基于同态加密的金融科技平台多机构联合风控模型与数据主权博弈分析

吴文蔚
Crystalline Network Pteltd, 新加坡 189352

摘　　要： 金融数字化转型的加速催生了多机构协同风控的迫切需求，但数据主权的法律约束与隐私泄露风险严重制约了跨机构数据共享的可行性。在《数据安全法》与《个人信息保护法》框架下，金融机构需在风险联防联控与数据资产保护间寻求平衡。传统联合建模方法因依赖明文数据交互或中间参数传输，难以规避隐私泄露与主权争议，而全流程密文计算技术成为破局关键。本文聚焦于上述问题，提出一种基于同态加密的多机构协同风控框架，并引入动态博弈模型解析数据主权博弈的均衡路径。

关 键 词： 同态加密；金融科技平台；联合风控模型；数据主权；博弈分析

Fintech Platform Multi-institution Joint Risk Control Model and Data Sovereignty Game Analysis Based on Homomorphic Encryption

Wu Wenwei
Crystalline Network Pteltd, Singapore 189352

Abstract: The acceleration of financial digital transformation has spawned an urgent need for multi-institutional collaborative risk control, but the legal constraints of data sovereignty and the risk of privacy disclosure have seriously restricted the feasibility of cross-institutional data sharing. Under the framework of the Data Security Law and the Personal Information Protection Law, financial institutions need to strike a balance between joint risk prevention and control and data asset protection. Traditional joint modeling methods rely on plaintext data interaction or intermediate parameter transmission, which is difficult to avoid privacy disclosure and sovereignty disputes, and the whole process ciphertext computing technology becomes the key to break the game. Focusing on the above problems, this paper proposes a multi-institution collaborative risk control framework based on homomorphic encryption, and introduces a dynamic game model to analyze the equilibrium path of data sovereignty game.

Keywords: homomorphic encryption; fintech platform; joint risk control model; data sovereignty; game analysis

传统风控模式因数据共享边界模糊，易引发隐私泄露与主权争议，难以满足《数据安全法》等合规要求。同态加密技术支持密文计算，为多方数据协同提供了“可用不可见”的解决方案，但其在复杂金融场景下的应用仍面临模型效率与协作机制的挑战。与此同时，多机构间的数据主权博弈涉及利益分配、监管合规与信任建立，亟需系统性分析框架以平衡风险防控与权益保护。

一、同态加密技术原理

同态加密（Homomorphic Encryption, HE）是一种允许在加密数据上直接进行代数运算的密码学技术，旨在确保密文计算结果的解密值与对明文进行相同操作的结果等价[1]。在金融场景中，同态加密支持密文状态下的数据聚合、模型训练与推理，实现跨机构间的隐私保护协同计算，规避了传统明文交互中的信息泄露风险，为多机构联合风控提供了可验证、可审计的底层技术架构。

二、基于同态加密的金融科技平台多机构联合风控模型设计

（一）系统构架与流程

在初始化环节，参与机构以密钥生成中心协商获取同态加密

作者简介：吴文蔚（1983.06-），男，汉族，籍贯：上海，大学本科，职位：CFO，研究方向：金融科技创新。

的公私钥对，公钥用于加密本地风控特征数据，私钥由可信第三方或分片式托管节点保管以防范单点泄露风险。数据预处理阶段采用标准化与特征分箱技术，确保各机构数据在密文空间内的可对齐性，并以安全握手协议验证数据格式兼容性[2]。密文协同计算阶段，各机构将加密数据上传至安全计算节点，基于同态加密的加法与标量乘法同态性实现跨机构特征加权聚合，其核心运算可形式化表达为：

$$\mathrm{Enc}(y)=\sum_{i=1}^{n} w_i \cdot \mathrm{Enc}(x_i)+\mathrm{Enc}(b)$$

其中 w_i 为特征权重，b 为偏置项，所有运算均在密文空间执行。聚合后的加密风控指标 Enc(y) 经共识协议验证后传输至解密节点，结合阈值同态解密技术恢复明文结果 y，并依据预设规则输出风险等级。为提升计算效率，系统采用稀疏化特征选择与并行化计算框架，利用分块加密与流水线调度降低通信开销。此外，模型以动态协调模块实现多方协作策略的实时调整，例如基于贡献度评估的数据权重更新机制，以及异常参与节点的主动隔离策略[3]。

（二）风控模型技术实现

模型采用轻量化逻辑回归与集成学习相结合的策略，以平衡计算复杂度与风控精度需求。具体而言，各参与机构基于本地加密数据集 $\mathrm{Enc}(X_i)$ 执行前向传播，通过同态加密的线性运算特性计算加密预测值 $\mathrm{Enc}(\hat{y}_i)=\mathrm{Enc}(X_i)\cdot\mathrm{Enc}(W)$，其中 $W\in R^d$ 为全局加密权重向量[4]。为规避密文非线性激活函数计算的瓶颈，模型采用近似多项式拟合技术替代传统 Sigmoid 函数，定义加密状态下的损失函数为：

$$\mathrm{Enc}(L)=\sum_{i=1}^{n}\left(\mathrm{Enc}(\hat{y}_i)-\mathrm{Enc}(y_{\mathrm{true}})\right)^2$$

该损失函数通过密文减法与平方运算实现误差度量，并基于梯度同态性反向更新权重。全局参数聚合阶段，各机构上传加密梯度 $\mathrm{Enc}(\nabla W_i)$ 至协调节点，利用同态加法实现梯度融合 $\mathrm{Enc}(\nabla W)=\sum_{i=1}^{n}\mathrm{Enc}(\nabla W_i)$，随后以安全多方计算协议解密并更新 W。为提升计算效率，系统引入批处理技术与稀疏化编码策略，将高维特征映射至低维密文空间，并采用异步并行计算框架减少通信轮次。同时，通过门限解密机制确保权重更新过程的安全性，要求至少 t 个机构联合解密以防范恶意节点篡改[5]。

（三）安全性分析与实验验证

在安全性层面，联合风控模型需满足数据隐私性、计算完整性与抗合谋攻击三大核心要求[6]。基于同态加密的语义安全性，模型以加密方案的形式化定义抵御窃听与中间人攻击：对于任意概率多项式时间敌手 A，其区分加密数据 $\mathrm{Enc}(x_0)$ 与 $\mathrm{Enc}(x_1)$ 的优势可忽略不计，即满足：

$$\left|\Pr\left[\mathcal{A}\left(\mathrm{Enc}(pk,x_0)\right)=1\right]-\Pr\left[\mathcal{A}\left(\mathrm{Enc}(pk,x_1)\right)=1\right]\right|\le \mathrm{negl}(\lambda)$$

其中 $\mathrm{negl}(\lambda)$ 为安全参数 λ 下的可忽略函数。针对模型反演攻击，系统通过动态噪声注入破坏敌手对密文统计特性的推断能力，定义噪声扰动为 $\Delta\sim N(0,\sigma^2)$，并确保扰动后的密文满足 $\mathrm{Enc}(x+\Delta)$ 与原始分布不可区分。在抗合谋场景下，假设恶意节点数不超过门限 t，门限解密协议要求至少 t+1 个机构协同解密，其安全性由 Shamir 秘密共享方案保障：

$$\Pr\left[\mathrm{Dec}\left(sk,\mathrm{Enc}(y)\right)=y|\mathcal{C}|\le t\right]=1$$

实验验证部分构建多银行联合反欺诈模拟环境，采用标准金融数据集（如 Lending Club）与 CKKS 同态加密方案[7]。模型训练阶段，加密梯度聚合误差被约束在 $\|\nabla W_{\mathrm{enc}}-\nabla W_{\mathrm{plain}}\|_2\le\epsilon$，其中 ϵ 为预设容差阈值，实验结果表明加密模型的决策边界与明文模型高度一致。计算效率方面，定义单次训练轮次时间为 $T=O(d\cdot k^2)$，其中 d 为特征维度，k 为多项式环次数，优化后的并行计算框架使 T 随参与方数量线性增长，满足实时风控的低延迟需求。此外，对抗测试验证了模型在成员推理攻击下的鲁棒性，敌手成功概率被抑制至可接受范围内。

三、基于同态加密的金融科技平台多机构数据主权博弈分析

（一）多机构参与方的利益冲突

基于同态加密的联合风控模型中，多机构参与方的利益冲突根植于数据主权的排他性、风险共担的公共性与收益分配的竞争性之间的矛盾。数据作为核心生产要素，其所有权、使用权与收益权的法律界定模糊性，导致机构在数据共享过程中面临“囚徒困境”，一方面，个体机构倾向于保留高价值数据以维持自身竞争优势，但局部数据垄断将削弱联合模型的全局风控效能；另一方面，过度共享可能引发数据资产贬值、商业机密泄露及合规风险，形成“搭便车”与“公地悲剧”并存的博弈格局。从博弈论视角，参与方的策略选择受信息不对称与动态偏好影响。在非合作博弈框架下，机构倾向于将数据加密粒度、特征维度及更新频率作为策略变量，通过隐藏关键特征或降低数据质量实现个体效用最大化。然而，此类策略的纳什均衡往往导致整体风控模型陷入次优状态，表现为模型精度下降与泛化能力受损。此外，风险责任的非对称分配加剧了利益冲突：主导机构因模型主导权承担更高监管问责风险，而边缘参与方则可能利用信息黑箱逃避责任，形成“风险－收益”错配[8]。

（二）博弈模型构建

多机构数据主权博弈的模型构建需从参与者策略空间、收益函数与均衡条件三要素展开，旨在刻画加密技术约束下的协作稳定性与效率边界[9]。假设存在 n 个参与机构，每个机构 i 的策略选择涵盖数据贡献量 $d_i\in[0,D_i]$（D_i 为机构 i 的数据上限）与加密参数 $\theta_i\in\Theta$，二者共同决定其数据共享的“质量－隐私”权衡。博弈收益函数 U_i 由三部分构成：联合风控模型的协同收益 $R(d_i,\theta_i;d_{-i},\theta_{-i})$、数据主权损耗成本 $C(d_i,\theta_i)$ 及外部激励 $S(d_i)$，可形式化为：

$$U_i=\alpha\cdot R\left(d_i,\theta_i;\sum_{j\ne i}^{n}d_j\right)-\beta\cdot C(\|\theta_i-\theta_0\|)+\gamma\cdot S(d_i)$$

其中 α，β，γ 为权重系数，θ0为合规加密标准，R(·)随总数据量∑ dj递增但边际收益递减，C(·)衡量因加密参数偏离标准导致的模型兼容性损失，S(d_i)为基于 Shapley 值的激励分配。由于信息不对称，机构仅能观测到自身策略 (d_i, θ_i)与历史协作结果，形成动态贝叶斯博弈框架。均衡存在的条件需满足以下约束：对任意机构 i，存在策略组合 (d_i*, θ_i*)使得 U_i(d_i*, θ_i*;d_{-i}*, θ_{-i}*) ≥ U_i(d_i, θ_i;d_{-i}*, θ_{-i}*)对所有可行 (d_i, θ_i)成立。

进一步地，引入激励相容约束以确保参与者真实披露数据价值。定义机构 i 的类型为数据质量 qi ∈ [0,1]，其私有信息仅自身可知。以机制设计理论，构造转移支付函数 $T_i(q_i, \hat{q}_i)$ 惩罚虚报行为$\hat{q}_i = q_i$，使真实披露成为占优策略。此时，均衡解需满足：

$$\mathbb{E}_{q_{-i}}[U_i(q_i, q_i)] \geq \mathbb{E}_{q_{-i}}[U_i(q_i, \hat{q}_i)], \quad \forall \hat{q}_i \neq q_i$$

该条件确保在期望效用最大化下，机构无动机扭曲数据质量信号。模型以同态加密的可验证计算特性，将数据质量验证嵌入密文计算流程，例如利用零知识证明验证 q_i 与加密数据 Enc(d_i)的一致性，从而降低信息租金与策略操纵空间。最终，博弈模型揭示了加密技术如何改变策略可行域与信息结构，引导参与方从非合作均衡转向帕累托改进的协作均衡，为跨机构数据主权分配提供可计算的决策依据 [5]。

（三）激励机制与均衡解

多机构数据主权博弈的均衡解依赖于激励机制设计，其核心在于将个体理性与集体理性对齐，借助加密可验证性与契约约束消除策略性扭曲。基于 Shapley 值理论，机构数据贡献的边际收益分配需满足对称性、线性性与有效性公理，定义机构 i 的收益份额为：

$$\phi_i = \sum_{S \subseteq N \setminus \{i\}} \frac{|S|!\,(n - |S| - 1)!}{n!} [v(S \cup \{i\}) - v(S)]$$

其中 v(S)表示联盟 S 的联合风控效能，N 为全体参与者集合。该公式以量化机构对任意子联盟的边际贡献，确保收益分配与数据价值严格正相关，从而激励高质量数据共享。为规避传统 Shapley 值计算的全排列组合爆炸问题，模型引入同态加密的密文聚合特性，在加密状态下计算局部联盟效能差值 Enc(v(S ∪ {i})−v(S))，并运用安全多方计算协议解密后加权求和，实现隐私保护的动态收益分配。在均衡分析中，激励机制需满足参与约束与激励相容约束，前者要求机构参与协作的收益不低于独立运营的保留效用，后者确保真实披露数据质量与加密参数为占优策略 [10]。通过构建贝叶斯纳什均衡框架，证明当收益函数满足单调性与拟凹性时，存在唯一纯策略均衡解 (d_i*, θ_i*)，使得所有机构在加密技术约束下最大化效用。此外，模型引入智能合约驱动的惩罚机制，对恶意篡改加密参数或虚报数据质量的行为实施链上可信制裁，例如削减收益份额或冻结数据访问权限，从而将非合作博弈的“囚徒困境”转化为重复博弈下的长期合作均衡。

四、结束语

本研究通过融合同态加密技术与动态博弈模型，构建了兼顾隐私安全与风控效能的多机构联合协作框架，为破解数据主权博弈困境提供了理论支撑与实践路径。模型在保障密文计算安全性的同时优化了计算效率；博弈均衡设计与激励机制实现了数据贡献与收益分配的动态平衡。未来，相关研究工作者应进一步探索轻量化加密算法的工程适配性、跨链协同治理机制，推动金融科技生态从“数据割据”向“安全共生”演进。

参考文献

[1] 白昌易，芦彦清，韩苗苗 . 金融科技平台监管的演化博弈研究 [J]. 科学决策，2024,(02):132-142.

[2] 宋华，韩思齐，刘文诣 . 数字化金融科技平台赋能的供应链金融模式——基于信息处理视角的双案例研究 [J]. 管理评论，2024,36(01):264-275.

[3] 杨拥军 . 金融科技平台公司的正反面 [J]. 中国外资，2024,(02):90-92.

[4] 南曦 . 供应链金融科技平台商业模式及服务效能比较研究 [D]. 电子科技大学，2023.

[5] 吕军 . 基于人工智能的金融科技平台欺诈风险管理研究 [D]. 北京邮电大学，2023.

[6] 陈小萌 . 基于同态加密的多源数据密态计算协议研究 [D]. 西安电子科技大学，2023.

[7] 余致远 . 金融科技平台特质、风险与监管研究 [D]. 北京邮电大学，2022.

[8] 方淳，郑珂，张津菲，等 . 国内金融科技平台运作模式特点、风险及监管探讨——基于案例法 [J]. 中国商论，2021,(22):95-100.

[9] 江奕 . 供应链金融科技平台运行模式研究 [D]. 华南理工大学，2021.

[10] 季成，叶军 . 金融科技平台的风险及管理框架 [J]. 河北金融，2019,(09):19-22+47.