ICS 35.240.01
CCS L 67

# 团　　体　　标　　准

T/CCSA 793–2026　　T/CAAAD 044–2026

# 互联网广告 隐私计算应用指南

Internet advertisement——Privacy-preserving computing application scenario guide

2026–03–02 发布　　2026–06–01 实施

中国通信标准化协会　　中国广告协会　　发布

# 版权声明

# 目　　次

# 前　言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国通信标准化协会和中国广告协会共同提出并分别归口。

本文件起草单位：北京巨量引擎网络技术有限公司、杭州阿里妈妈软件服务有限公司、中国信息通信研究院、北京勾正数据科技有限公司、中国传媒大学、上海原锐广告有限公司、秒针信息技术有限公司。

本文件主要起草人：张贝贝、蔡权伟、赵乃萱、张吉、杜蕾、李昳婧、张若寒、秦超、杨晓静、杨正军、朱岩、杨阳、马磊、李蔚文、马澈、张继红、赵悦、胡春磊、于晓蕾。

# 引　言

互联网广告业务是数据使用、加工、提供和委托处理密集的行业领域。在广告投放、程序化交易、广告归因等场景，均涉及到个人信息相关的数据在不同机构间的提供、加工、传输、使用等处理行为，由于互联网广告业务的多机构参与的特点，而数据的流动和利用面临着数据泄露和滥用的风险。通过隐私计算的方式，可以实现数据“可用不可见”，有效控制了数据使用的过程和目的范围，同时克服多方数据利用过程中的信任问题，提升数据利用价值。

互联网广告领域，已经在多个场景尝试利用隐私计算的方案，梳理隐私计算方案在广告场景下的应用，为互联网广告行业的隐私计算应用打下基础。

为适应信息通信业发展对标准文件的需求，由中国通信标准化协会和中国广告协会共同组织制定该团体标准，推荐有关方面采用。有关对本文件的建议和意见，向中国通信标准化协会和中国广告协会反映。

# 互联网广告　隐私计算应用指南

## 1　范围

本文件规定了隐私计算在互联网广告应用的目标、原则和适用场景，明确了隐私计算的技术分类和应用价值。本文件提出了互联网广告场景下应用隐私计算技术的建议，并给出了应用场景和应用技术的相关信息。

本文件适用于各类互联网广告业务，包括广告投放、程序化交易、广告归因等应用场景下的数据处理活动。

## 2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 35273 信息安全技术 个人信息安全规范

## 3　术语、定义和缩略语

### 3.1　术语和定义

下列术语和定义适用于本文件。

3.1.1

**隐私计算 privacy-preserving computation**

在提供数据安全及隐私保护的基础上，实现数据价值挖掘的技术体系，通常可以理解为一系列技术与解决方案的合集，是一套包含人工智能、密码学、数据科学在内的领域交叉融合的技术体系。

3.1.2

**个人信息 personal information**

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

3.1.3

**程序化广告 programmatic advertising**

是一种建立在数据和技术基础之上的广告交易形式，通过数字化、自动化、系统化的方式将广告主、媒体平台进行程序化对接，实现广告投放的自动化、精准化。

3.1.4

**广告主 advertiser**

为推销商品或者服务，自行或者委托他人设计、制作、发布互联网广告的自然人、法人或者其他组织。

3.1.5

**广告需求方平台 ad Demand-side platform**

指整合广告主需求，通过数据整合分析实现精准投放，为广告主提供服务的平台。

3.1.6

**广告归因 ad attribution**

是用于确定一个广告在多个媒体曝光/点击并发生转化后效果的归属的过程。

3.1.7

**媒体 media**

发布、展示广告的载体。

3.1.8　**匿名化 anonymization**

是指个人信息经过处理无法识别特定自然人且不能复原的过程。

注：匿名化是去标识化的极端情况，即在特定条件下对特定自然人的重标识风险极低。

## 3.2　缩略语

下列缩略语适用于本文件。

ADX：广告交易市场（Advertising Exchange）

DMP：数据管理平台（Data Management Platform）

DSP：需求方平台（Demand Side Platform）

IDFA/OAID：广告标识符（Identifier For Advertising）

MPC：安全多方计算（Secure Multi-Party Computation）

PSI：隐私集合求交（Privacy Set Intersection）

# 4　互联网广告领域隐私计算原则

## 4.1　概述

互联网广告业务是数据使用、加工、提供和委托处理密集的行业领域。在广告投放、程序化交易、广告归因等场景，均涉及到个人信息相关的数据在不同机构间的共享、使用等处理行为。隐私计算的应用，可以帮助各方避免直接共享明文数据，通过技术手段限定各参与方对共享数据的处理目的，确保数据流转后被固化在特定框架内。

## 4.2　基本原则

### 4.2.1　合法性原则

互联网广告领域涉及个人信息处理，需遵守《个人信息保护法》等相关法律法规的规定；对个人信息的处理，需具备合法性基础。

#### 4.2.2　目的限定原则

互联网广告领域采用隐私计算技术进行数据处理，需具备明确、合理的目的，采用的隐私计算方式、个人信息处理行为与处理目的直接相关，采取对个人权益影响最小的方式。

#### 4.2.3　数据可用原则

数据作为新型生产要素，通过隐私计算的方式，可实现其在互联网广告领域的可用性，为数据要素安全流通提供基础保障。

#### 4.2.4　安全可信原则

安全可信原则既是对数据处理安全性的要求，也包含对数据处理质量的要求，数据处理需具有保密性、准确性和完整性。

## 5　互联网广告隐私计算主要技术

### 5.1　联邦学习

联邦学习是一种机器学习技术，各参与方的原始数据存储在本地，不进行交换或传输，通过特定的中间计算结果的传输和聚合来达到机器学习模型训练的目标。

互联网广告各参与方掌握有不同类型的用户数据，存在重叠用户较多且分别掌握不同特征的情况。可采用联邦学习技术利用重叠用户的不同特征建模，提升广告转化预估模型的准确度，提升广告投放的精准性。

联邦学习技术在安全性上，须关注：原始数据不离开本地，仅交换加密模型参数或梯度；采用同态加密、差分隐私等技术防止中间结果泄露；确保模型聚合过程抗恶意攻击（如数据中毒或模型窃取）。

同时，联邦学习技术的应用，须防范潜在安全性风险：模型更新的梯度或参数可能被逆向推断，泄露敏感信息的风险；参与方可能伪造数据或模型更新，影响全局模型准确性的风险；参与方故障或被攻击可能破坏系统信任的风险。

### 5.2　安全多方计算

安全多方计算是一种用于多方协作的分布式计算技术，在多个数据参与方进行共同计算的情况下，保证各个参与方在获取所需计算结果的同时不会泄露原始数据信息。安全多方计算能够满足利用隐私数据进行保密计算的需求，有效解决数据的保密性和共享性之间的矛盾。

同态加密作为安全多方计算常用技术之一，其主要特征是在密文上进行操作得到的结果，经过解密后，与对明文数据进行对应操作得到的结果是一致的。同态加密使得数据处理方在不获取敏感数据的前提下，完成数据的分析处理。

隐私集合求交是安全多方计算中的一种技术，它允许参与计算的双方，在不获取对方额外信息的基础上，计算出双方数据的交集。

程序化广告场景下，通常存在广告请求发送、广告归因等大量级的数据交互，隐私集合求交技术的应用，可以最小化的限缩参与方的数据共享范围，降低数据非授权利用的风险。

安全多方计算技术在安全性上，须关注：通过安全多方技术确保输入数据的机密性；协议需满足计算正确性、所选择安全模型（如半诚实安全模型或恶意安全模型）下的安全性；支持对参与方实施身份认证和权限控制。

安全多方计算技术的应用，须防范潜在安全性风险：协议实现错误导致安全性不符合预期，进而引入数据泄漏风险；所选用的安全模型与实际风险不匹配，导致协议安全性无法保障。

### 5.3　差分隐私

差分隐私是为了防范差分攻击等方式对自然人个体粒度的个人信息进行攻击和窃取，通过添加噪声的方式，既能够保障正常产出的数据分析结果，同时又能够在数据的收集、传输以及对外发布的不同阶段提供对个体粒度数据的隐私保护，使攻击者难以利用相关背景知识识别查询结果的差异性，进而避免个体粒度的个人信息遭到窃取和泄露。

广告归因场景中，归因结果是用户广告数据的统计值，差分隐私技术的应用，有效防范差分攻击，降低个人信息泄漏风险。

差分隐私技术在安全性上，须关注：结合系统设计、应用场景正确设置差分隐私参数 $\varepsilon$，并提供验证差分隐私算法安全验证所需的清单（如使用的差分隐私模型、需要保护的数据类型、需要进行扰动的查询函数、相邻数据集定义、敏感度定义、隐私预算及其消耗率等）。

差分隐私技术的应用，须防范潜在风险：数据可用性（数据一致性、准确性）无法保证；差分隐私参数相关因素取值与实际不匹配，导致隐私保护能力不符合预期。

### 5.4　可信执行环境

可信执行环境是一种基于硬件的技术，可信执行环境将数据、特定功能、应用程序与操作系统、系统管理程序或虚拟机管理器以及其他特定进程隔离，通过软硬件方法在中央处理器中构建一个安全飞地，无法从外部查看数据或执行操作。

可信执行环境为广告建模、广告归因和广告数据分析提供安全执行环境，在不泄漏各自数据的前提下，按照约定的使用目的和数据处理方式，完成建模、广告归因和广告数据分析。

可信执行环境技术在安全性上，须关注：通过硬件隔离技术确保代码与数据在安全区域内执行和处理；基于安全启动保证应用程序与操作系统在内的计算环境完整性和真实性。

可信执行环境技术的应用，须防范潜在安全性风险：硬件安全漏洞导致的数据泄漏风险、应用程序、操作系统等存在的漏洞导致的数据泄漏风险。

## 6　广告场景隐私计算应用指引

### 6.1　数据来源的合规性

隐私计算的数据来源需合规，数据获取需获取用户授权，避免侵犯用户的个人信息和商业秘密。对于个人信息的委托处理或向其他个人信息处理者提供的场景，按照《个人信息保护法》的规定取得相应的合法性基础，如获取用户的同意、完成个人信息保护影响评估等。

如在特定的隐私计算技术应用场景，对于个人信息的技术处理如达到了匿名化的标准，则对匿名化的个人信息的处理，不需要经过个人信息主体的同意。

### 6.2　数据处理目的的限定性

隐私计算技术用于数据处理需具备明确、合理的目的，明确采用隐私计算技术所要达成的目标。选用的隐私计算技术，与所有达成的数据处理目的直接相关，且隐私计算技术的运用可实现相应目的；避免选取的技术与目的不适配，不能实现隐私计算的目标与安全性。

选用的隐私计算技术，需限定数据仅能应用于数据处理，避免数据直接共享造成数据参与方潜在的数据滥用风险。

### 6.3　数据处理的最小必要性

在可实现数据处理目的的情形下，需尽可能处理最小范围内的数据，如涉及个人信息，宜采取对个人权益影响最小的方式。

### 6.4　算法能力和安全性

算法能力和安全宜从以下几个方面进行考虑:

a) 隐私计算技术选择保证参与方无法从计算过程中获得出最终输出之外的信息，攻击者也不能通过观察计算过程来推断出其他方的输入数据；
b) 隐私计算过程需在数据操作环节进行身份认证，对数据使用须进行授权管理，对关键操作宜进行日志存证，日志中须不包含敏感数据；
c) 隐私计算技术应用须保证结果数据的准确性，性能需满足使用要求；
d) 隐私计算涉及数据传输的，须建立安全通信通道，对通信数据进行机密性、完整性保护；
e) 隐私计算所采用的密码算法、密钥长度及密钥管理方式须符合国家密码管理部门与行业主管要求；
f) 数据存储须做好加密存储等措施，防范未经授权访问；敏感个人信息须采取适当的脱敏或加密安全措施。
g) 隐私计算参与方须加强风险监测，发现因自身所提供的技术导致数据可能被泄露、未经授权访问等数据安全事件风险时，及时采取相应的补救措施。

### 6.5　制度保障

隐私计算各参与方可从以下方面考虑，建立安全保障制度:

a) 隐私计算参与方之间需通过合同等形式明确约定隐私计算的目的、隐私计算结果使用目的、数据安全保障义务等；
b) 需要全面考虑来自数据加工和流通活动的各类主体以及相关内部人员作恶的风险，各参与方均要做好数据最小必要的权限管控；对参与人员进行数据合规相关培训，提升合规意识；
c) 如涉及使用独立第三方的技术服务，隐私计算参与方须对技术提供方的技术能力安全性和稳定性、数据安全能力等各方面进行前置评估，以确信技术服务方的服务能力满足要求；
d) 技术提供方涉及到数据处理的，隐私计算参与方与技术提供方需签署合同，明确约定数据处理目的、期限、处理方式，如涉及个人信息的，宜约定个人信息的种类、保护措施以及双方的权利和义务等内容，须要求技术提供方在完成隐私计算后及时删除或销毁相关数据以防止数据滥用或泄漏，不得逆推、还原或用其他手段获取数据提供方的原始数据信息，并采取适当措施对技术提供方的数据处理行为进行监督。

## 7　互联网广告隐私计算应用场景

### 7.1　广告建模

#### 7.1.1　场景

在广告投放过程中，广告主持有用户的特征、深度转化特征数据，广告平台持有用户的标签及特征数据。双方可通过隐私计算技术技术,利用双方的特征数据共同训练广告算法模型，提升广告投放效果。

### 7.1.2　技术选型

广告建模场景下可采用的隐私计算技术主要包括两类：联邦学习和可信执行环境，可结合差分隐私和安全多方计算技术一并应用，进一步提升技术的安全性。

### 7.1.3　技术方案（以纵向联邦学习技术为例）

广告平台与广告主通过纵向联邦学习进行模型训练方案如图 1 所示。

在模型训练阶段，双方通过隐私集合求交的技术进行加密样本对齐。对于交集用户，广告主将用户特征根据本地模型进行计算得到中间结果，并以同态加密、差分隐私等技术保护后，向广告平台发送。广告平台结合自身的特征、模型结构和标签数据，与接收到的中间结果进行样本拼接以及后续计算，并对自身模型参数进行梯度更新。同时向广告主回传保护后梯度中间数据，由广告主接收后更新本地模型。重复上述过程直至模型收敛。

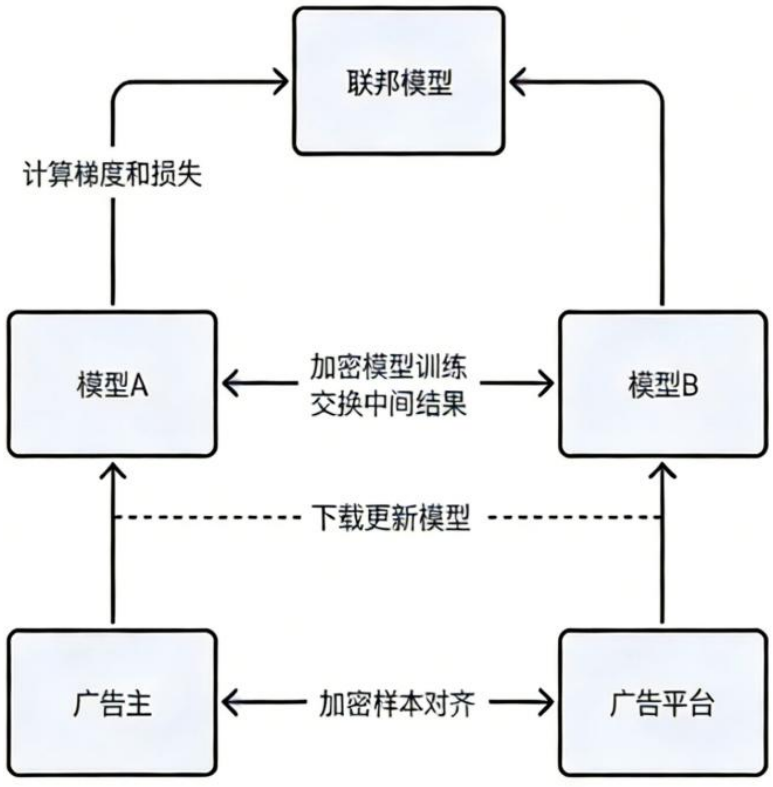


**图 1 广告建模场景技术方案流程图**

### 7.1.4　方案价值

联邦学习的方案之下，原始数据只在各参与方本地的联邦学习系统中进行计算，两方的系统之间只会传输加密后的中间结果，原始数据不会发生交互，一方面控制了数据处理的使用场景和目的，另一方面最大限度的降低了数据共享的范围。

## 7.2　程序化交易

### 7.2.1　场景

在程序化广告请求发送的场景下，第三方DSP平台拥有自己的DMP，广告平台向其发送包含用户ID的广告请求，由第三方DSP平台进行筛选后出价、竞价，完成程序化广告投放。为尽可能地降低广告请求发送过程中非必要的数据共享，可通过安全多方计算技术，降低数据共享的范围。

### 7.2.2　技术选型

程序化交易场景下主要采用安全多方计算技术，其中隐私集合求交技术应用范围最为广泛。

### 7.2.3　技术方案

广告平台与第三方DSP平台通过隐私集合求交的多方安全计算技术，进行程序化交易技术方案如图 2 所示：

a) 第三方 DSP 平台将用户 ID 信息哈希，并进行盲化处理后，发送给广告平台；
b) 广告平台收到第三方 DSP 平台盲化数据后，使用自身密钥完成密文处理后，返还给第三方 DSP 平台；
c) 广告平台同步将己方用户 ID 信息哈希后，使用自身密钥进行处理，发送给第三方 DSP 平台；
d) 第三方 DSP 平台对第三步消息去盲后，得到本方用户 ID 信息的密文，将其与广告平台发送的广告平台用户 ID 信息的密文进行匹配，最终匹配出交集用户。

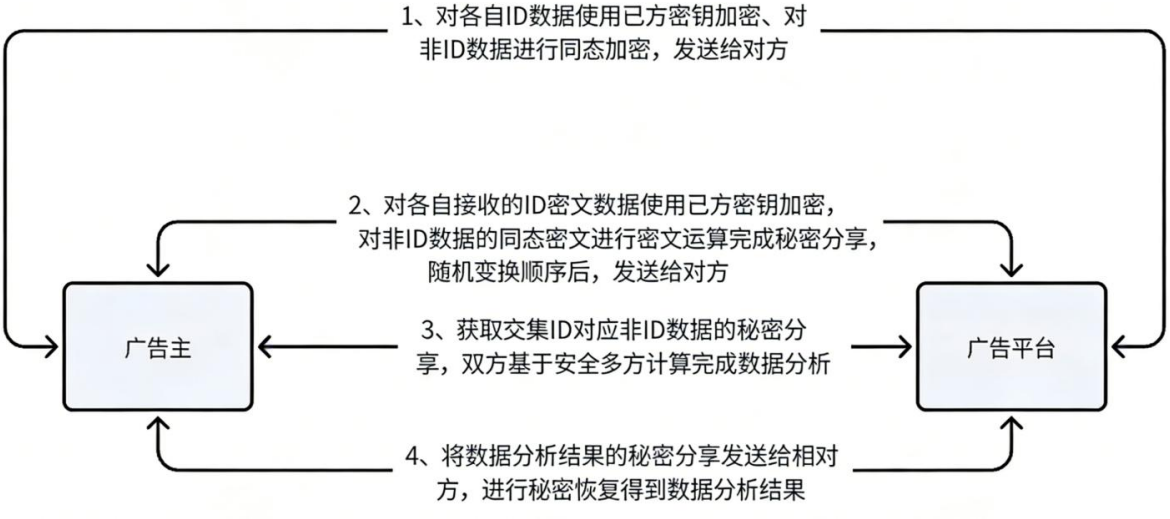


**图 2 程序化交易场景技术方案流程图**

### 7.2.4　方案价值

隐私集合求交的方案，参与计算的双方各自掌握密钥，各自只能获取最终交集用户，而无法获取对方非交集的用户信息，降低了数据共享的范围。

## 7.3　广告归因

### 7.3.1　场景

广告归因是用于确定一个广告在多个媒体曝光/点击并发生转化后效果的归属的过程。通常后链路转化数据由广告主，或为广告主提供技术服务的平台所掌握，因此广告归因需要双方数据合作完成。为降低归因过程中的数据共享，降低双方的隐私顾虑，可通过隐私计算技术方案，得出广告平台有触点行为用户和广告主转化用户的交集，进而实现归因。

### 7.3.2　技术选型

广告归因场景场景下采用的隐私计算技术包括：可信执行环境、安全多方计算、差分隐私，可以选择可信执行环境结合差分隐私技术方案，或者安全多方计算结合差分隐私的技术方案。

### 7.3.3　技术方案（以可信执行环境技术为例）

广告平台与广告主通过可信执行环境进行广告归因技术方案如图 3 所示：

a) 设置一个基于硬件的可信执行环境；
b) 广告主、广告平台把加密的转化数据和触点行为数据上传到可信执行环境中；同时将对应密钥上传至可信执行环境；
c) 加密数据在可信执行环境中经过解密处理后，完成计算，生成最终的交集用户数量，完成归因；
d) 归因结果在可信执行环境中根据差分隐私算法添加噪声后，最终发布。

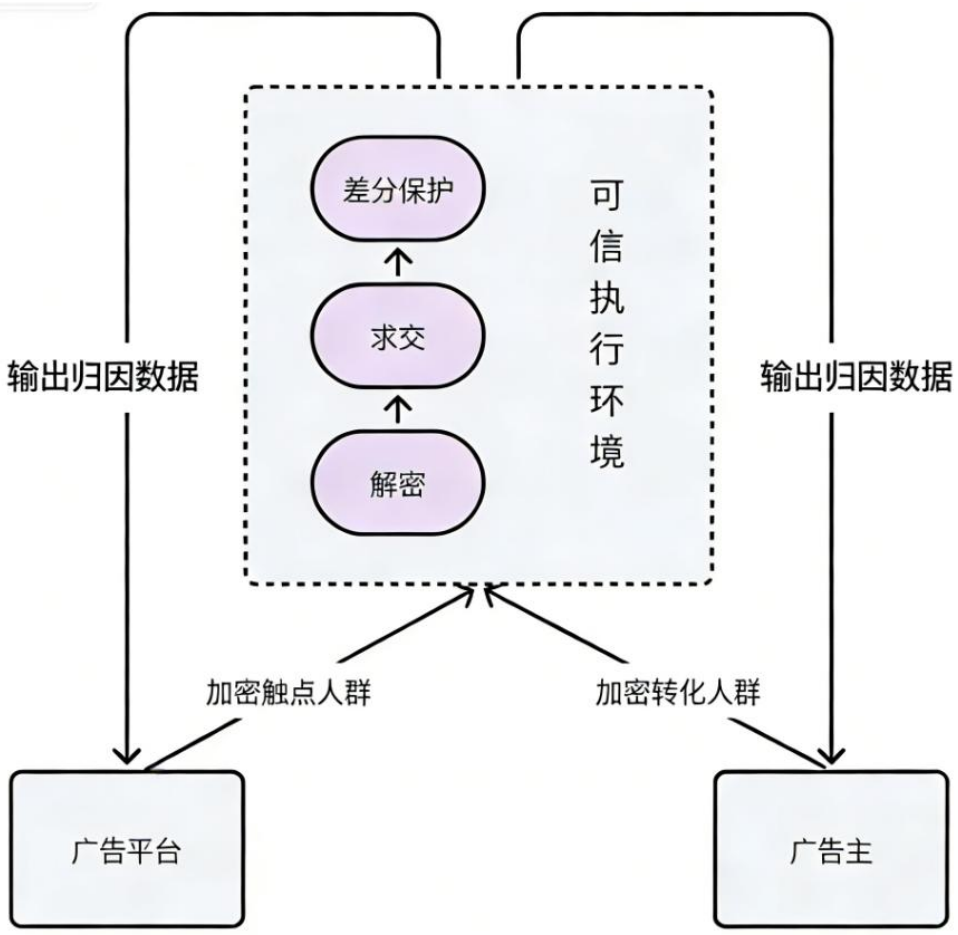


**图 3 广告归因场景技术方案流程图**

#### 7.3.4　方案价值

通过可信执行环境方案在隔离环境中完成相应的计算，一方面限制了数据的使用目的仅限于归因使用；另一方面，双方都无法接触对方的原始数据，最终只能得到归因的交集用户的统计数量，并非用户粒度的数据，避免了用户个人信息的共享；最后，统计数量经差分隐私保护，提升了个人信息面对差分攻击时的安全性。此方案中，个人信息经过加密处理后才上传到受控环境中，受控环境采用了可信计算等高安全保障的技术，同时对受控环境与外部交互的各个通道进行严格管控，仅有参与方可以知悉自己上传到受控环境的原始数据；相对方及非参与方均不得获取原始数据，最终受控环境输出的仅是广告归因后的群体数量信息，从输出的群体数量信息不可识别到特定个人信息主体，也不能复原到原始的个人信息，该技术也是匿名化处理个人信息的应用探索。

### 7.4　广告数据分析

#### 7.4.1　场景

广告数据分析为广告主对自己的数据进行共域数据洞察和分析的场景。通过隐私计算技术，可满足双方需要获知交集ID的数据分析结果的需求，同时避免相对方获取交集ID本身。

### 7.4.2　技术选型

广告数据分析场景下主要采用安全多方计算技术，常用技术包括隐私集合求交、同态加密、秘密分享等，通常会结合差分隐私技术一并使用。

### 7.4.3　技术方案

广告平台与广告主通过隐私集合求交进行广告数据分析技术方案如图 4 所示：

a) 广告主和广告平台对各自ID数据使用本方密钥加密、对非ID数据（行为、特征等数据）进行同态加密，发送给对方；

b) 双方对各自接收的相对方ID密文数据使用己方密钥加密，生成随机数对非ID数据的同态密文进行密文运算完成秘密分享，并将处理后的ID密文和非ID的同态密文随机变换顺序后，发送给对方；

c) 双方基于ID密文数据获取交集对应非ID数据的秘密分享，包括：针对本方数据，使用密钥解密同态密文；针对相对方的非ID数据，直接获取前述步骤中所使用的随机数；双方基于安全多方计算，在交集数据的秘密分享上完成数据分析（如加法、比较、乘法等），数据分析结果仍为秘密分享形式；

d) 双方将数据分析结果的秘密分享发送给相对方，相对方进行秘密恢复得到数据分析结果。

本方案中，ID数据使用双方密钥处理，且顺序被随机变换后，双方无法通过ID密文或相互顺序获取交集ID；非ID数据由同态加密保护，双方无法获取相对方的非ID数据；各自对相对方非ID数据的密文进行秘密分享，使得其无法通过非ID数据关联得到交集ID。

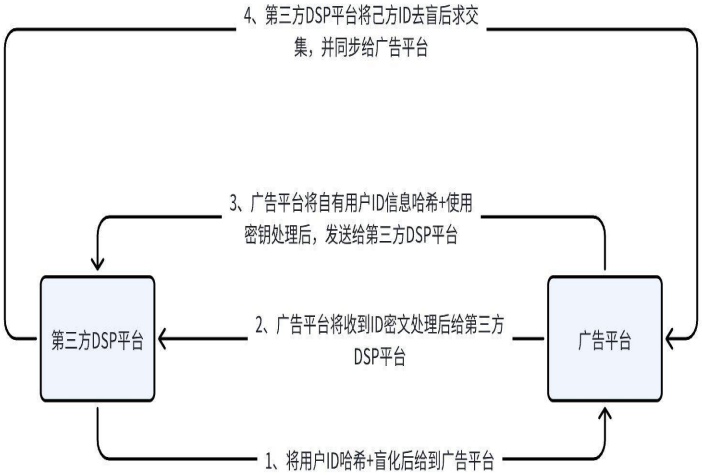


**图 4 广告数据分析场景技术方案流程图**

### 7.4.4　方案价值

在隐私集合求交方案之上仅能获取交集用户的数据分析结果（如交集数量），而不能获取特定的交集用户，进一步限制了各参与方通过隐私计算获取的信息范围。

## 参考文献

[1] GB/T 25069-2010 信息安全技术 术语
[2] GB/T 35273-2020 信息安全技术 个人信息安全规范
[3] GB/T 42574-2023 信息安全技术 个人信息处理中告知和同意的实施指南
[4] YD/T 4690-2024 隐私计算 多方安全计算产品安全要求和测试方法
[5] YD/T 4691-2024 隐私计算 联邦学习产品安全要求和测试方法
[6] YD/T 4947-2024 隐私计算 可信执行环境产品安全要求
[7] YD/T 4581-2024 隐私保护场景下安全多方计算技术指南
[8] 《中华人民共和国数据安全法》
[9] 《中华人民共和国个人信息保护法》
[10] 《电信和互联网个人信息主体个人信息保护规定》（2013 年 7 月 16 日中华人民共和国工业和信息化部第 24 号令公布）
[11] 《隐私计算法律使用规则报告》（2022 年抖音集团数据及隐私法务）
[12] 《联邦学习技术及实战》（彭南博、王虎等著）
[13] 《隐私计算产品通用安全分级白皮书》隐私计算联盟；
[14] 《隐私计算技术应用合规指南（2022 年）》中国信息通信研究院云计算与大数据研究所；