法的正确性前, 我们先给出与 CRT 相关的几个引理.

引理 28. 给定公共参数 PAR , 则当 $t \neq i$ 时有

$$\begin{aligned} [p_t \cdot \omega_t \cdot p_t]_q &= p_t; \\ [p_t \cdot \omega_t \cdot p_i]_q &= 0. \end{aligned}$$

证明. 因为 $\omega_t = (p_t)^{-1} \bmod q_t$, 故 $\omega_t \cdot p_t = 1 \bmod q_t$, 即存在一个整数 $k_t \in \mathbb{Z}$, 使得 $\omega_t \cdot p_t = 1 + k_t \cdot q_t$.

所以, 由 $p_t = q/q_t$ 可得

$$[p_t \cdot \omega_t \cdot p_t]_q = p_t.$$

因为 $q = \prod_{t=1}^N q_t$, 并且 $q_t, t \in [N]$ 两两互素, 所以当 $t \neq i$ 时, 则 q_t 整除 $p_i = q/q_i$. 故可得

$$[p_t \cdot \omega_t \cdot p_i]_q = 0.$$

证毕.

引理 29. 给定公共参数 PAR 和环 R_q 上任意两个 CRT 形式的元素 $\mathbf{a} = \text{CRT}(\mathbf{a}_1, \dots, \mathbf{a}_N)$, $\mathbf{b} = \text{CRT}(\mathbf{b}_1, \dots, \mathbf{b}_N)$, 则

$$\begin{aligned} [\mathbf{a} + \mathbf{b}]_q &= \text{CRT}(\mathbf{a}_1 + \mathbf{b}_1, \dots, \mathbf{a}_N + \mathbf{b}_N) \\ &= \text{CRT}([\mathbf{a}_1 + \mathbf{b}_1]_{q_1}, \dots, [\mathbf{a}_N + \mathbf{b}_N]_{q_N}) \quad (3) \end{aligned}$$

$$\begin{aligned} [\mathbf{a} \cdot \mathbf{b}]_q &= \text{CRT}(\mathbf{a}_1 \cdot \mathbf{b}_1, \dots, \mathbf{a}_N \cdot \mathbf{b}_N) \\ &= \text{CRT}([\mathbf{a}_1 \cdot \mathbf{b}_1]_{q_1}, \dots, [\mathbf{a}_N \cdot \mathbf{b}_N]_{q_N}) \quad (4) \end{aligned}$$

证明. 由第 6.1 节的式(2)和引理 28, 可得式(3)

$$\begin{aligned} [\mathbf{a} + \mathbf{b}]_q &= [\text{CRT}(\mathbf{a}_1, \dots, \mathbf{a}_N) + \text{CRT}(\mathbf{b}_1, \dots, \mathbf{b}_N)]_q \\ &= \left[\left[\sum_{t=1}^N \mathbf{a}_t \cdot p_t \cdot \omega_t \right]_q + \left[\sum_{t=1}^N \mathbf{b}_t \cdot p_t \cdot \omega_t \right]_q \right]_q \\ &= \left[\sum_{t=1}^N (\mathbf{a}_t + \mathbf{b}_t) \cdot p_t \cdot \omega_t \right]_q \\ &= \text{CRT}(\mathbf{a}_1 + \mathbf{b}_1, \dots, \mathbf{a}_N + \mathbf{b}_N) \\ &= \left[\sum_{t=1}^N ([\mathbf{a}_t + \mathbf{b}_t]_{q_t} + q_t \delta_t) \cdot p_t \cdot \omega_t \right]_q \\ &= \left[\sum_{t=1}^N [\mathbf{a}_t + \mathbf{b}_t]_{q_t} \cdot p_t \cdot \omega_t \right]_q \\ &= \text{CRT}([\mathbf{a}_1 + \mathbf{b}_1]_{q_1}, \dots, [\mathbf{a}_N + \mathbf{b}_N]_{q_N}), \end{aligned}$$

其中 $\delta_t, t \in [N]$ 为环 R 中未指定的元素, 下同.

类似地, 可得式(4)

$$\begin{aligned} [\mathbf{a} \cdot \mathbf{b}]_q &= [\text{CRT}(\mathbf{a}_1, \dots, \mathbf{a}_N) \cdot \text{CRT}(\mathbf{b}_1, \dots, \mathbf{b}_N)]_q \\ &= \left[\left[\sum_{t=1}^N \mathbf{a}_t \cdot p_t \cdot \omega_t \right]_q \cdot \left[\sum_{t=1}^N \mathbf{b}_t \cdot p_t \cdot \omega_t \right]_q \right]_q \\ &= \left[\sum_{t=1}^N \mathbf{a}_t \cdot \mathbf{b}_t \cdot p_t \cdot \omega_t \right]_q \\ &= \text{CRT}(\mathbf{a}_1 \cdot \mathbf{b}_1, \dots, \mathbf{a}_N \cdot \mathbf{b}_N) \\ &= \left[\sum_{t=1}^N ([\mathbf{a}_t \cdot \mathbf{b}_t]_{q_t} + q_t \delta_t) \cdot p_t \cdot \omega_t \right]_q \\ &= \text{CRT}([\mathbf{a}_1 \cdot \mathbf{b}_1]_{q_1}, \dots, [\mathbf{a}_N \cdot \mathbf{b}_N]_{q_N}). \quad \text{证毕.} \end{aligned}$$

从引理 29 可以看出, CRT 形式中各个分量是否进行相应模计算不影响 CRT 的结果, 即 CRT 形式中第 t 个分量是否取模 q_t 不影响 CRT 的结果, 因为根据 CRT 原理这个结果是唯一的.

引理 30. 给定公共参数 PAR 和任意向量 $(\mathbf{a}_1, \dots, \mathbf{a}_N)$, 则

$$\mathbf{a} = \text{CRT}(p_1 \mathbf{a}_1, \dots, p_N \mathbf{a}_N) = \left[\sum_{t=1}^N p_t \mathbf{a}_t \right]_q.$$

证明. 由 6.1 节 CRT 公式(2)和引理 28, 可得

$$\begin{aligned} \mathbf{a} &= \text{CRT}(p_1 \mathbf{a}_1, \dots, p_N \mathbf{a}_N) \\ &= \left[\sum_{t=1}^N (p_t \mathbf{a}_t) \cdot p_t \cdot \omega_t \right]_q \\ &= \left[\sum_{t=1}^N \mathbf{a}_t \cdot (p_t \cdot p_t \cdot \omega_t) \right]_q \\ &= \left[\sum_{t=1}^N p_t \mathbf{a}_t \right]_q. \end{aligned}$$

证毕.

引理 31. 给定公共参数 PAR , 则

$$p_{zt,j} = \left[\sum_{t=1}^N p_t p_{zt,j,t} \right]_q.$$

证明. 由引理 30 直接得证. 证毕.

引理 32. 高斯抽样 CRT 编码算法输出 $d_j \leftarrow \text{CRTSamp}(PAR)$ 为 0-级编码.

证明. 由 $d_j = \text{CRT}(d_{j,1}, \dots, d_{j,N})$ 可得

$$d_j = \text{CRT}\left(\left[\frac{d_{j,1}}{z_1^0}\right], \dots, \left[\frac{d_{j,N}}{z_N^0}\right]\right),$$

其中 $z_t^0 = 1, t \in [N]$. 证毕.

引理 33. 设 $u \leftarrow \text{ENC}(PAR, 1, \{d_j\}_{j \in [\tau]})$, 其中 $d_j \leftarrow \text{CRTSamp}(PAR)$, 则 u 为 1-级编码.

证明. 由引理 29 可得

$$\begin{aligned} u &= \left[\sum_{j \in [\tau]} d_j y_j \right]_q \\ &= \left[\sum_{j \in [\tau]} \text{CRT}(d_{j,1}, \dots, d_{j,N}) \text{CRT}(y_{j,1}, \dots, y_{j,N}) \right]_q \\ &= \left[\sum_{j \in [\tau]} \text{CRT}(d_{j,1} y_{j,1}, \dots, d_{j,N} y_{j,N}) \right]_q \\ &= \text{CRT}\left(\sum_{j \in [\tau]} d_{j,1} y_{j,1}, \dots, \sum_{j \in [\tau]} d_{j,N} y_{j,N}\right) \\ &= \text{CRT}\left(\left[\frac{\sum_{j \in [\tau]} d_{j,1} x_{j,1}}{z_1}\right]_{q_1}, \dots, \left[\frac{\sum_{j \in [\tau]} d_{j,N} x_{j,N}}{z_N}\right]_{q_N}\right) \\ &= \text{CRT}\left(\left[\frac{c_1}{z_1}\right]_{q_1}, \dots, \left[\frac{c_N}{z_N}\right]_{q_N}\right), \end{aligned}$$

其中 $c_t = \sum_{j \in [\tau]} d_{j,t} x_{j,t}, t \in [N]$. 证毕.

引理 34. 设 $u \leftarrow \text{ADD}(PAR, k, u_1, \dots, u_m)$ 为 m 个 k -级编码 u_r 的和, 则 u 仍为 k -级编码.

证明. 不失一般性, 设 k -级编码 u_r 为

$$u_r = \text{CRT}\left(\left[\frac{c_{r,1}}{z_1^k}\right]_{q_1}, \dots, \left[\frac{c_{r,N}}{z_N^k}\right]_{q_N}\right).$$

因为 $u = \left[\sum_{r=1}^m u_r \right]_q$, 所以

$$\begin{aligned} u &= \left[\sum_{r=1}^m \text{CRT}\left(\left[\frac{c_{r,1}}{z_1^k}\right]_{q_1}, \dots, \left[\frac{c_{r,N}}{z_N^k}\right]_{q_N}\right) \right]_q \\ &= \text{CRT}\left(\left[\frac{\sum_{r=1}^m c_{r,1}}{z_1^k}\right]_{q_1}, \dots, \left[\frac{\sum_{r=1}^m c_{r,N}}{z_N^k}\right]_{q_N}\right) \\ &= \text{CRT}\left(\left[\frac{c_1}{z_1^k}\right]_{q_1}, \dots, \left[\frac{c_N}{z_N^k}\right]_{q_N}\right), \end{aligned}$$

其中 $c_t = \sum_{r=1}^m c_{r,t}, t \in [N]$. 证毕.

引理 35. 设 $u \leftarrow \text{MUL}(PAR, 1, u_1, \dots, u_k)$ 为 k 个 1-级编码 u_l 的积, 则 u 为 k -级编码.

证明. 不失一般性, 设 1-级编码 u_r 为

$$u_r = \text{CRT}\left(\left[\frac{c_{r,1}}{z_1}\right]_{q_1}, \dots, \left[\frac{c_{r,N}}{z_N}\right]_{q_N}\right).$$

所以

$$\begin{aligned} u &= \left[\prod_{r=1}^k u_r \right]_q = \left[\prod_{r=1}^k \text{CRT}\left(\left[\frac{c_{r,1}}{z_1}\right]_{q_1}, \dots, \left[\frac{c_{r,N}}{z_N}\right]_{q_N}\right) \right]_q \\ &= \text{CRT}\left(\left[\frac{\prod_{r=1}^k c_{r,1}}{z_1^k}\right]_{q_1}, \dots, \left[\frac{\prod_{r=1}^k c_{r,N}}{z_N^k}\right]_{q_N}\right) \\ &= \text{CRT}\left(\left[\frac{c_1}{z_1^k}\right]_{q_1}, \dots, \left[\frac{c_N}{z_N^k}\right]_{q_N}\right), \end{aligned}$$

其中 $c_t = \prod_{r=1}^k c_{r,t}, t \in [N]$. 证毕.

虽然计算求解 κ -级编码 u 编码的明文是困难的, 但是利用“0”测试参数却可以判定一个 κ -级编码中明文编码是否为“0”. 因此, 根据编码的加法同态性, 我们能够判断两个 κ -级编码的差中明文元素是否为“0”, 即可以判定两个 κ -级编码中的明文元素是否相同.

引理 36. 设 $u = \text{CRT}\left(\left[\frac{c_1}{z_1^\kappa}\right]_{q_1}, \dots, \left[\frac{c_N}{z_N^\kappa}\right]_{q_N}\right)$ 为一个 κ -级编码, 则对任意 $t \in [N]$, $\|c_t\| \leq q_t^{1/8}$.

证明. 因为一个 κ -级编码是由 κ 个 1-级编码的乘积产生, 所以不失一般性, 设 u 为 κ 个 1-级编码 u_r 的乘积, 即 $u = \left[\prod_{r=1}^\kappa u_r \right]_q$.

因为 1-级编码 u_r 都是使用算法 ENC 产生, 故可设

$u_r \leftarrow \text{ENC}(PAR, 1, \{d_{r,j}\}_{j \in [\tau]}), r \in [\kappa]$, 其中 $d_{r,j} \leftarrow \text{CRTSamp}(PAR)$.

所以, 由引理 33 得

$$\begin{aligned} u_r &= \left[\sum_{j \in [\tau]} d_{r,j} y_j \right]_q \\ &= \left[\sum_{j \in [\tau]} \text{CRT}(d_{r,j,1}, \dots, d_{r,j,N}) \text{CRT}(y_{j,1}, \dots, y_{j,N}) \right]_q \\ &= \text{CRT}\left(\left[\frac{\sum_{j \in [\tau]} d_{r,j,1} x_{j,1}}{z_1}\right]_{q_1}, \dots, \left[\frac{\sum_{j \in [\tau]} d_{r,j,N} x_{j,N}}{z_N}\right]_{q_N}\right) \\ &= \text{CRT}\left(\left[\frac{c_{r,1}}{z_1}\right]_{q_1}, \dots, \left[\frac{c_{r,N}}{z_N}\right]_{q_N}\right), \end{aligned}$$

其中 $c_{r,t} = \sum_{j \in [\tau]} d_{r,j,t} x_{j,t}, t \in [N]$.

所以, 由引理 35 可得

$$u = \left[\prod_{r=1}^\kappa u_r \right]_q = \text{CRT}\left(\left[\frac{c_1}{z_1^\kappa}\right]_{q_1}, \dots, \left[\frac{c_N}{z_N^\kappa}\right]_{q_N}\right),$$

其中 $c_t = \prod_{r=1}^\kappa c_{r,t}$.

由第 6.2.2 节参数设置知, 以概率几乎为 1 有

$$\begin{aligned} \|c_{r,t}\| &\leq \tau \cdot n \cdot \|d_{r,j,t}\| \cdot \|x_{j,t}\| \\ &\leq 2n \cdot \sqrt{n} \sigma_1^* \cdot \sqrt{n} \sigma' \\ &\leq \tau n \cdot \sqrt{n} \cdot O(n^{5.5}) \cdot \sqrt{n} \cdot O(n^3) \\ &= O(n^{10.5}). \end{aligned}$$

因此,对任意 $t \in [N]$,

$$\begin{aligned}\|c_t\| &= \left\| \prod_{r=1}^{\kappa} c_{r,t} \right\| \\ &\leq n^{\kappa-1} O(n^{10.5})^{\kappa} \\ &< O(n^{11.5})^{\kappa} \\ &\leq (q_{\min})^{1/8} \\ &\leq (q_t)^{1/8}.\end{aligned}\quad \text{证毕.}$$

定理 1. 设参数大小设置如 6.2.2 节定义. 给定一个 κ -级编码 u , 则“0”测试算法 $\text{ISZero}(PAR, \{d_j\}_{j \in [z]}, u)$ 能够判定 u 中的明文元素是否为“0”, 其中 $d_j \leftarrow \text{CRTSamp}(PAR), j \in [\tau]$.

证明. 由引理 29 可得

$$\begin{aligned}p_{zt} &= \left[\sum_{j \in [\tau]} d_j p_{zt,j} \right]_q \\ &= \left[\sum_{j \in [\tau]} \text{CRT}(p_1 d_{j,1} p_{zt,j,1}, \dots, p_N d_{j,N} p_{zt,j,N}) \right]_q \\ &= \text{CRT}(p_1 \sum_{j \in [\tau]} d_{j,1} p_{zt,j,1}, \dots, p_N \sum_{j \in [\tau]} d_{j,N} p_{zt,j,N}) \\ &= \text{CRT}\left(p_1 \left[\frac{h_1 z_1^{\kappa}}{g_1} \right]_{q_1}, \dots, p_N \left[\frac{h_N z_N^{\kappa}}{g_N} \right]_{q_N}\right),\end{aligned}$$

其中 $h_t = \sum_{j \in [\tau]} d_{j,t} h_{j,t}, t \in [N]$.

又因 u 为 κ -级编码, 不失一般性, 设

$$u = \text{CRT}\left(\left[\frac{c_1}{z_1^{\kappa}}\right]_{q_1}, \dots, \left[\frac{c_N}{z_N^{\kappa}}\right]_{q_N}\right).$$

所以由引理 30 可得

$$\begin{aligned}[u \cdot p_{zt}]_q &= \\ &\text{CRT}\left(p_1 \left[\frac{h_1 z_1^{\kappa}}{g_1} \cdot \frac{c_1}{z_1^{\kappa}} \right]_{q_1}, \dots, p_N \left[\frac{h_N z_N^{\kappa}}{g_N} \cdot \frac{c_N}{z_N^{\kappa}} \right]_{q_N}\right) \\ &= \text{CRT}\left(p_1 \left[\frac{h_1 c_1}{g_1} \right]_{q_1}, \dots, p_N \left[\frac{h_N c_N}{g_N} \right]_{q_N}\right) \\ &= \left[\sum_{t=1}^N (p_t \cdot [h_t \cdot c_t / g_t]_{q_t}) \right]_q.\end{aligned}$$

现根据 u 中明文是否为“0”分别分析如下:

(1) 如果 κ -级编码 u 中的明文元素为“0”, 则

$$\| [u \cdot p_{zt}]_q \| \leq q / (q_{\min})^{1/8}.$$

因为 u 是明文“0”的编码, 所以对所有 $t \in [N]$, c_t 是理想 $I_t = \langle g_t \rangle$ 中元素, 故 $c_t / g_t \in R_{q_t}$ 与元素 $c_t \cdot g_t^{-1} \in \mathbb{Z}$ 相同.

又由引理 36 知 $\|c_t\| \leq q_t^{1/8}$, 所以,

$$\| [c_t / g_t]_{q_t} \| = \| c_t \cdot g_t^{-1} \| \leq n \cdot \| c_t \| \cdot \| g_t^{-1} \| \leq n^2 \cdot q_t^{1/8}.$$

又由 $h_t = \sum_{j \in [\tau]} d_{j,t} (e_{j,t} f + b_{j,t} g_t)$ 可得

$$\begin{aligned}\|h_t\| &= \left\| \sum_{j \in [\tau]} d_{j,t} (e_{j,t} f + b_{j,t} g_t) \right\| \\ &\leq 2n \cdot \|d_{j,t}\| \cdot \|e_{j,t} f + b_{j,t} g_t\| \\ &\leq 2n \cdot \sqrt{n} \sigma_1^* \cdot (2 \cdot n \cdot \|b_{j,t}\| \cdot \|g_t\|) \\ &< O(n^7) \cdot (2n \cdot \sqrt{n} \sigma^* \cdot \sqrt{n} \sigma) \\ &= O(n^{10} \log n) q_{\min}^{5/8} \\ &\leq O(n^{10} \log n) q_t^{5/8}.\end{aligned}$$

所以,

$$\begin{aligned}\|h_t \cdot c_t \cdot g_t^{-1}\| &\leq n \cdot \|h_t\| \cdot \|c_t \cdot g_t^{-1}\| \\ &\leq n \cdot O(n^{10} \log n) q_t^{5/8} \cdot (n^2 \cdot q_t^{1/8}) \\ &\leq O(n^{13} \log n) q_t^{3/4}.\end{aligned}$$

因此, $[h_t \cdot c_t / g_t]_{q_t} = h_t \cdot c_t \cdot g_t^{-1}$.

又因 $N = \kappa + 1 = \text{poly}(\lambda)$ 可得

$$\begin{aligned}\left\| \sum_{t=1}^N (p_t \cdot h_t \cdot c_t \cdot g_t^{-1}) \right\| &\leq \sum_{t=1}^N (p_t \cdot \|h_t \cdot c_t \cdot g_t^{-1}\|) \\ &\leq \sum_{t=1}^N p_t \cdot O(n^{13} \log n) q_t^{3/4} \\ &\leq q \cdot (q_{\min})^{-1/4} \cdot \sum_{t=1}^N O(n^{13} \log n) \\ &\leq q / (q_{\min})^{1/8},\end{aligned}$$

其中最后一个不等式由 $\sum_{t=1}^N O(n^{13} \log n) < (q_{\min})^{1/8}$ 得到, 这是因为 $\kappa \geq 2$ 和 $O(n^{11.5})^{\kappa} \leq (q_{\min})^{1/8}$.

因此,

$$\left[\sum_{t=1}^N (p_t \cdot h_t \cdot c_t \cdot g_t^{-1}) \right]_q = \sum_{t=1}^N (p_t \cdot h_t \cdot c_t \cdot g_t^{-1}).$$

所以,

$$\begin{aligned}\| [u \cdot p_{zt}]_q \| &= \left\| \left[\sum_{t=1}^N (p_t \cdot [h_t \cdot c_t / g_t]_{q_t}) \right]_q \right\| \\ &= \left\| \left[\sum_{t=1}^N (p_t \cdot h_t \cdot c_t \cdot g_t^{-1}) \right]_q \right\| \\ &= \left\| \sum_{t=1}^N (p_t \cdot h_t \cdot c_t \cdot g_t^{-1}) \right\| \\ &\leq q / (q_{\min})^{1/8}.\end{aligned}$$

(2) 如果 κ -级编码 u 中的明文元素为非“0”, 则

$$\| [u \cdot p_{zt}]_q \| > q / (q_{\min})^{1/8}.$$

因为 u 是非“0”的 κ -级编码, 所以至少存在一个 $t \in [N]$, c_t 不属于理想 $I_t = \langle g_t \rangle$.

不失一般性, 可设 S 为非空集, 当 $t \in S$ 时, c_t 不属于理想 $I_t = \langle g_t \rangle$; 当 $t \in \bar{S} = [N] - S$ 时, c_t 属于理想 $I_t = \langle g_t \rangle$.

又因 h_t 以概率几乎为 1 不属于理想 $\langle g_t \rangle$, 所以由引理 17 知当 $t \in S$ 时, $\| [h_t \cdot c_t / g_t]_{q_t} \| > q_t^{1-\epsilon}$, 其中 $0 < \epsilon < 1/8$ 为小常数. 这里假设 $(q_{\min})^{1/8} \geq 2(q_{S,\min})^{\epsilon}$, 其中 $q_{S,\min} = \min\{q_t, t \in S\}$.

因此, $\| p_t \cdot [c_t h_t / g_t]_{q_t} \| > p_t \cdot q_t^{1-\epsilon} = q / q_t^{\epsilon}$.

故以概率几乎为 1 有

$$\left\| \left[\sum_{t \in S} (p_t \cdot [c_t h_t / g_t]_{q_t}) \right]_q \right\| > q / (q_{S,\min})^{\epsilon}.$$

当 $t \in \bar{S}$ 时, 根据上述(1)中分析, 可得以概率几乎为 1 有

$$\left\| \left[\sum_{t \in \bar{S}} (p_t \cdot [c_t h_t / g_t]_{q_t}) \right]_q \right\| \leq q / (q_{\min})^{1/8}.$$

所以, 以概率几乎为 1 有

$$\begin{aligned}
\| [u \cdot p_{zt}]_q \| &= \left\| \left[\sum_{t \in S} p_t \cdot [c_t h_t / g_t]_{q_t} + \sum_{t \in S} p_t \cdot [c_t h_t / g_t]_{q_t} \right]_q \right\| \\
&> \left\| \left[\sum_{t \in S} p_t \cdot [c_t h_t / g_t]_{q_t} \right]_q \right\| - \left\| \left[p_t \cdot \sum_{t \in S} [c_t h_t / g_t]_{q_t} \right]_q \right\| \\
&> q / (q_{S, \min})^\epsilon - q / (q_{\min})^{1/8} \\
&> q / (q_{\min})^{1/8}.
\end{aligned}$$

因此,“0”测试算法 ISZero 能够正确判断 κ -级编码 u 中的明文元素(0-级编码)是否为“0”. 证毕.

定理 2. 如果两个 κ -级编码 u, u' 中的 0-级编码陪集相同,则以概率几乎为 1 有

$\text{EXT}(PAR, \{d_j\}_{j \in [\tau]}, u) = \text{EXT}(PAR, \{d_j\}_{j \in [\tau]}, u')$, 其中 $d_j \leftarrow \text{CRTSamp}(PAR), j \in [\tau]$.

证明. 因为构造中同级编码满足加法同态,所以如果两个 κ -级编码 u, u' 中的 0-级编码陪集相同,则 κ -级编码 $u - u'$ 中的 0-级编码将为“0”.

由定理 1 知 $\| (u - u') \cdot p_{zt} \|_q \leq q / (q_{\min})^{1/8}$, 其中 $p_{zt} = \left[\sum_{j \in [\tau]} d_j p_{zt,j} \right]_q$.

由此可得,提取编码 $v = [u \cdot p_{zt}]_q$ 和 $v' = [u' \cdot p_{zt}]_q$ 中每个系数的最有意义的 $(\log q_{\min})/8$ 个比特位只与 0-级编码陪集相关,而与具体使用的 0-级编码代表元素无关.

因此,如果 κ -级编码 u, u' 中的 0-级编码相等,且仅在 v, v' 的每个系数中提取 $l = (\log q_{\min})/8 - \lambda$ 个最有意义的比特位,则 v 和 v' 的提取比特串相等的概率几乎为 1. 证毕.

6.4 安全性

为给出构造安全性假设,本节首先引入无可信安装的难度假设问题 wots-ext-GCDH/wots-ext-GDDH,然后给出无可信安装构造的已知攻击分析.

6.4.1 安全假设

为定义 wots-ext-GCDH/wots-ext-GDDH 难度问题,我们先考虑无可信安装构造的安全实验过程:

(1) 产生公共参数 $PAR \leftarrow \text{INSTGen}(1^\lambda, 1^\kappa)$.

(2) 对于 $r=0, 1, \dots, \kappa$:

(2.1) 调用高斯抽样 CRT 编码算法抽样

$$d_{r,j} \leftarrow \text{CRTSamp}(PAR), j \in [\tau];$$

$$r_{r,j} \leftarrow \text{CRTSamp}(PAR), j \in [\tau].$$

(2.2) 计算产生 1-级编码:

$$u_r \leftarrow \text{ENC}(PAR, 1, \{d_{r,j}\}_{j \in [\tau]}).$$

(3) 计算 κ -级编码 $u^* = \left[\prod_{r=1}^{\kappa} u_r \right]_q$.

(4) 计算产生两个“0”测试参数

(4.1) 计算与编码 u_0 对应的“0”测试参数

$$p_{zt} = \left[\sum_{j \in [\tau]} d_{0,j} p_{zt,j} \right]_q;$$

(4.2) 计算随机的“0”测试参数

$$p_{zt, \text{Rand}} = \left[\sum_{j \in [\tau]} r_{0,j} p_{zt,j} \right]_q.$$

(5) 产生提取比特串

$$w_C = w_D = \text{MSB}_l([u^* \cdot p_{zt}]_q).$$

(6) 产生随机提取比特串

$$w_{\text{Rand}} = \text{MSB}_l([u^* \cdot p_{zt, \text{Rand}}]_q).$$

定义 6 (wots-ext-GCDH/wots-ext-GDDH). 根据上述安全实验,安全假设问题 wots-ext-GCDH/wots-ext-GDDH 定义如下:

无可信安装的 κ -级提取 CDH 问题(wots-ext-GCDH): 给定 $\{PAR, u_0, \dots, u_\kappa\}$, 计算输出提取比特串 w_C .

无可信安装的 κ -级提取 DDH 问题(wots-ext-GDDH): 给定 $\{PAR, u_0, \dots, u_\kappa\}$, 区分分布 w_D 和 w_{Rand} , 即区分分布:

$$D_{\text{wots-ext-GDDH}} = \{PAR, u_0, \dots, u_\kappa, w_D\},$$

$$D_{\text{wots-ext-Rand}} = \{PAR, u_0, \dots, u_\kappa, w_{\text{Rand}}\}.$$

评论 5. 虽然难度问题 wots-ext-GCDH/wots-ext-GDDH 与问题 ext-GCDH/ext-GDDH 在形式上相似,但是并不能在它们之间建立多项式时间计算难度上的等价关系. 因为虽然在公开参数 par_i 环境下, $([u_0]_{q_i}, \dots, [u_\kappa]_{q_i})$ 为其 1-级编码, $[u^*]_{q_i}$ 为其 κ -级编码,但是对于提取比特串 w_C, w_D , 并不能得到类似关系,即下面关系式并不成立:

$$[w_C]_{q_i} = [w_D]_{q_i} \neq \text{MSB}_l([u^* \cdot p_{zt}]_{q_i});$$

$$[w_C]_{q_i} = [w_D]_{q_i} \neq \text{MSB}_l\left(\sum_{t=1}^N \text{MSB}_l([u^* \cdot p_{zt}]_{q_i})\right).$$

由于无法建立 wots-ext-GCDH/wots-ext-GDDH 与 ext-GCDH/ext-GDDH 的提取比特串之间的关系,导致无法归约证明它们在计算难度上多项式时间等价.

假设 3. 假定任何概率多项式时间算法 A 攻击提取问题 wots-ext-GCDH/wots-ext-GDDH 的概率优势是可忽略的,即

对于 wots-ext-GCDH 问题,我们有

$$\Pr[A(\{PAR, u_0, \dots, u_\kappa\}) = w_C] \leq \text{negl}(\lambda);$$

对于 wots-ext-GDDH 问题,我们有

$$|\Pr[A(w_D) = 1] - \Pr[A(w_{\text{Rand}}) = 1]| \leq \text{negl}(\lambda),$$

其中算法 A 中省略了 $\{PAR, u_0, \dots, u_\kappa\}$.

评论 6. (1) 本文给出安全假设 6.15 也是为了便于证明基于无可信安装构造的应用安全性,否则基于构造的每个应用都要给出新的难度假设,容易导致应用的安全性不明确;(2) 判定问题 wots-ext-GDDH 能够归约到计算求解问题 wots-ext-GCDH. 因为如

果知道问题 wots-ext-GCDH 的提取比特串 w_C , 则能够判定 w_D 和 w_{Rand} , 即判定问题 wots-ext-GDDH. 然而, 还无法将计算问题 wots-ext-GCDH 归约到判定问题 wots-ext-GDDH.

6.4.2 已知攻击分析

无可信安装构造与基于 CRT 的 CLT13 构造不同之处主要在于: (1) 无可信安装构造中模 q 的素因子公开, 而 CLT13 构造中它们是秘密, 不能公开; (2) 无可信安装构造使用多项式环, 构造工作在理想格上, 而 CLT13 构造使用整数环, 构造工作在整数上; (3) 无可信安装构造中无明文“0”的编码, 而 CLT13 构造中存在明文“0”的编码; (4) 无可信安装构造的安全依赖于构造中多项式环的维数 n , 与模 q 的素因子个数无关, 而 CLT13 构造的安全则依赖于模 q 的素因子个数, 需要其足够大. 这些不同使得无可信安装构造避免了针对 CLT13 构造的攻击^[23,31].

由于无可信安装构造使用新随机化构造作为基本组件, 并运用多项式环上 CRT 将新随机化构造进行组合产生. 因此, 本节已知攻击分析主要包括两个方面: (1) 针对新随机化构造的攻击分析; (2) Cheon 等人的“0”化攻击扩展分析.

(1) 针对新随机化构造的攻击分析

因为各方都使用新随机化构造方法产生并发布各自的公开参数 $par_t, t \in \llbracket N \rrbracket$, 所以新随机化构造中易于计算量在无可信安装构造中同样可以计算. 例如攻击者能够通过参数 $par_t, t \in \llbracket N \rrbracket$ 计算 1-级编码 $y_{j,t}$ 与“0”测试参数 $p_{zt,j,t}$ 的交叉乘积, 从而得到主理想 $x_{j,t} = e_{j,t} + a_{j,t} g_t$ 的格基. 但从第 5.1 节分析可知, 目前利用这种格基并不能攻击新随机化构造.

(2) Cheon 等人的“0”化攻击扩展分析

本节主要分析 Cheon 等人^[31]破解 CLT13 构造的“0”化攻击方法扩展对新随机化构造的安全影响. Cheon 等人的“0”化攻击^[31]分为 3 个步骤:

第 1 步. 与 GGH13 构造^[11]中的“0”化攻击类似, 计算产生一些“0”的 κ -级编码, 并乘以“0”测试参数, 从而获得有理数 $\mathbb{Q}$ 上的矩阵方程, 即不是模归约的矩阵方程.

第 2 步. 先计算两个矩阵方程的比以移除共同项, 并产生特征值为有理数的矩阵; 然后通过计算特征值以获得对应于明文的 CRT 中各成分的比, 即在中国剩余定理中各个素数模下的余数比.

第 3 步. 使用 CRT 中各成分的比, 计算求解模的各个素因子, 并进而直接计算求解 CLT13 构造中的其它秘密量.

现在具体分析使用 Cheon 等人“0”化攻击的扩展攻击无可信安装构造方案的不可行性.

第 1 步. 这一步攻击能够实行, 但计算获得的矩阵方程是在域 $\mathbb{K} = \mathbb{Q}[x]/\langle x^n + 1 \rangle$ 上, 并不是在有理数域 $\mathbb{Q}$ 上. 由于公共参数 PAR 中无“0”的 1-级编码, 只能使用第 4.1 节的交叉乘积形式获得非模 q 归约的量.

设 $j, k, i \in \llbracket \tau \rrbracket$, 则由公共参数 PAR 可以计算得到非模 q 归约的元素 $v_{j,k,i}$:

$$\begin{aligned} v_{j,k,i} &= [y_j y_k y_i (y_1)^{\kappa-4} (y_1 p_{zt,2} - y_2 p_{zt,1})]_q \\ &= \left[\sum_{t=1}^N y_{j,t} y_{k,t} y_{i,t} (y_{1,t})^{\kappa-4} (y_{1,t} p_{zt,2,t} - y_{2,t} p_{zt,1,t}) \cdot p_t \right]_q \\ &= \left[\sum_{t=1}^N x_{j,t} x_{k,t} x_{i,t} h_t \right]_q, \end{aligned}$$

其中

$$\begin{aligned} h_t &= p_t \cdot (x_{1,t})^{\kappa-4} \cdot w_t, \\ w_t &= e_{1,t} b_{2,t} + e_{2,t} a_{1,t} f_t + a_{1,t} b_{2,t} g_t - \\ &\quad e_{2,t} b_{1,t} - e_{1,t} a_{2,t} f_t - a_{2,t} b_{1,t} g_t. \end{aligned}$$

元素 $v_{j,k,i}$ 能够被重写如下:

$$v_{j,k,i} = (x_{j,1}, \dots, x_{j,N}) \cdot \text{diag}(x_{i,1}, \dots, x_{i,N}) \cdot \text{diag}(h_1, \dots, h_N) \cdot (x_{k,1}, \dots, x_{k,N})^T,$$

其中符号 $\text{diag}(\cdot, \dots, \cdot)$ 为对角矩阵.

类似于 Cheon 等人的“0”化攻击^[31], 由选取索引对 $(j, k) \in \llbracket N \rrbracket \times \llbracket N \rrbracket$ (注意: 虽然公共参数中只包含两个 1-级编码 y_1, y_2 , 但是可以通过不同组合产生新的 1-级编码 $y = [d_1 y_1 + d_2 y_2]_q$ 以供选取, 具体细节略去), 则能够得到矩阵方程 $W_i \in \mathbb{K}^{N \times N}$ 如下:

$$W_i = \begin{pmatrix} x_{1,1} & \cdots & x_{1,N} \\ \vdots & & \vdots \\ x_{N,1} & \cdots & x_{N,N} \end{pmatrix} \cdot \begin{pmatrix} x_{i,1} & & 0 \\ & \ddots & \\ 0 & & x_{i,N} \end{pmatrix} \cdot \begin{pmatrix} h_1 & & 0 \\ & \ddots & \\ 0 & & h_N \end{pmatrix} \cdot \begin{pmatrix} x_{1,1} & \cdots & x_{N,1} \\ \vdots & \ddots & \vdots \\ x_{1,N} & \cdots & x_{N,N} \end{pmatrix}$$

$$= X \cdot \text{diag}(x_{i,1}, \dots, x_{i,N}) \cdot \text{diag}(h_1, \dots, h_N) \cdot X^T.$$

第 2 步. 这一步攻击实行时存在问题. 我们能够取 $i=1, 2$, 计算得到

$$W_1 \cdot W_2^{-1} = X \cdot \text{diag}\left(\frac{x_{1,1}}{x_{2,1}}, \dots, \frac{x_{1,N}}{x_{2,N}}\right) \cdot X^{-1},$$

这里假定 W_2 可逆.

这一步攻击计算存在两个问题: 一是目前不知道如何计算求解这种特征值, 因为特征多项式定义在域 $\mathbb{K}$ 上, 需要计算求解的元素也属于 $\mathbb{K}$, 而不是在有理数域 $\mathbb{Q}$ 上 (注意: 本文构造的公共参数中没有提供非“0”的 0-级编码, 故计算求解秘密元素时不同于 Coron 等人^[23]分析的情况); 二是即使通过特征值方法计算得到在域 $\mathbb{K}$ 上的比值. 不同于有理数域 $\mathbb{Q}$, 余数的比可直接用两个整数相除的最简分式表示, 而在域 $\mathbb{K}$ 上余数的比并不能通过消元法获得

最简的整数多项式的分式形式,即不能通过比值 $\mathbf{x}_{1,t}/\mathbf{x}_{2,t} \in \mathbb{K}$ 直接计算得到元素 $\mathbf{x}_{1,t}, \mathbf{x}_{2,t} \in R$. 实际上,通过新随机化构造中各方自己的公开参数 $\text{par}_t, t \in \llbracket N \rrbracket$,可以直接计算获得域 $\mathbb{K}$ 上这种余数的比,并不需要通过这种复杂的计算方式.

第3步. 这步攻击无需实行,因为本文构造中模的素因子公开,不需保密,然而 CLT13 构造中知道模的素因子就能求解所有秘密元素. 也就是说,通过使用 Cheon 等人的“0”化攻击^[31],攻击者获得的信息并不比直接使用第4.1节基于交叉乘积的已知攻击方法得到的信息更多.

因此, Cheon 等人的“0”化攻击^[31] 扩展不能用于攻击本文无可信安装的构造.

7 多方密钥交换协议

本文仅给出基于上述多线性映射的一轮多方密钥交换协议(MPKE)应用.

7.1 基于新随机化构造的 nr-MPKE

基于新随机化构造的一轮多方密钥交换协议(nr-MPKE)如下:

安装阶段 $\text{Setup}(1^\lambda, 1^N)$:

设 $\kappa = N-1$ 和 $S_t^* = \llbracket N \rrbracket - \{t\}, t \in \llbracket N \rrbracket$. 输出 $\text{par} \leftarrow \text{InstGen}(1^\lambda, 1^\kappa)$ 作为公共参数.

发布阶段 $\text{Publish}(\text{par}, t)$:

(1) 第 t 方抽样选择 $\mathbf{d}_{t,j} \leftarrow D_{\mathbb{Z}^n, \sigma_1^*}, j \in \llbracket \tau \rrbracket$, 并将 $\{\mathbf{d}_{t,j}\}_{j \in \llbracket \tau \rrbracket}$ 作为私钥保密.

(2) 第 t 方将 1-级编码 $u_t = \text{Enc}(\text{par}, 1, \{\mathbf{d}_{t,j}\}_{j \in \llbracket \tau \rrbracket})$ 作为公钥发布.

产生共享密钥阶段 $\text{KeyGen}(\text{par}, t, \{\mathbf{d}_{t,j}\}_{j \in \llbracket \tau \rrbracket}, \{\mathbf{u}_r\}_{r \in S_t^*})$:

(1) 第 t 方产生一个 κ -级编码 $\mathbf{u}'_t = \left[\prod_{r \in S_t^*} \mathbf{u}_r \right]_q$,

(2) 第 t 方提取共享密钥

$$sk_t = \text{Ext}(\text{par}, \{\mathbf{d}_{t,j}\}_{j \in \llbracket \tau \rrbracket}, \mathbf{u}'_t).$$

下面通过定理3和4给出上述 nr-MPKE 协议的正确性和安全性.

定理3. 上述 nr-MPKE 中算法 KeyGen 产生的 N 个共享密钥 $sk_t, t \in \llbracket N \rrbracket$ 以概率几乎为1相同.

证明. 对于任意 $t \in \llbracket N \rrbracket$, 根据提取算法 Ext 有

(1) 计算产生第 t 方的“0”测试参数

$$\begin{aligned} \mathbf{p}_{zt}^{(t)} &= \left[\sum_{j \in \llbracket \tau \rrbracket} \mathbf{d}_{t,j} \mathbf{p}_{zt,j} \right]_q \leq \\ &= \left[\sum_{j \in \llbracket \tau \rrbracket} \mathbf{d}_{t,j} (\mathbf{e}_j \mathbf{f} + \mathbf{b}_j \mathbf{g}) \mathbf{z}^\kappa / \mathbf{g} \right]_q \\ &= [(\mathbf{d}^{(t)} \mathbf{f} + \mathbf{b}^{(t)} \mathbf{g}) \mathbf{z}^\kappa / \mathbf{g}]_q, \end{aligned}$$

其中 $\mathbf{d}^{(t)} = \sum_{j \in \llbracket \tau \rrbracket} \mathbf{d}_{t,j} \mathbf{e}_j$, $\mathbf{b}^{(t)} = \sum_{j \in \llbracket \tau \rrbracket} \mathbf{d}_{t,j} \mathbf{b}_j$.

(2) 因为 $\mathbf{u}'_t = \left[\prod_{r \in S_t^*} \mathbf{u}_r \right]_q$, 所以

$$\mathbf{u}'_t = \left[\prod_{r \in S_t^*} \mathbf{x}^{(r)} / \mathbf{z}^\kappa \right]_q,$$

其中 $\mathbf{x}^{(r)} = \sum_{j \in \llbracket \tau \rrbracket} \mathbf{d}_{r,j} \mathbf{x}_j$.

又由 $\mathbf{x}_j = \mathbf{e}_j + \mathbf{a}_j \mathbf{g}$ 可得

$$\mathbf{x}^{(r)} = \mathbf{d}^{(r)} + \mathbf{a}^{(r)} \mathbf{g},$$

其中 $\mathbf{d}^{(r)} = \sum_{j \in \llbracket \tau \rrbracket} \mathbf{d}_{r,j} \mathbf{e}_j$, $\mathbf{a}^{(r)} = \sum_{j \in \llbracket \tau \rrbracket} \mathbf{d}_{r,j} \mathbf{a}_j$.

所以,计算产生提取编码 $\mathbf{v}^{(t)}$ 为

$$\begin{aligned} \mathbf{v}^{(t)} &= [\mathbf{u}'_t \cdot \mathbf{p}_{zt}^{(t)}]_q \\ &= [(\mathbf{d}^{(t)} \mathbf{f} + \mathbf{b}^{(t)} \mathbf{g}) \cdot \prod_{r \in S_t^*} \mathbf{x}^{(r)} / \mathbf{g}]_q \\ &= \left[\left(\mathbf{f} \prod_{r=1}^N \mathbf{d}^{(r)} + \mathbf{h}^{(t)} \mathbf{g} \right) / \mathbf{g} \right]_q, \end{aligned}$$

$$(\mathbf{d}^{(t)} \mathbf{f} + \mathbf{b}^{(t)} \mathbf{g}) \cdot \prod_{r \in S_t^*} \mathbf{x}^{(r)} - \mathbf{f} \prod_{r=1}^N \mathbf{d}^{(r)}$$

其中 $\mathbf{h}^{(t)} = \frac{\prod_{r \in S_t^*} \mathbf{x}^{(r)} - \mathbf{f} \prod_{r=1}^N \mathbf{d}^{(r)}}{\mathbf{g}}$.

根据3.1.3节参数设置可得, $\|\mathbf{h}^{(t)}\|_\infty < q^{7/8}$. 因此,提取码 $\mathbf{v}^{(t)}$ 中每个系数的最有意义的 $(\log q)/8$

比特位仅依赖于元素 $\left[\mathbf{f} \prod_{r=1}^N \mathbf{d}^{(r)} / \mathbf{g} \right]_q$.

因此,根据引理23可得,所有 N 方从各自提取码的每个系数中提取 $l = (\log q)/8 - \lambda$ 个最有意义的比特位都相同的概率约为 $1 - O(N2^{-\lambda})$, 即所有 $sk_t, t \in \llbracket N \rrbracket$ 以概率几乎为1相同. 证毕.

定理4. 如果 ext-GCDH/ext-GDDH 问题难度假设2成立,则 nr-MPKE 是一轮多方密钥交换协议.

证明. 我们仅证明基于 ext-GDDH 难度假设的 nr-MPKE 协议,而略去基于 ext-GCDH 难度假设的证明,因为其与基于 ext-GDDH 的证明类似.

我们需要证明给定公共参数 par 和所有方发布的公钥 $\mathbf{u}_t, t \in \llbracket N \rrbracket$, 攻击者并不能有效区分第1方共享密钥 sk_1 (其它方也一样,因为所有共享密钥相同) 和均匀随机比特串 s_{Rand} .

反证法. 给定 $\{\text{par}, \mathbf{u}_1, \dots, \mathbf{u}_N\}$ (下面算法中为符号简单,略去此项), 假设攻击者能够使用多项式时间算法 A 区分共享密钥 sk_1 和均匀随机串 s_{Rand} 的概率优势不可忽略, 即: 存在某个正常数 c , 算法 A 能以不可忽略的优势 $1/\lambda^c$ 区分 sk_1 和 s_{Rand} ,

$$|\Pr[A(sk_1) = 1] - \Pr[A(s_{\text{Rand}}) = 1]| \geq 1/\lambda^c.$$

如果设 $\mathbf{p}_{zt_Rand} = \left[\sum_{j \in \llbracket \tau \rrbracket} \mathbf{r}_j \mathbf{p}_{zt,j} \right]_q$, 其中 $\mathbf{r}_j \leftarrow D_{\mathbb{Z}^n, \sigma_1^*}$, $j \in \llbracket \tau \rrbracket$, 则随机提取比特串为

$$sk_{\text{Rand}} = \omega_{\text{Rand}} = \text{MSB}_l([\mathbf{u}'_1 \cdot \mathbf{p}_{zt_Rand}]_q),$$

其中 $\mathbf{u}'_1 = \left[\prod_{r \in S_1^*} \mathbf{u}_r \right]_q$.

由引理 7 知,元素 $[r_j]_g$ 为商环 $R/\langle g \rangle$ 中随机元素,即 sk_{Rand} 为 $\beta = |R/\langle g \rangle|$ 个提取比特串中任一个的概率为 $1/\beta$. 所以,任意多项式时间算法 B (包括算法 A) 能够区分 sk_{Rand} 与 s_{Rand} 的优势至多为 $O(1/\beta)$, 即

$$|\Pr[B(sk_{Rand})=1] - \Pr[B(s_{Rand})=1]| \leq O(1/\beta).$$

所以,我们有

$$\begin{aligned} & |\Pr[A(sk_1)=1] - \Pr[A(sk_{Rand})=1]| \\ & \geq |\Pr[A(sk_1)=1] - \Pr[A(s_{Rand})=1]| - \\ & \quad |\Pr[A(s_{Rand})=1] - \Pr[A(sk_{Rand})=1]| \\ & \geq 1/\lambda^c - O(1/\beta) \\ & > 1/(2\lambda^c). \end{aligned}$$

同时,我们易于验证,

$$\begin{aligned} D_{\text{ext-GDDH}} &= \{par, u_1, \dots, u_N, w_D = sk_1\}, \\ D_{\text{ext-Rand}} &= \{par, u_1, \dots, u_N, w_{Rand} = sk_{Rand}\}, \end{aligned}$$

满足定义 5 中难度假设问题 ext-GDDH.

所以,多项式时间算法 A 能够以不可忽略的概率优势(至少 $1/(2\lambda^c)$)判定问题 ext-GDDH,这与假设 2 矛盾. 证毕.

7.2 基于无可信安装构造的 wots-MPKE

基于无可信安装的多线性映射自适应地构造出一轮多方密钥交换协议(wots-MPKE)如下:

安装阶段 $\text{SETUP}(1^\lambda, 1^N)$:

设 $\kappa = N-1$ 和 $S_i^* = [N] - \{i\}$, $i \in [N]$. 输出 $PAR \leftarrow \text{INSTGen}(1^\lambda, 1^\kappa)$ 作为公共参数.

发布阶段 $\text{PUBLISH}(PAR, t)$:

(1) 第 t 方抽样选择 $d_{t,j} \leftarrow \text{CRTSamp}(PAR)$, $j \in [\tau]$, 并将 $\{d_{t,j}\}_{j \in [\tau]}$ 作为私钥保密.

(2) 第 t 方将 1-级编码 $u_t \leftarrow \text{ENC}(PAR, 1, \{d_{t,j}\}_{j \in [\tau]})$ 作为公钥发布.

产生共享密钥阶段 $\text{KEYGen}(PAR, t, \{d_{t,j}\}_{j \in [\tau]}, \{u_r\}_{r \in S_t^*})$:

(1) 第 t 方产生一个 κ -级编码 $u'_t = \left[\prod_{r \in S_t^*} u_r \right]_q$.

(2) 第 t 方提取所有方共享的密钥

$$SK_t = \text{EXT}(PAR, \{d_{t,j}\}_{j \in [\tau]}, u'_t).$$

下面通过定理 5、6 给出上述协议 wots-MPKE 的正确性和安全性.

定理 5. 上述 wots-MPKE 中算法 KeyGen 产生的 N 个共享密钥 SK_t , $t \in [N]$ 以概率几乎为 1 相同.

证明. 本定理证明方法与定理 3 相同.

定理 6. 如果问题 wots-ext-GCDH/wots-ext-GDDH 难度假设 3 成立, 则 wots-MPKE 是一轮多方密钥交换构造协议.

证明. 本定理证明方法与定理 4 相同.

8 结束语和公开问题

8.1 本文工作

首先,通过设计新的“0”测试参数,本文给出了新随机化的多线性映射构造.新随机化构造的安全仅能基于新的困难假设问题 ext-GDDH/ext-GCDH,并不能将其归约到经典困难问题.为此,本文详细分析了目前已知攻击方法并不能用于攻击新随机化构造,以证明该构造避免了“0”化攻击问题^[22-23].而且,针对新随机化构造中存在的主理想格问题潜在攻击^[57-59],本文给出了基于 Kilian 随机矩阵^[60]和 NTRU 型素数域^[61]的反制措施.

其次,通过使用中国剩余定理 CRT,本文给出了无可信安装的多线性映射构造.无可信安装构造的安全仅能基于新的难度假设问题 wots-ext-GCDH/wots-ext-GDDH,其同样不能归约到经典困难问题.为此,本文分析了目前已知攻击方法并不能用于攻击无可信安装的构造,以证明该构造避免了可信安装问题^[11-12,21].

最后,基于多线性映射构造,本文给出多方密钥交换协议 nr-MPKE 和 wots-MPKE.协议 nr-MPKE 的安全基于难度假设问题 ext-GCDH/ext-GDDH,协议 wots-MPKE 的安全基于难度假设问题 wots-ext-GCDH/wots-ext-GDDH.

8.2 应用价值与意义

本文研究成果的应用价值与意义主要体现在以下 3 个方面:

(1) 拓展了多线性映射构造的理论.最近由于“0”化攻击或其扩展已经导致现有构造方案被破解^[22-29,31,38],改进现有构造或构造新的多线性映射尤为迫切.本文通过设计新的“0”测试参数和运用中国剩余定理等方法构造新的多线性映射.这种方法不仅构造了新的安全多线性映射,也拓展了多线性映射构造理论研究.

(2) 提供了设计新密码原语的方法.虽然本文仅给出基于多线性映射的 MPKE 协议应用,但基于本文构造设计出其它密码应用是完全可能的.例如基于本文多线性映射易于构造出广播加密方案和基于身份加密方案.下面以新随机化构造应用为例:

为构造广播加密方案^[1],给定本文构造的公共参数,各方使用高斯抽样的明文元素作为私钥,并用私钥计算产生 1-级编码作为公钥.加解密时类似于 MPKE 协议产生共享密钥作为对称加密算法的密钥.

为构造基于身份加密方案^[4-5],除给定本文构造

的公共参数外,密钥中心还需提供另外两个非“0”元素的 1-级编码. 加密算法将接收者的身份使用 Hash 函数映射到两个环元素(范数较小),并将它们与另外提供的两个 1-级编码的乘积和作为接收者公钥,而密钥中心使用类似方法产生对应公钥的 1-级编码的“0”测试参数作为接收者私钥. 加解密时类似于 MPKE 协议产生共享密钥作为对称加密算法的密钥.

(3) 夯实了多线性映射应用的基础. 基于多线性映射构造的大量应用——多方密钥交换、广播加密、基于身份和属性加密、函数加密、证据加密、程序模糊器等,都需要依赖其安全性. 因此,构造安全的多线性映射方案为这些应用安全性提供了可靠的技术保障.

8.3 创新性和局限性

现有多线性映射构造^[11-12,39]及其改进^[21,25,37,30]已经被破解^[22-24,26-28,31,38]. 而且,据我们所知,目前并没有基于多线性映射构造的安全 MPKE 协议. 因此,本文研究具有创新性,但其解决方案也具有一定的局限性.

8.3.1 创新性

针对现有构造方案中存在的安全问题——“0”化攻击和可信安装问题,本文通过设计新的“0”测试参数和运用中国剩余定理的方法构造新的多线性映射,以解决现有构造方案的两个安全问题.

本文创新性主要有两点:

(1) 通过设计新的“0”测试参数以构造无“0”编码的多线性映射. 为避免“0”化攻击问题,本文设计新的“0”测试参数和构造无“0”编码的方法既能用于解决多线性映射构造的安全问题,也可能用于解决其它密码原语的安全问题. 所以,设计新的“0”测试参数,不仅为提升多线性映射构造的安全性提供了解决方案,也为提升其它密码原语的安全性提供了新的方法论.

(2) 通过使用中国剩余定理构造了无可信安装的多线性映射. 在无可信安装的构造中运用中国剩余定理,提供了构造无可信安装方案的新视角. 所以,在无可信安装构造中运用中国剩余定理,不仅为构造无可信安装的多线性映射提供候选方案和新的构造思路,也为构造无可信安装的其它密码原语提供了新的研究视角.

8.3.2 局限性

虽然新随机化构造和无可信安装构造能够避免“0”化攻击和可信安装的问题,但是本文构造仍然存在一定的局限性,主要有两点:

(1) 多线性映射构造的应用范围受到一定限

制. 例如基于新随机化构造不能直接产生安全的证据加密 WE 方案^[66]. 但是 WE 方案又是 GGH13 构造的重要应用之一,因此如何构造基于 GGH13 的 WE 改进方案将是我们下一步研究问题之一.

(2) 本文没有完全解决多线性映射构造的安全问题. 本文构造的安全性仍然基于新的难度假设,并不能归约到经典困难问题. 为此,本文仅通过安全攻击分析论证构造避免了“0”化攻击,并不是安全理论证明. 当然,目前现有构造的安全性都采用这种安全攻击分析方式,都未能提供安全理论证明. 因此,从可证安全角度而言,本文研究可以说仅仅获得了多线性映射构造的初步结果.

8.4 公开问题

本文工作仍然存在许多问题,需要进一步研究,主要包括构造安全性问题、通用多线性映射构造问题和基于多线性映射构造的应用问题.

本文需要进一步研究的公开问题如下:

(1) 简单难度假设问题

虽然在新随机化构造中,通过公共参数仍然能够计算一些与秘密参数相关的量,但是这些相关量并不包含秘密主理想格 $\langle g \rangle$ 的格基. 能否理论上证明攻击者无法计算得到新随机化构造中秘密理想格 $\langle g \rangle$ 的格基,即证明新随机化构造中简单难度假设^[30]成立,有待进一步研究.

(2) 基于容易计算量攻击的可行性

本文在第 4.1 节提出了基于容易计算量的攻击,但是该攻击需要基于假设条件成立,即假设单位元 δ 的逆元 δ^{-1} 的范数 $\|\delta^{-1}\|$ 较小. 因为量子多项式时间算法或经典次指数时间算法^[58-60]在计算产生主理想 $e_j + a_j g$ 的短的生成元 $\delta \cdot (e_j + a_j g)$ 时,仅能保证范数 $\|\delta \cdot (e_j + a_j g)\|$ 和 $\|\delta\|$ 较小,对于单位元 δ 的逆元 δ^{-1} 的系数向量范数则没有任何保证. 因此,针对这种假设,能否从理论上证明或实验上验证其是否成立,还有待进一步研究.

另外,由于目前量子多项式时间算法^[57-58]仅能计算分圆域上的主理想格“短”的生成元,这些算法能否扩展到一般数域,特别是 NTRU 型素数域,还有待研究.

(3) 研究反制措施的有效性

为抗量子多项式时间算法^[57-58]或经典计算机上次指数时间算法^[59]的攻击,本文提出了两个反制措施,即 Kilian 随机矩阵方法^[60]和 NTRU 型素数域方法^[61]作为攻击的反制措施. 这些反制措施的有效性需要进一步研究.

通过评论 3 中的简单分析表明,本文基于 Kilian 随机矩阵的改进构造已经去除了 GGH13 构造类中

存在的主理想格问题,问题是能否从理论上证明这种改进构造的安全性.

(4) 构造真正无可信安装的多线性映射

本文无可信安装的多线性映射构造的代价是其公共参数比新随机化构造的公共参数增加了 N 倍,并且多线性映射构造的安装阶段需要每个参与方参与,且每个参与方都需对自己选择的秘密参数进行保密.问题是能否构造出公共参数中不包含秘密参数的真正无可信安装的多线性映射,如离散对数上的单线性映射和椭圆曲线上的双线性映射.

(5) 研究基于新随机化构造新的密码应用

通过上述应用实例可以看出,构造设计新的密码应用有时直接使用新随机化构造即可,有时还需对新随机化构造进行自适应改造.因此,我们下一步将研究基于本文构造设计新的密码原语应用.

致 谢 在此,我们真诚感谢本文的匿名审稿专家所提供的宝贵修改意见.本文数值计算实验得到了中国科学技术大学超级计算中心的计算支持和帮助,作者在此表示感谢!

参 考 文 献

- [1] Boneh D, Silverberg A. Applications of multilinear forms to cryptography. *Contemporary Mathematics*, 2003, 324: 71-90
- [2] Sakai R, Ohgishi K, Kasahara M. Cryptosystems based on pairing//*Proceedings of the 2000 Symposium on Cryptography and Information Security (SCIS 2000)*. Okinawa, Japan, 2000: 26-28
- [3] Joux A. A one round protocol for tripartite Diffie-Hellman. *Journal of Cryptology*, 2004, 17(4): 263-276
- [4] Boneh D, Franklin M K. Identity-based encryption from the Weil pairing. *SIAM Journal on Computing*, 2003, 32(3): 586-615
- [5] Waters B. Efficient identity-based encryption without random oracles//*Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2005)*. LNCS 3494. Aarhus, Denmark, 2005: 114-127
- [6] Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data//*Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS 2006)*. Alexandria, USA, 2006: 89-98
- [7] Boneh D, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys//*Proceedings of the 25th Annual International Cryptology Conference (CRYPTO 2005)*. LNCS 3621. Santa Barbara, USA, 2005: 258-275
- [8] Rückert M, Schröder D. Aggregate and verifiably encrypted signatures from multilinear maps without random oracles//*Proceedings of the 3rd International Conference and Workshops (ISA 2009)*. LNCS 5576. Seoul, Korea, 2009: 750-759
- [9] Papamanthou C, Tamassia R, Triandopoulos N. Optimal authenticated data structures with multilinear forms//*Proceedings of the 4th International Conference (Pairing 2010)*. LNCS 6487. Yamanaka Hot Spring, Japan, 2010: 246-264
- [10] Rothblum R. On the circular security of bit-encryption//*Proceedings of the 10th Theory of Cryptography Conference (TCC 2013)*. LNCS 7785. Tokyo, Japan, 2013: 579-598
- [11] Garg S, Gentry C, Halevi S. Candidate multilinear maps from ideal lattices//*Proceedings of the 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2013)*. LNCS 7881. Athens, Greece, 2013: 1-17
- [12] Coron J S, Lepoint T, Tibouchi M. Practical multilinear maps over the integers//*Proceedings of the 33rd Annual Cryptology Conference, Part I (CRYPTO 2013)*. LNCS 8042. Santa Barbara, USA, 2013: 476-493
- [13] Garg S, Gentry C, Sahai A, Waters B. Witness encryption and its applications//*Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC 2013)*. Palo Alto, USA, 2013: 467-476
- [14] Garg S, Gentry C, Halevi S, et al. Attribute-based encryption for circuits from multilinear maps//*Proceedings of the 33rd Annual Cryptology Conference, Part II (CRYPTO(2) 2013)*. LNCS 8043. Santa Barbara, USA, 2013: 479-499
- [15] Garg S, Gentry C, Halevi S, et al. Candidate indistinguishability obfuscation and functional encryption for all circuits//*Proceedings of the 2013 IEEE 54th Annual Symposium on Foundations of Computer Science (FOCS 2013)*. Berkeley, USA, 2013: 40-49
- [16] Boneh D, Gentry C, Gorbunov S, et al. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits//*Proceedings of the 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2014)*. LNCS 8441. Copenhagen, Denmark, 2014: 533-556
- [17] Boneh D, Zhandry M. Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation //*Proceedings of the 34th Annual Cryptology Conference, Part I (CRYPTO 2014)*. LNCS 8616. Santa Barbara, USA, 2014: 480-499
- [18] Brakerski Z, Rothblum G N. Virtual black-box obfuscation for all circuits via generic graded encoding//*Proceedings of the 11th Theory of Cryptography Conference (TCC 2014)*. LNCS 8349. San Diego, USA, 2014: 1-25
- [19] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings. *Journal of the ACM*, 2013, 60(6): 1-35
- [20] Hoffstein J, Pipher J, Silverman J H. NTRU: A ring based public key cryptosystem//*Proceedings of the 3rd International Symposium, ANTS-III (ANTS 1998)*. LNCS 1423. Portland, USA, 1998: 267-288

- [21] Langlois A, Stehlé D, Steinfeld R. GGHLite: More efficient multilinear maps from ideal lattices//Proceedings of the 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2014). LNCS 8441. Copenhagen, Denmark, 2014: 239-256
- [22] Hu Yupu, Jia Huiwen. Cryptanalysis of GGH map//Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Part I (EUROCRYPT 2016). LNCS 9665. Vienna, Austria, 2016: 537-565
- [23] Coron J S, Gentry C, Halevi S, et al. Zeroizing without low-level zeroes: New attacks on multilinear maps and their limitations//Proceedings of the 35th Annual Cryptology Conference, Part I (CRYPTO 2015). LNCS 9215. Santa Barbara, USA, 2015: 247-266
- [24] Brakerski Z, Gentry C, Halevi S, et al. Cryptanalysis of the quadratic zero-testing of GGH. Nevada, USA; IACR, Cryptology ePrint Archive, Report 845, 2015
- [25] Halevi S. The state of cryptographic multilinear maps//Proceedings of the 35th Annual Cryptology Conference (CRYPTO 2015). Santa Barbara, USA, 2015
- [26] Albrecht M, Bai S, Ducas L. A subfield lattice attack on overstretched NTRU assumptions cryptanalysis of some FHE and graded encoding schemes//Proceedings of the 36th Annual International Cryptology Conference, Part I (CRYPTO 2016). LNCS 9814. Santa Barbara, USA, 2016: 153-178
- [27] Cheon J H, Jeong J, Lee C. An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low level encoding of zero. Nevada, USA; IACR, Cryptology ePrint Archive, Report: 139, 2016
- [28] Coron J S, Lee M S, Lepoint T, Tibouchi M. Cryptanalysis of GGH15 multilinear maps//Proceedings of the 36th Annual International Cryptology Conference, Part II (CRYPTO 2016). LNCS 9815. Santa Barbara, USA, 2016: 607-628
- [29] Miles E, Sahai A, Zhandry M. Annihilation attacks for multilinear maps: Cryptanalysis of indistinguishability obfuscation over GGH13//Proceedings of the 36th Annual International Cryptology Conference, Part II (CRYPTO 2016). LNCS 9815. Santa Barbara, USA, 2016: 629-658
- [30] Halevi S. Graded encoding, variations on a scheme. Nevada, USA; IACR, Cryptology ePrint Archive, Report: 866, 2015
- [31] Cheon J H, Han K, Lee C, et al. Cryptanalysis of the multilinear map over the integers//Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Part I (EUROCRYPT 2015). LNCS 9056. Sofia, Bulgaria, 2015: 3-12
- [32] Barak B, Garg S, Kalai Y T, et al. Protecting obfuscation against algebraic attacks//Proceedings of the 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2014). LNCS 8441. Copenhagen, Denmark, 2014: 221-238
- [33] Badrinarayanan S, Miles E, Sahai A, Zhandry M. Post-zeroizing obfuscation: New mathematical tools, and the case of evasive circuits//Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Part II (EUROCRYPT 2016). LNCS 9666. Vienna, Austria, 2016: 764-791
- [34] Chen Y, Gentry C, Halevi S. Cryptanalyses of candidate branching program obfuscators//Proceedings of the 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Part III (EUROCRYPT 2017). LNCS 10212. Paris, France, 2017: 278-307
- [35] Garg S, Gentry C, Halevi S, Zhandry M. Fully secure functional encryption without obfuscation. Nevada, USA; IACR, Cryptology ePrint Archive, Report: 666, 2014
- [36] Boneh D, Wu D J, Zimmerman J. Immunizing multilinear maps against zeroizing attacks. Nevada, USA; IACR, Cryptology ePrint Archive, Report: 930, 2014
- [37] Coron J S, Lepoint T, Tibouchi M. New multilinear maps over the Integers//Proceedings of the 35th Annual Cryptology Conference, Part I (CRYPTO 2015). LNCS 9215. Santa Barbara, USA, 2015: 267-286
- [38] Cheon J H, Fouque P A, Lee C, et al. Cryptanalysis of the new CLT multilinear map over the integers//Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Part I (EUROCRYPT 2016). LNCS 9665. Vienna, Austria, 2016: 509-536
- [39] Gentry C, Gorbunov S, Halevi S. Graph-induced multilinear maps from lattices//Proceedings of the 12th Theory of Cryptography Conference, Part II (TCC 2015). LNCS 9015. Warsaw, Poland, 2015: 498-527
- [40] Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based//Proceedings of the 33rd Annual Cryptology Conference, Part I (CRYPTO 2013). LNCS 8042. Santa Barbara, USA, 2013: 75-92
- [41] Regev O. On lattices, learning with errors, random linear codes, and cryptography//Proceedings of the 37th Annual ACM Symposium on Theory of Computing (2005 STOC). Baltimore, USA, 2005: 84-93
- [42] Feng Ke-Qin. Introduction to Algebraic Number Theory. Harbin: Harbin Institute of Technology Press, 2015 (in Chinese)
(冯克勤. 代数数论入门. 哈尔滨: 哈尔滨工业大学出版社, 2015)
- [43] Washington L C. Introduction to Cyclotomic Fields. Graduate Texts in Mathematics. New York, USA: Springer, 1997
- [44] Micciancio D, Goldwasser S. Complexity of Lattice Problems: A Cryptographic Perspective. Massachusetts, USA: Kluwer Academic Press, 2002
- [45] van Erven T, Harremoës P. Rényi divergence and Kullback-Leibler divergence. IEEE Transactions on Information Theory, 2014, 60(7): 3797-3820
- [46] Micciancio D, Regev O. Worst-case to average-case reductions based on Gaussian measures. SIAM Journal on Computing, 2007, 37(1): 267-302

- [47] von zur Gathen J, Gerhard J. Modern Computer Algebra. 3rd Edition. Cambridge, England: Cambridge University Press, 2013
- [48] Agrawal S, Gentry G, Halevi S, Sahai A. Discrete Gaussian leftover hash lemma over infinite domains//Proceedings of the 19th International Conference on the Theory and Application of Cryptology and Information Security, Part I (ASIACRYPT 2013). LNCS 8269. Bengaluru, India, 2013: 97-116
- [49] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions//Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC 2008). Victoria, Canada, 2008: 197-206
- [50] Stehlé D, Steinfeld R. Making NTRU as secure as worst-case problems over ideal lattices//Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2011). LNCS 6632. Tallinn, Estonia, 2011: 27-47
- [51] Yan S Y. Number Theory for Computing. 2nd Edition. Beijing: Beijing World Publishing Corporation, 2002
- [52] Garg S. Candidate Multilinear Maps [Ph. D. dissertation]. University of California, Los Angeles, 2013
- [53] Smart N P, Vercauteren F. Fully homomorphic encryption with relatively small key and ciphertext sizes//Proceedings of the 13th International Conference on Practice and Theory in Public Key Cryptography (PKC 2010). LNCS 6056. Paris, France, 2010: 420-443
- [54] Hastad J, Impagliazzo R, Levin L A, Luby M. A pseudo-random generator from any one-way function. SIAM Journal on Computing, 1999, 28(4): 1364-1396
- [55] Chen Yuanmi, Nguyen Phong Q. BKZ 2.0: Better lattice security estimates//Proceedings of the 17th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2011). LNCS 7073. Seoul, South Korea, 2011: 1-20
- [56] Albrecht M R, Cócis C, Laguillaumie F, Langlois A. Implementing candidate graded encoding schemes from ideal lattices//Proceedings of the 21st International Conference on the Theory and Application of Cryptology and Information Security, Part II (ASIACRYPT 2015). LNCS 9453. Auckland, New Zealand, 2015: 752-775
- [57] Cramer R, Ducas L, Peikert C, Regev O. Recovering short generators of principal ideals in cyclotomic rings//Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Part II (EUROCRYPT 2016). LNCS 9666. Vienna, Austria, 2016: 559-585
- [58] Eisentrager K, Hallgren S, Kitaev A, Song F. A quantum algorithm for computing the unit group of an arbitrary degree number field//Proceedings of the 46th Annual ACM Symposium on Theory of Computing (STOC 2014). New York, USA, 2014: 293-302
- [59] Biasse J F. Subexponential time relations in the class group of large degree number fields. Advances in Mathematics of Communications, 2014, 8(4): 407-425
- [60] Kilian J. Founding cryptography on oblivious transfer//Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC 1988). Chicago, USA, 1988: 20-31
- [61] Bernstein D J, Chuengsatiansup C, Lange T, van Vredendaa C. NTRU Prime. Nevada, USA: IACR, Cryptology ePrint Archive, Report: 461, 2016
- [62] Osada H. The Galois groups of the polynomials $X^n + aX^1 + b$. Journal of Number Theory, 1987, 25(2): 230-238
- [63] Gama N, Nguyen Phong Q. Finding short lattice vectors within Mordell's inequality//Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC 2008). Victoria, Canada, 2008: 207-216
- [64] López-Alt A, Tromer E, Vaikuntanathan V. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption//Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC 2012). New York, USA, 2012: 1219-1234
- [65] Kayal N. The complexity of the annihilating polynomial//Proceedings of the 2009 24th Annual IEEE Conference on Computational Complexity (CCC 2009). Paris, France, 2009: 184-193
- [66] Hu Yupu, Jia Huiwen. A comment on Gu Map-1. Nevada, USA: IACR, Cryptology ePrint Archive, Report: 448, 2015

附录 1. GGH13 构造.

为完整性,本节给出 GGH13 构造和其安全依赖的难度假设问题.由于变种 GGHLite 仅改进了 GGH13 构造中的参数大小设置,GGHLite 的其它部分与 GGH13 构造相同.因此,本节直接提供变种 GGHLite 作为 GGH13 构造.

1.1 GGH13 构造

为符号一致,本节参数符号与第 3.1.1 节相同,即 GGH13 构造中仍使用参数 $\lambda, \kappa, q, n, \sigma, \sigma', \sigma_1^*, \sigma^*, \tau, l_{-1}, l$.

设 l_b 为最小奇异值下界.对于 $k \in [\kappa]$,如果设 $\mathbf{b}_j^{(k)} = \mathbf{s}_j^{(k)} \mathbf{g}, j \in [\tau]$ 为公共参数中 τ 个 k -级编码对应的“0”元素,则矩阵 $\text{Rot}(\mathbf{B}^{(k)}) = (\text{Rot}(\mathbf{b}_1^{(k)}), \dots, \text{Rot}(\mathbf{b}_\tau^{(k)}))$ 的最小奇异值需

要满足条件 $\sigma_n(\text{Rot}(\mathbf{B}^{(k)})) \geq l_b$.

为提高 GGH13 构造的效率,变种 GGHLite^[21]对 GGH13 构造的改进主要有两点:

(1) 使用代数环上离散高斯 LHL,使得公共参数中的再随机化编码个数 τ 从 $O(n \log n)$ 减少到 2,并且高斯抽样随机化因子从整数 $\beta_j \leftarrow D_{\mathbb{Z}, \sigma_1^*}$ 变成环 R 中元素 $\beta_j \leftarrow D_{\mathbb{Z}^n, \sigma_1^*}$;

(2) 使用 Rényi 扩散技术,使得再随机化过程的抽样参数 σ_k^* 从 λ 的指数大小(即 2^λ)减少到多项式大小(即 $\text{poly}(\lambda)$).

变种 GGHLite 具体构造如下:

公共参数产生算法 $\text{par}_0 \leftarrow \text{InstGen}(1^\lambda, 1^\kappa)$:

- (1) 选择足够大素数 q .
- (2) 随机选择元素 $\mathbf{z} \leftarrow U(R_q)$, 满足 $\mathbf{z}^{-1} \in R_q$.
- (3) 抽样理想元素 $\mathbf{g} \leftarrow D_{\mathbb{Z}^n, \sigma}$, 满足 $I = \langle \mathbf{g} \rangle$ 为素理想, 并且 $\|\mathbf{g}\| \leq \sqrt{n}\sigma$ 和 $\|\mathbf{g}^{-1}\| \leq l_{-1}$.

(4) 抽样“1”的 1-级编码 $\mathbf{y} = \lfloor \mathbf{a}/\mathbf{z} \rfloor_q$, 其中 $\mathbf{a} \leftarrow D_{1+I, \sigma'}$, 即 $\mathbf{a} = 1 + \mathbf{s}\mathbf{g}$.

- (5) 对于 $k \in \llbracket \kappa \rrbracket$:

(5.1) 抽样 $\mathbf{B}^{(k)} = (\mathbf{b}_1^{(k)}, \mathbf{b}_2^{(k)})$, 其中 $\mathbf{b}_j^{(k)} \leftarrow D_{1, \sigma'}$, 即 $\mathbf{b}_j^{(k)} = s_j^{(k)} \mathbf{g}$, $j \in \llbracket 2 \rrbracket$. 如果 $\langle \mathbf{b}_1^{(k)}, \mathbf{b}_2^{(k)} \rangle \neq I$, 或 $\sigma_n(\text{Rot}(\mathbf{B}^{(k)})) < l_b$, 或 $\|\mathbf{B}^{(k)}\| > \sqrt{n}\sigma'$, 则重新抽样.

- (5.2) 产生元素“0”的 k -级编码:

$$\mathbf{x}_j^{(k)} = \lfloor \mathbf{b}_j^{(k)} / \mathbf{z}^k \rfloor_q, j \in \llbracket \tau \rrbracket, \text{ 这里 } \tau = 2.$$

- (6) 抽样元素 $\mathbf{h} \leftarrow D_{\mathbb{Z}^n, \sigma^*}$, 计算“0”测试参数:

$$\mathbf{p}_{zt} = \lfloor \mathbf{h} \cdot \mathbf{z}^k / \mathbf{g} \rfloor_q;$$

- (7) 输出公共参数为

$$\text{par}_0 = \{n, q, \tau, \mathbf{y}, \{\mathbf{x}_j^{(k)}\}_{j \in \llbracket 2 \rrbracket, k \in \llbracket \kappa \rrbracket}, \mathbf{p}_{zt}\}.$$

0-级编码算法 $\mathbf{d} \leftarrow \text{Samp}(\text{par}_0)$:

- (1) 高斯抽样选取 0-级编码 $\mathbf{d} \leftarrow D_{\mathbb{Z}^n, \sigma'}$.

k -级编码算法 $\mathbf{u} \leftarrow \text{Enc}(\text{par}_0, k, \mathbf{d})$:

- (1) 给定 0-级编码 $\mathbf{d}$, 产生 $\mathbf{d}$ 的 k -级编码

$$\mathbf{u}' = \lfloor \mathbf{d}\mathbf{y}^k \rfloor_q = \lfloor \mathbf{d}\mathbf{a}^k / \mathbf{z}^k \rfloor_q = \lfloor (\mathbf{d} + \mathbf{s}'\mathbf{g}) / \mathbf{z}^k \rfloor_q.$$

其中 $\mathbf{s}' = (\mathbf{d}\mathbf{a}^k - \mathbf{d}) / \mathbf{g}$.

- (2) 抽样选取元素 $\beta_j \leftarrow D_{\mathbb{Z}^n, \sigma_k^*}, j \in \llbracket 2 \rrbracket$;

(3) 给定 $\mathbf{d}$ 的 k -级编码 $\mathbf{u}'$, 使用再随机化方法产生 k -级编码

$$\mathbf{u} = \lfloor \mathbf{u}' + \sum_{j=1}^2 \beta_j \mathbf{x}_j^{(k)} \rfloor_q = \lfloor (\mathbf{d} + \mathbf{r}\mathbf{g}) / \mathbf{z}^k \rfloor_q,$$

其中 $\mathbf{r} = \mathbf{s}' + \sum_{j=1}^2 \beta_j \mathbf{s}_j^{(k)}$.

加法编码算法 $\mathbf{u} \leftarrow \text{Add}(\text{par}_0, k, \mathbf{u}_1, \dots, \mathbf{u}_m)$:

给定 m 个 k -级编码 $\mathbf{u}_j = \lfloor \mathbf{c}_j / \mathbf{z}^k \rfloor_q$, 则它们的和 $\mathbf{u} =$

$\lfloor \sum_{j=1}^m \mathbf{u}_j \rfloor_q$ 是元素 $\lfloor \sum_{j=1}^m \mathbf{c}_j \rfloor_g$ 的一个 k -级编码.

乘法编码算法 $\mathbf{u} \leftarrow \text{Mul}(\text{par}_0, 1, \mathbf{u}_1, \dots, \mathbf{u}_k)$:

给定 k 个 1-级编码 $\mathbf{u}_j = \lfloor \mathbf{c}_j / \mathbf{z} \rfloor_q$, 则它们的积 $\mathbf{u} =$

$\lfloor \prod_{j=1}^k \mathbf{u}_j \rfloor_q$ 是元素 $\lfloor \prod_{j=1}^k \mathbf{c}_j \rfloor_g$ 的一个 k -级编码.

“0”测试算法 $\text{isZero}(\text{par}_0, \mathbf{u})$:

给定一个 κ -级编码 $\mathbf{u} = \lfloor \mathbf{c} / \mathbf{z}^k \rfloor_q$, 计算测试函数

$$\text{isZero}(\text{par}_0, \mathbf{p}_{zt}, \mathbf{u}) = \begin{cases} 1, & \text{如果 } \|\lfloor \mathbf{u} \cdot \mathbf{p}_{zt} \rfloor_q\|_{\infty} < q^{3/4} \\ 0, & \text{否则} \end{cases}.$$

//“0”测试算法用于判定编码 $\mathbf{u}$ 中的明文元素 $\mathbf{c}$ 是否为“0”, 即元素 $\lfloor \mathbf{c} \rfloor_g$ 是否为“0”.

提取算法 $\mathbf{w} \leftarrow \text{Ext}(\text{par}_0, \mathbf{u})$:

(1) 给定一个 κ -级编码 $\mathbf{u} = \lfloor \mathbf{c} / \mathbf{z}^k \rfloor_q$, 计算提取编码 $\mathbf{v} = \lfloor \mathbf{u} \cdot \mathbf{p}_{zt} \rfloor_q$;

(2) 从 $\mathbf{v}$ 的每个系数中提取 $l = (\log q)/4 - \lambda$ 个最有意义的比特位, 输出提取比特串 $\mathbf{w}$:

$$\mathbf{w} = \text{Ext}(\text{par}_0, \mathbf{u}) = \text{MSB}_l(\mathbf{v}).$$

注意: 这里减去 λ 是为保证提取编码的错误容量.

//如果设 $\mathbf{c} = \lfloor \mathbf{c} \rfloor_g + \mathbf{r}\mathbf{g}$, 则以概率 $1 - \lambda^{-\omega(1)}$ 有

$$\text{MSB}_l(\mathbf{v}) = \text{MSB}_l\left(\left\lfloor \frac{\mathbf{h}}{\mathbf{g}} \cdot \lfloor \mathbf{c} \rfloor_g \right\rfloor_q\right).$$

1.2 安全假设

本节我们简要回顾分级判定和计算 Diffie-Hellman 困难问题(GDDH/GCDH)^[11]的定义, 同时也给出提取 GCDH (Ext-GCDH)困难问题^[21]的定义.

给定参数 λ, κ , GGH13 的安全实验过程如下:

- (1) 产生 $\text{par}_0 \leftarrow \text{InstGen}(1^\lambda, 1^\kappa)$.

- (2) 对于 $i = 0, \dots, \kappa$:

- (2.1) 抽样 $\mathbf{e}_i \leftarrow \text{Samp}(\text{par}_0)$ 和 $\mathbf{r}_i \leftarrow \text{Samp}(\text{par}_0)$;

- (2.2) 产生 $\mathbf{e}_i$ 的 1-级编码 $\mathbf{u}_i \leftarrow \text{Enc}(\text{par}_0, 1, \mathbf{e}_i)$;

其中 $\mathbf{u}_i = \lfloor \mathbf{e}_i \mathbf{y} + \sum_{j=1}^{\tau} \beta_{i,j} \mathbf{x}_j^{(1)} \rfloor_q$, 且对于 $j \in \llbracket \tau \rrbracket, \beta_{i,j} \leftarrow D_{\mathbb{Z}^n, \sigma_1^*}$.

- (3) 计算产生 $\mathbf{u}^* = \lfloor \prod_{i=1}^{\kappa} \mathbf{u}_i \rfloor_q$.

- (4) 计算产生 $\mathbf{v}_c = \lfloor \mathbf{e}_0 \mathbf{u}^* \rfloor_q$.

- (5) 对于 $j \in \llbracket \tau \rrbracket$, 抽样 $\beta_j \leftarrow D_{\mathbb{Z}^n, \sigma_k^*}$, 计算产生 $\mathbf{v}_D =$

$$\lfloor \mathbf{e}_0 \mathbf{u}^* + \sum_{j=1}^{\tau} \beta_j \mathbf{x}_j^{(\kappa)} \rfloor_q.$$

- (6) 对于 $j \in \llbracket \tau \rrbracket$, 抽样 $\beta_j \leftarrow D_{\mathbb{Z}^n, \sigma_k^*}$, 计算产生 $\mathbf{v}_{\text{Rand}} =$

$$\lfloor \mathbf{r}_0 \mathbf{u}^* + \sum_{j=1}^{\tau} \beta_j \mathbf{x}_j^{(\kappa)} \rfloor_q.$$

定义 7(GCDH/Ext-GCDH/GDDH^[21]). 根据上述 GGH13 构造的安全实验, 问题 GCDH, Ext-GCDH 和 GDDH 定义如下:

κ -级计算 Diffie-Hellman 问题 (GCDH): 给定输入

$\{\text{par}_0, \mathbf{u}_0, \dots, \mathbf{u}_\kappa\}$, 计算输出元素 $\prod_{i=0}^{\kappa} \mathbf{e}_i + I$ 的一个 κ -级编码

$\mathbf{w} \in R_q$, 满足 $\|\lfloor (\mathbf{w} - \mathbf{v}_c) \mathbf{p}_{zt} \rfloor_q\|_{\infty} < q^{3/4}$.

提取 κ -级计算 Diffie-Hellman 问题 (Ext-GCDH): 给定

输入 $\{\text{par}_0, \mathbf{u}_0, \dots, \mathbf{u}_\kappa\}$, 计算输出元素 $\prod_{i=0}^{\kappa} \mathbf{e}_i + I$ 的提取比特串

$\mathbf{w}$, 满足条件

$$\mathbf{w} = \text{Ext}(\text{par}_0, \mathbf{v}_c) = \text{MSB}_l(\lfloor \mathbf{v}_c \cdot \mathbf{p}_{zt} \rfloor_q).$$

κ -级判定 Diffie-Hellman 问题 (GDDH): 区分上述安全实验中的 $\mathbf{v}_D$ 和 $\mathbf{v}_{\text{Rand}}$, 即判定分布

$$D_{\text{GDDH}} = \{\text{par}_0, \mathbf{u}_0, \dots, \mathbf{u}_\kappa, \mathbf{v}_D\},$$

$$D_{\text{Rand}} = \{\text{par}_0, \mathbf{u}_0, \dots, \mathbf{u}_\kappa, \mathbf{v}_{\text{Rand}}\}.$$

评论 7. (1) 问题 Ext-GCDH 归约到问题 GCDH, 反之则不成立. 因为如果给定 GCDH 的 κ -级编码 $\mathbf{w} \in R_q$, 满足 $\|\lfloor (\mathbf{w} - \mathbf{v}_c) \mathbf{p}_{zt} \rfloor_q\|_{\infty} < q^{3/4}$, 则可得 Ext-GCDH 的提取比特串 $\mathbf{w} = \text{MSB}_l(\lfloor \mathbf{w} \cdot \mathbf{p}_{zt} \rfloor_q)$; 反之, 虽然给定 Ext-GCDH 的提取比特串 $\mathbf{w}$, 但是在产生 $\mathbf{w}$ 时, 为保证错误容量, 提取编码的每个系数中减少了 λ 个最有意义的比特位, 故不能由此获得满足条件的 κ -级编码 $\mathbf{w}$; (2) 问题 GDDH 归约到问题 GCDH 和 Ext-GCDH, 反之则无法归约证明. 因为如果给定 Ext-GCDH 的提取比特串 $\mathbf{w}$, 则可根据 $\text{MSB}_l(\lfloor \mathbf{v} \cdot \mathbf{p}_{zt} \rfloor_q)$ 与 $\mathbf{w}$ 是否相等, 以概率几乎为 1 判定 GDDH 问题中的 $\mathbf{v}$ 是 $\mathbf{v}_D$, 还是 $\mathbf{v}_{\text{Rand}}$.



GU Chun-Sheng, born in 1971, Ph.D., professor. His research interests include lattice-based cryptography and cryptanalysis.

JING Zheng-Jun, born in 1978, Ph.D., associate professor. His research interests include public key cryptography and cryptanalysis.

SHI Pei-Zhong, born in 1982, Ph.D., lecturer. His research interests include network security and protocol security analysis.

YU Zhi-Min, born in 1973, M.S., lecturer. His research interests include public key cryptography and cryptanalysis.

Background

The research on cryptographic multilinear maps is now a hot point. This reflects in the following two aspects. First, multilinear maps have found many applications in cryptography. Due to extensive applications based on bilinear mapping, such as identity-based encryption, attribute-based encryption, broadcast encryption, Boneh and Silverberg are inspired to study multilinear maps and its applications. Unlike the bilinear mapping using elliptic curves, how to construct cryptographic multilinear maps has been an open problem for several years. Although no known candidate multilinear maps, researchers have studied applications of cryptographic multilinear maps. After constructing the GGH13 and CLT13 approximate multilinear maps, the cryptographic applications based on multilinear maps have witnessed a series of work, including witness encryption, indistinguishability obfuscation, function encryption and many more. Second, currently only the GGH13, CLT13 and GGH15 constructions are known and all have zeroizing attacks, new hardness assumptions and trusted setup. In 2013, Garg, Gentry and Halevi (GGH13) described the first candidate multilinear maps using ideal lattices. Following the method of GGH13, Coron, Lepoint and Tibouchi (CLT13) described a relative practical multilinear maps over the integers applying Chinese remainder theorem. To improve the efficiency of GGH13, Langlois, Stehlé and Steinfeld recently presented a variant GGHlite by reanalyzing the security of re-randomization process in GGH13. However, the GGH13 and CLT13 constructions have been broken by using the zeroizing attacks. On one hand, Hu and Jia presented a polynomial time algorithm on GGH13, which has completely broken two important GGH13-based applications, i.e. multi-partite key exchange (MPKE) and the instance of witness encryption based on the hardness of 3-exact cover problem. On the other hand, Cheon, Han, Lee, Ryu and Stehle totally broke the CLT13 construction. Then, Garg, Gentry, Halevi and Zhandry, and Boneh, Wu and Zimmerman proposed two independent approaches to fix the CLT13 construction, respectively. However, Coron, Gentry, Halevi, Lepoint, Maji, Miles, Raykova, Sahai, and Tibouchi showed

that these fixes can be defeated using the extension of the Cheon et al.'s zeroizing attack. Very recently, Coron, Lepoint and Tibouchi (CLT15) described a new modification of CLT13, which makes a new zero-testing parameter. But the CLT15 construction also cannot prevent the zeroizing attack. Moreover, Gentry, Gorbunov and Halevi (GGH15) presented a graph-reduced multilinear map from lattices using approximate eigenvalue vector, however its efficiency was lower than the previous constructions. More unfortunately, Coron, Lee, Lepoint, and Tibouchi showed that the GGH15-based MPKE is also insecure.

In this paper, we mainly improve the GGH13 construction to solve its zeroizing attacks and trusted setup. To avoid the zeroizing attacks, we first describe a new randomization construction of multilinear maps by designing new zero-testing parameters. The security of our construction depends upon the new hardness assumptions ext-GDDH/ext-GCDH. Then, to remove the trusted setup, we describe a construction without trusted setup of multilinear maps using ideal lattices by applying Chinese remainder theorem. The security of our construction relies on the new hardness assumptions wots-ext-GDDH/wots-ext-GCDH. Finally, we present one-round multipartite key exchange protocols nr-MPKE and wots-MPKE using our improvement constructions of multilinear maps.

This work is supported by the National Natural Science Foundation of China (Grant Nos. 61672270 and 61602216), the Research Foundation for Humanities and Social Sciences of Ministry of Education, China (Grant Nos. 14YJAZH023 and 15YJCZH129), the Qing Lan Project for Young Researchers of Jiangsu Province of China (Grant No. KYQ14004), the Jiangsu Overseas Research & Training Program for University Prominent Young & Middle-aged Teachers and Presidents, the Open Fund of State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences (Grant No. 2015-MSB-10), and the Changzhou Application Fundamental Research Guidance Project of China (Grant No. 2016365).