# 基于同态加密的计算机隐私数据密码验证方法研究

郭 嘉[1] 黄玉帅[1] 吕兴胜[1] 徐迟阳[1] 韩 超[1]
GUO Jia HUANG Yushuai LÜ Xingsheng XU Chiyang HAN Chao

**摘 要** 随着信息技术的飞速发展，计算机隐私数据保护已成为全球关注的核心议题。在密码验证场景中，用户敏感数据面临潜在泄露与破解风险，如何构建安全可靠的验证机制以规避该问题，成为当前亟待解决的关键需求。文章聚焦基于同态加密的计算机隐私数据密码验证方法展开研究：首先阐述同态加密的基本原理与密码验证应用框架，明确密码存储策略与加密实现路径；其次详细梳理加密后验证的具体流程与操作步骤，进一步拓展多重身份认证机制设计及远程验证场景的应用模式；最后针对该方法实际应用中的性能瓶颈，提出针对性的性能优化与效率提升策略。研究旨在为计算机隐私数据的密码验证提供安全可行的技术方案，同时通过优化策略增强方法的实用性，为敏感数据保护领域的技术实践提供参考。

**关键词** 同态加密；隐私数据；密码验证

doi：10.3969/j.issn.1672-9528.2025.10.041

## 0 引言

随着信息技术的飞速发展，计算机系统的安全性和隐私保护问题成为全球范围内关注的焦点，尤其是在云计算、物联网、人工智能等技术的广泛应用下，隐私数据的保护显得尤为重要。随着互联网用户数量的激增和信息交换的日益频繁，个人数据和敏感信息在网络上传输和存储的风险极大增加。传统的密码验证方法，在确保数据安全的同时往往也伴随着隐私泄露的隐患，在数据存储和处理过程中，未加密的数据可能成为攻击者的攻击目标。

## 1 同态加密技术概述

同态加密技术是一种允许在加密数据上执行特定计算操作的加密方法，其核心优势在于能够在不解密数据的情况下对其进行处理，对于提升计算机隐私数据保护能力具有重要意义。传统加密方法如对称加密和非对称加密通常需要对加密数据进行解密后才可处理，这种操作不可避免地暴露了敏感信息，增加了数据泄露和篡改的风险。而同态加密技术通过其独特的数学结构，能够在密文状态下执行算术操作，如加法和乘法，使加密数据的隐私性在处理过程中持续保护。基于同态加密的计算机制具有可扩展性和灵活性，可以广泛应用于诸如云计算、分布式计算、隐私保护数据分析等领域，在计算机隐私数据密码验证中，能够实现无需解密密码即可完成身份验证、数据校验等任务，从而有效防止密码泄露、身份冒充及中间人攻击等安全威胁。具体而言，部分同态加密技术允许对加密数据进行加法操作，某些则支持加法与乘法操作的组合，使得其在不同场景下具有更广泛

1. 三未信安科技股份有限公司 山东济南 250000

[4] 赵征宇，罗景，涂新辉．基于多粒度语义融合的信息检索方法 [J]. 计算机应用，2024, 44(6):1775-1780.
[5] 旷灵，杨思超，刘谋苗．智能检索系统下语义检索的常见策略对比 [J]. 中国科技信息，2024(14):37-39.
[6] 杜鹏举．基于多模态数据语义检索的关键技术研究 [J]. 产业创新研究，2023(12):118-120.
[7] 李易玮，郭婉莹．基于智能化检索系统语义检索文本改写策略 [J]. 中国科技信息，2023(13):60-62.
[8] 滕少华，黄文彪，张巍，等．标签与样本双语义增强的跨模态检索 [J]. 江西师范大学学报：自然科学版，2023, 47(3):296-306.
[9] 周康宾，滕璐瑶，张巍，等．可判别性标签语义指导的域适应检索 [J]. 小型微型计算机系统，2024, 45(7):1639-1647.
[10] 王丽，蒋明，王伟，等．电力信息通信客服机器人特定语义数据检索优化 [J]. 电子设计工程，2024, 32(20):168-171.

【作者简介】
冶伟伟（1991—），男，甘肃陇南人，本科，工程师，研究方向：医院信息化。

（收稿日期：2025-05-14 修回日期：2025-09-29）

的适用性。

## 2 基于同态加密的隐私数据密码验证方法

### 2.1 同态加密在密码验证中的应用框架

在基于同态加密的密码验证方法框架中，用户输入密码后，根据加密算法对密码进行加密处理，生成密文。用户再将加密后的密码传输至认证服务器，而认证服务器无需解密该密文，仅需将加密密码与服务器存储的加密密码进行同态操作，比较两者的加密值是否匹配。根据同态加密技术，认证服务器能够在加密状态下直接执行加密密码与存储密码的比对运算，进而完成密码验证过程，而无需将数据暴露给服务器，从而有效保证用户密码的隐私性和安全性。此方法充分利用了同态加密支持的算术运算特性，允许加密数据在不解密的情况下进行复杂计算，在密码验证中起到了保护用户隐私、防止数据泄露的作用。

此外，该框架中的加密操作通常依赖于一些安全参数，确保加密数据的抗攻击性，包括密钥管理、加密深度以及加密算法的选择。在多用户环境下，基于同态加密的验证框架还支持多重身份认证机制，即通过多个加密步骤对用户身份进行综合验证，进一步增强了系统的安全性和容错性。同时，随着云计算和分布式存储的普及，基于同态加密的密码验证方法还能够在远程验证场景中有效应用，通过跨地域的数据中心进行加密操作，从而确保在云环境中的数据隐私保护与身份认证，如图 1 所示。

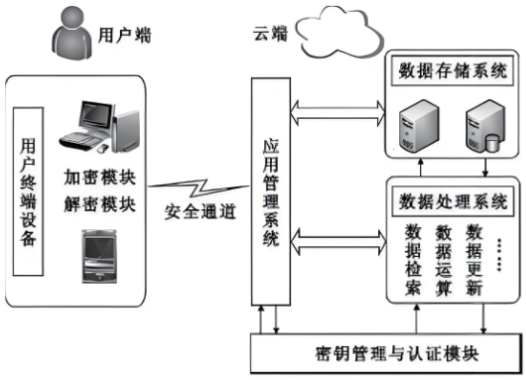


图 1 同态加密在密码验证中的应用图

### 2.2 密码存储与加密方法

在基于同态加密的密码验证方法中，密码存储与加密方法是确保系统安全性和隐私性的核心组成部分。在传统的密码存储方法中，用户密码通常以明文或加密形式保存在服务器端，但这些方法往往存在密码泄露的潜在风险，因此，基于同态加密的密码存储方法通过加密存储机制增强了密码验证过程的安全性和隐私性。

在这一框架下，用户密码在输入后通过高强度的加密算法进行加密，生成密文后即被存储在服务器中，而非以明文或可逆加密的形式存储，这意味着即使攻击者成功获取到存储的密码数据，因数据已加密，攻击者无法轻易获得密码的明文内容。

具体而言，基于同态加密的密码加密方法依赖于同态加密算法的数学特性，通过加密操作将用户密码转化为密文，而这一密文保留了进行验证所需的必要信息，使得即便在加密状态下，认证服务器也能够执行密码比对等操作而无需解密原始密码。在密码存储过程中，密码的加密过程通常结合了加密密钥管理和密文存储策略，以确保密码密文的抗攻击性和数据的完整性。

### 2.3 加密后验证的流程与步骤

加密后验证的流程与步骤是基于同态加密技术进行密码验证的核心环节，确保了在加密数据状态下对用户身份的验证，并保障了用户隐私的安全性。整个验证过程依赖于密文运算的特性，避免了对密码的解密操作，从而有效防止了密码泄露的风险。用户在进行身份验证时，首先由客户端将其输入的密码进行同态加密，生成密码的密文。此密文随后被发送至认证服务器，而无需透露密码的明文。认证服务器接收到加密后的密码后，依托同态加密技术，通过加密运算对比存储在服务器中的密码密文与传输过来的加密密码密文。在这一过程中，服务器无需解密任何数据，而是直接在密文层面进行运算和比对。这一验证步骤的关键在于同态加密支持的加法和乘法等运算特性，能够保证加密数据在计算过程中保持其隐私性，并且仅通过密文计算得出验证结果，而无需暴露原始密码信息。如果加密密码密文与服务器上存储的加密密码密文匹配，则验证成功，用户身份得以确认 [1]。

### 2.4 多重身份认证机制

多重身份认证（multi-factor authentication, MFA）机制不仅依赖传统的单一密码验证，还结合其他认证方法，如生物特征识别、智能卡、硬件令牌等。在同态加密技术的支持下，这些多重认证过程可在加密状态下进行，有效避免了敏感信息的泄露。具体而言，多重身份认证通过加密后的信息与多种身份验证因子的组合，提升了认证过程的安全性和防护能力。在同态加密框架下，首先对用户的主密码进行加密，后使用第二因素认证（如生物识别或时间动态密码），根据这些因素结合加密的方式进行验证，增加了攻击者伪造身份的难度。为实现这一机制，对输入的密码进行加密，生成密文后传输至服务器，服务器在接收到密文后与存储的加密密码进行同态运算，判断是否匹配，而这一过程并不暴露密码的明文。假设用户提交了包括密码、指纹和一次性密码的 3 个认证因子，可以利用以下公式来进行加密后的多重身份验证：

设用户的密码、指纹和一次性密码分别为 $P$、$F$、$T$，加密算法为 $E$，密钥为 $K$，认证因子加密后的结果为 $C_P=E(P, K)$、$C_F=E(F, K)$、$C_T=E(T, K)$，认证服务器接收到加密因子后进行验证：

$$E(P,K)\oplus E(P_{\text{stored}},K)=0 \quad (1)$$

$$E(F,K)\oplus E(F_{\text{stored}},K)=0 \quad (2)$$

$$E(T,K)\oplus E(T_{\text{stored}},K)=0 \quad (3)$$

式中：$P_{\text{stored}}$、$F_{\text{stored}}$ 和 $T_{\text{stored}}$ 分别为存储在服务器端的加密密码、指纹和一次性密码。

此时，若三项因子的同态加密结果均为零，表示输入的认证因子与存储的认证因子一致，身份验证成功 [2]。

2.5 远程验证应用场景

在传统的远程验证方法中，用户信息可能面临中间人攻击和数据泄露的风险，而利用同态加密技术，可以在不解密用户数据的情况下对其进行验证，从而确保数据在传输和存储过程中的安全性。通过对用户输入的密码或其他认证因子进行同态加密，远程服务器可以对加密信息进行验证计算，验证是否匹配，而无需暴露用户的明文密码或其他敏感信息，极大地降低了数据泄露的风险 [3-4]。在多种远程验证方法中，包括基于密码的验证、生物识别认证、一次性密码（OTP）、智能卡认证及多重身份认证等，每种方法在效率、安全性、隐私保护及成本方面具有不同的特点。表 1 展示了多种远程验证方法的加密强度、效率、安全性、数据隐私保护以及成本。每种方法都有其适用场景和优缺点。例如，基于密码的验证方式具有较高的效率和较低的成本，但其安全性和数据隐私保护相对较弱，而多重身份认证提供了极高的安全性和隐私保护，但其成本较高且验证效率较低 [5-6]。

表 1 多种远程验证方法的加密强度、效率、安全性、数据隐私保护以及成本数据

| 验证方法 | 加密级别 | 效率 /ms | 安全评分 (1~10) | 数据隐私保护级别 | 成本 / 元 |
|---|---|---|---|---|---|
| 基于密码的验证 | 中等 | 50 | 7 | 中等 | 5 |
| 生物识别认证 | 高 | 80 | 9 | 高 | 10 |
| 一次性密码 (OTP) | 中等 | 70 | 8 | 中等 | 3 |
| 智能卡认证 | 高 | 90 | 9 | 高 | 15 |
| 多重身份认证 | 非常高 | 120 | 10 | 非常高 | 30 |

2.6 性能优化与效率提升

尽管同态加密技术在确保数据隐私保护方面具有显著优势，但其计算复杂性较高，导致在实际应用中面临较大的性能挑战，因此，为了实现高效的密码验证过程，必须在保证数据安全性的前提下优化加密算法与计算过程。在具体实现中，常见的优化方法包括使用更高效的加密算法、采用简化的密钥管理结构，以及通过算法层面的优化来减少加密和解密操作的次数，具体可以根据公式来描述加密过程中的优化：

$$C_P=E(P,K) \quad (4)$$

式中：$C_p$ 表示加密后的密码；$P$ 表示明文密码；$K$ 表示加密密钥；$E$ 表示加密运算。

在此基础上，为了减少加密操作的复杂度，可以利用分层加密或密钥重用技术来进一步优化。

$$C_P^{'}=E(E(P,K_1),K_2) \quad (5)$$

式中：$C_P^{'}$ 为二次加密后的结果；$K_1$ 和 $K_2$ 分别为两个加密密钥；$E(P, K_1)$ 为对密码进行第一次加密的操作；$E(E(P, K_1), K_2)$ 为第二次加密的过程。

根据这种双重加密的方式，可以提高密码验证的安全性，同时由于密钥重用的特性，减少了计算量。在加密操作中，减少计算量和优化执行效率的另一个策略是通过并行化运算，尤其是在处理多个认证因子的验证时，可以将加密操作分配到多个计算单元，以实现并行计算，从而提高系统的总体效率。此外，根据采用更高效的加密算法，例如采用优化后的 Paillier 加密或 BFV 加密方案，可以在同样保证安全性的前提下减少加密和解密过程的计算开销 [7-8]。

## 3 技术应用测试

本实验的数据集是由作者根据实验设计模拟生成的，数据集的生成过程基于对 5 000 名用户的身份信息进行模拟，包括用户的加密密码、验证因子以及相应的性能指标。在数据使用方面，本数据集完全用于测试目的，没有用于训练任何模型。所有的数据都用于评估系统的功能与性能表现，具体而言，实验中包含 5 000 条数据，每条数据代表一个用户的认证过程及其对应的加密和验证信息。

在本实验中，数据集共进行了 5 轮测试，且测试数据没有进行分组。每轮测试的目的是全面评估基于同态加密的密码验证方法的性能，包括加密时间、解密时间、系统响应时间、安全性评分等关键指标。由于实验的主要目标是对整体系统性能进行测试，因此所有数据都统一纳入同一测试环境中，没有进行不同组别的区分。

测试指标包括：

加密时间（ms）：表示每个认证因子加密过程所需的时间，衡量加密算法的效率。

解密时间（ms）：表示验证过程中解密操作所需的时间，反映解密算法的执行速度。

安全性评分（1~10）：根据密码验证过程中的安全性考虑因素（如抗攻击能力、加密强度等），评定系统的安全性，评分越高表示系统的安全性越强。

数据隐私保护级别：衡量系统对用户数据隐私保护的能力，评分较高表示隐私保护措施更为完善。

验证成功率（%）：表示系统成功验证用户身份的比例，成功率越高说明系统的验证功能越稳定。

系统响应时间（ms）：表示完成一次身份验证所需的总时间，系统响应时间越短，说明验证过程越高效。

成本（USD）：表示系统运行和维护的费用，反映系统的经济效益。测试数据如表 2 所示。

表 2 测试数据

| 用户编号 | 加密时间/ms | 解密时间/ms | 安全性评分（1~10） | 数据隐私保护级别 | 验证成功率/% | 系统响应时间/ms | 成本（USD） |
|---|---|---|---|---|---|---|---|
| 1 | 45.27 | 48.36 | 8 | 高 | 99.83 | 102.67 | 9.35 |
| 2 | 39.58 | 42.19 | 9 | 高 | 99.92 | 94.18 | 8.26 |
| 3 | 41.91 | 44.23 | 8 | 高 | 99.65 | 98.92 | 10.11 |
| 4 | 47.63 | 50.47 | 7 | 中 | 99.85 | 106.41 | 7.49 |
| 5 | 43.25 | 46.02 | 8 | 高 | 99.91 | 100.88 | 8.94 |

从表 2 数据可以看出，随着系统的加密和解密时间的优化，系统的响应时间有所提高，尤其是在加密和解密时间较短的情况下，验证过程更为高效。安全性评分方面，较高的评分显示了优化后的同态加密算法在防止数据泄露和破解攻击方面的强大能力。数据隐私保护级别较高的用户，通常也表现出更高的安全性评分，表明更强的加密措施能更好地保护用户数据的隐私。验证成功率普遍较高，进一步证明了同态加密在实际应用中的可靠性。此外，系统响应时间较短，特别是在加密时间和解密时间优化后，系统整体的性能得到了有效提升。对于成本部分，尽管高效的加密和高安全性会导致系统成本上升，但其带来的性能和安全性提升对于长期运营是有益的。综上所述，实验结果表明，根据优化同态加密算法，可以在提高安全性的同时，显著提升系统的验证效率，为基于同态加密的密码验证方法的广泛应用提供了有力支持[9-10]。

## 4 结语

基于同态加密的计算机隐私数据密码验证方法在提升信息安全和保护用户隐私方面具有重要意义。根据同态加密技术，能够在加密数据上直接进行验证运算，避免了传统方法在数据存储和传输过程中的安全漏洞。本文深入分析了同态加密在密码验证中的应用框架及其优化策略，为计算机系统提供了更高效、更安全的解决方案。随着同态加密技术的不断发展，未来其在云计算、物联网等领域的应用前景将更加广阔，成为实现全面信息安全保护的关键技术之一。

**参考文献：**

[1] 张钧 , 沈轩 . 多级访问下多源医疗信息全同态加密仿真 [J]. 计算机仿真 , 2024, 41(12):321-325.

[2] 李秋贤 , 周全兴 . 基于全同态加密的联邦学习隐私保护技术研究 [J]. 现代信息科技 , 2024, 8(23): 170-174.

[3] 王明龙 . 基于多属性同态加密的医院电子档案信息安全防护算法 [J]. 电脑知识与技术 , 2024, 20(34):80-82.

[4] 汤殿华 , 曹云飞 , 黄云帆 , 等 . 基于 CKKS 同态加密的纵向联邦逻辑回归训练方案 [J]. 通信技术 , 2024, 57(11):1173-1180.

[5] 孙劲桐 , 周福才 , 王强 , 等 . 基于非交互零知识证明的可验证全同态加密算法 [J]. 东北大学学报 ( 自然科学版 ), 2024, 45(11): 1537-1546.

[6] 韩喆 , 陶晓英 , 徐文涛 . 同态加密与区块链技术助力破解跨境数据监管难题 [J]. 上海信息化 , 2024(11): 14-17.

[7] 隋彤彤 , 王继志 , 刘雯 . 基于同态加密的云控制系统研究综述 [J]. 软件导刊 , 2024, 23(11): 25-31.

[8] 李怀堂 , 马鹏 , 崔娟 , 等 . 基于同态加密的数据库信息安全应用研究 [J]. 科技创新与应用 , 2024, 14(30):80-82.

[9] 盛冶 , 涂广升 . 一种高效的 CCA1 安全的全同态加密方案 [J]. 网络安全技术与应用 , 2024(10): 24-28.

[10] 管桂林 , 支婷 , 陶政坪 , 等 . 物联网中多密钥同态加密的联邦学习隐私保护方法 [J]. 信息安全研究 , 2024, 10(10): 958-966.

**【作者简介】**

郭嘉（1996—），男，山东济南人，硕士，网络工程师，研究方向：数据安全、信息安全、商用密码。

（收稿日期：2025-04-16 修回日期：2025-10-10）