海南大学

研究生学位论文开题报告书

研究生类别：☐学术学位博士　☐专业学位博士

☐学术学位硕士　☑ 专业学位硕士

姓　　名：陈伟

学　　号：23220854120037

专业名称：网络与信息安全

研究方向：身份认证

导师姓名：田艳昭

入学年月：2023 年 9 月

填表日期：2024 年 10 月 15 日

论文题目	面向 IoT 设备具有密码泄露检测机制的多因素认证方案		
学位论文计划定稿时间	2026 年　3　月	是否与导师科研课题相关	是

一、研究来源

（一）研究的目的和意义

随着物联网（IoT）和网络技术的迅猛发展，大量智能设备通过互联网实现互联互通，极大地方便了人们的生活和工业生产。然而，IoT 设备的广泛部署也存在着严峻的安全隐患，尤其在身份认证中，密码泄漏和身份伪造问题愈发突出。因此，设计一个轻量级、多因素且具备密码泄漏检测功能的认证方案成为确保 IoT 系统安全的关键。本课题旨在开发一个高效、安全的认证方案，结合物理不可克隆函数（PUF）、生物特征（如指纹识别）等多因素认证方式，在保障安全性的同时实现设备的友好易用性。此外，该方案能够自动检测密码泄漏，一旦发生泄露事件，系统可迅速响应并进行风险防控，提升系统的整体安全性能。

研究意义如下：

1. 增强 IoT 系统的安全性和抗攻击能力

由于 IoT 系统中的设备受到算力等资源的限制，传统的认证方案需要针对 IoT 特殊场景重新设计。本课题提出的轻量级认证方案基于物理不可克隆函数（PUF）构建硬件级的安全认证机制，能有效防止设备克隆和物理攻击。通过引入指纹识别、PUF 等多因素认证方法，增强认证过程的抗攻击能力，能有效抵抗密码泄露、设备伪造及物理篡改等威胁，显著提升系统的整体安全性。

2. 保护用户隐私

个人信息的泄露会带来极大的隐私风险，且随着网络服务的增多，用户身份数据在网络环境中的暴露机会不断增加。本课题引入指纹识别等生物特征认证手段，使认证过程更加安全且难以伪造；同时，结合密码泄漏检测机制，能够在密码泄露的情况下及时发现并采取安全措施，有效保护用户的个人隐私安全。

3. 提升 IoT 系统的可用性和响应性

传统的认证方案在发生密码泄露时，通常依赖于用户主动修改密码，这既增加了用户负担，又影响系统的正常运行。本课题通过设计自动化的密码泄漏检测和响应机制，使系统在检测到密码泄露后能够自动执行保护措施，降低用户数据大范围扩散的

风险，确保系统的持续可用性与可靠性。同时，这种自动响应机制不仅减轻用户操作负担，而且提升了系统的便捷性和用户体验。

4. 推动轻量级多因素认证技术的发展

针对 IoT 设备的资源受限特性，本课题提出一种结合 PUF 和生物识别的轻量级认证方案，不仅满足了 IoT 设备的计算和存储约束，而且实现了较高的安全性。这为资源受限环境下的认证技术提供了新思路，并在技术上为 IoT 系统中大规模设备的身份认证带来了新的可能性。本研究可以作为轻量级多因素认证技术的实践参考，为 IoT 领域的学术研究和实际应用提供理论支持和技术基础。

5. 实现对工业和消费物联网的有效保护

随着工业互联网和消费物联网的快速发展，越来越多的设备通过网络连接起来，如何保证身份认证的安全性直接影响到工业控制和生产系统的安全。本课题提出的多因素认证方案，通过 PUF、指纹识别等多种手段建立了一套适合于消费和工业物联网的统一认证框架，为工业环境的身份认证提供更高的安全保障，帮助构建自主、可控的工业物联网系统，为未来工业互联网的安全发展奠定基础。

6. 保障数据安全与设备不可克隆性

本课题使用 PUF 作为一种不可克隆的物理特征，通过其生成独特的设备密钥，保障了设备唯一性和防克隆能力，使得即使在设备丢失或被攻击的情况下，攻击者也无法仿制或复制设备密钥。此外，结合多因素认证机制，进一步加强了数据传输过程的安全性，防止敏感数据被非法窃取与利用。

综上所述，本研究通过设计一个具备密码泄漏检测功能、轻量级、多因素的 IoT 认证方案，结合 PUF 和生物特征认证等技术，提供了更高效、安全和智能的物联网系统认证解决方案。

（二）文献综述及评价

1. 物联网认证技术

万物互联的物联网技术使得各种设备通过互联网相连成为现实，人们逐渐进入物联网时代。大量形体功能各异的实体对象存在于物联网中，主要包括用户终端、设备和云服务[1]。为确保各方的安全，这些相连实体对象均在进行连接时需进行身份认证，即用户终端和云服务之间、设备和用户终端之间、云服务和设备之间及设备和设备之间均存在身份认证的需求，所以物联网身份认证技术涵盖了其应用的各种场景[2]。同时匿名认证是保护用户身份隐私的有效手段，根据匿名认证使用的密码技术将已有的匿名认证技术分为基于对称加密的方案、基于非对称加密的方案、基于身份的签名方案、基于无证书的签名方案、基于群签名的方案[3]。

2. 物理不可克隆函数（PUF）技术

物理不可克隆函数（Physical Unclonable Function, PUF）是一种基于物理特性实现的硬件安全技术，广泛应用于身份认证、密钥生成和硬件防篡改等领域。PUF 利用制造工艺中的随机性和不可控性，使得每个设备在微观结构上具有独特的响应特性。通过输入挑战信号，PUF 可以生成特定的响应，类似于“指纹”式的唯一标识，从而实现不可复制的安全特征[4]。这种技术优势在于其无需存储或传输密钥，避免了传统方法中的安全漏洞。同时，PUF 具备低功耗、抗逆向工程和抗物理攻击的特性，在物联网、加密芯片和智能卡等领域展现出广泛的应用前景[4]。

同时 PUF 种类多样各基于不同的物理特性来实现独特的安全机制。硅工艺 PUF 利用半导体制造中的随机差异，如 SRAM 初始状态或环形振荡器的频率差异，实现轻量化身份认证和密钥生成；光学 PUF 则通过激光照射含微粒的透明材料，产生复杂的不可复制光学图像，用于高安全性设备；涡流 PUF 通过在表面涂覆含随机微粒的涂层来防止物理攻击，适合高安全场景。磁性 PUF 利用材料的随机磁性变化生成唯一响应，适用于对外部干扰敏感的高隐私场景；声音 PUF 则通过材料对声波的独特反应生成身份特征，适用于设备验证等特定应用。这些不同种类的 PUF 为身份验证、密钥管理和硬件防伪等领域提供了丰富的选择，增强了硬件安全性[5]。

3. Honeyword 技术

蜜语（Honeywords）技术是一种有效的密码泄露检测方法，通过在实际密码数据库中引入多个虚假密码（蜜语）来迷惑潜在的攻击者[6]。此技术不仅增加了攻击者的识别难度，而且能够在密码泄露或猜测时进行有效的检测。当攻击者在暴力破解或凭证填充攻击中尝试登录并使用到蜜语时，系统会立即产生警报，通知管理员发生了潜在的攻击行为，从而提供额外的安全防护层。

为确保蜜语的生成与真实密码具有相似的分布特性，齐夫定律（Zipf's Law）在该技术中提供了重要支持[7]。齐夫定律指出，在自然语言或特定数据集合中，数据频率与排名之间通常满足反比关系，即排名靠前的数据出现频率较高。在密码学中，密码的分布通常符合这一定律，即用户倾向于选择频率较高、容易记忆的弱密码。因此，通过参考齐夫定律生成蜜语，可以确保蜜语的分布特性接近真实密码，使攻击者难以凭借统计规律分辨出真实密码和蜜语的区别，从而提高密码数据库的安全性。

4. 基于图论的口令安全

此外，基于图论的口令安全机制进一步提升了蜜语的构造效果。Tian 提出通过拓扑图形序列生成蜜语，以此增加蜜语的平坦度和随机性[6]。这一方案利用拓扑图形矩阵，将用户密码与拓扑序列相结合，生成的蜜语序列在不同用户和不同拓扑图形间呈现出更

高的分布平坦度，使得蜜语在分布上更具多样性。拓扑图形矩阵的随机生成特性有效提高了蜜语生成的复杂度，增加了蜜语序列空间的随机性和难度，使得即使攻击者通过暴力破解获得了部分蜜语，系统也能凭借随机图形生成的蜜罐序列进行检测和识别。

图论方法还可以通过零因子图的结构实现蜜语的生成，其中，零因子图的团数计算成为关键。零因子图通过数学结构化方法生成大量虚假密码序列，使蜜语的排列组合方式更加多样，有助于提升蜜语的平坦度和防攻击性能。基于图论的零因子图方法可以生成序列化的蜜语集，为蜜语技术提供了广阔的生成空间。此外，在零因子图的支持下，不仅可以构造高平坦度的蜜语，还能够通过调整零因子的组合方式，形成更灵活和定制化的蜜语生成方案，提高其抗猜测攻击和抗暴力破解的能力[7]。

5. 基于对称加密的方案

基于对称加密的方案使用消息身份验证代码（MAC）来验证通信消息。具体来说，物联网设备使用共享密钥为每条消息生成 MAC，匿名集中的所有节点都使用相同的密钥来验证附加的 MAC。由于使用了对称加密技术，这种方法提供了高计算效率和低通信开销[8]。

在文献[9]中，Li 等人提出了一种利用 MAC 验证网络中数据包的方案，使用对称密钥生成 MAC，并由边缘设备（如路由器）验证这些 MAC，然后将消息的真实性传达给网络中的其他节点。在文献[10]中，Zhang 等人提出了类似的方案。相较于基于公钥基础设施（PKI）的椭圆曲线数字签名算法（ECDSA）和基于组签名的方案，Zhang 等人的方案实现了较低的通信开销，而 Li 等人的方案则在丢包率方面具有优势[9][10]。

此外，Chuang 等人提出的信任扩展身份验证机制和 Umar 等人提出的由物理不可克隆函数（PUF）支持的基于身份的轻量级身份验证协议都利用基本的加密操作（如 XOR 和哈希函数）来提高物联网网络的身份验证效率[10][11]。Chuang 等人特别采用了扩展信任关系的概念来提高认证过程中的性能[12][12][13]。

6. 基于非对称加密的方案

物联网中基于非对称加密的方案为每个设备配备了一个用于匿名通信的公钥-私钥对。设备使用其私钥生成数字签名，并将这些签名与相应的公钥证书附加到其消息中。接收方使用发送方的公钥验证消息，确保发送方的真实身份在整个通信过程中保持不公开[14]。

Schaub 等人提出了一种方案，该方案在不依赖假名和真实身份之间的映射的情况下实现问责制[15]。这种方法将身份信息直接嵌入到假名证书中，允许每个物联网设备携带自己的身份信息，从而增强可扩展性[16]。然而，该方案引入了与吊销假名证书相关的挑战。

7. 基于身份的加密方案

为了在物联网中开发更高效的通信和存储解决方案，研究人员利用基于身份的加密（IBE）技术来设计身份验证方案。Sun 等人提出了一种方案，该方案采用假名、阈值签名和阈值认证技术来实现物联网安全系统中的隐私保护。由于 IBE 系统无需证书，其方案占用的内存空间更少[17]。

在 IBE 系统的基础上，Zhang 等人引入了一种基于身份的一次性认证非对称组密钥协议，以安全地获取组密钥[18]。基于该协议，他们提出了 CMIX 协议来创建密码学混合区（CMIX），增强了网络对恶意窃听的抵抗力。在 CMIX 中，任何设备都可以充当组密钥分发器，而路由设备无法读取组密钥。因此，此方案不依赖于完全受信任的第三方实体[19][20][21]。

8. 基于身份的签名方案

在物联网中，基于身份的签名（IBS）方案使设备能够使用自己的身份信息作为公钥，并生成从此身份派生的私钥来签署消息。接收方可以使用发送方的身份信息验证这些签名，从而在验证过程中无需数字证书[22][23][24]。这种方法减少了通信开销并简化了密钥管理问题。

为了减少通信和存储开销，Shim 等人在计算 Diffie-Hellman 假设下提出了一种高效的条件隐私保护认证方案。在此方案中，网络节点可以同时验证大量接收到的消息[25]。HE 等人为物联网网络引入了一种高效的基于身份的条件隐私保护认证协议[26]。Zhang 等人提出了一种具有分层聚合和快速响应功能的隐私保护物联网通信认证协议[27]。两种协议都利用不同的技术来实现批量验证，从而减少通信和存储开销。Li 等人开发了一个有条件的隐私保护身份验证框架，该框架采用公钥加密技术来生成假名[28]。该框架使用现有的 IBS 和基于身份的在线/离线签名（IBOOS）方案来实现设备之间以及设备与服务器之间的匿名身份验证[29][30][31]。

9. 无证书签名方案

无证书签名方案缓解了基于身份的签名（IBS）系统中存在的密钥托管问题。Horng 等[32]提出了一种基于无证书短签名（CLSS）的物联网设备到基础设施（如路由器）通信的无证书聚合签名方案。该方案结合了无证书密码学和聚合签名的优点，实现了隐私性和可追溯性之间的平衡。它提供匿名身份验证、消息完整性和不可链接性。

Cui 等人提出了一种基于椭圆曲线密码学（ECC）的无证书聚合签名方案[33]。该方案确保物联网设备与网络基础设施之间的安全通信，并支持有条件的隐私保护。通过将来自设备的广播消息映射到假名身份来实现有条件的隐私；如有争议，当局可以从这些假名中检索真实身份[34][35][36]。

10. 基于群签名的方案

在基于群签名的方案中，允许有效的群管理员代表群成员对消息进行匿名签名，只有群管理员有能力确定谁是实际发送者，这能有效保护用户隐私，但其缺点是签名验证非常耗时，使得其不适用于物联网即时应用程序。Guo 等人提出了一种基于群签名技术的物联网隐私保护通信框架，该框架具有真实性、数据完整性、匿名性和可追责性[37]。此群签名方案中，攻击者可以轻松找到发送消息的群组，但无法跟踪消息的发送者[38][39]。

11. 去中心化的设备身份隐私技术

目前，为保护身份隐私，大部分方案基于已有的密码技术进行改进以实现假名性，但这些技术本身存在一些问题，例如基于对称加密的方案存在密钥分发繁杂、成本高的缺点，而基于非对称加密的方案具有计算代价高的缺点[40][41][42]。此外，密钥管理和证书吊销也是问题之一[43][44]。基于无证书签名的匿名认证技术具有无证书管理、系统轻量、通信开销低等优点，区块链则具备高安全性和不可篡改性，将无证书签名方案与区块链结合，有望实现更加适用于物联网的高效匿名身份认证方案[45]。

12. 自适应的假名变更技术

通过对匿名认证位置隐私的调查发现，基于 Mix-Context 的假名变更策略由物联网设备自行决定何时更改假名，与基于 Mix-Zone 的假名变更策略只能在固定位置更改假名相比，前者的灵活性更高，但其存在过分依赖中心设备的情况[46][47][48]。在设备密度较高时，频繁的假名变更可能会降低物联网网络的性能。未来的研究可以针对不同设备密度场景，研究出自适应的基于 Mix-Context 的假名变更技术[49][50][51]。

（三）主要参考资料（格式参照《海南大学研究生学位论文撰写规范》

[1] 物联网安全标准化白皮书(2019 版)[C]//《互联网文档资源（https://max.book118.）》, 2019.

[2] 闫宏强, 王琳杰. 物联网中认证技术研究[J]. 通信学报, 2020, 51(7):213–222.

[3] Wazid M, Das A K, Odelu V, et al. Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment[J]. IEEE Trans. Dependable Secur. Comput., 2020, 17(2):391–406.

[4] Z. Yang, J. He, Y. Tian, and J. Zhou, "Faster authenticated key agreement with perfect forward secrecy for industrial internet-of-things," IEEE Trans. Ind. Informatics., vol. 16, no. 10, pp. 6584–6596, 2020.

[5] S. A. Sheik and A. P. Muniyandi, "Secure authentication schemes in cloud computing with glimpse of artificial neural networks: A review," Cyber Security and Applications, vol. 1, p. 100002, 2023.

[6] 田艳昭.基于图论的口令安全机制研究[D].北京邮电大学,2022.DOI:10.26969/d.cnki.gbydu.2022.000245.

[7] C. Wang, D. Wang, Y. Tu, G. Xu, and H. Wang, "Evaluating the node capture attack in user authentication scheme of wireless sensor networks," IEEE Trans. Depend. Secur. Comput., vol. 19, no. 1, pp. 507–523, 2022.

[8] D. S. Gupta, S. H. Islam, M. S. Obaidat, P. Vijayakumar, N. Kumar, and Y. Park, "A provably secure and lightweight identity-based two-party authenticated key agreement protocol for iiot environments," IEEE Syst. J., vol. 15, no. 2, pp. 1732–1741, 2021.

[9] X. Li, T. Liu, M. S. Obaidat, F. Wu, P. Vijayakumar, and N. Kumar, "A lightweight privacy-preserving authentication protocol for vanets," IEEE Syst. J., vol. 14, no. 3, pp. 3547–3557, 2020.

[10] X. Li, J. Peng, M. S. Obaidat, F. Wu, M. K. Khan, and C. Chen, "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems," IEEE Syst. J., vol. 14, no. 1, pp. 39–50, 2020.

[11] M. Fotouhi, M. Bayat, A. K. Das, H. A. N. Far, S. M. Pournaghi, and M. Doostari, "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care iot," Comput. Networks., vol. 177, p. 107333, 2020.

[12] J. Srinivas, A. K. Das, M. Wazid, and A. V. Vasilakos, "Designing secure user authentication protocol for big data collection in iot-based intelligent transportation system," IEEE

Internet Things J., vol. 8, no. 9, pp. 7727–7744, 2021.

[13] F. Wu, X. Li, L. Xu, P. Vijayakumar, and N. Kumar, "A novel three-factor authentication protocol for wireless sensor networks with iot notion," IEEE Syst J, vol. 15, no. 1, pp. 1120–1129, 2021.

[14] F. G. Darbandeh and M. Safkhani, "SAPWSN: A secure authentication protocol for wireless sensor networks," Comput. Networks, vol. 220, p. 109469, 2023.

[15] K. Mahmood, J. Ferzund, M. A. Saleem, S. Shamshad, A. K. Das, and Y. Park, "A provably secure mobile user authentication scheme for big data collection in iot-enabled maritime intelligent transportation system," IEEE Trans. Intell. Transp. Syst., vol. 24, no. 2, pp. 2411–2421, 2023.

[16] Q. Zhang, J. Wu, H. Zhong, D. He, and J. Cui, "Efficient anonymous authentication based on physically unclonable function in industrial internet of things," IEEE Trans. Inf. Forensics Secur., vol. 18, pp. 233– 247, 2023.

[17] G. Sharma and S. Kalra, "Advanced lightweight multi-factor remote user authentication scheme for cloud-iot applications," J. Ambient. Intell. Humaniz Comput., vol. 11, no. 4, pp. 1771–1794, 2020.

[18] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," IEEE Trans. Dependable. Secur. Comput., vol. 17, no. 2, pp. 391–406, 2020

[19] J. Srinivas, A. K. Das, M. Wazid, and N. Kumar, "Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial internet of things," IEEE Trans. Dependable. Secur. Comput., vol. 17, no. 6, pp. 1133–1146, 2020.

[20] W. Wang, C. Qiu, Z. Yin, G. Srivastava, T. R. Gadekallu, F. Alsolami, and C. Su, "Blockchain and puf-based lightweight authentication protocol for wireless medical sensor networks," IEEE Internet Things J., vol. 9, no. 11, pp. 8883–8891, 2022.

[21] S.K. Jha, S. Prakash, R.S. Rathore, M. Mahmud, O. Kaiwartya, J. Lloret, Qualityof-service-centric design and analysis of unmanned aerial vehicles, Sensors 22 (15) (2022) 5477.

[22] Luo R, Jin H, He Q, Wu S, Xia X (2023) Enabling balanced data deduplication in mobile edge computing. IEEE Trans Parallel Distrib Syst 34(5):1420–1431

[23] Khanh QV, Nguyen VH, Minh QN, Van AD, Le Anh N, Chehri A (2023) An efcient edge computing management mechanism for sustainable smart cities. Sustain Comput Inf Syst 38(100):867

[24] Zheng X, Li M, Shah SBH, Do DT, Chen Y, Mavromoustakis CX, Mastorakis G, Pallis E (2022) Enhancing security-problem-based deep learning in mobile edge computing. ACM Trans Internet Technol 22(2):1–15

[25] Mahmood K, Ayub MF, Hassan SZ, Ghafar Z, Lv Z, Chaudhry SA (2022) A seamless anonymous authentication protocol for mobile edge computing infrastructure. Comput Commun 186:12–21

[26] Saqib M, Moon AH (2023) A systematic security assessment and review of internet of things in the context of authentication. Comput Secur 125:103053.

[27] C. Wang, D. Wang, Y. Duan and X. Tao, "Secure and Lightweight User Authentication Scheme for Cloud-Assisted Internet of Things," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2961-2976, 2023, doi: 10.1109/TIFS.2023.3272772.

[28] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, “Challenges and opportunities in securing the Industrial Internet of Things,” IEEE Trans. Ind. Informat., vol. 17, no. 5, pp. 2985–2996, May 2021.

[29] D. Kandris, C. Nakas, D. Vomvas, and G. Koulouras, “Applications of wireless sensor networks: An up-to-date survey,” Appl. Syst. Innov., vol. 3, no. 1, p. 14, 2020.

[30] B. Baruah and S. Dhal, “An efficient authentication scheme for secure communication between Industrial IoT devices,” in Proc. 11th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT), 2020, pp. 1–7.

[31] F. Wu, X. Li, L. Xu, P. Vijayakumar, and N. Kumar, “A novel three-factor authentication protocol for wireless sensor networks with IoT notion,” IEEE Syst. J., vol. 15, no. 1, pp. 1120–1129, Mar. 2021.

[32] Y. Su, X. Zhang, J. Qin, and J. Ma, “Efficient and flexible multiauthority attribute-based authentication for IoT devices,” IEEE Internet Things J., vol. 10, no. 15, pp. 13945–13958, Aug. 2023.

[33] M. Tanveer, A. Alkhayyat, A. U. Khan, N. Kumar, and A. G. Alharbi, “REAP-IIoT: Resource-efficient authentication protocol for the Industrial Internet of Things,” IEEE Internet Things J., vol. 9, no. 23, pp. 24453–24465, Dec. 2022.

[34] Y. Zhang, D. He, P. Vijayakumar, M. Luo, and X. Huang, “SAPFS: An efficient symmetric-key authentication key agreement scheme with perfect forward secrecy for Industrial Internet of Things,” IEEE Internet Things J., vol. 10, no. 11, pp. 9716–9726, Jun. 2023.

[35] Y. Chen et al., “ECC-based authenticated key agreement protocol for industrial control

system," IEEE Internet Things J., vol. 10, no. 6, pp. 4688–4697, Mar. 2023.

[36] H. Abdi Nasib Far, M. Bayat, A. Kumar Das, M. Fotouhi, S. M. Pournaghi, and M.-A. Doostari, "LAPTAS: Lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT," Wireless Netw., vol. 27, pp. 1389–1412, Jan. 2021.

[37] M. Shuai, L. Xiong, C. Wang, and N. Yu, "A secure authentication scheme with forward secrecy for Industrial Internet of Things using Rabin cryptosystem," Comput. Commun., vol. 160, pp. 215–227, Jul. 2020.

[38] R. Vinoth, L. J. Deborah, P. Vijayakumar, and N. Kumar, "Secure multifactor authenticated key agreement scheme for Industrial IoT," IEEE Internet Things J., vol. 8, no. 5, pp. 3801–3811, Mar. 2021.

[39] F. Rafique, M. S. Obaidat, K. Mahmood, M. F. Ayub, J. Ferzund, and S. A. Chaudhry, "An efficient and provably secure certificateless protocol for Industrial Internet of Things," IEEE Trans. Ind. Informat., vol. 18, no. 11, pp. 8039–8046, Nov. 2022.

[40] D. Xu, K. Yu, and J. A. Ritcey, "Cross-layer device authentication with quantum encryption for 5G enabled IIoT in industry 4.0," IEEE Trans. Ind. Informat., vol. 18, no. 9, pp. 6368–6378, Sep. 2022.

[41] Y. Zhang, B. Li, J. Wu, B. Liu, R. Chen, and J. Chang, "Efficient and privacy-preserving blockchain-based multifactor device authentication protocol for cross-domain IIoT," IEEE Internet Things J., vol. 9, no. 22, pp. 22501–22515, Nov. 2022.

[42] X. Liu, M. Wang, T. Wang, and R. Zhang, "A blockchain assisted multigateway authentication scheme for IIoT based on group," Peer-to-Peer Netw. Appl., vol. 16, no. 1, pp. 245–259, Jan. 2023.

[43] Xiao Chen, BaoCheng Wang, Haibin Li, A privacy-preserving multi-factor authentication scheme for cloud-assisted IoMT with post-quantum security, Journal of Information Security and Applications, Volume 81, 2024, 103708, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2024.103708.

[44] Wang C, Wang D, Xu G, et al. Efficient privacy-preserving user authentication scheme with forward secrecy for industry 4.0. Sci China Inf Sci, 2022, 65: 1–15

[45] Blanchet B, Smyth B, Cheval V, et al. Proverif 2.02 pl1: Automatic cryptographic protocol verifier, user manual and tutorial. 2020

[46] Vinoth R,Deborah L, Vijayakumar P, et al. Secure multi-factor authenticated key agreement

scheme for industrial iot. IEEE Internet Things J, 2021, 8: 3801–3811

[47] Masud M, Alazab M, Choudhary K, et al. 3psake: Privacy-preserving and physically secured authenticated key establishment protocol for wireless industrial networks. Comput Commun, 2021, 175: 82–90

[48] Garg S, Kaur K, Kaddoum G, et al. Toward secure and provable authentication for internet of things: Realizing industry 4.0. IEEE Internet Things J, 2020, 7: 4598–4606

[49] Zhang Y, He D, Vijayakumar P, et al. SAPFS: An Efficient Symmetric-Key Authentication Key Agreement Scheme with Perfect Forward Secrecy for Industrial Internet of Things. IEEE Internet Things J, 2023. DOI: 10.1109/JIOT.2023.3234178

[50] Zou S, Cao Q, Wang C, et al. A robust two-factor user authentication scheme-based ecc for smart home in iot. IEEE Syst J, 2022, 16: 4938–4949

[51] W. Li, H. Cheng, P. Wang, and K. Liang, “Practical threshold multifactor authentication,” IEEE Trans. Inf. Forensic Secur., vol. 16, pp. 3573–3588, 2021.

二、研究内容

（一）研究的主要内容 （摘要式描述）

本研究主要探讨并设计一种适用于物联网（IoT）环境的轻量级多因素认证方案，旨在提供密码泄漏检测的有效机制，图 1 所示为本方案的初步架构，包括云服务器、用户智能设备以及物联网设备，图 2 为 PUF 生成响应对的示例。

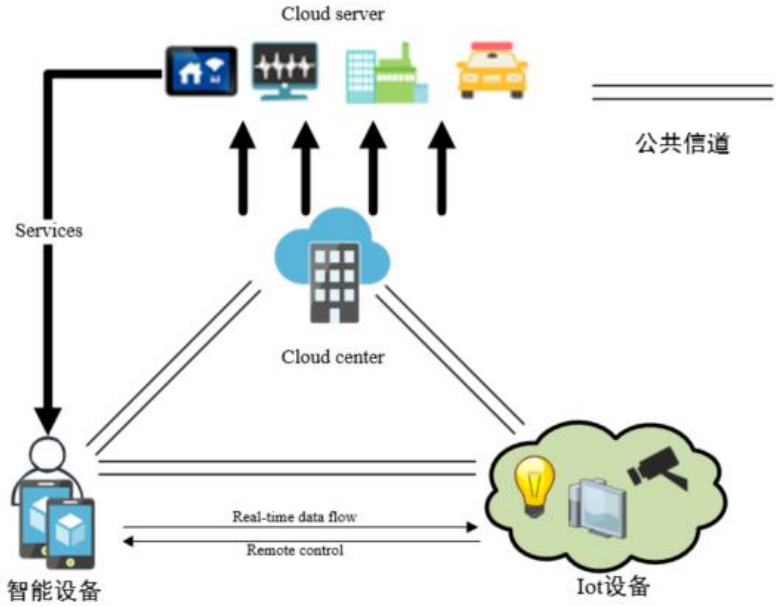

图 1.云辅助的物联网架构

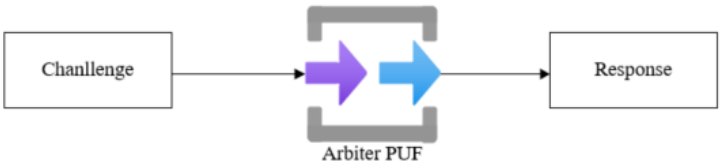

图 2.Arbiter PUF 示例

研究的主要内容包括以下方面：

多因素认证机制设计：结合密码、生物特征（如指纹）和物理不可克隆函数（PUF）等多因素，增强用户身份验证的安全性。该方案通过多层次验证因子保障系统在个别因子泄露的情况下仍然具备足够的安全性。

密码泄漏检测机制：引入蜜语（Honeywords）技术，将多个虚假密码与真实密码共同存储，模拟真实密码分布以迷惑攻击者。同时利用零因子图序列优化蜜语生成，使其更符合实际密码的使用频率，提升检测的准确性。

基于图论的密码保护：借助拓扑图形序列和零因子图理论，设计出具有高平坦度和随机性的蜜语生成机制，确保蜜语在分布上更具多样性，进一步增加攻击难度。通过拓扑图和零因子图的应用，使蜜语的排列方式更加复杂，提高方案的防护性能。

轻量化实现策略：针对 IoT 设备的资源受限特性，研究适合在设备上高效运行的轻量级认证与检测算法。方案通过分布式计算和云协作机制将部分计算任务转移至云端，减轻 IoT 设备的计算负担，同时保持高效的认证和检测性能。

安全性分析与性能评估：对该方案进行理论分析，验证其在抗攻击、检测密码泄漏和保护隐私数据方面的有效性。通过实验评估方案在多种攻击场景下的表现，以确保其具备低计算开销的同时，能够满足 IoT 环境的安全需求。

本研究的最终目标在于设计一种能够有效检测密码泄漏、适用于 IoT 设备的高效认证方案，为物联网环境中的身份认证安全提供理论支持和实现路径。

（二）研究的主要框架结构（原则上要求列出三级标题）

（三）可能的创新之处

1. 通过基于 PUF 的物联网（IoT）认证方案，可能实现设备之间无需完全依赖中心化密钥分发机构的相互认证。利用 PUF 特性，IoT 设备能够直接进行身份验证，从而减少了对中心化信任的依赖，提升了系统的容错性和可扩展性。这种去中心化的认证架构允许设备与多方之间直接建立可信连接，同时支持自适应和低延迟的认证机制，使其更适合 IoT 环境的复杂需求。

2. 用户设备密码安全以及 IoT 设备密码安全

在用户端，采用蜜语（Honeyword）方法保护密码，将多个虚假密码与真实密码一同存储在服务器数据库中，以迷惑潜在攻击者。用户实际的登录凭证与蜜语混合存储，一旦攻击者尝试使用蜜语登录，系统会立刻产生警报并采取防护措施。这种方法不仅提高了密码存储的安全性，还通过增加蜜语的平坦度，使其难以与真实密码区分，从而有效地增加了密码泄漏检测的准确性和防护效果。

在设备端，利用物理不可克隆函数（PUF）技术进行身份认证，从而实现“无密码存储”保护。设备通过 PUF 的物理特性生成独特的挑战-响应对，每次认证时由服务器向设备发送一个挑战，设备通过 PUF 计算出相应的响应，用于身份验证。这种方式避免了在设备端或服务器上存储静态密码，降低了密码泄露和被攻击的风险。通过 PUF 动态生成的认证响应，设备在认证过程中不依赖于存储的密码，进一步防止了物理攻击和凭证盗窃，显著增强了认证过程的安全性与设备隐私保护能力

3. 自适应的假名变更方案

在设计中，可以通过 PUF 生成的响应和认证密钥动态更新，有机会实现一次性身份认证，从而避免了设备身份的固定暴露，显著增强了隐私保护能力。每次通信时，PUF 可动态生成新的挑战-响应对，用于生成不同的密钥或身份凭证，有效抵御重放攻击和中间人攻击，提升了物联网设备在通信过程中的安全性和隐私性。这种基于 PUF 的自适应认证方式，兼顾了高效性与隐私保护，具备在多设备物联网环境中应用的广泛潜力。

（四）需要重点解决的问题

1.如何更好的将物联网设备信息与 PUF 响应结合起来？

2.如何降低中性化服务器的依赖？

（五）预期研究成果

提出一种新的具有密码泄漏检测的 IoT 轻量级多因素认证方案，并发表至少一篇学术论文。

三、研究进展计划

（一）研究的方法、技术方案、实验方法

一、研究的方法

1. 文献综述和现有方案分析

通过系统性文献回顾，分析当前在 IoT 认证方案中的密码保护、多因素认证和轻量级算法等方面的研究进展。针对不同方案的安全性、资源开销、用户体验等方面进行横向比较，识别当前方案的局限性，并从中提炼出设计改进的需求。

2. 威胁建模与安全需求分析

建立 IoT 环境的威胁模型，分析可能的攻击类型（如重放攻击、中间人攻击、暴力破解等），明确认证方案需应对的安全需求。针对 IoT 设备的多样性、低资源特性和分布式架构，提出具体的安全性和效率指标。

二、技术方案

1. 基于蜜语的密码泄漏检测技术

设计蜜语（Honeywords）生成机制，将虚假密码与真实密码混合存储，确保密码泄漏后能够及时检测。利用齐夫定律生成虚假密码，以匹配真实密码的分布特征，从而增加蜜语的欺骗性与检测准确性。

2. 物理不可克隆函数（PUF）技术的应用

在设备端部署 PUF，利用其物理特性生成独特的认证响应，避免静态密码存储带来的泄露风险。研究如何通过 PUF 生成动态的挑战-响应对，实现无密码存储的安全认证，并在每次通信时更新身份凭证，有效抵御重放攻击和中间人攻击。

3. 多因素认证设计

结合多因素认证（如密码、生物特征、PUF 响应），实现分层验证，确保即使部分因子泄露，系统仍能保持高安全性。设计轻量级的多因素认证协议，以满足 IoT 设备的低计算和低功耗需求。

4. 轻量级协议与算法优化

针对 IoT 设备的资源限制，优化认证协议中的加密、哈希和密钥生成算法，降低计算和通信开销。通过分布式计算和边缘协作，将部分认证计算转移至边缘节点或云端，减轻设备端负担。

5. 去中心化与动态密钥管理

研究如何基于 PUF 实现设备间的直接认证，减少对中心化密钥分发机构的依赖，

增强系统的容错性与扩展性。设计动态密钥生成和更新机制，通过挑战-响应动态生成认证密钥，确保密钥安全性和更新灵活性。

三、实验方法

1. 模拟实验与仿真分析

在仿真环境中搭建 IoT 认证架构，模拟不同攻击场景（如密码泄漏、重放攻击等），测试认证方案的抗攻击能力和检测响应速度。

在不同的仿真平台（如 NS3、OMNeT++）中模拟真实 IoT 环境，通过对计算开销、通信延迟等关键性能指标的分析评估方案的资源效率。

2. 基准测试与性能评估

针对认证方案的安全性、认证速度、能耗等进行基准测试，并与现有方案对比，分析其优势与不足。使用低功耗设备（如 Raspberry Pi、Arduino）测试协议在实际设备上的性能，重点关注 PUF 实现的响应时间和蜜语检测的准确率。

3. 安全分析与验证

使用形式化验证工具（如 ProVerif、Scyther）对认证协议的安全性进行形式化分析，验证方案对重放攻击、中间人攻击等常见威胁的防护能力。结合安全建模和动态检测分析，测试方案在不同场景下的故障恢复与自适应响应能力。

4. 消耗分析与能效评估

在实验平台上对不同算法（如 PUF 生成、蜜语生成和动态密钥管理）的能耗和计算消耗进行详细测量，确保其满足 IoT 设备的资源限制要求。通过模拟不同功耗模式，优化协议的能效，确保在能耗受限的环境中实现高效认证。

（二）可能遇到的困难或问题及解决方案

1.如何更好的将物联网设备信息与 PUF 响应结合起来？

可以引入缓存机制，针对频繁认证的场景，可以引入短期缓存机制，缓存设备最近的 PUF 响应-设备 ID 组合，减少重复认证的计算负担，同时加速多次认证过程。

2.如何降低中性化服务器的依赖？

可以通过分布式密钥生成与管理，利用设备之间的互信关系，通过分布式密钥生成协议，让多个设备共同生成并管理认证密钥。可通过去中心化密钥协商协议在设备之间直接生成共享密钥，减少对中心服务器的密钥依赖。或者利用 PUF 特性，支持设备间的直接认证。例如，每个设备可将自身的 PUF 响应与其他设备的挑战进行计算，直接实现相互认证，减少对中心服务器的单一依赖。

（三）时间安排（研究进度安排）

起止时间	主要研究内容
2024.09-2024.12	对 PUF、Honeyword 技术以及 IoT 设备数据安全共享进行总结，确定技术细节
2025.01-2025.03	学习具有密码泄漏检测的 IoT 轻量级多因素认证相关知识，确定方案所需要的技术。
2025.03-2025.07	学习掌握多因素认证的 IoT 设备数据共享方法，设计具有密码泄漏检测的 IoT 轻量级多因素认证方案。
2025.08-2025.12	实现面向 IoT 具有密码泄漏检测机制的设备多因素认证方案
2026.01-2026.05	文档整理，撰写毕业论文

四、保障条件

（一）本人已经或正在进行的相关研究工作

前期已对国内外研究做了足够的调研，从多个维度分析现有研究的优缺点，对于 V2X 方案已经非常的熟悉，同时也对加密方案的编写有了一定的熟悉和了解，对于 PUF 以及车联网隐私保护技术已经阅读过多篇论文。下面是已经做的工作：

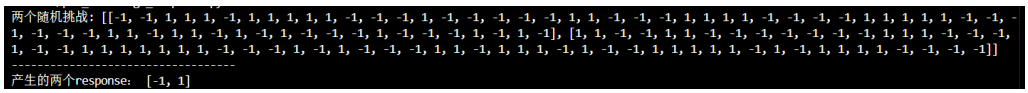

图 3.模拟 Arbiter-PUF 生成挑战响应对

图 3 为输入两个随机挑战，通过 PUF 模拟生成对应的两个响应对

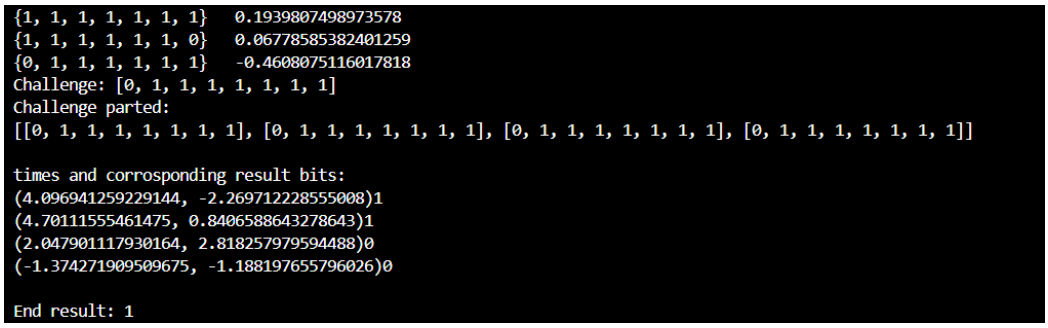

图 4.响应对的时延值与时间差的符号

图 4 为生成挑战响应对的的时延值与输出结果，可以看出模拟相同的 challenge 时延值不同，满足不同的 PUF 设备输入相同输出不同的结果。

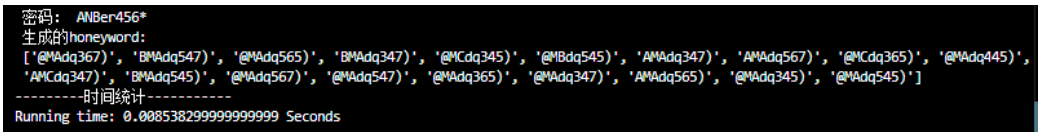

图 5.三元零因子图序列生成 Honeyword 示例

图 5 为以 ANBer456*为密码利用三元零因子图序列生成 Honeyword 的示例以及生成的时间开销，可见生成的 Honeyword 平坦度较优，生成快速。

（二）实验条件、图书资料及调研条件

学校在密码学、信息安全、网络通信和计算机科学等领域拥有丰富的图书资源，校图书馆藏有大量科技资料，并订购了多种国际知名电子数据库。这些资源为本课题的文献研究、数据收集和分析提供了良好的支持，有助于获取、整理和分析现有的信息和数据，以形成对研究领域的全面了解。

（三）研究所需经费来源

导师课题经费

指导教师审阅意见：

陈伟同学的开题报告题目为“面向 IoT 设备具有密码泄露检测机制的多因素认证方案”，针对 IoT 设备的认证问题，拟提出一种具有密码泄露检测的认证方案。开题报告内容完整，研究背景调研充分，反映出该同学对物联网设备安全需求有很好的理解。该同学在文献综述部分对相关研究进展做了较为全面的梳理，为后续研究展开奠定了基础。

开题报告中提出的技术方案和实验方法具有一定可行性，并在多因素认证与密码泄露检测的结合上有所创新。项目的预期成果符合学院的毕业要求，研究计划合理，目标明确。

综上所述，陈伟同学的开题报告准备充分，符合开题要求。我同意该同学开题。

指导教师签名：

年　月　日

开题报告评审小组意见（简要评议意见）：

□同意开题　□同意修改后开题　□不同意开题

组长签章：

年　月　日

学院审核意见：

盖　章：

年　月　日