信息安全研究 第10卷 第6期 2024年6月
Journal of Information Security Research Vol.10 No.6 June 2024
DOI:10.12379/j.issn.2096-1057.2024.06.03

一种安全高效的全匿踪纵向联邦学习方法

尤志强[1] 李 月[2] 姜 玮[3] 方 竞[1] 陈立峰[1] 卞 阳[1]
[1](上海富数科技有限公司 上海 200120)
[2](中国电子口岸数据中心上海分中心 上海 200120)
[3](上海海关科技处 上海 200135)
(yuanquan@fudata.cn)

A Secure and Efficient Method of Fully Anonymous Vertical Federated Learning

You Zhiqiang[1], Li Yue[2], Jiang Wei[3], Fang Jing[1], Chen Lifeng[1], and Bian Yang[1]
[1](*Shanghai Fudata Technology Co., Ltd., Shanghai* 200120)
[2](*China E-Port Data Center, Shanghai Branch, Shanghai* 200120)
[3](*Science & Technology Division of Shanghai Customs, Shanghai* 200135)

Abstract As a key technical paradigm to achieve "data availability and invisibility", the core process of vertical federated learning is sample alignment based on private set intersection. Although the private set intersection protects the privacy of non-intersected information, it can't meet the privacy protection requirements of user IDs in the intersected set. This paper proposes a fully anonymous vertical federated learning framework based on anonymous alignment to ensure that no private information of each holder set will be disclosed during the whole process. An implementation framework based on secure multi-party computation is proposed for fully anonymous joint modeling. The high performance and low error characteristics of the framework are verified through experiments, indicating it can be better applied in practice.

Key words vertical federated learning; private set intersection; anonymous alignment; secure multi-party computation; anonymous federated learning

摘 要 纵向联邦学习作为实现"数据可用不可见"的重要技术范式,其核心的学习过程是基于安全求交的样本对齐.已有的安全求交虽然保护了非交集信息的隐私不被泄露,但无法满足交集部分用户ID的隐私保护需求.抽象出一种基于匿踪对齐的全匿踪纵向联邦学习框架,确保联邦学习全链路都不会泄露各持有方集合的隐私信息;提出一种基于多方安全计算的框架实现方法,在保持全匿踪的条件下进行联合建模,迭代训练直到模型收敛;通过实验验证了该框架的高性能与低误差特性,能够较好地应用于实践.

收稿日期:2023-10-14
通信作者:方竞(linyuan@fudata.cn)
引用格式:尤志强, 李月, 姜玮, 等. 一种安全高效的全匿踪纵向联邦学习方法[J]. 信息安全研究, 2024, 10(6): 506-512

关键词 纵向联邦学习;安全求交;匿踪求交;多方安全计算;匿踪学习

中图法分类号 TP309.2

联邦学习通过对多方数据进行本地联合建模,实现“数据不动、算法动”,已经成为隐私计算的一种关键技术.其中,纵向联邦学习可以实现不同机构或组织间的数据共享及融合,挖掘更深层次的数据价值,在金融风控、联合营销、医疗保险、电力风控等领域已得到广泛应用.纵向联邦学习一般包括安全求交、特征工程、联合训练及联合预测等过程.其中,求交过程暴露了用户交集中的敏感个人信息,存在重大不合规风险.虽然联邦学习中个人标识信息、标签和特征信息不出域,交互的只是中间数据、加密数据和碎片化数据,且无法逆推出原始数据;但是在训练样本交集的过程中各方都获得了交集内的 ID 信息,无法满足相关机构的合规要求,需要通过创新技术解决联邦学习中的安全合规问题.

1 背景与现状

1.1 研究背景

2016 年,谷歌研究院提出了联邦学习[1]解决方案,其本质是一种分布式机器学习[2],各参与方原始数据保留在本地客户端,仅与中心服务器交互模型更新信息.纵向联邦学习把数据集按照纵向(即特征维度)切分,并取出双方用户相同而用户特征不完全相同的数据进行训练,以增强模型能力.因此,纵向联邦学习需要一种安全手段实现多方数据融合,然后再基于融合集进行加密训练,获得最终模型.

联邦学习中的安全求交方法虽然不暴露交集外的用户 ID,但暴露了交集内的用户 ID.为此,有必要研究一种匿踪求交的方法来确保不泄露交集以及非交集信息,以实现求交过程的匿踪隐私保护.针对纵向联邦学习而言,需要同时保护纵向联邦学习过程中数据水平对齐时的非交集信息和交集 ID,并基于此对纵向联邦学习的全链路过程进行保护.

1.2 研究现状

为解决上述安全求交过程中用户 ID 暴露的问题,Sun 等人[3]提出了一种基于数据集隐私求并集(PSU)的纵向联邦学习框架,PSU 协议不需要识别所有训练样本的交集,而是生成样本的并集作为训练实例.该方法虽然解决了安全求交隐私泄露问题,但由于引入了大量非真实的、通过策略生成的特征和标签,导致模型效果有所下降.

此外 Ion 等人[4]提出了 PIS-C 协议,基于 Diffie-Hellman(DH)算法使用随机不经意传输和加密布隆过滤器 2 种隐私求交(PSI)协议,该框架允许 2 个参与方在隐私保护状态下计算具有交集的数据记录值的和.Buddhavarapu 等人[5]为解决两方集合隐私求交并且任何一方都无法根据其中的交集反推出对应原始记录的问题,提出了 Private-ID 和 PS^3I 这 2 种算法.其中,Private-ID 是基于双重 DHKE(Diffie-Hellman key exchange),通过先求并集的方式实现隐私求交.PS^3I 方法采用了双重 DHKE+shuffle 的思路,但该方案存在暴露真实的交集量级,从而可能引发通过差分攻击造成交集信息泄露的风险.Rindal 等人[6]提出了一种 Circuit-PSI 的方法,基于 OPRF 框架和 Circuit 两方比较实现一种两方 PSI 协议,输出结果为碎片态形式.另外,朱悦等人[7]对服务器-客户端横向架构、点对点横向架构、有协调第三方纵向架构这 3 种联邦学习的合规框架及合规风险进行了分析.

1.3 本文贡献

当前,针对 PSI 的研究主要集中在各方 ID 求交本身,针对 PSI 过程中联合对应特征字段的统计分析、学习建模等研究甚少.随着纵向联邦学习的快速发展,基于 PSI 对齐后的学习建模需求越来越多,但原有 PSI 存在交集 ID 暴露的问题,因此有必要针对联邦学习的合规要求构建一种新型的全匿研究框架,并将其应用于纵向联邦学习.

本文梳理了纵向联邦学习在样本对齐方面的交集 ID 信息暴露问题,首次提出了匿踪对齐、匿踪场景匿名化以及匿踪学习等概念,并抽象出一种全匿踪纵向联邦学习框架(AnonymFL),允许各参与方在联合计算出集合交集的基础上完成纵向联邦学习,并确保全链路都不会泄露各持有方

集合的交集和非交集信息.同时,本文也提出了一种基于多方安全计算的 AnonymFL 框架.实证研究表明,该框架支持千万级平衡样本的全匿踪对齐及百万级平衡样本的全匿踪联邦建模.

2 概念定义

本节给出描述 AnonymFL 框架需要用到的概念定义.

一般求交过程由一个发送方 S 和一个接收方 R 参与.其中发送方持有集合 X,大小为 N_X;接收方持有集合 Y,大小为 N_Y.在大多数情况下 N_X 和 N_Y 是公开的.

安全求交 PSI.计算 X 和 Y 的交集,将 $X \cap Y$ 发送给接收者,不将任何信息发送给发送者.在此过程中,发送端和接收端集合交集所对应的 ID 集合 JID 是对双方公开的,在求交过程中暴露了该交集的 ID 信息,但非交集部分的 ID 信息是非公开、隐私的.

匿踪 PSI.计算 X 和 Y 的交集,不将任何敏感信息发送给发送者.在此过程中,发送端和接收端集合交集所对应的 ID 集合 JID 以及非交集部分的 ID 信息都是非公开、隐私的.

全匿踪分析建模.在匿踪 PSI 的基础上继续对发送端和接收端集合交集 ID 集合 JID 所对应的特征字段集合 JX 进行统计分析或学习建模过程中,不会泄露任何交集和非交集数据的隐私信息,即 $f(JX)$计算过程中保持全链路隐私.

全匿踪纵向联邦学习 AnonymFL.如果全匿踪技术实现过程中的计算函数 f 代表纵向联邦学习,则该过程称为全匿踪纵向联邦学习 AnonymFL.

3 框架与实现

全匿踪纵向联邦学习 AnonymFL 允许各参与方在联合计算出集合交集的基础上,完成纵向联邦学习建模,并在匿踪对齐、匿名化、匿踪学习等全链路过程中都不会泄露各持有方集合的任何隐私信息,实现保持匿踪的条件下进行联合建模,迭代训练直到模型收敛.

本文提出了一种基于多方安全计算(MPC)[8]的全匿踪纵向联邦学习 AnonymFL 框架,在基于 MPC 秘密分享协议的基础上,实现全匿踪纵向联邦学习的计算算子和应用模块,并对该方法进行了实证研究.

3.1 匿踪对齐

匿踪对齐是指纵向联邦学习过程中利用匿踪求交完成各参与方数据集水平对齐的过程.匿踪对齐模块主要是实现匿踪求交,虽然当前针对匿踪求交的方式比较少,但主要也还是以安全求交的原理为基础,涉及混淆电路[6]、不经意传输[9]、秘密共享[10]、同态加密[11]等集合元素比较技术的应用.

匿踪对齐把用户 ID 进行碎片化处理,并秘密分享给各个参与方,各方无法独立获取用户 ID 的完整信息,在碎片化状态下进行用户 ID 的比较对齐,以此实现敏感信息保护.

本文采用基于加法秘密分享机制的多方安全比较算法.针对多方安全计算的比较协议[12],需要解决 2 个密态数据 S_1 和 S_2 的大小比较问题.可以先求出 $w = S_1 - S_2$,再获取 w 的最高位值(most significant bit, MSB).要获取密态下的最高位 MSB,需要将算术域上的分享份额转换成布尔逻辑分享份额,再进行 MPC 加法电路计算.

3.2 匿名化

匿名化是指对匿踪对齐后的数据集中的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.匿名化处理可以实现个人信息记录的匿名,理想情况下无法识别到具体的“自然人”.常见的匿名化处理包括 k-匿名、l-多样性、t-闭合、差分隐私等方法.本文基于 MPC 算子实现常见的匿名化算法.以差分隐私为例,其原理主要是通过扰动的方式,给碎片化 ID 和标签特征添加适当的噪声,使得所有的秘密分享碎片即使都聚集在一起也无法进行恢复.

3.3 匿踪学习

匿踪学习是指对匿踪对齐后的数据集进行建模学习的过程,一般包括模型训练、模型推理和模型评估等步骤.虽然当前对匿踪学习的研究甚少,但隐私机器学习[13]的许多技术都可以迁移到匿踪学习,包括基于差分隐私的机器学习[14]、基于同态加密的机器学习[15]以及基于多方安全计算的机器学习[16]等.

本节以纵向逻辑回归模型为例,介绍逻辑回归模型的子模型拆分方式,然后对基于多方安全

秘密分享机制的隐私保护逻辑回归算法进行研究.在纵向联邦学习的计算中,只要能安全计算出梯度信息及损失函数就能完成模型的训练.多方安全秘密分享机制基于加法协议的同态性可以得到加法结果,利用辅助三元组生成的方法可以得到乘法结果,利用比较协议完成训练结果的判断.方法过程如下:

1) 各方联合初始化碎片态乘法三元组,对特征进行碎片化并进行分发完成特征拼接;

2) 各方基于秘密分享机制完成上述损失函数和梯度的碎片化计算;

3) 发起方判断连续 2 次的损失差值是否达到了预先设置的阈值,根据判断结果不断进行迭代;

4) 更新参数权重,直到模型收敛,各方分别保存训练好的碎片态模型权重参数,完成训练.

3.4 匿踪 PSI 性能优化

上述基于多方安全计算实现匿踪对齐方法涉及两方数据集之间的 ID 比较,具有指数级别的计算开销,在实际应用过程中不具备可行性.为优化上述比较模型的计算性能,可以基于 MPC-Ordering 的方法降低计算复杂度.通过对数据集 A 和数据集 B 的碎片态用户 ID 进行拼接,然后对秘密分享状态下的碎片 ID 进行排序,最后对排序后的 ID 信息进行批量比较.该方法减少了比较次数,提高了计算效率.方法过程如下:

1) 对原始 ID 作数值映射转换,对各方数据集的 ID 进行加密;

2) 对各方数据集进行样本矩阵增广(特征和标签数据对齐),解决由于 ID 排序造成的横向数据打乱的问题;

3) 对增广后的数据矩阵进行碎片化,并进行纵向拼接,执行 ID 列的碎片化排序;

4) 进行纯密态对齐,基于排序后的碎片态 ID 列执行批量比较操作,执行结束就会得到最终的全密态对齐样本.

由于基于排序优化的匿踪对齐对数据对齐等过程有一定量的修改,故后续联合建模过程也需要在此基础上进行完善.具体体现在联合建模训练过程中加载的数据集是全匿 PSI 样本的碎片,需要增加指示对齐碎片输入,用于统计当前 Batch 中交集的样本个数,该信息依然是碎片态形式.同时,联邦学习模型推理及评估指标计算函数全部实现匿踪化.

4 实证研究

下面,本文通过正确性、效率的实验评估全匿踪纵向联邦学习方案的性能.

4.1 数据集

本文通过 Kaggle 获取公开的 2 个数据集(Bank-Additional-Full 和 Credit-Card-Clients)评估了全匿踪纵向联邦学习中匿踪对齐和匿踪逻辑回归的性能.对数据集中非数值特征进行 WOE 转换,同时对特征进行标准化处理.Bank-Additional-Full 数据集包含 41 188 个样本,有 20 个输入变量,分类的目标是预测客户是否会订阅(是/否)定期存款(变量 y).将该数据集一拆为二,分别作为参与方 A 和参与方 B 的数据输入,其中参与方 A 持有 13 个特征及标签,参与方 B 持有另外 7 个特征;此外,对 41 188 个样本按照 80∶20 的比例拆分为训练集与测试集.

Credit-Card-Clients 数据集包含 3 万个样本,有 23 个特征,分类目标为下个月是否会付款(是/否).本文将数据集拆分为 2 份,分别作为参与方 A 与参与方 B 的数据输入,其中参与方 A 持有 12 个特征以及标签,参与方 B 持有另外 11 个特征.此外,对 3 万个样本按照 80∶20 的比例拆分为训练集与测试集.

4.2 评估方法

本文采用 *KS* 和 *AUC* 评价模型的准确性.*AUC*(area under the curve of ROC)是 ROC 曲线下方的面积,用于判断二分类模型的优劣.ROC 曲线的横坐标是伪阳性率(false positive rate),也叫假正类率,纵坐标是真阳性率(true positive rate),也叫真正类率.一般来说,*AUC* 值越大表示模型效果越好.*KS*(Kolmogorov-Smirnov)值是在模型中区分正负样本分隔程度的评价指标,取值范围是[0,1].通常值越大表明正负样本区分度越好.

同时,本文在耗时性能上进行了分析,分别针对匿踪对齐和全匿踪联邦学习进行了测试,并与安全求交以及 MPC-LR 的基准情况进行了对比.

4.3 评估结果分析

本文在 Kubernetes 私有云上进行实验,并为

每个参与节点分配了 16 个 CPU 核心和 64 GB RAM 的实验机器，网络采用千兆带宽.

本文针对基于多方安全计算的纵向联邦学习 MPC-FL 与基于 MPC-Ordering 的全匿踪纵向联邦学习 AnonymFL 进行了性能测试.以纵向逻辑回归 LR 为例，本文对基于 RSA 密码算法的安全求交 RSA-PSI 和基于全匿踪的安全求交 AnonymFL-PSI 进行耗时对比，其测试结果如表 1 所示；基于多方安全计算的纵向逻辑回归 MPC-LR 和经过排序优化后的全匿踪纵向逻辑回归 AnonymFL-LR 进行耗时对比，其测试结果如表 2 所示.其中对于 RSA-PSI 来说，1 024 b 的 RSA 密钥长度是过去常用的安全长度，但随着计算机计算能力的提升和攻击技术的发展，其安全性已无法满足现代应用的需求，因此不推荐在高密数据场景中使用 1 024 b 密钥长度，2 048 b 的 RSA 密钥长度是目前广泛使用的安全长度.

表 1　安全求交与匿踪求交耗时对比

耗时对比	数据集	
	Bank-Additional-Full	Credit-Card-Clients
RSA-PSI(1024)耗时/s	29	18
RSA-PSI(2048)耗时/s	72	52
AnonymFL-PSI 耗时/s	27	21
AnonymFL-PSI 与 RSA-PSI(2048)耗时比	0.375	0.404

表 2　纵向逻辑回归与全匿踪纵向逻辑回归耗时对比

耗时对比	数据集	
	Bank-Additional-Full	Credit-Card-Clients
MPC-LR 耗时/s	151	139
AnonymFL-LR 耗时/s	447	341
AnonymFL-LR 与 MPC-LR 耗时比	2.96	2.45

由表 1 可见，在计算性能方面，匿踪对齐 AnonymFL-PSI 的整体耗时仅为安全求交 RSA-PSI(2048)的 0.4 倍左右，计算效率具有明显优势.

由表 2 可见，在计算性能方面，相同训练参数下，全匿踪纵向逻辑回归 AnonymFL-LR 的整体相比基于多方安全计算的纵向逻辑回归 MPC-LR 耗时不到 3 倍，在保证交集 ID 信息无泄露的情况下仍能保持较好的计算性能.更大的数据集测试表明，该方案能够支持千万级平衡样本的全匿踪 PSI 对齐以及百万级平衡样本的全匿踪联邦学习.

另一方面，纵向逻辑回归 LR 模型准确性评估结果如表 3 所示.在参数设置方面，训练集数据记录的批次大小设为 2 万条和 5 000 条，学习率设为 0.1 和 0.01，所有批次的训练轮次均为 5 次.

表 3　纵向逻辑回归准确性测试结果

数据集	批量大小	学习率	LR	
			KS	*AUC*
Bank-Additional-Full	20 000	0.1	0.588	0.884
	20 000	0.01	0.549	0.866
	5 000	0.1	0.705	0.916
	5 000	0.01	0.559	0.872
Credit-Card-Clients	20 000	0.1	0.374	0.699
	20 000	0.01	0.368	0.692
	5 000	0.1	0.376	0.703
	5 000	0.01	0.37	0.696

全匿踪纵向逻辑回归 AnonymFL-LR 模型评估准确性测试结果如表 4 所示：

表 4　全匿踪纵向逻辑回归准确性测试结果

数据集	批量大小	学习率	AnonymFL-LR	
			KS	*AUC*
Bank-Additional-Full	20 000	0.1	0.592 2	0.880 5
	20 000	0.01	0.531 3	0.854 1
	5 000	0.1	0.703 7	0.915 7
	5 000	0.01	0.542 5	0.859 3
Credit-Card-Clients	20 000	0.1	0.387 5	0.717 1
	20 000	0.01	0.365 7	0.697 4
	5 000	0.1	0.389 7	0.728 2
	5 000	0.01	0.380 5	0.712 2

从明文 LR(基于 Numpy 实现的 LR 模型)与 AnonymFL-LR 的 *KS* 值和 *AUC* 值对比来看，全匿踪联邦学习方案能够保持和非匿踪联邦学习基本一致甚至更好的模型效果.

本文整体实验结果表明：

1) 匿踪对齐和匿踪学习方案适用于高密数据场景，特别是需要保护求交对齐过程中的交集与非交集信息都不暴露；

2) 匿踪对齐性能相对于 RSA-PSI(2048)具有明显优势，可在生产环境中进行部署；

3）匿踪学习算法在全流程密态数据形式下可以有效完成模型训练，不造成模型预测精度损失，模型具备可靠性；

4）匿踪学习方案可以应用于 $n(n\geqslant 2)$ 方高密数据场景，对于多节点高密联合建模场景具备较高适配性.

5 结　　语

本文提出了一个全匿踪纵向联邦学习框架 AnonymFL，在保持全匿踪的条件下进行联合建模，迭代训练直到模型收敛.本文基于多方安全计算秘密分享协议实现了该框架原理，并利用相关方法优化了匿踪求交的性能，使其在应用实践中能够支持千万级平衡样本的全匿踪 PSI 对齐以及百万级平衡样本的全匿踪联邦建模，在满足建模准确性要求的同时提升了计算效率.

未来研究方向：由于本文方案的全匿踪联邦学习算法是秘密分享全密态形式，存在通信量较大的问题，因此面对大规模的实际应用需求，未来还需要研究更加高效的多方安全计算协议，降低全匿踪纵向联邦学习的通信量，实现高效通信的全匿踪联邦学习算法，进一步实现支持亿级平衡样本的全匿踪 PSI 对齐和千万级平衡样本的全匿踪联邦建模等，这也是其大规模应用落地的重要保障.全匿踪纵向联邦学习使用了密态的排序方法，为降低其算法复杂度进一步提升运行效率，可以研究并行全匿 PSI 算法，例如用 GPU，FPGA 进行计算等；联邦图计算是未来数据应用的重要方向，对图数据之间的融合应用发挥着重要作用，实现全匿踪的联邦图计算也将促进图数据的大规模合规应用.

参 考 文 献

[1] McMahan H B, Moore E, Ramage D, et al. Federated learning of deep networks using model averaging [J]. arXiv preprint, arXiv:1602.05629, 2016

[2] McMahan H B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data [G] //Artificial Intelligence and Statistics. Lauderdale, FL, USA: AISTATS, 2017: 1273-1282

[3] Sun J, Yang X, Yao Y, et al. Verticalfederated learning without revealing intersection membership [J]. arXiv preprint, arXiv:2106.05508, 2021

[4] Ion M, Kreuter B, Nergiz A E, et al. On deploying secure computing: Private intersection-sum-with-cardinality [C/OL] 2020 [2023-11-01]. https://www.ieee-security.org/TC/EuroSP2020/

[5] Buddhavarapu P, Knox A, Mohassel P, et al. Private matching for compute [J/OL]. IACR Cryptol ePrint Arch, 2020 [2023-10-14]. https://eprint.iacr.org/2020/599

[6] Rindal P, Schoppmann P. VOLE-PSI: Fast OPRF andcircuit-PSI from vector-OLE [G] //Advances in Cryptology—EUROCRYPT. Berlin: Springer, 2021: 901-930

[7] 朱悦，庄媛媛. 联邦学习的个人信息保护合规分析框架 [J]. 信息安全研究，2023，9(2)：162-170

[8] Yao A C. Protocols for secure computations [C] //Proc of the 23rd Annual Symp on Foundations of Computer Science. Piscataway, NJ: IEEE, 1982: 160-164

[9] Pinkas B, Schneider T, Zohner M. Faster private set intersection based on OT extension (Full Version) [C] // Proc of the USENIX Security Symposium. Berkeley, CA: USENIX Association, 2014: 797-812

[10] Shamir A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612-613

[11] Freedman M J, Nissim K, Pinkas B. Efficient private matching and set intersection [G] //Advances in Cryptology—EUROCRYPT 2004. Berlin: Springer, 2004: 1-19

[12] Patra A, Schneider T, Suresh, A, et al. ABY2.0: Improved mixed-protocol secure two-party computation (full version) [C] //Proc of the USENIX Security Symp. Berkeley, CA: USENIX Association, 2021: 2165-2182

[13] Chanyaswad T, Chang J M, Kung S Y. A compressive multi-kernel method for privacy-preserving machine learning [EB/OL]. 2021 [2023-11-01]. https://doi.org/10.48550/arXiv.2106.10671

[14] Beaulieu-Jones B K, Wu Z S, Williams C, et al. Privacy-preserving generative deep neural networks support clinical data sharing [EB/OL]. 2017 [2023-11-01]. https://www.biorxiv.org/content/biorxiv/early/2017/07/05/159756.1.full.pdf

[15] Courbariaux M, Hubara I, Soudry D, et al. Binarized neural networks: Training deep neural networks with weights and activations constrained to +1 or −1 [EB/OL]. 2016 [2023-11-01]. https://arxiv.org/pdf/1602.02830.pdf

[16] Mohassel P, Zhang Y P, Secure M L. A system for scalable privacy-preserving machine learning [C] //Proc of the 38th IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2017: 19-38

尤志强
硕士.主要研究方向为隐私计算技术.
yuanquan@fudata.cn

方　竞
博士.主要研究方向为隐私计算技术应用与管理.
linyuan@fudata.cn

李　月
硕士,高级工程师.主要研究方向为信息技术应用及管理.
liyue@customs.gov.cn

陈立峰
博士.主要研究方向为隐私计算技术.
tianpu@fudata.cn

姜　玮
高级工程师.主要研究方向为信息安全管理.
jiangwei@shciq.gov.cn

卞　阳
硕士.主要研究方向为隐私计算技术应用与管理.
douheng@fudata.cn