密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2017, 4(3): 229–240

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

一种基于 LWE 问题的布尔电路同态加密方案*

姬 晨[1,2], 蔡 斌[1,2], 向 宏[1,2], 丁津泰[1,2], 桑 军[1,2]

1. 信息物理社会可信服务计算教育部重点实验室 (重庆大学), 重庆 400044
2. 重庆大学软件学院, 重庆 400044

通讯作者: 蔡斌, E-mail: caibin@cqu.edu.cn

摘 要: 传统密码学能保护数据在存储和传输中的安全性, 但密文信息持有者不能直接对密文数据进行计算. 2009 年第一个全同态加密方案的诞生, 使得对密文的直接计算成为可能. 本文在 GSW 全同态加密方案的基础上, 重新设计密钥生成、加密、解密、同态操作等函数, 提出了一种基于布尔电路的改进同态加密方案. 改进方案的同态加法和同态乘法对应矩阵加法和矩阵乘法, 不会造成密文维度扩张. 通过设计转换密钥生成函数、维度归约函数和模数转换函数, 本文给出了针对该方案的维度模数规约方法和相应的正确性分析. 同时, 本文还对提出的同态加密方案的正确性和安全性进行了理论分析. 分析表明, 改进方案的安全性依赖于 LWE 问题, 具有抵抗选择明文攻击的能力. 与 GSW 方案相比, 改进方案辅以 Peikert 等人提出的快速 bootstrapping 方法, 可以更加自然地转变为全同态加密方案. 此外, 本文给出了改进方案的参数选择规则, 开发软件实现了该方案和与、或、与非等同态计算电路门, 给出了主要参数和计算时间, 为全同态加密技术的进一步应用做出了铺垫.

关键词: 全同态加密; LWE 问题; 同态布尔电路; 软件实现

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000177

中文引用格式: 姬晨, 蔡斌, 向宏, 丁津泰, 桑军. 一种基于 LWE 问题的布尔电路同态加密方案[J]. 密码学报, 2017, 4(3): 229–240.

英文引用格式: JI C, CAI B, XIANG H, DING J T,SANG J. A boolean circuit homomorphic encryption scheme based on LWE problem[J]. Journal of Cryptologic Research, 2017, 4(3): 229–240.

A Boolean Circuit Homomorphic Encryption Scheme Based on LWE Problem

JI Chen[1,2], CAI Bin[1,2], XIANG Hong[1,2], DING Jin-Tai[1,2], SANG Jun[1,2]

1. Key Laboratory of Dependable Service Computing in Cyber Physical Society, Ministry of Education, Chongqing 400044, China
2. School of Software Engineering, Chongqing University, Chongqing 400044, China

Corresponding author: CAI Bin, E-mail: caibin@cqu.edu.cn

Abstract: Traditional cryptography can only protect the security of data in storage and transmission, and the ciphertext holders cannot operate encrypted data directly. In 2009, the emergence of the first FHE scheme makes it possible for the ciphertext holders to perform the ciphertext operation directly. Based on the GSW FHE scheme, this paper redesigns the key generation, encryption, decryption, and homomorphic operation functions, proposes an improved Boolean circuit homomorphic encryption

* 基金项目: 国家自然科学基金 (61472054); 中央高校基本科研业务费 (106112014CDJZR095501) 资助课题
收稿日期: 2016-07-28 定稿日期: 2017-04-01

scheme. The homomorphic addition and homomorphic multiplication of the improved scheme are corresponding to the addition and multiplication of the matrix, which does not result in the expansion of ciphertext dimension. In this paper, we propose a modules dimension reduction method aiming at designing the scheme and its corresponding correctness analysis. The homomorphic encryption scheme is proved to be correct and secure. The analysis shows that the security of the improved scheme depends on the LWE problem, and can resists CPA attack. Compared with the GSW scheme, the improved scheme can be changed more naturally to a FHE scheme with fast bootstrapping method proposed by Peikert et al in 2014. In addition, this paper provides the selection rules of the parameters, implements the scheme, the AND, OR, XOR and other homomorphic computing gates of the scheme, gives the main parameters and calculation time, which makes essential foreshadowing for the forthcoming applications of the scheme.

Key words: Fully Homomorphic Encryption (FHE); LWE problem; Homomorphic Boolean Circuit; Software Implementation

1 引言

传统密码学仅仅保护数据在存储和传输中的安全性, 用户处理数据时首先要解密数据. 全同态加密的诞生使得在不解密的条件下实现对密文的直接计算. 1978 年, 同态加密的思想由 Rivest、Adleman 与 Dertouzos [1] 共同提出. 从那以后, 密码学家们先后提出了一系列方案 [2–5], 这些方案或者仅支持加法同态, 或者仅支持乘法同态, 最好的方案也仅支持任意次的加法同态和单次乘法同态 [6]. 直到 2009 年, Gentry [7] 首次成功构造出了一个全同态加密方案, 并创新性的提出了 bootstrapping 技术, 可以把任意一个可自举的部分同态加密方案转化为一个全同态加密方案.

自 Gentry 的突破性进展之后, 针对全同态加密的构造方案或改进方案主要基于理想格. 但是这些方案普遍效率较低, 无法应用. 2011 年, Brakerski 和 Vaikuntanathan [8] 运用 Regev [9] 在 2005 年提出的 LWE(Learning With Errors) 问题构造出一套全同态加密方案, 该方案使用重线性技术和维度模数规约技术控制密文的维度和噪声的增长. 2013 年, Gentry, Sahai 和 Waters [10] 提出了一种基于近似特征向量的全同态加密方案 (简称 GSW 方案). 不同于标准 LWE 方案中的向量密文, 该方案的密文是一个矩阵, 不论矩阵加法还是乘法都不会增加密文的维度, 因此该方案不需要使用维度模数规约技术, 而其安全性依旧依赖于 LWE 问题. 但是该方案并不是一个全同态加密方案. 2014 年, Brakerski 和 Vaikuntanathan [11] 提出针对 GSW 方案的 bootstrapping 方法, 但该方法效率不高. 同年, Alperin-Sheriff 和 Peikert [12] 修改 GSW 方案的密文矩阵, 提出一种在同态解密时快速计算内积的方法, 并辅以 bootstrapping 技术, 构造出了一套误差项多项式级别增长的全同态加密方案. 2014 年, Halevi 和 Shoup [13,14] 提出 LWE 体系全同态加密的软件实现方案 HElib, 并公开源码. 2015 年, Alperin-Sheriff [15] 和 Ryo Hiromasa [16] 等人分别设计了文献 [12] 的多比特并行方案, 但缺乏对方案的软件实现. 同年, Leo-Ducas 和 Daniele Micciancio [17] 在文献 [12] 的基础上提出一种更加快速的 bootstrapping 方案, 其对单比特 NAND 门操作仅需半秒. 然而该方案实现复杂, 并且随机数生成过于简单, 存在安全隐患. 随后不久, Luis Ruiz [18] 等人又实现了方案 [17] 的多比特版本.

本文以 Alperin-Sheriff 和 Peikert [12] 提出的变体 GSW 方案为基础, 设计了一系列比特同态门电路操作, 构造了针对改进方案的维度模数规约方法, 并实验验证了改进方案的正确性. 在此基础上可以采用 Alperin-Sheriff 和 Peikert 提出的快速 bootstrapping 技术, 将改进方案转变成一个全同态加密方案. 本方案操作简便, 且易于理解.

本文的第 2 节介绍相关的背景知识; 第 3 节介绍了基于近似特征向量的全同态加密变体方案及相应的维度模数规约方法; 第 4 节从正确性、安全性和参数选择三个角度对改进方案作出了分析; 第 5 节给出了方案的软件实现结果; 第 6 节对全文进行总结.

2 预备知识

2.1 符号

本文中的所有向量默认为列向量, 使用粗体小写字母表示, 例如 $\boldsymbol{b}$. 向量 $\boldsymbol{b}$ 的转置表示为 $\boldsymbol{b}^{\mathrm{T}}$, 向量 $\boldsymbol{b}$ 的第 i 个分量表示为 $\boldsymbol{b}_i$. 矩阵使用粗体大写字母表示, 例如 $\boldsymbol{M}^{m\times n}$. 矩阵 $\boldsymbol{M}^{m\times n}$ 的第 i 行第 j 列元素表示为 $\boldsymbol{M}_{i,j}$. $\mathbb{Z}_q^n$ 表示 n 维模 q 整数环,$(\mathbb{Z}_q,+)$ 表示其加法群,$\mathbb{R}^n$ 表示 n 维实数.

本文中 $[\cdot]_q$ 表示模 q 操作. $\langle \boldsymbol{a},\boldsymbol{b}\rangle$ 表示两个向量的内积. 对于概率分布 $\chi, x \xleftarrow{\$} \chi$ 表示随机选取符合概率分布 χ 的变量 x. 其余符号含义见文中具体定义.

2.2 亚高斯随机变量

如果一个随机变量 X 对任意 $t\geq 0$, 有

$$\Pr[|X|\geq t]\leq 2\exp(-\pi t^2/s^2) \tag{1}$$

称该变量满足参数为 s 的亚高斯分布 [19]. 任意以 B 为界的随机变量 X 满足参数为 $B\sqrt{2\pi}$ 的亚高斯分布. 随机变量 X_1 和 X_2 分别满足参数为 s_1、s_2 的亚高斯分布, 则随机变量 X_1+X_2 满足参数为 $\sqrt{s_1^2+s_2^2}$ 的亚高斯分布.

这种性质可以扩展到向量中, 一个向量 x 满足参数为 s 的亚高斯分布, 指对于所有实数单位向量 $\boldsymbol{u}$, $\langle \boldsymbol{u},\boldsymbol{x}\rangle$ 也满足参数为 s 的亚高斯分布. 一些均满足参数为 s 的亚高斯分布的向量的串联也满足参数为 s 的亚高斯分布. 亚高斯分布向量的欧式范数满足如下命题.

命题 1 [19] 随机向量 $\boldsymbol{x}\in\mathbb{R}^n$, 其每个分量独立地满足参数为 s 的亚高斯分布, 则存在一个通用常数 $C>0$, 满足 $\Pr[\|\boldsymbol{x}\|_2>C\cdot s\sqrt{n}]\leq 2^{-\Omega(n)}$.

2.3 LWE 问题 (Learning With Errors)

LWE 问题由 Regev [9] 在 2005 年首次提出. LWE 参数包括: 正整数 n 和 $q>2$, 以及一个整数上的误差分布 χ. 为了确保正确, 通常取 χ 满足参数为 $\boldsymbol{\alpha}q$ 的离散高斯分布, 其中 $\alpha<1$ 称为 "误差率".

定义 1 [9](LWE 分布): n 维模 q 向量 $\boldsymbol{s}\in\mathbb{Z}_q^n$ 是秘密信息, $\mathbb{Z}_q^n\times\mathbb{Z}_q$ 上的 LWE 分布 $A_{s,\chi}$ 是指按如下方式抽样: 均匀随机地选取 $\boldsymbol{\alpha}\in\mathbb{Z}_q^n$, 按分布 χ 选取误差项 e 输出 $n+1$ 维向量 $(\boldsymbol{\alpha},\boldsymbol{b}=\langle s,\boldsymbol{\alpha}\rangle+e \bmod q)$.

LWE 问题衍生出如下两个版本: 搜索型 LWE 问题 (Search-LWE) 和判定型 LWE(Decision-LWE) 问题:

定义 2 [9](Search-LWE) 有 m 个相互独立的样本 $(\boldsymbol{\alpha}_i,\boldsymbol{b}_i)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$, 这些样本按照秘密信息为 $\boldsymbol{s}\in\mathbb{Z}_q^n$ 的 LWE 分布 $A_{s,\chi}$ 取得, 搜索型 LWE 问题就是在仅有足够多的 LWE 样本的条件下, 找出生成这些样本的秘密信息 $\boldsymbol{s}$.

定义 3 [9](Decision-LWE) 有两组样本，每组包含 m 个相互独立的个体 $(\boldsymbol{\alpha}_i,\boldsymbol{b}_i)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$, 两组样本分别按如下两种方式中的一种选取:(1) 按照秘密信息为 $s\in\mathbb{Z}_q^n$ 的分布 $A_{s,\chi}$ 抽样; (2) 在 $\mathbb{Z}_q^n\times\mathbb{Z}_q$ 中随机均匀地选取. 判定型 LWE 问题就是区分样本组是通过哪种方式选取的. DLWE 假设即假设上述两种选取方式不可区分.

Regev [9] 证明了在量子归约下, 判定型 LWE 问题可以规约到格上的近似 SVP 问题.

2.4 CPA 安全

针对密码学方案的攻击模式主要包括选择明文攻击 (CPA) 和选择密文攻击 (CCA) 等. 其中, CPA 是指攻击者任选一定数量的明文, 让被攻击的加密算法加密, 得到对应的密文, 攻击者在这一过程中可以获得加密算法的相关信息, 以帮助其在未来更有效地破解同样的加密算法.

在一般的公钥密码方案中, CPA 安全通常使用如下游戏定义:

定义 4 (CPA 攻击):

初始化: 挑战者运行密钥生成算法 $\mathrm{KenGen}_\varepsilon(\lambda)\xrightarrow{R}(\mathrm{sk},\mathrm{pk})$, 将公钥 pk 发给攻击者 A.

挑战: 攻击者 A 生成两个明文 $\pi_0,\pi_1\in P$ 发给挑战者, 挑战者随机选取 $b\in\{0,1\}$, 并使用 $\mathrm{Encrypt}_\varepsilon(\mathrm{pk},\pi_b^*)\xrightarrow{R}\psi^*$ 计算其密文, 再把密文 ψ^* 发给攻击者.

猜测: 攻击者 A 猜测一个明文标识 $b' \in \{0,1\}$, 如果 $b'=b$, 攻击者获胜.

在上述游戏中, 定义攻击者 A 攻击方案 ε 的优势为 Adv, 有:

$$\mathrm{Adv}(A,\varepsilon,\lambda) = |\Pr[b=b'] - \frac{1}{2}| \tag{2}$$

由文献 [20] 的结论可知, 要证明一个同态加密方案满足 CPA 安全, 只需证明该同态加密方案的原始公钥方案满足 CPA 安全即可.

2.5 完备电路

一个电路由多项式个输入门、输出门, 以及中间计算节点组成. 任何的函数都可以由电路来计算. 特别地, 如果一个电路门的集合能够计算所有的电路, 那么我们称这个集合是完备的. 考虑 F_2 上的布尔电路, 完备电路门的集合有: {AND-gate,NEG-gate}, {AND-gate,XOR-gate}, {NAND-gate} 等.

3 基于近似特征向量的全同态加密方案

本章将详细介绍基于 GSW 方案构造的变体方案, 包括公钥方案和在此基础上构造的同态门电路操作, 并给出针对改进方案设计的维度模数规约方法, 在此基础上采用文献 [12] 的快速 bootstrapping 技术可以将改进方案转变成一个高效的全同态加密方案.

3.1 矩阵展开

对于模数 q, 定义 $d = \lceil \log_2 q \rceil$, 定义向量 $\boldsymbol{v} = \mathrm{powersof2}(1) = (2^{d-1}, 2^{d-2}, \cdots, 2, 1)^{\mathrm{T}}$. 向量 $\boldsymbol{v}$ 的第二个元素 $\boldsymbol{v}_2 = 2^{d-2} \in [q/4, q/2)$.

由文献 [21] 可知, 对于任意矩阵 $\boldsymbol{C}^{m\times n} \in \mathbb{Z}_q^{m\times n}$, 可以定义一个随机函数 $f: \mathbb{Z}_q^{m\times n} \to \mathbb{Z}^{m\times nd}$, 使得 $X = f(\boldsymbol{C})$ 时, 有 $X \cdot \boldsymbol{M}_{\mathrm{powersof2}} = \boldsymbol{C}$. 而且，所有的 X 满足参数为 $O(1)$ 的亚高斯分布. 其中, 矩阵 $\boldsymbol{M}$ 定义如下:

$$\boldsymbol{M}_{\mathrm{powersof2}} = \boldsymbol{v} \otimes I_n = \begin{pmatrix} \boldsymbol{v} & & 0 \\ & \ddots & \\ 0 & & \boldsymbol{v} \end{pmatrix} \in \mathbb{Z}_q^{nd\times n} \tag{3}$$

3.2 基于 GSW 方案的变体方案

GSW 方案包括如下参数: 安全参数 λ , 密钥维度 $n = O(\lambda)$, 模数 q, 参数 $d = \lceil \log_2 q \rceil$, 以及误差满足参数为 $s = \Theta(\sqrt{n})$ 的亚高斯分布 χ. 基于 GSW 的变体方案 (Variant of GSW, 简称 VGSW) 介绍如下:

VGSW.skGen(params): 输入一系列 GSW 方案参数, 按照分布 χ 随机选取 $n-1$ 个数, 生成一个向量 $\boldsymbol{s}^{\mathrm{init}} \xleftarrow{\$} \chi^{n-1}$, 输出私钥 $\mathrm{sk} = (1, \boldsymbol{s}^{\mathrm{init}})^{\mathrm{T}} = (1, \boldsymbol{s}_1^{\mathrm{init}}, \boldsymbol{s}_2^{\mathrm{init}}, \cdots, \boldsymbol{s}_n^{\mathrm{init}})^{\mathrm{T}} \in \mathbb{Z}^n$.

VGSW.pkGen($\boldsymbol{s}^{\mathrm{init}}$): 输入 VGSW.skGen(params) 中生成的 $\boldsymbol{s}^{\mathrm{init}}$, 在 $\mathbb{Z}_q$ 上随机均匀地选取矩阵 $\boldsymbol{A} \xleftarrow{\$} \mathbb{Z}_q^{nd\times(n-1)}$, 同时在分布 χ 上选取误差 $\boldsymbol{e} \xleftarrow{\$} \chi^{nd}$. 然后计算向量 $\boldsymbol{b} = [\boldsymbol{A}\cdot\boldsymbol{s}^{\mathrm{init}} + \boldsymbol{e}]_q \in \mathbb{Z}_q^{nd}$. 此时, 定义公钥 $\mathrm{pk} = (\boldsymbol{b}| - \boldsymbol{A}) \in \mathbb{Z}_q^{nd\times n}$. 本文中的公钥 pk 和私钥 sk 具有与原 GSW 方案相同的性质, 即 $\mathrm{pk}\cdot\mathrm{sk} = \boldsymbol{e}$.

VGSW.pkEnc(sk,$m \in \{0,1\}$): 取私钥 sk 的后 $n-1$ 位, 即 $\boldsymbol{s}^{\mathrm{init}}$, 随机选取矩阵 $\boldsymbol{A} \xleftarrow{\$} \mathbb{Z}_q^{nd\times(n-1)}$, 误差 $\boldsymbol{e} \xleftarrow{\$} \chi^{nd}$, 并生成 $\boldsymbol{b} = [\boldsymbol{A}\cdot\boldsymbol{s}^{\mathrm{init}} + \boldsymbol{e}]_q \in \mathbb{Z}_q^{nd}$, 输出密文为:$\boldsymbol{C} = (\boldsymbol{b}| - \boldsymbol{A}) + m\boldsymbol{M}_{\mathrm{powersof2}}$, 其中 $\boldsymbol{M}_{\mathrm{powersof2}}$ 在 3.1 节中已有介绍.

VGSW.pkEnc(pk,$m \in \{0,1\}$): 以 VGSW.pkGen($\boldsymbol{s}^{\mathrm{init}}$) 生成的公钥作为输入, 随机均匀地选取矩阵 $\boldsymbol{R} \xleftarrow{\$} \{0,1\}^{nd\times nd}$, 输出密文 $\boldsymbol{C} = \boldsymbol{R}\cdot\mathrm{pk} + m\boldsymbol{M}_{\mathrm{powersof2}}$.

VGSW.UDec($\boldsymbol{C}$,sk) 以密文 $\boldsymbol{C}$ 和私钥 sk 作为输入, 解密过程如下: 选取密文 $\boldsymbol{C}$ 的第二行 $\boldsymbol{C}_{\mathrm{second}}$, 计算明文

$$m = \begin{cases} 0, & [\langle \boldsymbol{C}_{\mathrm{second}}, \mathrm{sk}\rangle]_q \to 0 \\ 1, & [\langle \boldsymbol{C}_{\mathrm{second}}, \mathrm{sk}\rangle]_q \to 2^{d-2} \end{cases} \tag{4}$$

即, 计算 $\boldsymbol{C}_{\text{second}}$ 与 sk 的内积 $m'=\langle \boldsymbol{C}_{\text{second}}, \text{sk}\rangle$, 对结果 m' 模 q , 当结果接近于 0 时, 明文 $m=0$. 当结果接近 2^{d-2} 时, 则明文 $m=1$.

VGSW.HomoAdd$(\boldsymbol{C}_1, \boldsymbol{C}_2)$ 直接定义为矩阵加法, 即计算 $\boldsymbol{C}_1 \oplus \boldsymbol{C}_2 = \boldsymbol{C}_1 + \boldsymbol{C}_2$.

VGSW.HomoMult$(\boldsymbol{C}_1, \boldsymbol{C}_2)$ 定义为 $\boldsymbol{C}_1 \otimes \boldsymbol{C}_2 = f(\boldsymbol{C}_1)\cdot \boldsymbol{C}_2$.

变体方案 VGSW 还可以定义以下针对布尔电路的同态操作:

同态与门 HomoAND$(\boldsymbol{C}_1, \boldsymbol{C}_2)$: 针对二进制比特的与门与 $\mathbb{Z}_2$ 上的乘法的真值表等效, 故而同态与门构造为:

$$\text{HomoAND}(\boldsymbol{C}_1, \boldsymbol{C}_2) = \boldsymbol{C}_1 \otimes \boldsymbol{C}_2 = f(\boldsymbol{C}_1)\cdot \boldsymbol{C}_2 \tag{5}$$

同态或门 HomoOR$(\boldsymbol{C}_1, \boldsymbol{C}_2)$: 由 HomoAdd 和 VGSW.UDec 的定义可知, 当 HomoAdd 函数的输入密文均为 $\{0,1\}$ 比特密文时, 恰好与 " 或" 运算具有相同的真值表, 因此定义 "同态或" 操作 HomoOR 为:

$$\text{HomoOR}(\boldsymbol{C}_1, \boldsymbol{C}_2) = \boldsymbol{C} = \text{HomoAdd}(\boldsymbol{C}_1, \boldsymbol{C}_2) \tag{6}$$

同态与非门 HomoAND$(\boldsymbol{C}_1, \boldsymbol{C}_2)$: 定义为

$$\text{HomoNAND}(\boldsymbol{C}_1, \boldsymbol{C}_2) = \boldsymbol{C} = \boldsymbol{M}_{\text{powersof2}} - \boldsymbol{C}_1 \otimes \boldsymbol{C}_2 = \boldsymbol{M}_{\text{powersof2}} - f(\boldsymbol{C}_1)\cdot \boldsymbol{C}_2 \tag{7}$$

同态异或门 HomoXOR$(\boldsymbol{C}_1, \boldsymbol{C}_2)$ 定义为

$$\text{HomoXOR}(\boldsymbol{C}_1, \boldsymbol{C}_2) = \boldsymbol{C} = (\boldsymbol{M}_{\text{powersof2}} - \boldsymbol{C}_2)\otimes \boldsymbol{C}_1 + (\boldsymbol{M}_{\text{powersof2}} - \boldsymbol{C}_1)\otimes \boldsymbol{C}_2 \tag{8}$$

3.3　维度模数规约

在传统的 LWE 同态加密方案中, 密文的乘法操作使得所得密文的维度和噪声增大, 需要使用维度模数规约的方式降维降噪. 在 VGSW 方案中, 虽然密文的乘法并不会造成密文维度的增加, 但是为了更高效地 bootstrapping, 在本文中依然需要使用维度模数规约.

VGSW 的维度规约操作包括两个函数:

(1) 转换密钥生成函数 SwitchKeyGen$(\boldsymbol{s}_{\text{in}}, \boldsymbol{s}_{\text{out}}, n_1, n_2, q)$, 以转换前后的密钥 $\boldsymbol{s}_{\text{in}}, \boldsymbol{s}_{\text{out}}$ 及其维度 n 和模数 q 作为输入, 输出一个变换矩阵 $\boldsymbol{\tau}_{\boldsymbol{s}_{\text{in}}\to \boldsymbol{s}_{\text{out}}}$;

(2) 维度规约函数 SwitchKey$(\boldsymbol{\tau}_{\boldsymbol{s}_{\text{in}}\to \boldsymbol{s}_{\text{out}}}, \boldsymbol{c}_{\text{in}}, n_1, n_2, q)$, 以 SwitchKeyGen$(\boldsymbol{s}_{\text{in}}, \boldsymbol{s}_{\text{out}}, n_1, n_2, q)$ 输出的变换矩阵和 $\boldsymbol{s}_{\text{in}}$ 下的密文 $\boldsymbol{c}_{\text{in}}$ 为输入, 输出密钥 $\boldsymbol{s}_{\text{out}}$ 下的密文 $\boldsymbol{c}_{\text{out}}$.

在 VGSW 方案的解密函数中, 选取密文的第二行, 执行解密操作 $\langle \boldsymbol{C}_{\text{second}}, \text{sk}\rangle$. 假定当前 VGSW 密文 $\boldsymbol{C}$ 的噪声已经达到上限, 无法再做更多的同态操作. 此时, 取 $\boldsymbol{C}$ 的第二行作为 $\boldsymbol{c}_{\text{in}}$, 使用维度规约函数生成规约后的密文 $\boldsymbol{c}_{\text{out}}$.

下面将针对 VGSW 方案构造维度规约函数:

(1) SwitchKeyGen$(\boldsymbol{s}_{\text{in}}, \boldsymbol{s}_{\text{out}}, n_1, n_2, q)$: 随机均匀地选取 $\bar{\boldsymbol{A}} \in \mathbb{Z}_q^{(n_2-1)\times(n_1\lceil \log q\rceil)}$, 按照分布 χ 选取误差项 $\boldsymbol{e} \leftarrow \chi^{n_1\lceil \log q\rceil}$, 定义:

$$\boldsymbol{b}^{\text{T}} = (\boldsymbol{e}^{\text{T}} - \bar{\boldsymbol{s}}_{\text{out}}^{\text{T}}\cdot \bar{\boldsymbol{A}}) \mod q \in \mathbb{Z}_q^{n_1\lceil \log q\rceil}$$

其中,$\bar{\boldsymbol{s}}_{\text{out}} \in \mathbb{Z}_q^{n_2-1}$ 且 $\boldsymbol{s}_{\text{out}} = (1, \bar{\boldsymbol{s}}_{\text{out}}^{\text{T}})$, 而 $\boldsymbol{s}_{\text{in}}, \boldsymbol{s}_{\text{out}}$ 均使用私钥生成函数 VGSW.SKGen(params) 生成. 根据式 (9) 计算中间结果 $\boldsymbol{A}$:

$$\boldsymbol{A} = \left[\frac{\boldsymbol{b}^{\text{T}}}{\bar{\boldsymbol{A}}}\right] \in \mathbb{Z}_q^{n_2\times(n_1\lceil \log q\rceil)} \tag{9}$$

观察式 (9), 有:

$$\boldsymbol{s}_{\text{out}}^{\text{T}}\cdot \boldsymbol{A} = (1, \bar{\boldsymbol{s}}_{\text{out}}^{\text{T}})\cdot \left[\frac{\boldsymbol{b}^{\text{T}}}{\bar{\boldsymbol{A}}}\right] = \boldsymbol{b}^{\text{T}} + \bar{\boldsymbol{s}}_{\text{out}}^{\text{T}}\cdot \bar{\boldsymbol{A}} = \boldsymbol{e}^{\text{T}}$$

输出

$$\boldsymbol{B} = \boldsymbol{A} + \left[\frac{\text{Powersof2}(\boldsymbol{s}_{\text{in}}^{\text{T}})}{\boldsymbol{O}}\right] \tag{10}$$

其中, 矩阵 $\boldsymbol{O} \in \{0\}^{(n_2-1)\times n_1\lceil \log q\rceil}$. 令 $\tau_{\boldsymbol{s}_{\text{in}}\to\boldsymbol{s}_{\text{out}}} = \boldsymbol{B}$.

(2) SwitchKey($\boldsymbol{\tau}_{\boldsymbol{s}_{\text{in}}\to\boldsymbol{s}_{\text{out}}}, \boldsymbol{c}_{\text{in}}, n_1, n_2, q$): 直接输出

$$\boldsymbol{c}_{\text{out}} = \boldsymbol{B}\cdot \text{BitDecomp}(\boldsymbol{c}_{\text{in}}) \tag{11}$$

VGSW 的模数规约按照如下方式定义.

密文 $\boldsymbol{c}_{\text{in}}$ 取自 VGSW 方案密文的第 2 行, 有 $\boldsymbol{c}_{\text{in}} \in \mathbb{Z}_q^n$, 密钥 $\boldsymbol{s}$ 是一个 LWE 短向量. 新密文 $\boldsymbol{c}_{\text{out}}$ 的本质是原密文 $\boldsymbol{c}_{\text{in}}$ 的约减, 即新密文 $\boldsymbol{c}_{\text{out}}$ 接近于 $(p/q)\boldsymbol{c}_{\text{in}}$. 其中, p 是新密文的模数, 即 $\boldsymbol{c}_{\text{out}} \in \mathbb{Z}_q^n$. 具体定义如下:

定义 5 (模数规约): 如果目标模数为 p, 对于密文 $\boldsymbol{c} \in \mathbb{Z}_q^n$ 的模数规约定义为 $\boldsymbol{c}' = \lfloor (p/q)\cdot \boldsymbol{c}\rceil = (\boldsymbol{c}'_1, \cdots, \boldsymbol{c}'_n)$, 其中 $\boldsymbol{c}'_i = \lfloor \delta \cdot \boldsymbol{c}_i\rceil$, 且

$$\delta = p/q \tag{12}$$

文献 [12] 指出, 采用其设计的快速 bootstrapping 技术, 将会输出 GSW 矩阵密文. 这样, 在本方案的维度模数规约之后, 运用文献 [12] 的快速 bootstrapping 技术, 也就可以生成 GSW 矩阵密文.

4 方案分析

本章将对 VGSW 方案的正确性和安全性进行分析, 并给出部分参数的选择方案.

4.1 正确性分析

(1) 加密方案正确性分析

对于使用 VGSW.skEnc(sk,m) 加密的密文 $\boldsymbol{C} = (\boldsymbol{b}|-\boldsymbol{A}) + m\boldsymbol{M}_{\text{powersof2}}$, 解密操作为 $[\langle \boldsymbol{C}_{\text{second}}, \text{sk}\rangle]_q$. 即:

$$\begin{aligned}\boldsymbol{C}_{\text{second}}\cdot \text{sk} &= [(\boldsymbol{b}|-\boldsymbol{A})]_{\text{second}}\cdot \text{sk} + m[\boldsymbol{M}_{\text{powersof2}}]_{\text{second}}\cdot \text{sk}\\ &= \boldsymbol{e}_{\text{second}} + m[\boldsymbol{M}_{\text{powersof2}}]_{\text{second}}\cdot \text{sk}\\ &= \boldsymbol{e}_{\text{second}} + m\langle (2^{d-2}, 0, \cdots, 0), (1, \boldsymbol{s}^{init})\rangle\\ &= \boldsymbol{e}_{\text{second}} + 2^{d-2}m\end{aligned}$$

这样，对于 VGSW.skEnc(sk.m) 加密函数，当 $|\boldsymbol{e}_{\text{second}}| < q/8$ 时, 解密正确.

对于使用 VGSW.skEnc(pk.m) 加密的密文 $\boldsymbol{C} = \boldsymbol{R}\cdot \text{pk} + m\boldsymbol{M}_{\text{powersof2}}$, 解密操作为 $\boldsymbol{C}_{\text{second}}\cdot \text{sk} = [\boldsymbol{R}\cdot \text{pk}]_{\text{second}}\cdot \text{sk} + m[\boldsymbol{M}_{\text{powersof2}}]_{\text{second}}\cdot \text{sk}$. 由于有式

$$\boldsymbol{R}\cdot \text{pk}\cdot \text{sk} = \boldsymbol{R}\cdot \boldsymbol{e}$$

成立. 而解密时是取密文第二行, 并且 $\boldsymbol{R}_{\text{second}} \in \{0,1\}^{nd}$, 故有:

$$\boldsymbol{R}_{\text{second}}\cdot \boldsymbol{e} \le \|\boldsymbol{e}\|_1$$

其中, $\|*\|_1$ 表示 * 的第一范数. 因此, 解密操作

$$\boldsymbol{C}_{\text{second}}\cdot \text{sk} = \boldsymbol{R}_{\text{second}}\cdot \boldsymbol{e} + m[\boldsymbol{M}_{\text{powersof2}}]_{\text{second}}\cdot \text{sk} \le \|\boldsymbol{e}\|_1 + 2^{d-2}m \tag{13}$$

由于 $q/4 \le 2^{d-2} < q/2$, 所以 $\|\boldsymbol{e}\|_1 < q/8$ 时解密正确.

为保证解密正确性，可以通过设置误差分布使得误差项满足上述条件.

(2) 同态操作正确性分析

由于私钥加密和公钥加密误差项近似, 如下分析过程仅以私钥加密的密文为例.

设 $\boldsymbol{C}_1$、$\boldsymbol{C}_2$ 为使用同一密钥分别加密明文 m_1 和 m_2 的密文, 解密同态加法 $\boldsymbol{C}_1 \oplus \boldsymbol{C}_2 = \boldsymbol{C}_1 + \boldsymbol{C}_2$ 可得:

$$\begin{aligned}(\boldsymbol{C}_1 \oplus \boldsymbol{C}_2)\mathrm{sk} &= \boldsymbol{C}_1 \cdot \mathrm{sk} + \boldsymbol{C}_2 \cdot \mathrm{sk} \\ &= \boldsymbol{e}_1 + m_1 \boldsymbol{M}_{\mathrm{powersof2}} \cdot \mathrm{sk} + \boldsymbol{e}_2 + m_2 \boldsymbol{M}_{\mathrm{powersof2}} \cdot \mathrm{sk} \\ &= (\boldsymbol{e}_1 + \boldsymbol{e}_2) + (m_1 + m_2)\boldsymbol{M}_{\mathrm{powersof2}} \cdot \mathrm{sk}\end{aligned} \tag{14}$$

只要误差 $\boldsymbol{e}_1 + \boldsymbol{e}_2 < 8/q$, 解密可得正确的明文.

对于同态乘法结果, 解密可得:

$$\begin{aligned}(\boldsymbol{C}_1 \otimes \boldsymbol{C}_2)\mathrm{sk} &= f(\boldsymbol{C}_1) \cdot \boldsymbol{C}_2 \cdot \mathrm{sk} = X_1 \cdot \boldsymbol{C}_2 \cdot \mathrm{sk} \\ &= X_1 \cdot (\boldsymbol{e}_2 + m_2 \boldsymbol{M}_{\mathrm{powersof2}} \cdot \mathrm{sk}) \\ &= X_1 \cdot \boldsymbol{e}_2 + m_2 \boldsymbol{C}_1 \cdot \mathrm{sk} \\ &= (X_1 \cdot \boldsymbol{e}_2 + m_2 \boldsymbol{e}_1) + m_1 m_2 \boldsymbol{M}_{\mathrm{powersof2}} \cdot \mathrm{sk}\end{aligned} \tag{15}$$

只要误差 $X_1 \cdot \boldsymbol{e}_2 + m_2 \boldsymbol{e}_1 < q/8$, 解密可得正确的明文. 另外, 由 $\boldsymbol{e}_1$、$\boldsymbol{e}_2$ 相互独立且满足参数为 $O(\|\boldsymbol{e}\|)$ 的亚高斯分布可以得出, 密文的误差以多项式因子增长.

(3) 同态电路门正确性分析

同态与门的正确性验证: 直接解密所得密文, 在 $(X_1 \cdot \boldsymbol{e}_2 + m_2 \boldsymbol{e}_1) + m_1 m_2 \boldsymbol{M}_{\mathrm{powersof2}} \cdot \mathrm{sk}$ 中, 由于明文属于空间 $\mathbb{Z}_2$, 新生成密文的噪声上限扩展为原有噪声的 $(nd+1)$ 倍, 选取恰当的参数即可保证一次 HomoAND 操作后解密的正确性.

同态或门的噪声增长情况与 VGSW.HomoAdd$(\boldsymbol{C}_1, \boldsymbol{C}_2)$ 相同, 满足噪声约束的情况下可以正确解密.

同态与非门的正确性验证: 直接解密所得密文

$$\begin{aligned}\mathrm{HomoNAND}(\boldsymbol{C}_1, \boldsymbol{C}_2) \cdot \mathrm{sk} &= (\boldsymbol{M}_{\mathrm{powersof2}} - f(\boldsymbol{C}_1) \cdot \boldsymbol{C}_2) \cdot \mathrm{sk} \\ &= \boldsymbol{M}_{\mathrm{powersof2}} \cdot \mathrm{sk} - X_1 \cdot (\boldsymbol{e}_2 + m_2 \boldsymbol{M}_{\mathrm{powersof2}} \cdot \mathrm{sk}) \\ &= \boldsymbol{M}_{\mathrm{powersof2}} \cdot \mathrm{sk} - X_1 \cdot \boldsymbol{e}_2 - m_2 C_1 \cdot \mathrm{sk} \\ &= \boldsymbol{M}_{\mathrm{powersof2}} \cdot \mathrm{sk} - (X_1 \cdot \boldsymbol{e}_1 + m_2 \boldsymbol{e}_1) - m_1 m_2 \boldsymbol{M}_{\mathrm{powersof2}} \cdot \mathrm{sk} \\ &= (1 - m_1 m_2)\boldsymbol{M}_{\mathrm{powersof2}} \cdot \mathrm{sk} - (X_1 \cdot \boldsymbol{e}_2 + m_2 \boldsymbol{e}_1)\end{aligned} \tag{16}$$

同样, 新密文的噪声上限扩展为原有噪声的 $(nd+1)$ 倍, 可以通过参数选取保证解密的正确性.

同态异或门的正确性验证: 直接解密所得密文

$$\begin{aligned}\boldsymbol{C} \cdot \mathrm{sk} =& ((\boldsymbol{M}_{\mathrm{powersof2}} - \boldsymbol{C}_2) \otimes \boldsymbol{C}_1 + (\boldsymbol{M}_{\mathrm{powersof2}} - \boldsymbol{C}_1) \otimes \boldsymbol{C}_2) \cdot \mathrm{sk} \\ =& (\boldsymbol{M}_{\mathrm{powersof2}} \otimes \boldsymbol{C}_1 - \boldsymbol{C}_2 \otimes \boldsymbol{C}_1 + \boldsymbol{M}_{\mathrm{powersof2}} \otimes \boldsymbol{C}_2 - \boldsymbol{C}_1 \otimes \boldsymbol{C}_2) \cdot \mathrm{sk} \\ =& (\boldsymbol{M}_{\mathrm{powersof2}} - \boldsymbol{C}_2) \otimes \boldsymbol{C}_1 \cdot \mathrm{sk} + (\boldsymbol{M}_{\mathrm{powersof2}} - \boldsymbol{C}_1) \otimes \boldsymbol{C}_2 \cdot \mathrm{sk} \\ =& (\boldsymbol{M}_{\mathrm{powersof2}} - \boldsymbol{C}_2)(\boldsymbol{e}_1 + m_1 \cdot \boldsymbol{M}_{\mathrm{powersof2}} \cdot \mathrm{sk}) \\ &+ (\boldsymbol{M}_{\mathrm{powersof2}} - \boldsymbol{C}_1)(\boldsymbol{e}_2 + m_2 \cdot \boldsymbol{M}_{\mathrm{powersof2}} \cdot \mathrm{sk}) \\ =& \boldsymbol{M}_{\mathrm{powersof2}} \cdot \boldsymbol{e}_1 + m_1 \cdot \boldsymbol{M}_{\mathrm{powersof2}} \otimes \boldsymbol{M}_{\mathrm{powersof2}} \cdot \mathrm{sk} - \boldsymbol{C}_2 \cdot \boldsymbol{e}_1 - m_1 \cdot \boldsymbol{C}_2 \otimes \boldsymbol{M}_{\mathrm{powersof2}} \cdot \mathrm{sk} \\ &+ \boldsymbol{M}_{\mathrm{powersof2}} \cdot \boldsymbol{e}_2 + m_2 \cdot \boldsymbol{M}_{\mathrm{powersof2}} \otimes \boldsymbol{M}_{\mathrm{powersof2}} \cdot \mathrm{sk} - \boldsymbol{C}_1 \cdot \boldsymbol{e}_2 - m_2 \cdot \boldsymbol{C}_1 \otimes \boldsymbol{M}_{\mathrm{powersof2}} \cdot \mathrm{sk}\end{aligned} \tag{17}$$

由 3.1 节函数 f 的定义可知

$$f(\boldsymbol{M}_{\text{powersof2}}) = \boldsymbol{M}_{\text{powersof2}} \cdot \boldsymbol{M}_{\text{powersof2}}^{-1}$$

于是

$$f(\boldsymbol{M}_{\text{powersof2}}) \cdot \boldsymbol{M}_{\text{powersof2}} = \boldsymbol{M}_{\text{powersof2}}$$

结合本节的同态乘法定义可知

$$\boldsymbol{M}_{\text{powersof2}} \otimes \boldsymbol{M}_{\text{powersof2}} = f(\boldsymbol{M}_{\text{powersof2}}) \cdot \boldsymbol{M}_{\text{powersof2}} = \boldsymbol{M}_{\text{powersof2}} \tag{18}$$

再由 3.1 节函数 f 的定义可知

$$f(\boldsymbol{C}) = \boldsymbol{C} \cdot \boldsymbol{M}_{\text{powersof2}}^{-1}$$

于是

$$f(\boldsymbol{C}) \cdot \boldsymbol{M}_{\text{powersof2}} = \boldsymbol{C}$$

因此, 有

$$\boldsymbol{C} \otimes \boldsymbol{M}_{\text{powersof2}} = f(\boldsymbol{C}) \cdot \boldsymbol{M}_{\text{powersof2}} = \boldsymbol{C} \tag{19}$$

由式 (18) 和式 (19) 可知, 式 (17) 可化简为:

$$\begin{aligned}
\boldsymbol{C} \cdot \text{sk} =& \boldsymbol{M}_{\text{powersof2}} \cdot \boldsymbol{e}_1 + m_1 \cdot \boldsymbol{M}_{\text{powersof2}} \cdot \text{sk} - \boldsymbol{C}_2 \cdot \boldsymbol{e}_1 - m_1 \cdot \boldsymbol{C}_2 \cdot \text{sk} \\
&+ \boldsymbol{M}_{\text{powersof2}} \cdot \boldsymbol{e}_2 + m_2 \cdot \boldsymbol{M}_{\text{powersof2}} \cdot \text{sk} - \boldsymbol{C}_1 \cdot \boldsymbol{e}_2 - m_2 \cdot \boldsymbol{C}_1 \cdot \text{sk} \\
=& \boldsymbol{M}_{\text{powersof2}} \cdot (\boldsymbol{e}_1 + \boldsymbol{e}_2) + (m_1 + m_2) \cdot \boldsymbol{M}_{\text{powersof2}} \cdot \text{sk} \\
&- 2m_1 \cdot m_2 \cdot \boldsymbol{M}_{\text{powersof2}} \cdot \text{sk} - \boldsymbol{C}_1 \cdot \boldsymbol{e}_2 - \boldsymbol{C}_2 \cdot \boldsymbol{e}_1 \\
=& (m_1 + m_2 - 2m_1 m_2) \cdot \boldsymbol{M}_{\text{powersof2}} \cdot \text{sk} \\
&+ (\boldsymbol{M}_{\text{powersof2}} - \boldsymbol{C}_1) \cdot \boldsymbol{e}_2 + (\boldsymbol{M}_{\text{powersof2}} - \boldsymbol{C}_2) \cdot \boldsymbol{e}_1
\end{aligned} \tag{20}$$

对于 $m_1, m_2 \in \{0,1\}, m_1, m_2$ 的异或为:

$$m_1 \text{XOR} m_2 = m_1(1 - m_2) + m_2(1 - m_1) = m_1 + m_2 - 2m_1 m_2 \tag{21}$$

故由式 (20) 可以看到, 为了保证同态异或操作后解密可以得到正确的结果, 需要控制 $(\boldsymbol{M}_{\text{powersof2}} - \boldsymbol{C}_1) \cdot \boldsymbol{e}_2 + (\boldsymbol{M}_{\text{powersof2}} - \boldsymbol{C}_2) \cdot \boldsymbol{e}_1$ 的噪声. 事实上, $|(\boldsymbol{M}_{\text{powersof2}} - \boldsymbol{C}) \cdot \boldsymbol{e}| \leq nd\|\boldsymbol{e}\|_2$, 即新密文的噪声上界扩大为原有的 $2nd$ 倍, 同样可以通过选取合理的参数保证解密的正确性.

(4) 维度模数规约正确性分析

对维度规约后得到的新密文 $\boldsymbol{c}_{\text{out}}$ 直接解密可得:

$$\begin{aligned}
\langle \boldsymbol{s}_{\text{out}}, \boldsymbol{c}_{\text{out}} \rangle &= \boldsymbol{s}_{\text{out}}^{\text{T}} \cdot \boldsymbol{B} \cdot \text{BitDecomp}(\boldsymbol{c}_{\text{in}}) \\
&= \boldsymbol{s}_{\text{out}}^{\text{T}} \cdot (\boldsymbol{A} + \left[\frac{\text{Powersof2}(\boldsymbol{s}_{\text{in}}^{\text{T}})}{\boldsymbol{O}}\right]) \cdot \text{BitDecomp}(\boldsymbol{c}_{\text{in}}) \\
&= (\boldsymbol{s}_{\text{out}}^{\text{T}} \cdot \boldsymbol{A} + (1, \bar{S}_{\text{out}}^{\text{T}}) \cdot \left[\frac{\text{Powersof2}(\boldsymbol{s}_{\text{in}}^{\text{T}})}{\boldsymbol{O}}\right]) \cdot \text{BitDecomp}(\boldsymbol{c}_{\text{in}}) \\
&= (\boldsymbol{e}^{\text{T}} + \text{Powersof2}(\boldsymbol{s}_{\text{in}}^{\text{T}})) \cdot \text{BitDecomp}(\boldsymbol{c}_{\text{in}}) \\
&= \boldsymbol{e}^{\text{T}} \cdot \text{BitDecomp}(\boldsymbol{c}_{\text{in}}) + \boldsymbol{s}_{\text{in}}^{\text{T}} \cdot \boldsymbol{c}_{\text{in}}
\end{aligned} \tag{22}$$

由于 $\mathrm{BitDecomp}(a) \in \mathbb{Z}_2^{n\cdot\lceil\log q\rceil}$, 因此 $\boldsymbol{e}^{\mathrm{T}}\mathrm{BitDecomp}(\boldsymbol{c}_{\mathrm{in}})$ 的值很小, 从而维度规约后的新密文解密可以得到正确的明文.

对模数规约后的新密文直接解密可得:

$$\begin{aligned}\langle \boldsymbol{s}, \boldsymbol{c}'\rangle &= \langle \boldsymbol{s}, \lfloor\frac{p}{q}\rceil\cdot\boldsymbol{c}\rangle \\ &\in \langle \boldsymbol{s}, \frac{p}{q}\cdot\boldsymbol{c} + [-\frac{1}{2}, \frac{1}{2}]^n\rangle \\ &\subseteq (\frac{p}{q}\cdot\boldsymbol{e} + \|\boldsymbol{s}\|\sqrt{n}\cdot[-\frac{1}{2}, \frac{1}{2}]) + p\mathbb{Z}\end{aligned} \tag{23}$$

可见, 解密可得正确的结果, 并且噪声有所降低.

4.2 安全性分析

命题 2 设 n、q 等系统参数都是安全参数 λ 的多项式,χ 是参数为 $\boldsymbol{s} := \Theta(\sqrt{n})$ 的亚高斯分布, 在 DLWE 假设的前提下, 本方案是 IND-CPA 安全的.

证明: 采用基于游戏的方法来证明 IND-CPA 安全性, 使用优势 $\mathrm{Adv}_{\mathrm{Game}}[A]$ 来定义攻击者 A 在 Game 中获胜的概率.

Game0: 挑战者调用密钥生成算法 VGSW.pkGen 生成公钥 pk, 并将其交给攻击者 A. 攻击者 A 选择明文消息 $m_0, m_1 \in \{0,1\}$ 发送给挑战者. 挑战者随机选择 $b \in \{0,1\}$, 并使用加密函数 VGSW.pkEnc 加密明文 m_b, 将得到的挑战密文 c 发送给攻击者 A. 攻击者 A 猜测密文 c 所对应的明文标识为 b', 其优势定义为:

$$\mathrm{Adv}_{\mathrm{CPA}}[A] = \mathrm{Adv}_{\mathrm{Game0}} = |\Pr[b = b'] - 1/2| \tag{24}$$

Game1: Game1 和 Game0 的区别在于公钥的生成方式不同, Game1 中公钥的生成方式不再是 Game0 中采用的 VGSW.pkGen, 而是在 $\mathbb{Z}_q^{nd\times n}$ 上随机均匀地选取. 挑战密文的生成方式不变. 由 DLWE 假设可知, 攻击者对公钥生成方式区分优势等于其解决 DLWE 问题的优势, 即

$$|\mathrm{Adv}_{\mathrm{Game1}}[A] - \mathrm{Adv}_{\mathrm{CPA}}[A]| = \mathrm{DLWE}_{n,q,\chi}\mathrm{Adv}[A] \tag{25}$$

Game2: Game2 和 Game1 的区别在于密文的生成方式不同, Game2 中密文不再是通过 Game0 中采用的 VGSW.pkEnc 生成, 而是在 $\mathbb{Z}_q^{nd\times n}$ 上随机均匀地选取. 而 VGSW.pkEnc 的加密过程 $\boldsymbol{C} = \boldsymbol{R}\cdot\mathrm{pk} + m\boldsymbol{M}_{\mathrm{powersof2}}$ 符合 Regev 版加密方案, 且 $\boldsymbol{R}$ 的行数 $nd = n\lceil\log q\rceil$, 符合 Regev 版加密方案的安全性条件. 根据剩余哈希引理 [22], 攻击者 A 对 Game2 和 Game1 中的密文不可区分. 即对于 n 的可忽略函数 $\mathrm{negl}(n)$, 有

$$|\mathrm{Adv}_{\mathrm{Game2}}[A] - \mathrm{Adv}_{\mathrm{Game1}}[A]| \le \mathrm{negl}(n) \tag{26}$$

综上所述，在 DLWE 假设成立的前提下, VGSW 方案具有 IND-CPA 安全性. □

4.3 参数选择

由 2.5 节关于完备电路的介绍可知, AND 和 XOR 构成一组完备电路 {AND-gate , XOR-gate}, NAND 构成一组完备电路 {NAND-gate}. 因此, 关于这两组完备电路的参数选取需要分别介绍.

因为同态乘法操作对噪声的影响远大于同态加法, 所以一般情况下仅考虑同态乘法产生的噪声. 在由完备电路 {AND-gate , XOR-gate} 构成的同态加密方案中, 一次 HomoAND 需要一次同态乘法操作, 一次 HomoXOR 需要两次同态乘法操作. 因此, 噪声评估时以 HomoXOR 为主. 设 B 为新鲜密文的噪声上界, 那么一次同态异或操作的噪声上界为 $2ndB$. 在 L 层的同态加密方案中, L 层 HomoXOR 后的密文噪声上限值需要满足条件:

$$(2nd)^L B < q/8 \tag{27}$$

因此, 在安全性足够的前提下, 选择恰当的分布 χ 使误差上界 B 尽量小, 可以保证方案正确. 参数 q 和 n 的选取规则与 GSW 方案一致.

在由完备电路 {NAND -gate} 构成的同态加密方案中, 一次 HomoNAND 仅需一次同态乘法操作, 若 B 为新鲜密文的噪声上界, 那么一次同态与非操作的噪声上界为 ndB. 在 L 层的同态加密方案中, L 层 HomoXOR 后的密文噪声上限值需要满足条件:

$$(nd)^L B < q/8 \tag{28}$$

因此, 在安全性足够的前提下, 选择恰当的分布 χ 使误差上界 B 尽量小, 可以保证方案正确. 参数 q 和 n 的选取规则与 GSW 方案一致.

5 实验方案

5.1 实验环境

本文使用 C++ 语言编写所有算法, 软件运行在 Visual Studio 2010 上. 测试环境如下: CPU: Intel(R) Core(TM) i5-3230M 2.60GHz RAM: 8GB OS: Windows 7

5.2 实验结果

首先对 VGSW 方案的加密和解密效率进行测试. 随机选择 100 个二进制比特明文, VGSW 方案参数 n、q、d、χ 如表 1 所示. 按照 VGSW 方案中的定义，分别执行 100 次加密解密操作, 统计平均的加密和解密时间 (以毫秒为单位), 结果如表 1 所示. 可以发现, 随着 n、q 的增长, 加密时间也不断增长, 但解密速度很快, 都没有超过 1 毫秒.

表 1 加密解密测试实验结果

Table 1 Result of encryption and decryption test

n	q	d	加密时间 (ms)	解密时间 (ms)
16	2310	12	1.66	<1
32	30030	16	5.96	<1
64	510510	19	23.25	<1
128	9699690	24	92.48	<1
256	223092870	28	441.41	<1

接下来对同态电路门的计算效率进行测试. 随机选择 50 组二进制比特明文, 每组共两个明文 m_1 和 m_2. 其中,$m_1, m_2 \in \{0, 1\}$. 使用 VGSW 方案中的 pkEnc 函数分别对两个明文加密后依次执行方案中的 HomoAND、HomoNAND、HomoXOR、HomoOR 运算各 50 次, 最后调用 UDec 函数解密. 统计每个门操作的平均耗时 (以秒为单位, 不含加解密时间), 结果如表 2 所示. 可以发现, 随着 n、q 的增长, 同态门的计算时间也不断增长, 而且 q 相等的情况下, n 对各个同态门的计算效率影响很大. 但 n 相等时, 改变 q 对效率的影响不大.

综合上述所有实验数据, 在参数 n、q 取值较大时, 加密和同态操作的耗时较大. 因此, 本方案在算法的效率方面, 仍有较大的提升空间. 具体来说, 可以从如下几个方面进行:

(1) 采用快速傅里叶变换技术, 可以大大提升同态乘法的效率;

(2) 采用 SIMD 技术, 修改 VGSW 方案为每次加密一组明文, 甚至一个明文矩阵, 实现信息打包处理来提升效率;

(3) 采用硬件加速技术, 将耗时较大的矩阵运算部分定制成专用硬件设备, 进一步加速运算.

表 2 同态门操作实验结果

Table 2 Result of homomorphic gate operation test

n	q	HomoOR	HomoAND	HomoXOR	HomoNAND
16	2310	< 0.001	0.066	0.138	0.067
16	223092870	<0.001	0.069	0.141	0.070
32	30030	< 0.001	0.561	1.170	0.563
64	510510	< 0.001	3.718	7.657	3.765
128	9699690	< 0.001	31.967	64.862	32.603
256	223092870	< 0.001	314.553	640.438	327.254

6 结束语

本文提出了一种改进的 GSW 同态加密变体方案——VGSW 方案. 该改进方案结合本文提出的维度模数规约方法, 并使用文献 [12] 的快速 bootstrapping 技术, 可以直接转变成全同态加密方案. 与文献 [10] 中的 GSW 方案相比, 本文提出的 VGSW 方案与文献 [12] 的密文结构类似, 从而与其设计的快速 bootstrapping 兼容性更好. 与文献 [12] 中提出的变体 GSW 方案的不同之处在于, 本文在提出 VGSW 方案的基础上, 设计了相应的维度模数规约方法, 形成了一个完整的同态加密方案. 而文献 [12] 的变体 GSW 方案侧重于实现快速 bootstrapping 技术, 本质上并不是一个同态加密方案. 本文用软件实现了 VGSW 同态加密方案, 为同态加密技术的进一步应用做出了铺垫. 不过, VGSW 方案仍有较大的效率提升空间, 可以从算法理论、软件实现和硬件设计三方面来提升计算效率.

References

[1] RIVEST R, ADLEMAN L, DERTOUZOS M L. On data banks and privacy homomorphisms[J]. Foundations of Secure Computation, 1978, 4(11): 169–180.

[2] RIVEST R, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120–126.

[3] GOLDWASSER S, MICALI S. Probabilistic encryption[J]. Journal of Computer and System Sciences, 1984, 28(2): 270–299.

[4] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]. In: Advances in Cryptology—EUROCRYPT 1999. Springer Berlin Heidelberg, 1999: 223–238.

[5] DAMGÅRD I, JURIK M. A generalisation, a simplication and some applications of paillier's probabilistic public-key system [C]. In: Public Key Cryptography. Springer Berlin Heidelberg, 2001: 119–136.

[6] BONEH D, GOH E J, NISSIM K. Evaluating 2-DNF formulas on ciphertexts[C]. In: Theory of Cryptography. Springer Berlin Heidelberg, 2005: 325–341.

[7] GENTRY C. A fully homomorphic encryption schem [D]. Stanford University, 2009.

[8] BRAKERSKI Z, VAIKUNTANATHAN V. Efficient fully homomorphic encryption from (standard) LWE[C]. In: Proceedings of IEEE 52nd Annual Symposium on Foundations of Computer Science(FOCS2011). Springer Berlin Heidelberg, 2011: 97–106.

[9] REGEV O. On lattices, learning with errors, random linear codes, and cryptography[C]. In: ACM Symposium on Theory of Computing. Springer Berlin Heidelberg, 2005: 84–93.

[10] GENTRY C, SAHAI A, WATERS B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based[C]. In: Advances in Cryptology—CRYPTO 2013, Springer Berlin Heidelberg, 2013: 75–92.

[11] BRAKERSKI Z, VAIKUNTANATHAN V. Lattice-Based FHE as Secure as PKE[C]. In: International Conference on Information Technology and Computer Science. Springer Berlin Heidelberg, 2014: 1–21

[12] ALPERIN-SHERIFF J, PEIKERT C. Faster bootstrapping with polynomial error[C]. In: Advances in Cryptology—CRYPTO 2014. Springer Berlin Heidelberg, 2014: 297–314.

[13] HALEVI S, SHOUP V. Bootstrapping for HElib[C]. In: Advances in Cryptology—EUROCRYPT 2015. Springer Berlin Heidelberg, 2015: 641–670.

[14] HALEVI S, SHOUP V. Algorithms in HElib[C]. In: Advances in Cryptology—CRYPTO 2014, Springer Berlin Heidelberg, 2014: 554–571.
[15] ALPERINSHERIFF J. Towards practical fully homomorphic encryption[D]. Georgia Institute of Technology, 2015.
[16] HIROMASA R, ABE M, OKAMOTO T. Packing messages and optimizing bootstrapping in GSW-FHE[J]. Ieice Transactions on Fundamentals of Electronics Communications & Computer Sciences, 2016, E99.A(1): 73–82.
[17] DUCAS L, MICCIANCIO D. FHEW: bootstrapping homomorphic encryption in less than a second[C]. In: Advances in Cryptology—EUROCRYPT 2015. Springer Berlin Heidelberg, 2015: 617–640.
[18] BIASSE J F, RUIZ L. FHEW with efficient multibit bootstrapping[C]. In: Progress in Cryptology—LATINCRYPT 2015. Springer International Publishing, 2015.
[19] LYUBASHEVSKY V, PEIKERT C, REGEV O. A toolkit for ring-lwe cryptography[C]. In: Advances in Cryptology—EUROCRYPT 2013. Springer Berlin Heidelberg, 2013: 35–54.
[20] GOLDREICH O. Foundations of Cryptography[M]. Publishing House of Electronics Industry, 2005.
[21] MICCIANCIO D, PEIKERT C. Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller[C]. In: Advances in Cryptology—EUROCRYPT 2012. Springer Berlin Heidelberg, 2011:700–718.
[22] HASTAD J, IMPAGLIAZZO R, LEVIN LA, et al. A pseudorandom generator from any one-way function[J]. SIAM Journal on Computing, 1999, 28(4): 1364–1396.

作者信息

姬晨 (1991-), 陕西宝鸡人, 硕士生, 主要研究领域为抗量子密码.
E-mail:jichen@cqu.edu.cn

蔡斌 (1979-), 山西朔州人, 博士. 主要研究领域为信息安全、智能计算等.
E-mail:caibin@cqu.edu.cn

向宏 (1964-), 四川成都人, 博士, 教授. 主要研究领域为密码学、网络攻防模型、信息安全工程标准、软件安全及安全软件等.
E-mail:
xianghong@cqu.edu.cn

丁津泰 (1966-), 江苏人, 博士, 教授. 主要研究领域为密码学、后量子密码学、多变量公钥密码学等.
E-mail:jtding@cqu.edu.cn

桑军 (1968-), 重庆人, 博士, 教授. 主要研究领域为信息安全、信息隐藏与数字水印、数字图像处理及软件工程等.
E-mail:jsang@cqu.edu.cn