# CryptDB数据库接口

## 1、业务逻辑一：创建数据库

接口函数：Connection（数据库地址，管理员账户/密码）

CreateDB （数据库名 管理员账户/密码）

Disconnection（数据库名）

交互流程如图1：

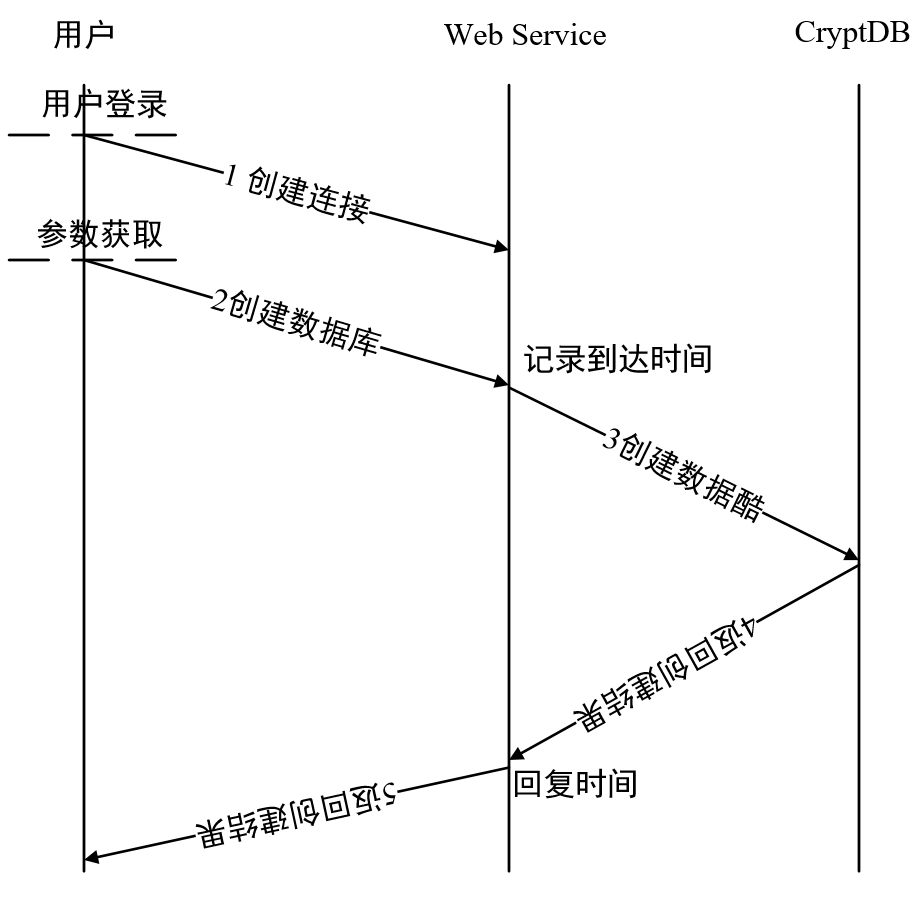


图 1 创建数据库交互流程

## 2、业务逻辑二:建立数据库表

接口函数：CreateTable: （表名, 字段名/类型 （无符号整型/整型/定点数型/字符型））

交互流程如图2：

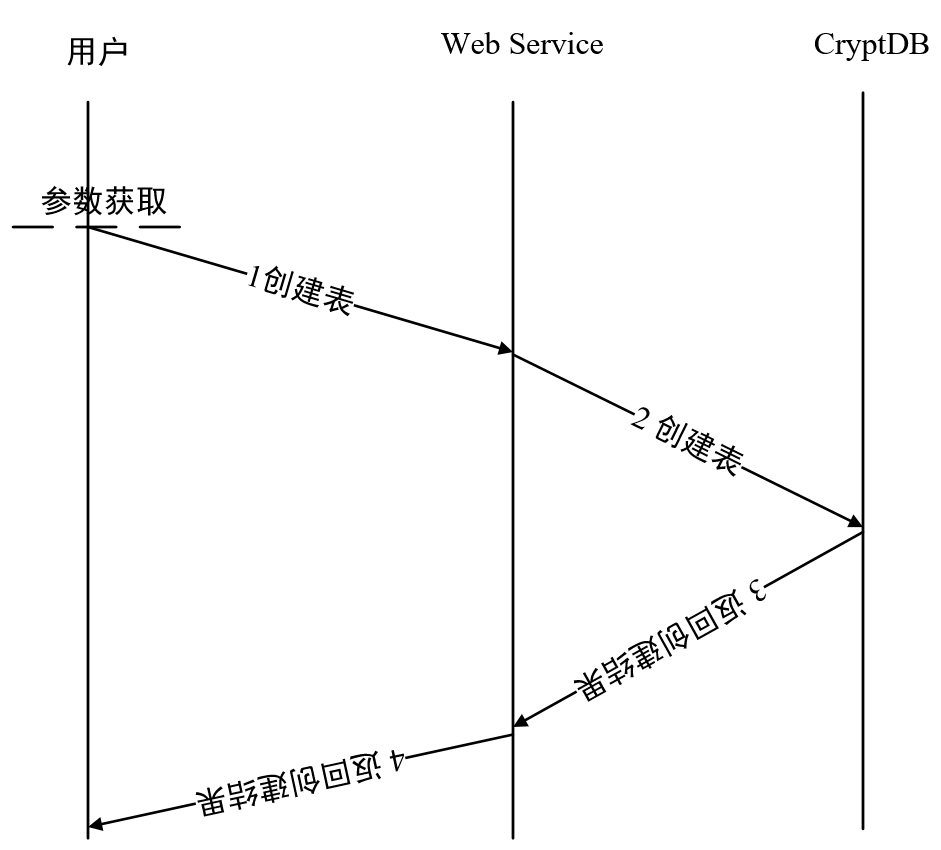


图 2 创建数据库表流程

## 3、业务逻辑三：数据的增删改

接口函数：Insert（表名 表项数据）

Update（表名 字段-数据序列 条件）

Delete（表名 条件）

交互流程如图3：

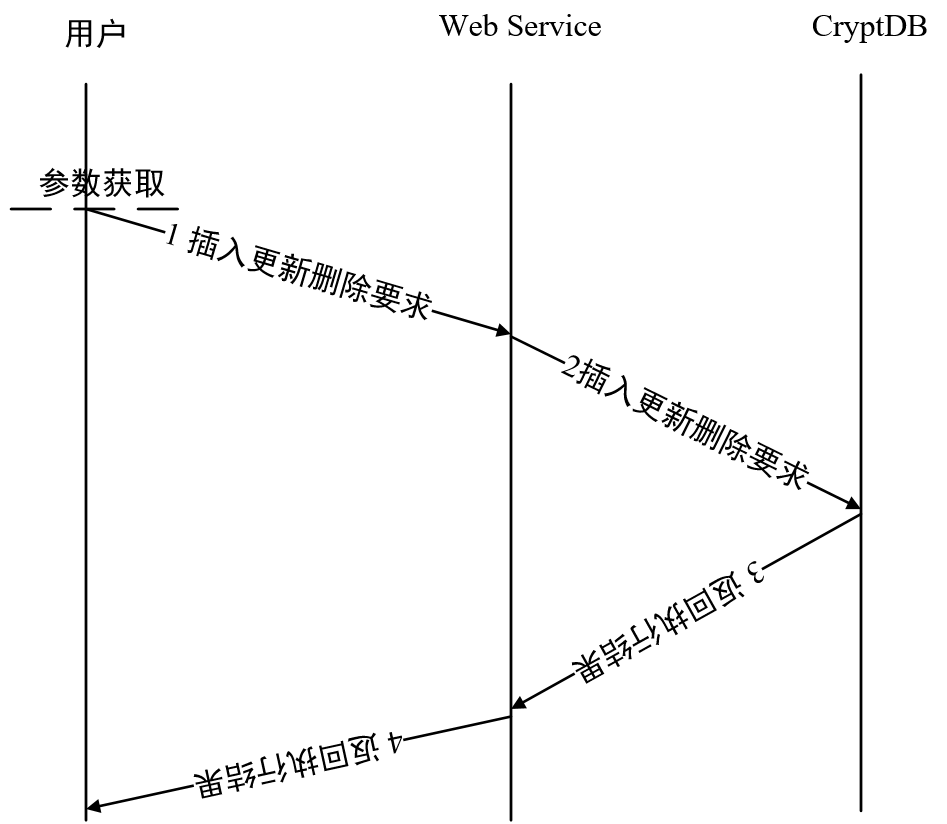


图 3 数据增删改交互流程

## 4、业务逻辑四：同态加密初始化（加解密前操作）

接口函数：CipherInit（算法/方案 密钥及其他初始数据）

交互流程如图4:

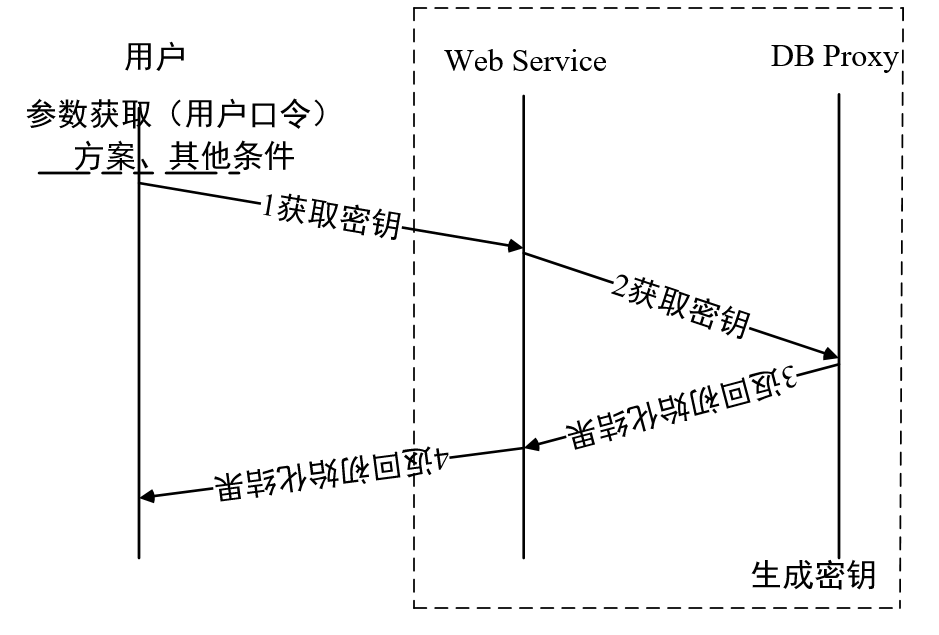


图 4 同态加密初始化

5、业务逻辑五：同态加密以及运算

接口函数：Encryption（数据明文）

HomAdd（数据密文1，数据密文2）

HomMul（数据密文1，数据密文2）

Decryption（数据密文）

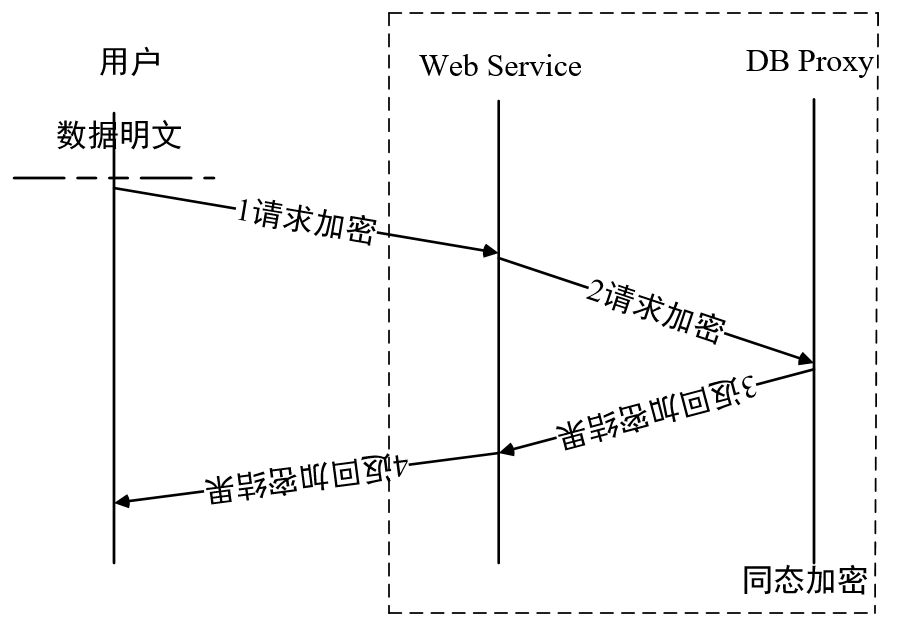


图 5 Encryption加密交互流程图

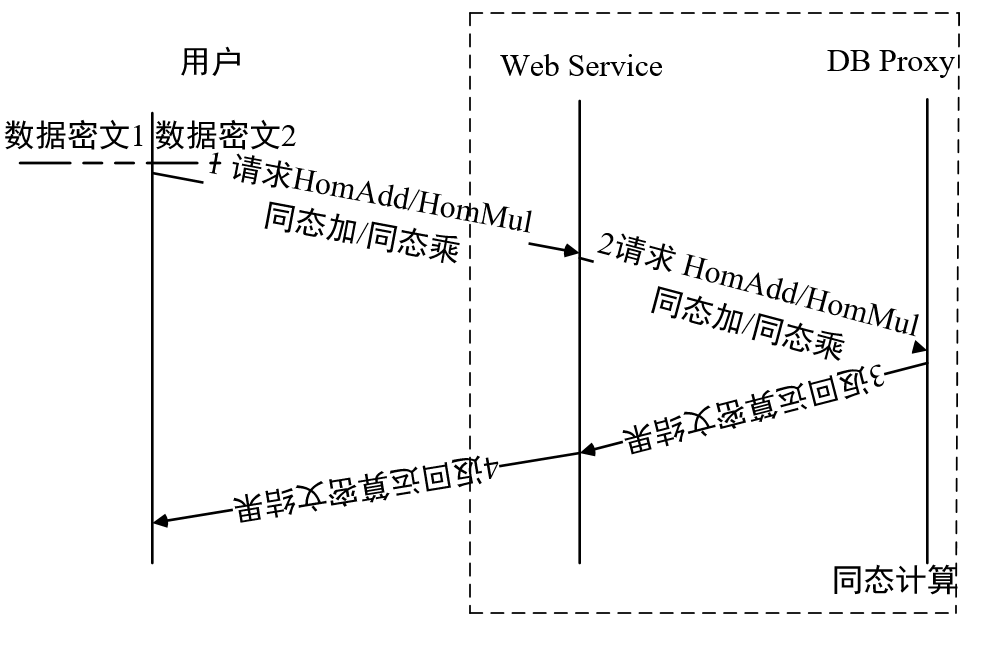


图 6 同态计算交互流程图

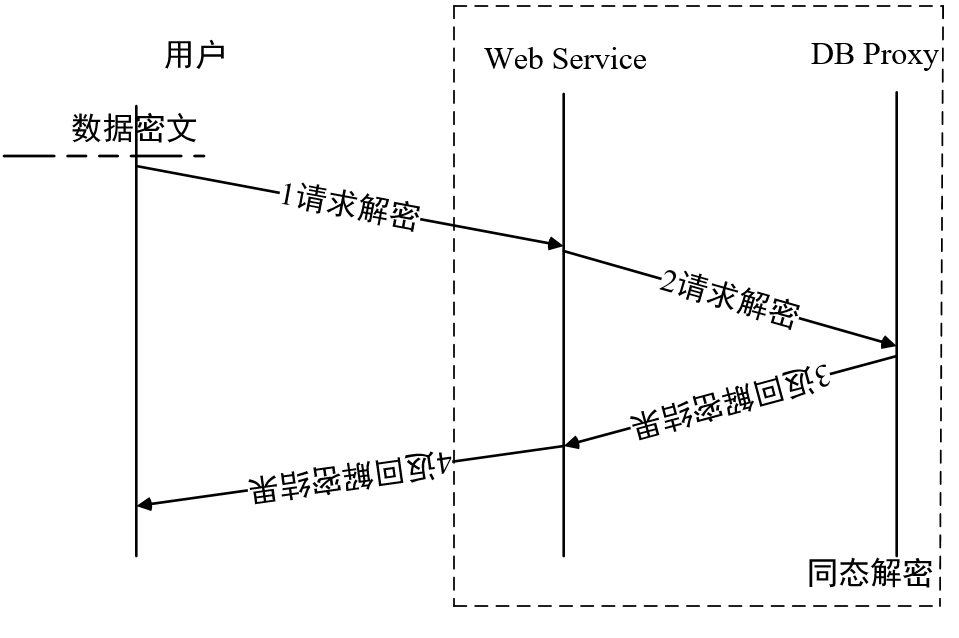


图 7 Decryption 解密交互流程图

## 6、业务逻辑六：求平均值/均方差/线性回归

接口函数：AverageWithEncryption（表名 字段 条件 密文返回）

StandardDeviationWithEncryption（表名 字段 条件 密文返回）

LinearRegressionWithEncryption（表名 字段1 字段2 条件 密文返回）

交互流程如图5：

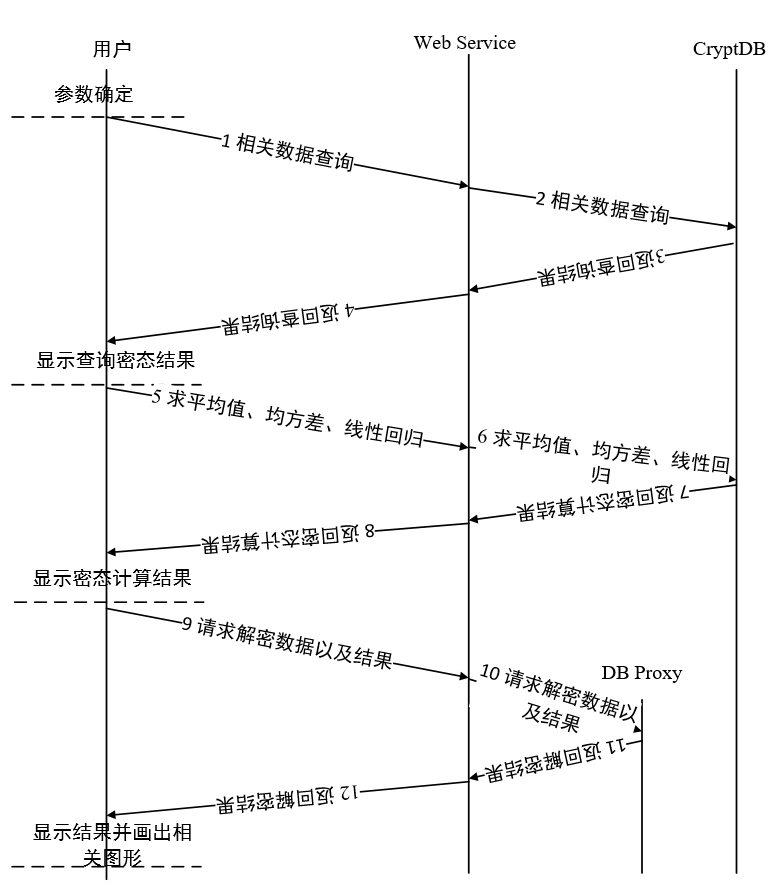


图 8 求平均值、方差、线性回归交互流程

## 7、业务逻辑七：普通查询、包含密态比较/排序

接口函数：QueryWithEncryption（表名 字段序列 条件 密文返回 (体现密态比较, 密态排序功能)）

交互流程类似图8，只是没有求解均值/均方差/线性回归的步骤。