分 类 号： TP309　　单位代码： 10422
密　　级： 公　开　　学　　号： 202117047

山东大学
SHANDONG UNIVERSITY

博士学位论文

Dissertation for Doctoral Degree

论文题目： **安全多方计算中的多方隐私集合运算研究**

Research on Multi-Party Private Set Operations in Secure Multi-Party Computation

作 者 姓 名　董明朗
培 养 单 位　网络空间安全学院
专 业 名 称　网络空间安全
指 导 教 师　陈宇
合 作 导 师

2026 年 5 月 29 日

原 创 性 声 明

本人郑重声明：所呈交的学位论文，是本人在导师指导下，独立进行研究所取得的成果。除文中已经注明引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的科研成果。对本论文的研究作出重要贡献的个人和集体，均已在文中以明确方式标明。本声明的法律责任由本人承担。

论文作者签名：_____ 日 期：_____

关于学位论文使用授权的声明

本人完全了解山东大学有关保留、使用学位论文的规定，同意学校保留或向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅；本人授权山东大学可以将本学位论文全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或其他复制手段保存论文和汇编本学位论文。

（保密的论文在解密后应遵守此规定）

论文作者签名：_____ 导师签名：_____ 日 期：_____

摘　要

随着大数据与人工智能技术的飞速发展，跨机构的数据融合与协同计算已成为释放数据价值的关键途径。然而，数据孤岛现象与日益严格的隐私保护法律法规之间的矛盾，使得如何在保护数据隐私的前提下实现数据价值的安全流通成为亟待解决的问题。作为安全多方计算（Secure Multi-party Computation, MPC）的重要分支，隐私集合运算（Private Set Operations, PSO）允许参与方在不泄露私有数据的前提下协同计算集合的交集、并集等信息。尽管两方场景下的技术已趋于成熟，但多方场景（Multi-Party Private Set Operations, MPSO）在安全性、实用性、功能性和统一性方面都存在严重不足，仍面临严峻挑战：一方面，现有的多方隐私集合求并（Multi-party Private Set Union, MPSU）协议或依赖不切实际的“非合谋假设”，难以抵御现实世界存在的任意共谋攻击，或在计算与通信复杂度上未能达到线性，性能难以满足实际应用的需求；另一方面，现有 MPSO 协议功能单一，难以满足现实场景中的复杂需求，且技术异构，开发部署维护成本高。目前学术界缺乏能够支持任意集合公式计算的 MPSO 统一框架。

针对上述挑战，本文深入研究了 MPSO 的核心理论与关键技术，从具体协议的突破到通用框架的构建，取得了一系列创新性成果：

首先，针对 MPSU 协议安全性弱与效率低下的痛点，本文提出了一种新的密码学组件——批量秘密分享隐私成员测试（batch secret-shared private membership test, batch ssPMT）协议，并以此为基础分别基于对称密钥技术和公钥密码技术提出了两种安全高效的 MPSU 协议。其中在对称技术路线中，本文构造了首个在标准半诚实模型下证明安全的基于对称密钥的 MPSU 协议。该协议不仅成功消除了之前的 SOTA 协议 [1] 对非共谋假设的依赖，显著增强了安全性，还表现出更加优异的具体性能。在局域网（LAN）环境下，其在线阶段的运行效率提升了 3.9 ∼ 10.0 倍，整体运行效率提升了 1.2 ∼ 7.8 倍。在公钥技术路线中，本文构造了首个同时实现线性计算复杂度和线性通信复杂度的 MPSU 协议，其总通信量相比于之前 SOTA 协议 [1] 降低了 3.0 ∼ 36.5 倍，在带宽受限的广域网（WAN）环境下具有显著优势。

其次，为了解决现有 MPSO 协议功能局限以及缺乏统一性的难题，本文通过引入新的密码学原语——谓词零分享（Predicative Zero-Sharing），基于对称密钥技术构建了首个实用的 MPSO 统一框架。该框架不仅能够计算由交、并、差运算任意组合构成的集合公式，还可扩展至支持更为复杂的任意集合公式结果求势（MPSO-card）及基于电路的通用 MPSO（Circuit-MPSO）功能。

最后，基于该 MPSO 框架，本文实例化了一系列安全高效的具体协议，填补了 MPSO 各个子领域的多项研究空白。其中，实例化的多方隐私集合求交（Multi-party Private Set Intersection, MPSI）协议是首个在标准半诚实模型下实现最优渐进复杂度（与明文传输方案相同量级）的基于对称密钥的 MPSI 方案，同时也是目前在线效率最高的 MPSI 协议，在 LAN 环境下比之前 SOTA 协议 [2] 快了 2.4 ∼ 5.2 倍；实例化的

多方隐私交集求势（MPSI-card）协议和多方隐私交集求势与和（MPSI-card-sum）协议是首个在标准半诚实模型下实现最优渐进复杂度的同类方案，其中 MPSI-card 协议具有目前同类协议中在线阶段的最佳性能，其在线通信量比 SOTA [3] 降低了 14.0 ∼ 20.3 倍，而 MPSI-card 协议是唯一拥有具体实现的同类方案；实例化的基于电路的 MPSI 协议（Circuit-MPSI）协议是首个在不诚实大多数设定下安全的同类方案，突破了 Circuit-MPSI 仅限于诚实大多数安全的局限；实例化的 MPSU 协议是标准半诚实模型下基于对称密钥的又一高效 MPSU 方案，在理论上实现了更优的渐进复杂度；实例化的多方隐私并集求势协议（MPSU-card）协议和基于电路的 MPSU 协议（Circuit-MPSU）是目前唯一可用的同类构造。此外，本文还探索了基于公钥体制的 MPSO 框架构造，完善了 MPSO 的理论技术体系。

关键词：安全多方计算；隐私集合运算；多方隐私集合运算；多方隐私集合求交；多方隐私集合求并

ABSTRACT

This document introduces a LaTeX template for writing doctoral dissertations at Shandong University. The template is designed to help doctoral students write and format their dissertations quickly and efficiently according to the school's requirements. The template includes format settings for the cover, abstract, table of contents, main text, references, etc., and provides detailed instructions and sample code. By using this template, users can focus on writing the content of the dissertation without worrying about formatting issues, thereby improving the efficiency and quality of dissertation writing.

This template is based on the sduthesis.cls template (https://github.com/Liam0205/sduthesis/), and I would like to thank the original author for his hard work. This template modifies some formats based on the referenced template, eliminates some warnings about fonts, and allows it to compile normally in my environment. However, due to my limited technical level, the template inevitably has some problems and shortcomings. I hope that users can criticize and correct them to improve them together.

Keywords: Shandong University; Doctoral Thesis; LaTeX Template

目 录

Contents

插 图 目 录

表 格 目 录

1 绪论

1.1 研究背景与意义

随着大数据、人工智能和云计算技术的飞速发展，数据已演变为驱动社会创新与经济增长的关键生产要素。政府部门、金融机构、医疗系统以及互联网企业积累了海量的高价值数据，通过跨机构的数据融合与联合分析，可以挖掘出更深层次的数据价值，赋能精准医疗、金融风控、联合营销等应用场景。然而，在数据共享的过程中，“数据孤岛”与“隐私保护”之间的矛盾日益凸显。

一方面，数据孤岛现象严重阻碍了数据价值的释放。出于商业机密保护或行政壁垒的考量以及对数据流失的担忧，各数据持有方往往不愿或不能将其私有数据直接对外开放。另一方面，日益严格的隐私保护法律法规对数据流通提出了极高的合规要求。欧盟的《通用数据保护条例》（GDPR）、中国的《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》等均明确规定，个人信息的处理必须遵循合法、正当、必要的原则，且严厉限制了未经授权的数据共享行为。如何在严格保护各方数据隐私及主权的前提下，实现数据的“可用不可见”，已成为学术界和产业界共同关注的焦点。

在这一背景下，安全多方计算（Secure Multi-party Computation, MPC）技术应运而生。作为密码学的一个重要分支，MPC 允许互不信任的多个参与方在不泄露各自私有输入的前提下，协同计算某个约定函数的输出。姚期智院士在 1982 年提出的“百万富翁问题”奠定了 MPC 的理论基础 [4]，随后 GMW 协议 [5] 和 BGW 协议 [6] 进一步完善了其通用框架。

尽管通用 MPC 协议在理论上能够计算任意函数，但在处理大规模数据集的实际应用中，将其编译为布尔电路或算术电路往往会带来巨大的计算和通信开销，难以满足高频、海量数据场景下的实时性需求。因此，针对特定功能设计高效的**专用 MPC 协议**成为了该领域的重要研究方向。在众多专用协议中，**隐私集合运算（Private Set Operations, PSO）**因其在现实场景中的广泛适用性而备受瞩目，以 Google、Facebook、Microsoft 等为代表的科技公司投入了大量资源研究 PSO 技术。PSO 允许参与方在各自持有私有集合的前提下，协同完成对私有集合的计算，且不泄露任何额外信息。根据参与方的数量，PSO 可划分为**两方隐私集合运算**和**多方隐私集合运算（Multi-party Private Set Operations, MPSO）**。

两方 PSO 因只涉及两个输入集合 X、Y，通常只考虑计算交集 $X \cap Y$ 和并集 $X \cup Y$，功能相对局限。具体地，两方 PSO 主要包括以下三类功能：

- **两方隐私集合求交（Private Set Intersection, PSI）.** 允许持有隐私集合的双方共同计算交集 $X \cap Y$。该技术已广泛应用于隐私保护下的联系人发现 [7]、广告转化率归因 [8] 等场景。

- **两方隐私交集计算（Private Computation on Set Intersection, PCSI）.** 在不泄露交集的前提下，允许持有隐私集合的双方共同计算交集 $X \cap Y$ 的部分或汇总信息（如基数或关联数据之和）。这在需要统计分析但严禁泄露个体身份的场景（如打击儿童性虐待材料传播 [9]、疫情流调统计 [10]）中至关重要。

- **两方隐私集合求并（Private Set Union, PSU）.** 允许持有隐私集合的双方共同计算并集 $X \cup Y$。常用于两家机构联合构建全量的 IP 黑名单库或漏洞数据库 [11]。

目前，两方 PSO 技术已相对成熟。特别是两方 PSI 取得了巨大进展 [12, 13, 14, 15, 16, 17, 18]，现有最先进的协议 [18] 已能实现与不安全的朴素哈希 PSI 方案相当的性能。近年来，两方 PCSI 和两方 PSU 也迅猛发展，出现了一系列高效且安全的两方 PCSI [19, 20] 和两方 PSU [21, 19, 22, 23, 20, 24] 协议构造，并形成了统一的两方 PSO 框架 [20]，开始在实际业务中逐步大规模落地。

与两方场景不同，MPSO 涉及多个输入集合 $X_1, \ldots, X_m$ $(m > 2)$。由于集合运算的组合方式呈指数级增长，理想条件下的 MPSO 协议应该能够计算由有限次二元集合运算（包括交集、并集和差集）组成的任意集合公式 $f(X_1, \ldots, X_m)$。[1]这使得 MPSO 涵盖了更加丰富的功能。然而，目前 MPSO 的研究主要聚焦于以下四类特定功能：

- **多方隐私集合求交（Multi-party Private Set Intersection, MPSI）.** 允许 m $(m > 2)$ 个参与方分别持有隐私集合 X_i $(1 \le i \le m)$，最终准确地共同计算出所有集合的交集 $\bigcap_{i=1}^{m} X_i$。其典型应用包括隐私保护下的位置信息共享 [7]、隐私通讯录的公共联系人发现 [25]、DNA 检测和模式匹配 [26]、以及联合僵尸网络检测等。

- **多方隐私交集计算（Multi-party Private Computation on Set Intersection, MPCSI）.** 允许 m 个参与方分别持有隐私集合 X_i，最终输出交集 $\bigcap_{i=1}^{m} X_i$ 的部分或汇总信息。MPCSI 主要包括基于电路的 MPSI 协议（Circuit-MPSI）、多方隐私交集求势协议（MPSI-card）和多方隐私交集求势与和协议（MPSI-card-sum）。其中，Circuit-MPSI 允许参与方在交集上计算任意函数 $f(\bigcap_{i=1}^{m} X_i)$；MPSI-card 用于计算交集的基数；MPSI-card-sum 用于计算交集基数及对应权值的总和。这类功能被广泛应用于在线广告效果评估 [8]、打击儿童性虐待材料（CSAM）传播 [9] 以及 COVID-19 隐私接触者追踪 [10, 27, 28]。

- **多方隐私集合求并（Multi-party Private Set Union, MPSU）.** 允许 m 个参与方分别持有隐私集合 X_i，最终准确地共同计算出所有集合的并集 $\bigcup_{i=1}^{m} X_i$。该功能是信息安全风险评估 [29]、IP 黑名单和漏洞数据聚合 [11]、联合图计算 [30]、分布式网络监控 [31] 的核心技术，也是构建支持全连接的隐私数据库 [21] 和 Private ID 协议 [19] 的核心组件。

[1]在 MPSO 中，通常规定仅由一名参与方（称为 Leader）获得结果集合，而其他参与方（称为 Client）无法获取除自身输入外的任何信息。

- **多方隐私并集计算(Multi-party Private Computation on Set Union, MPCSU)**. 允许 m 个参与方分别持有隐私集合 X_i，最终输出并集 $\bigcup_{i=1}^{m} X_i$ 的部分或汇总信息。MPCSU 主要包括基于电路的 MPSU 协议（Circuit-MPSU）和多方隐私并集求势协议（MPSU-card)。该类功能同样存在许多潜在应用，例如，政府卫生部门可以通过 MPSU-card 协议统计某月内所有医院确诊某类传染病的总人数（即并集基数)，而在统计过程中不泄露任何患者的具体身份。

虽然多方场景赋予了 MPSO 更加广阔的应用前景，但其复杂性导致了两方场景下的成熟技术无法直接迁移，进一步增加了 MPSO 协议设计的难度与挑战。具体地，MPSO 领域面临着以下的重大挑战：

1. **安全性弱.** 许多现有的 MPSO 协议(甚至是部分最新的研究成果，如 [1, 32, 33, 34])的安全性依赖于“非共谋假设”（Non-collusion Assumption)，即假设某些参与方之间不会共谋。该假设在现实世界的开放网络环境或存在利益冲突的商业合作中难以成立，导致这些协议难以抵御实际场景中的任意共谋攻击，一旦落地存在严重的安全风险。

2. **效率低下.** 现有的 MPSO 协议的构造主要遵循两类技术路线，包括基于公钥密码技术的路线和基于不经意传输（Oblivious Transfer, OT）与对称密钥技术的路线。前者由于涉及大量昂贵的公钥操作，实际运行效率极低；后者虽然执行速度快，但渐进复杂度较差。目前的各类 MPSO 协议尚未能做到统筹兼顾，难以在保证理论最优性的同时实现实际可用的性能。

3. **功能局限.** 现有的 MPSO 协议功能单一，缺乏对计算任意集合公式的支持，难以满足现实场景中的复杂需求。例如，公共卫生部门希望筛选某项健康计划的候选人，条件是“患有特定疾病”且“收入低于特定标准”。这需要各医院首先联合计算患病人员的**并集**，随后与福利部门的低收入名单计算**交集** [31]。这种“先求并、再求交”的复合运算超出了现有仅关注单一功能的 MPSO 协议的能力范畴，缺乏实用的专用解决方案。

4. **缺乏统一性.** 现有的 MPSO 研究呈现出严重的“功能孤岛”特征。研究工作大多聚焦于某一特定功能（如仅针对 MPSI 或仅针对 MPSU）的优化，并采用了异构的技术路线，导致产生了大量孤立的协议，缺乏一个统一的理论框架。这种现状不仅增加了系统的开发与维护成本，也使得难以通过模块化组合来应对复杂多变的业务需求。

针对上述背景与挑战，本文致力于研究安全、高效的多方隐私集合运算协议，并构建支持任意集合公式计算的多方隐私集合运算统一框架，从而解决现有 MPSO 领域安全性弱、效率低下、功能局限及缺乏统一性等关键问题，为打破数据孤岛、促进数据要素的安全流通提供坚实的技术支撑。

1.2 研究现状

据粗略估计，多方隐私集合运算（MPSO）领域的相关研究文献已达数百篇，且正以指数级的速度增长。然而，在这海量的文献中，大部分工作并未给出严谨的安全性证明。即便着眼于那些提供了安全性证明的文献，许多协议在安全性假设或正确性保障上仍存在显著局限。例如，部分协议 [35, 36, 37, 38, 1, 32, 33, 34] 引入了云服务器辅助（Server-Aided）模型或依赖于“特定参与方不共谋”的非共谋假设，这使其难以抵御现实应用场景中复杂的任意共谋攻击；另一些协议 [39, 40] 则存在不可忽略的假阳性率（False Positives），即以不可忽略的概率错误地将原本不属于结果集合的元素包含在协议输出中，这在金融风控误报、医疗误诊等高敏感场景下是不可接受的。

鉴于此，本文将重点关注那些在标准半诚实模型下安全（即能够抵抗任意参与方的共谋）、且协议输出的错误概率可忽略的 MPSO 协议。同时，为了梳理技术演进脉络，本文也会回顾部分虽然未完全达到标准半诚实安全，但其构造思想对后续工作产生深远影响的经典协议。

目前 MPSO 的研究分布呈现出极端的不均衡性：多方隐私集合求交（MPSI）占据 90% 以上的比例，得到了广泛的研究 [41, 31, 42, 43, 44, 45, 46, 47, 2]；多方隐私集合求并（MPSU）受到的关注相对稀缺 [31, 48, 49]。不过，随着近年来 Liu 和 Gao [1] 等高影响力工作的发表，该方向的研究热度正出现上涨趋势。至于多方隐私交集计算（MPCSI）和多方隐私并集计算（MPCSU），相关的安全协议寥寥无几 [31, 3, 50]。特别是在不诚实大多数（Dishonest Majority）[2]设定下，学术界甚至尚未有工作能够实现 Circuit-MPSI、MPSU-card 以及 Circuit-MPSU 协议。

下面我们将分类详细阐述各类协议的研究现状。

1.2.1 多方隐私集合求交

作为 MPSO 中研究最为深入的功能，MPSI 协议主要遵循两条技术路线：基于公钥密码技术的路线和基于对称密钥技术的路线。

基于公钥密码技术的 MPSI. Freedman 等人 [41] 基于不经意多项式求值（Oblivious Polynomial Evaluation, OPE）提出了首个 MPSI 协议，其中 OPE 利用加法同态加密（Additively Homomorphic Encryption, AHE）实现。Kissner 和 Song [31] 同样利用 OPE 技术结合多项式表示提出了一个 MPSI 协议。然而，这两个协议的计算复杂度对于每个参与方而言均为集合大小 n 的二次方，导致其实际效率低下，根本难以应用于大规模数据集。

[2]不诚实大多数要求敌手腐化参与方数量的阈值 t 满足 $t \geq m/2$，而标准半诚实安全要求 $t = m-1$（即最大腐化阈值）。安全性依赖于非共谋假设的协议不满足半诚实安全定义，但往往能实现不诚实大多数。

基于对称密钥技术的 MPSI. 近年来，基于不经意传输（OT）和对称密钥操作的 MPSI 协议因其实际可用的效率成为了研究主流。Kolesnikov 等人 [43] 提出了两个 MPSI 协议：第一个协议实现了最优渐进复杂度[3]，但仅在增强半诚实模型（Augmented Semi-Honest Model）下安全。（增强半诚实模型的安全性要弱于标准半诚实模型，关于两者的关系详见文献 [51] 的 2.4.4 节）。第二个协议虽然在标准半诚实模型下安全，但 Client 的复杂度依赖于腐化阈值 t，未能达到最优。

Garimella 等人 [45] 通过提出并优化不经意键值存储（Oblivious Key-Value Store, OKVS）[16, 18, 52] 对上述协议的效率进行了改进，并证明了第一个协议实际上支持恶意安全。在此基础上，Nevo 等人 [46] 进一步优化了 $t < m - 1$ 设定下的恶意 MPSI 协议。Inbar 等人 [44] 基于 OT 和混淆布隆过滤器（Garbled Bloom Filter），分别在增强半诚实和标准半诚实模型下各提出了一个 MPSI 协议，但其每个参与方的计算复杂度均为 $O(mn)$。Ben-Efraim 等人 [47] 随后将其扩展至恶意安全模型。

最近，Wu 等人 [2] 基于不经意伪随机函数（OPRF）和 OKVS 提出了两个满足标准半诚实安全的 MPSI 协议，展现出了优于前人工作的性能，但其 Client 的复杂度依然依赖于腐化阈值 t，并非最优。

综上所述，尽管 MPSI 领域的研究已相当成熟，但目前尚无满足标准半诚实安全的基于对称密钥技术的 MPSI 协议能够达到与 [43] 中增强半诚实协议相同的最优渐进复杂度。

1.2.2 多方隐私交集计算

MPCSI 旨在计算交集的统计信息而非交集本身。目前仅有极少数工作关注了其中的 MPSI-card 和 MPSI-card-sum 这两类功能。

多方隐私交集求势 / 求势与和. Kissner 和 Song [31] 的方案虽然在理论上支持 MPSI-card 功能，但由于依赖昂贵的同态加密，其构造效率低下，仅具备理论价值。Chen 等人 [3] 提出了首个基于 OT 和对称密钥操作的 MPSI-card 和 MPSI-card-sum 协议，这也是目前在标准半诚实模型下唯一实用的同类协议。然而，其协议复杂度尚未达到最优，其中 Leader 的复杂度为 $O(mn + tn \log n)$，Client 的复杂度为 $O(tn)$（t 为腐化阈值）。

综上所述，目前尚无满足标准半诚实安全的 MPSI-card 和 MPSI-card-sum 协议能够实现最优渐进复杂度，且现有方案的实际运行效率仍有较大的提升空间。此外，目前学术界尚缺乏满足标准半诚实安全性的 Circuit-MPSI 协议。

[3]在 MPSI 和 MPCSI 中，最优渐进复杂度定义为 Leader 的计算和通信复杂度均为 $O(mn)$，且每个 Client 的计算和通信复杂度均为 $O(n)$（其中 n 为集合大小，m 为参与方数量）。这是因为在不考虑隐私的朴素方案中（即各 Client 直接发送集合给 Leader，由 Leader 直接计算出结果集合），所需的复杂度即为此量级。

1.2.3 多方隐私集合求并

与 MPSI 相比，MPSU 的研究相对滞后且挑战更大。现有的 MPSU 工作同样主要分为基于公钥密码技术和基于对称密钥技术两类。

基于公钥密码技术的 MPSU. Kissner 和 Song [31] 基于多项式表示和加法同态加密（AHE）提出了首个 MPSU 协议。但由于涉及大量的 AHE 操作和高次多项式计算，该协议完全不具备实用性。Frikken [48] 通过降低多项式次数改进了 [31]，但该协议仍需对加密多项式进行多点求值，导致 AHE 的操作次数仍高达 $O(n^2)$，其实际效率难以满足大规模应用需求。

Vos 等人 [40] 提出了一种基于位向量表示和 ElGamal 加密的 MPSU 协议，通过对位向量执行隐私 OR 操作来计算并集。然而，据 Liu 和 Gao [1] 的实验报告，该协议的具体效率较差（例如，在 10 个参与方、每方集合大小为 2^{10} 的规模下，运行时间长达 75 秒），且 Leader 的计算和通信复杂度随参与方数量 m 呈二次增长。

最近，Gao 等人 [49] 基于多密钥重随机化公钥加密（Multi-Key Rerandomizable Public-Key Encryption, MKR-PKE）提出了一种渐进复杂度较优的 MPSU 协议。尽管该协议是目前渐进复杂度最佳的 MPSU 协议，但其仍未能达到线性复杂度[4]。

基于对称密钥技术的 MPSU. Liu 和 Gao [1] 提出了首个 (也是目前唯一一个) 基于 OT 和对称密钥操作的 MPSU 协议。该协议在性能上取得了巨大突破，是首个实际可用的 MPSU 协议。在 3 方参与，每个参与方的集合大小为 2^{10} 的设定下，该协议比 [40] 快了 109 倍。然而，该协议的安全性依赖于“非共谋假设”，无法在标准半诚实模型下证明安全。

此外，Blanton 等人 [36] 基于不经意排序和通用 MPC 构造了 MPSU，但由于严重依赖通用 MPC，效率极低。

综上所述，目前尚不存在基于对称密钥技术且满足标准半诚实安全的 MPSU 协议，现有方案在安全性与实用性之间存在权衡。此外，在理论层面，目前也未有 MPSU 协议能够实现严格的线性复杂度。

1.2.4 多方隐私集合运算框架

构建能够支持任意集合公式计算（后文中我们统称该功能为通用 MPSO 功能）的 MPSO 框架是该领域长期以来的一个开放性问题。Kissner 和 Song [31] 在 MPSO 发展的早期阶段就尝试构建一个 MPSO 框架，但该框架并未能完全实现通用 MPSO 功能。其方案仅支持计算由交集和并集组成的集合公式，无法处理差集运算（例如计算

[4]在 MPSU 中，线性复杂度意味着每个参与方的复杂度与所有参与方集合大小的总和呈线性关系。本文考虑平衡设定，即每个参与方持有的集合大小相等，因此线性复杂度指每个参与方的复杂度与参与方数量 m 和集合大小 n 均呈线性关系。

$X_2 \setminus (X_1 \cap X_3))$，且严重依赖于加法同态加密，计算成本极高。Blanton 和 Aguiar [36] 通过重新设计集合运算电路，并结合通用 MPC 协议，实现了对交、并、差运算的任意组合的计算支持。尽管该方案依靠通用 MPC 技术在功能上实现了通用性，但这也带来了巨大的计算开销。例如，其实验报告中仅针对 3 个参与方、每方 2^{11} 个元素的最基础 MPSI 任务，耗时就长达 24.8 秒，且仅支持诚实大多数（Honest Majority）设定。

综上所述，目前学术界尚缺乏一个在标准半诚实模型下，既能完全实现通用 MPSO 功能（支持任意集合公式计算），又具备实际可用效率的统一框架。

1.3 本文主要贡献

针对目前多方隐私集合运算（MPSO）领域在安全性、效率、功能完备性及统一性方面存在的显著不足，以及研究资源在不同功能间分布极度不均衡的现状，本文开展了系统性的研究工作，主要研究内容和贡献总结如下：

1.3.1 多方隐私集合求并协议的研究

首先，本文从应用价值巨大但研究相对匮乏的多方隐私集合求并（MPSU）入手，直面现有 MPSU 协议面临的“安全性弱”（依赖于非共谋假设）与“效率低下”（实际性能难以支撑应用或理论复杂度未达线性）两大核心痛点，分别基于对称密钥和公钥体制提出了安全高效的解决方案：前者是首个在标准半诚实模型下证明安全的实际可用的 MPSU 协议，后者则是首个在理论上实现线性复杂度的 MPSU 协议。

具体创新点和贡献如下：

1. **高效的批量秘密分享隐私成员测试（batch ssPMT）原语.** 本文深入分析了现有唯一的基于对称密钥技术的 MPSU 协议 [1]，并针对其核心组件——多查询秘密分享隐私成员测试（multi-query secret-shared private membership test, mq-ssPMT）协议，抽象出一种全新的原语——批量秘密分享隐私成员测试（batch secret-shared private membership test, batch ssPMT）。相比于 mq-ssPMT 的实例化严重依赖于昂贵的通用 MPC 技术所导致的性能瓶颈，本文提出的 batch ssPMT 能够仅利用轻量级密码学组件进行高效实例化。通过结合哈希分桶（hashing-to-bins）技术，该原语能够在不引入任何额外信息泄露的前提下，完全替代现有基于对称密钥技术的 MPSU 框架中的 mq-ssPMT 组件。该原语不仅构成了本文两个 MPSU 协议的核心构建模块，其高效的构造也是协议实际性能获得显著提升的关键所在。此外，该原语在本文后续构建的 MPSO 框架中也发挥着关键作用，被用于高效构造其核心共性子协议——成员零分享（Membership Zero-Sharing）协议，从而为任意集合公式的计算提供了底层支撑。

2. **首个标准半诚实模型下基于对称密钥的 MPSU 协议.** 本文将随机不经意传输（Random Oblivious Transfer, ROT）的概念推广至多方场景，定义并构造了多方秘密分享随机不经意传输（multi-party secret-shared ROT, mss-ROT）原语。基于 batch ssPMT 和 mss-ROT，本文提出了首个在标准半诚实模型下证明安全且基于对称密钥技术的 MPSU 协议。该协议不仅成功消除了现有基于对称密钥的方案对非合谋假设的依赖，显著增强了安全性，还表现出更加优异的具体性能。特别是在局域网（LAN）环境下，其在线阶段的运行效率比 SOTA 协议 [1] 提升了 3.9 ∼ 10.0 倍，整体运行效率提升了 1.2 ∼ 7.8 倍。

3. **首个具有线性复杂度的 MPSU 协议.** 基于 batch ssPMT 和多密钥重随机化公钥加密（Multi-Key Rerandomizable Public-Key Encryption, MKR-PKE）[53]，本文提出了首个同时实现线性计算复杂度和线性通信复杂度的 MPSU 协议。得益于其优越的渐进复杂度，该协议极大地降低了通信开销。实验数据显示，相比于 SOTA 协议 [1]，该协议的总通信量降低了 3.0 ∼ 36.5 倍，使其在带宽受限的广域网（WAN）环境下具有显著的应用优势。

1.3.2 多方隐私集合运算框架的研究

为了突破 MPSO 领域“功能局限”与“缺乏统一性”的瓶颈，本文随后聚焦于支持任意集合公式计算的通用 MPSO 功能，在标准半诚实模型下，利用不经意传输（OT）与对称密钥技术，构建了首个能够高效实现通用 MPSO 功能的统一框架，并将该框架进一步扩展，实现了更为复杂的任意集合公式结果求势（MPSO-card）及基于电路的通用 MPSO（Circuit-MPSO）功能。

具体创新点和贡献如下：

- **任意集合公式的统一谓词公式表示.** 为了解决现有 MPSO 框架在表示层面的两极化难题——要么将目标集合公式表示为交、并及元素规约（element reduction）操作的组合导致通用性受限 [31]，要么直接基于集合代数运算的组合导致协议严重依赖于通用 MPC 从而效率低下 [36]，本文引入了一种名为“规范集合谓词公式”（Canonical Set Predicate Formula, CSPF）的新型表示方法，将目标集合公式表示为一类由原子集合谓词（形如 $x \in X_i$ 或 $x \notin X_i$）构成的析取范式，其中每个子公式满足特定的结构，子公式共同表示了目标集合的一个划分。本文严格证明了任意集合公式均可转化为 CSPF 表示，且 CSPF 的结构特性（如子公式数量）直接决定了协议的性能。

- **谓词零分享（Predicative Zero-Sharing）与其松弛定义.** 本文提出了一类新型的密码学原语“谓词零分享”（Predicative Zero-Sharing）。该原语表示一族协议，其中每个协议均关联一个谓词公式，如果该公式在所有参与方输入上的真值为真，

那么各方输出 0 的加法秘密分享；否则，输出随机值的加法秘密分享。本文首先给出了一种简化的、基于模拟范式的谓词零分享安全性定义，并严格证明了其与标准半诚实安全定义的等价性。基于此定义，本文进一步提出了谓词零分享的松弛版本（Relaxed Predicative Zero-Sharing），该版本具有极强的抽象能力，能够涵盖随机不经意传输（ROT）、等值条件随机数生成（ECRG）[24] 等现有原语。在此基础上，本文建立了针对松弛谓词零分享的**组合技术（Composition Technique）**与**转化技术（Transformation Technique）**。结合这两项技术，可以以模块化的方式，从关联于原子命题（或其否定）的松弛谓词零分享出发，自底向上地构造出关联于任意复杂谓词公式的、满足标准半诚实安全的谓词零分享协议。这一通用的构造范式是本文 MPSO 框架能够灵活支持任意集合公式计算、并保持协议结构统一性的核心技术支撑。

- **高效的成员零分享（Membership Zero-Sharing）原语.** 为了将谓词零分享这一抽象原语应用于具体的集合运算，本文引入了其在 MPSO 场景下的特化实例——“成员零分享”（Membership Zero-Sharing）。具体而言，该协议指定一名参与方（记作 P_{pivot}）输入单个元素 x，而其他每个参与方 P_i 输入集合 X_i。每个协议实例均关联一个由原子集合谓词 $x \in X_i$ 和 $x \notin X_i$ 通过逻辑与 AND、逻辑或 OR 操作符连接而成的集合谓词公式。如果 P_{pivot} 的输入元素 x 使得该公式成立，则各方输出 0 的加法秘密分享；否则，输出随机值的加法秘密分享。基于不经意可编程伪随机函数（oblivious programmable pseudorandom function, OPPRF）、批量秘密分享隐私成员测试（batch ssPMT）和随机不经意传输（ROT）等轻量级组件，本文分别针对 $x \in X_i$ 和 $x \notin X_i$ 给出了成员零分享的松弛版本（Relaxed Membership Zero-Sharing）的高效实例化。进而，遵循任意谓词零分享的通用构造范式，本文成功实例化了关联于任意集合谓词公式的标准安全成员零分享协议。该协议作为 MPSO 统一框架的核心底层组件，成功弥合了 MPSO 领域中“通用性”与“实用性”之间的鸿沟：其对任意集合谓词公式的支持赋予了框架计算任意集合运算的通用能力，而其基于轻量级组件的高效实例化则保障了框架优异的实际性能。

- **实现通用 MPSO 功能的统一框架及其扩展.** 基于上述集合公式的统一表示和成员零分享协议作为底层原语，本文构建了支持任意集合公式计算的 MPSO 统一框架：首先，利用 CPSF 表示法将目标集合公式转化为若干结构化的子公式；随后，针对每一个子公式，参与方以各自的隐私集合为输入，调用关联于该子公式的标准安全成员零分享协议，生成关于目标集合元素的加法秘密分享序列；为了消除该秘密分享顺序可能泄露的元数据信息（如元素来源），参与方调用多方秘密分享洗牌（multi-party secret-shared shuffle）协议对所有分享进行随机置换。为实现标准 MPSO 功能，打乱后的秘密分享将被直接发送给结果接收方进行重构，通过特定的编码格式筛除随机值后即可恢复出目标集合。此外，得益于洗牌后的输出仍保持秘密分享的形式，该框架具有极强的扩展性，首次实现了更为复杂的任意集

合公式结果求势（MPSO-card）及基于电路的通用 MPSO（Circuit-MPSO）功能：若应用场景仅需输出集合的统计信息或需进行后续保密计算，参与方可直接对秘密分享进行操作（如统计有效分享数量以计算基数，或将秘密分享作为输入馈送至通用 MPC 电路计算关于结果集合的任意函数）。

除了上述对 MPSO 框架的研究本身做出的理论贡献外，通过对该框架进行实例化，本文在 MPSO 的各个具体子领域亦取得了突破性进展，解决了一系列长期存在的开放性问题。具体贡献点如下：

- **多方隐私集合求交.** 基于本文框架实例化的 MPSI 协议是首个在标准半诚实模型下实现**最优渐进复杂度**（即达到与不考虑隐私的明文传输方案相同量级的复杂度——Leader 的计算与通信复杂度为 $O(mn)$，Client 的计算与通信复杂度为 $O(n)$）基于对称密钥技术的 MPSI 构造。此前达到该复杂度的协议 [43] 仅在增强半诚实模型（Augmented Semi-Honest）下安全，本文填补了这一空白。同时，该协议也是目前在线效率最高的 MPSI 协议，在 LAN / WAN 环境下比 SOTA 协议 [2] 快 2.4 ∼ 5.2 / 1.1 ∼ 2.6 倍。

- **多方隐私交集计算.** 基于本文框架实例化的 MPSI-card 和 MPSI-card-sum 协议是首个在标准半诚实模型下实现**最优渐进复杂度**的 MPSI-card 和 MPSI-card-sum 协议。其中，MPSI-card 协议也是目前在线阶段最高效的同类协议，其在线通信量比 SOTA [3] 降低了 14.0 ∼ 20.3 倍；MPSI-card-sum 协议是目前唯一一个给出了具体实现的同类协议，实验表明其计算与通信开销仅约为前述 MPSI 协议的两倍。此外，基于本框架实例化的 Circuit-MPSI 协议是首个在**不诚实大多数（Dishonest Majority）**设定下安全的 Circuit-MPSI 协议，突破了以往工作仅限于诚实大多数（Honest Majority）安全的局限。

- **多方隐私集合求并.** 基于本文框架实例化的 MPSU 协议是标准半诚实模型下基于对称密钥的另一高效 MPSU 方案。尽管其实际计算性能略逊于本文第三章提出的 MPSU 协议，但其在理论上实现了**更优的渐进复杂度**，并且其在线通信开销降低了 1.8 倍，因此在带宽受限网络中具有更强的竞争力。

- **多方隐私并集计算.** 基于本文框架实例化的 MPSU-card 和 Circuit-MPSU 协议是目前**唯一可用**的 MPSU-card 和 Circuit-MPSU 构造，其性能与该框架下实例化的 MPSU 协议基本相同。

最后，作为对基于对称密钥的 MPSO 框架的补充，本文在第六章提出了一个**基于公钥体制的 MPSO 框架**，同样实现了通用的 MPSO 功能（该框架的扩展能力略弱于对称密钥版本，可实现 MPSO-card 功能但无法实现 Circuit-MPSO 功能）。尽管受限于公钥密码操作昂贵的计算开销，该框架实际运行效率较低，但其在渐进复杂度上相比对

称密钥版本具有独特的理论优势。这一工作与对称密钥框架互为补充，共同构建了涵盖实用性能与理论边界的完整 MPSO 技术体系。

1.4 本文组织结构

本文共分为七章，各章节的组织结构安排如下：

第一章 绪论：阐述了本文的研究背景与意义，系统地梳理了隐私集合运算领域研究现状，总结了现有技术面临的难题和挑战，并介绍了本文的主要研究内容与创新贡献。

第二章 预备知识：定义了本文使用的符号系统，详细描述了标准半诚实安全模型及基于模拟范式的安全性定义。同时，回顾了不经意传输、秘密分享、伪随机函数、哈希分桶等本文后续章节所需的基础密码学组件。

第三章 基于对称密钥的高效多方隐私集合求并协议：针对现有高效 MPSU 协议依赖非合谋假设的缺陷，提出了一种基于不经意传输和对称密钥操作的 MPSU 协议。本章详细描述了核心原语“批量秘密分享隐私成员测试”与“多方秘密分享随机不经意传输”的构造，给出了协议的具体流程与安全性证明，并通过实验展示了其在局域网环境下的性能优势。

第四章 基于公钥体制的线性多方隐私集合求并协议：针对广域网环境下通信瓶颈问题，提出了一种具有线性通信复杂度的 MPSU 协议。本章详细阐述了基于多密钥重随机化公钥加密的协议构造，重点分析了其在渐进复杂度上的理论突破，并通过实验对比验证了其在低带宽环境下的优越性。

第五章 基于对称密钥的通用多方隐私集合运算框架：为了解决协议功能单一的问题，本章构建了首个支持任意集合公式计算的 MPSO 统一框架。本章引入了“规范集合谓词公式”表示法和“谓词零分享”原语，详细描述了从底层原语到通用框架的自底向上构造过程，并给出了 MPSI、MPCSI 及 MPSU 等多种功能的实例化协议及其性能评估。

第六章 基于公钥体制的通用多方隐私集合运算框架：作为对第五章的理论补充，本章探讨了基于公钥体制的通用框架构造。本章引入了“谓词加密零”原语，构建了相应的通用框架，并重点讨论了其在渐进复杂度上的理论特性，从而与对称密钥框架共同构成了完整的技术体系。

第七章 总结与展望：对全文的研究成果进行了系统总结，并结合当前领域的发展趋势，对多方隐私集合运算未来的研究方向（如恶意模型下的安全性扩展、非平衡集合场景的优化等）进行了展望。

2 预备知识

2.1 符号说明

2.2 安全模型

2.3 基本组件

3 基于对称密钥的高效多方隐私集合求并协议

3.1 引言

3.2 批量秘密分享隐私成员测试

3.3 协议构造及安全性证明

3.4 复杂度分析与对比

3.5 本章小结

4 基于公钥体制的线性多方隐私集合求并协议

4.1 引言

4.2 协议构造及安全性证明

4.3 复杂度分析与对比

4.4 MPSU 协议的实现与性能评估

4.5 本章小结

5 基于对称密钥的通用多方隐私集合运算框架

5.1 引言

5.2 规范集合谓词公式表示

5.3 谓词零分享

5.4 成员零分享

5.5 框架构造及安全性证明

5.6 本章小结

6 基于对称密钥的实例化协议与综合性能评估

6.1 引言

6.2 多方隐私集合求交、求势及电路 MPSI

6.3 多方隐私交集求势与和

6.4 多方隐私集合求并、求势及电路 MPSU

6.5 实现与综合性能评估

6.6 本章小结

7 基于公钥体制的通用多方隐私集合运算框架

7.1 引言

7.2 谓词零加密

7.3 成员零加密

7.4 框架构造

7.5 典型实例化

7.6 理论分析与对比

7.7 本章小结

8 总结与展望

8.1 全文总结

8.2 未来工作展望

参考文献

[1] X. Liu and Y. Gao, "Scalable multi-party private set union from multi-query secret-shared private membership test," in *ASIACRYPT 2023*, Springer, 2023.

[2] M. Wu, T. H. Yuen, and K. Y. Chan, "O-ring and k-star: Efficient multi-party private set intersection," in *USENIX Security 2024*, 2024.

[3] Y. Chen, N. Ding, D. Gu, and Y. Bian, "Practical multi-party private set intersection cardinality and intersection-sum under arbitrary collusion," in *Inscrypt 2022*, Lecture Notes in Computer Science, Springer, 2022.

[4] A. C.-C. Yao, "Theory and applications of trapdoor functions (extended abstract)," in *23rd Annual Symposium on Foundations of Computer Science, FOCS 1982*, pp. 80–91, IEEE Computer Society, 1982.

[5] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game or A completeness theorem for protocols with honest majority," in *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987*, pp. 218–229, ACM, 1987.

[6] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract)," in *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, 1988*, pp. 1–10, ACM, 1988.

[7] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location privacy via private proximity testing," in *NDSS 2011*, 2011.

[8] M. Ion, B. Kreuter, A. E. Nergiz, S. Patel, S. Saxena, K. Seth, M. Raykova, D. Shanahan, and M. Yung, "On deploying secure computing: Private intersection-sum-with-cardinality," in *IEEE European Symposium on Security and Privacy, EuroS&P 2020*, pp. 370–389, IEEE, 2020.

[9] A. Bhowmick, D. Boneh, S. Myers, K. Talwar, and K. Tarbe, "The apple psi system," 2021.

[10] A. Berke, M. Bakker, P. Vepakomma, R. Raskar, K. Larson, and A. Pentland, "Assessing disease exposure risk with location histories and protecting privacy: A cryptographic approach in response to a global pandemic," 2020.

[11] K. Hogan, N. Luther, N. Schear, E. Shen, D. Stott, S. Yakoubov, and A. Yerukhimovich, "Secure multiparty computation for cooperative cyber risk assessment," in *IEEE Cybersecurity Development, 2016*, pp. 75–76, IEEE Computer Society, 2016.

[12] B. Pinkas, T. Schneider, and M. Zohner, "Faster private set intersection based on OT extension," in *USENIX Security 2014*, pp. 797–812, 2014.

[13] V. Kolesnikov, R. Kumaresan, M. Rosulek, and N. Trieu, "Efficient batched oblivious PRF with applications to private set intersection," in *CCS 2016*, pp. 818–829, ACM, 2016.

[14] B. Pinkas, M. Rosulek, N. Trieu, and A. Yanai, "Spot-light: Lightweight private set intersection from sparse OT extension," in *Advances in Cryptology - CRYPTO 2019*, vol. 11694 of *Lecture Notes in Computer Science*, pp. 401–431, Springer, 2019.

[15] M. Chase and P. Miao, "Private set intersection in the internet setting from lightweight oblivious PRF," in *Advances in Cryptology - CRYPTO 2020*, vol. 12172 of *Lecture Notes in Computer Science*, pp. 34–63, Springer, 2020.

[16] B. Pinkas, M. Rosulek, N. Trieu, and A. Yanai, "PSI from paxos: Fast, malicious private set intersection," in *EUROCRYPT 2020*, Springer, 2020.

[17] P. Rindal and P. Schoppmann, "VOLE-PSI: fast OPRF and circuit-psi from vector-ole," in *EUROCRYPT 2021*, vol. 12697, pp. 901–930, Springer, 2021.

[18] S. Raghuraman and P. Rindal, "Blazing fast PSI from improved OKVS and subfield VOLE," in *ACM CCS 2022*, ACM, 2022.

[19] G. Garimella, P. Mohassel, M. Rosulek, S. Sadeghian, and J. Singh, "Private set operations from oblivious switching," in *Public-Key Cryptography - PKC 2021*, vol. 12711 of *Lecture Notes in Computer Science*, pp. 591–617, Springer, 2021.

[20] Y. Chen, M. Zhang, C. Zhang, M. Dong, and W. Liu, "Private set operations from multi-query reverse private membership test," in *Public-Key Cryptography - PKC 2024*, Springer, 2024.

[21] V. Kolesnikov, M. Rosulek, N. Trieu, and X. Wang, "Scalable private set union from symmetric-key techniques," in *Advances in Cryptology - ASIACRYPT 2019*, vol. 11922 of *Lecture Notes in Computer Science*, pp. 636–666, Springer, 2019.

[22] Y. Jia, S. Sun, H. Zhou, J. Du, and D. Gu, "Shuffle-based private set union: Faster and more secure," in *USENIX 2022*, 2022.

[23] C. Zhang, Y. Chen, W. Liu, M. Zhang, and D. Lin, "Optimal private set union from multi-query reverse private membership test," in *USENIX 2023*, pp. 337–354, USENIX Association, 2023.

[24] Y. Jia, S. Sun, H. Zhou, and D. Gu, "Scalable private set union, with stronger security," in *USENIX Security 2024*, 2024.

[25] D. Demmler, P. Rindal, M. Rosulek, and N. Trieu, "PIR-PSI: scaling private contact discovery," *Proc. Priv. Enhancing Technol.*, vol. 2018, no. 4, pp. 159–178, 2018.

[26] J. R. Troncoso-Pastoriza, S. Katzenbeisser, and M. U. Celik, "Privacy preserving error resilient dna searching through oblivious automata," in *ACM CCS 2007*, pp. 519–528, 2007.

[27] T. Duong, D. H. Phan, and N. Trieu, "Catalic: Delegated psi cardinality with applications to contact tracing," in *Advances in Cryptology – ASIACRYPT 2020*, Springer, 2020.

[28] S. Dittmer, Y. Ishai, S. Lu, R. Ostrovsky, M. Elsabagh, N. Kiourtis, B. Schulte, and A. Stavrou, "Function secret sharing for PSI-CA: with applications to private contact tracing," *IACR Cryptol. ePrint Arch.*, p. 1599, 2020.

[29] A. K. Lenstra and T. Voss, "Information security risk assessment, aggregation, and mitigation," in *Information Security and Privacy: 9th Australasian Conference, ACISP 2004.*, vol. 3108 of *Lecture Notes in Computer Science*, pp. 391–401, Springer, 2004.

[30] J. Brickell and V. Shmatikov, "Privacy-preserving graph algorithms in the semi-honest model," in *Advances in Cryptology - ASIACRYPT 2005, 11th International Conference on the Theory and Application of Cryptology and Information Security*, vol. 3788 of *Lecture Notes in Computer Science*, pp. 236–252, Springer, 2005.

[31] L. Kissner and D. X. Song, "Privacy-preserving set operations," in *Advances in Cryptology - CRYPTO 2005*, vol. 3621 of *Lecture Notes in Computer Science*, pp. 241–257, Springer, 2005.

[32] S. Zhang, "Efficient VOLE based multi-party PSI with lower communication cost," *IACR Cryptol. ePrint Arch.*, p. 1690, 2023.

[33] J. Gao, N. Trieu, and A. Yanai, "Multiparty private set intersection cardinality and its applications," *Proc. Priv. Enhancing Technol.*, vol. 2024, no. 2, 2024.

[34] J. Su and Z. Chen, "Secure and scalable circuit-based protocol for multi-party private set intersection," *CoRR*, vol. abs/2309.07406, 2023.

[35] R. Li and C. Wu, "An unconditionally secure protocol for multi-party set intersection," in *Applied Cryptography and Network Security - ACNS 2007*, vol. 4521 of *Lecture Notes in Computer Science*, pp. 226–236, Springer, 2007.

[36] M. Blanton and E. Aguiar, "Private and oblivious set and multiset operations," in *ASIACCS 2012*, pp. 40–41, ACM, 2012.

[37] J. H. Seo, J. H. Cheon, and J. Katz, "Constant-round multi-party private set union using reversed laurent series," in *Public Key Cryptography - PKC 2012*, pp. 398–412, Springer, 2012.

[38] N. Chandran, N. Dasgupta, D. Gupta, S. L. B. Obbattu, S. Sekar, and A. Shah, "Efficient linear multiparty PSI and extensions to circuit/quorum PSI," in *CCS '21*, pp. 1182–1204, ACM, 2021.

[39] A. Bay, Z. Erkin, J. Hoepman, S. Samardjiska, and J. Vos, "Practical multi-party private set intersection protocols," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 1–15, 2022.

[40] J. Vos, M. Conti, and Z. Erkin, "Fast multi-party private set operations in the star topology from secure ands and ors," *IACR Cryptol. ePrint Arch.*, p. 721, 2022.

[41] M. J. Freedman, K. Nissim, and B. Pinkas, "Efficient private matching and set intersection," in *Advances in Cryptology - EUROCRYPT 2004*, vol. 3027 of *Lecture Notes in Computer Science*, pp. 1–19, Springer, 2004.

[42] C. Hazay and M. Venkitasubramaniam, "Scalable multi-party private set-intersection," in *Public-Key Cryptography - PKC 2017*, vol. 10174 of *Lecture Notes in Computer Science*, pp. 175–203, Springer, 2017.

[43] V. Kolesnikov, N. Matania, B. Pinkas, M. Rosulek, and N. Trieu, "Practical multi-party private set intersection from symmetric-key techniques," in *CCS 2017*, pp. 1257–1272, ACM, 2017.

[44] R. Inbar, E. Omri, and B. Pinkas, "Efficient scalable multiparty private set-intersection via garbled bloom filters," in *SCN 2018*, vol. 11035 of *Lecture Notes in Computer Science*, pp. 235–252, Springer, 2018.

[45] G. Garimella, B. Pinkas, M. Rosulek, N. Trieu, and A. Yanai, "Oblivious key-value stores and amplification for private set intersection," in *Advances in Cryptology - CRYPTO 2021*, vol. 12826 of *Lecture Notes in Computer Science*, pp. 395–425, Springer, 2021.

[46] O. Nevo, N. Trieu, and A. Yanai, "Simple, fast malicious multiparty private set intersection," in *CCS 2021*, pp. 1151–1165, ACM, 2021.

[47] A. Ben-Efraim, O. Nissenbaum, E. Omri, and A. Paskin-Cherniavsky, "Psimple: Practical multiparty maliciously-secure private set intersection," in *ASIA CCS '22*, pp. 1098–1112, ACM, 2022.

[48] K. B. Frikken, "Privacy-preserving set union," in *ACNS 2007*, vol. 4521 of *Lecture Notes in Computer Science*, pp. 237–252, Springer, 2007.

[49] J. Gao, S. Nguyen, and N. Trieu, "Toward A practical multi-party private set union," *Proc. Priv. Enhancing Technol.*, vol. 2024, no. 4, pp. 622–635, 2024.

[50] P. Giorgi, F. Laguillaumie, L. Ottow, and D. Vergnaud, "Fast secure computations on shared polynomials and applications to private set operations," in *ITC 2024*, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024.

[51] C. Hazay and Y. Lindell, *Efficient Secure Two-Party Protocols - Techniques and Constructions*. Information Security and Cryptography, Springer, 2010.

[52] A. Bienstock, S. Patel, J. Y. Seo, and K. Yeo, "Near-Optimal oblivious Key-Value stores for efficient PSI, PSU and Volume-Hiding Multi-Maps," in *USENIX Security 2023*, pp. 301–318, 2023.

[53] J. Gao, S. Nguyen, and N. Trieu, "Toward a practical multi-party private set union." Cryptology ePrint Archive, Paper 2023/1930, 2023. Version: 20240316:210303, https://eprint.iacr.org/archive/2023/1930/20240316:210303.

致　谢

在此，我要特别感谢 LaTeX 模板 sduthesis.cls 的原作者 Liam Huang（https://github.com/Liam0205/sduthesis/），感谢他辛勤的劳动和无私的分享。正是因为有了他的工作，我才能在此基础上进行修改，得到当前的 LaTeX 模板。

感谢所有为开源社区做出贡献的开发者们，你们的努力使得学术研究和论文写作变得更加高效和便捷。

攻读博士学位期间发表的学术论文

1. **Guodong Li**, Ningning Wang, Sihuang Hu, and Min Ye. MSR Codes With Linear Field Size and Smallest Sub-Packetization for Any Number of Helper Nodes. *IEEE Transactions on Information Theory*, pages 1–1, 2024.

攻读博士学位期间所获奖项

1. 山东大学新生入学学业奖学金，2020.10