

鸿蒙系统中基于同态加密的婚介系统设计与实现

杨军伟¹, 欧东阳²

(1. 浙江同济科技职业学院 经济与信息学院, 浙江 杭州 311200;

2. 杭州电子科技大学 计算机学院, 浙江 杭州 310018)

摘要: 针对在线婚介系统中用户隐私数据易泄露的问题, 提出一种基于鸿蒙平台与CKKS同态加密方案的婚介系统设计与实现方法。首先, 阐述了CKKS同态加密的基本原理及技术特点, 采用Microsoft SEAL开源库进行数据加密, 确保用户数据在上传和存储过程中始终处于密文状态; 其次, 设计了基于用户基本特征的特征匹配算法, 通过计算密文向量的同态相似度, 实现对加密用户数据的精准匹配和推荐; 最后, 在系统架构设计方面, 利用鸿蒙系统的Ability架构特性, 清晰划分客户端与服务器端功能模块。结果表明, 系统在保护用户隐私的同时, 相比明文匹配推荐, 在密文状态下的匹配计算准确率可达99.9%, 具备良好的安全性和实用性, 为隐私保护型婚介应用提供了可行方案。

关键词: CKKS; 同态加密; 特征匹配算法; HarmonyOS; 在线婚介系统

DOI: 10.11907/rjdk.251361

开放科学(资源服务)标识码(OSID):

中图分类号: TP309.7

文献标识码: A

文章编号: 1672-7800(2025)008-0152-06



Design and Implementation of A Homomorphic Encryption-Based Matchmaking System in HarmonyOS

YANG Junwei¹, OU Dongyang²

(1. College of Economics and Information, Zhejiang Tongji Vocational College of Science and Technology, Hangzhou 311200, China;

2. School of Computer Science, Hanzhou Dianzi University, Hangzhou 310018, China)

Abstract: To address the issue of user privacy data leakage in online matchmaking systems, this paper proposes a design and implementation method for a privacy-preserving matchmaking system based on the HarmonyOS platform and the CKKS homomorphic encryption scheme. First, the fundamental principles and technical features of the CKKS approximate homomorphic encryption scheme are introduced. The Microsoft SEAL open-source library is utilized to perform data encryption, ensuring that user data remains encrypted throughout the upload and storage processes. Second, a feature matching algorithm based on users' basic attributes is designed. By computing the homomorphic similarity of ciphertext vectors, the system achieves accurate matching and recommendation of encrypted user profiles. In terms of system architecture, the design fully leverages the HarmonyOS Ability framework to clearly separate client-side and server-side functional modules. Experimental results demonstrate that the proposed system effectively protects user privacy while achieving a matching accuracy of up to 99.9% under ciphertext conditions—comparable to plaintext matching. The system delivers efficient and accurate feature matching, offering strong security and practical applicability, thereby providing a feasible solution for privacy-preserving matchmaking applications.

Key Words: CKKS; homomorphic encryption; feature-matching algorithm; HarmonyOS; online matchmaking systems

0 引言

随着物联网、云计算和人工智能的快速发展, 数据安

全与用户隐私保护成为各领域关注的焦点。在线婚介交友应用中, 用户通常需要提交个人基本信息(如年龄、职业、兴趣爱好等)以匹配合适的对象, 但这些敏感数据在上传至服务器后若缺乏有效防护, 可能导致隐私泄露事件,

收稿日期: 2025-05-26

扫描二维码阅读全文:



基金项目: 浙江同济科技职业学院校级一般科研项目(FRF24YB014)

作者简介: 杨军伟(1987-), 男, 硕士, 浙江同济科技职业学院经济与信息学院讲师, 研究方向为信息安全、人工智能、云计算与大数据等; 欧东阳(1980-), 男, 博士, 杭州电子科技大学计算机学院讲师, 研究方向为云计算、边缘计算、人工智能、信息安全等。
本文通讯作者: 杨军伟。

进而影响此类应用的市场信誉和用户信任^[1]。现有的部分隐私保护方案, 要么需要借助不可信的第三方中介, 要么需以服务准确性下降为代价^[2-3]。因此, 如何在不暴露用户明文信息的前提下实现婚介匹配功能, 成为一个亟待解决的问题。通过结合匹配推荐算法和同态加密方案, 本文实现了在兼顾用户隐私保护和匹配推荐准确性的同时, 与国内自主研发的鸿蒙系统相结合, 构建一个既安全又有效的隐私保护型婚介应用系统。

1 相关研究

目前, 与同态加密方案有关的匹配算法的应用领域主要有社交匹配、推荐系统和基因比对等。例如, 在社交匹配领域, Wang等^[4]提出的方案是: 客户端将用户属性进行分组加密后上传至服务器, 存储加密数据。当有新用户进行匹配查询时, 服务器在这些密文上计算该用户与其他用户在各属性分组上的匹配程度。在技术实现上, 引入了Gentry^[5]提出的全同态加密方案作为基础, 推测所采用的时基于格的同态加密, 实现了端到端的用户隐私防护。然而, 该方法计算复杂度较高, 难以满足实时应用需求。在推荐系统领域, Perifanis等^[6]提出的FedPOIRec将同态加密融入联邦学习, 用于位置兴趣点(POI)推荐。虽然该方法的推荐精度没有下降, 但是用户端的加密计算产生了额外的计算和通信开销。在基因比对领域, Intel研究院的De Souza等^[7]提出了一种基于同态加密的安全计算方法用于亲属检测。通过采用高度优化的CKKS实现方案, 能够在数秒内处理包含2 000个基因样本的数据库中的400项查询。该方案的高效性能主要得益于对本地硬件加速的利用以及SIMD(单指令多数据)并行计算的支持。Shokri等^[8]提出了通过引入MinHash等方法将复杂的DNA匹配问题转化为简化的同态运算。然而, 本研究并非简单地将某一同态加密算法直接应用于匹配算法, 而是深度定制了匹配算法, 以更好地契合CKKS的计算范式。尽管Lagesse等^[9]开发了一个Android原型应用, 并集成到移动设备以实现加密视频相似度匹配, 但其在同态加密预处理时长1min的视频仍需17s。Apple公司近期也在iOS系统中引入了同态加密技术, 用于来电号码的匹配查询, 使手机端能够查询服务器数据库中的匹配号码, 而无需泄露号码明文。^[10]。尽管移动端部署同态加密展现了巨大潜力, 但在HarmonyOS平台上集成CKKS同态计算模块的实践尚未有公开报道。本研究首次将CKKS同态计算模块嵌入HarmonyOS移动端, 实现了用户设备直接进行加密匹配计算, 这一创新填补了当前研究空白。通过实际系统开发和测试, 验证了该方案在实际移动环境中的可行性和性能表现。

综上所述, 本文在同态加密与鸿蒙系统的交叉应用领域提供了新的研究视角与实践案例, 丰富了隐私保护型婚介应用的技术路径。

2 相关知识

2.1 同态加密及CKKS方案

同态加密是一种特殊的加密技术, 允许在不解密数据的情况下直接对密文执行运算, 运算结果解密后与对明文执行相应运算的结果相同^[4]。这意味着使用同态加密, 云端服务器可以对用户加密后的敏感数据进行计算, 而无法得知明文内容, 从而在提供服务的同时保障数据机密性。根据支持运算的丰富程度, 同态加密可分为部分同态加密(支持特定的加法或乘法)、有限次的全同态加密(支持一定深度的电路运算)以及完全全同态加密(支持任意深度的运算, 即FHE)^[11]。2009年, Gentry等^[5]首次构造了完全同态加密方案之后, 全同态加密(FHE)技术迅速发展, 涌现出多种基于格密码的方案。如Brakerski等^[12]提出的基于标准LWE(Learning With Errors)难题的效率更高的方案, Fan等^[13]提出的基于环LWE的更高效方案(如BV(Brakerski和Vaikuntanathan)、FV(Fan和Vercauteren)等)以及张兴兰等^[14]提出的基于没有高斯函数生成噪声的LWE问题的高效方案等。这些工作为隐私计算奠定了重要基础。然而, 早期FHE方案主要针对整数或二进制比特的精确计算, 在面对现实应用中大量涉及实数数据(如用户评分、传感器数据等)的计算需求时, 效率和精度方面面临着挑战。

2017年, Cheon等^[15]提出了支持近似计算的全同态加密方案, 即CKKS方案。CKKS(也称为Homomorphic Encryption for Arithmetic of Approximate Numbers, HEAAN), 其特点是在允许对密文进行加、乘运算的同时, 引入一定的数值近似误差, 从而大幅降低噪声增长和密文尺寸, 实现对实数/复数数据的同态计算。其核心思想是将明文空间定义为固定精度的实数集, 利用多项式近似替代Bootstrapping过程中的精确位提取操作, 以换取更高的运算效率^[16-17]。CKKS方案在结构上与传统的BFV/BGV等基于环状LWE的方案类似, 采用多项式环上的加密方式, 其安全性基于RLWE(Ring Learning With Errors)困难问题, 具有准则下的IND-CPA语义安全性。不同之处在于CKKS将明文编码为多元复数向量(通常采用定点表示实数), 并引入可控的误差完成同态计算。通过在计算深度较大时进行适当尺度缩放处理, 可以去除多余噪声, 从而在解密后保留所需的精度。由于许多实际应用并不要求绝对精确的计算结果(例如推荐评分、统计分析等允许一定误差), CKKS方案在这些场景中具有独特优势。

Microsoft SEAL库是微软研究院开发的开源同态加密库, 提供了包括CKKS在内多种主流方案的实现^[18]。本文系统使用SEAL库直接调用CKKS方案的接口, 对实数明文向量进行编码加密、同态运算和解密, 屏蔽了底层复杂的数学运算, 实现了“开箱即用”的同态加密功能。这为在

HarmonyOS 移动应用中集成同态加密提供了可能。由于 CKKS 方案的性能在近年不断提升,其已能够支持中等规模的数据计算。例如,Choi 等^[19]提出的研究方法在 128 维特征向量上实现了同态余弦相似度计算,并能在不到 1s 内匹配数千条加密特征。这些研究进展表明,将 CKKS 加密方案应用于实时婚介匹配计算,在技术层面具备可行性。

2.2 特征匹配算法

婚介系统的匹配推荐需要将用户信息转换为适合计算的数学形式,即特征向量^[20-21]。本文选择年龄、身高、学历、收入等级及兴趣爱好等基本属性构成用户特征向量^[22]。数值型特征通过归一化处理为 $[0, 1]$ 区间值,而类别型特征(如兴趣类别)采用独热编码或预定义类别指数表示。在同态加密场景下,特征的离散化需与 CKKS 方案支持的明文空间适配^[4, 23]。鉴于 CKKS 方案支持实数运算,无需过度离散化,仅做适度量化即可保留足够的匹配信息。

确定特征向量后,需定义 2 个用户间的匹配度或相似度以进行匹配计算。常用方法包括欧氏距离和余弦相似度。其中,余弦相似度因能有效反映用户兴趣偏好的相似方向,在推荐系统中被广泛使用。具体如公式(1)所示:

$$\text{sim}(A, B) = \frac{\langle X_A, X_B \rangle}{\|X_A\| \|X_B\|} \quad (1)$$

其中, $\langle X_A, X_B \rangle$ 为特征向量的点积。考虑到同态加密场景下难以直接执行除法和开方运算,实际实现中可提前对特征向量归一化,使向量点积直接单调对应余弦相似度,简化为仅需执行同态点积计算。此外,为降低噪声增长和运算复杂度,可采用将高维特征向量拆分成多个低维片段分别进行同态计算的优化策略。这种分块计算方法已被研究证明可有效提高匹配效率和精度。

匹配算法还包括筛选排序和稳定匹配机制。本文选择评分排序的策略,即服务器在密文域内计算用户与异性候选对象的匹配度评分,并返回给客户端解密、排序和推荐。这种方法计算简单、高效且易于在加密域实现,服务器全程无法获知明文信息,能够确保隐私安全。

3 系统总体架构设计

3.1 系统架构概述

系统采用客户端-服务器的分布式架构,由 HarmonyOS 移动客户端和后端服务器共同构成。图 1 展示了系统的总体架构。其中,客户端负责采集用户信息、执行加解密操作以及呈现匹配结果;服务器端承担存储加密数据和在密文上执行匹配计算的功能。两端通过安全通信信道交互数据。

客户端为 HarmonyOS 原生应用,应用架构遵循 HarmonyOS 分层设计思想,由用户交互层、业务逻辑层和数据管理层组成。用户交互层提供用户交互,包括注册登录界面、资料填写界面和匹配结果展示界面等;业务逻辑层实

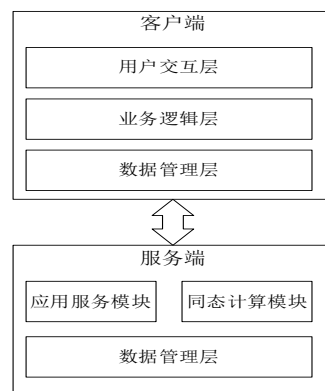


Fig. 1 Overall system architecture diagram

图 1 系统总体架构图

现应用逻辑,如调用加密库进行数据加密、向服务器发送请求及处理响应等;数据管理层则管理本地的数据存储,如缓存的密文和密钥等。

服务器由应用服务模块和同态计算服务模块组成。应用服务模块提供常规的业务逻辑接口(如用户注册登录、资料上传、配对请求等);同态计算模块则集成了 CKKS 算法库,用于执行加密数据匹配计算。此外,服务器还包含数据库,用于存储用户的加密特征信息和必要的密钥公参数。

3.2 HarmonyOS 应用框架设计

HarmonyOS 引入了独特的 Ability 架构,将应用功能单元抽象为不同类型的“能力”^[24-25]。本系统在客户端设计中充分利用了这种架构,如图 2 所示,将应用划分为前台与后台 2 个部分,即界面 Ability 和服务 Ability。界面 Ability 属于 Feature Ability 的一种,实现应用的 UI 界面和用户交互。本项目采用 Page Ability 模板来组织不同页面(如资料编辑页、匹配结果页等),保证良好的用户体验。服务 Ability 则属于 Particle Ability,在后台运行且无界面,用于执行密文加解密和网络通信等任务,相当于 Android 中的 Service。这种前后端分离的设计使得应用在获取用户输入后,能够立刻交由后台线程进行加密和数据上传,而前台界面不被阻塞,极大提升了系统的响应性。

此外,考虑到婚介应用需要长期保存用户资料及密钥,客户端引入 Data Ability 来管理本地数据存取。Data Ability 提供统一的数据访问接口,将用户的密钥对、安全参数等存储于其管理的数据库中,并对其他 Ability 开放查询接口。借助 HarmonyOS 提供的组件生命周期管理和分布式任务调度功能,本应用能够在不同设备之间实现平滑迁移或协同工作。例如,用户在手机上加密上传资料后,登录同一 HarmonyOS 账号的平板设备就能自动接收匹配结果,无需重复输入数据——这得益于 HarmonyOS 的分布式数据管理机制。通过合理利用 HarmonyOS 架构特点,系统将模块职责划分清晰,各模块在独立运行的同时,通过系统服务紧密协作,成功实现了端到端的安全婚恋匹配服务。

3.3 功能模块划分

根据上述架构,本系统的主要功能模块及其作用如下:

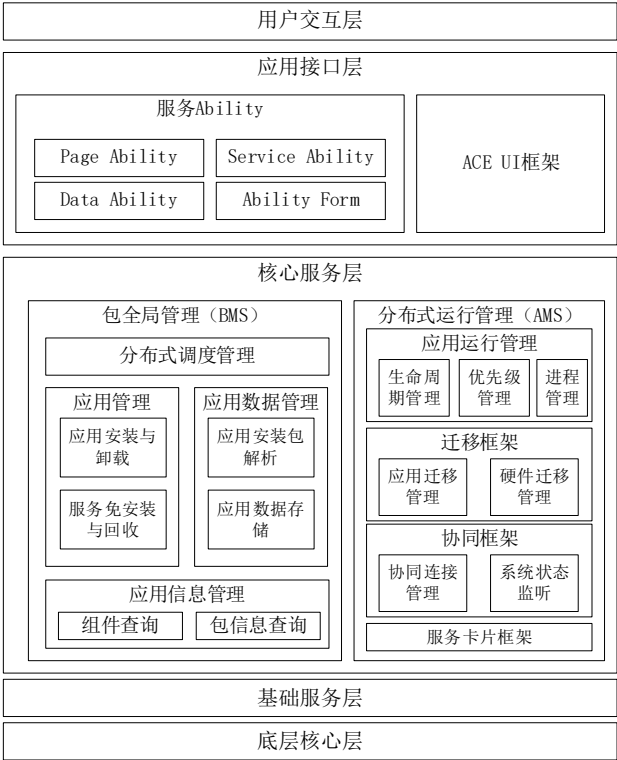


Fig. 2 Structure diagram of HarmonyOS distributed application
图 2 HarmonyOS 分布式应用程序结构图

(1)用户管理模块(客户端)。包括用户注册、登录与认证功能。用户在首次使用时需要注册账号,并生成用于同态加密的公私钥对。私钥安全保存在本地设备中,而公钥和加密数据会被上传到服务器以便保存。完成登录后,用户可以编辑个人资料中的特征信息。

(2)加解密模块(客户端)。封装 Microsoft SEAL 库接口,实现 CKKS 方案的本地调用。主要功能有 3 种:①根据系统预设参数生成 CKKS 公私钥和加密参数(由客户端或可信机构生成后分发);②将用户明文特征向量编码加密得到密文;③对服务器返回的密文匹配结果进行解密,输出可读的推荐名单。加密模块由 Service Ability 调用,在后台执行,以免阻塞 UI。

(3)通信模块(客户端)。负责客户端与服务器的网络交互。通过 HarmonyOS 提供的通信框架,与服务器建立 TLS 加密连接,发送加密后的用户数据和匹配请求,并接收服务器返回的加密匹配结果。通信模块需要确保请求格式和加密数据格式正确,并处理异常情况。

(4)匹配计算模块(服务器)。服务器端的核心模块。首先,接受来自客户端的新用户密文特征数据,将其存入数据库。随后,当有匹配请求时,提取请求方的密文特征,利用同态加密库依次与数据库中其他用户密文特征进行匹配度计算。由于所有数据均为密文,服务器在计算过程中无法访问到明文数据,但仍能执行批量计算任务,计算所得的匹配分数也同样是密文形式。此外,服务器为了处理排序操作,且考虑到同态加密环境下比较运算的复杂度较高,系统采用了一种优化策略:将匹配分数发送到请求

客户端,客户端在解密后进行排序,然后将排序后的密文分数返回至服务器,从而实现高效的处理流程。最终,服务器将筛选出的若干潜在匹配对象的加密标识发送给请求用户。

(5)结果处理模块(客户端)。收到服务器返回的匹配结果密文后,调用加密模块解密。客户端可以获得推荐的匹配对象清单,然后通过用户管理模块从服务器请求该匹配用户的公开资料,最终在界面上呈现给用户浏览和选择联系。

上述模块各司其职,构成完整的婚介服务流程:用户—加密—上传—匹配—解密—展示。在系统架构设计上,通过前后端解耦和模块化,确保即使在引入复杂的同态加密计算后,系统仍具备良好的可维护性和扩展性。例如,未来若需替换更先进的加密算法,整体架构将不受影响;同时,可以轻松集成新的特征类型或匹配算法,仅需修改相关模块。

4 系统实现与测试

4.1 关键功能实现

按照架构设计,系统基于 HarmonyOS SDK 和 Microsoft SEAL 库完成了系统各功能的编码实现。客户端采用 HarmonyOS 3.1 平台,使用方舟编译器支持的 JavaScript(eTS)语言编写 UI 页面,C++编写本地服务。利用 HarmonyOS 提供的 NDK 机制,将 SEAL 库打包成静态库供应用使用,在 ARM64 手机上实现了顺利运行。

(1)密钥管理与分发。系统初始化时,由客户端生成 CKKS 所需的密钥和参数。为了兼顾安全与效率,系统选择多项式模数 q 和多项式环度 N ,用以满足 128-bit 安全水平,同时,支持一次加密多个特征。生成的公钥和重线性化密钥等,通过安全信道上传存储在服务器,便于服务器在加密域执行匹配计算时使用;私钥则严格保存在用户设备的 Keystore 中,不传至服务器,从而保证服务器即使存储和计算了密文数据,也无法自行解密获取用户隐私信息。

(2)用户特征加密存储。用户在填写或更新个人资料后,客户端会调用加密模块,将用户特征向量进行加密。系统对每位用户定义了包含 5 个属性的特征向量:年龄差距容忍度、地区编码以及含有阅读、音乐和运动的 3 个兴趣类别向量。其中年龄、地区等以离散区间或类别数值表示,兴趣类别向量为 0/1 值表示是否有共同偏好。客户端将上述 5 维向量使用 CKKS 方案加密,得到密文大小约为 1KB。密文通过通信模块发送到服务器,并存储于数据库相应用户的记录中。数据库仅保存加密后的特征,而非存储明文数据,从而提高了数据存储的安全性。

(3)匹配请求与同态计算。当用户发起匹配请求时,客户端将该用户的用户 ID 发送至服务器。服务器查询数据库获取此用户的特征密文 c_A 。随后,服务器遍历候选池

中的其他用户密文 c_B , 利用同态计算模块对 c_A 和 c_B 执行匹配度运算。具体包括: 模式(a)同态相似度计算和模式(b)属性条件匹配。其中, 模式(a)计算 c_A 和 c_B 的内积, 同态结果记为 c_{sim} 。由于 CKKS 支持近似算术, 直接将归一化处理留给客户端, 即服务器只需计算内积结果密文即可。模式(b)逐项比较主要属性是否相等, 即兴趣类别是否有重合。由于 CKKS 本身不支持直接比较, 故采用将布尔属性值 0/1 以明文方式嵌入密文向量, 通过同态乘积和加法计算得到表示“是否相同”的密文标志位。例如, 对兴趣爱好而言, 令 3 个兴趣维度各计算一次 $e_i = c_{A_i} - c_{B_i}$ 的同态差, 然后再计算 e_i 同态乘积 $prod = e_1 \cdot e_2 \cdot e_3$, 如果兴趣完全相同则 $prod$ 结果为 0, 否则为非零。这个结果在密文中无法直接判定, 但可以发送给客户端解密判断。基于判定结果, 服务器对匹配对象进行筛选。上述 2 种模式中, (a) 更为灵活, 可排序推荐; (b) 强调严格匹配但无法排序。在本系统中综合采用如下方案: 首先筛选与用户关键属性不匹配的内容, 然后按照模式(a)对剩余候选内容进行评分。

(4) 密文结果处理与返回。服务器将计算得到的若干候选对象的匹配度密文结果返回给请求用户的客户端。由于统一使用一把公钥, 加密结果可以被请求用户所在客户端解密。客户端解密后获得候选对象列表及其匹配评分明文。随后, 客户端可以按照评分高低排序并展示。例如, 系统实现了一个简洁的推荐列表 UI, 顶部显示匹配度最高的 3 个匹配用户 ID 及与自己的匹配度的值。在整个过程中, 服务器始终处理的是密文信息。一旦用户信息离开客户端设备, 则以密文形式存在。尽管服务器完成了匹配计算, 但对具体的匹配结果和用户数据仍然不知情, 这一设计充分保障了系统的核心安全目标。

4.2 测试与评估

通过对系统的功能和性能进行测试, 结果表明, 基于同态加密的婚介匹配在 HarmonyOS 环境下是可行的。

(1) 功能正确性。测试集构造了一个包含 10 对用户的模拟数据集。每对用户双方在兴趣爱好等方面都具有较高的契合度。我们期望系统能够将对用户相互推荐。首先, 将这 20 个用户数据加密后存入服务器, 并随机选择其中一人作为主动查询发起匹配。随后, 客户端对加密数据进行解密, 前 3 名推荐中成功包含了契合度最高的用户对象, 匹配成功率达到 100%, 如表 1 所示。此外, 系统还验证了不同属性的影响。当人为修改某用户的兴趣偏好, 使其与原匹配对象存在显著差异时, 系统推荐结果也随之发生变化, 不再将二者匹配。实验结果表明, 基于同态加密计算获得的匹配评分能够准确反映原始明文数据的实际相似度关系, 验证了该算法在加密域下的逻辑正确性。

(2) 性能评估。在服务器端, 同态匹配计算的开销是主要关注点。系统的测试环境包括: 一台配备 4 核(vCPU) 和 8GiB 内存的阿里云服务器, 以及一部搭载高通骁龙 778G 处理器和 8GB RAM 的华为 nova 11 Pro 终端手机。针

Table 1 Comparison table of plaintext-ciphertext matching results

表 1 明文密文匹配结果对比表

被匹配用户 ID	明文匹配		密文匹配	
	匹配用户 ID	匹配度	匹配用户 ID	匹配度
U00009	U00016	97.07%	U00016	97.06%
	U00002	67.01%	U00002	67.02%
	U00013	65.85%	U00013	65.85%
U00016	U00009	97.07%	U00009	97.06%
	U00002	68.47%	U00002	68.47%
	U00013	61.94%	U00013	61.92%

对 5 个、10 个、15 个、20 个属性特征维度和不同用户规模, 系统测量了匹配计算耗时, 结果如表 2 所示。

Table 2 Matching time consumption under different feature dimensions and user scales

表 2 不同特征维度不同用户规模的匹配耗时

候选用户数量	5 维匹配耗时	10 维匹配耗时	15 维匹配耗时	20 维匹配耗时
10	0.065s	0.139s	0.205s	0.274s
100	0.5s	1.075s	1.594s	2.115s
500	2.53s	5.538s	8.233s	11s
1000	4.8s	10.655s	15.877s	21.877s

由表 2 可知, 随着用户规模和维度的增长, 耗时呈线性增长趋势。这一性能主要受限于 CKKS 同态乘法和轮循处理的开销。然而, 相较于早期全同态加密方案动辄数分钟的计算时间, 如今的 CKKS 方案效率已有质的飞跃。但由于参数选择较为保守且未充分并行优化, 系统的实现仍有很大的提升空间。通过启用多线程并行处理多用户匹配, 以及采用更大的明文批处理技术, 预计可进一步降低系统延迟, 使其达到实时交互的要求。在客户端方面, 加密一个用户特征向量耗时约 50ms, 解密推荐结果耗时约 20ms, 在用户可感知范围内几乎瞬时完成。在密文通信量方面, 每个用户特征密文大小约 1KB, 而推荐结果返回的密文数据量仅为数百字节(B), 对移动网络负担较小。

(3) 安全性分析。系统利用 CKKS 同态加密, 确保了用户敏感数据在传输和服务器存储、计算过程中, 始终保持加密状态。攻击者即使截获通信数据或侵入服务器数据库, 也只能获得无法解读的密文。CKKS 方案基于 RLWE 难题, 具有抗多项式时间攻击的能力。在系统的实现中, 参数选择满足 HES (Homomorphic Encryption Standard) 推荐的 128 位安全强度。同时, 系统采取了多项防护措施以抵御常见的实现层面攻击, 具体包括: 限制同态计算过程中可能出现的明文空间溢出问题, 避免攻击者通过观察解密是否失败来推测明文信息; 服务器仅返回有限的候选结果, 防止恶意用户通过反复查询大量密文结果的方式, 逐步推测出他人的隐私信息。值得注意的是, CKKS 作为一种近似同态加密方案, 其解密结果会包含微小的噪声误差。如表 1 所示, 明文匹配度与密文匹配度的计算结果存在差异, 但误差范围控制在 0.02% 以内。但在实际的匹配应用中, 这并非严重问题, 因为系统主要关注的是匹配对象的排序和整体匹配度, 少量误差不会对匹配决策产生显

著影响。此外,一些最新研究表明,可结合差分隐私等技术增强 CKKS 方案对明文分布信息泄露的抗性。综上,本文系统在当前配置下可以提供令人满意的安全性。

5 结语

本文围绕鸿蒙系统中的基于同态加密的婚介应用,阐述了其设计方案与实现过程。通过引入 CKKS 同态加密算法,系统实现在服务端对加密的用户特征数据直接进行匹配计算,既保证了婚介推荐功能的有效性,又最大程度地保护了用户隐私。设计架构利用了 HarmonyOS 的优势,将应用前端与加密计算后端解耦,有效地组织了功能模块。测试结果表明,在几十至上百人的用户规模下,系统能够在秒级时间内完成匹配计算,具有初步的实用性。当然,本研究仍属于探索性的原型实现,还有进一步优化空间。例如,在更大规模用户集下的性能提升,多用户公钥环境下的匹配机制,以及更丰富特征和偏好指标的引入等。未来工作可考虑引入更高级的密码工具,以实现真正端到端无信任的匹配服务,并针对 HarmonyOS 设备的算力特点进行加速优化。同时,可在真实应用场景中部署试用,收集用户体验反馈,不断完善系统功能和安全机制。

综上所述,本文提出的基于同态加密技术的婚介系统为实现隐私保护的社交应用提供了一种可行方案。随着相关技术的不断发展,其在实际应用中的前景具有重要研究价值与发展潜力。

参考文献:

- [1] WANG W, WANG S, HUANG J. Privacy preservation for friend-recommendation applications[J]. Security and Communication Networks, 2018 (2018): 1265352:1-1265352:11.
- [2] HUANG W H, ZANG H, FENG J Y, et al. A data protection scheme based on multi-authorization center collaboration[J]. Journal of Xi'an University of Posts and Telecommunications, 2023, 28(5): 67-74. 黄文华, 臧浩, 冯景瑜, 等. 一种基于多授权中心协同的数据保护方案[J]. 西安邮电大学学报, 2023, 28(5): 67-74.
- [3] YANG Z N, FAN J L, ZHU J, et al. Industrial internet storage device privacy security[J]. Journal of Xi'an University of Posts and Telecommunications, 2022, 27(1): 35-42. 杨珍娜, 范九伦, 祝剑, 等. 工业互联网存储设备隐私安全[J]. 西安邮电大学学报, 2022, 27(1): 35-42.
- [4] WANG W, WANG S. Privacy preservation for dating applications[J]. Procedia Computer Science, 2018, 129: 263-269.
- [5] GENTRY C. Computing arbitrary functions of encrypted data[J]. Communications of the ACM, 2010, 53(3): 97-105.
- [6] PERIFANIS V, DROSATOS G, STAMATELATOS G, et al. FedPOIRec: privacy preserving federated POI recommendation with social influence[J]. Information Sciences, 2023, 623: 767-790.
- [7] DE SOUZA F D M, DE LASSUS H, CAMMAROTA R. Private detection of relatives in forensic genomics using homomorphic encryption[J]. BMC Medical Genomics, 2024, 17(1): 273.
- [8] SHOKRI R, GOUERT C, TSOUTSOS N G. Helix: genome similarity detection in the encrypted domain[EB/OL]. https://eprint.iacr.org/2024/1088.
- [9] LAGESSE B, NGUYEN G, GOSWAMI U, et al. You had to be there: private video sharing for mobile phones using fully homomorphic encryption[C]//2021 IEEE International Conference on Pervasive Computing and Communications Workshops, 2021: 730-735.
- [10] Homomorphic encryption in iOS 18 | Hacker News[EB/OL]. https://news.ycombinator.com/item?id=42666959.
- [11] DAI Y R, ZHANG J, XIANG B W, et al. Overview on the research status and development route of fully homomorphic encryption technology[J]. Journal of Electronics & Information Technology, 2024, 46(5): 1774-1789. 戴怡然, 张江, 向斌武, 等. 全同态加密技术的研究现状及发展路线综述[J]. 电子与信息学报, 2024, 46(5): 1774-1789.
- [12] BRAKERSKI Z, VAIKUNTANATHAN V. Efficient fully homomorphic encryption from (standard) LWE[C]//2011 IEEE 52nd Annual Symposium on Foundations of Computer Science, 2011: 97-106.
- [13] FAN J, VERCAUTEREN F. Somewhat practical fully homomorphic encryption[EB/OL]. https://eprint.iacr.org/2012/144.
- [14] ZHANG X L, LU Y S. Identity-based fully homomorphic encryption from LWR[J]. Software Guide, 2018, 17(10): 200-203, 208. 张兴兰, 卢玉顺. 利用 LWR 构造基于身份的全同态加密方案[J]. 软件导刊, 2018, 17(10): 200-203, 208.
- [15] CHEON J H, KIM A, KIM M, et al. Homomorphic encryption for arithmetic of approximate numbers[EB/OL]. https://eprint.iacr.org/2016/421.
- [16] BADAWI A A, POLYAKOV Y. Demystifying bootstrapping in fully homomorphic encryption[EB/OL]. https://eprint.iacr.org/2023/149.
- [17] KLUCZNIK K, SCHILD L. FDFB: full domain functional bootstrapping towards practical fully homomorphic encryption[DB/OL]. http://arxiv.org/abs/2109.02731.
- [18] GitHub - microsoft/SEAL: Microsoft SEAL is an easy-to-use and powerful homomorphic encryption library[EB/OL]. https://github.com/microsoft/SEAL?tab=readme-ov-file#readme.
- [19] CHOI H, KIM J, SONG C, et al. Blind-Match: efficient homomorphic encryption-based 1:n matching for privacy-preserving biometric identification[C]//Proceedings of the 33rd ACM International Conference on Information and Knowledge Management, 2024: 4423-4430.
- [20] YUAN H. Research and implementation of intelligent marriage recommendation system[D]. Chengdu: University of Electronic Science and Technology of China, 2024. 袁欢. 智能婚恋推荐系统的研究与实现[D]. 成都: 电子科技大学, 2024.
- [21] YU Z H. The current situation and trend of the application of AI in dating[J]. Software Guide, 2021, 20(3): 90-94. 余忠华. 人工智能应用于婚恋交友的现在与未来[J]. 软件导刊, 2021, 20(3): 90-94.
- [22] LI H L, HUANG Y P. Contextual information and geometric feature fusion for stereo matching with fast attention cost volume[J/OL]. Software Guide, 2025-06-10. https://link.cnki.net/urlid/42.1671.TP.20250428.2224.012. 李瀚灵, 黄影平. 基于上下文信息-几何特征融合及快速注意力代价体的立体匹配方法[J/OL]. 软件导刊, 2025-06-10. https://link.cnki.net/urlid/42.1671.TP.20250428.2224.012.
- [23] HU J F, WANG F Q, CHEN K F. The approximate homomorphic evaluation method of determinant based on CKKS scheme[J]. Journal of Xi'an University of Posts and Telecommunications, 2023, 28(5): 75-85. 胡积发, 王付群, 陈克非. 基于 CKKS 方案的行列式的近似同态计算方法[J]. 西安邮电大学学报, 2023, 28(5): 75-85.
- [24] Ability kit introduction-ability kit (framework service)-application framework[EB/OL]. https://developer.huawei.com/consumer/cn/doc/harmonys-guides/abilitykit-overview. Ability Kit 简-Ability Kit(程序框架服务)-应用框架[EB/OL]. https://developer.huawei.com/consumer/cn/doc/harmonys-guides/abilitykit-overview.
- [25] HarmonyOS development core: deep dive into ability [HarmonyOS topic 08]-Huawei cloud community[EB/OL]. https://bbs.huaweicloud.com/blogs/330071. 鸿蒙开发核心: Ability 详解[鸿蒙专题 08]-华为云社区[EB/OL]. https://bbs.huaweicloud.com/blogs/330071.

(责任编辑:陈维捷)