基于国密SM2支持动态口令恢复的多因素认证方案

汪 定[1),2),3)] 朱留富[1),2),3)]

[1)](南开大学密码与网络空间安全学院 天津 300350)

[2)](数据与智能系统安全教育部重点实验室(南开大学) 天津 300350)

[3)](天津市网络与数据安全技术重点实验室(南开大学) 天津 300350)

摘 要 多因素认证使用两种及以上认证因素(如口令、智能卡或生物特征等)来验证用户身份,有效缓解了单一认证因素被攻破所带来的安全风险,增强了身份认证系统的安全性和可靠性,被普遍应用于金融交易、电子政务和军事国防等关键领域。当前广泛采用的多因素认证方案主要依赖国外密码算法标准构建,一旦这些国外算法存在潜在缺陷或安全隐患,可能对个人、企业甚至国家信息安全构成重大风险,未能顺应国家在网络安全领域实现技术自主可控的战略要求。此外,现有基于口令的多因素认证方案没有考虑口令恢复机制,即当用户遗忘和丢失口令时,方案无法协助用户找回口令。然而,为增强身份认证的安全性,越来越多的系统要求用户设置复杂口令,如包含大小写字母、数字、特殊字符等,增加了用户的记忆负担。尽管现有多因素认证方案提供口令更新功能,但通常要求用户首先提交原始口令,同样无法避免口令遗忘和丢失时的恢复问题。因此,当遗忘和丢失口令时,用户极有可能无法找回口令从而永久丢失该账户。为解决上述问题,本文基于国密SM2算法、密保问题以及秘密共享技术,提出一种支持动态口令恢复的多因素认证方案,为构造国密算法框架下的多因素认证方案提供了可行路径,并进一步解决了口令遗忘和丢失问题。本文构造的基于国密SM2的签密算法,可同时保证认证凭证和通信数据的机密性和完整性,有效降低执行数据加密和签名操作的计算开销和通信开销,适用于轻量级应用场景;使用秘密共享技术,将口令恢复凭证与用户密保问题进行绑定,并利用智能卡存储口令恢复凭证。当遗忘和丢失口令时,用户需要提供有效的智能卡,通过回答密保问题从口令恢复凭证获得秘密值份额,重构该秘密值并利用国密SM4解密算法恢复原始口令;此外,用户可以在本地更新密保问题,SM4加解密密钥和口令恢复凭证,避免隐私信息泄露,从而实现动态口令恢复功能。本文方案使用模糊验证和诱饵口令技术计算用户认证凭证,降低口令猜测攻击威胁并提供错误口令实时监测功能。在随机预言机模型下,本文提供了形式化安全性证明。性能对比结果表明,本文方案在提供安全可靠身份认证的同时具备可行性。

关键词 多因素认证;SM2;动态口令恢复;随机预言机模型;非形式化分析

中图法分类号 TP391 **DOI号** 10.11897/SP.J.1016.2025.02241

Multi-Factor Authentication on SM2 with Dynamic Password Recovery

WANG Ding[1),2),3)] ZHU Liu-Fu[1),2),3)]

[1)](College of Cryptology and Ciber Science, Nankai University, Tianjin 300350)

[2)](Tianjin Key Laboratory of Network and Data Security, Nankai University, Tianjin 300350)

[3)](Key Laboratory of Data and Intelligent System Security, Nankai University, Tianjin 300350)

Abstract Multi-factor authentication (MFA) employs two or more distinct authentication factors (e.g., passwords, smart cards, or biometrics) to verify user identity, thereby mitigating security risks caused by the compromise of a single factor. It enhances the security and reliability of authentication systems and has been widely adopted in critical fields such as e-commerce, e-government, and military defense. However, most existing MFA schemes rely on foreign cryptographic algorithm standards. If these cryptographic algorithms contain design flaws or vulnera-

收稿日期:2025-01-06;在线发布日期:2025-05-23。本课题得到国家自然科学基金(62222208)、京津冀基础研究合作专项(21JCZXJC00100)资助。**汪 定**,博士,教授,中国计算机学会(CCF)高级会员,主要研究领域为密钥安全、身份认证。E-mail:wangding@nankai.edu.cn。**朱留富**,博士研究生,主要研究领域为密码安全协议。

bilities, they could pose significant security threats to individuals, enterprises, and even national security, conflicting with the strategic goal of achieving independent and controllable core cybersecurity technologies. Additionally, current password-based MFA schemes often fail to take password recovery mechanisms into account. When users forget or lose their passwords, these schemes fail to help users find their passwords. In addition, to strengthen security, many systems enforce complex password policies (e.g., requiring uppercase/lowercase letters, numbers, and special characters), increasing users′ memory burdenat at the same time. Although such schemes typically allow password modification, they still require users to submit the original password for performing authentication during login and authentication, relying on it for updating passwords. Consequently, if users lose their original passwords, the system cannot work normally, potentially leading to permanent account loss. To address these issues, this paper proposes an MFA scheme supporting dynamic password recovery, based on the domestic SM2 cryptographic algorithm, user private questions, and secret sharing techniques. Specifically, a signcryption algorithm is constructed based on the SM2 algorithm, ensuring both confidentiality and integrity of authentication credentials and communication data while reducing computational and communication overhead, making it suitable for lightweight applications. The password recovery credential is bound to user privacy questions via secret sharing, with the credential stored in a smart card. If the password is lost, users are required to present a valid smart card and answer private questions correctly to retrieve secret shares. The original password is then recovered using the SM4 decryption algorithm via the secret key. Particularly, in the proposed scheme, users can update private questions, secret keys, and recovery credentials by themselves, preventing privacy leakage and enabling dynamic password recovery. Authentication credentials are generated using fuzzy verification and honeyword techniques to resist password-guessing attacks and provide real-time monitoring. The proposed scheme is formally proven secure in the random oracle model, with informal analysis further showing its robustness. Security analysis demonstrates resistance against password-guessing attacks, smart card stolen attacks, device capture attacks, man-in-the-middle attacks, and impersonation attacks, while offering forward secrecy, anonymity, and dynamic password recovery. Performance comparisons demonstrate that the proposed scheme balances robust security with operational efficiency, ensuring its viability for real-world deployment. Through rigorous comparison with existing multi-factor authentication (MFA) schemes, the proposed scheme exhibits lower computational overhead while maintaining strong resistance against common attacks, such as password-guessing attacks and message replay attacks. Additionally, the use of secret sharing and fuzzy verification techniques minimizes latency during authentication, making it suitable for resource-constrained environments, including IoT devices and mobile applications. The scheme's dynamic password recovery method further enhances usability, reducing the risk of permanent account loss while preserving security. Comparative analyses highlight its advantages over traditional MFA schemes, particularly regarding scalability and adaptability to ensure desirable properties. These results show that the proposed scheme is not only theoretically sound but also practically feasible for implementation across industries such as e-commerce and government services, where both security and performance are critical.

Keywords multi-factor authentication; SM2; dynamic password recovery; random oracle model; informal analysis

1 引　言

随着计算科学、移动通信及无线传感器网络等关键技术的突破性进展,移动互联网、物联网以及车联网等新兴技术已在电子商务、政务信息化、工业自动化及国防安全等关键领域实现广泛应用。然而,新兴技术的快速普及也引发了诸多安全隐患,包括但不限于身份伪造、网络钓鱼以及敏感数据泄露等安全风险。因此,如何确保信息系统安全、避免数据非法访问是亟待解决的关键问题[1]。身份认证是信息系统安全防护体系的第一道防线,能避免系统遭受非授权访问。在身份认证中,系统主要依据以下三类因素实现身份认证:已知信息(如口令)、生物特征(如指纹)和物理凭证(如智能卡)。多因素认证方案[2-4]通过组合两种或以上独立认证要素进行身份验证,即使部分(非全部)认证凭据遭到泄露,仍可有效保障系统的安全性与可靠性。

在多因素认证方案中,系统通常包含三类实体:用户(User, UE)、认证网关(Authentication Gateway, AG)以及服务器(Server, SN)。实体之间的交互过程如图 1 所示。首先,UE 向 AG 发送注册请求;当收到该请求后,AG 生成注册响应并发送给 UE;当 UE 尝试与 SN 建立会话密钥时,UE 向 AG 发送登录认证请求;当成功验证 UE 身份后,AG 向 SN 发送认证请求;此时,若接受该认证请求,SN 向 UE 发送认证响应;最后,UE 和 SN 共同建立会话密钥 SK。

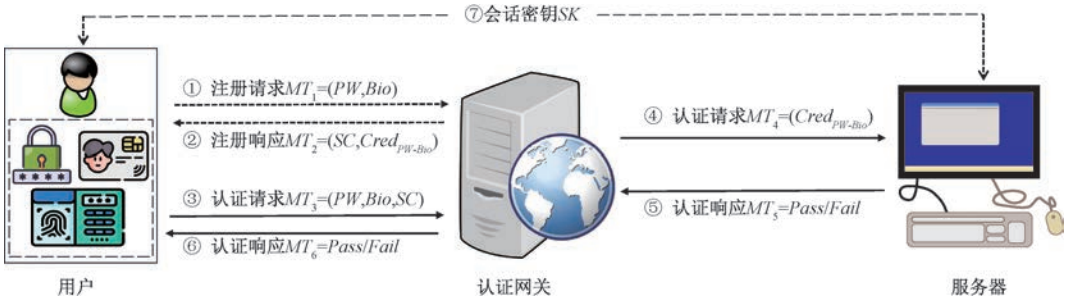

图 1　多因素认证框架。用户 UE、认证网关 AG 和服务器 SN 执行相互认证,并安全地建立会话密钥 SK

口令作为基于用户所知的认证因素,其优势是易于部署和更改[5],因此被广泛用于设计身份认证方案[6-9]。然而,这些方案都假设口令不会被遗忘和丢失,要求用户在登录认证阶段和口令更新阶段提供原始口令。由于记忆能力的限制,用户无法准确记忆熵值较高的口令[10]。据 NordPass 研究报告统计[11],2024 年全球人均拥有的口令数量为 100 个。因此,用户极有可能遗忘和丢失在不同系统上设置的口令。口令恢复机制能够帮助用户通过安全验证重新获取账户访问权限,提升身份认证系统的容错性和可靠性。因此,在多因素认证中部署口令恢复机制具有重要的现实意义。但通过与服务器交互实现口令恢复可能会泄露用户秘密信息,如验证码或密保问题。一旦这些信息被泄露,攻击者可能恶意地恢复口令并进一步实施身份仿冒攻击等。此外,大多数已知口令恢复方法(如文献[12-16])无法更新隐私信息,无法降低因隐私信息泄露而导致的安全威胁。

在多因素认证方案中,实现口令恢复是在缺少主认证因素时如何对用户进行辅助认证。一方面,较之口令,用于辅助认证的因素不仅需要更容易被记忆和提取,而且其安全性也不应低于口令[17]。另一方面,使用辅助因素设计口令恢复方法需要建立完备的敌手模型,并考虑密保问题猜测攻击和邮件/短信欺骗等攻击,进一步增强安全模型并分析多因素认证方案的整体安全性。因此,如何在多因素认证方案中实现动态口令恢复充满挑战。

当前,主流的多因素认证方案主要依赖国外密码算法标准构建,难以满足我国对网络安全核心技术自主创新的战略需求。面对日益复杂的国际环境,保障网络空间安全自主权、突破关键技术的对外依赖已成为亟待攻克的重要课题。中国自主研发的 SM2 椭圆曲线公钥密码算法[18]于 2010 年被正式采纳为商用密码行业标准(GM/T 0003－2012),并于 2016 年成为国家密码标准(GB/T 32918－2016)。在国密 SM2 算法框架下构造多因素认证方案符合核心技术自主可控的发展战略,但直接部署国密 SM2 算法可能导致昂贵的计算和通信开销,降低运行效率,不适用于轻量级环境。因此,如何基于国密 SM2 算法构造安全且实用的多因素认证方案值得进一步研究。

综上所述,基于国密 SM2 算法构造支持动态

口令恢复的多因素认证方案值得进一步研究。

2 相关工作

2008 年,Juang 等人[19]设计一种结合智能卡和口令的多因素认证协议,该协议支持密钥交换功能,但在安全性方面存在缺陷,无法抵御在线口令猜测攻击和智能卡泄露攻击。针对这一局限性,Sun 等人[20]随后提出了一种改进的多因素认证方案,改进的方案可以抵抗智能卡泄露攻击,并降低了口令猜测威胁。Qin 等人[21]进一步增强方案安全性,提出了一种具有可验证门限功能的多因素认证协议,该协议要求不少于门限个认证网关协作才能为用户生成合法的认证凭证并在随机预言机模型下完成了形式化安全证明。为提高认证方案的运行效率,Yang 等人[22]基于轻量级的密码算法提出一种高效身份认证方案,支持生物密钥的动态更新避免隐私信息泄露。

上述方案在注册阶段需要公开传输真实身份标识,无法提供完美匿名性。为解决该问题,Kumar 等人[23]利用云存储技术提出一种面向物联网设备的多因素认证与密钥协商方案,但无法提供前向安全性。为实现前向安全性,Braeken[24]基于椭圆曲线密码算法提出一种后量子安全的多因素认证方案并支持前向安全性,但该方案无法抵抗侧信道攻击。为避免上述威胁,Wang 等人[25]设计了一种结合物理不可克隆函数(Physical unclonable function, PUF)的多因素身份认证协议。该协议在安全性方面实现了以下特性:有效防御节点捕获攻击与在线/离线口令猜测攻击;保障用户身份匿名性;具备前向安全特性。

生物特征是个体唯一拥有的生物信息,可以被测量、识别和验证。2010 年,Li 等人[26]结合生物特征以及智能卡设计一种多因素认证协议,该方案在随机预言机模型下是可证明安全的。Dhillon 等人[27]通过安全性分析表明,Li 等人[26]所提方案存在功能性缺陷,无法提供认证因素更新。Dhillon 等人[27]提出一种具有更新功能的多因素认证方案。该方案可以抵抗主动和被动攻击,但无法避免生物特征信息泄露。为解决该问题,Feng 等人[28]提出一种具有用户隐私保护的多因素认证方案。该方案隐藏用户生物特征信息和身份标识,但计算开销较大,无法应用于轻量级设备。为降低计算开销,Li 等人[29]设计了一种计算高效的多因素认证协议。该协议通过采用轻量级密码学原语(主要包括哈希函数和异或运算等基础操作),提升了系统的运行效率,但无法避免生物特征提取时的噪声污染。针对这一安全缺陷,Wang 等人[30]创新性地提出了一种基于数字签名的匿名生物特征认证机制,使用汉明距离度量生物特征并实现条件隐私保护,但该方案无法提供恶意用户检测功能;为解决该问题,Yang 等人[31]提出一种基于个人信用的认证方案,使用布隆过滤器设计重用检测机制从而识别恶意用户,但该方案无法提供前向安全性。为解决该问题,Le 等人[32]提出一种基于设备的多因素认证方案,通过凭证更新和设备撤销实现认证因素更新和设备退出;然而,上述方案没有考虑量子计算攻击,从而无法提供后量子安全性。为解决该问题,Bahache 等人[33]和 Taj 等人[34]分别提出具有后量子安全的身份认证与密钥协商协议,并在随机预言机模型下证明了协议的安全性。

由于缺乏科学、系统的评价指标体系,多因素认证研究往往陷入“攻防对抗”的被动局面,即安全方案被攻破后被改进,继而再次面临新的攻击,形成一种迭代循环。图 2 给出经典多因素认证方案研究的内在关联。其中,父节点代表被攻击或存在缺陷的多因素认证方案,子节点代表改进的多因素认证方案。例如,2013 年,Xue 等人[35]设计了一种基于数字证书的多因素认证协议,但该方案无法抵御口令猜测攻击,同时无法提供用户匿名性。为避免上述安全威胁,Wang 等人[36]提出一个改进的多因素方案,并声称可以抵抗离线口令攻击和服务器仿冒攻击,但该方案无法部署在轻量级设备中。为提升方案运行效率,Kumar 等人[37]提出一种用于车联网的身份认证协议;然而,Kumar 等人方案[37]无法提供错误口令检测,无法避免离线口令猜测攻击且不提供用户匿名性;因此,Khan 等人[38]提出一种用于智能电网设备且具有用户匿名性的身份认证协议。

2009 年,Das 等人[39]首次提出了一种面向无线传感器网络的多因素认证协议,该协议整合了密钥协商机制。然而,Li 等人[40]通过安全性分析证实,该协议存在安全缺陷:即无法实现用户与认证网关的相互认证;Li 等人[40]进一步提出一种多因素认证协议,该方案利用临时凭证实现实体之间的相互身份认证;Chang 等人[41]通过安全性分析发现,Li 等人[40]提出的认证协议缺乏完美前向安全性且无法实现后向安全。针对这些问题,

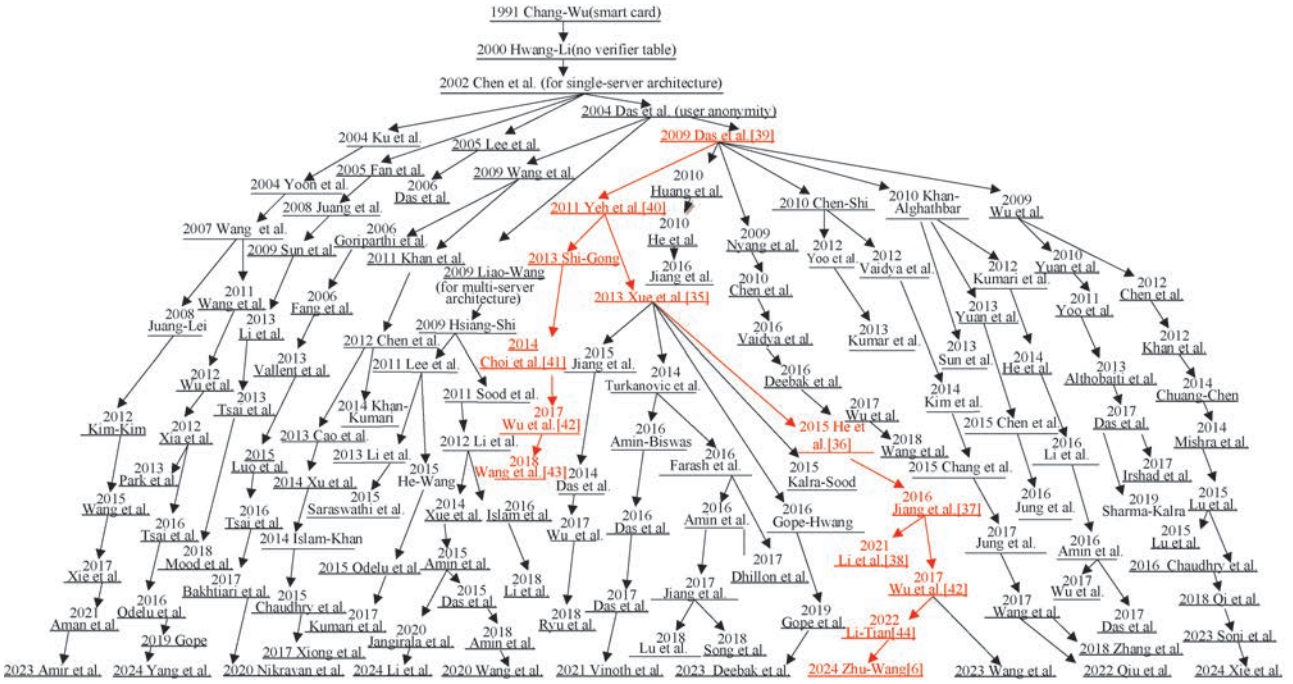

图 2　多因素认证方案研究进展关系(父节点表示的方案被子节点论文指出存在安全缺陷。标红子树涉及的方案在文中作为分析案例,用于说明多因素认证方案在不断地被“攻破→改进→攻破→改进”。)

Chang 等人[41]设计了一种基于椭圆曲线密码机制且具有后向安全的多因素认证协议。然而,上述协议需要使用复杂的密码学操作,造成高昂的计算开销。为此,Wazid 等人[42]进一步提出一种适用于物联网环境的轻量级匿名身份认证协议,在具体协议中仅使用哈希和异或操作,降低了身份认证阶段的计算开销,并提供了严格的形式化安全证明,但该方案无法完全抵抗仿冒攻击;为解决该问题,Shen 等人[43]利用区块链技术提出一种用于车联网的轻量级身份认证协议,并证明该协议可以有效抵抗仿冒攻击,但该协议无法提供多节点与认证网关的快速认证。为解决该问题,Li 等人[44]提出一种支持多节点的快速身份认证协议,该协议可以并行处理不同实体的身份认证请求,但该协议没有考虑多因素安全。为提供多因素安全,Zhu-Wang[6]基于公钥加密算法提出一种具有动态口令恢复的多因素认证方案。

由于易部署和更改的特性,口令被广泛用于构造多因素认证方案[45-46]。然而,目前构造多因素认证方案没有考虑口令恢复机制,一旦遗忘和丢失口令,用户将可能永久丢失该账户。为解决上述问题,Ellison 等人[47]基于对称加密算法构造口令恢复方案。该方案在本地生成口令密文,用户可以使用门限个密保问题的答案重构解密密钥,但没有提供形式化的安全性证明。为解决该问题,Frykholm 和 Juels[48]提出一种可证明安全的口令恢复方案。该方案将密保问题形式化为一组低熵秘密,用户可以利用这些秘密的子集进行口令恢复。然而,该方案要求用户存储与秘密相关的所有子集,该方案存在存储开销过大的问题。

为优化存储资源利用率,Chmielewski 等人[49]设计了一种基于 C/S(客户端-服务器)架构的口令恢复机制。该方案要求用户在服务器端存储口令密文并通过与服务器交互获得解密密钥。然而,该方案无法解决单点故障问题。为解决该问题,Little 等人[16]提出一种基于多服务器的账户恢复方法,用户将恢复凭证存储在两个物理隔离的服务器中,降低了单个服务器被攻破导致的安全威胁。

随着国际形势日益严峻,网络空间安全关系到国家和民族发展的核心利益。国产密码技术对于保障国家网络空间安全、促进技术自主创新以及维护国家主权和经济独立具有至关重要的作用。国密 SM2 算法是自主研发设计的密码算法标准,于 2016 年被列为标准 GB/T 32918.1-2016。此后,众多学者围绕国密 SM2 算法展开深入研究,丰富和扩展了国密 SM2 算法的应用场景。例如,韩庆迪等人[50]提出一种基于 SOTP 加密保护签名私钥的国密 SM2 签名方案,使用 SOTP 技术加密签名密钥

从而避免密钥泄露。为提高签名算法和验证算法的效率,韦薇等人[51]利用单指令多数据集的特性,提出一种基于单指令多数据集的国密 SM2 数字签名算法,该算法适用于轻量级设备。张可臻等人[52]基于国密 SM2 算法设计了两方门限盲协同计算方案,该方案通过盲签名技术隐藏通信双方的身份。

国密 SM2 算法需要群元素乘法运算等计算复杂度较高的密码学操作。为优化算法性能,王明登[53]等人提出一种基于 RISC-V 扩展的国密 SM2、SM3 和 SM4 算法高效实现方式;吴雯等人[54]提出一种利用国产硬件 GPU 的国密 SM2 算法实现方法;乔晗等人[55]提出了一种面向 GmSSL 密码库的国密 SM2 算法快速优化实现方法,降低了部署国密 SM2 算法时的计算开销和通信代价。

2.1 动 机

鉴于其部署便捷和修改灵活的特点,基于口令的认证机制在身份验证系统中得到普遍应用。然而,相关研究[56-57]揭露用户设定的口令通常呈现 Zipf 分布特征,这种规律性使得系统容易遭受基于统计分析的口令猜测攻击。针对该安全风险,当前系统规定用户口令必须包含多字符类别组合(如字母、数字、符号),以提高破解难度。但由于记忆能力受限,用户通常只能正确记忆 5～7 个不同的口令。因此,用户极有可能遗忘和丢失在不同系统上设置的口令。然而,现有的多因素认证方案[58-59]假设用户不会遗忘和丢失口令,要求用户在登录认证阶段提供原始口令进行身份认证。此外,这些方案现需要用户提供原始口令以提供口令更新服务。因此,一旦发生口令遗忘和丢失事件,系统将无法提供正常服务。

针对用户口令遗忘与丢失的问题,众多学者陆续提出了多种口令恢复机制。然而,现有口令恢复方法无法直接部署于多因素认证方案。一方面,现有口令恢复方法(如文献[49])需要用户与服务器交互,并将口令恢复凭证存储在服务器中。然而,这些凭证中可能包含一些隐私信息,如密保问题、生物特征和邮件地址等。另一方面,现有口令恢复方法(如文献[47,48])无法更新隐私信息,如密保问题、密钥以及口令恢复凭证等。此外,现有口令恢复方法没有考虑密保问题猜测攻击、邮件/短信欺骗攻击等敌手模型,方案依赖强安全性假设而无法衡量安全性。

在多因素认证方案中,实现口令恢复是在缺少主认证因素时对用户进行辅助认证。较之口令,辅助认证因素应当更容易被记忆,并且其安全性不应弱于口令能提供的安全性[17]。现有口令恢复方法主要有基于密保问题的口令恢复以及基于短信/邮件验证码的口令恢复。然而,已有方法[47-50]没有考虑现实敌手及其攻击能力,如密保问题猜测攻击和邮件/短信欺骗攻击,无法衡量现实安全性。因此,在多因素方案中实现安全的动态口令恢复具有重要的研究价值。

当前,主流多因素认证方案在密码算法设计上仍高度依赖国际标准,难以满足我国网络空间安全领域对核心技术自主可控与安全可靠的战略需求。一旦国外密码算法存在后门或未公开的缺陷,攻击者可以恶意监控或解密机密数据。因此,使用国产密码算法对保障国家网络空间安全、促进技术自主创新以及维护国家主权具有至关重要的作用。国密 SM2 算法是我国自主研发设计的密码算法标准,包括数字签名算法、密钥交换算法以及公钥加密算法,并于 2016 年正式成为国家密码标准 GB/T 32918.1—2016。基于国密 SM2 算法构造多因素认证方案可以解决多因素认证方案国产化问题,但直接部署 SM2 算法可能导致昂贵的通信和计算开销。因此,构建基于国密 SM2 密码体系的高效多因素认证方案仍面临诸多技术挑战,有待进一步研究。

综上所述,基于国密 SM2 算法构造具有动态口令恢复的多因素认证方案是亟待解决的关键问题。

2.2 本文贡献

本文在国密 SM2 加密和数字签名算法框架下,提出一种具有动态口令恢复的多因素认证方案,解决了基于国密算法框架构造多因素认证方案以及口令遗忘和丢失等现实挑战。本文核心贡献如下:

(1) 本文基于国密 SM2 提出一种支持动态口令恢复的多因素认证方案 (Multi-factor authentication on SM2 with dynamic password recovery),符合网络空间安全领域核心技术安全可控的战略要求;

(2) 本文使用秘密共享技术,将密保问题与口令恢复凭证绑定,提出一种动态口令恢复方法。该方法允许用户在本地恢复口令并更新密保问题、秘密值以及口令恢复凭证;基于密保问题猜测攻击构建敌手模型和安全模型,并形式化分析了方法的安全性;利用模糊验证和诱饵口令技术计算用户认证凭证,从而隐藏口令的分布并进一步提供错误口令检测;支持用户直接在本地更新口令;设计国密 SM2 签密算法,同时保证数据机密性和完整性,降低了计算和通信开销;

(3) 在随机预言机模型下,本文形式化证明了方案的安全性,并通过非形式化分析证明方案可以抵抗已知攻击;实验对比分析显示,相较于现有方案,本研究在确保安全性的同时提升了方案的实用性和可部署性,可被应用于轻量级场景。

2.3　本文框架

本文第 2 节介绍预备知识;在第 3 节提出基于国密 SM2 算法支持动态口令恢复的多因素认证方案;在第 4 节给出形式化安全证明和启发式分析;在第 5 节给出性能对比分析;在第 6 节对本文进行总结。本文使用的符号如表 1 所示,相关符号与国密 SM2 算法一致。

3　预备知识

本节介绍国密 SM2 签名/加密算法、秘密共享技术、Honeyword(诱饵口令)、现实攻击者模型和方案的评价指标。

3.1　国密 SM2 签名算法

该算法包含下面四个阶段。

(1)设置. 将参数 λ 设置为公共安全参数,令 F_q 为有限域,系统选取 F_q 上的椭圆曲线 $E:y^2=x^3+ax+b \bmod q$。其中,大素数 q 是有限域 F_q 的元素个数且 $a,b\in[0,q-1]$;随机选取 E 上的 n 阶基点 $G=(x_G,y_G)$,一个密码学哈希函数 $H:\{0,1\}^* \to \{0,1\}^*$,其中 n 为大素数且为 $\sharp E(F_q)$ 的素因子,$\sharp E(F_q)$ 表示域 F_q 上椭圆曲线 E 的所有有理点的数目。令公开参数 $params=\{G,n,H\}$。

(2)密钥生成. 随机选取 $d\in[0,q-1]$,计算 $[d]G=(x_d,y_d)$;输出 $(PK,SK)=((x_d,y_d),d)$。

(3)签名. 输入消息 M,签名者私钥 SK,令 $M^*=Z_S\|M$,其中 Z_S 是由签名者标识和椭圆曲线部分参数组成的随机字符串。签名者随机选取 $k\in[0,n-1]$,计算 $e=H(M^*)$,$(x_1,y_1)=[k]G$,$r=(e+x_1)\bmod n$,$s=((1+d)^{-1}(k-rd))\bmod n$。此时,若 $r=0$ 或 $r+k=n$ 或 $s=0$,重新选取 k 并计算。否则,输出 $(M,(r,s))$。

(4)验证. 输入 $(M',(r',s'))$ 和 PK。验证者首先判断 $r',s'\in[0,n-1]$ 是否成立。若不成立,验证者拒绝该签名;否则,令 $M^*=Z_S\|M'$,计算 $e'=H(M^*)$,$t=(r'+s')\bmod n$。若 $t=0$,验证者拒绝该签名。否则,计算 $(x'_1+x'_2)=[s']G+[t]P$,$R=(e'+x'_1)\bmod n$。若 $R=r$,接受该签名。

3.2　国密 SM2 加密算法

该算法包含下面四个阶段。

(1)设置. 令 λ 为系统安全参数,选取有限域 F_q 和定义在 F_q 上的椭圆曲线 $E:y^2=x^3+ax+b \bmod q$。其中,大素数 q 是有限域 F_q 的元素个数且 $a,b\in[0,q-1]$;随机选取 E 上的 n 阶基点 $G=(x_G,y_G)$,一个密码学哈希函数 $H:\{0,1\}^* \to [0,q-1]$ 和一个密钥派生函数 $KDF:\{0,1\}^* \to \{0,1\}^{klen}$。其中,$klen$ 表示密钥长度,n 为大素数且为 $\sharp E(F_q)$ 的素因子,$\sharp E(F_q)$ 表示域 F_q 上椭圆曲线 E 的所有有理点的数目。令公开参数 $params=\{G,n,H,KDF\}$。

(2)密钥生成. 随机选取 $d\in[0,q-1]$,计算 $[d]G=(x_d,y_d)$;输出 $(PK,SK)=((x_d,y_d),d)$。

(3)加密. 输入消息 M,解密者公钥 PK,加密者随机选取 $k\in[0,n-1]$,计算 $C_1=[k]G=(x_1,y_1)$,$[k]PK=(x_2,y_2)$,$t=KDF(x_2\|y_2,klen)$。若 t 为全 0 比特串,则重新选取 k 并执行上述步骤。否则,计算 $C_2=M\oplus t$,$C_3=H(x_2\|M\|y_2)$。输出密文 $C=\{C_1,C_2,C_3\}$。

(4)解密. 输入密文 $C=\{C_1,C_2,C_3\}$,解密者私钥 d,解密者从 C 提取 C_1。若 C_1 不满足椭圆曲线方程,则解密失败;否则,计算 $(x'_2,y'_2)=[d]G$,$t=KDF(x'_2\|y'_2,klen)$,$M=C_2\oplus t$,$u=H(x'_2\|M\|y'_2)$。此时,若 $u\neq C_3$,则解密失败;否则成功解密并获得 M。

3.3　Shamir 秘密共享算法

令 F_q 表示由大素数 q 生成的一个有限域,分享者选取秘密值 $s\in F_q/0$,以及定义在 F_q 上的 $t-1$ 次多项式 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1} \bmod q$,$a_0=s$,$a_i\in[0,q-1]$,$i\in[1,t-1]$。分享者计算 n 个份额 $(i,f(i))$,并依次分发给 n 个参与者。当不少于 t 个参与者恢复秘密值 s 时,参与者利用差值公式重构 $f(x)$。

$$f(x)=\sum_{i=1}^{t}f(x_i)\prod_{1\leqslant j\leqslant t,j\neq i}\frac{x-x_j}{x_j-x_i}\bmod q,$$

$$s=(-1)^{t-1}\sum_{i=1}^{t}f(x_i)\prod_{1\leqslant j\leqslant t,j\neq i}\frac{x_j}{x_j-x_i}\bmod q。$$

3.4　诱饵口令

诱饵口令是被添加进数据库中的虚假口令,用于检测口令数据集是否发生泄露。如图 3 所示,诱饵口令检测系统包含 4 类实体,用户、认证网关、诱饵口令检测器以及潜在的攻击者。当用户提交注册

信息(ID,PW)时,认证网关保存用户真实注册信息,生成与该身份标识 ID 相关的虚假口令,并存储在诱饵口令检测器中。当潜在攻击者提交登录信息(ID,PW')时,诱饵口令检测器检查 PW' 是否为诱饵口令。若是诱饵口令,则检测器将标识 ID 的错误登录次数增加 1。当超过门限值时,该登录请求将被拒绝。在方案中部署诱饵口令技术可以实时检测攻击者的恶意登录行为。

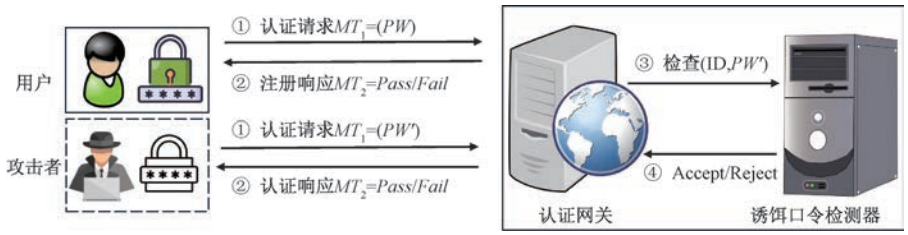

图 3 诱饵口令检测框架(PW' 可能是诱饵口令。)

3.5 敌手模型

Adv1. 敌手$\mathcal{A}$能有效访问数据|ID|和|PW|。

Adv2. 敌手$\mathcal{A}$控制公开通信道上的数据。

Adv3. 敌手$\mathcal{A}$窃取智能卡并提取隐私数据(进一步猜测密保问题),或窃取用户生物特征。

Adv4. 敌手$\mathcal{A}$窃取服务器的秘密信息,试图重构之前协商的会话密钥。

Adv5. 敌手$\mathcal{A}$窃取认证网关的临时密钥,试图重构会话密钥。

Adv6. 敌手$\mathcal{A}$是合法实体,试图获得其他实体的秘密信息,如密钥、随机值等。

3.6 评价准则

本文评价准则 **C2** 用于分析多因素方案是否支持动态口令恢复,评价准则 **C13** 用于衡量多因素方案是否符合国密 SM 标准。

C1. 无口令相关列表。任何其他实体无口令相关信息。

C2. 认证因素更新和动态口令恢复。用户可以在本地更新认证因素,通过动态口令恢复功能找回口令。

C3. 认证因素隐私性保护。公开数据不包含任何关于认证因素的隐私信息。

C4. 抗智能卡丢失。当用户丢失智能卡后,攻击者无法从智能卡中提取任何隐私信息。

C5. 抗已知攻击。方案可以抵抗设备捕获攻击、消息重放攻击等。

C6. 动态注册和更新。用户可以自主注册和更新账户。

C7. 会话密钥建立。实体间共同建立会话密钥。

C8. 异步时钟机制。方案无需进行时钟同步。

C9. 错误口令的实时检测与响应。

C10. 提供实体间相互身份认证。

C11. 身份匿名与行为不可追踪。方案有效隐藏用户身份信息且认证行为不被恶意攻击者追踪。

C12. 前向安全。当认证网关的长期密钥被泄露时,先前建立的会话密钥仍能保持机密性。

C13. 符合国密 SM 标准。基于国密算法构造方案。

其中,**C2** 要求多因素认证方案实现认证因素更新和动态口令恢复,不仅避免了认证因素泄露,而且解决了口令遗忘和丢失问题。**C13** 要求方案基于国密 SM 系列标准,符合国家在网络安全领域推动核心技术自主可控的战略要求。

4 方案设计

本节详细阐述所提方案的系统架构,以及方案具体构造。方案具体包含以下六个关键流程:系统初始化阶段;密钥生成阶段;用户注册和登录认证阶段;动态口令恢复阶段;认证因素更新阶段。表 1 是本文常用的符号和表示。

4.1 设计思想

本文方案的系统模型如图 4 所示,系统流程如图 5 所示。在注册阶段,用户输入 PW_{UE} 和 BIO_{UE},利用签密技术生成注册请求。此时,认证网关利用私钥 d_{AG} 执行解密算法,并通过签名验证注册请求的真实性和有效性。同时,认证网关利用诱饵口令技术生成诱饵口令列表 $Honeyword_{\text{list}}$。此外,用户计算 $CR_1=H_1(H_1(MID_{UE})\oplus H_1(HPW_{UE})\oplus H_1(PID_{UE})\bmod n_p)$,$\mathrm{CR}_2=H_2(PID_{UE}\parallel d_{AG},n)\oplus H_2(H_2(MID_{UE}\parallel HPW_{UE})\bmod n_p)$。在用户认证阶段,系统要求提交用户标识 ID_{UE},口令 PW_{UE} 以及生物特征 BIO_{UE}。当检测到攻击者尝试使用

表 1　主要参数对照表

符号	表示	符号	表示
UE	用户	AG	认证网关
SN	服务器	ID_{UE}	身份标识
PW_{UE}	口令	SM2	国密 SM2 算法
SM4	国密 SM4 算法	SC_{UE}	智能卡
G	基点	Bio_{UE}	生物特征
$H_i(\cdot)$	哈希函数	n_p	固定常数
$KDF(\cdot)$	密钥派生函数	F_q	q 阶有限域
q	大素数	(PK,SK)	公私钥对
$params$	公共参数	SK	会话密钥
PWC	口令密文	ASW_i	密保问题答案
$\oplus$	异或运算	$\|$	级联运算

诱饵口令时,认证网关会执行以下防护机制:首先将该异常行为记录至诱饵口令数据库;其次,当特定标识 MID_{UE} 的失败尝试次数达到预设阈值时,系统将自动阻断该标识的所有后续认证请求。

此外,本文方案支持动态口令恢复,允许用户在本地恢复口令并更新隐私信息。本文提出的动态口令恢复方法主要包含三个阶段:(1) 口令恢复凭证生成阶段。用户利用国密 SM4 加密算法生成口令密文,即 $PWC=\mathrm{SM4}.Enc_{a_0}(PW_{UE})$;利用 Shamir 秘密共享技术,将密钥 a_0 的份额 β_i 与密保问题 Q_i 绑定,即 $\delta_i=\beta_i\oplus H_2(H_1(ASW_i)\|H_1(\sigma_{UE})\bmod n)$;

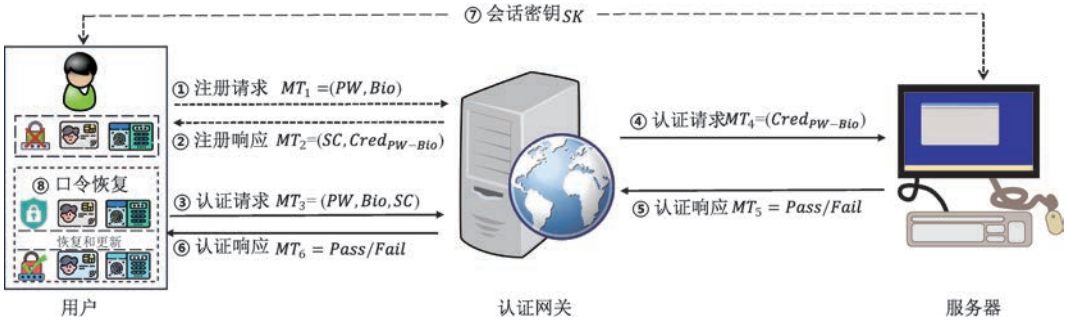

图 4　本文方案系统框架(用户 UE、网关 AG 和服务器 SN 执行相互认证,并安全地建立会话密钥 SK。此外,UE 可以在本地恢复口令 PW_{UE} 并动态地更新隐私息。)

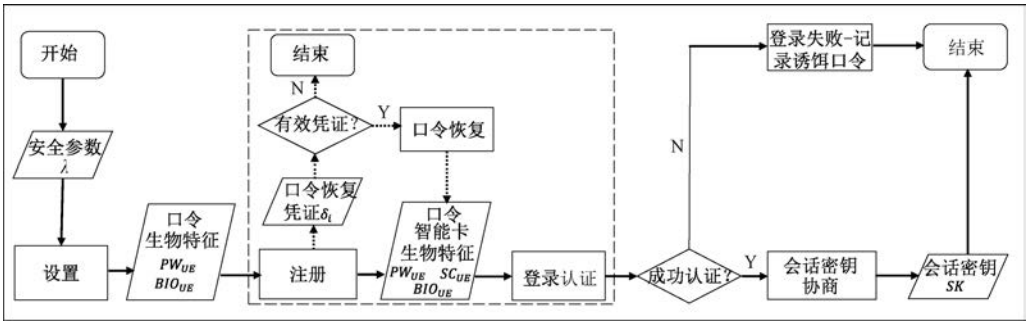

图 5　本文方案流程图

最后,用户将 $\{\{Q_i\}_{1\leqslant i\leqslant N},\{\delta_i\}_{1\leqslant i\leqslant N},PWC\}$ 存储在智能卡中;(2) 口令恢复阶段。用户从智能卡中提取隐私数据,通过回答每个密保问题 Q_i 从而恢复密钥 a_0 的份额,即 $\beta_i=\delta_i\oplus H_2(H_1(ASW_i)\|H_1(\sigma_{UE})\bmod n)$,并重构 $a_0=f(0)$,$f(x)=\sum_{i=1}^{N}\beta_i\prod_{1\leqslant j\leqslant N,j\neq i}\frac{x-x_j}{x_j-x_i}\bmod q$;

最后,用户执行国密 SM4 解密算法从而成功恢复口令,即 $PW_{UE}=\mathrm{SM4}.Dec_{a_0}(PWC)$;(3) 隐私数据更新阶段。用户在本地更新智能卡中的隐私数据:密保问题 $Q_i\to Q_i^{\mathrm{new}}$,秘密值 $a_0\to a_0^{\mathrm{new}}$,以及多项式 $f(x)\to f(x)^{\mathrm{new}}$,重新生成口令恢复凭证 $\delta_i\to\delta_i^{\mathrm{new}}$。

结合多因素认证框架,本文提出的动态口令方法将口令恢复凭证和密保问题存储在智能卡中,一方面用户可以直接在本地恢复口令,从而避免与服务器交互,降低了通信开销。另一方面,只有合法用户才能提取智能卡中的数据,降低了密保问题猜测威胁。此外,为进一步保护密保问题安全,根据文献[60,61]的研究结果,本文使用数字驱动型密保问题设计动态口令恢复方法。为提供多因素安全,本文假设敌手可以同时获取两个认证因素从而试图攻击第三个认证因素:(1) 利用智能卡 SC_{UE} 和生物特征 BIO_{UE} 攻击口令 PW_{UE};(2) 利用智能卡 SC_{UE} 和口令 PW_{UE} 攻击生物特征 BIO_{UE};(3) 利用口令 PW_{UE} 和生物特征 BIO_{UE} 攻击智能卡 SC_{UE}。为实

现口令恢复算法安全性，本文假设敌手可以进行密保问题猜测攻击，即当窃取智能卡 SC_{UE} 和生物特征 BIO_{UE} 时，敌手猜测密保问题答案 ASW_i。

4.2 设置阶段

令 λ 为系统安全参数，系统选取有限域 F_q 和定义在 F_q 上的椭圆曲线 $E: y^2 = x^3 + ax + b \bmod q$。其中，大素数 q 是有限域 F_q 的元素个数且 $a, b \in [0, q-1]$；随机选取 E 上的 n 阶基点 $G = (x_G, y_G)$，其中 n 为大素数且为 $\sharp E(F_q)$ 的素因子，$\sharp E(F_q)$ 表示域 F_q 上椭圆曲线 E 的所有有理点的数目；随机选取哈希函数 $H_1: \{0,1\}^* \rightarrow \{0,1\}^*$；$H_2: \{0,1\}^* \rightarrow [1, n-1]$；$H_3: \{0,1\}^* \rightarrow \{0,1\}^*$ 和密钥派生函数 $KDF: \{0,1\}^* \rightarrow \{0,1\}^{klen}$，其中 $klen$ 表示派生密钥的长度。设置固定常数 n_p，该常数满足条件 $2^4 \leqslant n_p \leqslant 2^8$。最后，系统设置公开参数为 $params = \{G, n, H_1, H_2, H_3, KDF, n_p\}$。

4.3 密钥生成阶段

UE 随机选取 $d_{UE} \in [0, n-1]$，计算 $P_{UE} = d_{UE}G = (x_{UE}, y_{UE})$。系统设置用户公私钥为 $(PK_{UE}, SK_{UE}) = (P_{UE}, d_{UE})$。同理，系统生成认证网关 AG 和服务器 SN 的公私钥对：$(PK_{AG}, SK_{AG}) = (P_{AG}, d_{AG})$ 和 $(PK_{SN}, SK_{SN}) = (P_{SN}, d_{SN})$。此时，系统将公钥作为公开参数，即 $params = \{G, n, H_1, H_2, H_3, KDF, n_p, PK_{UE}, PK_{AG}, PK_{SN}\}$。

4.4 注册阶段

用户注册阶段如图 6 所示。

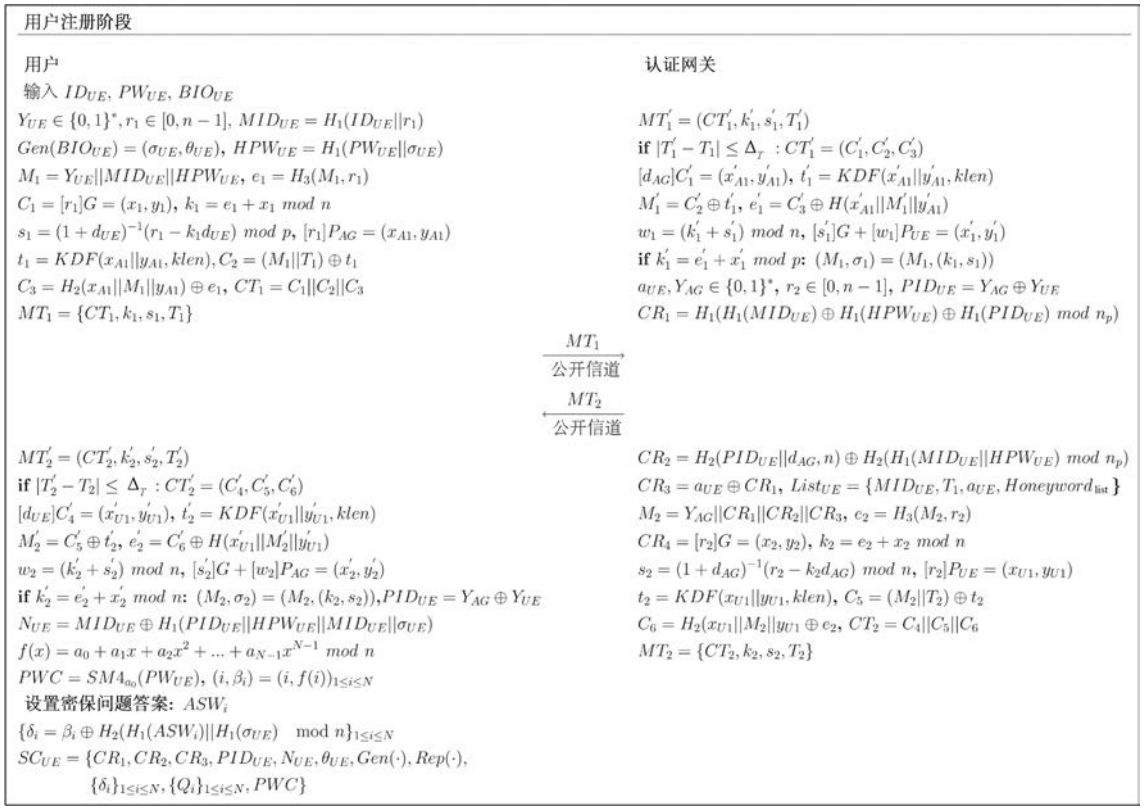

图 6 注册阶段（UE 向 AG 发送注册请求，AG 返回注册响应。）

(1) UE 输入标识 ID_{UE}，口令 PW_{UE} 以及生物特征 BIO_{UE}，计算 $Gen(BIO_{UE}) = (\sigma_{UE}, \theta_{UE})$，$HPW_{UE} = H_1(PW_{UE} \| \sigma_{UE})$，$MID_{UE} = H_1(ID_{UE} \| r_1)$，其中 $r_1 \in [0, n-1]$，$Gen(\cdot)$ 和 $Rep(\cdot)$ 表示模糊提取器概率生成函数。UE 随机选取 $Y_{UE} \in \{0,1\}^*$，令 $M_1 = Y_{UE} \| MID_{UE} \| HPW_{UE}$，计算 $e_1 = H_3(M_1, r_1)$，$C_1 = [r_1]G = (x_1, y_1)$，$k_1 = (e_1 + x_1) \bmod n$，$s_1 = (1 + d_{UE})^{-1}(r_1 - k_1 d_{UE})$，$[r_1]P_{AG} = (x_{A1}, y_{A1})$，$t_1 = KDF(x_{A1} \| y_{A1})$，$C_2 = (M_1 \| T_1) \oplus t_1$，$C_3 = H_2(x_{A1} \| M_1 \| y_{A1})$，其中 T_1 表示当前时间戳。令 $CT_1 = C_1 \| C_2 \| C_3$，UE 将注册请求 $MT_1 = \{CT_1, k_1, s_1, T_1\}$ 通过公开信道发送给 AG。

(2) AG 收到注册请求 CT'_1, k'_1, s'_1, T'_1 后，判断 T'_1 是否满足时效性，即 $|T'_1 - T_1| \leqslant \Delta_T$；若满足要求，提取 $CT'_1 = \{C'_1, C'_2, C'_3\}$，验证 C'_1 是否满足椭圆曲线方程；若满足，AG 计算 $d_{AG}C'_1 = (x'_{A1}, y'_{A1})$，$t'_1 = KDF(x'_{A1} \| y'_{A1}, klen)$，$M'_1 = C'_2 \oplus t'_1$，$e'_1 = C'_3 \oplus H_2(x'_{A1} \| M'_1 \| y'_{A1})$，$w'_1 = (k'_1 +$

$s'_1)\bmod n,(x'_1,y'_1)=[s'_1]G+[w'_1]P_{UE}$。AG 验证等式 $k'_1=(e'_1+x'_1)\bmod n$ 是否成立。若成立,则 AG 恢复 M_1,k_1,s_1。进一步地,AG 随机选取 a_{UE},$Y_{AG}\in\{0,1\}^*$,$r_2\in[0,n-1]$,计算 $PID_{UE}=Y_{AG}\oplus Y_{UE}$,$CR_1=H_1(H_1(MID_{UE})\oplus H_1(HPW_{UE})\oplus H_1(PID_{UE})\bmod n_p$,$CR_1=H_2(PID_{UE}\parallel d_{AG},n)\oplus H_2(H_2\oplus(MID_{UE}\parallel HPW_{UE})\bmod n_p)$,$CR_3=a_{UE}\oplus CR_1$。AG 创建关于标识 MID_{UE} 的一个列表 $List_{UE}=\{MID_{UE},T_1,a_{UE},Honeyword_{list}\}$。令 $M_2=\{Y_{AG}\parallel CR_1\parallel CR_2\parallel CR_3\}$,AG 计算 $e_2=H_3(M_2,r_2)$,$C_4=[r_2]G=(x_2,y_2)$,$k_2=e_2+x_2\bmod n$,$s_2=(1+d_{AG})^{-1}(r_2-k_2d_{AG})\bmod n$,$[r_2]P_{UE}=(x_{U2},y_{U2})$,$t_2=KDF(x_{U2}\parallel y_{U2},klen)$,以及 $C_5=(M_2\parallel T_2)\oplus t_2$,$C_6=H_2(x_{U2}\parallel M_1\parallel y_{U2})\oplus e_2$。令 $CT_2=\{C_4\parallel C_5\parallel C_6\}$,AG 将 $MT_2=\{CT_2,k_2,s_2,T_2\}$ 发送给 UE。

(3) 当 UE 收到注册响应 (CT'_2,k'_2,s'_2,T'_2) 后,判断 T_2 是否满足时效性,即 $|T'_2-T_2|\leqslant\Delta_T$;若满足要求,提 $CT'_2=\{C'_4,C'_5,C'_6\}$;验证 C'_4 是否满足椭圆曲线方程;若满足,UE 进一步计算 $[d_{UE}]C'_4=(x'_{U1},y'_{U1})$,$t'_2=KDF(x'_{U1}\parallel y'_{U1},klen)$,$M'_2=C'_5\oplus t'_2$,以及 $e'_2=C'_6\oplus H(x'_{U1}\parallel M'_2\parallel y'_{U1})$,$w_2=(k'_2+s'_2)mod\ n$,$(x'_2,y'_2)=[s'_2]G+[w_2]P_{AG}$;验证等式 $k'_2=(e'_2+x'_2)mod n$ 是否成立。若成立,UE 恢复 $(M_2,(k_2,s_2))$并计算 $PID_{UE}=Y_{AG}\oplus Y_{UE}$,以及 $N_{UE}=MID_{UE}\oplus H_1(PID_{UE}\parallel HPW_{UE}\parallel ID_{UE}\parallel\sigma_{UE})$;随机选取 $N-1$ 次多项式 $f(x)=a_0+a_1x_1+a_2x_2^2+\cdots+a_{N-1}x_{N-1}^{N-1}\bmod n,a_i\in[0,n-1]$,计算 $PWC=\mathrm{SM4}.Enc_{a_0}(PW_{UE})$,$(i,\beta_i)=(i,f(i))$,其中 $1\leqslant i\leqslant N$。由文献[60,61]研究结果可知,数字驱动型问题比个人偏好型问题更难被猜测。因此,UE 设置 N 个数字驱动型问题,如“你之前使用的手机号?”“使用的 XXX 网站用户名”“父母的生日?”等,设置每个密保问题答案,记为 ASW_i,然后 UE 计算 $\delta_i=\beta_i\oplus H_2(H_1(ASW_i\parallel H_1(\sigma_{UE}))\bmod n)$,并将$\{CR_1,CR_2,CR_3,PID_{UE},N_{UE},\theta_{UE},Gen(\cdot),Rep(\cdot),PWC,\{Q_i\}_{i\in[1,N]},\{\delta_i\}_{i\in[1,N]}\}$ 存储到 SC_{UE}。

4.5　登录认证阶段

登录认证阶段如图 7 所示。

图 7　登录认证阶段(UE 向 AG 发送登录及认证请求,实体之间进行相互认证并建立会话密钥)

(1) UE 将 SC_{UE} 插入特定的设备,输入因素 ID^*_{UE},PW^*_{UE} 以及 BIO^*_{UE},然后进一步计算 $\sigma^*_{UE}=Rep(BIO^*_{UE},\theta_{UE})$,$HPW^*_{UE}=H_1(PW^*_{UE}\parallel\sigma^*_{UE})$,$MID^*_{UE}=N_{UE}\oplus H_1(PID_{UE}\parallel HPW^*_{UE}\parallel ID^*_{UE}\parallel\sigma^*_{UE})$,$CR^*_1=H_1(H_1(MID^*_{UE})\oplus H_1(HPW^*_{UE})\oplus H_1(PID_{UE})\bmod n_p)$。若 $CR^*_1=CR_1$,UE 随机选取 $r_{s3},r_3\in[0,n-1]$。令 $M_3=MID_{UE}\parallel r_3\parallel SID_{SN}$,UE 计算 $e_3=H_3(M_3,r_{s3})$,$C_7=[r_{s3}]G=(x_3,y_3)$,$k_3=e_3+x_3\bmod n$,$s_3=(1+d_{UE})^{-1}(r_{s3}-k_3d_{UE})\bmod n$,$[r_{s3}]P_{AG}=(x_{A2},y_{A2})$,$t_3=KDF(x_{A2}\parallel y_{A2},klen)$,$C_8=(M_3\parallel T_3)\oplus t_3$,$C_9=H_2(x_{A2}\parallel M_3\parallel y_{A2})\oplus e_3$。然后,UE 进一步计算 $k=H_2(PID_{UE}\parallel sk_{ID_{AG}}$,

$p)=CR_2\oplus H_2(H_2(MID_{UE}\|HPW_{UE})\bmod n_p)$，以及 $a_{UE}=CR_3\oplus CR_1$，$CAK_{UE}=(a_{UE}\|k)\oplus H_1(r_3\|T_3)$，其中 T_3 表示当前时间戳。令 $CT_3=C_7\|C_8\|C_9$，UE 将 $MT_3=\{CT_3,k_3,s_3,T_3,CAK_{UE}\}$ 作为认证请求发送给 AG。

(2) 当 AG 收到登录和认证请求 CT'_3,k'_3,s'_3,T'_3 后，判断 T_3 是否满足时效性，即 $|T'_3-T_3|\leqslant\Delta_T$；若满足要求，提取 $CT'_3\rightarrow(C'_7,C'_8,C'_9)$；验证 C'_7 是否满足椭圆曲线方程；若满足，AG 计算 $[d_{AG}]C'_7=(x'_{A2},y'_{A2})$，$t'_3=KDF(x'_{A2}\|y'_{A2},klen)$，以及 $M'_3=C'_8\oplus t'_3$，$e'_3=C'_9\oplus H_2(x'_{A2}\|M'_3\|y'_{A2})$，$w_3=k'_3+s'_3\bmod n$，$(x'_3,y'_3)=[s'_3]G+[w_3]P_{UE}$。AG 验证等式 $k'_3=(e'_3+x'_3)\bmod n$ 是否成立。若上述等式成立，然后 AG 进一步计算以下值，包括 $k=H_2(PID_{UE}\|d_{AG},n)$，以及 $CAK^*_{UE}=(a_{UE}\|l)\oplus H_2(r'_3\|T_3)$。然后，AG 比较等式 $CAK^*_{UE}=CAK_{UE}$ 是否成立。若不成立，AG 计算 $(a'_{UE}\|k')=CAK_{UE}\oplus H_2(r'_3\|T_3)$。若 $a'_{UE}=a_{UE}$，$k'\neq k$，则表明 SC_{UE} 至少以 $1-1/2^{n_p}$ 概率被攻破，因此 AG 将 k' 添加到 $Honeyword_{\text{list}}$。若该列表的大小超过阈值 T_S，AG 将拒绝任何来自该智能卡的认证请求。否则，AG 恢复 (M_3,h'_3,s_3)。令 $M_4=MID_{UE}\|r_3\|SID_{SN}$，AG 随机选取 $r_4\in[0,n-1]$，并计算 $e_4=H_3(M_4,r_4)$，$C_{10}=[r_4]G=(x_4,y_4)$，以及 $k_4=(e_4+r_4)\bmod n$，$s_4=(1+d_{AG})^{-1}(r_4-k_4d_{AG})\bmod n$，$[r_4]P_{SN}=(x_{S1},y_{S1})$，$t_4=KDF(x_{S1}\|y_{S1},klen)$，$C_{11}=(M_4\|T_4)\oplus t_4$，$C_{12}=H_2(x_{S1}\|M_4\|y_{S1})\oplus e_4$ 其中 T_4 表示当前时间戳。令 $CT_4=C_{10}\|C_{11}\|C_{12}$，AG 将 $MT_4=\{CT_4,k_4,s_4,T_4\}$ 作为认证请求发送给 SN。

(3) 当 SN 收到认证请求 $\{CT'_4,k'_4,s'_4,T'_4\}$ 后，判断 T_4 是否满足时效性，即 $|T'_4-T_4|\leqslant\Delta_T$；若满足要求，提取 $CT'_4=\{C'_{10},C'_{11},C'_{12}\}$；验证 C'_{10} 是否满足椭圆曲线方程；若满足，SN 计算 $[d_{SN}]C'_{10}=(x'_{S1},y'_{S1})$，$t'_4=KDF(x'_{S1}\|y'_{S1},klen)$，$M'_4=C'_{11}\oplus t'_4$，$e'_4=C'_{12}\oplus H(x'_{S1}\|M'_3\|y'_{S1})$，$w_4=(k'_4+s'_4)\bmod n$，$(x'_4,y'_4)=[s'_4]G+[w_4]P_{AG}$。然后，SN 进一步验证等式 $k'_4=(e'_4+x'_4)\bmod n$ 是否成立。若成立，SN 恢复 (M_4,k_4,s_4)。SN 随机选取 $r_{s5},r_5\in[0,n-1]$，令 $M_5=SID_{SN}\|r_5\|MID_{UE}$，SN 计算 $e_5=H_3(M_5,r_{s5})$，$C_{13}=[r_{s5}]G=(x_5,y_5)$，$k_5=(e_5+x_5)\bmod n$，$s_5=(1+d_{SN})^{-1}(r_{s5}-k_5d_{SN})\bmod n$，$[r_{s5}]P_{UE}=(x_{U2},y_{U2})$，$t_5=KDF(x_{U2}\|y_{U2},klen)$，$C_{14}=(M_5\|T_5)\oplus t_5$，$C_{15}=H_2(x_{U2}\|M_5\|y_{S1})\oplus e_5$，其中 T_5 表示当前时间戳；计算 $SK=KDF(r_3\|r_5\|SID_{SN}\|MID_{UE},klen)$；令 $CT_5=C_{13}\|C_{14}\|C_{15}$，SN 将 $MT_5=\{CT_5,k_5,s_5,T_5\}$ 作为认证响应发送给 UE。

(4) 当 UE 收到访问响应 MT_5 后，判断 T_5 是否满足时效性，即 $|T'_5-T_5|\leqslant\Delta_T$；若满足要求，提取 $CT'_5=\{C'_{13},C'_{14},C'_{15}\}$；验证 C'_{13} 是否满足椭圆曲线方程；若满足，UE 进一步计算 $[d_{UE}]C'_{13}=(x'_{U2},y'_{U2})$，$t'_5=KDF(x'_{U2}\|y'_{U2},klen)$，$M'_5=C'_{14}\oplus t'_5$，$e'_5=C'_{15}\oplus H_2(x'_{U2}\|M'_5\|y'_{U2})$，以及 $w_5=(k'_5+s'_5)\bmod n$，$(x'_5,y'_5)=[s'_5]G+[w_5]P_{SN}$。UE 验证等式 $k'_5=(e'_5+x'_5)\bmod n$ 是否成立。若成立，则恢复 (M_5,k_5,s_5)。UE 计算 $SK=KDF(r_3\|r_5\|SID_{SN}\|MID_{UE},klen)$。最后，UE 和 SN 成功建立会话密钥 SK。

4.6 动态口令恢复阶段

动态口令恢复阶段如图 8 所示。

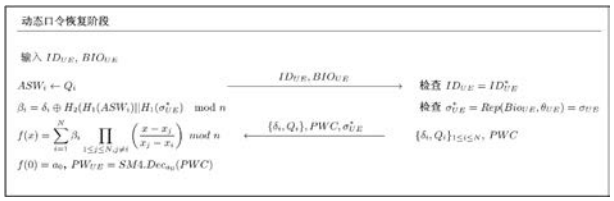

图 8 动态口令恢复阶段(拥有智能卡 SC_{UE} 且知道密保问题答案 ASW_i 的用户在本地进行口令恢复)

当遗忘和丢失口令时，UE 首先从 SC_{UE} 中提取口令恢复数据 δ_i；然后，依次回答设置的 N 个问题。此时，令每个密保问题的答案为 ASW_i，UE 计算 $\beta_i=\delta_i\oplus H_2(H_1(ASW_i)\|H_1(\sigma_{UE})\bmod n)$。当正确地回答完 N 个密保问题后，UE 可以成功地重构多项式 $f(x)=\sum_{i=1}^{N}\beta_i\prod_{1\leqslant j\leqslant N,j\neq i}\frac{x-x_j}{x_j-x_i}\bmod n$，计算 $f(0)=a_0$，并执行解密算法 $SM4.Dec_{a_0}(PWC)=PW_{UE}$ 从而恢复口令。此外，UE 可以更新密保问题 $ASW_i\rightarrow ASW_i^{\text{new}}$，秘密值 $a_0\rightarrow a_0^{\text{new}}$，以及多项式 $f(x)\rightarrow f(x)^{\text{new}}$，并重新生成口令恢复凭证 $\delta_i\rightarrow\delta_i^{\text{new}}$。动态更新这些秘密信息避免隐私数据泄露，进一步增强口令恢复的安全性。

4.7 口令和智能卡更新阶段

当获得原始口令 PW_{UE} 后，用户执行以下步骤。UE 将 SC_{UE} 插入特定设备，输入 PW_{UE}，ID_{UE}，BIO_{UE}。设备执行验证算法(与登录认证阶段相

同)认证 UE 的真实性。若验证成功,UE 输入新口令 PW_{UE}^{new},计算 $CR_1^{new}=H_1(H_1(MID_{UE})\oplus H_1(HPW_{UE}^{\text{new}})\oplus H_1(PID_{UE})\bmod n_p)$,$CR_2^{\text{new}}=CR_2\oplus H_2(H_2(MID_{UE}\parallel HPW_{UE})\bmod n_p)\oplus H_2(H_2(MID_{UE}\parallel HPW_{UE}^{\text{new}})\bmod n_p)$,$CR_3^{\text{new}}=CR_3\oplus CR_1\oplus CR_1^{\text{new}}$,$N_{UE}^{\text{new}}=MID_{UE}\oplus H_1(PID_{UE}\parallel HPW_{UE}^{\text{new}}\parallel ID_{UE}\parallel\sigma_{UE})$;UE 随机选取一个 $N-1$ 次多项式 $f^{\text{new}}(x)=a_0^{\text{new}}+a_1^{\text{new}}x_1+a_2^{\text{new}}x_2^2+\cdots+a_{N-1}^{\text{new}}x_{N-1}^{N-1}\bmod n$,计算 $PWC^{\text{new}}=\text{SM4}.Enc_{a_0^{\text{new}}}(PW_{UE}^{\text{new}})$,$N$ 个多项式值$(i,\beta_i^{\text{new}})=(i,f^{\text{new}}(i))$,更新密保问题 Q_i^{new} 并计算 $\delta_i^{\text{new}}=\beta_i^{\text{new}}\oplus H_2(H_1(ASW_i^{\text{new}})\parallel H_1(\sigma_{UE})\bmod n)$。进一步地,UE 更新 $SC_{UE}\rightarrow SC_{UE}^{\text{new}}$。

5　方案的安全性分析

5.1　安全模型

多因素认证方案的安全模型刻画了敌手的主动攻击和被动攻击能力,如文献[62－64]中的安全模型。令参数 θ_{UE}、θ_{AG}、θ_{SN} 表示不同实体 UR、AG 以及 SN。

(1) $Extract(\theta_{UE},\theta_{AG},\theta_{SN})$:该询问描述被动攻击能力,如 $\mathcal{A}$ 可以获得在公开信道中传输的数据。

(2) $Send(\theta_{UE},\theta_{AG},\theta_{SN},M)$:该询问描述主动攻击能力,$\mathcal{A}$ 向 θ_{UE},θ_{AG},θ_{SN} 发送 M 并获得响应。

(3) $Reveal(\theta_{UE},\theta_{SN})$:若 θ_{UE} 与 θ_{SN} 成功建立会话密钥,该询问将当前建立的会话密钥 SK 发送给 $\mathcal{A}$;否则,该查询返回空符号 $\perp$。

(4) $Corrupt(\theta_{UE},b)$:该查询将 PW_{UE},SC_{UE} 以及 BIO_{UE} 中的任何两个因素发送给 $\mathcal{A}$,存在三种情况,

① $Corrupt(\theta_{UE},1)$:窃取 PW_{UE} 和 SC_{UE};

② $Corrupt(\theta_{UE},2)$:窃取 BIO_{UE} 和 PW_{UE};

③ $Corrupt(\theta_{UE},3)$:窃取 BIO_{UE} 和 SC_{UE};

此外,$\mathcal{A}$ 获得认证网关密钥,即 $Corrupt(\theta_{AG},4)$:该查询验证前向安全性。当进行 $Corrupt(\theta_{UE},3)$ 查询时,$\mathcal{A}$ 窃取智能卡 SC_{UE} 和生物特征 BIO_{UE},并进行密保问题猜测攻击。

(5) $H(\cdot)$:哈希查询将随机值返回给 $\mathcal{A}$。

(6) $Test(\theta_{UE},\theta_{SN})$:当 θ_{UE} 和 θ_{SN} 诚实地执行方案并建立会话密钥 SK 时,该查询根据抛币 b 的结果执行以下步骤。当 $b=1$ 时,该查询将正确的会话密钥 SK 发送给 $\mathcal{A}$;当 $b=0$ 时,该查询返回一个等长的随机字符串 SK'。此时,安全模型需要限制敌手进行 $Corrupt(\theta_{UE},b)$ 以及 $Reveal(\theta_{UE},\theta_{SN})$ 查询。

5.2　形式化安全性证明

定理 1. 假设存在一个概率多项式时间敌手 $\mathcal{A}$ 在经过有限的 q_E 次 $Extract(\theta_{UE},\theta_{AG},\theta_{SN})$ 查询,q_S 次 $Send(\theta_{UE},\theta_{AG},\theta_{SN},M)$ 查询,q_H 次 $H(\cdot)$ 查询,q_C 次 $Corrupt(\cdot)$ 查询,以及 q_{SM4} 次 SM4 解密算法查询,能够以 $Adv_{\mathcal{A}}$ 优势攻破本文方案。$\mathcal{A}$ 的优势定义如下:

$$Adv_{\mathcal{A}}\leqslant 2C'q_s^{\eta'}+\frac{1}{2^{n_p}}+\frac{q_S}{2^{l_2}}+\frac{q_{\text{SM4}}^2}{2^{l_3}}+\frac{3q_S+q_{H_2}^2}{2^{l_{H_2}}}+\frac{q_S+q_{H_3}^2}{2^{l_{H_3}}}+\frac{(q_E+q_S)^2}{n}+\frac{3q_S+q_{H_1}^2}{2^{l_{H_1}}}+\frac{2Adv_{\mathcal{A}}^{\text{SM4}}}{q_{\text{SM4}}}+\frac{q_CN\lambda_{ASW_i}}{G_{ASW_i}}。$$

其中,C' 和 η' 表示与口令集大小和分布相关的常数,l_3 表示生物特征模糊提取函数返回值尺寸,l_3 表示 SM4 密文尺寸,$Adv_{\mathcal{A}}^{\text{SM4}}$ 表示敌手成功破解国密 SM4 加密算法的优势,$\boldsymbol{G}_{ASW_i}$ 和 $\boldsymbol{\lambda}_{ASW_i}$ 表示与密保问题有关的常数,$\boldsymbol{l}_{H_i}$ 表示哈希函数 H_i 返回值的大小。

定义游戏 $Game_1\sim Game_6$,此时 $\mathcal{A}$ 赢得游戏 $Game_i(1\leqslant i\leqslant 6)$ 的条件为 $\mathcal{A}$ 成功猜测 b。令 $Pr[G_i]$ 表示 $\mathcal{A}$ 在游戏 $Game_i$ 中获胜的概率。

(1)$Game_1$:$Game_1$ 模拟 $\mathcal{A}$ 对现实方案的攻击行为。因此,有 $Adv_{\mathcal{A}}=2Pr[G_1]-1$;

(2)$Game_2$:$\mathcal{A}$ 可以进行 $Extract(\theta_{UE},\theta_{AG},\theta_{SN})$ 查询。该查询将$\{MT_1,MT_2,MT_3,MT_4,MT_5\}$ 发送给 $\mathcal{A}$。$\mathcal{A}$ 输出一个猜测值 b'。此时,$Game_2$ 与 $Game_1$ 是计算不可区分的,有 $Pr[G_2]=Pr[G_1]$;

(3)$Game_3$:在 $Game_3$ 中,若查询响应值出现碰撞,该游戏会发生终止。该游戏可能存在以下碰撞事件,

① 查询 H_1、H_2、H_3 时,哈希值发生碰撞;

② 查询 SM4 密文发生碰撞;

③ 查询获得的其他通信数据发生碰撞。

$\mathcal{A}$ 获胜的概率为 $|Pr[G_3]-Pr[G_2]|\leqslant\frac{q_{H_1}^2}{2^{l_{H_1}}}+\frac{q_{H_2}^2}{2^{l_{H_2}}}+\frac{q_{H_3}^2}{2^{l_{H_3}}}+\frac{q_{\text{SM4}}^2}{2^{l_3}}+\frac{(q_E+q_S)^2}{2n}$;

(4)$Game_4$:若 $\mathcal{A}$ 在本地成功猜测 H_1,H_2 以及

H_3 时，游戏终止。此时 $|Pr[G_4]-Pr[G_3]|\leqslant\frac{q_S}{2^{l_{H_1}}}+\frac{q_S}{2^{l_{H_2}}}+\frac{q_S}{2^{l_{H_3}}}$；

(5)$Game_5$：$\mathcal{A}$执行 $Corrupt(\theta_{UE},1)$查询时，获得 SC_{UE} 和 PW_{UE}，并猜测 BIO_{UE}，成功猜测概率为 $\frac{q_S}{2^{l_2}}$；当执行 $Corrupt(\theta_{UE},2)$查询时，$\mathcal{A}$获得 BIO_{UE} 和 PW_{UE}，并猜测 SC_{UE} 信息，成功猜测概率为 $\frac{q_S}{2^{l_{H_1}}}+\frac{q_S}{2^{l_{H_2}}}$；当执行 $Corrupt(\theta_{UE},3)$查询时，$\mathcal{A}$获得 SC_{UE} 和 BIO_{UE}，猜测 PW_{UE}，成功猜测概率为 $C'q_s^{\eta'}$；当执行 $Corrupt(\theta_{AG},1)$查询时，$\mathcal{A}$获得长期密钥，猜测会话密钥 SK，成功猜测概率为 $\frac{1}{2^q}$。因此，有 $|Pr[G_5]-Pr[G_4]|\leqslant\frac{1}{2^q}+\frac{q_S}{2^{l_2}}+\frac{q_S}{2^{l_{H_1}}}+\frac{q_S}{2^{l_{H_2}}}+C'q_s^{\eta'}$；

(6)$Game_6$：假设 $\mathcal{A}$进行 q_C 次 $Corrupt(\cdot)$查询，从 SC_{UE} 中获得数据 $\{PWC,\{Q_i\},\{\delta_i\}_{i\in[1,N]}\}$ 并窃取 BIO_{UE}，考虑以下情况。

$-G6_0$：$\mathcal{A}$直接猜测口令，其优势为 $\frac{1}{2^{n_p}}$；

$-G6_1$：若 $\mathcal{A}$可以直接从密文 PWC 获得任何关于口令 PW_{UE} 的信息，则 $\mathcal{A}$能够以不可忽略的概率攻破 SM4 算法。$|Pr[G6_1]-Pr[G6_0]|\leqslant Adv_{\mathcal{A}}^{SM4}$；

$\cdot G6_2$：若 $\mathcal{A}$尝试从密保问题和口令恢复凭证 $\{\{Q_i\}_{i\in[1,N]},\{\delta_i\}_{i\in[1,N]}\}$ 中获得解密密钥 a_0(利用 a_0 解密密文 PWC 获得口令)。由本文口令恢复安全性分析可知，$|Pr[G6_2]-Pr[G6_1]|\leqslant\frac{1}{2^{qN}}+\frac{N\lambda_{ASW_i}}{G_{ASW_i}}$。

此时，通过以上不等式可知 $|Pr[G_6]-Pr[G_5]|\leqslant\frac{1}{2^{nN}}+Adv_{\mathcal{A}}^{SM4}+\frac{1}{2^{n_p}}+\frac{q_CN\lambda_{ASW_i}}{G_{ASW_i}}$。由 $Game_1$ 至 $Game_6$ 可知，$\mathcal{A}$的优势为

$$Adv_{\mathcal{A}}\leqslant 2C'q_s^{\eta'}+\frac{1}{2^{n_p}}+\frac{q_S}{2^{l_2}}+\frac{q_{SM4}^2}{2^{l_3}}+\frac{3q_S+q_{H_2}^2}{2^{l_{H_2}}}+\frac{q_CN\lambda_{ASW_i}}{G_{ASW_i}}+\frac{q_S+q_{H_3}^2}{2^{l_{H_3}}}+\frac{(q_E+q_S)^2}{n}+\frac{1}{2^{nN}}+\frac{3q_S+q_{H_1}^2}{2^{l_{H_1}}}+\frac{q_{SM4}^2}{2^{l_3}}+\frac{2Adv_{\mathcal{A}}^{SM4}}{q_{SM4}}.$$

5.3 非形式化分析

本文利用模糊认证技术和诱饵口令方法，设计基于国密 SM2 支持动态口令恢复的多因素认证方案。

(1)口令猜测攻击。假设 $\mathcal{A}$窃取 SC_{UE} 以及 BIO_{UE}，并从 SC_{UE} 中提取用户隐私数据 $\{CR_1,CR_2,CR_3,PID_{UE},N_{UE},\theta_{UE},Gen(\cdot),Rep(\cdot),PWC,Q_i,\delta_i\}$，计算 $\sigma_{UE}^*=Rep(BIO_{UE},\theta_{UE})$ 和 $CR_1=H_1(H_1(MID_{UE})\oplus H_1(HPW_{UE})\bmod n_p)$；令标识和口令大小为 $|ID_{UE}|\approx|PW_{UE}|\approx 32bit$。当 $n_p=2^8$ 时，将有 $\frac{2^{32}\times 2^{32}}{2^8}$ 个元组(ID,PW)满足等式 $CR_1=CR_1^*$。当进行在线口令猜测攻击时，$\mathcal{A}$通过诱饵口令方法实时检测错误口令，当错误登录次数超过预定的门限 T_S 后，认证网关 AG 将拒绝该智能卡的登录请求。此外，CR_2 与认证网关密钥 $sk_{ID_{AG}}$ 相关，在 $\mathcal{A}$不知道密钥 $sk_{ID_{AG}}$ 时，CR_2 不会泄露口令的有效信息。

(2)设备捕获攻击。一方面 $\mathcal{A}$获得服务器密钥 $sk_{ID_{SN}}$；另一方面，$\mathcal{A}$获得认证网关密钥 $sk_{ID_{AG}}$。根据密钥生成算法可知，$\mathcal{A}$无法从 $sk_{ID_{SN}}$，$sk_{ID_{AG}}$ 推断用户、其他认证网关以及其他服务器的密钥，所以无法恢复隐私数据。在每一次登录和认证过程中，随机值$\{r_1,r_2,r_3,r_4,r_5\}$将在会话结束后被删除，从而抵抗设备捕获攻击。

(3)内部攻击。$\mathcal{A}$尝试恢复口令 PW_{UE}。从方案可知，$CT_1=\{CT_1,k_1,s_1,T_1\}$是由密文、消息签名和时间戳构成。由于不知道密钥 $sk_{ID_{AG}}$，$\mathcal{A}$无法获得有关认证因素 PW_{UE},BIO_{UE},SC_{UE} 的有效信息。当服务器密钥 $sk_{ID_{SN}}$ 或者用户密钥 $sk_{ID_{UE}}$ 没有被泄露时，$\mathcal{A}$也无法从 $CT_2=\{c_2,s_2,t_2,T_2\}$，$CT_4=\{c_4,s_4,t_4,T_4\}$，$CT_5=\{c_5,s_5,t_5,T_5\}$获得任何有效信息。

(4)仿冒攻击。发送方为每个消息 M_i 计算签名，接收者验证签名是否有效从而判断 M_i 的真实性和有效性。

(5)消息重放攻击。本文将时间戳 T_i 引入密文 CT_i，其中包括密文 $C_2=(M_1\|T_1)\oplus t_1$，$C_5=(M_2\|T_2)\oplus t_2$，$C_8=(M_3\|T_3)\oplus t_3$，$C_{11}=(M_4\|T_4)\oplus t_4$ 以及 $C_{14}=(M_5\|T_5)\oplus t_5$。同时，时间戳也在

通信数据 $CT_i=\{CT_i,k_i,s_i,T_i\}$ 中被传输。当解密获得时间戳 T_i 后,实体可以检查不等式 $|T'_i-T_i|\leqslant\Delta_T$ 是否成立。

(6)用户匿名性。UE 在注册时利用随机数隐藏真实身份,即 $MID_{UE}=H_1(ID_{UE}\|r_1)$。因此,$\mathcal{A}$ 无法通过 MID_{UE} 得到用户真实身份信息。

(7)前向安全性。假设 $\mathcal{A}$ 窃取认证网关的密钥 $sk_{ID_{AG}}$ 并试图计算会话密钥 SK。但由于不知道密钥 $sk_{ID_{UE}}$,$\mathcal{A}$ 无法通过密文 CT_5 恢复 r_5 从而无法重构密钥 SK。

(8)口令恢复和更新。当遗忘和丢失口令时,UE 插入有效的智能卡 SC_{UE},输入身份标识 ID_{UE} 和生物特征 BIO_{UE}。通过验证后,UE 需要正确回答预设的密保问题才能从恢复凭证成功计算秘密份额 $\beta_i=\delta_i\oplus H_2(H_1(ASW_i)\|H_1(\sigma_{UE})\bmod n)$。最后,用户重构密钥 a_0 并解密密文 PWC,即 $f(x)=\sum_{i=1}^{N}\beta_i\prod_{1\leqslant j\leqslant N,j\neq i}(x-x_j/x_j-x_i)\bmod n$,$f(0)=a_0$,SM4.$DEC_{a_0}(PWC)=PW_{UE}$。此外,UE 可以更新密保问题 $ASW_i\rightarrow ASW_i^{\text{new}}$,秘密值 $a_0\rightarrow a_0^{\text{new}}$,以及多项式 $f(x)\rightarrow f(x)^{\text{new}}$,并重新生成口令恢复凭证 $\delta_i\rightarrow\delta_i^{\text{new}}$。

5.4　口令恢复安全性分析

定理 2. 假设存在一个概率多项式时间的敌手 $\mathcal{A}$ 拥有智能卡 SC_{UE} 和生物特征 BIO_{UE},试图从 $\{\delta_i\}_{i\in[1,N]}$ 和 PWC 中恢复 PW_{UE}。$\mathcal{A}$ 的优势为 $Adv_{\mathcal{A}}\leqslant\frac{1}{2^{nN}}+\frac{1}{2^{n_p}}+Adv_{\mathcal{A}^{\text{SM4}}}+\frac{N\lambda_{ASW_i}}{G_{ASW_i}}$。

(1)$Game_0$:$\mathcal{A}$ 直接进行口令猜测。由方案构造可知,$\mathcal{A}$ 成功的优势 $Pr[G_0]\leqslant\frac{1}{2^{n_p}}$。

(2)$Game_1$:假设 $\mathcal{A}$ 从智能卡 SC_{UE} 中提取 $\{\delta_i\}_{i\in[1,N]}$ 以及 PWC,但无法从 $\{\delta_i\}_{i\in[1,N]}$ 获得关于口令的有效信息。由于 PWC 是由 SM4 算法加密生成的口令密文,$\mathcal{A}$ 恢复口令的优势 $|Pr[G_1]-Pr[G_0]|\leqslant Adv_{\mathcal{A}}^{\text{SM4}}$。

(3)$Game_2$:假设 $\mathcal{A}$ 可以获得密保问题 Q_i 及其相关信息,并尝试从 δ_i 重构多项式 $f(x)$。将函数 $H_2(\cdot)$ 看作随机预言机。由方案构造可知,$f(x)$ 是定义在素域 F_q 上的 $N-1$ 次随机多项式。因此,UE 计算的 N 个多项式值 $\{(i,\beta_i)=(i,f(i))\}$ 和 $\{\delta_i=\beta_i\oplus H_2(ASW_i)\}$ 是 F_q 上的随机值。假设 $F_q[x]$ 是定义在 F_q 上的所有多项式集合,$S_\delta^*[x]$ 表示与 δ_i 相关的多项式集合,此时有 $S_\delta^*[x]\subset F_q[x]$。当 $\mathcal{A}$ 从 δ_i 直接猜测份额 β_i 时,其优势为 $\frac{1}{2^n}$。若 $\mathcal{A}$ 通过猜测密保问题 Q_i 的答案 ASW_i 恢复份额 β_i 时,由于 $\delta_i=\beta_i\oplus H_2(ASW_i)$,所以获得 δ_i 后,$\mathcal{A}$ 成功恢复份额 β_i 的最大优势与 $S_\delta^*[x]$ 相关。$\mathcal{A}$ 恢复口令的优势为

$$|Pr[G2]-Pr[G1]|\leqslant\frac{1}{2^{nN}}+\sum_{1\leqslant i\leqslant N}\frac{Pr[H_2(H_1(ASW_i)\cdots)]}{\prod_{Max_{S_{\delta_i}^*[x]}}Pr[H_2(H_1(ASW_i)\cdots)]}.$$

在上述不等式中,令 $Pr[H_2(ASW_i)\cdots]$ 表示 $H_2(ASW_i)$ 与 $S_{\delta_i}^*[x]$ 相关的概率。假设哈希函数 $H_2(\cdot)$ 为随机预言机,该函数将 ASW_i 映射为 F_q 上的随机值且 $H_2(ASW_i)$ 与 $H_2(ASW_j)$ 互相独立。因此 $\frac{1}{|S_{\delta_i}^*[x]|}\approx\frac{1}{|F_q[x]|}$,即 $\mathcal{A}$ 恢复口令的优势可以规约到 $\mathcal{A}$ 成功猜测多项式 $f(x)$ 的概率。本文使用最大边界描述与 $H_2(ASW_i)$ 相关的概率:

$$Max_i=Max_{S_{\delta_i}^*[x]}Pr[H_2(ASW_i)\cdots],$$

可以得到以下不等式 $\prod_{Max_{S_{\delta_i}^*[x]}}Pr[H_2(ASW_i)\cdots]\geqslant\prod_{1\leqslant i\leqslant N,Max_i}Pr[H_2(ASW_i)\cdots]\approx\frac{1}{2^{nN}}\prod_{1\leqslant i\leqslant N}Max_i$。

当 $\mathcal{A}$ 利用 Q_i 进行密保问题猜测攻击时,其最大猜测优势为 $\prod_{1\leqslant i\leqslant N}Max_i\approx\frac{N\lambda_{ASW_i}}{G_{ASW_i}}$。$\mathcal{A}$ 的优势为 $|Pr[G_2]-Pr[G_1]|\leqslant\frac{1}{2^{nN}}+\frac{N\lambda_{ASW_i}}{G_{ASW_i}}$。

综上所述,$\mathcal{A}$ 从口令恢复方法猜测口令的优势为 $Adv_{\mathcal{A}}\leqslant\frac{1}{2^{nN}}+Adv_{\mathcal{A}}^{\text{SM4}}+\frac{1}{2^{n_p}}+\frac{N\lambda_{ASW_i}}{G_{ASW_i}}$。

6　性能分析

本节给出方案的性能分析,分析结果如下。

表 2 给出了方案在认证因素、敌手模型和评价指标方面的对比分析。其中,文献[65]提出了可用于数据采集传感网并具有数据完整性保护的认证方案,该方案使用基于身份的密码算法框架,因此无法提供匿名性;文献[66]提出具有用户匿名性的认证方案,通过加密算法保证认证凭证的机密性,避免凭证泄露;文献[67]提出一种具有多因素模糊提取功

能的身份认证方案，将生物特征和标识作为认证因素，通过模糊提取函数生成凭证，避免了生物特征泄露；针对空天通信网络的安全需求，现有研究提出了多种认证方案。例如，文献[68]设计了一种支持快速路由的匿名认证机制，但其计算复杂度较高；为此，文献[69]开发了适用于无线体域网的轻量级认证协议；

表 2 方案安全属性对比分析

方案	时间	文献	认证因素	敌手模型						评价准则												
				Adv1	Adv2	Adv3	Adv4	Adv5	Adv6	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13
Zhou et al.	2015	[65]	身份+口令+智能卡	√	√	√	×	×	√	√	×	√	×	×	√	√	√	√	√	×	×	×
Azees et al.	2021	[66]	身份+证书	√	√	−	√	×	√	−	−	−	−	×	√	√	×	√	√	×	√	×
Tran et al.	2024	[67]	口令+生物特征+证书	√	√	√	×	×	√	√	×	√	−	×	√	√	√	√	√	×	×	×
Yang et al.	2019	[68]	身份+证书	√	√	−	√	×	√	−	−	−	−	√	√	√	√	√	√	√	√	×
Affaoui et al.	2020	[69]	身份+证书	√	√	−	×	×	√	−	−	−	−	×	√	×	×	√	√	×	×	×
Jiang et al.	2024	[70]	口令+生物特征	√	√	√	×	×	√	×	×	√	−	×	√	√	√	×	×	√	×	×
Song et al.	2024	[71]	口令+属性	√	√	−	√	√	√	√	×	√	−	×	√	√	√	√	√	√	√	×
Braeken et al.	2023	[72]	口令+生物特征+智能卡	√	√	√	×	×	√	√	×	√	√	×	√	√	√	×	√	×	×	×
Tahir et al.	2023	[73]	口令+生物特征	√	√	√	×	×	√	√	×	√	−	×	√	√	√	×	×	×	×	×
Li et al.	2021	[62]	口令+证书	√	√	−	×	×	√	√	×	√	−	×	√	√	√	×	√	×	×	×
Wei et al.	2016	[74]	口令+生物特征+证书	√	√	√	√	×	√	√	×	√	−	×	×	√	√	√	√	√	×	×
Wang et al.	2020	[75]	口令+生物特征+智能卡	√	√	√	√	√	√	√	×	√	√	√	√	√	√	√	√	√	√	×
Wang et al.	2025	[30]	身份+生物特征+证书	√	√	√	√	√	√	√	−	−	−	√	√	√	√	×	√	√	×	×
Yang et al.	2025	[31]	声誉+证书	√	√	−	√	×	×	√	−	−	−	√	√	×	√	×	√	√	√	×
Le et al.	2025	[32]	口令+生物特征+智能卡	√	√	√	√	×	√	√	×	√	√	×	√	√	√	×	√	√	×	×
本文方案	2025	[—]	口令+生物特征+智能卡	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√

进一步地，文献[70]提出一种融合生物特征与口令的多因素认证方案，有效解决了生物特征低熵问题，增强了方案的安全性；文献[71]提出了具有一种细粒度访问控制的多因素认证方案，用属性代替用户标识，只有满足访问策略和拥有正确口令的用户才能通过身份验证；文献[72]提出一个适用于资源受限环境的多因素认证方案，提供匿名性和前向安全性。文献[73]设计了一种面向车联网的高效多因素认证协议，经安全性分析表明，该方案能够有效防御拒绝服务攻击及身份伪造攻击；文献[62]增强了现有多因素方案的安全模型，允许敌手控制、修改公开信道中传输的数据并与用户合谋，所提出的多因素认证方案被证明可以抵抗此类攻击；文献[74]提出了一种在标准模型下可证明安全的多因素认证方案并实现了用户生物特征隐私保护；文献[75]提出一种改进的多因素认证方案，该方案被证明可以抵抗离线口令猜测攻击和内部人员攻击。

现有研究方案主要基于国际密码标准设计，未能满足我国网络安全领域核心技术自主可控的战略要求，在评价指标 C13(算法国产化)方面存在不足；上述口令认证方案，包括文献[62,65,67,70-75]没有考虑口令遗忘和丢失问题，无法提供口令恢复，不

满足评价指标 C2。

此外,从表 2 可以看出,文献[62,65,67,69,72,73]无法同时满足敌手模型 Adv4 和 Adv5,因此当服务器的密钥被泄露后,敌手可以进行节点捕获攻击从而重新建立会话密钥;文献[62,69-74]无法满足评价指标 C5,易遭受已知攻击;文献[62,65,66,69,72,73]无法提供匿名性,对用户隐私性造成威胁;文献[62,65,67,69-74]方案无法实现前向安全性,即认证网关的长期密钥泄露会增加先前会话密钥泄露的风险;虽然文献[75]满足上述敌手模型,并且符合评价指标 C1,C3～C12,但无法实现评价指标 C2 和 C13,即无法实现动态口令恢复以及无法满足国产化需求。因此,现有多因素认证方案在以下方面仍存在局限:(1)未能实现基于国密算法构造多因素认证方案;(2)缺乏有效的口令恢复机制。从表 2 可以发现,只有本文方案可以同时满足评价指标 C1～C13。

表 3 给出了方案的计算和通信开销分析。其中,T_H 表示一次密码学哈希运算;T_M 表示一次密码学群元素乘积运算;T_E 表示一次密码学群元素幂运算;T_B 表示一次生物特征模糊提取函数运算;T_{Enc} 表示一次密码学对称加密运算;T_{Sig} 表示一次密码学数字签名运算;T_P 表示一次密码学双线性映射运算;T_{Prf} 表示一次密码学伪随机函数运算,l 表示消息空间大小,l_a 表示属性集大小,t 表示用户和服务器数量。为了简化分析,假设生物特征,随机数,模糊提取函数值大小为 160 bit;哈希函数值大小为 256 bit;国密 SM4 加密算法密文大小为 128 bit,AES 加密算法密文大小为 256 bit。本文通过调用密码学库 PBC(Pairing-Based Cryptography)对上述密码学操作进行测试。

表 3　方案性能对比分析

方案	时间	文献	计算开销/ms			通信开销/bit		
			用户	服务器	合计	用户	服务器	合计
Zhou et al.	2015	[65]	$21T_H+4T_M+2T_{Enc}+2T_P$	$9T_H+2T_M+7T_E+4T_P$	134.432	5888	2304	8192
Azees et al.	2021	[66]	$5T_H+2T_M+2T_{Enc}$	$7T_H+4T_M+2T_{Enc}+4T_P$	82.374	2816	2560	5376
Tran et al.	2024	[67]	$T_H+3T_E+T_P$	$T_H+2T_E+4T_M+T_P$	51.535	8448	3840	12288
Yang et al.	2019	[68]	$11T_H+4T_M+20T_E+2T_{Sig}$	$4T_H+8T_E+2T_M+T_{Sig}$	161.746	4608	1280	5888
Affaoui et al.	2020	[69]	$8T_H+2T_E+4T_M+2T_{Enc}$	$7T_H+4T_M+2T_E+2T_{Enc}+4T_P$	103.327	3840	768	4608
Jiang et al.	2024	[70]	$T_H+3T_{Prf}+26T_E+T_{Enc}$	$20T_H+T_{Prf}+84T_E+T_{Enc}$	427.408	2472	1504	3976
Song et al.	2024	[71]	$8T_H+(11+2l_a)T_M+(12+3l_a)T_E+5T_P$	$(1+4l_a)T_M+(3+8l_a)T_E$	422.451	8704	16384	25088
Braeken et al.	2023	[72]	$2T_H+2T_M+T_B+4T_{Enc}$	$5T_H+5T_M+T_B+T_{Enc}$	55.413	1024	768	1792
Tahir et al.	2023	[73]	$3T_H+2T_B$	$3T_H$	14.674	1280	1280	2560
Li et al.	2021	[62]	$3T_H+lT_M+(6+l)T_E+2T_{Enc}$	$3T_H+T_M+4T_E$	113.232	1792	1792	3584
Wei et al.	2016	[74]	$2T_H+T_M+2T_B+4T_E+6T_{Prf}$	$2T_H+3T_M+5T_E+T_{Enc}+6T_{Prf}$	90.118	2048	2048	4096
Wang et al.	2020	[75]	$17T_H+2T_B+3T_M$	$4T_H+2T_M$	43.722	2304	768	3072
Wang et al.	2025	[30]	$2T_H+T_B+(t+1)T_M+tT_f+(2t+3)T_E$	$T_H+(t+1)T_E$	165.018	2048	512	2560
Yang et al.	2025	[31]	$3T_H+7T_E+4T_M$	$2T_H+4T_M+6T_E$	71.806	4608	2560	7168
Le et al.	2025	[32]	$15T_H+T_B+6T_M$	$10T_H+(t+6)T_M$	88.756	2560	4352	6912
本文方案	2025	[—]	$13T_H+2T_B+2T_M+T_{Enc}$	$6T_H+5T_M+T_{Enc}$	61.169	2048	2048	4096

性能对比分析表明,本方案在计算效率方面显著优于现有研究[30-32,62,65-71,74],同时在通信效率上较文献[31,32,62,65,68,74]具有优势。如图 9 所示的计算开销对比结果证实,本方案的计算复杂度低于对比方案[30-32,62,65,68,74]。图 10 的通信开销对比显示,尽管本文方案在用户端产生的通信开销略高于文献[30,62,74]中的用户通信开销,且服务器端的通信开销较文献[30,31,62,68,75]有所增加,但本文方案提出动态口令恢复方法解决了口令遗忘和泄露问题,并在注册阶段避免使用安全信道。因此,与相关方案对比可知,本文方案具有更广泛的应用前景。

从表 4 可知,本文提出的动态口令恢复方法主要使用哈希运算、异或运算用、乘法运算以及国密 SM4 加解密运算等密码操作。其中,口令恢复过程包含一次国密 SM4 加解密运算;$2N+1$ 次哈希运算;N 次乘法运算。因此降低了计算开销;同时,用户将口令恢复凭证存储在智能卡中,不需要与其他

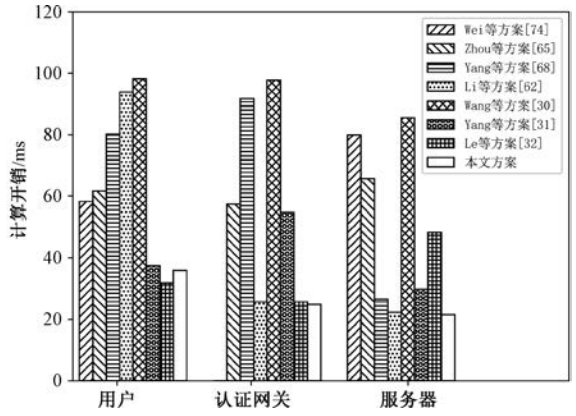

图 9 方案的计算开销对比

额外设备交互，因此降低了通信开销。其中，$|Z_n|$ 表示群 Z_n 中元素大小。

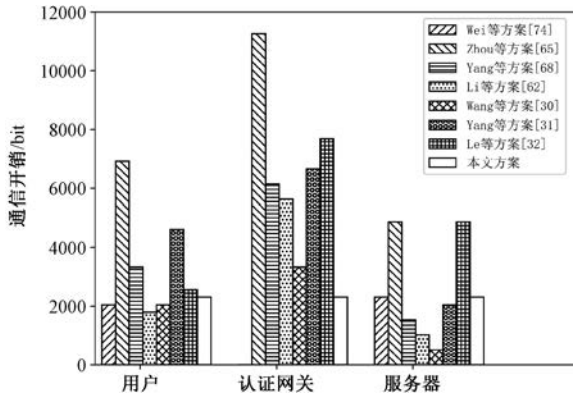

图 10 方案的通信开销对比

表 4 动态口令恢复方法性能分析

本文方法	口令恢复凭证生成	口令恢复
计算开销	$2T_{Enc}+(2N+1)T_H$	$NT_M+T_{Enc}+(2N+1)T_H$
通信开销	$(2N+1)\|Z_n\|$	$\|Z_n\|$

本文方法主要针对单个用户场景中的口令遗忘和丢失问题。当被部署到大规模用户场景中时，为保证口令安全，每个用户需要独立选择密保问题 $\{Q_i\}_{1\leqslant i\leqslant N}$、多项式 $f(x)$，生成口令恢复凭证 $\{\delta_i\}_{1\leqslant i\leqslant N}$ 并存储在智能卡中。此外，用户需要提供智能卡用于更新操作。因此，在大规模用户场景中，算法复杂度与用户数量线性相关。未来我们将继续研究如何在大规模用户场景下设计相关密码学方案。

7 结束语

为了解决多因素认证方案国产化问题以及口令遗忘和丢失问题，本文基于国密 SM2 算法，提出一种支持动态口令恢复的多因素认证方案。该方案基于国密 SM 系列标准，符合国家在网络安全领域推动核心技术自主可控的战略要求；当用户遗忘和丢失口令时，方案支持动态口令恢复，允许用户更新秘密值、密保问题以及口令恢复凭证，避免隐私信息泄露。与现有的多因素认证方案相比，本文方案能够抵抗已知攻击并提供前向安全性以及动态口令恢复等理想安全属性。性能分析结果表明本文方案具有可行性。

致 谢 衷心感谢《计算机学报》编辑部老师和各位评审专家花费宝贵的时间和精力对本论文进行审阅！

参 考 文 献

[1] Feng Deng-Guo, Zhang Min, Li Hao. Big data security and privacy protection. Chinese Journal of Computers, 2014, 37(1): 246-258 (in Chinese)
(冯登国，张敏，李昊. 大数据安全与隐私保护. 计算机学报，2014，37(1)：246-258)

[2] Al-AttarZ S, Abbes H, Zerai F. Smartphone-key: Hands-free two-factor authentication for voice-controlled devices using Wi-Fi location. IEEE Transactions on Network and Service Management, 2023,20(3): 3848-3864

[3] Pernpruner M, Carbone R, Sciarretta G, and Ranise S. An automated multi-layered methodology to assist the secure and risk-aware design of multi-factor authentication protocols. IEEE Transactions on Dependable and Secure Computing, 2024, 20(4): 1935-1950

[4] Białas K, Kedziora M, Chałupnik R, and Song H. Multi-factor authentication system using simplified EEG brain-computer interface. IEEE Transactions on Human-Machine Systems, 2022, 52(5): 867-876

[5] Bonneau J, Schechter S. Towards reliable storage of 56-bit secrets in human memory//Proceedings of the 23rd USENIX Security Symposium, Seattle, USA, 2014: 607-623

[6] Zhu L, Wang D. Robust multi-factor authentication for WSNs with dynamic password recovery. IEEE Transactions on Information Forensics and Security, 2024, 19: 8398-8413

[7] Groce A, Katz J. A new framework for efficient password-based authenticated key exchange//Proceedings of the 17th ACM conference on Computer and Communications Security. Chicago, USA, 2010: 516-525

[8] Agrawal S, Miao P, Mohassel P, Mukherjee P. PASTA: Password-based threshold authentication//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. Toronto, Canada, 2018: 2042-2059

[9] Xu M, Wang D. Practical Two-Factor Authentication Protocol for Real-Time Data Access in WSNs. IEEE Transactions on

Dependable and Secure Computing, 2025, doi: 10.1109/TDSC.2025.3563552

[10] Denning T, Bowers K, Van Dijk M, Juels A. Exploring implicit memory for painless password recovery//Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Vancouver, Canada, 2011: 2615-2618

[11] Juggling security: How many passwords does the average person have in 2024? https://nordpass.com/blog/how-many-passwords-does-average-person-have, 2024

[12] Narendar D, Mathew P, Padmavathi G, and Rao K. G. Password recovery of android devices//Proceedings of the 2nd International Conference on Recent Trends in Microelectronics, Automation, Computing and Communications Systems. Hyderabad, India, 2024: 762-769

[13] Hintea D, Bird R, Moss J. An investigation into identifying password recovery and data retrieval in the android operating system//Proceedings of the 16th European Conference on Cyber Warfare and Security. Dublin, Ireland, 2017: 165

[14] Li Y, Chen Z, Wang H, Sun K, and Jajodia S. Understanding account recovery in the wild and its security implications. IEEE Transactions on Dependable and Secure Computing, 2020, 19(1): 620-634

[15] Zhang L, Yu F. The research on Outlook password recovery//Proceedings of the International Conference on Mechatronic Sciences, Electric Engineering and Computer. Shengyang, China, 2013: 1715-1719

[16] Little R, Qin L, Varia M. Secure account recovery for a privacy-preserving web service//Proceedings of the 33rd USENIX Conference on Security Symposium. Philadelphia, USA, 2024: 1993-2010

[17] Lassak L, Golla M, Stobert E, and Durmuth M. A comparative long-term study of fallback authentication schemes//Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems. Honolulu, USA, 2024: 1-19

[18] National Cryptography Administration, SM2 elliptic curve public key cryptography algorithm. Beijing: China Standard Press, 2010 (in Chinese)
(国家密码管理局, SM2 椭圆曲线公钥密码算法. 北京: 中国标准出版社, 2010)

[19] Juang W, Chen S, Liaw H. Robust and efficient password-authenticated key agreement using smart cards. IEEE Transactions on Industrial Electronics, 2008, 55(6): 2551-2556

[20] Sun D, Huai J, Sun J, Li J, Zhang J, and Feng Z. Improvements of Juang′s password-authenticated key agreement scheme using smart cards. IEEE Transactions on Industrial Electronics, 2009, 56(6): 2284-2291

[21] Qin S, Xiao Y, Xin Y, Gao Y, and Zhang R. Practical and veritable threshold multi-factor authentication for mobile devices. The Computer Journal, 2025, https://doi.org/10.1093/comjnl/bxaf001

[22] Yang X, Jia Z, Liu L, and Li H. A Secure and efficient multi-factor user authentication protocol//Proceedings of the International Conference on Cyberspace Simulation and Evaluation. Shenzhen, China, 2024: 306-319

[23] Kumar V, Ali R, Sharma P K. A Secure Multi-factor authentication framework for IoT-environment using cloud computing//Proceedings of the International Conference On Innovative Computing And Communication. Zhengzhou, China, 2024: 477-494

[24] Braeken A. Flexible hybrid post-quantum bidirectional multi-factor authentication and key agreement framework using ECC and KEM. Future Generation Computer Systems, 2025, 166: 107634

[25] Wang D, Cao Y, Lam K Y, Hu, Y, and Kaiwartya O. Authentication and key agreement based on three factors and PUF for UAVs-assisted post-disaster emergency communication. IEEE Internet of Things Journal, 2024, 11(11): 20457-20472

[26] Li C, Hwang M S. An efficient biometrics-based remote user authentication scheme using smart cards. Journal of Network and Computer Applications, 2010, 33(1): 1-5

[27] Dhillon P K, Kalra S. A lightweight biometrics based remote user authentication scheme for IoT services. Journal of Information Security and Applications, 2017, 34: 255-270

[28] Feng Q, He D, Zeadally S, and Wang, H. Anonymous biometrics-based authentication scheme with key distribution for mobile multi-server environment. Future Generation Computer Systems, 2018, 84: 239-251

[29] Li Y, Tian Y. A lightweight and secure three-factor authentication protocol with adaptive privacy-preserving property for wireless sensor networks. IEEE Systems Journal, 2022, 16(4): 6197-6208

[30] Wang L, Xu J, Qin B, Wen M, and Chen K. An efficient fuzzy certificateless signature-based authentication scheme using anonymous biometric edentities for VANETs. IEEE Transactions on Dependable and Secure Computing, 2025, 22(1): 292-307

[31] Yang X, Zhu F, Luo J, Yi X, Ning J, and Huang X. Secure reputation-based authentication with malicious detection in VANETs. IEEE Transactions on Dependable and Secure Computing, 2025, 22(1): 359-372

[32] Le T-V, Yang M, Khalid M, Hamed T, Li C, Lee, Cheng C, Anwar G, and Chen C. An enhanced multi-factor device authentication protocol in IoLT healthcare environment. IEEE Transactions on Network Science and Engineering, 2025, 12(2): 571-583

[33] Bahache A N, Chikouche N, Akleylek S. Securing cloud-based healthcare applications with a quantum-resistant authentication and key agreement framework. Internet of Things, 2024, 26: 101200

[34] Taj I, Adnan M. Quantum-Resistant Security Framework for Secure and Scalable IoT-enabled Metaverse Environments. IEEE Transactions on Consumer Electronics, 2025, doi: 10.1109/TCE.2025.3558268

[35] Xue K, Ma C, Hong L, and Ding R. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. Journal of Network Computer Applications, 2013, 36(1): 316-323

[36] Wang F, Xu Y, Zhang H, Zhang Y, and Zhu L. 2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET. IEEE Transactions on Vehicular Technology, 2015, 65(2): 896-911

[37] Kumar V, Ahmad M, Mishra D, Kumari S, and Khan M. K. RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing. Vehicular Communications, 2020, 22: 100213

[38] Khan A A, Kumar V, Ahmad M, Rana S, and Mishra D. PALK: Password-based anonymous lightweight key agreement framework for smart grid. International Journal of Electrical Power & Energy Systems, 2020, 121: 106121

[39] Das M. Two-factor user authentication in wireless sensor networks. IEEE Transactions on Wireless Communications, 2009, 8(3): 1086-1090

[40] Li C, Weng C, Lee C. An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks. Sensors, 2013, 13(8): 9589-9603

[41] Chang C, Le H. A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. IEEE Transactions on wireless communications, 2015, 15(1): 357-366

[42] Wazid M, Das A K, Bhat V, and Vasilakos A. V. LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment. Journal of Network and Computer Applications, 2020, 150: 102496

[43] Shen M, Lu H, Wang F, Liu H, and Zhu L. Secure and efficient blockchain-assisted authentication for edge-integrated Internet-of-Vehicles. IEEE Transactions on Vehicular Technology, 2022, 71(11): 12250-12263

[44] Li J, Jin J, Lyu L, Yuan D, Yang Y, Gao L, and Shen C. A fast and scalable authentication scheme in IOT for smart living. Future Generation Computer Systems, 2021, 117: 125-137

[45] Qin X, Li W, Rosenberg P. RoundImage: towards secure graphical password authentication via rounded image selection in IoT. IEEE Internet of Things Journal, 2025, doi: 10.1109/JIOT.2025.3547816

[46] Zhou Z, Yang C N, Wang S, Nan G, Cimato S, ZhengY, and Wang Q. Google map-based password authentication systems using tolerant distance and homomorphic encryption. IEEE Transactions on Dependable and Secure Computing, 2025, doi: 10.1109/TDSC.2025.3549028

[47] Ellison C, Hall C, Milbert R, and Chneier B. Protecting secret keys with personal entropy. Future Generation Computer Systems, 2000, 16(4): 311-318

[48] Frykholm N, Juels A. Error-tolerant password recovery// Proceedings of the 8th ACM Conference on Computer and Communications Security, Philadelphia, USA 2001: 1-9

[49] Chmielewski L, Hoepman J, Rossum P. Client-server password recovery//Proceedings of the Move to Meaningful Internet Systems: OTM 2009, Vilamoura, Portugal, 2009: 861-878

[50] Han Qing-Di, Lu Si-Qi. SM2 signature scheme for protecting signature private key based on SOTP cryptography technology. Journal of Cryptologic Research, 2024, 11(5): 991-1002 (in Chinese)
(韩庆迪, 陆思奇. 基于 SOTP 加密保护签名私钥的 SM2 签名方案. 密码学报(中英文), 2024, 11(5): 991-1002)

[51] Wei Wei, Luo Min, Bai Ye, Peng Cong, and He De-Biao. Fast implementation of SM2 digital signature algorithm using SIMD instructions. Journal of Cryptologic Research, 2023, 10(4): 720-736 (in Chinese)
(韦薇, 罗敏, 白野, 彭聪, 何德彪, 基于 SIMD 指令集的 SM2 数字签名算法快速实现. 密码学报, 2023, 10(4): 720-736)

[52] Zhang Ke-Zhen, Lin Jing-Qiang, Wang Wei, Liu Yong, Li Guang-Zheng, and Liu Zhen-Ya. Research on two-party SM2 threshold signature schemes with a blind cooperative server. Journal of Cryptologic Research, 2024, 11(4): 945-962(in Chinese)
(张可臻,林璟锵,王伟,刘勇,李光正,刘振亚. SM2 签名算法两方门限盲协同计算方案研究,密码学报, 2024, 11(4): 945-962)

[53] Wang Ming-Deng, Yan Ying-Jian, Guo Peng-Fei, Zhang Fan. Efficient implementation of national security algorithms SM2, SM3 and SM4 based on RISC-V instruction extension method. Acta Electronica Sinica, 2024, 52(8):2850-2865 (in Chinese)
(王明登,严迎建,郭朋飞,张帆. 基于 RISC-V 指令扩展方式的国密算法 SM2、SM3 和 SM4 的高效实现. 电子学报, 2024, 52(8): 2850-2865)

[54] Wu Wen, Dong Jian-Kuo, Liu Peng-Bo, Dong Zhen-Jiang, Hu Xin, Zhang Pin-Chang, Xiao Fu. High performance parallel acceleration method for domestic public key cryptographic algorithm SM2 based on domestic GPU. Journal on Communications, 2025, http://kns.cnki.net/kcms/detail/11.2102.TN.20250515.1629.008.html(in Chinese)
(吴雯, 董建阔, 刘鹏博, 董振江, 胡昕, 张品昌, 肖甫. 基于国产 GPU 的国产公钥密码 SM2 高性能并行加速方法. 通信学报,2025, http://kns.cnki.net/kcms/detail/11.2102.TN.20250515.1629.008.html)

[55] Qiao Han, Wang An, Wang Bo, Su Chang-Shan, Li Gen, Tang Yu-Xing, and Zhu Lie-Huang. Optimized implementation of the SM2 algorithm on the GmSSL cryptography library. Chinese journal of computers, 2025, 48(2): 463-476 (in Chinese)
(乔晗, 王安, 王博, 苏长山, 李根, 唐遇星, 祝烈煌. 面向 GmSSL 密码库的 SM2 算法快速优化实现. 计算机学报,

2025, 48(2): 463-476)

[56] Wang D, Cheng H, Wang P, Huang X, and Jian G. Zipf's law in passwords. IEEE Transactions on Information Forensics and Security, 2017, 12(11): 2776-2791

[57] Hou Z, Wang D. New Observations on Zipf's law in passwords. IEEE Transactions on Information Forensics and Security, 2023, 18: 517-532

[58] Zhu Liu-Fu, Wang Ding. A multi-factor authentication scheme under the SM9 framework. Journal of Electronics & Information Technology, 2024, 46(5): 2137-2148
(朱留富, 汪定, 支持商密 SM9 算法框架的多因素认证方案. 电子与信息学报, 2024, 46(5): 2137-2148)

[59] Pradhan M, Mohanty S. A blockchain-assisted multifactor authentication protocol for enhancing IoMT security. IEEE Internet of Things Journal, 2024, 11(24):39323-39332

[60] Bonneau J, Bursztein E, Caron I, Jackson R, and Williamson M. Secrets, lies, and account recovery: Lessons from the use of personal knowledge questions at google//Proceedings of the 24th International Conference on World Wide Web. Florence, Italy, 2015: 141-150

[61] Rabkin A. Personal knowledge questions for fallback authentication: Security questions in the era of Facebook//Proceedings of the 4th Symposium on Usable Privacy and Security. Pittsburgh, USA, 2008: 13-23

[62] Li W, Cheng H, Wang P and Liang K. Practical threshold multi-factor authentication. IEEE Transactions on Information Forensics and Security, 2021, 16: 3573-3588

[63] Jiang Jin-Wei, Wang Ding, Zhang Guo-Yin, and Chen Zhi-Yuan. Private key management scheme for mobile edge computing. Chinese Journal of Computers, 2022, 45(6): 1348-1372 (in Chinese)
(蒋京玮,汪定,张国印,陈志远,面向移动边缘计算的密钥管理协议. 计算机学报,2022,45(6):1348-1372)

[64] Wu Y, Pang M, Ma J, Qu W, Yue Q, and HanW. An identity management scheme based on multi-factor authentication and dynamic trust evaluation for telemedicine. Sensors, 2025, 25(7): 2118

[65] Zhou Q, Tang C, Zhen X, and Rong C, A secure user authentication protocol for sensor network in data capturing. Journal of Cloud Computing, 2015, 4(1), doi: 10.1186/s13677-015-0030-z

[66] Azees M, Vijayakumar P, Karuppiah M, and Nayyar A. An efficient anonymous authentication and confidentiality preservation schemes for secure communications in wireless body area networks. Wireless Networks, 2021, 27(3): 2119-2130

[67] Tran H, Hu J, Hu W. Biometrics-based authenticated key exchange with multi-factor fuzzy extractor. IEEE Transactions on Information Forensics and Security, 2024, 19: 9344-9358

[68] Yang Q, Xue K, Xu J, Wang J, Li F, and Yu N. AnFRA: Anonymous and fast roaming authentication for space information network. IEEE Transactions on Information Forensics and Security, 2019, 14(2): 486-497

[69] Arfaoui A, Boudia OR, Kribèche A, Senouci SM and Hamdi M. Context-aware access control and anonymous authentication in WBAN. Computer Security, 2020, 88, doi: 10.1016/j.cose.2019.03.017

[70] Jiang C, Xu C, Han Y, Zhang Z, and Chen K. Two-factor authenticated key exchange from biometrics with low entropy rates. IEEE Transactions on Information Forensics and Security, 2024, 19: 3844-3856

[71] Song M, Wang D. AB-PAKE: Achieving fine-grained access control and flexible authentication. IEEE Transactions on Information Forensics and Security, 2024, 19: 6197-6212

[72] Braeken A. Highly efficient bidirectional multifactor authentication and key agreement for real-time access to sensor data. IEEE Internet of Things Journal, 2023, 10(23): 21089-21099

[73] Tahir H, Mahmood K, Ayub M, and Saleem M. Lightweight and secure multi-factor authentication scheme in VANETs. IEEE Transactions on Vehicular Technology, 2023, 72(11): 14978-14986

[74] Wei Fu-Shan, Zhang Gang, Ma Jian-Feng, and Ma Chuan-Gui. Privacy-preserving multi-factor key exchange protocol in the standard model. Journal of Software, 2016, 27(6): 1511-1522 (in Chinese)
(魏福山, 张刚, 马建峰, 马传贵, 标准模型下隐私保护的多因素密钥交换协议. 软件学报, 2016, 27(6): 1511-1522)

[75] Wang Chen-Yu, Wang Ding, Wang Fei-Fei, and Xu Guo-Ai. Multi? factor user authentication scheme for multi? gateway wireless sensor networks. Chinese Journal of Computers, 2020, 43(4): 683-700 (in Chinese)
(王晨宇, 汪定, 王菲菲, 徐国爱, 面向多网关的无线传感器网络多因素认证协议. 计算机学报, 2020, 43(4): 683-700)

WANG Ding, Ph. D., professor. His research interests focus on secret key security and identity authentication.

ZHU Liu-Fu, Ph. D. candidate. His research interests focus on cryptographic protocols.

Background

Multi-factor authentication utilizes multiple authentication factors to identify users, reducing the security threats posed by the exposure of some factors (not all of them). However, nearly all current schemes are based on foreign cryptographic standards, which do not align with the national strategy for autonomous and controllable cyberspace security. Once foreign cryptographic algorithms have backdoors or undisclosed flaws, attackers can maliciously monitor or decrypt to obtain confidential messages, which may pose a significant security threat to individuals, businesses, and even countries.

In particular, passwords are widely applied in constructing authentication schemes because of the easy deployment and modification. Yet, researchers have shown that human-generated passwords often follow the Zipf distribution and are vulnerable to password guessing attacks. To reduce the above threats, more and more systems require users to set complex passwords. However, due to the limited memory capability, users typically can only correctly remember 5-7 different passwords, which may lead to password forgetting and losing issues. However, most existing multi-factor authentication schemes assume that users will not forget or lose passwords, and require users to resubmit original passwords for authentication. Although some password recovery methods have been proposed, they cannot be directly applied in MFA. On the one hand, most current recovery methods involve direct interactions between users and servers. On the other hand, server failures can prevent password recovery service, and even worse, the password-related table stored on servers may further lead to password-guessing attacks.

This paper proposes a multi-factor authentication scheme based on the SM2 algorithm with dynamic password recovery. On the one hand, it addresses the localization issues of multi-factor authentication schemes; in particular, we propose a signcryption scheme based on the SM2 signature scheme and encryption scheme to ensure confidentiality and integrity simultaneously. On the other hand, it addresses the password forgetting and losing issues via employing the Shamir Secret Sharing technique to bind private questions with password recovery credentials. The proposed recovery method supports updating secret questions, secret key, and recovery credentials to address the private information leakage issues. Furthermore, it also applies the fuzzy verifier technique and honeyword method to resist password guessing attacks.

This work was supported by the National Natural Science Foundation of China under Grant 62222208 and by the Natural Science Foundation of Tianjin, China, under Grant 21JCZXJC00100.