# 安全多方计算研究方向和研究课题
# Research Fields and Topics in MPC

杨鹏

2022/11/18

安全多方计算（Secure Multi-Party Computation，MPC）允许多个互不信任的参与方共同计算一个功能函数并各自得到函数计算结果，在这个过程中需要保证各方输入的隐私性和计算结果的正确性。安全多方计算起源于 1982 年姚期智提出的“百万富翁问题”，自此许多学者针对安全多方计算在理论上的可行性展开了大量的工作。2004 年，第一个通用安全多方计算平台 Fairplay 的诞生拉开了实用安全多方计算的序幕。目前，安全多方计算（MPC）的主要研究方向为恶意模型下的安全多方计算，安全多方计算在机器学习、信息检索等方面的应用，以及安全多方计算和其他方法的结合。

进一步地，本文在上述研究方向的基础上，提出安全多方计算理论、隐私保护机器学习、密态数据库查询等方面可供研究的课题。

# 目录

# 1 恶意模型下的安全多方计算

经过 40 多年的发展，安全多方计算理论已经趋于成熟，半诚实模型下安全多方计算通用协议在计算效率和通信开销上已经可以被业界接受，需要进一步研究的是恶意模型下的安全多方计算通用协议，半诚实模型下或恶意模型下安全多方计算专用协议。本节简单介绍一些恶意模型下安全多方计算通用协议研究，第 2 节将介绍半诚实模型下或恶意模型下安全多方计算专用协议。

恶意模型下的安全多方计算协议考虑恶意敌手，其通过控制参与方来执行自己的指令以对协议进行攻击。假设有 $n(n \geq 2)$ 个参与方执行协议，按照不诚实参与方的数量 $t$ 可将其分类为：1）$1 \leq t \leq n/2$：诚实大多数的安全多方计算协议和，2）$n/2 < t \leq n-1$：不诚实大多数的安全多方计算协议。恶意模型下的安全多方计算协议的通信开销和计算开销较大，因为在恶意模型中，需要进行大量交互来确保交互信息的正确性，因此小数量方的诚实大多数安全多方计算协议被大量研究，此类协议可以实现较高的效率。另外，不诚实大多数的安全多方计算协议也被大量研究，因为恶意模型下的安全两方计算协议对应着不诚实大多数的情况（$t = 1, n = 2$）。

**小数量参与方的诚实大多数安全多方计算协议** 此类协议考虑诚实大多数的设置，不诚实参与方的数量最多为 $\lfloor n/2 \rfloor$，因此需要协议考虑 $3 \sim 5$ 个参与方的情况，如论文 [1,2] 等。在这种情况下，诚实方的数量多于不诚实方的数量，利用这一点便可以减少交互或者降低通信开销。

**诚实大多数的安全多方计算协议** 此类协议允许不诚实参与方数量最多为 $n-1$。最常见的设置是恶意模型下的安全两方计算，其天然是不诚实大多数的情况。目前诚实大多数的安全多方计算协议主要是 SPDZ 系列协议 [3–12]，如图 1 所示。

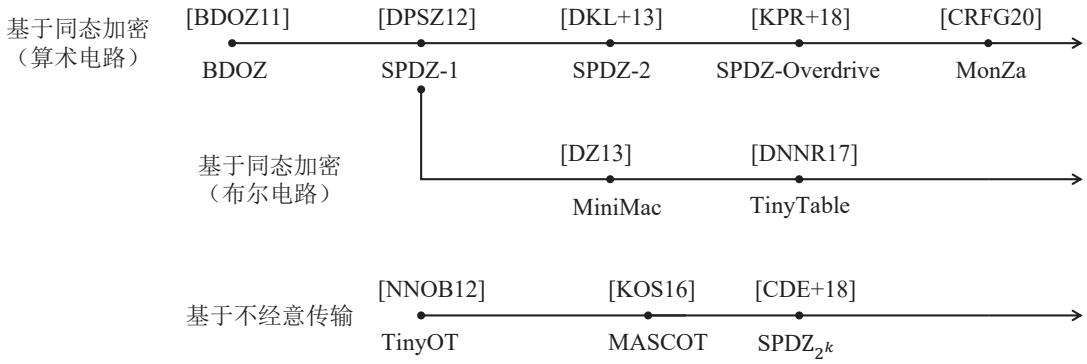


图 1: SPDZ 系列协议

# 2 安全多方计算应用

安全多方计算可以支持互不信任的各方在不泄露隐私数据的情况下进行联合计算，被广泛用于隐私计算应用场景中。在这里，主要关注半诚实模型下安全多方计算协议在机器学习、数据库查询和统计分析等领域的应用。

## 2.1 半诚实模型下安全多方计算

在介绍具体应用之前，可以先介绍常用的半诚实模型下安全多方计算框架。主要有基于混淆电路的 MPC 协议 [13] 和基于秘密共享的 MPC 协议 [14]：前者主要基于布尔电路进行计算，其通信轮数是常数轮，但通信带宽非常高，往往适用于广域网环境；后者基于算术电路进行计算，其通信带宽较低，但通信轮数和电路深度成正比，在局域网环境下表现更好。在实际应用中，大多数函数表示为算术电路的电路复杂度更低，因此目前大多数实际协议多考虑基于秘密共享的 MPC 协议。

基于秘密共享的 MPC 协议可以在本地进行加法，而乘法需要进行多轮交互，为降低乘法运算的交互轮数，通常采用 Beaver 三元组进行预处理计算 [15][1]，这一范式也称为预处理模型。预处理模型下的 MPC 协议将协议分为预处理阶段和在线阶段，并将大部分通信量都转移到预处理阶段，从而大大降低了在线阶段的通信开销。预处理模型下的 MPC 协议可以以很低的通信开销计算算术电路，但计算布尔电路的通信开销仍然较大，因此一些工作提出基于电路转换的混合协议来解决这一问题。2015 年，Demmler 等人 [20] 提出了基于电路转换的混合协议，称为 ABY 协议。该协议利用布尔秘密份额、算术秘密份额和姚氏秘密份额之间的转换实现了布尔电路和算术电路的转换，使其可以为不同的运算生成更合适的电路表示。2021 年 Patra 等人 [21] 提出了 ABY2.0 协议，进一步降低了电路计算和电路转换阶段的通信量。

在预处理模型下的 MPC 协议中，根据参与方数量的不同，使用的秘密共享方案也有所不同（主要体现在乘法运算上），下面是常用的几种方案：

1. 参与方数量 $n = 2$：考虑利用加性秘密共享，采用 Beaver 三元组计算乘法
2. 参与方数量 $n = 3$：考虑利用加性秘密共享或复制秘密共享，一般复制秘密共享 [1] 的效率更高
3. 参与方数量 $n > 3$：考虑利用加性秘密共享或 Shamir 秘密共享

## 2.2 隐私保护机器学习

安全多方计算技术允许互不信任的参与方基于各自隐私输入进行联合计算某一函数，除函数结果外不泄漏任何信息。基于安全多方计算的隐私保护机器学习能够保证数据拥有方在不泄漏隐私数据的情况下进行模型训练和推理，已有大量工作对其进行研究，下面简单介绍一下隐私保护机器学习的进展和未来的方向。

2017 年，Mohassel 等人 [17] 提出了安全机器学习框架 SecureML，基于混合协议 ABY 构建了两方服务器模型下的半诚实隐私保护机器学习系统，提出了隐私保护线性回归、逻辑回归和神经网络训练协议。2018 年，Riazi 等人 [22] 基于 ABY 框架提出了半诚实模型下的安全推理系统 Chameleon，并提出在离线阶段引入半诚实第三方辅助生成乘法三元组，提高协议效率。同年，Mohassel 等人 [1] 将两方

[1] 一些工作也考虑其他形式的相关随机性，2013 年，Keller 等人 [16] 考虑到了相关随机性的形式，提出了除常见的 Beaver 三元组外的 Square 元组、Bit 元组、Input 元组和 Inv 元组，从而提高某些算术操作的效率。2017 年，Mohassel 等人 [17] 提出了一个隐私保护机器学习系统 SecureML，该系统设计中将 Beaver 三元组矢量化，实际上提出了矩阵形式的乘法三元组。2020 年，Chen 等人 [18] 提出了隐私保护深度学习系统，该系统将 Beaver 三元组扩展到矩阵形式和卷积形式的乘法三元组。2022 年，Reisert 等人 [19] 则进一步扩展了 Beaver 三元组和二项式元组（Binomial Tuples），提出了算术元组（Arithmetic Tuples）的概念去计算多元多项式。

的 ABY 框架扩展成三方 ABY3 协议，实现了恶意安全，并基于复制秘密共享技术设计和实现三方设置下隐私保护线性回归、逻辑回归和神经网络协议，但该协议只在半诚实模型下安全。2019 年，Wagh 等人 [23] 提出了隐私保护神经网络训练系统 SeucreNN，其基于加性秘密共享技术实现了安全三方神经网络训练，并在不诚实大多数的设置下保证半诚实安全和恶意安全。2020 年，Rathee 等人 [24] 提出了半诚实模型下的安全两方神经网络推理协议 CrypTFlow2，其基于同态加密和 OT 协议提出了新的安全比较协议、新的除法算法，进一步降低了协议的通信复杂度。2021 年，Wagh 等人 [25] 基于 SecureNN 和 ABY3 协议提出了安全三方的隐私保护机器学习训练和推理框架 Falcon，其支持批量归一化操作，并在诚实大多数的设置下保证隐私。2022 年，Huang 等人 [26] 基于同态加密和秘密共享实现了半诚实模型下高效安全两方推理系统 Cheetah，其基于同态加密实现了无需任何昂贵的旋转操作即可评估线性层，并设计了几个用于非线性函数的高效原语言，相比于 CrypTFlow2 大幅降低了推理时间和通信开销。

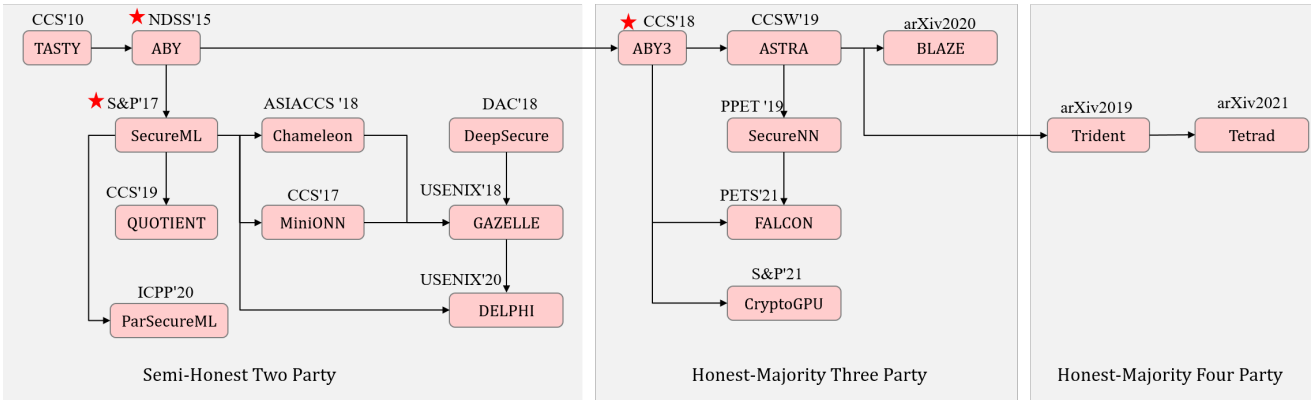


图 2: 隐私保护机器学习进展

近些年，基于安全多方计算的隐私保护机器学习发展迅猛，相关技术也十分成熟，未来的方向是恶意模型下的隐私保护机器学习、小数量参与方的隐私保护机器学习，以及结合新技术的隐私保护机器学习。其中新技术有同态加密 [26]、差分隐私 [27]、函数秘密共享 [28] 等等。

在另一方面，常见的隐私保护机器学习专注于机器学习算法的计算，部分工作也关注训练数据特性，工作 [29] 考虑了低维数据的线性回归模型训练，工作 [30] 则考虑稀疏矩阵的神经网络训练。进一步地，可以考虑非结构化数据的机器学习训练和推理，这一部分有待更多工作进行探索。

## 2.3 密态数据库查询

在这里，考虑的密态数据库查询（Database Query for Secret Shared Data）是这样的场景：有若干个云数据库 $S_1, S_2, ..., S_n$，数据拥有者将其数据放在数据库中，为了不让单一数据库知晓自己数据（数据中存在隐私），数据拥有者将自己的数据通过加性秘密共享技术分发给云数据库 $S_1, S_2, ..., S_n$，例如下面的一种方式：

1. 数据拥有者拥有数据 $x$，拟将其存储在云数据库 $S_1, S_2, ..., S_n$ 中

2. 数据拥有者随机选择 $n-1$ 个随机数 $r_1, r_2, ...r_{n-1}$，并计算 $[x]_1 = r_1, [x]_2 = r_2, ..., [x]_{n-1} =$

$r_{n-1}, x_n = x - r_1 - r_2 - ... - r_{n-1}$

3. 数据拥有者将 $[x]_i$ 发送给云数据库 $S_i$，其中 $i = 1, 2, ..., n$

通过这种方式，云数据库 $S_i$ 分别拥有数据 $x$ 的一部分 $[x]_i$，而且 $[x]_1 + [x]_2 + ... + [x]_n = x$，通常将 $[x]_i$ 称为数据的秘密份额，通过秘密份额 $[x]_i$ 数据库无法知晓原始数据 $x$。同样地，众多的数据拥有者将自己的数据以上述方式上传到云数据库，云数据库从而拥有了所有数据拥有者数据的秘密份额，因此可将这些云数据库称之为分布式密态数据库。

分布式密态数据库一旦形成，可以提供这样的服务：用户想要根据关键词（例如查询年龄大于 18 岁的男生）查询数据库，将其查询的关键字送给所有云数据库，云数据库通过执行一个安全多方计算协议来输出得到查询结果，并将查询结果返回给用户。在这个过程中，用户不会知道数据库中隐私数据，云数据库也不会泄露数据的隐私，这种范式称为 Database Query for Secret Shared Data。

目前，两方设置和三方设置被广泛考虑，两方设置下通常使用加性秘密共享，三方设置下通常使用复制秘密共享 [31, 32]。未来的研究方向是针对不同的数据库查询场景利用合适的安全多方计算协议来设计特定的密态数据库查询协议。

### 2.4 其他安全多方计算应用

其他安全多方计算应用有隐私保护统计分析 [33]、隐私集合计算 [34, 35]、隐私信息检索 [36]、隐私频繁项查询 [37] 等，下面进行简单介绍：

1. 隐私保护统计分析（Privacy Protection Statistical Analysis，PPSA）：统计分析是数据挖掘的常用工具之一，其通过建立预报变量和响应变量之间的统计模型，从而实现变量的预测建模任务。隐私保护统计分析和隐私保护机器学习的基本运算很类似，但目前关于隐私保护统计分析的研究较少，值得进一步研究。

2. 隐私集合计算（Private Set Computation，PSC）：隐私集合计算是安全多方计算中特定应用之一，目前有隐私集合求交（Private Set Intersection，PSI）被广泛研究。例如，隐私集合求交考虑这样的场景：多个参与方拥有数据集合，它们希望能够在不泄露自己数据集合的情况下计算得到所有参与方数据集合的交集。在金融、医疗等领域需要此类技术，进一步地，这种技术被扩展为隐私集合计算，包括求交集、并集和差集等等。

3. 隐私信息检索（Private Information Retrieval，PIR，也称匿踪查询）是安全多方计算中很实用的一项技术，用来保护用户的查询隐私。其目的是保证用户向服务器（数据源方）提交查询请求时，在用户查询信息不被泄漏的条件下完成查询，即整个查询过程中服务器不知道用户具体查询信息及查询出的数据项[2]。

4. 隐私频繁项查询（Private Heavy Hitters，）：隐私频繁项查询考虑这样的问题：许多用户拥有一定数据（比如浏览器中的查询记录），客户端希望得到所有用户查询记录中最频繁的前 $k$ 条记录（Top k

[2]进一步了解，请参考【隐语小课｜私有信息检索 (PIR) 及其应用场景】https://mp.weixin.qq.com/s/Vf5AFep2JKztXpOt95WW8g

问题），为避免用户数据被泄露给客户端，要求多个客户端一起执行安全多方计算协议来进行计算。实际上，这类应用是密态数据库查询的特例，这类只要求查询最频繁的前 $k$ 条记录。

实际上，无论是哪一种安全多方计算应用，最关键的是弄明白底层运算是什么，并利用安全多方计算协议来实现底层运算，然后搭建该安全多方计算应用的各计算模块，最终完成安全计算，这也是安全多方计算实现各种应用的本质。面向特定场景的安全多方计算专用协议是未来的方向，目前值得进一步研究的有：

1. 考虑数据特性的隐私保护机器学习算法：例如工作 [29] 考虑了低维数据的线性回归模型训练，但该工作计算效率和通信开销不高，值得进一步研究
2. 特定场景下的密态数据库查询和隐私频繁项查询问题：结合特定查询算法，如 SkyLine 查询算法 [38]，设计特定的安全数据库查询协议。
3. 多服务器的隐私信息检索问题：单服务器的隐私信息检索可以用同态加密解决 [39]，而安全多方计算能够解决多服务器的隐私信息检索问题。

# 3 安全多方计算方法和其他方法的结合

本节简单介绍一些安全多方计算方法和其他方法相结合的协议或框架。这些所谓的其他方法包括混淆电路、函数秘密共享、同态加密、差分隐私、联邦学习等等。

**混淆电路** 前述提到，MPC 协议常用的技术有秘密共享技术和混淆电路技术，其中秘密共享技术被大多数应用所采用，而混淆电路技术一直是理论研究的热点，二者各有优势。因此，一些工作结合混淆电路和秘密共享通过优势互补来实现高效安全多方计算协议 [29]。

**函数秘密共享** 近些年，一种被称为函数秘密共享（Function Secret Sharing，FSS）的概念被提出并应用于预处理模型下的 MPC 协议，大大降低了 MPC 协议的通信开销 [40,41]。2019 年，Bolye 等人 [42] 结合函数秘密共享和加性秘密共享，提出了基于函数秘密共享的安全两方计算框架，该框架被用于构建预处理模型下混合模式安全计算协议。2021 年，Boyle 等人 [43] 进一步扩展了工作 [42] 的结果，并表示基于函数秘密共享的 MPC 协议具有最优的在线阶段通信复杂度。这种技术也在最近几年得到了广泛的应用，2022 年，Ryffel 等人 [28] 提出基于函数秘密共享设计了半诚实两方计算协议，利用优化分布式比较函数为神经网络训练算法中 ReLU、MaxPool 和 BatchNorm 等函数设计了安全计算构造模块。2022 年，Wagh [44] 提出基于函数秘密共享的常数轮安全计算协议，该协议利用分布式查找表来安全计算除法、指数、对数等非线性函数。2022 年，Agarwal [27] 等人结合基于函数秘密共享的 MPC 协议和基于加性秘密共享的 MPC 协议提出了隐私保护逻辑回归方案，其中提出了许多基于函数秘密共享的安全计算模块。

**同态加密** 同态加密也是常用的密码学方法，其通信开销很低而计算开销很高，因此一些工作结合同态加密和秘密共享 [30] 来提高安全多方计算协议的计算效率和降低通信开销。同时，一些工作还考虑同态秘密共享概念 [45–47]，利用该技术也可以实现安全多方计算。

**差分隐私和联邦学习** 基于密码学的隐私计算技术在安全性是有可靠的保障，但有时在应用中被认为是“过于安全”，因此目前一些研究通过引入安全性较低的技术，如差分隐私技术 [27]，来实现效率的提升，这在一些安全性要求不高的场景获得了很好的效果。另一方面，在一些安全性不高的领域，如联邦学习，可以利用安全多方计算来保护隐私 [48]。

本质上，这类“混合模型”是试图实现效率-安全性的平衡，这一思想并不适合构建通用协议，但在特定的场景下是非常有用的，因此非常适合在特定场景下设计专用协议时考虑此方法。

# 4 研究方向总结

恶意模型下的安全多方计算偏向于理论研究，专注于通用协议框架的设计和进一步降低通信开销。而安全多方计算的应用则是考虑专用协议设计和降低通信开销和计算开销，其中预处理模型下的安全多方计算是使用最频繁的协议框架。同时，由于参与方越多，安全多方计算通信开销和计算开销越大，因此小数量参与方被考虑，并通过计算外包范式[3]满足数据拥有方可扩展性。进一步地，“混合模型”的思想被考虑，通过结合安全多方计算方法和其他隐私计算方法来平衡安全性和效率。

总结来说，希望研究理论则可以考虑恶意模型下的安全多方计算协议，而偏好实践则可以考虑安全多方计算在各种场景下的应用。事实上，每一个方向都是值得研究的方向，通过努力研究，多看论文，总能获得一些好的成果，这一点是永恒不变的真理。

表 1: MPC 方向总结

| | 理论性 | 实践性 | 难度 |
|---|---|---|---|
| 恶意模型下安全多方计算 | ⋆⋆⋆⋆ | ⋆⋆ | ⋆⋆⋆⋆ |
| 安全多方计算的应用 | ⋆⋆ | ⋆⋆⋆⋆ | ⋆⋆⋆⋆ |
| 安全多方计算与其他方法结合 | ⋆⋆⋆ | ⋆⋆⋆⋆ | ⋆⋆⋆ |

# 5 研究课题介绍

本节简单介绍一些目前安全多方计算领域的研究课题。

## 5.1 恶意模型下安全两方计算研究

研究基于可认证秘密共享 [4] 和可认证混淆电路 [49] 方法实现恶意模型下更低通信复杂度的安全两方计算。

[3]指数据拥有方将数据秘密分发给云服务器，云服务器运行 MPC 协议来进行计算。

### 5.2 How to share a function?

函数秘密共享的基本思想是将函数安全地进行秘密分发，目前已有的方法包括真值表法 [40, 44]、基于 PRG 的 GGM 方法 [40,41]，另外工作 [50] 利用布谷鸟哈希方法实现了分布式多点函数，工作 [51] 提出了新的方法来构造分布式点函数。进一步地，研究如何安全地分发函数是一项非常具有挑战性的工作。

### 5.3 基于函数秘密共享和同态秘密共享的恶意安全两方计算

研究基于函数秘密共享 [40] 和同态秘密共享 [45] 恶意模型下更低通信复杂度的安全两方计算。

### 5.4 基于快速矩阵运算的水平分布低维数据隐私保护机器学习

工作 [29] 提出当数据是水平分布且特征维度较低时，利用直接求解线性方程组的方法来计算隐私保护线性回归将会十分高效。因此，基于水平分布低维数据的设定研究基于快速矩阵运算（矩阵乘法、矩阵求逆）的隐私保护线性回归和逻辑回归是一个非常有前景的方向。

### 5.5 基于同态加密和秘密共享的垂直分布高维稀疏数据隐私保护机器学习

工作 [30] 提出面向垂直分布高维稀疏数据的基于安全稀疏矩阵乘法的隐私保护逻辑回归算法。进一步地，可将该思路扩展到其他安全多方计算场景下。

### 5.6 安全两方二值神经网络训练和推理研究

工作 [52] 提出了安全三方二值神经网络推理。进一步地，可以研究基于秘密共享或函数秘密共享的安全两方二值神经网络训练和推理，同时也可以针对更多机器学习算法设计特定的隐私保护协议。

### 5.7 特定场景下的密态数据库查询算法研究

工作 [38] 面向 Skyline 查询算法提出了基于秘密共享的安全 Skyline 查询系统，工作 [37] 针对频繁项查询问题提出了隐私频繁项查询算法。进一步地，可以考虑其他特定场景下的密态数据库查询算法。

### 5.8 基于函数秘密共享的两方服务器隐私信息检索研究

工作 [53] 基于分布式点函数提出了第一个两方服务器隐私信息检索协议。进一步地，研究基于函数秘密共享的两方服务器隐私信息检索。

### 5.9 基于函数秘密共享和加性秘密共享的隐私保护统计分析研究

工作 [33] 提出了基于函数秘密共享的安全两方泊松回归分析算法。进一步地研究基于函数秘密共享和加性秘密共享的隐私保护统计分析，如线性回归、泊松回归等。

### 5.10 基于函数秘密共享隐私集合计算

工作 [54,55] 提出了基于函数秘密共享的隐私集合求交运算。进一步地研究基于函数秘密共享的隐私集合计算，如隐私集合求交、隐私集合求并等。

## 参考文献


[1] Payman Mohassel and Peter Rindal. ABY3: A mixed protocol framework for machine learning. In *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, pages 35–52, 2018.

[2] Anders Dalskov, Daniel Escudero, and Marcel Keller. Fantastic Four:Honest-Majority Four-Party Secure Computation With Malicious Security. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 2183–2200, 2021.

[3] Rikke Bendlin, Ivan Damgård, Claudio Orlandi, and Sarah Zakarias. Semi-homomorphic Encryption and Multiparty Computation. In *Advances in Cryptology –EUROCRYPT 2011*, pages 169–188. Springer, 2011.

[4] Ivan Damgård, Valerio Pastro, Nigel Smart, and Sarah Zakarias. Multiparty Computation from Somewhat Homomorphic Encryption. In *Advances in cryptology –CRYPTO 2012*, pages 643–662. Springer, 2012.

[5] Jesper Buus Nielsen, Peter Sebastian Nordholt, Claudio Orlandi, and Sai Sheshank Burra. A New Approach to Practical Active-secure Two-party Computation. In *Advances in cryptology –CRYPTO 2012*, pages 681–700. Springer, 2012.

[6] Ivan Damgård and Sarah Zakarias. Constant-overhead Secure Computation of Boolean Circuits Using Preprocessing. In *Theory of Cryptography Conference*, pages 621–641. Springer, 2013.

[7] Ivan Damgård, Marcel Keller, Enrique Larraia, Valerio Pastro, Peter Scholl, and Nigel P Smart. Practical Covertly Secure MPC for Dishonest Majority–or: Breaking the SPDZ Limits. In *European Symposium on Research in Computer Security*, pages 1–18. Springer, 2013.

[8] Marcel Keller, Emmanuela Orsini, and Peter Scholl. MASCOT: Faster Malicious Arithmetic Secure Computation with Oblivious Transfer. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 830–842, 2016.

[9] Ivan Damgård, Jesper Buus Nielsen, Michael Nielsen, and Samuel Ranellucci. The TinyTable Protocol for 2-party Secure Computation, or: Gate-scrambling Revisited. In *Advances in Cryptology –CRYPTO 2017*, pages 167–187. Springer, 2017.

[10] Ronald Cramer, Ivan Damgård, Daniel Escudero, Peter Scholl, and Chaoping Xing. SPD$\mathbb{Z}_{2^k}$: Efficient MPC mod $2^k$ for Dishonest Majority. In *Advances in Cryptology –CRYPTO 2018*, 2018.

[11] Marcel Keller, Valerio Pastro, and Dragos Rotaru. Overdrive: Making SPDZ Great Again. In *Advances in Cryptology –EUROCRYPT 2018*, pages 158–189. Springer, 2018.

[12] Dario Catalano, Mario Di Raimondo, Dario Fiore, and Irene Giacomelli. MonZa: Fast Maliciously Secure Two Party Computation on $\mathbb{Z}_{2^k}$. In *Public-Key Cryptography - PKC 2020*, pages 357–386. Springer, 2020.

[13] Andrew Chi Chih Yao. How to Generate and Exchange Secrets. In *Proceedings of the 27th Annual Symposium on Foundations of Computer Science*, pages 162–167, Toronto, Canada, 1986. IEEE.

[14] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game. In *Proceedings of the Nineteenth ACM Symposium on Theory of Computing*, pages 218–229. ACM, ACM, 1987.

[15] Donald Beaver. Efficient Multiparty Protocols using Circuit Randomization. In *Advances in Cryptology —CRYPTO 1991*, pages 420–432, Santa Barbara, USA, 1991. Springer.

[16] Marcel Keller, Peter Scholl, and Nigel P Smart. An architecture for practical actively secure mpc with dishonest majority. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 549–560, 2013.

[17] Payman Mohassel and Yupeng Zhang. SecureML: A system for scalable privacy-preserving machine learning. In *2017 IEEE symposium on security and privacy*, pages 19–38. IEEE, 2017.

[18] Hao Chen, Miran Kim, Ilya Razenshteyn, Dragos Rotaru, Yongsoo Song, and Sameer Wagh. Maliciously Secure Matrix Multiplication with Applications to Private Deep Learning. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 31–59. Springer, 2020.

[19] Pascal Reisert, Marc Rivinius, Toomas Krips, and Ralf Kuesters. Arithmetic Tuples for MPC. *Cryptology ePrint Archive*, 2022.

[20] Daniel Demmler, Thomas Schneider, and Michael Zohner. ABY-A Framework For Efficient Mixed-Protocol Secure Two-party Computation. In *Proceedings of the 22nd Annual Network and Distributed System Security Symposium*, San Diego, USA, 2015. Internet Society.

[21] Arpita Patra, Thomas Schneider, Ajith Suresh, and Hossein Yalame. ABY2.0: Improved Mixed-Protocol Secure Two-Party Computation. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 2165–2182, 2021.

[22] M Sadegh Riazi, Christian Weinert, Oleksandr Tkachenko, Ebrahim M Songhori, Thomas Schneider, and Farinaz Koushanfar. Chameleon: A hybrid secure computation framework for machine learning applications. In *Proceedings of the 2018 on Asia conference on computer and communications security*, pages 707–721, 2018.

[23] Sameer Wagh, Divya Gupta, and Nishanth Chandran. SecureNN: 3-Party Secure Computation for Neural Network Training. *Proceedings on Privacy Enhancing Technologies*, 2019(3):26–49, 2019.

[24] Deevashwer Rathee, Mayank Rathee, Nishant Kumar, Nishanth Chandran, Divya Gupta, Aseem Rastogi, and Rahul Sharma. Cryptflow2: Practical 2-party secure inference. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pages 325–342, 2020.

[25] Sameer Wagh, Shruti Tople, Fabrice Benhamouda, Eyal Kushilevitz, Prateek Mittal, and Tal Rabin. Falcon: Honest-majority maliciously secure framework for private deep learning. *Proceedings on Privacy Enhancing Technologies*, 2021(1):188–208, 2021.

[26] Zhicong Huang, Wen-jie Lu, Cheng Hong, and Jiansheng Ding. Cheetah: Lean and Fast Secure Two-Party Deep Neural Network Inference. *31th USENIX Security Symposium (USENIX Security 22)*, 2022:207, 2022.

[27] Amit Agarwal, Stanislav Peceny, Mariana Raykova, Phillipp Schoppmann, and Karn Seth. Communication efficient secure logistic regression. *Cryptology ePrint Archive*, 2022.

[28] Théo Ryffel, Pierre Tholoniat, David Pointcheval, and Francis Bach. Ariann: Low-interaction privacy-preserving deep learning via function secret sharing. *Proceedings on Privacy Enhancing Technologies*, 1:291–316, 2022.

[29] Linpeng Lu and Ning Ding. Horizontal Privacy-Preserving Linear Regression Which is Highly Efficient for Dataset of Low Dimension. In *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, pages 604–615, 2021.

[30] Chaochao Chen, Jun Zhou, Li Wang, Xibin Wu, Wenjing Fang, Jin Tan, Lei Wang, Alex X Liu, Hao Wang, and Cheng Hong. When homomorphic encryption marries secret sharing: Secure large-scale sparse logistic regression and applications in risk control. In *Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining*, pages 2652–2662, 2021.

[31] Payman Mohassel, Peter Rindal, and Mike Rosulek. Fast database joins and psi for secret shared data. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pages 1271–1287, 2020.

[32] John Liagouris, Vasiliki Kalavri, Muhammad Faisal, and Mayank Varia. Secrecy: Secure collaborative analytics on secret-shared data. *arXiv preprint arXiv:2102.01048*, 2021.

[33] Mahimna Kelkar, Phi Hung Le, Mariana Raykova, and Karn Seth. Secure poisson regression. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 791–808, 2022.

[34] Mike Rosulek and Ni Trieu. Compact and malicious private set intersection for small sets. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 1166–1181, 2021.

[35] Yanxue Jia, Shi-Feng Sun, Hong-Sheng Zhou, Jiajun Du, and Dawu Gu. Shuffle-based private set union: Faster and more secure. *31th USENIX Security Symposium (USENIX Security 22)*, 2022:2947–2964, 2022.

[36] Liang Feng Zhang, Huaxiong Wang, and Li-Ping Wang. Byzantine-Robust Private Information Retrieval with Low Communication and Efficient Decoding. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, pages 1079–1085, 2022.

[37] Dan Boneh, Elette Boyle, Henry Corrigan-Gibbs, Niv Gilboa, and Yuval Ishai. Lightweight techniques for private heavy hitters. In *2021 IEEE Symposium on Security and Privacy*, pages 762–776. IEEE, 2021.

[38] Yifeng Zheng, Weibo Wang, Songlei Wang, Xiaohua Jia, Hejiao Huang, and Cong Wang. Secskyline: Fast privacy-preserving skyline queries over encrypted cloud databases. *IEEE Transactions on Knowledge and Data Engineering*, 2022.

[39] Henry Corrigan-Gibbs, Alexandra Henzinger, and Dmitry Kogan. Single-server private information retrieval with sublinear amortized time. In *Advances in Cryptology –EUROCRYPT 2022*, pages 3–33. Springer, 2022.

[40] Elette Boyle, Niv Gilboa, and Yuval Ishai. Function secret sharing. In *Advances in Cryptology – EUROCRYPT 2015*, pages 337–367. Springer, 2015.

[41] Elette Boyle, Niv Gilboa, and Yuval Ishai. Function secret sharing: Improvements and extensions. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1292–1303, 2016.

[42] Elette Boyle, Niv Gilboa, and Yuval Ishai. Secure computation with preprocessing via function secret sharing. In *Theory of Cryptography Conference*, pages 341–371. Springer, 2019.

[43] Elette Boyle, Nishanth Chandran, Niv Gilboa, Divya Gupta, Yuval Ishai, Nishant Kumar, and Mayank Rathee. Function secret sharing for mixed-mode and fixed-point secure computation. In *Advances in Cryptology –EUROCRYPT 2021*, pages 871–900. Springer, 2021.

[44] Sameer Wagh. Pika: Secure computation using function secret sharing over rings. *Proceedings on Privacy Enhancing Technologies*, 4:351–377, 2022.

[45] Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, and Michele Orrù. Homomorphic secret sharing: optimizations and applications. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 2105–2122, 2017.

[46] Elette Boyle, Niv Gilboa, Yuval Ishai, Huijia Lin, and Stefano Tessaro. Foundations of Homomorphic Secret Sharing. In *9th Innovations in Theoretical Computer Science Conference (ITCS 2018)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.

[47] Elette Boyle, Lisa Kohl, and Peter Scholl. Homomorphic secret sharing from lattices without FHE. In *Advances in Cryptology –EUROCRYPT 2019*, pages 3–33. Springer, 2019.

[48] Stacey Truex, Nathalie Baracaldo, Ali Anwar, Thomas Steinke, Heiko Ludwig, Rui Zhang, and Yi Zhou. A hybrid approach to privacy-preserving federated learning. In *Proceedings of the 12th ACM workshop on artificial intelligence and security*, pages 1–11, 2019.

[49] Xiao Wang, Samuel Ranellucci, and Jonathan Katz. Authenticated garbling and efficient maliciously secure two-party computation. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, pages 21–37, 2017.

[50] Phillipp Schoppmann, Adrià Gascón, Leonie Reichert, and Mariana Raykova. Distributed vector-ole: Improved constructions and implementation. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 1055–1072, 2019.

[51] Elette Boyle, Niv Gilboa, Yuval Ishai, and Victor I Kolobov. Programmable distributed point functions. In *Annual International Cryptology Conference*, pages 121–151. Springer, 2022.

[52] Wenxing Zhu, Mengqi Wei, Xiangxue Li, and Qiang Li. Securebinn: 3-party secure computation for binarized neural network inference. In *European Symposium on Research in Computer Security*, pages 275–294. Springer, 2022.

[53] Niv Gilboa and Yuval Ishai. Distributed point functions and their applications. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 640–658. Springer, 2014.

[54] Samuel Dittmer, Yuval Ishai, Steve Lu, Rafail Ostrovsky, Mohamed Elsabagh, Nikolaos Kiourtis, Brian Schulte, and Angelos Stavrou. Function secret sharing for psi-ca: With applications to private contact tracing. *Cryptology ePrint Archive*, 2020.

[55] Samuel Dittmer, Yuval Ishai, Steve Lu, Rafail Ostrovsky, Mohamed Elsabagh, Nikolaos Kiourtis, Brian Schulte, and Angelos Stavrou. Streaming and unbalanced psi from function secret sharing. In *International Conference on Security and Cryptography for Networks*, pages 564–587. Springer, 2022.