ICS 01.100.01
CCS J 04

团　　体　　标　　准

T/SCGS 313007—2024

隐私增强的医学影像联合建模规范

Privacy-enhanced joint modeling specifications for medical imaging

2024-04-16 发布　　2024-04-17 实施

中国图学学会　发布
中国标准出版社　出版

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》的规定起草。

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。

本文件由中国图学学会提出并归口。

本文件起草单位：中国科学院自动化研究所、澳门城市大学、北京航空航天大学、广东省人民医院、珠海市人民医院、河南省人民医院、北京大学人民医院、北京大学第三医院。

本文件主要起草人：刘西蒙、刘振宇、应作斌、刘建刚、刘再毅、陆骊工、王梅云、王姝、卢剑、蔡剑平、刘明昊、方一晨、张国扬。

隐私增强的医学影像联合建模规范

1 范围

本文件规定了医学影像数据联合建模的流程与规范。

本文件适用于医学影像数据联合建模的各种流程，包括建模、评价、部署等范围。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

医学影像 medical imageing

利用医学成像设备及技术所得到的图像。

3.2

数据隐私 data privacy

一个数据保护领域，涉及正确处理敏感数据，尤其是个人数据以及其他机密数据。

注：包括某些财务数据和知识产权数据，以满足监管要求以及保护数据的机密性和不变性。

[T/CESA 1049—2018，定义 3.3，有修改]

3.3

隐私增强 privacy-enhanced

保护敏感信息隐私或机密性的技术方法。

注：隐私增强包括在隐私信息采集、存储，以及在执行搜索或分析过程中对于保护和增强隐私安全性的数据安全技术，旨在遵守隐私和数据保护原则，同时保持从用户提供的数据中提取价值的能力。

[ISO/IEC 20889：2018，定义 3.3，有修改]

3.4

联邦学习 federated learning

一种多个参与方在保证各自原始数据不出数据方定义的可信域前提下，以保护隐私数据的方式交互中间数据，从而协作完成某项人工智能和机器学习任务的模式。

3.5

多方安全计算 secure multi-party computation

基于多方数据协同完成计算目标的密码技术，获得除计算结果及其可推导出的信息之外，不会泄漏各方隐私数据。

注：多方安全计算常采用的技术有混淆电路、不经意传输、秘密分享、同态加密等。

3.6

差分隐私 differential privacy

一种数据共享手段，实现仅分享可以描述数据库的一些统计特征，而不公开具体个人信息的。

注：差分隐私背后的直观想法，是如果随机修改数据库中的一个记录造成的影响足够小，获得的统计特征就不能被用来反推出单一记录的内容。

3.7

本地差分隐私　local differential privacy

在不可信第三方的前提下，将数据隐私化的工作转移到每个用户，用户自己运用差分隐私算法保护个人数据的过程。

3.8

混淆电路　garbled circuit

双方进行安全计算的布尔电路。混淆电路将计算电路中的每个门都加密并打乱，确保加密计算的过程中不会对外泄露计算的原始数据和中间数据。双方根据各自的输入依次进行计算，解密方可得到最终的正确结果，但无法得到除了结果以外的其他信息，从而实现双方的安全计算。

3.9

同态加密　homomorphic encryption

一种对称或非对称加密，它允许第三方（既不是加密方也不是解密方）以加密的形式对数据执行计算，同时实现保留明文数据的机密性。

3.10

群同态　group homomorphism

群论中两个群之间保持群乘法结构的一种映射。

3.11

联邦学习算法　federated learning algorithm

联邦学习参与方使用的机器学习算法，一般由非联邦的机器学习算法演化而来。

注：主要包括传统机器学习、分布式机器学习、加密算法、安全多方计算、硬件加密技术、差分隐私等。

3.12

对称加密算法　symmetric-key encryption

密码学中的一类加密算法，这类算法在加密和解密时使用相同的密钥，或是使用两个可以简单地相互推算的密钥。

3.13

数据采集　data acquisition

从传感器和其他待测设备等模拟和数字被测单元中自动采集非电量或者电量信号，送到计算机中进行分析、处理。

3.14

身份验证　authentication

通过一定的手段，完成对用户身份的确认。

注：其目的是确认当前所声称为某种身份的用户，确实是所声称的用户。

3.15

特征提取　feature extraction

从初始的一组测量数据开始，并建立旨在提供信息和非冗余的特征，从而促进后续的学习和泛化步骤，并且在某些情况下带来更好的可解释性的方法。

3.16

敏感度　sensitivity

某方法对单位浓度或单位量待测物质变化所致的响应量变化程度。

3.17

数据清洗　data cleaning

删除重复的数据，统一数据格式，去除不相关、不准确或损坏数据的过程。

3.18

任务发起方　task initiator

发起联邦学习任务的联邦学习参与方，通常也是结果方。

3.19

调度方　dispatcher

根据算法流程分发联邦学习任务并协调计算过程中各方资源和行为的联邦学习参与方。

注：调度方通过调度数据方、计算方、算法方等多个联邦学习参与方完成联邦学习任务。

3.20

算法方　algorithm party

提供联邦学习需要的算法参与方，提供算法描述。

注：如算法的标识符、版本号以及兼容性说明。

3.21

数据方　data party

提供联邦学习需要的数据和算力的参与方。

注：包括对训练任务，提供联邦学习模型训练需要的训练数据；对推理任务，提供联邦学习模型参数或待推理数据；数据方本地数据计算需要的算力；多个数据方交互计算需要的算力。

3.22

辅助计算方　auxiliary calculating party

为联邦学习任务辅助服务的联邦学习参与方。

3.23

结果方　result party

最终获得联邦学习计算结果的联邦学习参与方。

4　缩略语

下列缩略语适用于本文件。

DP：差分隐私（differential privacy）

FHE：全同态加密（fully homomorphic encryption）

FL：联邦学习（federated learning）

HE：同态加密（homomorphic encryption）

LDP：本地差分隐私（local differential privacy）

MPC：多方安全计算（secure multi-party computation）

PHE：单同态加密（partially homomorphic encryption）

RR：随机回应（randomized response）

SDK：软件开发工具包（software development kit）

SWHE：浅同态加密（somewhat homomorphic encryption）

5　医学影像数据联合建模流程与隐私增强

5.1　概述

医学影像数据联合建模流程包括制定目标、数据准备、联合建模、模型评价、结果呈现、模型部署。

5.2 制定目标

在联合建模开始前明确目标及预期达到的效果如下。

a) 研究方向和问题：明确要研究的具体医学问题，包含肿瘤诊断、疾病预测等，以及需要解决的具体问题，可包括提高准确性、加快诊断速度等。

b) 成功标准：所制定的联合建模成功的标准可包括提高模型的精度、降低误诊率、提高预测准确性等内容。

c) 隐私保护目标和要求：明确保护患者隐私的目标和要求，应包括匿名化、数据脱敏、限制数据使用等。

d) 数据收集和样本选择：确定应收集的医学影像数据类型、数量和来源，并考虑如何选择合适的样本进行联合建模。应考虑数据的多样性、覆盖范围和代表性，以及数据质量和完整性等方面的问题。

e) 数据共享协议和权限：明确数据共享的协议和权限，可包括谁可以访问和使用数据，如何保证数据安全等。应遵守相关的法规和规定，以及保护数据所有者的权益。

5.3 数据准备

5.3.1 数据要求

应明确联合建模所用数据，并预先对数据做出一定的处理。

5.3.2 特征提取

特征提取从原始数据中提取有用信息的过程，以便用于机器学习、数据分析或其他应用。具体要求如下。

a) 明确建模所需的数据指标。

b) 明确各项数据指标的含义。

c) 明确该场景中的特征类型，如基本特征、统计特征等。

d) 应确保不同图像所提取的特征是相同的。

e) 确定特征提取算法。

5.3.3 数据预处理

5.3.3.1 概述

数据预处理是数据挖掘、机器学习和数据分析过程中非常重要的一步。它涉及对原始数据进行清洗、转换和整理，以便更好地理解数据并为分析和建模做好准备。数据预处理的主要目标是提高数据质量、减少噪声、消除异常值以及解决不一致性和数据缺失问题。

5.3.3.2 数据预处理要求

数据预处理要求如下。

a) 如果数据满足建模要求，则可以进行进一步加工。

b) 对部分不可用的数据，应予以剔除。

c) 应将数据转换为统一的标准和格式。

d) 数据应分为训练集和测试集。

5.4 联合建模

5.4.1 通用要求

联合建模宜由联邦学习与常见隐私增强技术实现。

5.4.2 联邦学习

5.4.2.1 概述

联邦学习是一种分布式机器学习方法，它允许多个设备或服务器共同训练一个机器学习模型，而无须直接共享原始数据。这种方法在保护数据隐私和安全方面具有优势，因为原始数据永远不会离开拥有数据的设备或组织。

5.4.2.2 联邦学习参与方角色

联邦学习参与方角色主要有：任务发起方、调度方、算法方、数据方、计算方、辅助计算方、结果方、证书颁发机构(Certificate Authority，CA 认证方)、可信存证方(可信任的第三方机构或服务，负责记录和存储某些信息的证明或签名，并且这些信息在之后不能被篡改)等。

5.4.2.3 联邦学习一般流程

联邦学习一般流程如下。

a) CA 认证方为各联邦学习参与方、算法等提供认证服务，确保参与方和算法安全可靠，此步骤是一个可以事先执行且不必在每次联邦学习时都重新执行的步骤。
b) 算法方把联邦学习算法发布在联邦学习系统中。
c) 任务发起方通过调度方发起联邦学习任务。
d) 调度方下达计算任务：根据资源管理、算法管理组件提供的信息将任务下发到计算方。当存在且需要辅助计算方时，任务会被同时下发到辅助计算方。
e) 计算方基于原始数据进行计算。
f) 计算方进行交互，完成联邦学习任务，若在步骤 d)中辅助计算方下达了任务，则辅助计算方会同时参与联邦学习计算任务。
g) 结果方从各计算方获取结果数据，如：训练模型、推理结果等。
h) 根据业务需求可以将各方结果数据合并成最终结果。
i) 可信存证方将联邦学习的算法、输入、过程、结果等信息进行存证。

5.4.3 常见隐私增强技术

5.4.3.1 通用要求

联邦学习中常用的隐私增强技术包括多方安全计算、差分隐私、同态加密等。

5.4.3.2 多方安全计算

多方安全计算目的是协同地从每一方的隐私输入中计算函数的结果，而不用将这些输入展示给其他方。多方安全计算流程如下。

a) 任务创建。调度方提供了与任务发起方的交互接口，能够创建多方安全计算任务。通过与调度方交互创建多方安全计算任务，包括指定可用的数据源，以及其他参与方等；任务创建成功后可查看配置信息，包括所用数据源、其他参与方等。

b) 任务分配。发现新添加的计算节点，给新节点分配计算任务，并将新节点纳入整体任务分配体系中；任务量发生变化时可通过增加服务能力保证任务的正常执行；此外，当某个计算节点空闲时，能够自动为该节点自动分配剩余任务。任务分配的主要内容：添加计算节点、执行多任务、查看任务分配情况；根据任务量发生变化时的任务执行情况。

c) 数据接入。技术文档中对多方安全计算任务计算流程进行了描述，能够涵盖任务创建、任务分配、数据接入、任务执行、结果解析等步骤；并使系统中多方安全计算任务能够顺利执行，工作步骤与文档描述一致。

d) 任务执行。为了使多任务处理系统能够对任务进行调度管理，如排队、负载、优先级调度等；并确保各任务都能够执行成功，输出执行结果。

e) 结果解析。对安全计算的结果进行解析，判断计算工作是否正常进行。

5.4.3.3 差分隐私

差分隐私的中心思想是当敌方试图从数据库中查询个体信息时将其混淆，使得敌方无法从查询结果中辨别个体级别的敏感性。

差分隐私保护可通过在查询函数返回值中加入适量的干扰噪声来实现，但过多会影响结果可用性，过少则无法提供足够安全保障。敏感度是决定噪声量的关键参数。数据加噪有两种方法：一种是根据函数敏感性加噪、另一种是根据离散值的指数分布选择噪声。

差分隐私可抵抗成员推理攻击，核心是对梯度信息添加噪声。应明确添加噪声的种类，目前主要用拉普拉斯噪声、高斯噪声。在联邦学习场景下，应考虑数据层面与用户层面的安全问题，保证每个客户端的本地数据隐私安全与客户端间信息安全。联邦学习中可使用本地差分隐私实现各方在分散数据集上进行模型训练，中心思想是随机回应。

5.4.3.4 同态加密

同态加密是一种加密方法，通过对相关密文进行有效操作（无须解密密钥），实现加密内容上的特定代数运算。主要用于联合建模的参数交互计算过程，实现预测模型的联合确立。同态加密分为单同态加密、浅同态加密和全同态加密。

单同态加密是一种群同态技术。特别地，若其中运算符是加法运算符，则该方案被称为加法同态；同理，若运算符是乘法运算符，则该方案被称为乘法同态。

浅同态同态加密是同态加密方法中的一些运算操作（如加法和乘法）只能执行有限次。为了安全性，使用了噪声数据。每一次在密文上的操作会增加密文上的噪声量，而乘法操作是增加噪声量的主要技术手段。当噪声量超过一个上限值后，解密操作就不能得出正确结果了。因此，使用时应限制计算操作次数。

全同态加密是允许对密文进行无限次数的加法运算和乘法运算操作。全同态加密算法主要包括以Gentry方案为代表的第一代方案；以BGV方案和BFV方案为代表的第二代方案；以GSW方案以及支持浮点数近似计算的CKKS方案为代表的第三代方案。其次确定其具体算法方案。

5.5 模型评价

5.5.1 安全测评

5.5.1.1 模型安全

模型安全要求如下。

a) 应保证除计算结果及其可推导出的信息之外，不泄露各方隐私数据。

b) 应保证多个数据提供方在构建输入数据是相互独立的。

c) 确认在该模型下采用的 MPC 协议的安全性是否满足要求。
d) 在应用中可以根据相应的安全模型选择和管理各个参与主体。
e) 评估系统在恶意模型下的安全性是否满足要求。系统应提供恶意参与方模拟测试功能，披露相关的系统模型设计和代码，用以模拟恶意计算节点，随机将正确的计算因子替换为随机数，实现错误注入。

5.5.1.2 认证授权

认证授权内容如下。
a) 应提供各参与方之间进行通信时的双向身份认证的机制，如：挑战应答模式。
b) 检查对接入系统的用户是否提供身份鉴别能力，可包括口令认证、证书认证、令牌认证等内容。
c) 尝试使用正确的鉴别信息和错误的鉴别信息分别登录系统，检查是否仅在输入正确的鉴别信息时，才能进入系统并执行相关操作。
d) 应对各参与方进行相应的权限设置和控制，避免出现信息泄露。
e) 检查调度方是否能够对未被授权的计算请求协调发起数据使用授权申请。
f) 检查医学影像数据联合建模中是否在数据提供方同意后向使用方发送授权，用于权限认证。
g) 检查调度方是否对每个任务请求验证其数据使用授权的合法性。

5.5.1.3 密码安全

密码安全如下。
a) 检查医学影像数据联合建模中使用的密码算法是否符合国家密码管理部门的要求。
b) 检查医学影像数据联合建模中使用的密码算法的密钥长度是否符合国家密码管理部门的要求。
c) 检查医学影像数据联合建模中密钥管理是否符合国家密码管理部门的要求。

5.5.1.4 存证与日志

存证与日志的内容如下。
a) 医学影像联合建模(如联邦学习)的各参与方应保存用户的操作日志。
b) 联合建模的各参与方应对计算过程中的相关结果和信息进行存证。
c) 应具备对各参与方的用户操作日志和结果存证的审计能力，对于违背约定的数据提供方、计算方和结果使用方应能通过存证、审计等方法发现和追踪。
d) 对数据提供方和结果使用方的每次计算任务角色进行存证和记录，保证信息安全性与结果可追溯性。

5.5.2 性能测评

首先，应对联合建模进行目标评估，判断是否满足预期标准。其次，进行准确性评估，可以通过使用与集中数据模型训练的精度之间的距离来衡量联合建模的性能。最后，进行计算效率评估，常见的计算效率评估指标包括结果准确性、计算耗时、通信费用等，详细按附录 A。

5.6 结果呈现

在确保前期数据、隐私、效率等方面达标的情况下，联合建模完成预期目标，接下来进行结果呈现，内容如下。
a) 医学影像数据联合建模的呈现结果应是脱敏数据。
b) 医学影像数据联合建模的呈现结果应与建模目标一致。

c） 医学影像数据联合建模的呈现结果应体现出解决问题的步骤。

5.7 模型部署

5.7.1 部署场景

5.7.1.1 中心服务器云端部署

医学影像数据联合建模的模型部署（见图 1）在云端服务器，用户通过网页访问或者 API 接口调用等形式向云端服务器发出请求，云端收到请求后处理并返回结果。

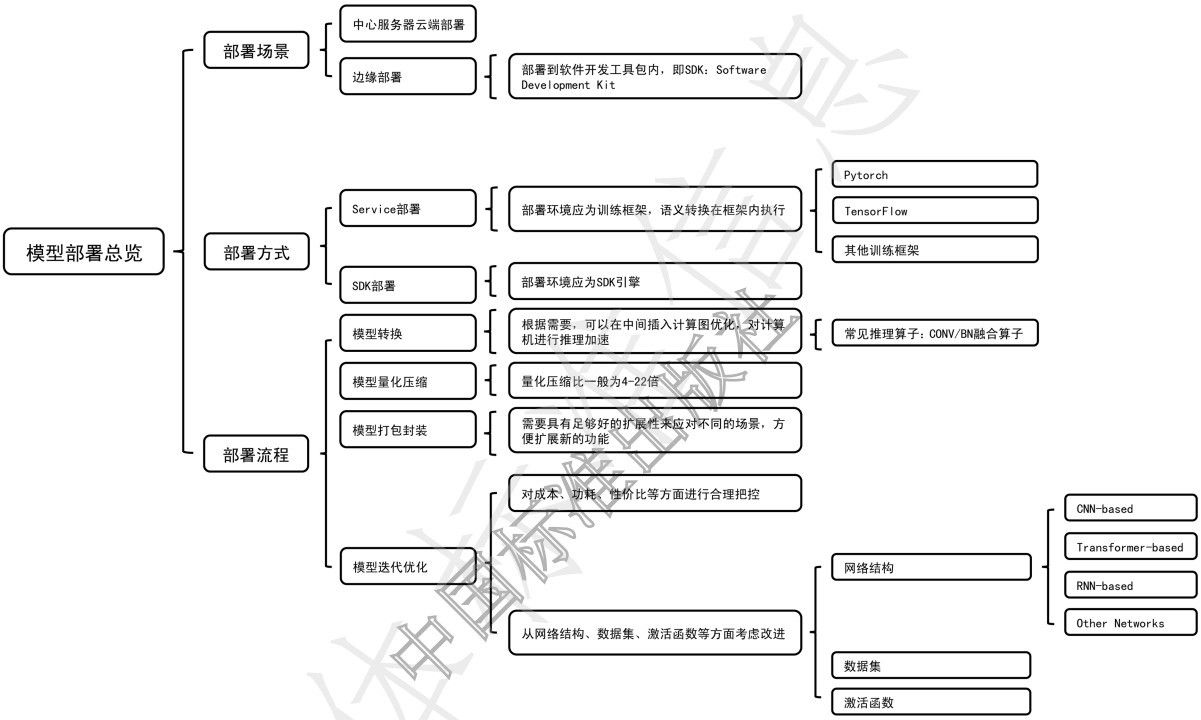

图 1 医学影像数据联合建模的模型部署图

5.7.1.2 边缘部署

将模型打包封装到软件开发工具包，并集成到嵌入式设备，数据的处理和模型推理都在终端设备上执行。

5.7.2 部署方式

5.7.2.1 Service 部署

Service 部署应以训练的引擎库作为推理服务的载体，部署环境应为训练框架，语义转换在框架内执行。

5.7.2.2 SDK 部署

应对模型转换（动态图静态化）、模型联合编译等进行深度优化，部署环境应为 SDK 引擎。

5.7.3 部署流程

5.7.3.1 概述

模型部署流程涉及将训练好的模型集成到生产环境，以便模型能够处理实际数据并为最终用户提供预测或分析。

5.7.3.2 模型转换

模型在不同框架之间流转，应进行模型转换，如联合推理场景的连接。根据需要，可以在中间插入计算图优化，对计算机进行推理加速，常见的推理加速有：CONV/BN 的算子融合等。

5.7.3.3 模型量化压缩

终端场景中，出于对内存和传输速率等因素的考虑，应进行模型量化压缩，量化压缩比为 16 倍。在确保模型可用的前提下，使模型尽可能小，同时保证较高的吞吐率。

5.7.3.4 模型打包封装

根据实际业务的需要，应将模型的前后处理，一个或者多个模型整合到一起，再加入描述性的文件（前后处理的参数、模型相关参数、模型格式和版本等）来实现一个完整的功能。SDK 应具有通用前后处理的高效实现，对齐训练时的前后处理逻辑，还应具有足够好的扩展性来应对不同的场景，方便扩展新的功能。

5.7.3.5 模型迭代优化

在进行模型迭代优化时，应尝试多次不同的数据集划分和不同的参数选取，还要结合模型表现判断当前是欠拟合还是过拟合。

改进可以从以下几个方面考虑：网络结构、数据集、激活函数等。常用的模型迭代与调优方式有交叉验证和超参数搜索等。

应对成本、功耗、性价比等方面进行合理把控。应根据性能需求、不同医疗场景、价格等因素合理选择芯片。

附 录 A
（规范性）
联合建模的性能指标

A.1 结果准确性

模型部署对应模型最终的落地应用，测试联合建模的模型结果的准确性见表 A.1。

表 A.1 逻辑回归场景准确性测试

测试项目	联合建模准确性测试
测试目的	检验联合建模的模型结果准确性
测试环境	部署完成的联合计算系统
前置条件	1） 输入数据已接入或已配置 2） 联合建模任务已配置 3） 联合建模参数已配置 4） 本地明文使用训练集联合建模，测试集得到模型评价指标的基准值
测试步骤	1） 启动联合建模任务 2） 在联合建模任务完成后，查看对应的训练结果，并记录联合建模训练得出的模型的评价指标：AUC、KS 值 3） 对比联合建模和本地建模中的模型评价指标偏差绝对值
预期结果	1） 联合建模任务执行成功 2） 联合建模和本地建模的模型评价指标的绝对值偏差应控制在如下范围内： ——AUC 绝对值偏差＜0.05 ——KS 绝对值偏差＜0.05
备注	无

A.2 计算耗时

模型部署对应模型最终的落地应用，测试建模的耗时情况见表 A.2。

表 A.2 逻辑回归场景计算耗时

测试项目	联合建模耗时测试
测试目的	检验联合建模的耗时情况
测试环境	部署完成的联合计算系统
前置条件	1） 输入数据已接入或已配置 2） 联合建模任务已配置 3） 联合建模参数已配置

表 A.2　逻辑回归场景计算耗时（续）

测试步骤	1）　启动联合建模任务 2）　联合建模任务达到验收条件、得出结果模型后，记录联合建模阶段总耗时 3）　恢复环境，重复步骤 1）、2）两轮，取最优结果作为最终测试结果
预期结果	1）　联合建模任务执行成功 2）　联合建模的耗时情况满足业务场景需求
备注	无

A.3　通信费用

模型部署对应模型最终的落地应用，测试建模的通信费用是否符合需求，见表 A.3。

表 A.3　逻辑回归场景通信费用

测试项目	联合建模通信费用测试
测试目的	检验联合建模的通信费用情况
测试环境	部署完成的联合计算系统
前置条件	1）　输入数据已接入或已配置 2）　联合建模任务已配置 3）　联合建模参数已配置
测试步骤	1）　启动联合建模任务 2）　每进行一轮联合建模分别记录客户端，服务端的通信费用如计算时延、吞吐量、计算精度 3）　在联合建模任务完成后，记录总费用
预期结果	1）　联合建模任务执行成功 2）　联合建模的通信费用情况满足医学场景需求
备注	无

参 考 文 献

[1] JR/T 0196—2020 多方安全计算金融应用技术规范

[2] T/CESA 1049—2018 区块链 隐私保护规范

[3] T/CESA 1109—2020 智能医疗影像辅助诊断系统技术要求和测试评价方法

[4] T/NAHIEM 47—2022 医学影像数据人工智能分析方法评估规范

[5] ISO/IEC 18033-6：2019 IT Security techniques-Encryption algorithms—Part 6：Homomorphic encryption

[6] ISO/IEC 20009-4：2017 Information technology-Security techniques-Anonymous entity authentication—Part 4：Mechanisms based on weak secrets

[7] ISO/IEC 20889：2018 Privacy enhancing data de-identification terminology and classification of techniques