多方隐私集合交集计算技术综述

高 莹*①②③ 王 玮①

①(北京航空航天大学网络空间安全学院 北京 100191)

②(中关村实验室 北京 100094)

③(空天网络安全工业和信息化部重点实验室 北京 100191)

摘 要：随着互联网、大数据等新技术的快速发展，越来越多的分布式数据需要多方协作处理，隐私保护技术由此面临更大的挑战。安全多方计算是一种重要的隐私保护技术，可为数据的安全高效共享问题提供解决方案。作为安全多方计算的一个重要分支，隐私集合交集(PSI)计算技术可以在保护参与方的数据隐私性前提下计算两个或多个参与者私有数据集的交集，按照参与方数目可分为两方PSI和多方PSI。随着私人数据共享规模的扩大，多于两个参与方的应用场景越来越常见。多方PSI具有与两方PSI相似的技术基础但又有本质的不同。该文首先讨论了两方PSI的研究进展，其次详细梳理多方PSI技术的发展历程，将多方PSI技术依据应用场景的不同分为传统多方PSI技术以及门限多方PSI技术，并在不同场景下按照协议所采用密码技术和功能进行更细致的划分；对典型多方PSI协议进行分析，并对相关密码技术、敌手模型以及计算与通信复杂度进行对比。最后，给出了多方PSI技术的研究热点和未来发展方向。

关键词：隐私集合交集；不经意传输；不经意伪随机函数；加法同态加密；零秘密分享

中图分类号：TN918; TP309.2 **文献标识码**：A **文章编号**：1009-5896(2023)05-1859-14

DOI: 10.11999/JEIT220664

A Survey of Multi-party Private Set Intersection

GAO Ying①②③ WANG Wei①

①(*School of Cyber Science and Technology*, *Beihang University*, *Beijing* 100191, *China*)

②(*Zhongguancun Laboratory*, *Beijing* 100094, *China*)

③(*Key Laboratory of Aerospace Network Security*, *Ministry of Industry and Information Technology*, *Beijing* 100191, *China*)

Abstract: With the rapid development of new technologies, such as the Internet and big data, more and more distributed data need to be processed by multiple parties. Therefore, privacy protection technology is facing greater challenges. Secure multi-party computation is an important privacy protection technology, which can provide solutions for the secure and efficient sharing of data. As an important branch of secure multi-party computation, Private Set Intersection (PSI) technology can calculate the intersection of private data sets of two or more participants under the premise of protecting the data privacy of participants. It can be divided into two-party PSI and multi-party PSI according to the number of participants. With the expansion of private data sharing scale, application scenarios with more than two participants are more and more common. Multi party PSI has the same technical basis as the two party PSI, but has essential differences. Firstly, the research progress of the two-party PSI is discussed. Then the development processes of multi-party PSI are analyzed in detail. The multi-party PSI is divided into traditional multi-party PSI and threshold multi-party PSI according to the different scenarios. At the same time, protocols in different scenarios are divided more carefully according to the different basic cryptographic protocols they used and their different functions. The typical protocols are analyzed, and the cryptographic protocols, security model, computation and communication complexity of the protocols are discussed. Finally, the research hotspots and future development directions of multi-party PSI are pointed out.

收稿日期：2022-05-23；改回日期：2022-11-22；网络出版：2022-11-25

*通信作者： 高 莹 gaoying@buaa.edu.cn

基金项目：国家自然科学基金(61932011, 61972017)，北京市自然科学基金(M21033)

Foundation Items: The National Natural Science Foundation of China (61932011, 61972017), The Natural Science Foundation of Beijing (M21033)

Key words: Private Set Intersection (PSI); Oblivious Transfer (OT); Oblivious pseudorandom function; Additively homomorphic encryption; Zero secret sharing

1 引言

近年来随着互联网技术的蓬勃发展，公司和个人可以便捷地以低成本获取信息内容，极大地促进了信息的分发和交流。然而隐私数据在网络上被过度采集、非法滥用将会导致用户的个人信息被泄露，如：在寻找新型冠状病毒(COrona VIrus Disease 2019, COVID-19)肺炎患者的密切接触者时，暴露患者的行程信息可能会使其面临网暴；在拼车服务中，公司员工可以轻而易举地拿到用户的位置变化情况，使用“上帝视角”跟踪用户[1]。

为了保护数据隐私，多个国家和地区已经颁布了相关的法律法规。其中2018年5月生效的欧盟《通用数据保护条例》[2]被誉为世界上最全面的数据隐私法，2021年11月1日起实施的《中华人民共和国个人信息保护法》是我国专门保护公民个人信息的法律，在全球隐私保护、数据合规等监管要求之下，如何促进数据安全合规流通成为重要研究课题。安全多方计算(Secure Multi-Party Computation, SMPC)技术[3]是一种密码原语，在解决数据可控共享问题和保证数据信息安全方面具有天然优势。

隐私集合交集(Private Set Intersection, PSI)计算是一种特殊的安全多方计算协议，允许两个或多个参与者秘密地计算他们的交集而不泄露除交集之外的其他任何信息。两个参与者场景下的PSI(简称两方PSI)已有多种高效且安全的实现方案[4–28]。随着私人数据共享规模的扩大，参与方多于两方的场景更为常见，因此产生了多方PSI技术。目前已经有一些关于PSI技术的综述文献[29–32]，申立艳等人[29]在2017年表明两方PSI的研究趋势是均衡协议的安全性、高效性和可扩展性。崔泓睿等人[30]在2019年对基于简单哈希、基于公钥、基于混淆电路、基于不经意传输(Oblivious Transfer, OT)的两方PSI进行通信复杂度和计算复杂度的理论对比，同时在局域网和广域网场景下测试性能。魏立斐等人[31]在2021年在两方PSI的基础上，阐述了适用于新场景的PSI方案：云辅助的PSI、非平衡的PSI、门限PSI以及多方PSI，但该综述对多方PSI的最新研究进展总结较为简略，且并未涵盖最新的多方PSI协议。黄翠婷等人[32]在2021年阐述了PSI在金融行业的应用价值。通过对现有PSI综述的调研，可以发现现有综述依旧聚焦于两方PSI，对多方PSI的最新研究进展尚未有系统且全面的梳理。本文在对多方PSI综述的过程中，将多方PSI按照功能分为传统多方PSI和门限多方PSI两个大类，传统多方PSI是3个或以上参与方进行交集计算，最终输出交集结果；门限多方PSI是指在传统多方PSI的基础上增加门限约束条件，根据门限约束内容的不同又可以分为约束交集大小的门限多方PSI和约束元素出现次数的门限多方PSI。隐私集合交集计算技术在参与方数目、功能和技术方面的分类如图1所示。其中，不经意传输协议常被用来构造不经意伪随机函数(Oblivious PseudoRandom Function, OPRF)，从而实现PSI协议。RSA是指由Rivest, Shamir和Adleman 3人提出并以首字母命名的加密算法，GMW是指Goldreich, Micali和Wigderson 3人提出并以首字母命名的协议。

本文的结构如下：考虑综述的完整性，首先在第2节简要介绍两方PSI技术的相关分类及典型协议。第3节介绍传统多方PSI技术，将其依据密码技术和功能进行分类，讨论协议采用的密码技术、安

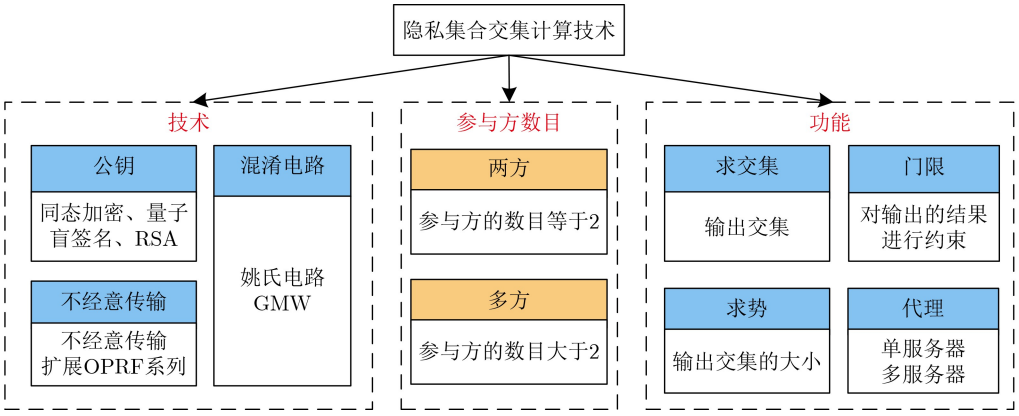


图 1 隐私集合交集计算技术分类图

全模型以及计算与通信复杂度。第4节介绍门限多方PSI技术，并将其进行分类和对比。第5节总结多方PSI技术的研究热点和未来发展方向。

2　两方PSI协议

根据两方PSI协议所采用的技术的不同，可将其分为基于公钥加密体制的PSI协议[4–11]、基于混淆电路的PSI协议[12–16]以及基于OT的PSI协议[17–27]3种类型，本节将对这3种类型的典型协议进行简要介绍。

基于公钥加密体制的两方PSI协议最早在1986年由Meadows[4]提出，Meadows基于离散对数困难问题实现了Diffie-Hellman密钥交换协议，将两个集合的明文对比转换为会话密钥的对比，从而实现PSI的功能；同样基于“将明文对比转换为其他形式的对比”的思想，文献[7]将集合的对比转换为盲签名结果的对比。除此之外，最经典的基于公钥的两方PSI协议是Freedman等人[6]在2004年提出的协议，该协议借助了不经意多项式求值技术(Oblivious Polynomial Evaluation, OPE)和同态加密技术，同时关注了多方PSI协议的架构。

混淆电路是安全多方计算的常用工具，任意的函数均可以转化为布尔电路进行计算，因此使用混淆电路可以计算任意的功能函数[31]，这对于多功能的PSI协议(如求势、求交集和、门限)的研究有重要作用。Huang等人[12]在2012年通过Yao电路构造排序-比较-打乱电路，实现了半诚实敌手模型下安全的PSI协议。在此之后基于混淆电路的PSI协议的优化着重于计算开销的优化。为了降低计算开销，节约运行耗时，Pinkas等人[13]在2015年提出基于置换哈希的PSI协议，比Huang等人[12]的协议快约5倍；2018年，基于2维布谷鸟哈希技术，Pinkas等人[14]提出的PSI协议的计算和通信开销几乎为线性；2019年，Pinkas等人[15]在文献[14]的基础上利用不经意可编程伪随机函数(Oblivious Programmable PseudoRandom Function, OPPRF)技术实现了第1个与集合大小呈线性通信复杂度的基于电路的PSI协议。为了解决超线性计算的问题，Chandran等人[16]基于批处理OPPRF构造的PSI协议在计算开销和通信开销方面均具有线性复杂度。基于混淆电路的PSI协议的瓶颈问题在于功能函数的电路设计较复杂，门电路个数多且电路深度较大，通信复杂度较高。

OT协议及OT扩展协议[33–36]是两方或多方PSI中常见的基础密码原语，既可以满足安全多方计算对安全性的要求，保护参与方的隐私，又可以相较于公钥和混淆电路，在计算开销和通信开销方面达到平衡，满足对实用性的需求。基于OT的PSI协议是目前两方平衡PSI场景下最高效的实现方案，其关键在于OT扩展协议的构造与选择。首个基于OT协议的PSI协议为Dong等人[17]于2013年提出的基于布隆过滤器(Bloom Filter, BF)和混淆布隆过滤器(Garbled Bloom Filter, GBF)的PSI协议，与基于公钥的PSI协议中常用的多项式存储数据相比，使用BF和GBF存储数据可以节约计算开销。在此之后，Pinkas等人[18,23]基于布谷鸟哈希方案对通信开销进行优化；2016年，Kolesnikov等人[19]基于批处理技术构造较前人更高效的半诚实安全的两方PSI协议。在对恶意敌手模型的研究方面，Orru等人[20]提出了对抗单个恶意参与方的PSI协议；Rindal等人[21]对Dong等人的恶意方案进行改进，使用cut-and-choose技术构造恶意安全的PSI协议；文献[22]提出在构造PSI协议中增加批量双执行的思想，实现了发送方和接收方均是恶意敌手模型下的安全。通过多点OPRF技术将集合元素的对比转换为对元素密文的对比是PSI协议的实现方式之一，2019年，Pinkas等人[24]提出了多点OPRF的概念，依赖高阶多项式构造，减少发送方对元素加密的次数的同时降低通信开销；2020年，Chase等人[26]提出基于矩阵和对称密钥的轻量级多点OPRF，实现了半诚实敌手模型下的PSI协议和一方恶意的PSI协议。在存储结构优化方面，Pinkas等人[25]基于混淆布谷鸟哈希表提出了节约存储开销且恶意敌手模型下安全的PSI协议。

随着公钥、混淆电路和OT技术的发展，更多新型场景下的两方PSI协议被设计和优化，如非平衡场景、云辅助场景、有门限约束场景等的PSI协议，这些协议均可以延用传统两方PSI协议的基础框架进行构造。然而，在多方参与计算交集的场景中，若依旧使用传统两方PSI协议框架，在多个参与方之间多次进行两方PSI协议以达到多方PSI的功能，则会带来非常数轮的通信开销以及较高的计算开销，所以多方PSI协议框架需要单独设计。

3　传统多方PSI协议

本节将根据协议所采用的底层密码学技术对传统多方PSI进行梳理，主要分为基于公钥的多方PSI[6,37–50]和基于OT的多方PSI[51–57]，由于混淆电路在预计算阶段构造复杂，且内存占用较高，并没有基于混淆电路的传统多方PSI协议的研究，但又鉴于混淆电路可以方便地计算任何功能函数的特性，其更适用于构造门限等特殊场景下的多方PSI协议。除此之外，本节还简要概述了代理多方PSI[58–68]、多对一PSI[69]、多方隐私集合交集求势(Private Set

Intersection CArdinality, PSI-CA)[70–73]等其他功能变体。

3.1 基于公钥的多方PSI

基于公钥的多方PSI方案主要采用同态加密技术[74]。第1个基于同态加密技术的多方PSI协议方案由Freedman等人[6]提出，首先使用加法同态加密实现的OPE技术，将集合元素表示为多项式的根从而代替集合进行运算，实现了在半诚实敌手模型下的两方PSI，其次提出了针对恶意的客户端、恶意的服务端、恶意的两方以及多方的情况下的PSI协议的构造思路。

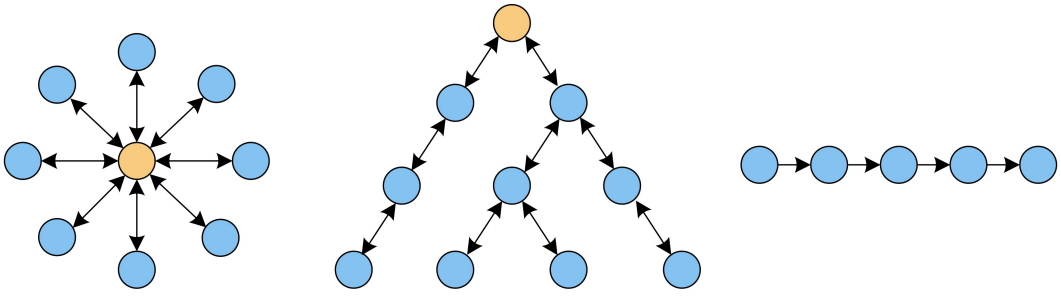
在此之后，对基于同态加密技术的多方PSI协议的通信和计算开销的优化、协议安全性的提升成为研究者的重要研究目标，本文分别对半诚实敌手模型和恶意敌手模型下的优化进展进行讨论。

在半诚实敌手模型中，Kissner等人[37]在2005年对加法同态加密的私钥进行秘密共享，协议的计算复杂度和通信复杂度是集合大小和参与方数目的2次方。2017年，Hazay等人[38]使用星型通信模型将多方PSI协议的通信轮数从$O(n)$降低为$O(1)$，且加解密的操作数与参与方集合大小呈线性关系。其中，星型通信结构是最直观的多方通信结构，多个参与方与同一个中心参与方进行交互，此结构对中心参与方的带宽和计算能力要求较高。此外，还有树型通信结构和路径通信结构。树型通信结构是二叉树状的结构，可以降低中心参与方的通信带宽和计算开销；路径通信结构是消息在所有参与方中依次传递，不再设置中心参与方，真正实现了通信开销和计算开销的平均分摊。各通信结构图如图2所示。

采用与两方PSI协议相同的数据存储的思想，为降低使用多项式代替集合所带来的较高的计算开销，一般使用比特串或其他特定数据存储结构，如BF。2021年，Bay等人[39]将全集设为定长字符串，如果私有集合包含某个元素，则该比特串的对应位置为1，反之则为0。这种替代方法使协议的计算和通信复杂度主要依赖全集大小，当参与者数目增加时，显著优于其他基于公钥的多方PSI协议。同年，Bay等人[40]对Davidson等人[75]提出的两方PSI协议进行扩展，将n个参与方分为$n-1$个客户端和1个服务端，且集合大小是公开的。服务端与客户端使用BF和比特反转并加密的BF进行元素的插入和查询，利用门限加法同态加密的性质对多个客户端的BF进行加法操作而在不影响解密结果的前提下求得交集。此协议在大量参与方和小集合的场景下降低了公钥计算与通信复杂度。基于整数的同态加密操作是多方PSI与多方隐私集合求并(Private Set Union, PSU)的常用方法，但是在实际使用中会带来繁重的开销。2022年，Vos等人[41]基于椭圆曲线实现私有集合元素的“与”操作，针对小集合和大集合分别实现多方PSI协议，该协议在小集合的运行耗时方面比Bay等人[40]的协议快两个数量级；在大集合运行耗时方面是目前最优的多方PSI协议。同年，在对小集合的场景的优化方面，张蕾等人[42]基于双线性映射和三方密钥协商协议，提出了半诚实敌手模型和恶意敌手模型下的三方PSI协议，该协议实现了3个参与方和小集合场景下最优的通信复杂度。

在对恶意敌手模型下的多方PSI协议的开销优化方面，Sang等人[44]首先在2007年提出了基于交互式零知识证明的算法，高成本的多项式乘法带来了高计算复杂度，而后在2008年[45]基于双线性群减少计算开销，在2009年使协议达到通用可组合(Universally Composable, UC)安全[46]。2012年，Cheon等人[47]使用分布式秘密共享对基于双线性群的协议[45]进行了有效的改进，使计算开销对输入集合的2次型依赖减少为准线型，是第1个计算和通信开销均与输入集合呈准线型关系的协议。2019年，Ghosh等人[48]在恶意敌手模型下提出了基于不经意线性函数估值(Oblivious Linear function Evaluation, OLE)的多方PSI协议，而后该文献在没有显著增加复杂度的前提下扩展到了门限多方PSI。

随着抗量子的公钥密码技术的发展，抗量子计



(a) 星型通信结构 (b) 树型通信结构 (c) 路径通信结构

图 2 通信结构分类图

算机的多方PSI协议设计也成为一个重要的研究方向。2021年，Debnath等人[50]提出第1个抗量子多方PSI协议，该协议基于BF和格密码构造，基于标准模型和有错误的决策学习假设证明了协议在半诚实敌手模型下的安全性。

对典型的基于公钥的多方PSI协议的比较如表1所示。其中，Leader为服务器，是指需要与其他所有参与方通信并输出交集的一方；Client是除Leader外的其他参与方。抗勾结能力是指协议抵抗两个及以上腐败的参与方相互勾结的能力。由表1得知，现有的基于公钥的多方PSI协议均具有抗勾结能力，在通信复杂度和计算复杂度的优化方面，均从最早的与参与方数目和交集大小呈2次方逐渐优化至线性关系。

3.2 基于OT的多方PSI

基于OT协议的多方PSI协议主要分为两种，一是使用OT协议构造OPRF，OPPRF和多点OPRF等一系列协议，而后基于OPRF系列协议构造多方PSI协议；二是多方直接使用OT协议进行数据传输。

使用OT协议构造OPRF的主要思想为：接收方对每个输入元素以不经意的方式计算伪随机函数(PseudoRandom Function, PRF)值后再与发送方输入元素的PRF值进行对比求交集。OPRF是一个两方计算协议，通过正确执行协议，接收方输入元素r，发送方得到密钥K，接收方得到加密值$F(K,r)$，但是接收方不知道密钥K的具体值，发送方也对接收方的输入一无所知，发送方可以使用获得的密钥对任意元素进行加密。在OPRF中，由于接收方1次只能输入1个元素r，且发送方收到的密钥K与接收方输入的元素r一一对应，因此OPRF也可以称为单点OPRF。

在使用单点OPRF构造两方PSI协议的过程中，发送方会得到多个密钥，然而对于发送方来讲，密钥具有不可区分性，因此发送方需要对每个私有元素进行多次加密，无疑增大了通信和计算开销。为降低开销，基于矩阵和OT扩展协议的轻量级的多点OPRF协议应运而生[26]，与单点OPRF协议相比，其优势在于在构造两方PSI协议的过程中，发送方的每个元素均只需要加密计算1次即可。2021年，Kavousi等人[52]基于上述多点OPRF降低了多方PSI协议的计算开销。该协议除参与方P_n外，其他参与方的通信和计算开销与参与方数目无关，平衡了各个参与方的开销，该方案的局限性在于只有1个参与方可以得到交集结果。

基于OPRF的多方PSI协议中最经典的同时也是首篇将多方PSI进行代码实现的协议为Kolesnikov等人[51]在2017年提出的方案。该文献首次提出了使用OPRF构造OPPRF的概念，旨在使用发送方的输入来对OPRF的密钥进行编程，其与单点OPRF的区别在于OPPRF中密钥与发送方的私有集合元素相关。其基于OPPRF和零秘密分享协议分别构造半诚实敌手模型下和增强的半诚实敌手模

表 1　基于公钥的多方PSI协议比较

协议	安全性	抗勾结	通信复杂度		计算复杂度	
			Leader	Client	Leader	Client
文献[37]	半诚实	√	$O(n^2m^2\lambda)$	$O(n^2m^2\lambda)$	$O(n^2m+n\lambda m^2)$	$O(n^2m+n\lambda m^2)$
文献[38]	半诚实	√	$O(nm\lambda)$	$O(m\lambda)$	$O(nm\log_2{}^{m\kappa})$	$O(m\kappa)$
	恶意	√	$O((n^2+nm\log_2{}^m)\kappa)$	$O((n+m\log_2{}^m)\kappa)$	$O(m^2)$	$O(m^2)$
文献[39]	半诚实	√	$O\left(dn\log_2{}^{\lvert X\rvert}\right)$	$O\left(d\log_2{}^{\lvert X\rvert}\right)$	$O(d)$	$O(d)$
			$O\left(d\ell\log_2{}^{\lvert X\rvert}\right)$	$O\left(d\log_2{}^{\lvert X\rvert}\right)$	$O(d)$	$O(d)$
文献[40]	半诚实	√	$O\left(m\ell\log_2{}^{\lvert X\rvert}\right)$	$O\left(\lambda m\log_2{}^{\lvert X\rvert}\right)$	$O(m)$	$O(\lambda m)$
文献[41]	半诚实	√	$O(nd)$	$O(d)$	$O(nd)$	$O(d)$
			$O(nm)$	$O(m)$	$O(nmk)$	$O(m)$
文献[44]	恶意	√	$O(\ell n^2m^2\kappa)$	$O(\ell n^2m^2\kappa)$	$O(\ell^2m^2\kappa^3)$	$O(\ell^2m^2\kappa^3)$
文献[45]	恶意	√	$O(nm^2\kappa)$	$O(nm^2\kappa)$	$O(nm^2\kappa)$	$O(nm^2\kappa^3)$
文献[46]	UC	√	$O(nm^2\kappa)$	$O(nm^2\kappa)$	$O(\ell m^2\kappa^3)$	$O(\ell m^2\kappa^3)$
文献[47]	恶意	√	$O(\lambda n^2m)$	$O(\lambda n^2m)$	$O(n^2m+nm\lambda)$	$O(n^2m+nm\lambda)$
文献[48]	恶意	√	$O((n^2+nm)\kappa)$	$O((n^2+nm)\kappa)$	$O(nm\log_2{}^m)$	$O\left(m(\log_2{}^m)^2\right)$
文献[49]	恶意	√	$O(n^2\kappa+nm(\kappa+\lambda+\log_2{}^m))$	$O(m(\kappa+\lambda+\log_2{}^m))$	$O(nm)$	$O(m)$

注：在复杂度对比中，n为参与方数目，w为腐败方数目，m为集合大小，λ和κ分别为统计和计算安全参数，k为哈希函数的个数，d为域的大小，ℓ为同态公钥加密系统的门限值，$\log_2{}^{|X|}$为二进制密文X的大小。补充说明的是：任意腐败方数目w的最大值应小于总参与方数目。

型下的多方PSI协议。其中，增强的半诚实敌手模型比普通的半诚实敌手模型的安全性更弱一些，允许敌手更改腐败方的输入。零秘密分享协议的主要功能是如果一个参与方含有元素x，那么其会收到一份x对应的共享值，当且仅当所有参与方均包含元素x时，所有参与方含有的对于x的共享值的异或值为0。

在直接使用OT协议作为数据传输协议方面，2018年，Inbar等人[53]在半诚实敌手模型和增强的半诚实敌手模型中分别提出了两种多方PSI协议，是对Dong等人[17]两方PSI协议的扩展。Inbar等人[53]的协议与Kolesnikov等人[51]的协议相比的优势在于随着参与方数目的增多，协议消耗时间增长缓慢，与参与方数目呈次线性关系；而Kolesnikov等人[51]的协议的最后一个步骤中需要多次计算和比较，计算开销较大。

另外，基于OT扩展的面向恶意敌手模型的研究在2019年也有了突破。Zhang等人[54]使用文献[38]中的星型通信模型和BF技术，在恶意两方PSI[21]的基础上提出了对抗恶意敌手的多方协议，本质上是运行$O(n)$次底层两方PSI(假设n为参与方个数)，所以时间开销也为两方PSI的$O(n)$倍，然而此协议规定两个特定的参与方不同时被腐败，所以不是标准的恶意敌手模型。为解决此问题，2021年，Ben-Efraim等人[55]在标准的恶意敌手模型下，使用GBF技术在恶意两方PSI[21]和半诚实多方PSI[53]基础上设计了可以对抗任意多个腐败方的恶意安全多方PSI协议。

在存储结构的优化方面，不经意键值存储(Oblivious Key-Value Store, OKVS)[76]与传统多项式相比节约计算开销，与GBF相比节约存储开销，对计算和存储开销实现了有效的平衡，主要包括混淆的布谷鸟哈希表等数据存储结构。Nevo等人[56]基于OKVS，根据恶意敌手腐化参与方之后参与方是否勾结分为两种情况分别设计协议，是目前为止表现最优的针对恶意敌手的多方PSI协议。在恶意敌手只腐败1个参与方且参与方不互相勾结的场景中，仅使用对称密钥原语分别构造递归$O(n)$轮和$O(1)$轮的两种协议；在腐败参与方可以相互勾结的场景中，将参与方分为3组：客户端、中心、服务端进行交互。通过实验证明该方案在效率方面与现有的其他多方PSI协议相比，计算开销和通信开销均有大程度优化。2022年，Gordon等人[57]基于多方PSI的公平性问题，提出了所有参与方均可以获得交集结果的恶意多方PSI协议。

对典型的基于OT的传统多方PSI协议的比较如表2所示。通过表1和表2可以得知，与基于公钥的多方PSI协议相比，基于OT的多方PSI协议增加了对增强的半诚实敌手模型下的多方PSI协议的研究。并且，在相同的安全性的条件下[38,51]，基于OT的多方PSI协议[51]的计算复杂度要低于基于公钥的多方PSI协议[38]的计算复杂度。

3.3 代理多方PSI协议及其他技术方案

与两方PSI协议类似，多方PSI协议也可借助云服务器来分摊参与方的计算开销[58]，同时也可以使用BF作为数据存储结构降低通信开销。如：Miyaji等人[59]的协议和Zhu等人[60]的协议均基于BF来构造。在2021年，王勤等人[61]将GBF、多项式插值技术统称为键值对打包，并对两种技术应用在代理多方PSI协议中的性能进行对比，证明计算

表 2 基于OT的多方PSI协议比较

协议	安全性	抗勾结	通信复杂度		计算复杂度	
			Leader	Client	Leader	Client
文献[51]	半诚实	√	$O(nm\lambda)$	$O(mw\lambda)$	$O(n\kappa)$	$O(w\kappa)$
	增强的半诚实	√	$O(nm\lambda)$	$O(m\lambda)$	$O(n\kappa)$	$O(\kappa)$
文献[52]	半诚实	√	$O(nm\kappa)$	$O(m\kappa k)$	$O(nm\kappa)$	$O(m\kappa k)$
文献[53]	半诚实	√	$O(nm\kappa k)$	$O(nm\kappa k)$	$O(nm\kappa k)$	$O(nm\kappa k)$
	增强的半诚实	√	$O(m\kappa k\log_2{}^{n})$	$O(m\kappa k\log_2{}^{n})$	$O(nm\kappa k)$	$O(nm\kappa k)$
文献[54]	恶意	√	$O\left(nm\lambda^2+nm\lambda\log_2{}^{(m\lambda)}\right)$	$O\left(nm\lambda^2+nm\lambda\log_2{}^{(m\lambda)}\right)$	$O(nmk)$	$O(nmk)$
文献[55]	恶意	√	$O\left(nm\kappa^2+nm\kappa\log_2{}^{(m\kappa)}\right)$	$O\left(m\kappa^2+m\kappa\log_2{}^{(m\kappa)}\right)$	$O(nm\kappa)$	$O(nm\kappa)$
文献[56]	恶意	×	$O((m+n)\kappa)$	$O(m\kappa)$	$O(nm\kappa)$	$O(m\kappa)$
		√	$O(m\kappa\cdot\max\{w,n-w\})$	$O(m\kappa)$	$O(m\kappa(n-w))$	$O(mw\kappa)$
文献[57]	恶意	√	$O\left(nm\kappa+n^2\lambda\kappa\log_2{}^{m}\right)$	$O(m\kappa+n\lambda\kappa\log_2{}^{m})$	$O\left(nm\kappa+m(\log_2{}^{m})^2\right)$	$O\left(m\kappa+m(\log_2{}^{m})^2\right)$

注：在复杂度对比中，n为参与方数目，w为腐败方数目，m为集合大小，λ和κ分别为统计和计算安全参数，k为哈希函数的个数，d为域的大小，ℓ为同态公钥加密系统的门限值，$\log_2{}^{|X|}$为二进制密文X的大小。补充说明的是：任意腐败方数目w的最大值应小于总参与方数目。

开销低的GBF技术适用于网络宽松但算力不足的场景，而存储开销低的多项式插值技术更适用于通信紧张但算力充足的场景。

除了对通信开销的优化，Abadi等人[62–65]还在代理多方PSI协议的功能完备性方面，如是否可验证、是否支持各参与方私有集合更新等，做出了贡献。除此之外，代理服务器的数目不只局限于1个。2016年，Zhang等人[66]分别在半诚实敌手模型下和社会理性参与方模型下提出了双服务器辅助的代理PSI协议，参与方的计算和通信复杂度与集合大小呈线性关系。同样地，张恩等人[67]在2018年基于BF以及同态加密、代理重加密技术提出了半诚实敌手模型下的代理多方PSI协议。

对典型的代理多方PSI协议的比较如表3所示。其中，公平性是指所有参与方均能获得交集计算结果，可验证是指客户端可以验证交集结果的正确性。

从功能上来讲，传统多方还有其他变体，如多对一PSI协议[69]和多方PSI-CA协议[70–73]，同时在其他隐私计算领域如纵向联邦学习方面也发挥了重要作用[77]。

通常，两方PSI仅涉及1个服务端和1个客户端，但不排除多个客户端同时分别向1个服务端请求交集计算的需求。在此场景下，通用的方法是服务端分别与每个客户端均经历1次完整的两方PSI协议。这可能会给服务端带来沉重的、不可扩展的代价。2017年，Hu等人[69]针对上述场景提出了多对一的PSI协议。主要思想为：将所有客户端虚拟成一个虚拟的客户端后，使用类似Pinkas等人[18]的方法与服务器端进行交互，并且使用依赖于服务器辅助的秘密加密方案保护客户端的隐私。

多方PSI-CA协议的主要功能是在超过两个参与方($n \geqslant 3$)参与、不泄露其他隐私的前提下协同计算所有参与方集合交集的大小。

2020年，Debnath等人[70]基于BF和ElGamal同态加密提出了在半诚实敌手模型和Diffie-Hellman假设下安全的多方PSI-CA协议，是第1个实现计算和通信复杂度与输入集合呈线性关系的方案。同年，Shi提出了基于量子的多方PSI-CA协议[71]，借助量子计算的并行性显著降低通信复杂度至$O\left(n^2\right)$，与其他传统多方PSI-CA相比，敌手即使拥有无限的计算能力去窃听或攻击，势必会改变其量子状态被通信方发现，保障了密码系统的无条件安全性，也称信息论安全性。

2022年，赵雪玲等人[72]基于门限ElGamal同态加密在不泄露交集内容的情况下，构造了半诚实敌手模型下的多方集合交(并)集的势与阈值、元素与多方集合交(并)集、集合与多方集合交(并)集关系的判定3类协议。

4　门限多方PSI技术

根据门限多方PSI的功能可以将其分为以下两种：假设t为门限值，一种是对元素出现次数的约束，让每个参与方知道自己有哪些元素出现在超过t个参与方的集合中[78]；另一种是对交集大小的约束，当交集大小大于t时，输出交集[6]。

4.1　约束元素出现次数的方案

2004年，Kissner等人[78]首先提出对元素出现次数进行门限约束的半诚实敌手模型下的多方PSI协议。他们允许多个参与方进行交集计算，且参与方的私有集合可以是多重集。协议中所有参与者均可得知哪些元素至少t次出现在输入集合里，

表 3　代理多方PSI协议比较表

协议	敌手模型		公平性	可验证	服务器数量
	服务器	客户端			
文献[58]	半诚实、恶意	恶意	√	√	1
文献[59]	诚实	半诚实	√	×	1
文献[60]	诚实	半诚实	√	×	1
文献[61]	半诚实	半诚实	×	×	1
文献[62]	半诚实	半诚实	×	×	1
文献[63]	恶意	半诚实	×	√	1
文献[64]	半诚实	半诚实	×	×	1
文献[65]	半诚实	半诚实	×	×	1
文献[66]	半诚实、社会理性	社会理性	√	×	2
文献[67]	半诚实	半诚实	√	×	2
文献[68]	半诚实	半诚实	√	×	1

并且可以明确得知出现的次数。该协议使用加法同态加密系统和多项式环等密码学原语，需要$O(n)$轮交互，本地计算分解$O(nm)$次的多项式或使用$O(nm)$个点重构多项式，因此造成了较高的计算和通信开销。此后，现有的方案主要聚焦于通信开销优化和计算开销优化两个方面。

在通信开销优化方面，Mahdavi等人[79]在2020年利用Shamir秘密共享[80]、OPRF和Paillier同态加密[81]构造不经意伪随机秘密共享(Oblivious Pseudo-Random Secret Sharing, OPR-SS)协议，而后提出了新的门限多方PSI协议并与Kissner等人[78]的方案进行对比，将通信轮数降低到了常数轮并显著减少了通信开销。

在计算开销优化方面，为了避免多项式求值和插值带来昂贵的计算开销，利用和两方PSI相同的方法，可以使用BF代替多项式来存储数据，如2015年Miyaji等人[59]提出的代理门限多方PSI协议。该方案中，每一方的集合大小是独立的，不需要所有参与方的集合大小均相等，所以该协议在私有集合大小方面具有较好的可扩展性。同样基于BF，Bay等人[40]在2021年提出的门限多方PSI协议中采用基于同态加密的私有元素安全比较协议(Secure Comparison Protocol, SCP)[82]来判断两个加密元素的大小关系，在计算复杂度和通信复杂度上均与最大集合元素数目呈线性关系，同时此协议也是第1个开源的对元素出现次数约束的门限多方PSI协议。

除此之外，由于混淆电路具有计算任何功能函数的特性，可以方便地设计多功能的安全计算协议，因此基于混淆电路的门限多方PSI也是研究方向之一。2021年，Chandran等人[83]提出了半诚实敌手模型下的多方PSI协议，并设计了两种变体协议，门限多方PSI便在其研究范围中。协议主要分两部分，首先选择一个特定参与方与其他所有参与方两两交互进行元素相等性判断，此后所有参与方交互通过电路计算结果。

约束元素出现次数的门限多方PSI协议的比较结果如表4所示。

4.2 约束交集大小的方案

自Freedman等人[6]在2004年提出两方门限的概念开始，对两方门限PSI协议的研究从未间断。门限两方PSI是指判断两个参与方的隐私集合交集的大小是否大于某个设定的门限值或两个参与方的隐私集合的差集不大于某个设定的门限值，如果满足条件，则输出交集，典型的门限两方PSI协议如文献[84–88]。

2019年Ghosh等人[86]对开销为次线性的门限两方PSI协议进行研究，主要解决当两个参与方私有集合相差小于门限时计算并输出交集的问题；同时提出了一种基于加法全同态加密的多方交集大小测试协议[89]和一种基于通用安全多方计算的门限多方PSI协议，通信复杂度均满足上界为$\tilde{O}(t)$。虽然其讨论了通信复杂度的上界，但是从实用的角度来看，该协议只是理论研究，开发高效的协议仍是有待解决的问题。

2021年，Badrinarayanan等人[90]基于文献[86]，研究了门限多方PSI的通信上界的问题。在协议中，研究者考虑了两个功能：一是所有参与方的集合与交集差集元素个数不超过门限t，则输出交集；二是如果各个参与方的集合并集与交集的差集不超过门限t，则输出交集。指出所有满足上述两个条件之一的门限多方PSI协议均拥有通信上限$\Omega(nT)$，并且基于门限全同态加密构造了通信复杂度为$O(nT)$的门限多方PSI协议，解决了Ghosh等人[86]的协议中两方扩展为多方需要多轮通信的问题。

近年来，对多方交集求势协议也有了进一步研究，如Branco等人[91]提出的基于多项式插值和不经意矩阵乘法的集合大小测试协议，主要功能是判断n个参与方私有集合交集大小是否大于$n-t$。与

表 4 约束元素出现次数的门限多方PSI协议比较

协议	安全性	抗勾结	通信复杂度		计算复杂度	
			Leader	Client	Leader	Client
文献[40]	半诚实	√	$O\left(mn\ell\log_2{}^{\lvert X\rvert}\right)$	$O\left(\max(\lambda,n)\,m\log_2{}^{\lvert X\rvert}\right)$	$O(mn)$	$O(\max(\lambda,n)\,m)$
文献[59]	半诚实	×	$O\left(\lambda n^2 m\log_2{}^{\lvert X\rvert}\right)$	$O\left(n^2 m\log_2{}^{\lvert X\rvert}\right)$	$O\left(\lambda nm\log_2{}^{\lvert X\rvert}\right)$	$O(\lambda nm)$
文献[78]	半诚实	√	$O(n^3 m\lambda)$	$O(n^3 m\lambda)$	$O(t^4 n^2 m^2)$	$O(t^4 n^2 m^2)$
文献[79]	半诚实	√	$O(nmtw)$	$O(nmtw)$	$O\left(m\left(n\log_2{}^{m/t}\right)^{2t}\right)$	$O\left(m\left(n\log_2{}^{m/t}\right)^{2t}\right)$
文献[83]	半诚实	√	$O(nm(\lambda+\kappa+\log_2{}^m))$	$O(m(\lambda+\kappa+\log_2{}^m))$	$O(nm\kappa)$	$O(m\kappa)$

注：在复杂度对比中，n为参与方数目，w为腐败方数目，t为协议门限值，m为集合大小，λ和κ分别为统计和计算安全参数，ℓ为同态公钥加密系统的门限值，$\log_2{}^{|X|}$为二进制密文X的大小。补充说明的是：任意腐败方数目w的最大值应小于总参与方数目。

Badrinarayanan等人[90]的协议相同点是，该协议也是将Ghosh等人[86]的协议从两方扩展为多方。该方案使用门限加法同态公钥加密系统来代替文献[86]中的OLE，提出的门限多方PSI协议的通信复杂度为$O\left(nt^2\kappa\lambda\right)$。约束交集大小的门限多方PSI协议的比较结果如表5所示。

表 5　约束交集大小的门限多方PSI协议比较

协议	安全性	抗勾结	通信轮数	通信复杂度
文献[86]	半诚实	×	$O\left(n\right)$	$O\left((nt)^2\right)$
文献[90]	半诚实	√	$O\left(1\right)$	$O\left(nt\cdot\mathrm{poly}\left(\lambda\right)\right)$
文献[91]	半诚实	√	$O\left(1\right)$	$O\left(nt^2\kappa\lambda\right)$

注：在复杂度对比中，n为参与方数目，t为协议门限值，λ和κ分别为统计和计算安全参数。

5　结论与展望

多方PSI技术是安全多方计算的重要模块之一，在医疗、交通及联系人追踪等多个领域均有所应用。本文主要对多方PSI技术进行了详细分类，梳理和概述了其发展历程和方案构造，对比了典型方案所采用的密码技术、安全性及计算和通信复杂度。

从传统多方PSI方案主要采用的密码技术来看，同态加密的应用极大地方便了加密数据的求和与乘积运算，多个参与方通过将私有数据集插值成多项式，对多项式的系数使用同态加密技术进行加密，以便其他参与方在不解密的情况下正确计算。但是同态加密需要大量的公钥操作，且多项式插值技术也会带来额外的计算开销，而在基于OT扩展的多方PSI协议中，OT扩展协议使用少量的公钥结合对称密钥即可产生大量OT实例，节约计算开销，其中公钥操作的数目是固定的，不依赖于数据集的大小，可扩展性较好。在相同的安全参数下，基于OT扩展的协议比基于公钥的协议总通信复杂度略高，总计算复杂度显著降低。通常来讲，使用OT扩展技术构造单点OPRF、多点OPRF或OPPRF，既保证了安全性，也可以在没有显著增加通信开销的同时，降低计算复杂度。

在安全性方面，基于公钥的多方PSI协议可以使用零知识证明来对抗恶意敌手，基于OT扩展的协议可以使用cut-and-choose技术来对抗恶意敌手。无论多方PSI协议是半诚实敌手模型下安全还是恶意敌手模型下安全，多数多方PSI协议可以通过采用GBF或多项式等数据结构、门限加法同态加密或零秘密共享等密码技术来抵抗任意参与方勾结，但是部分协议赋予了中心参与方或者部分参与方太大的权力，导致协议仅能抵抗半数腐败方勾结，甚至不能抵抗腐败方相互勾结。

展望多方PSI技术在未来的研究方向，主要可以归纳为以下3个方面。

第一，门限多方PSI协议的效率优化问题研究。虽然现有的门限多方PSI协议在通信开销上达到渐近最优，但因其使用了大量的同态公钥加密操作，计算开销过大，难以在实际场景中应用。如何借鉴基于OT扩展的传统多方PSI协议的优势，提高门限多方PSI的计算效率和实用性是未来的研究重点。

第二，多方PSI协议中各参与方之间的开销平衡问题研究。现有多方PSI协议常用星型通信结构，导致中心参与方的开销过大。如何选取合适的通信结构来平衡协议中各参与方的开销，是未来的发展方向。

第三，新场景下的多方PSI协议构造。考虑交集小于某门限值时输出交集的情况，以及在交集输出阶段，并不是所有参与方都同时在线的场景，设计交集小于某门限值或交集在某一个区间时输出交集的多方PSI协议和对获得交集的参与方数目进行约束的多方PSI协议是重要的研究方向。

参 考 文 献

[1] HALLGREN P, ORLANDI C, and SABELFELD A. PrivatePool: Privacy-preserving ridesharing[C]. 2017 IEEE 30th Computer Security Foundations Symposium, Santa Barbara, USA, 2017: 276–291. doi: 10.1109/CSF.2017.24.

[2] European Union. Regulation (EU) 2016/679 of the European parliament and of the council[R]. Brussels: European Union, 2016.

[3] ZHAO Chuan, ZHAO Shengnan, ZHAO Minghao, *et al*. Secure multi-party computation: Theory, practice and applications[J]. *Information Sciences*, 2019, 476: 357–372. doi: 10.1016/j.ins.2018.10.024.

[4] MEADOWS C. A more efficient cryptographic matchmaking protocol for use in the absence of a continuously available third party[C]. 1986 IEEE Symposium on Security and Privacy, Oakland, USA, 1986: 134–134. doi: 10.1109/SP.1986.10022.

[5] HUBERMAN B A, FRANKLIN M, and HOGG T. Enhancing privacy and trust in electronic communities[C]. The 1st ACM Conference on Electronic Commerce, Denver, USA, 1999: 78–86. doi: 10.1145/336992.337012.

[6] FREEDMAN M J, NISSIM K, and PINKAS B. Efficient private matching and set intersection[C]. International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2004: 1–19. doi: 10.1007/978-3-540-24676-3_1.

[7] DE CRISTOFARO E and TSUDIK G. Practical private set intersection protocols with linear complexity[C]. 14th International Conference on Financial Cryptography and Data Security, Tenerife, Spain, 2010: 143–159. doi: 10.1007/978-3-642-14577-3_13.

[8] FREEDMAN M J, HAZAY C, NISSIM K, *et al*. Efficient set intersection with simulation-based security[J]. *Journal of Cryptology*, 2016, 29(1): 115–155. doi: 10.1007/s00145-014-9190-0.

[9] 窦家维, 刘旭红, 周素芳, 等. 高效的集合安全多方计算协议及应用[J]. 计算机学报, 2018, 41(8): 1844–1860. doi: 10.11897/SP.J.1016.2018.01844.

DOU Jiawei, LIU Xuhong, ZHOU Sufang, *et al*. Efficient secure multiparty set operations protocols and their application[J]. *Chinese Journal of Computers*, 2018, 41(8): 1844–1860. doi: 10.11897/SP.J.1016.2018.01844.

[10] 周素芳, 李顺东, 郭奕旻, 等. 保密集合相交问题的高效计算[J]. 计算机学报, 2018, 41(2): 464–480. doi: 10.11897/SP.J.1016.2018.00464.

ZHOU Sufang, LI Shundong, GUO Yimin, *et al*. Efficient secure set intersection problem computation[J]. *Chinese Journal of Computers*, 2018, 41(2): 464–480. doi: 10.11897/SP.J.1016.2018.00464.

[11] 唐春明, 林旭慧. 隐私保护集合交集计算协议[J]. 信息网络安全, 2020, 20(1): 9–15. doi: 10.3969/j.issn.1671-1122.2020.01.002.

TANG Chunming and LIN Xuhui. Protocol of privacy-preserving set intersection computation[J]. *Netinfo Security*, 2020, 20(1): 9–15. doi: 10.3969/j.issn.1671-1122.2020.01.002.

[12] HUANG Yan, EVANS D, and KATZ J. Private set intersection: Are garbled circuits better than custom protocols?[C]. 19th Annual Network and Distributed System Security Symposium, San Diego, USA, 2012.

[13] PINKAS B, SCHNEIDER T, SEGEV G, *et al*. Phasing: Private set intersection using permutation-based hashing[C]. The 24th USENIX Conference on Security Symposium, Washington, USA, 2015: 515–530.

[14] PINKAS B, SCHNEIDER T, WEINERT C, *et al*. Efficient circuit-based PSI via cuckoo hashing[C]. 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, 2018: 125–157. doi: 10.1007/978-3-319-78372-7_5.

[15] PINKAS B, SCHNEIDER T, TKACHENKO O, *et al*. Efficient circuit-based PSI with linear communication[C]. 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, 2019: 122–153. doi: 10.1007/978-3-030-17659-4_5.

[16] CHANDRAN N, GUPTA D, and SHAH A. Circuit-PSI with linear complexity via relaxed batch OPPRF[J]. *Proceedings on Privacy Enhancing Technologies*, 2022, 2022(1): 353–372. doi: 10.2478/popets-2022-0018.

[17] DONG Changyu, CHEN Liqun, and WEN Zikai. When private set intersection meets big data: An efficient and scalable protocol[C]. The 2013 ACM SIGSAC Conference on Computer & Communications Security, Berlin, Germany, 2013: 789–800. doi: 10.1145/2508859.2516701.

[18] PINKAS B, SCHNEIDER T, and ZOHNER M. Faster private set intersection based on OT extension[C]. The 23rd USENIX Conference on Security Symposium, San Diego, USA, 2014: 797–812.

[19] KOLESNIKOV V, KUMARESAN R, ROSULEK M, *et al*. Efficient batched oblivious PRF with applications to private set intersection[C]. The 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 2016: 818–829. doi: 10.1145/2976749.2978381.

[20] ORRÙ M, ORSINI E, and SCHOLL P. Actively secure 1-out-of-N OT extension with application to private set intersection[C]. Cryptographers' Track at the RSA Conference 2017, San Francisco, USA, 2017: 381–396. doi: 10.1007/978-3-319-52153-4_22.

[21] RINDAL P and ROSULEK M. Improved private set intersection against malicious adversaries[C]. 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, 2017: 235–259. doi: 10.1007/978-3-319-56620-7_9.

[22] RINDAL P and ROSULEK M. Malicious-secure private set intersection via dual execution[C]. The 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, USA, 2017: 1229–1242. doi: 10.1145/3133956.3134044.

[23] PINKAS B, SCHNEIDER T, and ZOHNER M. Scalable private set intersection based on OT extension[J]. *ACM Transactions on Privacy and Security*, 2018, 21(2): 7. doi: 10.1145/3154794.

[24] PINKAS B, ROSULEK M, TRIEU N, *et al*. SpOT-light: Lightweight private set intersection from sparse OT extension[C]. 39th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, 2019: 401–431. doi: 10.1007/978-3-030-26954-8_13.

[25] PINKAS B, ROSULEK M, TRIEU N, *et al*. PSI from PaXoS: Fast, malicious private set intersection[C]. 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques on Advances in

Cryptology, Zagreb, Croatia, 2020: 739–767. doi: 10.1007/978-3-030-45724-2_25.

[26] CHASE M and MIAO Peihan. Private set intersection in the internet setting from lightweight oblivious PRF[C]. 40th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, 2020: 34–63. doi: 10.1007/978-3-030-56877-1_2.

[27] RINDAL P and SCHOPPMANN P. VOLE-PSI: Fast OPRF and circuit-PSI from vector-OLE[C]. 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, Zagreb, Croatia, 2021: 901–930. doi: 10.1007/978-3-030-77886-6_31.

[28] 程楠, 赵运磊. 一种高效的关于两方集合并/交集基数的隐私计算方法[J]. 密码学报, 2021, 8(2): 352–364. doi: 10.13868/j.cnki.jcr.000443.
CHENG Nan and ZHAO Yunlei. Efficient approach regarding two-party privacy-preserving set union/intersection cardinality[J]. *Journal of Cryptologic Research*, 2021, 8(2): 352–364. doi: 10.13868/j.cnki.jcr.000443.

[29] 申立艳, 陈小军, 时金桥, 等. 隐私保护集合交集计算技术研究综述[J]. 计算机研究与发展, 2017, 54(10): 2153–2169. doi: 10.7544/issn1000-1239.2017.20170461.
SHEN Liyan, CHEN Xiaojun, SHI Jinqiao, *et al*. Survey on private preserving set intersection technology[J]. *Journal of Computer Research and Development*, 2017, 54(10): 2153–2169. doi: 10.7544/issn1000-1239.2017.20170461.

[30] 崔泓睿, 刘天怡, 郁昱. 带隐私保护的集合交集计算协议的发展现状综述[J]. 信息安全与通信保密, 2019(3): 48–67. doi: 10.3969/j.issn.1009-8054.2019.03.010.
CUI Hongrui, LIU Tianyi, and YU Yu. A survey on private set intersection[J]. *Information Security and Communications Privacy*, 2019(3): 48–67. doi: 10.3969/j.issn.1009-8054.2019.03.010.

[31] 魏立斐, 刘纪海, 张蕾, 等. 面向隐私保护的集合交集计算综述[J]. 计算机研究与发展, 2022, 59(8): 1782–1799. doi: 10.7544/issn1000-1239.20210685.
WEI Lifei, LIU Jihai, ZHANG Lei, *et al*. Survey of privacy preserving oriented set intersection computation[J]. *Journal of Computer Research and Development*, 2022, 59(8): 1782–1799. doi: 10.7544/issn1000-1239.20210685.

[32] 黄翠婷, 张帆, 孙小超, 等. 隐私集合求交技术的理论与金融实践综述[J]. 信息通信技术与政策, 2021, 47(6): 50–56. doi: 10.12267/j.issn.2096-5931.2021.06.006.
HUANG Cuiting, ZHANG Fan, SUN Xiaochao, *et al*. A survey of private set intersection technology and finance practice[J]. *Information and Communications Technology and Policy*, 2021, 47(6): 50–56. doi: 10.12267/j.issn.2096-5931.2021.06.006.

[33] RABIN M O. How to exchange secrets with oblivious transfer[R]. Cambridge: Harvard University, 2005.

[34] ISHAI Y, KILIAN J, NISSIM K, *et al*. Extending oblivious transfers efficiently[C]. 23rd Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, 2003: 145–161. doi: 10.1007/978-3-540-45146-4_9.

[35] KOLESNIKOV V and KUMARESAN R. Improved OT extension for transferring short secrets[C]. 33rd Annual Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, 2013: 54–70. doi: 10.1007/978-3-642-40084-1_4.

[36] YANG Kang, WENG Chenkai, LAN Xiao, *et al*. Ferret: Fast extension for correlated OT with small communication[C/OL]. The 2020 ACM SIGSAC Conference on Computer and Communications Security, 2020: 1607–1626. doi: 10.1145/3372297.3417276.

[37] KISSNER L and SONG D. Privacy-preserving set operations[C]. 25th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, 2005: 241–257. doi: 10.1007/11535218_15.

[38] HAZAY C and VENKITASUBRAMANIAM M. Scalable multi-party private set-intersection[C]. 20th IACR International Conference on Practice and Theory in Public-Key Cryptography, Amsterdam, The Netherlands, 2017: 175–203. doi: 10.1007/978-3-662-54365-8_8.

[39] BAY A, ERKIN Z, ALISHAHI M, *et al*. Multi-party private set intersection protocols for practical applications[C/OL]. The 18th International Conference on Security and Cryptography, 2021: 515–522. doi: 10.5220/0010547605150522.

[40] BAY A, ERKIN Z, HOEPMAN J H, *et al*. Practical multi-party private set intersection protocols[J]. *IEEE Transactions on Information Forensics and Security*, 2022, 17: 1–15. doi: 10.1109/TIFS.2021.3118879.

[41] VOS J, CONTI M, and ERKIN Z. Fast multi-party private set operations in the star topology from secure ANDs and ORs[EB/OL].https://eprint.iacr.org/2022/721, 2022.

[42] 张蕾, 贺崇德, 魏立斐. 高效且恶意安全的三方小集合隐私交集计算协议[J]. 计算机研究与发展, 2022, 59(10): 2286–2298. doi: 10.7544/issn1000-1239.20220471.
ZHANG Lei, HE Chongde, and WEI Lifei. Efficient and malicious secure three-party private set intersection computation protocols for small sets[J]. *Journal of Computer Research and Development*, 2022, 59(10): 2286–2298. doi: 10.7544/issn1000-1239.20220471.

[43] LI Ronghua and WU Chuankun. An unconditionally secure protocol for multi-party set intersection[C]. 5th International Conference on Applied Cryptography and Network Security, Zhuhai, China, 2007: 226–236. doi: 10.

1007/978-3-540-72738-5_15.

[44] SANG Yingpeng and SHEN Hong. Privacy preserving set intersection protocol secure against malicious behaviors[C]. Eighth International Conference on Parallel and Distributed Computing, Applications and Technologies, Adelaide, Australia, 2007: 461–468. doi: 10.1109/PDCAT.2007.59.

[45] SANG Yingpeng and SHEN Hong. Privacy preserving set intersection based on bilinear groups[C]. The Thirty-First Australasian Conference on Computer Science, Wollongong, Australia, 2008: 47–54.

[46] SANG Yingpeng and SHEN Hong. Efficient and secure protocols for privacy-preserving set operations[J]. *ACM Transactions on Information and System Security*, 2009, 13(1): 9. doi: 10.1145/1609956.1609965.

[47] CHEON J H, JARECKI S, and SEO J H. Multi-party privacy-preserving set intersection with quasi-linear complexity[J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2012, E95.A(8): 1366–1378. doi: 10.1587/transfun.E95.A.1366.

[48] GHOSH S and NILGES T. An algebraic approach to maliciously secure private set intersection[C]. 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, 2019: 154–185. doi: 10.1007/978-3-030-17659-4_6.

[49] QIU Zhi, YANG Kang, YU Yu, *et al*. Maliciously secure multi-party PSI with lower bandwidth and faster computation[C]. 24th International Conference on Information and Communications Security, Canterbury, UK, 2022: 69–88. doi: 10.1007/978-3-031-15777-6_5.

[50] DEBNATH S K, CHOUDHURY T, KUNDU N, *et al*. Post-quantum secure multi-party private set-intersection in star network topology[J]. *Journal of Information Security and Applications*, 2021, 58: 102731. doi: 10.1016/j.jisa.2020.102731.

[51] KOLESNIKOV V, MATANIA N, PINKAS B, *et al*. Practical multi-party private set intersection from symmetric-key techniques[C]. The 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, USA, 2017: 1257–1272. doi: 10.1145/3133956.3134065.

[52] KAVOUSI A, MOHAJERI J, and SALMASIZADEH M. Efficient scalable multi-party private set intersection using oblivious PRF[C]. 17th International Workshop on Security and Trust Management, Darmstadt, Germany, 2021: 81–99. doi: 10.1007/978-3-030-91859-0_5.

[53] INBAR R, OMRI E, and PINKAS B. Efficient scalable multiparty private set-intersection via garbled bloom filters[C]. 11th International Conference on Security and Cryptography for Networks, Amalfi, Italy, 2018: 235–252. doi: 10.1007/978-3-319-98113-0_13.

[54] ZHANG En, LIU Fenghao, LAI Qiqi, *et al*. Efficient multi-party private set intersection against malicious adversaries[C]. The 2019 ACM SIGSAC Conference on Cloud Computing Security Workshop, London, England, 2019: 93–104. doi: 10.1145/3338466.3358927.

[55] BEN-EFRAIM A, NISSENBAUM O, OMRI E, *et al*. PSImple: Practical multiparty maliciously-secure private set intersection[C]. The 2022 ACM on Asia Conference on Computer and Communications Security, Nagasaki, Japan, 2022: 1098–1112. doi: 10.1145/3488932.3523254.

[56] NEVO O, TRIEU N, and YANAI A. Simple, fast malicious multiparty private set intersection[C]. The 2021 ACM SIGSAC Conference on Computer and Communications Security, Seoul, Korea, 2021: 1151–1165. doi: 10.1145/3460120.3484772.

[57] GORDON S D, HAZAY C, and LE P H. Fully secure PSI via MPC-in-the-head[EB/OL]. https://eprint.iacr.org/2022/379, 2022.

[58] KAMARA S, MOHASSEL P, RAYKOVA M, *et al*. Scaling private set intersection to billion-element sets[C]. 18th International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 2014: 195–215. doi: 10.1007/978-3-662-45472-5_13.

[59] MIYAJI A and NISHIDA S. A scalable multiparty private set intersection[C]. 9th International Conference on Network and System Security, New York, USA, 2015: 376–385. doi: 10.1007/978-3-319-25645-0_26.

[60] ZHU Hongliang, CHEN Meiqi, SUN Maohua, *et al*. Outsourcing set intersection computation based on bloom filter for privacy preservation in multimedia processing[J]. *Security and Communication Networks*, 2018, 2018: 5841967. doi: 10.1155/2018/5841967.

[61] 王勤, 魏立斐, 刘纪海, 等. 基于云服务器辅助的多方隐私交集计算协议[J]. 计算机科学, 2021, 48(10): 301–307. doi: 10.11896/jsjkx.210300308.

WANG Qin, WEI Lifei, LIU Jihai, *et al*. Private set intersection protocols among multi-party with cloud server aided[J]. *Computer Science*, 2021, 48(10): 301–307. doi: 10.11896/jsjkx.210300308.

[62] ABADI A, TERZIS S, and DONG Changyu. O-PSI: Delegated private set intersection on outsourced datasets[C]. 30th IFIP TC 11 International Conference on ICT Systems Security and Privacy Protection, Hamburg, Germany, 2015: 3–17. doi: 10.1007/978-3-319-18467-8_1.

[63] ABADI A, TERZIS S, and DONG Changyu. VD-PSI: Verifiable delegated private set intersection on outsourced private datasets[C]. 20th International Conference on Financial Cryptography and Data Security, Christ Church,

Barbados, 2016: 149–168. doi: 10.1007/978-3-662-54970-4_9.

[64] ABADI A, TERZIS S, METERE R, *et al*. Efficient delegated private set intersection on outsourced private datasets[J]. *IEEE Transactions on Dependable and Secure Computing*, 2019, 16(4): 608–624. doi: 10.1109/TDSC.2017.2708710.

[65] ABADI A, DONG Changyu, MURDOCH S J, *et al*. Multi-party updatable delegated private set intersection[C]. 26th International Conference on Financial Cryptography and Data Security, Grenada, Grenada, 2022: 100–119. doi: 10.1007/978-3-031-18283-9_6.

[66] ZHANG En, LI Fenghua, NIU Ben, *et al*. Server-aided private set intersection based on reputation[J]. *Information Sciences*, 2017, 387: 180–194. doi: 10.1016/j.ins.2016.09.056.

[67] 张恩, 金刚刚. 基于同态加密和Bloom过滤器的云外包多方隐私集合比较协议[J]. 计算机应用, 2018, 38(8): 2256–2260. doi: 10.11772/j.issn.1001-9081.2018010075.
ZHANG En and JIN Ganggang. Cloud outsourcing multiparty private set intersection protocol based on homomorphic encryption and Bloom filter[J]. *Journal of Computer Applications*, 2018, 38(8): 2256–2260. doi: 10.11772/j.issn.1001-9081.2018010075.

[68] MIYAJI A, NAKASHO K, and NISHIDA S. Privacy-preserving integration of medical data[J]. *Journal of Medical Systems*, 2017, 41(3): 37. doi: 10.1007/s10916-016-0657-4.

[69] HU Keji and ZHANG Wensheng. mPSI: Many-to-one private set intersection[C]. 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing, New York, USA, 2017: 187–192. doi: 10.1109/CSCloud.2017.35.

[70] DEBNATH S K, STĂNICĂ P, KUNDU N, *et al*. Secure and efficient multiparty private set intersection cardinality[J]. *Advances in Mathematics of Communications*, 2021, 15(2): 365–386. doi: 10.3934/amc.2020071.

[71] SHI Runhua. Quantum multiparty privacy set intersection cardinality[J]. *IEEE Transactions on Circuits and Systems II:Express Briefs*, 2021, 68(4): 1203–1207. doi: 10.1109/TCSII.2020.3032550.

[72] 赵雪玲, 家珠亮, 李顺东. 集合交集问题的安全计算[J]. 密码学报, 2022, 9(2): 294–307. doi: 10.13868/j.cnki.jcr.000520.
ZHAO Xueling, JIA Zhuliang, and LI Shundong. A secure multiparty intersection computation[J]. *Journal of Cryptologic Research*, 2022, 9(2): 294–307. doi: 10.13868/j.cnki.jcr.000520.

[73] TRIEU N, YANAI A, and GAO Jiahui. Multiparty private set intersection cardinality and its applications[EB/OL]. https://eprint.iacr.org/2022/735, 2022.

[74] 杨亚涛, 赵阳, 张卷美, 等. 同态密码理论与应用进展[J]. 电子与信息学报, 2021, 43(2): 475–487. doi: 10.11999/JEIT191019.
YANG Yatao, ZHAO Yang, ZHANG Juanmei, *et al*. Recent development of theory and application on homomorphic encryption[J]. *Journal of Electronics & Information Technology*, 2021, 43(2): 475–487. doi: 10.11999/JEIT191019.

[75] DAVIDSON A and CID C. An efficient toolkit for computing private set operations[C]. 22nd Australasian Conference on Information Security and Privacy, Auckland, New Zealand, 2017: 261–278. doi: 10.1007/978-3-319-59870-3_15.

[76] GARIMELLA G, PINKAS B, ROSULEK M, *et al*. Oblivious key-value stores and amplification for private set intersection[C/OL]. 41st Annual International Cryptology Conference on Advances in Cryptology, 2021: 395–425. doi: 10.1007/978-3-030-84245-1_14.

[77] LU Linpeng and DING Ning. Multi-party private set intersection in vertical federated learning[C]. 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, Guangzhou, China, 2020: 707–714. doi: 10.1109/TrustCom50675.2020.00098.

[78] KISSNER L and SONG D. Private and threshold set-intersection[R]. Pittsburgh: Carnegie Mellon University, 2004.

[79] MAHDAVI R A, HUMPHRIES T, KACSMAR B, *et al*. Practical over-threshold multi-party private set intersection[C]. Annual Computer Security Applications Conference, Austin, USA, 2020: 772–783. doi: 10.1145/3427228.3427267.

[80] SHAMIR A. How to share a secret[J]. *Communications of the ACM*, 1979, 22(11): 612–613. doi: 10.1145/359168.359176.

[81] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]. International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, 1999: 223–238. doi: 10.1007/3-540-48910-X_16.

[82] KERSCHBAUM F, BISWAS D, and DE HOOGH S. Performance comparison of secure comparison protocols[C]. 2009 20th International Workshop on Database and Expert Systems Application, Linz, Austria, 2009: 133–136. doi: 10.1109/DEXA.2009.37.

[83] CHANDRAN N, DASGUPTA N, GUPTA D, *et al*. Efficient linear multiparty PSI and extensions to circuit/quorum PSI[C/OL]. The 2021 ACM SIGSAC Conference on Computer and Communications Security, 2021: 1182–1204. doi: 10.1145/3460120.3484591.

[84] ZHAO Yongjun and CHOW S S M. Are you the one to share? Secret transfer with access structure[J]. *Proceedings*

on Privacy Enhancing Technologies, 2017, 2017(1): 149–169. doi: 10.1515/popets-2017-0010.

[85] ZHAO Yongjun and CHOW S S M. Can you find the one for me?[C]. The 2018 Workshop on Privacy in the Electronic Society, Toronto, Canada, 2018: 54–65. doi: 10.1145/3267323.3268965.

[86] GHOSH S and SIMKIN M. The communication complexity of threshold private set intersection[C]. 39th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, 2019: 3–29. doi: 10.1007/978-3-030-26951-7_1.

[87] ZHANG En, CHANG Jian, and LI Yu. Efficient threshold private set intersection[J]. *IEEE Access*, 2021, 9: 6560–6570. doi: 10.1109/ACCESS.2020.3048743.

[88] ZHAO Shengnan, MA Ming, SONG Xiangfu, *et al*. Lightweight threshold private set intersection via oblivious transfer[C]. 16th International Conference on Wireless Algorithms, Systems, and Applications, Nanjing, China, 2021: 108–116. doi: 10.1007/978-3-030-86137-7_12.

[89] BONEH D, GENNARO R, GOLDFEDER S, *et al*. Threshold cryptosystems from threshold fully homomorphic encryption[C]. 38th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, 2018: 565–596. doi: 10.1007/978-3-319-96884-1_19.

[90] BADRINARAYANAN S, MIAO Peihan, RAGHURAMAN S, *et al*. Multi-party threshold private set intersection with sublinear communication[C/OL]. 24th IACR International Conference on Practice and Theory of Public Key Cryptography, 2021: 349–379. doi: 10.1007/978-3-030-75248-4_13.

[91] BRANCO P, DÖTTLING N, and PU Sihang. Multiparty cardinality testing for threshold private intersection[C/OL]. 24th IACR International Conference on Practice and Theory of Public Key Cryptography, 2021: 32–60. doi: 10.1007/978-3-030-75248-4_2.

高 莹：女，副教授，研究方向为隐私计算与密码学应用.

王 玮：女，硕士生，研究方向为多方隐私集合交集计算.

责任编辑：余 蓉