文章编号:1671-4229(2022)04-0001-11

不可区分混淆的回顾与展望

郁 昱[1,2], 姚 立[1]
(1. 上海交通大学 计算机科学与工程系, 上海 200240; 2. 上海期智研究院,上海 200232)

摘 要: 不可区分混淆是密码学中一个功能非常强大的原语,它可以实现在一个可运行的程序中隐藏某些信息。尽管研究者们在过去十年间已经展示了如何在不可区分混淆的基础上实现各种密码学应用,然而距离基于标准假设的高效不可区分混淆方案仍有很长一段路要走。事实上,已经有很多工作提出了多种不可区分混淆的候选方案或是对这些方案进行了密码分析。不可区分混淆相关技术的发展大致经历了以下4个阶段:最初,需要假设多项式阶多线性映射,这是一类非标准的假设;接着,试图降低多线性映射的阶数使之接近并达到标准假设的要求;如今,正试图构造后量子安全的不可区分混淆;未来,将会在效率上改进不可区分混淆,使之能够被应用在一般化的场景中。

关键词: 不可区分混淆; 多线性映射; 后量子安全
中图分类号: TP 301.6 **文献标志码**: A

Indistinguishability obfuscation: Retrospect and prospect

YU Yu[1,2], *YAO Li*[1]
(1. Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China;
2. Shanghai Qi Zhi Institute, Shanghai 200232, China)

Abstract: Indistinguishability Obfuscation (iO) is an extremely powerful primitive which allows a runnable program to hide some information. Although researchers have shown how to base cryptographic applications on iO over the last decade, we are still far away from the goal of basing efficient iO on standard assumptions. In fact, many works have proposed various candidates or made cryptanalysis on these candidates. The state of art of iO has experienced roughly the following four stages: At the beginning, we need to assume multi-linear map with polynomial degree, a non-standard assumption. Then we try to decrease the degree to more closely to and finally fit the standard assumption. Now, we are trying to construct post-quantum secure iO. In the future, we will improve the efficiency of iO so that it can be applied in general scenarios.

Key words: indistinguishability obfuscation; multi-linear map; post-quantum secure

1 程序混淆

一个程序代码中有代码的框架结构、组件间的调用关系和算法思想等信息,有时还包含一些硬编码的字符,这些硬编码的字符或算法都可以被看作程序中隐藏的一些秘密信息。显然,软件行业往往并不希望软件中的算法随着软件的售卖而被泄露,也不希望软件被任意修改(例如运用反编译等手段对付费软件进行破解)。程序混淆便可用于解决这一问题(也许有人声称一份写得极为糟糕的代码也能达到类似的效果,但这种做法的有效性无法被严格证明,同时也会增加软件产生bug的风险)。

程序混淆(program obfuscation)保证了程序中确实能够隐藏某些秘密信息,即使是拥有这个程序并且能够

收稿日期: 2022-09-30; **修回日期**: 2022-11-07
作者简介: 郁昱(1981—),男,教授. E-mail:yyuu@sjtu.edu.cn
引文格式: 郁昱, 姚立. 不可区分混淆的回顾与展望[J]. 广州大学学报(自然科学版),2022,21(4):1-11.

任意运行这个程序的人也无法得知这些秘密信息。

1.1 正确性

实现程序混淆需要有程序混淆器(program obfuscator)。程序混淆器(记为 Obf)可以被视为一个特殊的编译器,这个编译器的输入(例如一段代码)对应于某个程序,将输入对应的这个程序记为 P,编译器将 P 编译后会输出一个混淆后的程序,记为 $\hat{P}$。那么要求:

(1)这2个程序的功能完全一致;

(2)从实用性的角度出发,Obf 和 $\hat{P}$ 都应当是高效的。

1.2 安全性

人们希望 $\hat{P}$ 尽可能地隐藏 P 中包含的秘密信息。密码学常见的安全性刻画方式有2类:基于模拟的(SIM-based)和基于不可区分的(IND-based),前者称为虚拟黑盒混淆(Virtual Black Box Obfuscation, VBBO),后者称为不可区分混淆(Indistinguishability Obfuscation, iO)。

1.2.1 虚拟黑盒混淆

虚拟黑盒混淆指对于一个得到了 $\hat{P}$ 的学习者和一个只能对 P 进行黑盒访问的模拟器,二者的能力是完全一致的。换言之,得到 $\hat{P}$ 并没有给学习者带来任何通过黑盒调用无法得到的信息(即使学习者可以研究 $\hat{P}$ 的运算步骤,查看计算过程中某些变量值的变化,设置断点,甚至在运算进行过程中直接修改某些寄存器的值,并观察产生的影响……)。虽然这个安全性定义非常强,但是事实上它是无法达成的。比如至少有一项能力是学习者有而模拟器没有的,那就是学习者可以输出一个和 P 功能一致的程序(这个程序就是 $\hat{P}$),而模拟器仅靠对 P 进行的多项式次黑盒访问根本不可能写出一份和 P 功能一致的代码。在2001年,Barak 等[1]最早注意到这一点并证明了不存在通用的虚拟黑盒混淆(VBBO 和 iO 的定义也是由他们在同一篇文章中提出的)。

1.2.2 不可区分混淆

不可区分混淆指对于2个功能完全一致的程序 P_1 和 P_2,任何区分器都无法区分 $\hat{P}_1$ 和 $\hat{P}_2$。这个安全性的定义直觉上并没有特别强(事实上即使 P = NP,iO 仍然能够存在,但这种情形下 iO 几乎隐藏不了什么信息),2007年,Goldwasser 等[2]证明了 iO 是有可能被实现的最好的混淆器。为了简述其思想,假设 VBBO 是可能存在的,并证明此时 iO 至少和 VBBO 一样安全。对于程序 P 和 $VBBO(P)$,显然这二者功能一样,于是,根据 iO 的定义,任何多项式的敌手都无法区分 $iO(P)$ 和 $iO(VBBO(P))$。$VBBO(P)$ 已经实现了虚拟黑盒安全,对其应用任何算法(包括 iO)都无法打破虚拟黑盒混淆的安全性,因此,$iO(VBBO(P))$ 也实现了虚拟黑盒混淆安全;同时,$iO(P)$ 与 $O(VBBO(P))$ 不可区分,因此,$iO(P)$ 自然也符合虚拟黑盒混淆的安全性定义。

1.3 应用

由于通用 VBBO 的不可实现以及 iO 具有很强的安全性,目前,已有大量根据 iO 来构造密码学组件的研究成果,其中最早的是 Sahai 等[3]在2014年通过 iO 和一些基础的密码学假设(例如单向函数(one-way function))构造了公钥加密(public-key encryption)、数字签名(digital signature)和可否认加密(deniable encryption)等组件。

综合这些研究成果可以看到,iO 不仅能用于构造已经熟知的经典密码学组件,更可以作为桥梁构造大量功能十分强大的"新"密码学组件(其中一部分组件目前只能基于 iO 构造)。

1.4 构造

尽管在如何应用 iO 方面已经有了很多可喜的研究成果,但至今仍无法构造出安全且高效的 iO。这并不意味着研究者止步不前,事实上,自2013年 Garg 等[4]提出第一个 iO 的候选方案以来,iO 的构造方案已经经历了多次演进。本文将这些年来 iO 构造的发展历程大致分为4个阶段,并选取有代表性以及突破性的工作逐一进行介绍。

2 第一代 iO:基于多项式阶多线性映射

自2013年起,有一系列工作基于多线性映射构造 iO。相比于接下来的几代 iO 构造,第一代 iO 的构造非常直接高效,且易于理解。但由于多线性映射候选方案在安全性方面的缺失,从第一个 iO 候选方案[4]被提出算起,这些方案已经经历了多轮攻击与修补[5-10]。时至今日,针对第一个 iO 候选方案的某些变体方案仍然没有提出有效的攻击,与此同时,也没有人能够用数学工具来证明这些变体的安全性,除非借助于一些非常强的理想化模型。

2.1 多线性映射

代数群是密码学中常用的经典结构,RSA 公钥加密及 DH 密钥交换等算法都运用了代数群以及群相关的困难假设。由于离散对数假设的存在,可以粗略地将 g^a 视为 a 在群 G 上的编码,而代数群的一个特点便是加法同态性,即 $g^a \cdot g^b = g^{a+b}$,这也意味着可以利用代数群的结构安全地进行加法计算。由于环上的任意计算都可以分解为加法和乘法,因此,如果能够进一步找到一类特殊的环,使得乘法同态也一并满足,那么这一代数结构将在密码学中具有极其广泛的应用。

在研究中,人们逐渐发现,在同一个环上实现加法和乘法同态是十分困难的,因此,线性映射的概念出现了。以 Miller[11] 提出的双线性映射为例,对于一个属于群 G_1 的元素 g_1^a,一个属于群 G_2 的元素 g_2^b 和一个群 G_T,存在一个特殊的映射 $G_1 \times G_2 \to G_T$,当输入 g_1^a 和 g_2^b,输出群 G_T 上的元素 g_T^{ab}(G_1 和 G_2 可以是同一个群)。也就是说,双线性映射允许安全地计算一次乘法,但是乘法计算的结果被编码到了另一个群上。

虽然 Miller 的这篇文章被计算机理论科学的顶级会议 STOC 以没有应用为由拒稿,此后一直未公开发表,但是在 20 年后,基于双线性映射的基于身份加密(Identity Based Encryption, IBE)、基于属性加密(Attribute Based Encryption, ABE)和 BLS 短签名(BLS short signature)等密码学原语相继发表,证明了双线性映射在密码学领域有着广泛的应用场景。

类似的,可以定义 k 阶多线性映射 $G_1 \times G_2 \times \cdots \times G_k \to G_T$($G_1, G_2 \cdots G_k$ 可以是同一个群)。然而,当试图将双线性映射的构造推广到三阶时,得到的映射将不再是多项式时间可计算的[12]。这也说明,构造多线性映射需要新的技术和方法。

2013 年,Garg 等[13] 提出了第一个多线性映射的备选方案,此后陆续有其他候选方案[14-15] 被提出。这些多线性映射的备选方案有着一些共同特点:

(1)带噪声编码:同一个元素在同一个群上的编码很可能不相同,它们之间会相差一个较小的噪声。

(2)零元素测试:由于同一个元素的编码往往不同,当它们相减时,会得到某一个而非唯一的零元素编码。因此,需要零元素测试算法来判断编码是否是零元素编码。

(3)分级编码:并非是将 k 个元素一次性映射到 G_T,而是所有初始元素都位于 1 级,一个 m 级的 a 的编码 g_m^a 和一个 n 级的 b 的编码 g_n^b 可以被映射为 $m+n$ 级的 ab 的编码 g_{m+n}^{ab},零元素测试只能用于测试 k 级的元素是否为 0。

(4)无法维持经典假设:在这些多线性映射群上,经典的假设(双线性映射群上常见假设的推广),例如判定性线性(Decisional Linear, DLIN)假设等均不成立。

2.2　用于对数深度电路的 iO

有了多线性映射,便可以着手进行 iO 的构造了。下面介绍最经典的构造,同时也是第一个 iO 候选方案[4]。这一方案首先构造了只能用于对数深度电路的 iO,之后利用自举技术将其适用性拓展为所有多项式大小的电路。尽管这一方案在理想的多线性映射代数系统中是可证明安全的,由于目前已有的多线性映射候选方案均无法维持经典假设,因此,这一类方案整体的安全性至今无法在标准模型中得到证明。

2.2.1　分支程序

早在 1986 年,Barrington[16] 就证明了任意一个 NC^1 的电路可以被表示为宽度为 5 的多项式大小的分支程序。这意味着一个 NC^1 电路的计算可以被表示为多项式个五维矩阵的乘积,其中的每个矩阵都是从一对矩阵中依据某个输入位的值选取的。例如对于一对矩阵 $(\boldsymbol{A}_1, \boldsymbol{A}_2)$,其关联的输入位为 x_i,那么有一种可能的情况:如果 x_i 为 0,就选取 $\boldsymbol{A}_2$,否则,选取 $\boldsymbol{A}_1$。需要注意的是,一个输入位可能会多次决定矩阵的选取。

2.2.2　类拼图游戏

多线性映射允许计算多项式个矩阵的乘积,但是却无法保证攻击者能够诚实地选取这些矩阵并诚实地进行运算。例如如果 x_i 为 0,应选取 $\boldsymbol{A}_2$ 和 $\boldsymbol{B}_1$ 参与运算,反之选取 $\boldsymbol{A}_1$ 和 $\boldsymbol{B}_2$ 参与运算,而敌手可能会选取 $\boldsymbol{A}_1$ 和 $\boldsymbol{B}_1$ 参与运算,这无疑会得到除电路正常输出以外的信息,从而利用这一信息打破 iO(iO 的安全定义中要求 2 个程序的功能完全一样,这也意味着往往只有正常的电路输出才能保证不会泄露信息)。再比如,程序正常计算时,应该是 $\boldsymbol{C}_1/\boldsymbol{C}_2$ 乘以 $\boldsymbol{D}_1/\boldsymbol{D}_2$,而敌手可能会计算 $\boldsymbol{D}_1$ 乘以 $\boldsymbol{C}_1$,从而得到额外的信息(矩阵乘法不满足交换律)。因此,仿照拼图游戏去设计一些算法来避免这一点,例如针对第一种情况,可以把 $\boldsymbol{A}_2$ 和 $\boldsymbol{B}_1$ 设计为一块拼图,只能同时选或同时不选;针对第二种情况,可以让 $\boldsymbol{C}_1/\boldsymbol{C}_2$ 这 2 块拼图右侧的锯齿和 $\boldsymbol{D}_1/\boldsymbol{D}_2$ 这 2 块拼图左侧的锯齿相吻合,这样只有将 $\boldsymbol{C}_1/\boldsymbol{C}_2$ 放在 $\boldsymbol{D}_1/\boldsymbol{D}_2$ 左侧才能使得拼图呈现吻合的状态。在密码学中,这类操作通常通过添加噪声来实现,当程序按照预定的方式计算时,这些噪声的乘积刚好会相互抵消,得到正确的计算结果;总之,这些噪声糅合在一起,将原本会被泄露的额外信息掩盖起来。同时,也需要给这些拼图添加一些随机性,例如当 $\boldsymbol{C}_1$ 和 $\boldsymbol{C}_2$ 完全一样时,它们的锯齿也会完全一样,那么此时会出现 2 块完全一样的拼图。而对于另一个功能一样的分支程序,可能不存在 2 块完全一样的拼图,这样敌手就可以轻易地区分这 2 个程序。所以,需要给拼图注入随机性,使得出现 2 块完全相同拼图的概率是可忽略的。

2.3　自举

自举(bootstrapping)技术最早出现在全同态加密(Fully Homomorphic Encryption, FHE)中,其核心思想是,当需要实现一个强大的功能时,也许只需要实现一个弱的版本,并利用这个弱的版本来构造出那个强大的功能。一个形象的例子是,当组装一个机器人时,只需

组装出机器人的手,接下来便可以让机器人的手去组装机器人剩余的部分。为了实现 iO 的自举,还需要用到全同态加密和通用电路。

相比于通常的加密,全同态加密允许在不知道明文的情况下直接对密文进行操作。同时,全同态加密的解密函数较为简单,可以用一个 NC^1 的电路表示。

通用电路(Universal Circuit,UC)可以用来模拟任意电路的计算过程,它将电路 C 的描述和电路 C 的输入作为输入,并得到电路 C 的输出。通用电路也可以交换电路 C 和电路 C 的输入立场,通过将电路 C 的输入硬编码在通用电路里,使 $UC(\cdot,x)$ 成为电路,而电路 C 的输入成为该电路的输入。

为了构造 iO,可以将电路用全同态加密进行加密,得到 $\hat{C}$,对于某个输入 x,将其转化为电路 $UC(\cdot,x)$,将 $\hat{C}$ 作为该电路的输入进行同态计算,得到 $C(x)$ 的加密 $\widehat{C(x)}$。此时,只需要 $iO(Dec_{sk}(\cdot))$ 便可解密 $\widehat{C(x)}$ 并得到电路的输出。密钥 sk 是敏感信息,需要将包含这一信息的解密电路进行混淆,同时还需要利用一个低深度证明系统,解密电路的输入还需要包含一个证明,以证明 $\widehat{C(x)}$ 是 $C(x)$ 的加密,其中,$C(x)$ 是电路 C 在输入 x 上对应的输出。如果没有这一限制,敌手可以直接利用解密电路解密 $\hat{C}$。

也就是说,要构造适用于所有多项式大小电路的 iO,构造一个适用于 NC^1 电路的 iO 就足够了。NC^1 的电路可以表示为多项式个矩阵的乘积,多项式个矩阵的乘积需要多项式次乘法运算,因此,可以通过多项式阶的多线性映射来完成这一任务。

3 第二代 iO:基于常数(≥3)阶多线性映射

目前,密码学标准假设中只有双线性映射,因此,自 2015 年起,有一系列工作[17-24]试图将 iO 规约到(相较于 iO)稍弱的密码学组件中,从而最终只需要依赖三阶多线性映射,这与双线性映射已经十分接近了。

3.1 规约到亚线性简明随机化编码

随机化编码(Randomized Encoding, RE)可以用来保护一次计算,例如混淆电路(Garble Circuit, GC)就可以视为 RE,它包含有 2 个算法:

(1)$\mathrm{Encode}(C,x)\to\widehat{C_x}$:将电路 C 在输入 x 上的计算编码为 $\widehat{C_x}$;

(2)$\mathrm{Decode}(\widehat{C_x})\to C(x)$:依据 $\widehat{C_x}$ 计算得到 $C(x)$。

在安全性方面,要求 $\widehat{C_x}$ 不会泄露除 $C(x)$ 以外的任何信息。在效率方面,RE 的效率取决于其 Encode 算法的效率,而 Encode 算法的效率通常与电路 C 的大小(记为 s)挂钩,例如 GC 的 Encode 算法的时间复杂度关于 s 呈线性增长。如果算法的时间复杂度关于 s 呈亚线性增长,则称 RE 满足亚线性简明(sublinear compactness);如果算法的输出长度关于 s 呈亚线性增长(时间复杂度关于 s 仍可能是呈线性增长),则称 RE 满足弱亚线性简明(weakly sublinear compactness);如果算法的时间复杂度与 s 无关,而是关于电路的输出长度呈线性增长,则称 RE 满足紧凑性(succinctness)。这一定义同样适用于函数加密(Functional Encryption, FE)及其加密算法。

函数加密是一类特殊的加密方式,不同于传统加密要么持有密钥得到全部的秘密,要么没有密钥从而对秘密一无所知的加密模式,FE 存在有一个主密钥 msk,通过主密钥可以派生与某个函数 f 相关的密钥 sk_f,通过用该密钥对消息 m 的加密进行解密,可以得到 $f(m)$。公钥 FE(也可称作非对称 FE 或 PKFE)包含 4 个算法:

(1)$\mathrm{Setup}(1^\lambda)\to(pk,msk)$:生成公钥和主密钥;

(2)$\mathrm{Enc}(pk,x)\to\hat{x}$:对 x 进行加密得到密文 $\hat{x}$;

(3)$\mathrm{KeyGen}(msk,C)\to sk_C$:生成与电路 C 对应的解密密钥 sk_C;

(4)$\mathrm{Dec}(sk_C,\hat{x})\to C(x)$:用密钥 sk_C 对密文 $\hat{x}$ 进行解密得到 $C(x)$。

私钥 FE(也可称作对称 FE 或 SKFE)只需要将 pk 替换为 msk,如果 FE 只支持执行一次 KeyGen 算法,则称该 FE 是 1-key FE;如果支持执行任意次 KeyGen 算法,则称其为抗合谋(collusion-resistance) FE。如非特殊说明,FE 指 PKFE。

在安全性方面,要求 sk_C 和 $\hat{x}$ 不会泄露除 $C(x)$ 以外的任何信息。FE 和 RE 有着紧密的联系,记 $(\widehat{C},x)$ 是 (C,x) 的加密,密钥 sk_{UC} 对应于一个通用电路,使得 $UC(C,x)=C(x)$。将 sk_{UC} 作为公共引用串(Common Reference String, CRS)公开(这是一种只需生成一次便可以重复使用的字符串)。此时 $(\widehat{C},x)$ 就是 $\widehat{C_x}$,由于只需要生成一次密钥 sk_{UC},因此,1-key FE 可以蕴含 RE,且二者的效率相同(因为 $|(C,x)|<2s$)。

RE 可以保护电路在一个输入上的计算,而 iO 需要保护电路在 2^n 个输入(n 是电路输入的长度)上的计算。因此我们想到了使用 GGM 树,它最早被用于将在一个种子上输出一个随机数的伪随机数发生器(Pseudorandom Generator, PRG)转化为在一个密钥上输出 2^n 个随机数的伪随机函数(Pseudorandom Function, PRF),这与我们的目的十分类似。以一个 3 比特输入的电路为例,演示计算电路在 010 上的输出的过程。这棵树每个

节点都是一个 RE,根节点的 RE 记为$\widehat{C_{xxx}}$,通过对其 Decode 可以得到$\widehat{C_{0xx}}$和$\widehat{C_{1xx}}$,然后继续 Decode $\widehat{C_{0xx}}$,得到$\widehat{C_{00x}}$和$\widehat{C_{01x}}$,接着 Decode $\widehat{C_{01x}}$,得到$\widehat{C_{010}}$和$\widehat{C_{011}}$,而$\widehat{C_{010}}$ Decode 的结果就是 $C(010)$。由 RE 的安全性可知,最底层的 RE 只包含了电路在相应输入上的输出信息,因此,通过逐层规约,可知根节点也只包含了电路在任意输入上的输出信息。而这个根节点的 RE 就是这个程序的混淆,即 $iO(C)$。

那么通过 GC,就可以实现 iO 了吗? 答案是否定的,这是因为 GC 的 Encode 算法的时间复杂度是 $ploy(\lambda)\cdot s$,将这一算法用电路表示,电路大小也是 $ploy(\lambda)\cdot s$,而 GGM 树的倒数第二层需要输出 2 个上述的 RE,因此,耗时至少是 $ploy(\lambda)^2\cdot s$,以此类推,每一层电路的大小都会增大 $ploy(\lambda)$倍,根节点计算 RE 的耗时是 $ploy(\lambda)^n\cdot s$。如果给定电路 C,计算根节点的 RE 并输出需要耗费指数大小的时间,则需要一个高效的 RE。自 2015 年起的一些工作[17-19]证明了,当 RE 满足亚线性简明时,这一构造才是可用的。

3.2　规约到弱亚线性简明随机化编码

由于构造亚线性简明随机化编码过于困难,研究者们把目光暂时转向了当时已有的最高效的 FE/RE,即 Goldwasser 等[25]提出的 succinct 1-key FE,该构造基于带噪声学习(Learning with Errors, LWE)假设,试图通过利用这一构造进一步将 iO 规约到更弱的密码学原语上。

该构造与第一代 iO 的构造有相似之处,它将消息 x 利用全同态加密得到 $\hat{x}$,之后在解密阶段对其进行同态计算得到$\widehat{C(x)}$,并利用 FHE 解密电路对这一密文进行解密得到 $C(x)$。由于这是一个 1-key FE,因此每个密文只会被唯一一个密钥进行解密(至多进行一次计算),从而不再需要利用 iO 混淆解密电路,只需要利用 GC。把 FHE 解密电路的 GC 放在密文中,由于解密电路只与其要解密的密文大小有关,即与$\widehat{C(x)}$有关,而与电路 C 无关,从而满足紧凑性。由于 GC 的输入不再是$\widehat{C(x)}$,而是$\widehat{C(x)}$对应的标签,则需要同时将 $2|\widehat{C(x)}|$个标签封装在密文里,当$\widehat{C(x)}$的比特等于 0 或 1 时,允许解密相对应的那个标签。这一特性与 ABE 的性质完全一致,ABE 加密时会将消息 m 与属性 x 进行绑定,解密密钥会与某个政策(policy) f 进行绑定,只有当$f(x)=1$ 时才能解密成功。而将标签作为消息,$\hat{x}$ 作为属性,$f(\hat{x})=1$ 当且仅当 $\hat{x}$ 经过同态计算后,$\widehat{C(x)}$的某个比特与标签相对应。但是 ABE 只能保护消息,无法保护属性,$\hat{x}$ 作为属性的同时本身已经是 FHE 的密文,恰好不需要保护。这样,就得到了一个 succinct 1-key FE,FE 加密时会输出 $2|\widehat{C(x)}|$个 ABE 的密文和一个 FHE 解密电路的 GC,它们的大小只和$|\widehat{C(x)}|$有关。FE 生成密钥时会产生 $2|\widehat{C(x)}|$个 ABE 的密钥,在解密阶段,这些密钥可以解密一半的密文,得到与$\widehat{C(x)}$对应的标签,并通过 GC 计算得到 $C(x)$。需要注意的是,由于 ABE 和 FHE 都是分层的(leveled),它们虽不关注电路 C 的大小却关心电路 C 的深度,因此,为了使这个 FE 与电路 C 的深度 d 无关,可以假定电路 C 是一个 NC^1 的电路。在后文将会介绍 FE 的自举算法,通过自举,一个能够用于 NC^0 电路的 FE 将可以用于任意多项式大小的电路。

现在已经有了 succinct RE,如果将其与 weakly sublinear compact RE 组合起来,会发生什么呢? 用 weakly sublinear compact RE 计算$\widehat{C_x}$时,可以将这个计算过程看作是一个输入为 x 的电路 C',由 weakly sublinear compactness 可得,电路 C'的输出长度是关于 s 的亚线性级;接着用 succinct RE 计算 $C'(x)$的 RE,由 succinctness 可得,其计算时间是关于 C'的输出长度的线性级,即关于 s 的亚线性级。Decode 时,先 Decode 得到$C'(x)=\widehat{C_x}$,再 Decode $\widehat{C_x}$得到 $C(x)$。至此将 iO 规约到了 LWE + weakly sublinear compact RE。

3.3　规约到指数 iO

指数 iO (Exponential iO, XiO)进一步放宽了 iO 的要求,$iO(C)$的输出长度应该是 $poly(\lambda,|C|)$,而 XiO 则允许输出长度达到 $poly(\lambda,|C|)\cdot 2^{n(1-\epsilon)}$,一个电路的真值表可以看作一个平凡的混淆,其输出长度至多为 $|C|\cdot 2^n$,因此,XiO 仅仅要求我们能够做得比直接输出真值表好一点。同时注意到,这一定义并没有对 XiO 的运行时间做任何规定,也就是说 XiO 运行的时间可以达到指数大小,这也是它被命名为指数 iO 的原因。2016 年,Lin 等[20]将 iO 规约到了 LWE + XiO,这是一个比较反直觉的结论,只要能够对将混淆程序的大小压缩为亚指数,就能够将其压缩为多项式。这一规约的过程便是通过 succinct 1-key FE 和 XiO 构造 weakly sublinear compact 1-key FE。

由于 succinctness 意味着 FE 的加密只和输出长度有关,与电路大小无关,因此,当计算 1 比特输出时,加密的复杂度将是 $poly(\lambda,|x|)$(因为密文需要包含消息 x 的信息,所以必定与消息长度和安全参数有关)。对于一个 n'比特输出的电路,可以用 n'个 succinct 1-key FE 的实例分别计算 $C(x)$的每个比特,即消息 x 分别用 n'个 FE 实例加密,同时这 n'个 FE 的实例各自生成一个密钥,对应于计算电路 C 各个输出位的电路。把这 n'个

FE 的加密过程封装进同一个电路 D,当输入 $i\in[n']$ 时,输出 x 被第 i 个 FE 的实例加密的密文。将 $XiO(D)$ 作为 weakly sublinear compact 1-key FE 加密算法的输出,把 n' 个 FE 实例各自生成的密钥作为密钥生成算法的输出。由于 D 的输入总共有 n' 个,且 n' 一定不大于电路大小 s,由 XiO 的定义,$XiO(D)$ 的输出长度为 $poly(\lambda,|D|)\cdot s^{1-\epsilon}$,由于电路 D 的功能是计算 x 经由某个 succinct 1-key FE 加密的密文,而 succinct 1-key FE 加密的复杂度将是 $poly(\lambda,|x|)$,因此,$XiO(D)$ 的输出长度为 $poly(\lambda,|x|)\cdot s^{1-\epsilon}$,从而满足 weakly sublinear compactness。

3.4 对指数 iO 作进一步规约

从 XiO 继续向下规约,有 2 条路线,分别基于函数编码(functional encoding)和弱亚线性简明单密钥对称函数加密(weakly sublinear compact 1-key SKFE)。

Functional encoding 可以视为 FE 的弱化,它包含 3 个算法:

(1) $\mathrm{Encode}(x;r)\to\hat{x}$: 随机算法,输入 x 并计算其编码 $\hat{x}$。

(2) $\mathrm{Opening}(C,x,r)\to h$: 确定性算法,除了电路 C,还会输入 x 和 r,其中,r 是 Encode 时用到的随机数,因此,该算法可以完全复现 Encode 的过程。输出一个解码提示 h_C。

(3) $\mathrm{Decode}(\hat{x},h)\to C(x)$: 输入编码 $\hat{x}$ 和解码提示 h_C,输出 $C(x)$。

在安全性方面,要求 h_C 和 $\hat{x}$ 不会泄露除 $C(x)$ 以外的任何信息;在简明性方面,要求 $h_C\ll C(x)$;在效率方面,要求 Encode 算法的输出长度与电路的输出长度呈线性相关。

可以将 FE 视为特殊的 functional encoding。与 FE 相比,functional encoding 弱在其提示 h_f 可能与 Encode 过程绑定,即其不能支持解码任意编码,而只能用于解码与其输入对应的 $\mathrm{Encode}(x;r)$。因此,与 1-key many-ciphertexts FE 对应的,functional encoding 类似于 1-ciphertext many-keys FE,也就是多个解码提示可对应于某一个编码。

假设有一个电路 D,它能输出电路完整的真值表:$D(C)=C(0)\|C(1)\|\cdots\|C(2^n-1)$,这个电路可以看作通用电路的变体,那么可以设 $XiO(C)=(\hat{C},h_D)$。根据 functional encoding 的定义,只能得到真值表的信息。

接下来还要考虑 XiO 压缩真值表的特性,这就要求 $|\hat{C}|$ 和 $|h_D|$ 较小。由简明性可知,$|h_D|$ 远小于 $|D(C)|$,但是 $|\hat{C}|$ 通常与 $|D(C)|$(真值表)线性相关,这样压缩真值表的要求就失败了。

为了解决这一问题,可以将真值表拆分成 2^{n_1} 份,每份包含 2^{n_2} 项,其中,$n_1+n_2=n$。那么,总共需要一个 $\hat{C}$ 和 2^{n_1} 个解密提示,分别解密每一份子真值表。因此,提示的数量是与 2^{n_1} 线性相关,而 $|\hat{C}|$ 与电路的输出,即子真值表的大小 2^{n_2} 线性相关,由于这两者都小于 2^n,因此,$XiO(C)=(\hat{C},h_{D_1},h_{D_2},\cdots,h_{D_{2^{n_1}}})$ 关于 2^n 亚线性相关,即实现了压缩真值表的要求。

类似的,真值表拆分也可以将 XiO 规约到 weakly sublinear compact 1-key SKFE。假设电路 D 在一个 n_1 比特的输入 x 上输出以 x 为前缀的 2^{n_2} 项个真值表项,那么 $XiO(C)=(\widehat{x_1},\widehat{x_2},\cdots,\widehat{x_{2^{n_1}}},sk_D)$,由于 D 的功能是输出 2^{n_2} 项个真值表项,其大小与 2^{n_2} 线性相关,则 $|sk_D|$ 也与 2^{n_2} 线性相关,weakly sublinear compactness,$|\widehat{x_i}|$ 则与 2^{n_2} 亚线性相关,这样的密文总共 2^{n_1} 个,$n_1+(1-\epsilon)n_2=(1-\epsilon')n<n$,其中,$\epsilon'<\epsilon$,由此实现了压缩真值表的要求。

3.5 FE 中的自举技术

因为 1-key FE 只需要支持生成一次密钥,所以可以将保护一次计算的 RE 与之结合,即当想要计算电路 C 在输入 x 上的输出 $C(x)$ 时,只需要计算 $\widehat{C_x}$,即计算 $RE.Encode(C,x)$。可以看到,$RE.Encode(C,\cdot)$ 也是一个以 x 为输入的电路,如果 $RE.Encode(C,\cdot)$ 总是可以表示为一个 NC^0 的电路,且电路的大小是 $poly(\lambda)\cdot|C|$,此时仅支持 NC^0 电路的 1-key FE 实际上可以用于任意多项式大小的电路,且 FE 的效率保持不变。下面介绍 2 个经典的 RE,分别是混淆电路和 AIK RE:

(1)混淆电路可以对电路的每个门分别生成真值表的混淆,生成混淆电路的过程可以用一个 NC^0 电路表示,且这个电路可以表示为 $|C|$ 个子电路,每个子电路用于混淆一个门,而混淆一个门的复杂度是与电路 C 无关的,这一特性被称为可分解的(decomposable)。最初的这类自举方案中需要使用 PRF(NC^0 上不存在),研究者们只将支持多项式大小电路的 FE 规约到支持 NC^1 电路的 FE[26],后来才注意到能用 PRG 代替 PRF[27]。

(2)AIK RE 是一个作用于分支程序的 RE[28],只能支持将 NC^1 上的电路进行编码,生成 AIK RE 的过程同样可以用一个 NC^0 的电路表示。不仅如此,AIK RE 的每个输出比特至多只和输入 x 的某一个比特及用到的随机串 r 的某 3 个比特有关。

与此同时,Lin[23] 基于常数阶多线性映射的 SXDH 假设构造出了支持 NC^0 电路的 SKFE,由于 NC^0 电路的每个输出最多与 c 个输入相关(c 是常数),因此至多需要进行 c 次乘法计算,才可以利用 c 阶多线性映射。不仅如此,构造得到的 FE 还满足线性效率,即加密的时间

复杂度随消息的长度$|x|$呈线性增长。这样,只需要用这一 SKFE 去加密 RE 的输入,似乎就可以构造得到用于任意多项式大小电路的 SKFE。但是,RE 的输入除了消息 x,还需要使用随机串,随机串的大小与电路大小$|C|$是线性关系,无法实现 sublinear compactness。为此,可以将加密的内容由随机串换成 PRG 的种子,并用 PRG 生成的伪随机串来代替随机串。为了实现 sublinear compactness,要求 PRG 的种子长度是输出长度的亚线性,即 PRG 的拉伸度(stretch)是 $n^{1+\epsilon}$。目前,NC^0 上具有超线性 stretch 的 PRG 只有 Goldreich[29] 提出的候选方案,而无法规约到现有的其他标准假设,因此,iO 的构造中将 NC^0 上存在具有超线性 stretch 的 PRG 作为一个假设提出。需要注意的是,目前已经证明了 NC^0 上存在具有超线性 stretch 的 PRG 的 locality 必须大于等于 5[30]。由于 PRG 的种子被 FE 加密在密文里,而 PRG 的种子被使用 2 次以上会影响安全性,虽然 Lin[23] 构造的是 collusion-resistance 的 SKFE,但是当其用于计算 NC^0 上的 $RE.Encode(C,\cdot)$时,就退化成了 1-key SKFE,好在 1-key sublinear compact SKFE 已经足以构造 iO。

下面进一步分析上述方案具体需要用到多少阶的多线性映射。根据 AIK RE 的特性,每个输出位与 1 个输入位和 3 个随机串位有关,随机串又是由 PRG 生成的,且 PRG 的 locality 至少是 5,即 PRG 每个输出位与 5 个输入种子位有关,则总共与 1 个输入位和 15 个输入种子位有关。由于在安全证明中,需要加入一些额外的行为,因此,还会引入一个额外的输入比特 b。当 $b=0$ 时,电路会正常计算 $RE.Encode(C,\cdot)$;当 $b=1$ 时,电路会进行一些其他计算,这个计算涉及的比特位少于计算 $RE.Encode(C,\cdot)$,且 $b=1$ 这一情况只在安全证明中才会出现。上述方案每个输出位至多会用到 17 个输入位,即需要 17 阶多线性映射。

3.6　降低至三阶线性映射

为了进一步降低多线性映射的阶数,Lin[23] 同时指出可以赋予 PRG 特定的结构,并利用预处理的方法。由于 GC 具有 decomposable 的特性,因此,可以将 $RE.Encode(C,\cdot)$的计算拆分为$|C|$个计算,每个计算混淆 C 的一个电路门,每个计算的电路大小及需要用到的随机串均为 $poly(\lambda)$。之后再用 AIK RE 进一步 Encode,则此时 Encode 过程只和一个电路门以及 $poly(\lambda)$个随机数相关。可以使用 $poly(\lambda)$个完全相同的子 PRG 来生成随机串,这些子 PRG 的输出长度为$|C|$,这 $poly(\lambda)$个子 PRG 输出的第 i 个比特可以拼成长为 $poly(\lambda)$的伪随机串,用于混淆 C 的第 i 个电路门。在这种结构下,第 i 个 AIK RE 使用的随机数是由这些子 PRG 的第 i 个比特的输出拼成的,又因为这些子 PRG 完全相同,因此,子 PRG 第 i 个比特的输出一定对应于某 5 个特定的输入位置。虽然最终一个输出位会关联 15 个 PRG 输入位,但这 15 个输入位只来自于 5 个输入位置,每个位置取 3 个输入位。有了这一结构,就可以将每个输入位置的输入提前相乘,而不是使用多线性映射的能力计算乘法。由于总共有 $poly(\lambda)$个子 PRG,因此,每个输入位置有 $poly(\lambda)$个输入,从中任取 3 个(也可以不取),总共情况不超过$(1+poly(\lambda))^3$。仍然是关于 λ 的与$|C|$无关的多项式,从而不会影响 sublinear compactness。由于每个位置的输入已经提前乘好,剩下的计算则是围绕这 5 个位置进行的,b 和 x 也可以用类似的预处理技术,因此,五阶多线性映射就足够了。

Lin 等[24] 又在 2017 年进一步降低了多线性映射的阶数,由于 NC^0 上存在具有超线性 stretch 的 PRG 的 locality 必须大于等于 5,他们提出了一种新的 PRG,即 block-wise PRG,PRG 的每个输出对应的输入可以来自于常数多个分块,每个分块含有 $\log(\lambda)$个比特,这样通过预处理,可以将分块内的乘法提前算好,总共 $2^{\log(\lambda)}$种情况。由于每个分块都含有大量比特,这样似乎可以不受 locality 必须大于等于 5 的限制。最初,他们宣称 block-wise PRG 的每个输出可以只依赖 2 个 block,因而可以将 iO 规约到双线性映射这一标准假设,但是随后攻击这类 PRG 的方法被提出[31],他们只得宣称 block-wise PRG 的每个输出至少要依赖 3 个 block,最终 iO 被规约到三阶线性映射,离标准假设的目标仍有一步之遥。

4　第三代 iO:基于双多线性映射

2015 年,Gorbunov 等[32] 首次提出了部分隐藏(Partial Hiding, PH)的概念,并将其与 FHE 的部分解密结合,构造了谓词加密(Predicate Encryption, PE)。PE 是 ABE 的升级版,可以隐藏属性 $attr$ 的同时计算 $policy(attr)$的值,从这个角度看,它也可以说是一个特殊的 FE,对于构造 FE 有着借鉴意义。PH 是指加密消息时,将消息分为 2 个部分,即公开部分 P 和秘密部分 S,同时 PHPE 只支持对秘密部分 S 做一些轻量级的计算(内积计算)。可以将 $attr$ 在同态加密下的密文作为公开信息,将同态加密的密钥作为秘密信息。由于同态加密的密文是公开信息,因此,可以对它进行同态计算,得到 $policy(attr)$的加密,而同态加密的解密算法正是计算内积并通过模数运算去除噪声。如果只计算内积的话,会得到 $policy(attr)+noise$,只计算内积也被称作部分解密。在 PE 特殊的安全定义下,这个噪声的泄露将不会

影响安全性。

运用类似的思想,Jain 等[33-35]提出了相似的 SKFE 构造。强化了 Lin[23]在 2017 年构造出的 FE,基于双线性映射构造了 PHFE。PHFE 除了能够对秘密部分进行一次乘法计算外,还能对公开部分进行常数深度的计算。由于只需要构造一个支持 NC^0 电路的 SKFE,因此不需要使用全同态加密,只需要支持 NC^0 电路的同态加密。同样的,会得到 $C(x)$ 的加密,并用秘密部分的密钥来解密,解密操作是内积计算,得到的结果是 $C(x)+noise$,不同于 PE,这里的噪声会影响安全性,而模数操作又太复杂,无法依靠 PHFE 完成。为此,设想存在一个特殊的 PRG,通过将种子加密在秘密部分和公开部分中,可以用 PHFE 计算得到 PRG 的输出,并用这个输出去掩盖噪声。也就是说,这个特殊的 PRG 输出的每个比特可以表示为秘密部分的至多 2 个比特和公开部分的至多常数个比特的乘积和。至此,iO 被规约到了一个特殊的 PRG。

2021 年,Jain 等[36]最终构造出了这一 PRG,完成了基于标准假设构造 iO 的最后一块拼图。为此引入 LPN 假设,LPN 假设与 LWE 假设有相似之处,主要区别在于 LPN 中的噪声虽然可能很大,但数量少;LWE 中的噪声都很小,但很少出现为 0 的情况。将 PRG 的种子用 LPN 加密,并同态计算一个 NC^0 上的 PRG,最终同样得到 $PRG(seed)+noise$。LPN 的噪声很稀疏,不同于 LWE 的噪声,其可能被 PHFE 去掉。具体做法是提前计算出 LPN 的噪声,并将其一并放在 PHFE 密文的秘密部分。解密时算出 $PRG(seed)+noise$ 后,将其与 PHFE 中的噪声相减以抵消噪声。但是,噪声向量长度为 $|PRG(seed)|$,为了 sublinear compactness,只能加密长度小于这个值的输入(例如 seed)。为此,需要将稀疏的噪声向量压缩后存储在 PHFE 密文的秘密部分,同时又要能够用一次乘法就将压缩的噪声向量还原回来(因为 PHFE 只支持对秘密部分计算一次乘法)。因此,用到了矩阵的分解,即将噪声向量排列为矩阵形式。由于其稀疏性,矩阵的秩很低,一个秩很低的 $m\times m$ 的矩阵可以分解为一个 $m\times rank$ 的矩阵和一个 $rank\times m$ 的矩阵的乘积。就这样,基于 SXDH, LPN, LWE 和 NC^0 上存在 PRG 这 4 个假设的 iO 被构造了出来。之后,又利用 LPN 在 NC^0 上的同态性去代替 LWE(还包括一些其他技术),将假设减少为 3 个,即去掉了 LWE 假设[37]。

5 新的目标:后量子安全

群的特殊结构使得在面对量子计算机时,群上的安全假设(DH、RSA 等)都会被攻破,因此,也有一些工作试图用 LWE 加上一些其他假设构造后量子安全的 iO。这些候选方案有的是基于更强的循环安全(circular security)假设[38-40],循环安全假设是用于构造 FHE 的重要假设,也是得到了较为广泛认可的假设。虽然这类 iO 方案同样使用了 FHE 及其相关的技术,但是它们所依赖的假设却强于 FHE 所需的假设。与此同时,Wee 等[41]也展示了不经意的 LWE 采样可以蕴含 iO 并且给出了一个基于类似于循环安全的假设候选方案。然而,Hopkins 等[42]针对上述候选方案的假设给出了反例。2021 年,Wee 等[43]进一步改进了他们先前的工作,基于一个更弱的密码学原语(紧凑 LWE 采样(succinct LWE sampling))构造出了 iO,同时也给出了一个紧凑 LWE 采样的候选方案,该方案的安全性与求解多项式等式系统的困难性相关联。除了基于循环安全方面的假设,也有一些工作试图基于带噪声的线性函数加密(noisy linear functional encryption)来构造 iO[44-45]。除此之外有个特殊的用于仿射行列式程序的混淆方案[46],它的效率相较于其他方案非常高,而且安全性没有基于任何传统的假设,目前的量子技术对于攻击该方案也没有表现出特别的优势。但该方案的安全性无法规约到任何简明的具体假设上,且目前仅有唯一一篇针对该方案的安全分析[47]。

在这些工作中,基于更强的循环安全假设的工作最具代表性,也是本章重点介绍的方案。这类工作都是通过构造 functional encoding 从而构造 iO,与上一节类似的是,他们也使用 FHE 加密消息,并在解密阶段对其进行解密。但是,FHE 解密时不存在紧凑的解密提示,为此,使用了支持生成紧凑解密提示的线性同态加密(Linear Homomorphic Encryption, LHE)方案;同时,采用密钥交换技术,能把消息在 FHE 下的加密转换为消息在 LHE 下的加密。最初这类方案[38]使用的 LHE 基于的是 DCR 假设[48],因而无法实现后量子安全,后来这类方案[40]中的 LHE 被替换为基于 LWE 的 LHE。

其中,线性同态加密只能支持线性函数的同态加密,其中一些构造可以将解密分为 2 步:①根据密钥和密文生成短的解密提示;②根据解密提示对密文进行解密。

密钥交换技术最早出现在全同态加密的构造中,通常把解密过程视为用密钥对密文进行操作,如果转换视角,解密过程也可以理解为用密文对密钥进行操作。假设有第一个同态加密方案的密钥 sk_1,那么用 x 在第一个同态加密方案上的密文对该密钥进行操作可以解密得到 x;现在,将用第二个同态加密方案同态地进行这一操作,即最初持有地将不再是密钥 sk_1,而是用第二个同

态加密方案加密过的 sk_1;同理,此时的输出也不再是 x,而是 x 在第二个同态加密方案上的密文。这样就完成了密钥的切换,需要注意的是,切换能够成功的前提是第二个同态加密方案支持同态地运行第一个同态加密方案的解密电路。FHE 的部分解密是线性函数(计算内积),因此,可以被 LHE 同态计算。但是,FHE 部分解密得到的是 $C(x)+noise$,至此,他们遇到了和之前的构造一样的问题,即如何掩盖噪声。

针对噪声的泄露通常只有 2 类方法:去除噪声或者用一个更大的随机噪声去掩盖。去除噪声是一个十分复杂的功能,无法用线性函数去解决(LHE 只支持线性函数),因此,只剩下用一个更大的噪声去掩盖这条路可以走。理想情况下,有一个预言机(oracle),它能够产生一个 LHE 的密文,这个密文对应的明文是一个较大的随机噪声,通过 LHE 将两者进行叠加(加法是一个十分简单的线性函数,可以通过 LHE 的同态性完成),就可以掩盖 FHE 产生的噪声。

现实情况下显然没有如此方便的 oracle,但可以使用随机预言机(random oracle)产生一个随机数,前文提到的那几种 LHE 方案还具有一个非常好的性质,它们的密文空间很"稠密"(这意味着随机数有极大概率能被当成 LHE 的密文成功进行解密)。随机数对应的明文可能是个非常大的数,而需要的仅仅是一个稍大的噪声,这个噪声能够掩盖 FHE 解密时产生的噪声又不至于掩盖解密后的明文。此时,需要将明文的高位设为 0,这又是一个十分复杂的操作,无法用线性函数完成,因此,使用密钥交换技术把 LHE 的密文转为 FHE 的密文,通过 FHE 全同态的能力去除明文的高位,之后再次利用密钥交换技术把 FHE 的密文转回 LHE 的密文,这样,就能得到一个经 LHE 加密的较大噪声。到这里仍然有一个小问题,就是利用密钥交换将 FHE 的密文转回 LHE 的密文时又会产生一个小噪声,这个小噪声会引入一定的相关性,虽然这个相关性看上去很难被敌手利用,但是这给安全性证明带来了困难。同时,由于密文需要在 FHE 和 LHE 之间互相转换,因此,这一构造在证明时需要用到循环安全假设。各类方案的对比见表 1。

Gay 等[39]随后对该方案做了进一步的改进,将 random oracle 替换为一串很长的 CRS,并且发现 FHE 可以给密文附上新的噪声(同态地加上一个 0 的加密),因此,通过给 FHE 密文附上较大噪声的方式去掩盖会产生相关性的小噪音。同时,给出了安全证明,将方案的安全性规约到了一个更强的循环安全假设。各类方案的对比见表 1。

表 1　iO 主流候选方案对比

Table 1　Comparison among the popular iO candidates

分 类	效率	安全性	典型技术
基于多线性映射	高	低	类拼图游戏 + 通过 FHE 自举
基于标准假设	低	高	稀疏矩阵分解 + 部分解密 + 规约到 XiO
基于格上困难问题	中	中	密钥切换 + 部分解密 + 规约到 XiO

6　总结与展望

经过了十年的发展,构造可证明安全的 iO 已经初步取得了成功,一些曾经质疑 iO 是否有可能存在的研究者也开始转而投入相关的工作当中。尽管这一构造目前不是后量子安全的,但是研究者们也已经开始朝着这个方向前进。这类可证明安全的构造在安全性方面虽然更有保证,但是也会牺牲效率,而且完整的规约过程也十分复杂。除了实现后量子安全,这类方案未来可以朝着更少假设、更少规约和更高效实现这 3 个方向进一步前进。

另外,也有一些更为直接的构造,例如基于多线性映射以及矩阵随机化的候选方案。这类方案效率更高,但是在安全性方面需要大量的安全分析,并经受多轮攻击修复的循环才能得到较为广泛的信任。未来可以尝试提出各种直接构造 iO 的方案,并尝试对这些方案进行分析、攻击与修复。这类方案的高效性使得 iO 能更早地从理论世界进入应用领域。

参考文献:

[1] Barak B, Goldreich O, Impagliazzo R, et al. On the (im)possibility of obfuscating programs[C]//The 21st Annual International Cryptology Conference, CRYPTO 2001. Berlin: Springer, 2001: 1-18.

[2] Goldwasser S, Rothblum G N. On best-possible obfuscation[C]//Theory of Cryptography-5th International Conference, TCC 2007. Berlin: Springer, 2007: 194-213.

[3] Sahai A, Waters B. How to use indistinguishability obfuscation: Deniable encryption, and more[C]//The 46th Annual ACM Symposium on Theory of Computing, STOC 2014. New York: ACM, 2014: 475-484.

[4] Garg S, Gentry C, Halevi S, et al. Candidate indistinguishability obfuscation and functional encryption for all circuits[C]//The 54th Annual Symposium on Foundations of Computer Science, FOCS 2013. Piscataway: IEEE, 2013: 40-49.
[5] Barak B, Garg S, Kalai Y T, et al. Protecting obfuscation against algebraic attacks[C]//The 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2014. Berlin: Springer, 2014: 221-238.
[6] Brakerski Z, Rothblum G N. Virtual black-box obfuscation for all circuits via generic graded encoding[C]//Theory of Cryptography-12th International Conference, TCC 2014. Berlin: Springer, 2014: 1-25.
[7] Cheon J H, Han K, Lee C, et al. Cryptanalysis of the multilinear map over the integers[C]//The 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2015. Berlin: Springer, 2015: 3-12.
[8] Hu Y, Jia H. Cryptanalysis of GGH map[C]//The 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2016. Berlin: Springer, 2016: 537-565.
[9] Miles E, Sahai A, Zhandry M. Annihilation attacks for multilinear maps: Cryptanalysis of indistinguishability obfuscation over GGH13[C]//The 36th Annual International Cryptology Conference, CRYPTO 2016. Berlin: Springer, 2016: 629-658.
[10] Chen Y, Gentry C, Halevi S. Cryptanalyses of candidate branching program obfuscators[C]//The 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2017. Berlin: Springer, 2017: 278-307.
[11] Miller V S. Short programs for functions on curves[EB/OL]. (2002-08-26)[2022-09-10]. https://crypto.stanford.edu/miller.
[12] Boneh D, Silverberg A. Applications of multilinear forms to cryptography[J]. Contemporary Mathematics, 2003, 324: 71-90.
[13] Garg S, Gentry C, Halevi S. Candidate multilinear maps from ideal lattices[C]//The 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2013. Berlin: Springer, 2013: 1-17.
[14] Coron J S, Lepoint T, Tibouchi M. Practical multilinear maps over the integers[C]//The 33rd Annual International Cryptology Conference, CRYPTO 2013. Berlin: Springer, 2013: 476-493.
[15] Gentry C, Gorbunov S, Halevi S. Graph-induced multilinear maps from lattices[C]//Theory of Cryptography-13th International Conference, TCC 2015. Berlin: Springer, 2015: 498-527.
[16] Barrington D A. Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1[C]//The 18th Annual ACM Symposium on Theory of Computing, STOC 1986. New York: ACM, 1986: 1-5.
[17] Ananth P, Jain A. Indistinguishability obfuscation from compact functional encryption[C]//The 35th Annual International Cryptology Conference, CRYPTO 2015. Berlin: Springer, 2015: 308-326.
[18] Bitansky N, Vaikuntanathan V. Indistinguishability obfuscation from functional encryption[C]//The 56th Annual Symposium on Foundations of Computer Science, FOCS 2015. Piscataway: IEEE, 2015: 171-190.
[19] Lin H, Pass R, Seth K, et al. Output-compressing randomized encodings and applications[C]//Theory of Cryptography-14th International Conference, TCC 2016. Berlin: Springer, 2016: 96-124.
[20] Lin H, Pass R, Seth K, et al. Indistinguishability obfuscation with non-trivial efficiency[C]//The 19th IACR International Conference on Practice and Theory of Public-Key Cryptography, PKC 2016. Berlin: Springer, 2016: 447-462.
[21] Lin H. Indistinguishability obfuscation from constant-degree graded encoding schemes[C]//The 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2016. Berlin: Springer, 2016: 28-57.
[22] Lin H, Vaikuntanathan V. Indistinguishability obfuscation from DDH-like assumptions on constant-degree graded encodings[C]//The 57th Annual Symposium on Foundations of Computer Science, FOCS 2016. Piscataway: IEEE, 2016: 11-20.
[23] Lin H. Indistinguishability obfuscation from SXDH on 5-Linear maps and locality-5 PRGs[C]//The 37th Annual International Cryptology Conference, CRYPTO 2017. Berlin: Springer, 2017: 599-629.
[24] Lin H, Tessaro S. Indistinguishability obfuscation from trilinear maps and block-wise local PRGs[C]//The 37th Annual International Cryptology Conference, CRYPTO 2017. Berlin: Springer, 2017: 630-660.
[25] Goldwasser S, Kalai Y, Popa R A. Reusable garbled circuits and succinct functional encryption[C]//The 45th Annual ACM Symposium on Theory of Computing, STOC 2013. New York: ACM, 2013: 555-564.
[26] Ananth P, Brakerski Z, Segev G, et al. From selective to adaptive security in functional encryption[C]//The 35th Annual International Cryptology Conference, CRYPTO 2015. Berlin: Springer, 2015: 657-677.
[27] Ananth P, Jain A, Sahai A. Achieving compactness generically: Indistinguishability obfuscation from non-compact functional encryption[EB/OL]. (2015-07-24)[2022-09-22]. https://eprint.iacr.org/archive/2015/730.
[28] Applebaum B, Ishai Y, Kushilevitz E. Cryptography in NC^0[C]//The 45th Annual Symposium on Foundations of Computer Science, FOCS 2004. Piscataway: IEEE, 2004: 166-175.
[29] Goldreich O. Candidate one-way functions based on expander graphs[EB/OL]. (2000-12-03)[2022-09-10]. https://

eprint. iacr. org/2000/063.

[30] Mossel E, Shpilka A, Trevisan L. On ε-biased generators in NC^0[C]//The 44th Annual Symposium on Foundations of Computer Science, FOCS 2003. Piscataway: IEEE, 2003: 136-145.

[31] Barak B, Brakerski Z, Komargodski I. Limits on low-degree pseudorandom generators (or: sum-of-squares meets program obfuscation)[C]//The 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2018. Berlin: Springer, 2018: 649-679.

[32] Gorbunov S, Vaikuntanathan V, Wee H. Predicate encryption for circuits from LWE[C]//The 35th Annual International Cryptology Conference, CRYPTO 2015. Berlin: Springer, 2015: 503-523.

[33] Jain A, Lin H, Matt C, et al. How to leverage hardness of constant-degree expanding polynomials over R to build iO[C]//The 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2019. Berlin: Springer, 2019: 251-281.

[34] Ananth P, Jain A, Lin H, et al. Indistinguishability obfuscation without multilinear maps: New paradigms via low degree weak pseudorandomness and security amplification[C]//The 39th Annual International Cryptology Conference, CRYPTO 2019. Berlin: Springer, 2019: 284-332.

[35] Gay R, Jain A, Lin H, et al. Indistinguishability obfuscation from simple-to-state hard problems: New assumptions, new techniques, and simplification[C]//The 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2021. Berlin: Springer, 2021: 97-126.

[36] Jain A, Lin H, Sahai A. Indistinguishability obfuscation from well-founded assumptions[C]//The 53rd Annual ACM Symposium on Theory of Computing, STOC 2021. New York: ACM, 2021: 60-73.

[37] Jain A, Lin H, Sahai A. Indistinguishability obfuscation from LPN over Fp, DLIN, and PRGs in NC^0[C]//The 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2022. Berlin: Springer, 2022: 670-699.

[38] Brakerski Z, Döttling N, Garg S, et al. Candidate iO from homomorphic encryption schemes[C]//The 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2020. Berlin: Springer, 2020: 79-109.

[39] Gay R, Pass R. Indistinguishability obfuscation from circular security[C]//The 53th Annual ACM Symposium on Theory of Computing, STOC 2021. New York: ACM, 2021: 736-749.

[40] Brakerski Z, Döttling N, Garg S, et al. Factoring and pairings are not necessary for iO: Circular-secure LWE suffices[EB/OL]. (2020-08-27)[2022-09-22]. https://eprint. iacr. org/2020/1024.

[41] Wee H, Wichs D. Candidate obfuscation via oblivious LWE sampling[C]//The 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2021. Berlin: Springer, 2021: 127-156.

[42] Hopkins S, Jain A, Lin H. Counterexamples to new circular security assumptions underlying iO[C]//The 41st Annual International Cryptology Conference, CRYPTO 2021. Berlin: Springer, 2021: 673-700.

[43] Devadas L, Quach W, Vaikuntanathan V, et al. Succinct LWE sampling, random polynomials, and obfuscation[C]//Theory of Cryptography-19th International Conference, TCC 2021. Berlin: Springer, 2021: 256-287.

[44] Agrawal S. Indistinguishability obfuscation without multilinear maps: New methods for bootstrapping and instantiation[C]//The 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2019. Berlin: Springer, 2019: 191-225.

[45] Agrawal S, Pellet M A. Indistinguishability obfuscation without maps: Attacks and fixes for noisy linear FE[C]//The 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2020. Berlin: Springer, 2020: 110-140.

[46] Bartusek J, Ishai Y, Jain A, et al. Affine determinant programs: A framework for obfuscation and witness encryption[C]//The 11th Annual Innovations in Theoretical Computer Science Conference, ITCS 2020. Washington: LIPIcs, 2020, 151(82):1-39.

[47] Yao L, Chen Y L, Yu Y. Cryptanalysis of candidate obfuscators for affine determinant programs[C]//The 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2022. Berlin: Springer, 2022: 645-669.

[48] Damgård I, Jurik M. A generalisation, a simplification and some applications of Paillier's probabilistic public-key system[C]//The 4th IACR International Conference on Practice and Theory of Public-Key Cryptography, PKC 2001. Berlin: Springer, 2001: 119-136.

【责任编辑: 卓祯雨】