

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(10) 国际公布号
WO 2024/139273 A1

(43) 国际公布日
2024 年 7 月 4 日 (04.07.2024)

- (51) 国际专利分类号:
G06N 20/00 (2019.01) *G06F 21/57* (2013.01)
- (21) 国际申请号: PCT/CN2023/114304
- (22) 国际申请日: 2023 年 8 月 22 日 (22.08.2023)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202211676596.8 2022 年 12 月 26 日 (26.12.2022) CN
- (71) 申请人: 支付宝 (杭州) 信息技术有限公司 (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) [CN/CN]; 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。
- (72) 发明人: 刘焱 (LIU, Yan); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

- (74) 代理人: 北京博思佳知识产权代理有限公司 (BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区上地三街 9 号嘉华大厦 B 座 409, Beijing 100085 (CN)。
- (81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。
- (84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚

(54) Title: FEDERATED LEARNING METHOD AND APPARATUS, READABLE STORAGE MEDIUM, AND ELECTRONIC DEVICE

(54) 发明名称: 联邦学习方法、装置、可读存储介质及电子设备

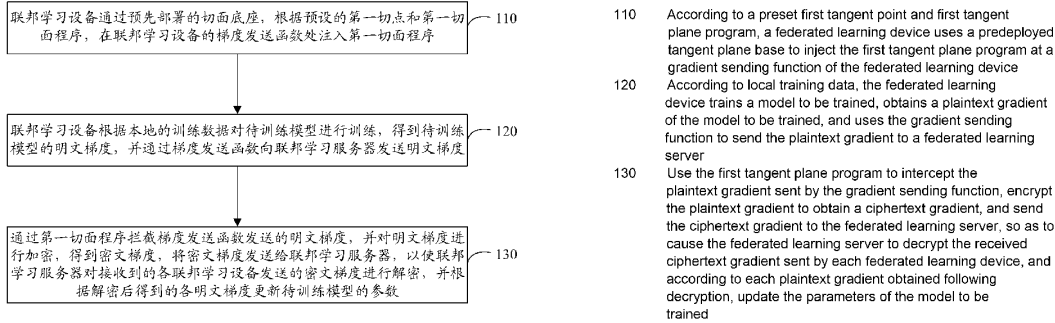


图 1

(57) Abstract: The present application relates to a federated learning method and apparatus, a readable storage medium, and an electronic device. The method comprises: using a predeployed tangent plane base, injecting a first tangent plane program at a gradient sending function of a federated learning device; according to local training data, training a model to be trained, obtaining a plaintext gradient of the model to be trained, and using the gradient sending function to send the plaintext gradient to a federated learning server; using the first tangent plane program to intercept the plaintext gradient, encrypt the plaintext gradient to obtain a ciphertext gradient, and send the ciphertext gradient to the federated learning server, so as to cause the federated learning server to decrypt the received ciphertext gradient sent by each federated learning device, and according to each plaintext gradient obtained following decryption, update the parameters of the model to be trained. The federated learning method and apparatus of the present application involve encrypting a plaintext gradient of a federated learning device, and sending the encrypted ciphertext gradient to a federated learning server, thereby avoiding privacy leaks caused by an attacker obtaining the plaintext gradient.

[见续页]

WO 2024/139273 A1

(AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：
— 包括国际检索报告(条约第21条(3))。

(57) 摘要: 本申请涉及一种联邦学习方法、装置、可读存储介质及电子设备, 所述方法包括: 通过预先部署的切面底座, 在联邦学习设备的梯度发送函数处注入第一切面程序; 根据本地的训练数据对待训练模型进行训练, 得到待训练模型的明文梯度, 并通过梯度发送函数向联邦学习服务器发送明文梯度; 通过第一切面程序拦截明文梯度, 并加密, 得到密文梯度, 将其发送给联邦学习服务器, 以使联邦学习服务器对接收到的各联邦学习设备发送的密文梯度进行解密, 并根据解密后得到的各明文梯度更新待训练模型的参数。本申请的联邦学习方法及装置, 对联邦学习设备的明文梯度进行加密, 并将加密后的密文梯度发送至联邦学习服务器, 可避免明文梯度被攻击者获取而导致隐私泄露。