标题：基于BCP算法的多密钥SVM联邦学习算法研究与实现

类型：软件设计

内容：

联邦学习是当下热门的保障数据安全的机器学习建模方法，能够解决数据无法直接整合进行机器学习模型训练的问题，避免数据从本地的移动和泄漏。目前联邦学习的实现方案大多采用单密钥的方式，即各个数据拥有方拥有相同的公钥和私钥，并将用公钥加密后的模型参数上传至中心节点。这样做的缺陷是可以通过模型参数推导出数据的分部信息。

本系统将提出一种基于BCP算法的支持多密钥的联邦学习支持向量机的实现方案。在联邦分布式系统下，各个数据提供方独立求解支持向量机模型，将模型参数上传至中心节点，并采用支持多密钥的同态加密算法，同时选择分布式机器学习模型聚合策略，对模型做安全聚合，实现数据的隐私保护。

性能指标：

整个训练过程分为模型求解、秘钥分发、安全聚合三个部分。

主要的性能指标有训练中各环节运算时间，各个数据方得到的模型预测召回率、精确率等。

所需知识：同态加密、多密钥加密、联邦学习、支持向量机算法。

使用仪器：PC机、Linux服务器。