ESCI, EI 等数据库收录期刊

ISSN 1009-5896
CODEN DKXUEC
CN 11-4494/TN

电子与信息学报

JOURNAL OF ELECTRONICS & INFORMATION TECHNOLOGY

5

2024. Vol.46

45 YEARS

1979-2024

《电子与信息学报》创刊四十五周年专刊

Special Issue on the 45th Anniversary of JEIT

科学出版社

电子与信息学报

Dianzi Yu Xinxi Xuebao

（月刊，1979年1月创刊）

第46卷 第5期，2024年5月

Journal of Electronics & Information Technology

(Monthly, Started in Junuary 1979)

Vol.46 No.5 May 2024

主　　管	中国科学院
主　　办	中国科学院空天信息创新研究院
编　　辑	《电子与信息学报》编辑部 信址：北京2702信箱学报编辑部 地址：北京市北四环西路19号（邮政编码：100190） 电话：010-58887066 http://jeit.ac.cn E-mail: jeit@mail.ie.ac.cn
主　　编	付　琨
编辑部主任	陈　倩
出　　版	中国科技出版传媒股份有限公司 地址：北京东黄城根北街16号 邮政编码：100717
印刷装订	北京科信印刷有限公司
总 发 行	中国科技出版传媒股份有限公司 地址：北京东黄城根北街16号 邮政编码：100717 电话：010-64017032 E-mail: journal@mail.sciencep.com
国外发行	中国国际图书贸易总公司 地址：北京399信箱 邮政编码：100044

Supervised by	Chinese Academy of Sciences
Sponsored by	Aerospace Information Research Institute, Chinese Academy of Sciences and Department of Information Science
Edited by	Editorial Department of Journal of Electronics & Information Technology P. O. Box 2702, Beijing 100190, China Telephone: 010-58887066 http://jeit.ac.cn E-mail: jeit@mail.ie.ac.cn
Editor-in-Chief:	FU Kun
Editorial Director:	CHEN Qian
Published by	Science Press No.16 Donghuangchenggen North Street, Beijing 100717, China
Printed by	Beijing Kexin Printing Co., Ltd.
Distributed by	Science Press No.16 Donghuangchenggen North Street, Beijing 100717, China Telephone: 010-64017032 E-mail: journal@mail.sciencep.com
Overseas distribution:	China International Book Trading Corporation P. O. Box 399, Beijing 100044, China

国内统一连续出版物号：CN 11-4494/TN　　国内邮发代号：2-179　　国外发行代号：M412　　定价：80.00元

国 内 外 公 开 发 行

ISSN 1009-5896

9 771009 589247 05>

支持商密SM9算法框架的多因素认证方案

朱留富 汪 定*

①(南开大学网络空间安全学院 天津 300350)

②(天津市网络与数据安全技术重点实验室 天津 300350)

③(数据与智能系统安全教育部重点实验室 天津 300350)

摘 要：无线传感器技术使用公开无线信道且存储和计算资源受限，这使其容易遭受潜在的主动攻击(篡改等)和被动攻击(监听等)。身份认证是保障信息系统安全的第一道防线，如何为无线传感器设备设计多因素认证方案是目前安全协议研究的热点。目前，大多数身份认证方案都基于国外密码标准设计，不符合国家核心技术自主可控的网络空间安全发展战略。商密SM9标识密码算法是中国密码标准，已由ISO/IEC标准化并被广泛使用。因此，该文研究如何在商密SM9标识密码算法框架下，将口令、生物特征以及智能卡相结合来设计多因素身份认证方案，并利用模糊验证技术和蜜罐口令方法增强口令安全。该文在随机谕言模型(Random Oracle Model, ROM)下证明了方案的安全性，并给出启发式安全分析。与相关身份认证方案的对比结果表明，该文提出的身份认证方案在提供安全性的同时能够适用于资源受限的无线传感器网络。

关键词：多因素认证；国产密码；随机谕言模型

中图分类号：TN918.2 **文献标识码**：A **文章编号**：1009-5896(2024)05-2137-12

DOI: 10.11999/JEIT231197

A Multi-Factor Authentication Scheme Under the SM9 Algorithm Framework

ZHU Liufu WANG Ding

①(*College of Ciber Science*, *Nankai University*, *Tianjin* 300350, *China*)

②(*Tianjin Key Laboratory of Network and Data Security*, *Nankai University*, *Tianjin* 300350, *China*)

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

Abstract: Wireless sensor networks use public wireless channels and their storage and computing resources are limited, making them vulnerable to active attacks and passive attacks. Identity authentication acts as the first line to ensure the security of information systems. Then, how to design multi-factor authentication schemes for wireless sensor devices is currently a hot topic. Nowadays, most existing schemes are based on foreign cryptographic standards that do not comply with the autonomous and controllable cyberspace security development strategy. SM9 is an identity-based cryptographic algorithm that has become a Chinese cryptographic standard recently. Therefore, this paper focuses on how to combine passwords, biometrics, and smart cards to design a multi-factor authentication scheme that can be used for wireless sensor networks under the framework of SM9. The proposed scheme applies the fuzzy verifier technique and the honeyword method to resist password guessing attacks and further enables session key negotiation and password update. The security is proved under the Random Oracle Model (ROM) and a heuristic security analysis is provided additionally. The comparison results show that the proposed scheme can be deployed to wireless sensor networks.

Key words: Multi-factor authentication; Chinese cryptographic standard; Random oracle model

收稿日期：2023-10-31；改回日期：2023-12-20；网络出版：2024-05-02

*通信作者： 汪定 wangding@nankai.edu.cn

基金项目：京津冀基础研究合作专项(21JCZXJC00100)，国家自然科学基金 (62222208)，天津市自然科学基金重点项目(21JCZDJC00190)

Foundation Items: The Natural Science Foundation of Tianjin, China (21JCZXJC00100), The National Natural Science Foundation of China (62222208), The Natural Science Foundation of Tianjin, China (21JCZDJC00190)

1 引言

无线传感器技术的发展已经深刻改变了社会生活和生产方式，被广泛用于工业、农业以及国防等领域。无线传感器技术具有开放性、设备异构性以及设备轻量级等特点，因此如何保障通信用户的真实性、传输数据的准确性、防止资源被非法访问，确保无线传感器网络的可用性，是无线传感器技术面临的严峻挑战。

身份认证[1–5]是保障通信网络的重要安全技术，在验证用户身份时，通常包含3类认证信息：用户已知信息，如口令；用户生物特征，如指纹；用户拥有的物理设备，如智能卡。多因素认证方案使用两种及以上的认证因素验证用户，只有当用户满足所有认证条件时才能获得系统授权。2004年，Watro等人[6]将口令和智能卡作为认证因素首次提出适用于无线传感器网络的多因素认证方案，确保只有合法用户才能访问传感器节点中的实时数据。然而，Das[7]指出文献[6]无法抵抗口令猜测攻击和智能卡泄露攻击，进而提出一个新的多因素认证方案支持用户远程登录和访问传感器节点。但Huang等人[8]指出文献[7]无法抵抗内部攻击和口令猜测攻击，并构造了一个可以抵抗离线口令猜测攻击和内部攻击的多因素认证方案。

但文献[6–8]没有考虑用户匿名性，Wang等人[9]分析了认证方案中实现用户隐私保护设计原则，并给出了一个提供用户匿名性保护的认证方案。进一步，Sadri等人[10]利用哈希承诺算法隐藏用户标识提出一种具有匿名性的多因素认证方案，该方案提供口令更新功能。但文献[10]假设本地物理设备是安全的，Alladi等人[11]指出对本地物理设备的攻击会造成传感器节点篡改和替换攻击，因此他们提出一种基于物理不可克隆函数的认证方案，增强了本地设备的安全性。而随着量子计算技术的发展，传统的认证方案可能无法抵抗量子计算的攻击，Jiang等人[12,13]利用基于哈希的抗量子算法提出多因素认证方案从而获得后量子安全。

上述方案假设用户的注册信息可以在安全信道中传输。然而，在网络系统中部署安全信道需要消耗宝贵的网络资源，增加了方案部署和应用的难度；因此，如何构造基于公开信道的多因素认证需要进一步研究。

由于缺少系统性评价指标和评估方法，设计认证方案经常陷入“攻破-改进-再攻破-再改进”的循环。2018年，Wang等人[14]分析了多因素认证方案的安全性，给出了衡量其安全性的系统性评价指标，并为构造多因素认证方案提供了形式化设计原则。为进一步完善该评价体系，2023年，Wang等人[15]又给出认证方案形式化安全证明的缺陷并给出分析认证方案安全性证明的评价指标。

上述多因素认证方案大多基于国外密码技术标准构造，若国外密码算法标准存在陷门，将给个人、企业甚至国家造成极大的安全威胁，不符合国家网络空间安全核心技术自主可控的发展战略。商密SM9是我国自主设计的基于标识密码算法的中国商用密码学标准，包括加密、密钥封装、密钥协商以及数字签名算法。2019年，Cheng[16]给出了商密SM9加密算法和密钥协商算法的安全性分析和形式化证明。2021年，赖建昌等人[17]分析了商密SM9数字签名算法和密钥封装算法的安全性，并给出了形式化证明。由于商密SM9密码算法需要使用椭圆曲线上的配对运算，增加了运算的复杂度。2022年，Lai等人[18]利用在线/离线签名技术，构造了可离线计算的商密SM9数字签名方案，减少了在线签名算法的开销。为了提供数据机密性，赖建昌等人[19]提出了基于商密SM9的广播加密方案，并在随机谕言模型下证明方案具有CCA安全。

由文献[15]可知，使用公钥密码算法可以提高多因素认证方案的安全性。而公钥算法中的密码操作具有较高的计算代价，如幂运算、配对运算等。因此，如何在应用公钥算法的同时降低计算开销是亟需解决的问题。在商密SM9密码算法扩建下构造多因素认证方案的需要研究如何将商密SM9密码算法与认证因素相结合，在提高认证方案的安全性的同时又可以保证方案的效率。

尽作者所知，尚未发现在商密SM9密码算法框架下设计安全高效多因素认证方案，本文提出了首个基于商密SM9的多因素认证方案(Multi-Factor Authentication Scheme Based on SM9, MFAS-SM9)，解决了多因素认证方案国产化、避免使用安全信道以及防止口令猜测攻击等现实挑战，核心贡献如下：

(1) 基于商密SM9密码算法框架构造多因素认证方案，将口令、生物特征以及智能卡作为认证因素，提高了认证的安全性和可靠性，符合国家核心技术自主可控的发展战略；

(2) 在用户注册和登录认证阶段避免使用安全信道，因此，所有数据都可在公开信道传输并保障内容的机密性；具有自主的口令更新功能，不需要与认证网关交互，用户在本地就能实现口令更新；使用模糊验证和蜜罐口令技术，可以削弱离线口令猜测攻击和在线口令猜测攻击。同时，蜜罐口令技术也可以作为口令更新的触发机制，当错误登录次数超过门限值时，用户需要更新原始口令；

(3) 在随机谕言模型(ROM)中给出了方案安全性的形式化证明，并进一步通过启发式方法分析方案的安全性；实验对比结果表明，本文方案适用于无线传感器网络。

2　预备知识

本节介绍文中使用的背景知识，包括商密SM9数字签名算法、商密SM9密钥封装算法、模糊验证技术、模糊提取函数、敌手模型以及方案评价指标。

2.1　商密SM9数字签名算法框架

商密SM9数字签名算法包含设置、密钥生成、签名以及验证4个算法。

设置　给定安全参数λ，密钥生成中心选取椭圆曲线群$(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_\mathrm{T},\mathrm{e},p)$，其中$e$为双线性映射：$\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_\mathrm{T}$；$p$为大素数，满足$p>2^\lambda$；随机选取群$\mathbb{G}_1$的生成元$P_1$，群$\mathbb{G}_2$的生成元$P_2$，存在同构映射$P_1=\psi(P_2)$；选取两个密码学杂凑函数$H_1:\{0,1\}^*\times\mathbb{Z}_p^*\to\mathbb{Z}_p^*$，$H_2:\{0,1\}^*\times\mathbb{Z}_p^*\to\mathbb{Z}_p^*$，并随机选取$\alpha\in\mathbb{Z}_p^*$，其中$\mathbb{Z}_p^*=\{1,2,\cdots,p-1\}$；计算群$\mathbb{G}_2$中的元素$P_{\mathrm{pub}}=\alpha P_2$和群$\mathbb{G}_\mathrm{T}$中的元素$g=e(P_1,P_{\mathrm{pub}})$；此外，随机选取长度为1 Byte的函数识别符hid。输出公开参数$\mathrm{params}=\{\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_\mathrm{T},e,p,P_1,P_2,P_{\mathrm{pub}},H_1,H_2,\mathrm{hid}\}$，保留主密钥$\mathrm{msk}=\alpha$。

密钥生成　输入用户标识$\mathrm{ID}\in\{0,1\}^*$，主密钥msk，密钥生成中心计算用户密钥$\mathrm{sk_{id}}=\dfrac{\alpha}{H_1(\mathrm{ID}\parallel\mathrm{hid},p)+\alpha}P_1$。

签名　输入消息$M\in\{0,1\}^*$，签名者标识ID以及密钥$\mathrm{sk_{id}}$，签名者随机选取$r\in\mathbb{Z}_p^*$，计算$w=g^r$，$h=H_2(M||w,p)$，$l=(r-h)\bmod p$；若$l=0$，则重新选取r并计算；否则，继续计算$S=l\mathrm{sk_{id}}$。最后，输出消息签名对(M,σ)，其中$\sigma=(h,S)$。

验证　输入消息签名对(M',σ')，验证者计算$t'=g^{h'}$，$h_1=H_1(\mathrm{ID}||\mathrm{hid},p)$，$P=h_1P_2+P_{\mathrm{pub}}$，$u=\mathrm{e}(S',P)$，$w'=u\cdot t$，$h_2=H_2\left(M'\middle||w',p\right)$。最后，若等式$h_2=h'$成立，输出accept；否则，输出reject。

2.2　商密SM9密钥封装算法

商密SM9密钥封装算法包含设置、密钥生成、密文/密钥封装、密文/密钥解密4个算法。

设置　输入安全参数λ，密钥生成中心选取椭圆曲线群$(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_\mathrm{T},e,p)$，其中$e$为双线性映射：$\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_\mathrm{T}$；$p$为大素数，满足$p>2^\lambda$；随机选取群$\mathbb{G}_1$的生成元$P_1$，群$\mathbb{G}_2$的生成元$P_2$，存在同构映射$P_1=\psi(P_2)$；选取两个密码学哈希函数$H_1:\{0,1\}^*\times\mathbb{Z}_p^*\to\mathbb{Z}_p^*$，$\mathrm{KDF}:\{0,1\}^*\to\{0,1\}^{\mathrm{klen}}$；随机选取$\alpha\in\mathbb{Z}_p^*$，其中$\mathbb{Z}_p^*=\{1,2,\cdots,p-1\}$；计算群$\mathbb{G}_2$中的元素$P_{\mathrm{pub}}=\alpha P_2$和群$\mathbb{G}_T$中的元素$g=\mathrm{e}(P_1,P_{\mathrm{pub}})$；此外，随机选取长度为1Byte的函数识别符hid。输出公开参数$\mathrm{params}=\{\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_\mathrm{T},\mathrm{e},p,P_1,P_2,P_{\mathrm{pub}},H_1,\mathrm{KDF},\mathrm{hid}\}$，保留主密钥$\mathrm{msk}=\alpha$。

密钥生成　输入用户标识$\mathrm{ID}\in\{0,1\}^*$，主密钥msk，密钥生成中心计算用户密钥$\mathrm{sk_{id}}=\dfrac{\alpha}{H_1(\mathrm{ID}\parallel\mathrm{hid},p)+\alpha}P_1$。

密文/密钥封装　输入用户标识ID，加密者随机选取$r\in\mathbb{Z}_p^*$，计算$C=r\cdot(H_1(\mathrm{ID}\parallel\mathrm{hid},\mathrm{p})P_1+P_{\mathrm{pub}})$，$w=\mathrm{e}(P_{\mathrm{pub}},P_1)^r$，$K=\mathrm{KDF}(C\parallel w\parallel\mathrm{ID},l)$。

密文/密钥解密　输入封装密文C，解密密钥$\mathrm{sk_{id}}$，解密者计算$w'=e(C,\mathrm{sk_{id}})$，$K'=\mathrm{KDF}(C\parallel w'\parallel\mathrm{ID},l)$。

2.3　模糊验证技术[14]

切比雪夫映射。给定两个实数$n\in\mathbb{Z}^+$, $x\in[-1,1]$，令多项式$T_n(x):[-1,1]\to[-1,1]$为切比雪夫多项式且可表示为$T_n(x)=\cos(n\cdot\cos^{-1}(x))$，其递归形式可表示为$T_n(x)=2T_{n-1}(x)-T_{n-2}(x)$。

扩展切比雪夫多项式。给定两个实数$n\in\mathbb{Z}^+$, $x\in[-\infty,+\infty]$以及一个大素数p，扩展切比雪夫多项式为$T_n(x)=\cos\left(n\cdot\cos^{-1}(x)\right)\bmod p$，其递归形式可表示为$T_n(x)=2T_{n-1}(x)-T_{n-2}(x)\bmod p$。

模糊验证技术。. 模糊验证技术基于扩展切比雪夫多项式构造。用户的输入通过模运算被随机映射到$[0,p-1]$上，即使敌手获得该输出值也无法确定用户的真实输入。因此，模糊验证技术极大地提高了认证方案的安全性，保证了用户隐私数据的安全。

2.4　生物模糊提取函数[20]

生物模糊提取函数包含两个算法，提取算法$\mathrm{Gen}(\cdot)$和恢复算法$\mathrm{Rep}(\cdot)$，定义如下。

(1) $\mathrm{Gen}(\mathrm{Bio})=(\sigma,\theta)$。$\mathrm{Gen}(\cdot)$是概率性算法。算法输入用户生物特征Bio，输出生物密钥σ和辅助信息θ。

(2) $\mathrm{Rep}\left(\mathrm{Bio}',\theta\right)=\sigma$。$\mathrm{Rep}(\cdot)$是一个确定性算法。算法输入用户生物特征Bio和辅助信息θ，输出生物密钥σ'。

注意，此时若$\mathrm{Bio}'\cong\mathrm{Bio}$，该模糊提取函数可以在误差范围内恢复相同的生物密钥$\sigma=\sigma'$。

2.5　敌手模型

文献[14,15]分析了外部敌手和内部敌手可能发起的攻击方式，并给出了在各个敌手模型下多因素认证方案的安全性，上述敌手模型已被广泛用于分析多因素认证方案的安全性。

敌手1　一个概率多项式时间敌手$\mathcal{A}$可以访问标识空间|ID|和口令空间|PW|的每一个元素$(\mathrm{ID}_i,\mathrm{PW}_i)$。

敌手2 敌手$\mathcal{A}$控制公开通信信道，可以截取、修改、监听和重放所有在公开通信信道上传输的数据。

敌手3 敌手$\mathcal{A}$可以获得智能卡并通过侧信道攻击、能量分析攻击等方式恢复智能卡中的数据。

敌手4 敌手$\mathcal{A}$腐化一个传感器节点。$\mathcal{A}$利用这些秘密信息执行伪造攻击并试图获得之前建立的会话密钥。

敌手5 敌手$\mathcal{A}$可以获得认证网关的密钥并试图恢复用户和传感器节点共享的会话密钥。

敌手6 敌手$\mathcal{A}$是一个合法用户、认证网关或者传感器节点，并试图恢复其他实体的秘密信息。

2.6 方案评价指标

文献[14, 15]给出了衡量多因素认证方案安全性的系统评价指标，考虑了认证因素的安全以及方案的安全性质等。该系统评价指标已被广泛接受并被用于评价多因素认证方案。

评价1 无口令列表。认证网关和传感器节点没有建立与口令相关的任何列表。

评价2 口令/生物特征更新。用户可以自主更新认证因素，如口令、生物特征以及智能卡。

评价3 无口令泄露。在公开信道上传输的数据不会泄露任何与口令相关的信息。

评价4 抵抗智能卡丢失攻击。智能卡丢失不会造成口令信息泄露，并且不会泄露会话密钥。

评价5 抵抗已知攻击。方案可以抵抗口令猜测攻击、内部攻击、传感器节点捕获攻击以及重放攻击等。

评价6 动态加入或撤销。用户或传感器节点可以自主加入或退出该认证系统。

评价7 会话密钥建立。用户和传感器节点可以建立一个安全的共享会话密钥。

评价8 时钟异步。所提出的方案应避免时钟同步。

评价9 实时检测。认证方案可以实时检测错误的用户口令。

评价10 相互认证。通信双方可以互相认证彼此的身份以及传输数据的真实性和有效性。

评价11 用户匿名性和不可追踪性。用户的真实身份对系统外实体保持隐私，且无法被追踪。

评价12 前向安全性。认证网关密钥的泄露不会造成用户和传感器节点之间的会话密钥泄露。

2.7 方案安全模型

Bellare等人[21]和Wang等人[14]提出的安全模型已被广泛用于分析多因素认证的安全性。参考文献[21]和文献[14]，本节给出多因素认证方案的安全模型。

令Ω_{UE}^{i}, Ω_{AG}, Ω_{SN}^{j}分别表示用户、认证网关以及传感器节点。假设存在一个敌手$\mathcal{A}$可以在概率多项式时间内与上述实体进行以下交互询问：

(1) Extract($\Omega_{\mathrm{UE}}^{\mathrm{i}}$, Ω_{AG}, $\Omega_{\mathrm{SN}}^{\mathrm{j}}$)：该询问模拟被动攻击，如模拟监听攻击获取公开信道中的数据副本。

(2) Send($\Omega_{\mathrm{UE}}^{\mathrm{i}}$, Ω_{AG}, $\Omega_{\mathrm{SN}}^{\mathrm{j}}$, M)：该询问模拟主动攻击，敌手$\mathcal{A}$可以分别向实体$\Omega_{\mathrm{UE}}^{\mathrm{i}}$, Ω_{AG}, $\Omega_{\mathrm{SN}}^{\mathrm{j}}$发送消息$M$，并按照方案执行过程得到关于$M$的一个响应。

(3) Reveal($\Omega_{\mathrm{UE}}^{\mathrm{i}}$, $\Omega_{\mathrm{SN}}^{\mathrm{j}}$)：当$\Omega_{\mathrm{SN}}^{\mathrm{j}}$与$\Omega_{\mathrm{UE}}^{\mathrm{i}}$创建会话密钥时，将此次会话密钥返回给敌手$\mathcal{A}$；否则，返回$\perp$表示空。

(4) Corrupt($\Omega_{\mathrm{UE}}^{\mathrm{i}}$, b)：该询问允许敌手$\mathcal{A}$询问并获得3个认证因素中的任何两个因素，如下所示，

(a) Corrupt($\Omega_{\mathrm{UE}}^{\mathrm{i}}$, 1)：敌手$\mathcal{A}$可以获得口令$\mathrm{PE}_{\mathrm{UE}}$和智能卡$\mathrm{SC}_{\mathrm{UE}}$。

(b) Corrupt($\Omega_{\mathrm{UE}}^{\mathrm{i}}$, 2)：敌手$\mathcal{A}$可以获得口令$\mathrm{PW}_{\mathrm{UE}}$和生物特征$\mathrm{BIO}_{\mathrm{UE}}$。

(c) Corrupt($\Omega_{\mathrm{UE}}^{\mathrm{i}}$, 3)：敌手$\mathcal{A}$可以获得智能卡$\mathrm{SC}_{\mathrm{UE}}$和生物特征$\mathrm{BIO}_{\mathrm{UE}}$。

(5) Corrupt(Ω_{AG}, 1)：该询问模拟前向安全性，允许敌手$\mathcal{A}$获得认证网关的密钥。

(6) Hash($\cdot$)：该询问返回一个随机哈希值。

(7) Test($\Omega_{\mathrm{UE}}^{\mathrm{i}}$, $\Omega_{\mathrm{SN}}^{\mathrm{j}}$)：当实体$\Omega_{\mathrm{UE}}^{\mathrm{i}}$, $\Omega_{\mathrm{SN}}^{\mathrm{j}}$忠诚地执行认证方案，并且产生一个会话密钥SK，该询问谕言机抛币b，若$b=1$，输出正确会话密钥SK；否则，输出一个随机产生的等长字符串SK'。此时，要求$\Omega_{\mathrm{UE}}^{\mathrm{i}}$, $\Omega_{\mathrm{SN}}^{\mathrm{j}}$未被执行过Reveal($\Omega_{\mathrm{UE}}^{\mathrm{i}}$, $\Omega_{\mathrm{SN}}^{\mathrm{j}}$)以及Corrupt($\Omega_{\mathrm{UE}}^{\mathrm{i}}$, b)询问。

定理2 假设存在一个敌手$\mathcal{A}$在多项式时间内执行q_{E}次Extract($\Omega_{\mathrm{UE}}^{\mathrm{i}}$, Ω_{AG}, $\Omega_{\mathrm{SN}}^{\mathrm{j}}$)询问，$q_{\mathrm{S}}$次Send($\Omega_{\mathrm{UE}}^{\mathrm{i}}$, Ω_{AG}, $\Omega_{\mathrm{SN}}^{\mathrm{j}}$, M)询问，q_{H}次Hash($\cdot$)询问，q_{C}次Corrupt($\Omega_{\mathrm{UE}}^{\mathrm{i}}$, b)询问，q_{f}次模糊提取函数询问，q_{δ}次公钥加密解密询问，敌手$\mathcal{A}$攻破方案的优势$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{MFAS\text{-}SM9}}$定义为

$$\begin{aligned}\mathrm{Adv}_{\mathcal{A}}^{\mathrm{MFAS\text{-}SM9}} \le & 2C'q_{\mathrm{s}}^{\eta'}+\frac{1}{2^{p}}+\frac{q_{\delta}^{2}}{2^{l_3}}\\ &+\frac{3q_{\mathrm{S}}+q_{H_2}^{2}}{2^{l_{H_2}}}+\frac{q_{\mathrm{S}}+q_{H_3}^{2}}{2^{l_{H_3}}}\\ &+\frac{(q_{\mathrm{E}}+q_{\mathrm{S}})^{2}}{p}+\frac{2q_{\mathrm{S}}+q_{\mathrm{f}}^{2}}{2^{l_2}}\\ &+\frac{3q_{\mathrm{S}}+q_{H_1}^{2}}{2^{l_{H_1}}}+2q_{\mathrm{S}}\mathrm{Adv}_{\mathcal{A}'}^{\mathrm{SM9}}。\end{aligned}$$

其中C', η'是与口令集合大小相关的常数，l_2, l_3分别表示模糊提取函数输出值的长度以及公钥加密算

法的密文长度，$\mathrm{Adv}_{\mathcal{A}'}^{\mathrm{SM9}}$表示敌手$\mathcal{A}'$攻破底层商密SM9算法的优势。

3　方案设计

MFAS-SM9方案的系统框架如图1所示，包含用户、认证网关以及传感器3个实体。当需要与传感器建立会话时，用户首先需要在认证网关进行注册；当注册成功后，用户向认证网关发送登录及认证请求；若用户通过身份认证，认证网关向传感器转交该认证请求；当收到认证请求后，传感器验证认证网关的真实性，若通过验证，则传感器向用户发送认证响应；用户验证传感器的身份以及发送的响应，若成功验证，则用户与传感器建立安全会话密钥。

MFAS-SM9方案包括设置、密钥生成、注册、登录/认证4个算法。方案中的符号及数学表示与商密SM9标识密码算法保持一致。在注册算法中，用户利用基于SM9的签密算法生成关于注册信息的签密密文。此时，只有认证网关可以利用私钥解密获得该注册信息，并进一步验证该信息的有效性。注册信息的签密密文可以在公开信道中传输。认证网关在收到用户的注册信息后，会为用户生成蜜罐口令列表并存储到智能卡中；使用模糊验证技术生成认证信息并存储到智能卡中。在登录/认证算法中，用户输入口令、智能卡和生物特征信息并登录系统。此时，若敌手输入蜜罐口令并伪装用户尝试登录，认证网关将识别该行为并将蜜罐口令列表中该用户对应的登录失败次数增加一次。当失败次数超过预定的门限值时，认证系统将拒绝该敌手的任何登录请求。若成功登录系统，用户可以和传感器节点安全地协商一个会话密钥。

3.1　设置算法

令λ为系统安全参数，密钥生成中心选取双线性群$\mathrm{Bp}=\{\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,p\}$，其中$p>2^{\lambda}$，$e:\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_{\mathrm{T}}$，大素数$p$是群$\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_{\mathrm{T}}$的阶。随机选取$\mathbb{G}_1$的生成元$P_1$，$\mathbb{G}_2$的生成元$P_2$，存在同构映射$\psi(P_2)\to P_1$。然后，随机选取$\alpha\in\mathbb{Z}_p^*$，并计算$P_{\mathrm{pub}}=\alpha P_2$，$g=e(P_1,P_{\mathrm{pub}})$。随机选取3个哈希函数$H_1:\{0,1\}^*\to\mathbb{Z}_p^*,H_2:\{0,1\}^n\times\mathbb{G}_{\mathrm{T}}\times p\to\mathbb{Z}_p^*,H_3:\{0,1\}^*\times\mathbb{G}_{\mathrm{T}}\times\{0,1\}^*\to\mathbb{Z}_p^*$，以及一个密钥封装函数$\mathrm{KDF}:\{0,1\}^*\to\{0,1\}^{\mathrm{klen}}$，其中$n$为签名的长度，klen为会话密钥长度。最后选取用一个二进制字符串表示的函数识别符hid。令$\mathrm{msk}=\alpha$为主密钥，$\mathrm{params}=(\mathrm{BP},P_1,P_2,P_{\mathrm{pub}},g,H_1,H_2,H_3,\mathrm{KDF},\mathrm{hid})$为公开参数。

3.2　密钥生成

算法输入主密钥msk，标识$\mathrm{ID}\in\{0,1\}^*$(包含用户标识$\mathrm{ID_{UE}}$，认证网关标识$\mathrm{ID_{AG}}$，传感器节点标识$\mathrm{ID_{SN}}$)以及公开参数params。密钥生成中心计算签名者密钥$\mathrm{sk_{ID}}=\dfrac{\alpha}{H_1(\mathrm{ID}||\mathrm{hid},p)+\alpha}\cdot P_2$。此时，若$H_1(\mathrm{ID}||\mathrm{hid},p)+\alpha=0$，密钥生成中心重新生成主密钥msk并再次为标识ID生成密钥$\mathrm{sk_{ID}}$。

3.3　用户注册算法

在用户注册阶段，用户向认证网关发送注册请求。当收到注册请求后，认证网关生成一个注册响应并发送给用户。注册过程如图2所示，具体算法如下：

(1) 用户输入标识$\mathrm{ID_{UE}}$，口令$\mathrm{PW_{UE}}$以及生物特征$\mathrm{BIO_{UE}}$，并计算$\mathrm{Gen(BIO_{UE})}=(\sigma_{\mathrm{UE}},\theta_{\mathrm{UE}})$，$\mathrm{HPW_{UE}}=H_1(\mathrm{PW_{UE}}||\sigma_{\mathrm{UE}})$，$\mathrm{MID_{UE}}=H_1(\mathrm{ID_{UE}}||r_1)$，其中$r_1\in\mathbb{Z}_p^*$。然后，随机选取二进制字符串$Y_{\mathrm{UE}}\in\{0,1\}^{\mathrm{Blen}}$。计算$Q_1=H_1(\mathrm{ID_{AG}}||\mathrm{hid},p)P_1+\psi(P_{\mathrm{pub}})$，$w_1=g^{r_1}$；令$M_1=Y_{\mathrm{UE}}||\mathrm{MID_{UE}}||\mathrm{HPW_{UE}}$，计算$h_1=H_2(M_1||w_1,p)$，$l_1=(r_1-h_1)\bmod p$，$s_1=l_1\psi(\mathrm{sk_{ID_{UE}}})$，$t_1=r_1Q_1$，其中$r_1\in\mathbb{Z}_p^*$。若$l_1=0$，重新选取$r_1$并计算。计算$c_1=(M_1||T_1)\oplus H_3(t_1||w_1||\mathrm{ID_{AG}})$，将$\mathrm{CT_1}=\{c_1,s_1,t_1,T_1\}$通过公开信道发送给认证网关，$T_1$为当前时间戳。

(2) 当认证网关接收到$\mathrm{CT_1}$，计算$w_1'=\mathrm{e}(t_1,\mathrm{sk_{ID_{AG}}})$，$M_1'||T_1'=c_1\oplus H_3(t_1||w_1||\mathrm{ID_{AG}})$。提取$M_1'$和$T_1'$，此时若$|T_1'-T_1|\le\Delta T$，表明$\mathrm{CT_1}$满足时效性。然后，计算$h_1'=H_2\left(M_1'\middle||w_1',p\right)$，$t_1'=g^{h_1'}$，$P_{\mathrm{UE}}=H_1(\mathrm{ID_{UE}}||\mathrm{hid},p)P_2+P_{\mathrm{pub}}$。验证等式$e(s_1,$

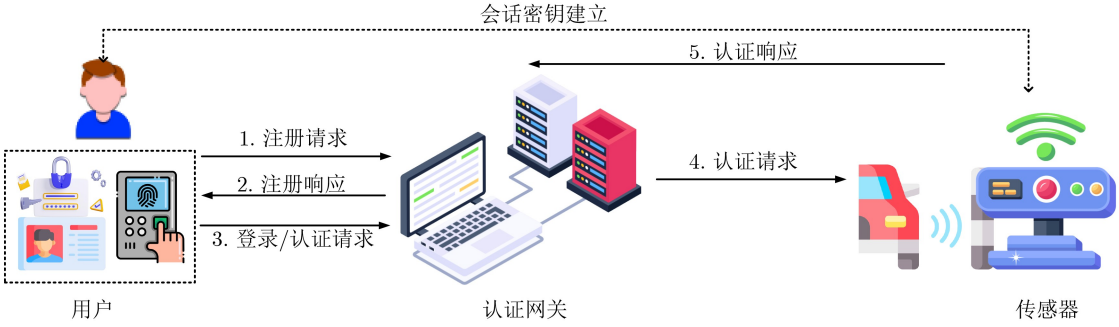

图 1 MFAS-SM9方案的系统框架

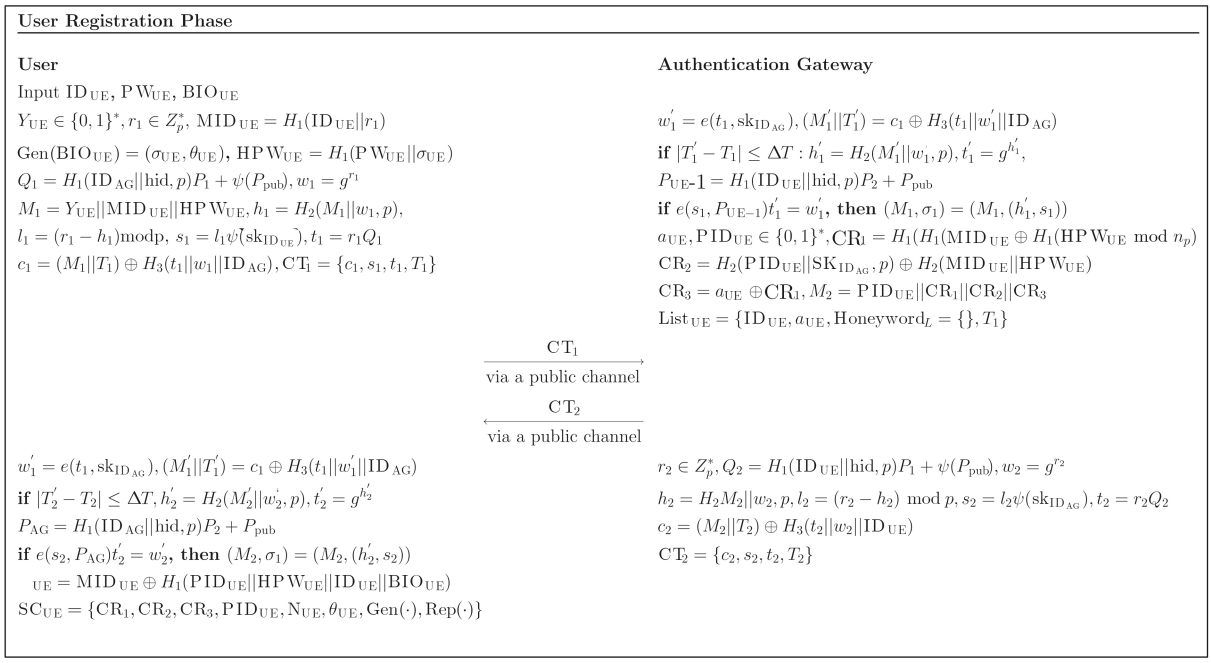

图 2 用户注册

$P_{\mathrm{UE}})\, t_1' = w_1'$是否成立。若成立，则成功恢复$(M_1, \sigma_1)$，其中$\sigma_1 = (h_1', s_1)$。此时消息签名对满足验证算法，认证用户身份的真实性和有效性。认证网关随机选取$a_{\mathrm{UE}}, \mathrm{PID_{UE}} \in \{0,1\}^{\mathrm{Blen}}$，然后进一步计算 $\mathrm{CR_1} = H_1(H_1(\mathrm{MID_{UE}}) \oplus H_1(\mathrm{HPW_{UE}}) \mathrm{mod} n_{\mathrm{p}})$，$\mathrm{CR_2} = H_2(\mathrm{PID_{UE}}||\mathrm{sk_{ID_{AG}}}, p) \oplus H_2(\mathrm{MID_{UE}}||\mathrm{HPW_{UE}})$，$\mathrm{CR_3} = a_{\mathrm{UE}} \oplus \mathrm{CR_1}$。认证网关创建并存储关于标识 $\mathrm{ID_{UE}}$ 的一个列表$\mathrm{List_{UE}} = \{\mathrm{ID_{UE}}, T_1, a_{\mathrm{UE}}, \mathrm{Honeyword}_L = \{\}\}$。令$M_2 = \mathrm{PID_{UE}}||\mathrm{CR_1}||\mathrm{CR_2}||\mathrm{CR_3}$，然后计算$Q_2 = H_1(\mathrm{ID_{UE}}||\mathrm{hid}, p)P_1 + \psi(P_{\mathrm{pub}})$，$w_2 = g^{r_2}$，$h_2 = H_2(M_2||w_2, p)$，$l_2 = (r_2 - h_2) \mathrm{mod} p$，$t_2 = r_2Q_2$，$s_2 = l_2\psi(\mathrm{sk_{ID_{AG}}})$，其中$r_2 \in \mathbb{Z}_p^*$。此时，若$l_2 = 0$，则重新选取$r_2$并计算。然后计算$c_2 = (M_2||T_2) \oplus H_3(t_2||w_2||\mathrm{ID_{UE}})$，将$\mathrm{CT_2} = \{c_2, s_2, t_2, T_2\}$通过公开信道发送给用户，$T_2$为当前时间戳。

(3) 当用户接收$\mathrm{CT_2} = \{c_2, s_2, t_2, T_2\}$后，计算$w_2' = \mathrm{e}(t_2, \mathrm{sk_{ID_{UE}}})$，$M_2'||T_2' = c_2 \oplus H_3(t_2||w_2||\mathrm{ID_{UE}})$。提取$M_2'$和$T_2'$，此时若$|T_2' - T_2| \le \Delta T$，表明$\mathrm{CT_2}$满足时效性。然后，计算$h_2' = H_2\left(M_2'||w_2', p\right)$，$t_1' = g^{h_2'}$，$P_{\mathrm{AG}} = H_1(\mathrm{ID_{AG}}||\mathrm{hid}, p)P_2 + P_{\mathrm{pub}}$。验证等式$\mathrm{e}(s_2, P_{\mathrm{AG}})\, t_2' = w_2'$是否成立。若等式成立，则成功恢复$(M_2, \sigma_2)$，其中$\sigma_2 = (h_2', s_2)$。然后进一步计算$N_{\mathrm{UE}} = \mathrm{MID_{UE}} \oplus H_1(\mathrm{PID_{UE}}||\mathrm{HPW_{UE}}||\mathrm{ID_{UE}}||\mathrm{BIO_{UE}})$。最后，用户将秘密消息$\{\mathrm{CR_1}, \mathrm{CR_2}, \mathrm{CR_3}, \mathrm{PID_{UE}}, \mathrm{N_{UE}}, \theta_{\mathrm{UE}}, \mathrm{Gen}(\cdot), \mathrm{Rep}(\cdot)\}$嵌入到智能卡$\mathrm{SC_{UE}}$中。

3.4 登录和认证算法

在用户登录及认证阶段，用户向认证网关发送登录及认证请求。当认证网关收到该请求后，若成功验证该用户的身份，认证网关将该请求发送给传感器节点。最后，当成功执行相互认证后，用户和传感器节点生成一个共享密钥。用户登录及认证过程如图3所示，具体算法如下：

(1) 用户插入智能卡$\mathrm{SC_{UE}}$并输入标识$\mathrm{ID_{UE}^*}$，口令$\mathrm{PW_{UE}^*}$以及生物特征$\mathrm{BIO_{UE}^*}$，计算$\sigma_{\mathrm{UE}}^* = \mathrm{Rep}(\mathrm{BIO_{UE}^*}, \theta_{\mathrm{UE}})$，$\mathrm{HPW_{UE}^*} = H_1(\mathrm{PW_{UE}^*}||\sigma_{\mathrm{UE}}^*)$，$\mathrm{MID_{UE}^*} = N_{\mathrm{UE}} \oplus H_1(\mathrm{PID_{UE}}||\mathrm{HPW_{UE}}||\mathrm{ID_{UE}}||\mathrm{BIO_{UE}^*}$，$\mathrm{CR_1^*} = H_1(H_1(\mathrm{MID_{UE}^*}) \oplus H_1(\mathrm{HPW_{UE}}) \mathrm{mod} n_{\mathrm{p}})$。若$\mathrm{CR_1^*} = \mathrm{CR_1}$，用户随机选取$r_3 \in \mathbb{Z}_p^*$，令$M_3 = \mathrm{MID_{UE}}||r_3||\mathrm{SID_{SN}}$，计算$Q_3 = H_1(\mathrm{ID_{AG}}||\mathrm{hid}, p)P_1 + \psi(P_{\mathrm{pub}})$，$w_3 = g^{r_3}$，$h_3 = H_2(M_3||w_3, p)$，$l_3 = (r_3 - h_3) \mathrm{mod} p$，$s_3 = l_3\psi(\mathrm{sk_{ID_{UE}}})$，$t_3 = r_3Q_3$。若$l_3 = 0$，则重新选取$r_3$并计算，然后计算$c_3 = (M_3||T_3) \oplus H_3(t_3||w_3||\mathrm{ID_{AG}})$，$k = H_2(\mathrm{PID_{UE}}||\mathrm{sk_{ID_{AG}}}, p) = \mathrm{CR_2} \oplus H_2(\mathrm{HPW_{UE}^*}||\mathrm{MID_{UE}^*})$，$a_{\mathrm{UE}} = \mathrm{CR_3} \oplus \mathrm{CR_1}$，$\mathrm{CAK_{UE}} = (a_{\mathrm{UE}}||k) \oplus H_1(r_3||T_3)$，其中$T_3$表示当前时间戳。最后，用户将$\mathrm{CT_3} = \{c_3, s_3, t_3, T_3, \mathrm{CAK_{UE}}\}$发送给认证网关。

(2) 当认证网关接收到$\mathrm{CT_3}$后，计算$w_3' = \mathrm{e}(t_3, \mathrm{sk_{ID_{AG}}})$，$M_3'||T_3' = c_3 \oplus H_3(t_3||w_3||\mathrm{ID_{AG}})$。提取$M_3'$和$T_3'$，此时若$|T_3' - T_3| \le \Delta T$，表明$\mathrm{CT_3}$满足时效性。然后，认证网关计算$k = H_2(\mathrm{PID_{UE}}||\mathrm{sk_{ID_{AG}}}, p)$，$\mathrm{CAK_{UE}^*} = (a_{\mathrm{UE}}||k) \oplus H_1(r_3||T_3)$，比较等式$\mathrm{CAK_{UE}^*} = \mathrm{CAK_{UE}}$是否成立。若等式不成立，认证网关计算$\left(a_{\mathrm{UE}}'\middle|\middle|k'\right) = \mathrm{CAK_{UE}} \oplus H_1(r_3||T_3)$。若

$a'_{\mathrm{UE}}=a_{\mathrm{UE}}$，$k'\neq k$，则表明用户智能卡至$1-\dfrac{1}{2^{n_p}}$率被攻破，因此认证网关将$k'$添加到列表$\mathrm{Honeyword_L}=\{\}$。若该列表中的元素超过预定的门限值$T_{\mathrm{S}}(\approx 10)$，认证网关将不再受理该智能卡的登录请求。否则，成功恢复(M_3,σ_3)，其中$\sigma_3=(h'_3,s_3)$。此时，验证方程成立。令$M_4=\mathrm{MID_{UE}}\,||\,r_3$，认证网关计算$Q_4=H_1(\mathrm{ID_{SN}}||\mathrm{hid},p)P_1+\psi(P_{\mathrm{pub}})$，$w_4=g^{r_4}$，$h_4=H_2(M_4||w_4,p)$，$l_4=(r_4-h_4)\mathrm{mod}p$，$t_4=r_4Q_4$，$s_4=l_4\psi(\mathrm{sk_{ID_{AG}}})$，$c_4=(M_4||T_4)\oplus H_3(t_4||w_4||\mathrm{ID_{SN}})$，其中$r_4\in\mathbb{Z}_p^*$，$T_4$表示当前时间戳。若$l_4=0$，则重新选取$r_4$并计算。最后，将$\mathrm{CT_4}=\{c_4,s_4,t_4,T_4\}$通过公开信道发送给传感器节点。

（3）在收到消息$\mathrm{CT_4}$后，传感器节点计算$w'_4=\mathrm{e}(t_4,\mathrm{sk_{ID_{SN}}})$，$M'_4\,||\,T'_4=c_4\oplus H_3(t_4||w_4||\mathrm{ID_{SN}})$。提取$M'_4$和$T'_4$，此时若$|T'_4-T_4|\leq\Delta T$，表明$\mathrm{CT_4}$满足时效性。然后，计算$h'_4=H_2\left(M'_4||w'_4,p\right)$，$t'_4=g^{h'_4}$，$P_{\mathrm{SN}}=H_1(\mathrm{ID_{AG}}||\mathrm{hid},p)P_2+P_{\mathrm{pub}}$。验证等式$\mathrm{e}(s_4,P_{\mathrm{SN}})t'_4=w'_4$是否成立。若等式成立，则成功恢复$(M_4,\sigma_4)$，其中$\sigma_4=(h'_4,s_4)$。此时消息签名对满足验证算法，从而证明了消息的真实性和有效性。传感器节点随机选取$r_5\in\mathbb{Z}_p^*$，令$M_5=\mathrm{SID_{SN}}\,||\,r_5$，计算$Q_5=H_1(\mathrm{ID_{UE}}||\mathrm{hid},p)P_1+\psi(P_{\mathrm{pub}})$，$w_5=g^{r_5}$，$h_5=H_2(M_5||w_5,p)$，$l_5=(r_5-h_5)\,\mathrm{mod}p$，$s_5=l_5\psi(\mathrm{sk_{ID_{SN}}})$，$t_5=r_5Q_5$，$c_5=(M_5||T_5)\oplus H_3(t_5||w_5||\mathrm{ID_{UE}})$，其中$T_5$表示当前时间戳。若$l_5=0$，则重新选取$r_5$并计算。利用商密SM9密钥封装算法生成会话密钥$\mathrm{SK}=\mathrm{KDF}(g^{r_3}||g^{r_5}||S\mathrm{ID_{SN}}||\mathrm{MID_{UE}},\mathrm{klen})$。认证网关将$\mathrm{CT_5}=\{c_5,s_5,t_5,T_5\}$通过公开信道发送给用户。

（4）用户在接收到$\mathrm{CT_5}$后，计算$w'_5=e(t_5,\mathrm{sk_{ID_{UE}}})$，$M'_5\,||\,T'_5=c_5\oplus H_3(t_5||w_5||\mathrm{ID_{UE}})$。提取$M'_5$和$T'_5$，此时若$|T'_5-T_5|\leq\Delta T$，表明$\mathrm{CT_5}$满足时效性。然后，计算$h'_5=H_2(M'_5||w'_5,p)$，$t'_5=g^{h'_5}$，$P_{\mathrm{UE-2}}=H_1(\mathrm{ID_{SN}}||\mathrm{hid},p)P_2+P_{\mathrm{pub}}$。验证等式$e(s_5,P_{\mathrm{UE-2}})t'_5=w'_5$是否成立。若等式成立，则成功恢复$(M_5,\sigma_5)$，其中$\sigma_5=(h'_5,s_5)$。然后，用户计算$\mathrm{SK}=\mathrm{KDF}(g^{r_3}||g^{r_5}||S\mathrm{ID_{SN}}||\mathrm{MID_{UE}},\mathrm{klen})$。最后，用户和传感器节点建立安全会话密钥SK。

3.5 口令更新算法

用户插入智能卡$\mathrm{SC_{UE}}$并输入原始口令$\mathrm{PW_{UE}}$和更新后口令$\mathrm{PW_{UE}^{new}}$，计算

$$\mathrm{CR_1^{new}}=H_1(H_1(\mathrm{MID_{UE}})\oplus H_1(\mathrm{HPW_{UE}})\oplus H_1(\mathrm{PW_{UE}^{new}}))$$

$$\mathrm{CR_2^{new}}=\mathrm{CR_2}\oplus H_2(\mathrm{MID_{UE}}||\mathrm{HPW_{UE}})\oplus H_2(\mathrm{MID_{UE}}||\mathrm{PW_{UE}^{new}})$$

$$\mathrm{CR_3^{new}}=\mathrm{CR_3}\oplus\mathrm{CR_1}\oplus\mathrm{CR_1^{new}},$$

$$N_{\mathrm{UE}}^{\mathrm{new}}=N_{\mathrm{UE}}\oplus H_1(\mathrm{PID_{UE}}||\mathrm{HPW_{UE}}||\mathrm{ID_{UE}}||\mathrm{BIO_{UE}})\oplus H_1(\mathrm{PID_{UE}}||\mathrm{HPW}_{\mathrm{UE}}^{\mathrm{new}}||\mathrm{ID_{UE}}||\mathrm{BIO_{UE}})。$$

更新

$$\mathrm{SC_{UE}}=\{\mathrm{CR_1^{new}},\mathrm{CR_2^{new}},\mathrm{CR_3^{new}},\mathrm{PID_{UE}},N_{\mathrm{UE}},\theta_{\mathrm{UE}},\mathrm{Gen}(\cdot),\mathrm{Rep}(\cdot)\}。$$

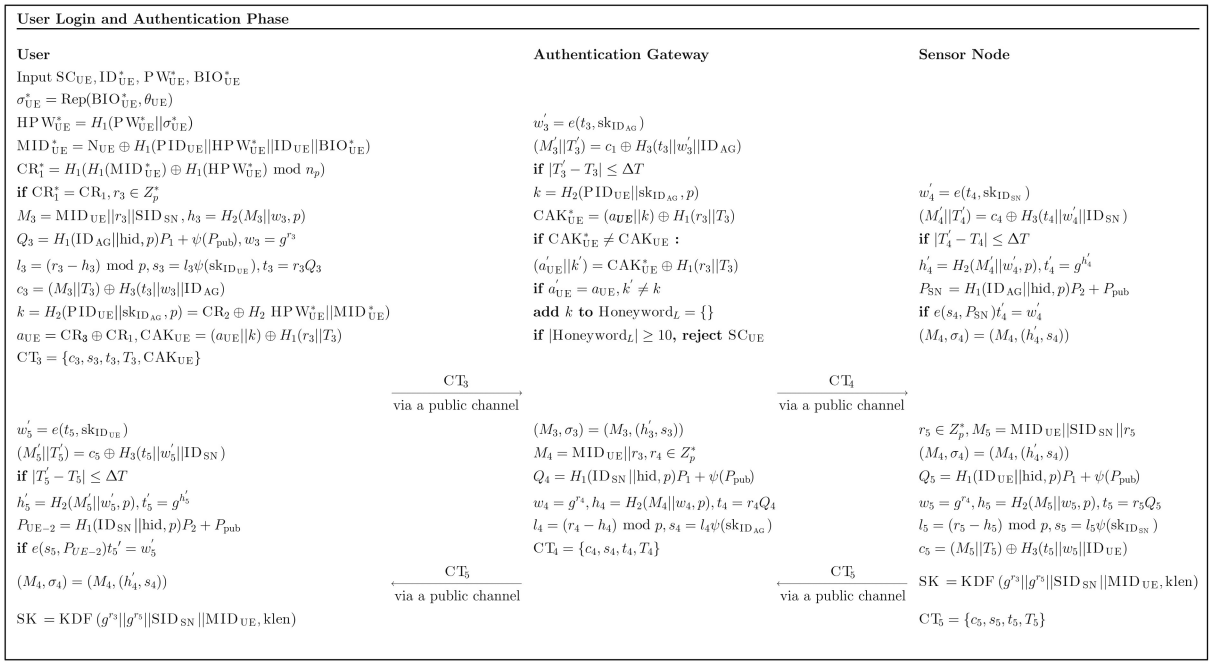

图 3 用户登录及认证

此时，当需要更新生物特征时，用户计算

$$\begin{aligned}&\mathrm{Gen}\left(\mathrm{BIO}_{\mathrm{UE}}^{\mathrm{new}}\right)=\left(\sigma_{\mathrm{UE}}^{\mathrm{new}},\theta_{\mathrm{UE}}^{\mathrm{new}}\right),\\&\mathrm{HP}W_{\mathrm{UE}}^{\mathrm{new}}=H_1\left(\mathrm{PW}_{\mathrm{UE}}||\sigma_{\mathrm{UE}}^{\mathrm{new}}\right),\\&\mathrm{CR}_2^{\mathrm{new}}=\mathrm{CR}_2\oplus H_2\left(\mathrm{MID}_{\mathrm{UE}}||\mathrm{HPW}_{\mathrm{UE}}\right)\\&\quad\oplus H_2(\mathrm{MID}_{\mathrm{UE}}||\mathrm{PW}_{\mathrm{UE}}^{\mathrm{new}}),\\&N_{\mathrm{UE}}^{\mathrm{new}}=N_{\mathrm{UE}}\oplus H_1\left(\mathrm{PID}_{\mathrm{UE}}||\mathrm{HPW}_{\mathrm{UE}}||\mathrm{ID}_{\mathrm{UE}}||\mathrm{BIO}_{\mathrm{UE}}\right)\\&\quad\oplus H_1\left(\mathrm{PID}_{\mathrm{UE}}||\mathrm{HP}W_{\mathrm{UE}}^{\mathrm{new}}||\mathrm{ID}_{\mathrm{UE}}||\mathrm{BIO}_{\mathrm{UE}}^{\mathrm{new}}\right)\end{aligned}$$

4 安全性分析

4.1 MFAS-SM9方案的形式化安全分析

参考Bellare等人[21]和Wang等人[14]提出的认证方案安全模型，本节给出MFAS-SM9方案的形式化安全证明并给出启发式分析。

设置以下交互游戏Game_1 ~ Game_6，当且仅当敌手$\mathcal{A}$在游戏Game_i中成功猜测抛币b的值时，$\mathcal{A}$赢得游戏Game_$i(1\le i\le 6)$。令Pr[G_i]表示敌手$\mathcal{A}$赢得游戏Game_i的概率。

Game_1：该游戏模拟敌手$\mathcal{A}$对真实方案的攻击，因此，$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{MFAS-SM9}}=2\Pr\left[\mathrm{G}_1\right]-1$。

Game_2：在该游戏中，允许敌手$\mathcal{A}$执行$\mathrm{Extract}(\Omega_{\mathrm{UE}}^{\mathrm{i}},\Omega_{\mathrm{AG}},\Omega_{\mathrm{SN}}^{\mathrm{j}})$询问。因此，敌手$\mathcal{A}$可以获取在公开信道中传输的数据$\{\mathrm{CT}_1,\mathrm{CT}_2,\mathrm{CT}_3,\mathrm{CT}_4,\mathrm{CT}_5\}$。但由于这些数据是加密后的密文，在敌手$\mathcal{A}$不知道实体密钥的条件下，这些密文无法提供有效信息帮助敌手$\mathcal{A}$猜测b值。游戏Game_2与游戏Game_1不可区分，即$\Pr\left[\mathrm{G}_1\right]=\Pr\left[\mathrm{G}_2\right]$。

Game_3：该游戏在询问中发生碰撞事件时会立即终止，考虑以下碰撞事件，

(1) 询问哈希函数H_1, H_2, H_3时，其返回值发生碰撞；

(2) 模糊提取函数Gen(·), Rep(·)的返回值发生碰撞；

(3) 加密密文发生碰撞；

(4) 生成的消息发生碰撞。

因此，敌手$\mathcal{A}$赢得Game_3的概率为，$\left|\Pr\left[\mathrm{G}_3\right]-\Pr\left[\mathrm{G}_2\right]\right|\le\frac{q_{H_1}^2}{2^{l_{H_1}}}+\frac{q_{H_2}^2}{2^{l_{H_2}}}+\frac{q_{H_3}^2}{2^{l_{H_3}}}+\frac{q_{\mathrm{f}}^2}{2^{l_2}}+\frac{q_\delta^2}{2^{l_3}}+\frac{\left(q_{\mathrm{E}}+q_{\mathrm{S}}\right)^2}{2p}$。

Game_4：在该游戏中，若敌手$\mathcal{A}$成功猜测出哈希值$H_1\left(\mathrm{ID}||\mathrm{hid},p\right)$, $H_2\left(M||w,p\right)$, $H_3\left(t||w||ID\right)$，时，游戏终止。因此，有$\left|\Pr\left[\mathrm{G}_4\right]-\Pr\left[\mathrm{G}_3\right]\right|\le\frac{q_{\mathrm{S}}}{2^{l_{H_1}}}+\frac{q_{\mathrm{S}}}{2^{l_{H_2}}}+\frac{q_{\mathrm{S}}}{2^{l_{H_3}}}$。

Game_5：该游戏允许敌手$\mathcal{A}$执行$\mathrm{Corrupt}(\Omega_{\mathrm{UE}}^{\mathrm{i}},b)$和$\mathrm{Corrupt}(\Omega_{\mathrm{AG}},1)$询问。当执行$\mathrm{Corrupt}(\Omega_{\mathrm{UE}}^{\mathrm{i}},1)$询问时，敌手$\mathcal{A}$猜测用户生物特征信息$\mathrm{BIO}_{\mathrm{UE}}$，其概率为$\frac{q_{\mathrm{S}}}{2^{l_2}}$；当执行$\mathrm{Corrupt}(\Omega_{\mathrm{UE}}^{\mathrm{i}},2)$询问时，敌手$\mathcal{A}$猜测智能卡$\mathrm{SC}_{\mathrm{UE}}$信息，其概率约为$\frac{q_{\mathrm{S}}}{2^{l_{H_1}}}+\frac{q_{\mathrm{S}}}{2^{l_{H_2}}}$；当执行$\mathrm{Corrupt}(\Omega_{\mathrm{UE}}^{\mathrm{i}},3)$询问时，敌手$\mathcal{A}$猜测口令$\mathrm{PW}_{\mathrm{UE}}$，其概率为$C^{'}q_{\mathrm{s}}^{\eta^{'}}$；当执行$\mathrm{Corrupt}(\Omega_{\mathrm{AG}},1)$询问时，其概率为$\frac{1}{2^p}$。因此，有$\left|\Pr\left[\mathrm{G}_4\right]-\Pr\left[\mathrm{G}_3\right]\right|\le\frac{1}{2^p}+\frac{q_{\mathrm{S}}}{2^{l_2}}+\frac{q_{\mathrm{S}}}{2^{l_{H_1}}}+\frac{q_{\mathrm{S}}}{2^{l_{H_2}}}+C^{'}q_{\mathrm{s}}^{\eta^{'}}$。

Game_6：假设存在敌手$\mathcal{A}^{'}$以$\mathrm{Adv}_{\mathcal{A}^{'}}^{\mathrm{SM9}}$的优势攻破底层SM9算法，该游戏允许敌手$\mathcal{A}$与敌手$\mathcal{A}^{'}$进行交互。在该游戏中，用一个理想函数$F_{\mathrm{ideal}}(\cdot)$代替密钥封装函数KDF(·)，理想函数$F_{\mathrm{ideal}}(\cdot)$的输出对敌手$\mathcal{A}$是不可预测的。因此，有$\Pr\left[\mathrm{G}_6\right]=\frac{1}{2}$。用事件$\beta$表示攻击者查询$\mathrm{SK}=\mathrm{KDF}\left(g^{r_3}||g^{r_5}||\mathrm{SID}_{\mathrm{SN}}||\mathrm{MID}_{\mathrm{UE}},\mathrm{klen}\right)$的值。若事件$\beta$不发生则游戏Game_5和游戏Game_6不可区分，即$\left|\Pr\left[\mathrm{G}_6\right]-\Pr\left[\mathrm{G}_5\right]\right|\le\Pr\left[\beta\right]$。若敌手$\mathcal{A}$经过$q_{\mathrm{S}}$次查询后能够区分理想函数$F_{\mathrm{ideal}}(\cdot)$以及密钥封装函数KDF(·)，那么必然存在一个敌手$\mathcal{A}^{'}$以$\mathrm{Adv}_{\mathcal{A}^{'}}^{\mathrm{SM9}}$的优势攻破底层商密SM9算法，即$\Pr\left[\beta\right]\le q_S\mathrm{Adv}_{\mathcal{A}^{'}}^{\mathrm{SM9}}$。

综上所述，通过游戏Game_1 ~ Game_6可知，敌手$\mathcal{A}$攻破方案的优势$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{MFAS-SM9}}$为

$$\begin{aligned}\mathrm{Adv}_{\mathcal{A}}^{\mathrm{MFAS-SM9}}\le&2C^{'}q_{\mathrm{s}}^{\eta^{'}}+\frac{1}{2^p}+\frac{q_\delta^2}{2^{l_3}}+\frac{3q_{\mathrm{S}}+q_{H_2}^2}{2^{l_{H_2}}}\\&+\frac{q_{\mathrm{S}}+q_{H_3}^2}{2^{l_{H_3}}}+\frac{\left(q_{\mathrm{E}}+q_{\mathrm{S}}\right)^2}{p}+\frac{2q_{\mathrm{S}}+q_{\mathrm{f}}^2}{2^{l_2}}\\&+\frac{3q_{\mathrm{S}}+q_{H_1}^2}{2^{l_{H_1}}}+2q_{\mathrm{S}}\mathrm{Adv}_{\mathcal{A}^{'}}^{\mathrm{SM9}}\end{aligned}$$

4.2 MFAS-SM9启发式安全分析

本文提出的MFAS-SM9方案基于商密SM9密码算法框架构造，并采用模糊验证和蜜罐口令等安全技术增强方案的安全性。本节利用启发式安全分析方法证明MFAS-SM9方案能够抵抗口令猜测攻击、设备捕获攻击、内部攻击以及重放攻击等，并具有前向安全性和匿名性。

口令猜测攻击 本文在MFAS – SM9方案中引入模糊验证和蜜罐口令技术，增强认证系统的安全性，防止口令被成功猜测。假设敌手$\mathcal{A}$获得智能卡$\mathrm{SC}_{\mathrm{UE}}$以及用户生物特征$\mathrm{BIO}_{\mathrm{UE}}$，敌手$\mathcal{A}$从智能卡$\mathrm{SC}_{\mathrm{UE}}$提取数据$\{\mathrm{CR}_1,\mathrm{CR}_2,\mathrm{CR}_3,\mathrm{PID}_{\mathrm{UE}},N_{\mathrm{UE}},\theta_{\mathrm{UE}},\mathrm{Gen}(\cdot),\mathrm{Gen}(\cdot)\}$，进一步恢复$\sigma_{\mathrm{UE}}^*=\mathrm{Rep}(\mathrm{BIO}_{\mathrm{UE}},\theta_{\mathrm{UE}})$。由于$\mathrm{CR}_1=H_1\left(H_1(\mathrm{MID}_{\mathrm{UE}})\oplus H_1\left(\mathrm{HPW}_{\mathrm{UE}}\right)\mathrm{mod}n_{\mathrm{p}}\right)$使用模糊验证技术，假设用户标识和口令长度为32 Byte，当$n_{\mathrm{p}}=2^8$时，将存在$\frac{2^{32}\times2^{32}}{2^8}$个可能标识口令对$(\mathrm{ID},\mathrm{PW})$满足$\mathrm{CR}_1=\mathrm{CR}_1^*$。而当敌手$\mathcal{A}$执行在线猜测攻击时，认证网关利用蜜罐口令技术实时检测敌手$\mathcal{A}$的攻击行为，一旦可疑行为超过门限

$T_{\mathrm{S}}(\approx 10)$后，认证网关拒绝响应来自该智能卡的登录请求。此外，CR_2时认证网关利用密钥$\mathrm{sk}_{\mathrm{ID_{AG}}}$产生的一个伪随机值，只要密钥$\mathrm{sk}_{\mathrm{ID_{AG}}}$不被泄露，则敌手$\mathcal{A}$无法从$\mathrm{CR}_2$获得有关口令的任何信息。而$\mathrm{CR}_3$与$\mathrm{CR}_1$相关，因此敌手$\mathcal{A}$无法执行在线猜测攻击。

设备捕获攻击　假设传感器节点的密钥发生泄露，即敌手$\mathcal{A}$获得密钥$\mathrm{sk}_{\mathrm{ID_{SN}}}$，但敌手$\mathcal{A}$无法通过$\mathrm{sk}_{\mathrm{ID_{SN}}}$得到其他传感器节点的密钥，因此不会对用户、认证网关以及其他传感器节点产生威胁。由于方案中每一次会话中使用的随机数r_1, r_2, r_3, r_4, r_5不会被存储，因此即使获得密钥$\mathrm{sk}_{\mathrm{ID_{SN}}}$，敌手$\mathcal{A}$也无法重构之前的会话密钥。假设认证网关的密钥$\mathrm{sk}_{\mathrm{ID_{AG}}}$发生泄露，但随机值$r_5$对认证网关保持机密，且在不知道用户密钥$\mathrm{sk}_{\mathrm{ID_{UE}}}$的前提下无法通过公开信息$\mathrm{CT}_5$恢复$r_5$。因此，MFAS-SM9方案可以抵抗设备捕获攻击。

内部攻击　假设存在内部攻击敌手$\mathcal{A}$，尝试从注册信息获取口令$\mathrm{PW}_{\mathrm{UE}}$的值。从MFAS-SM9方案可知，注册信息$\mathrm{CT}_1=\{c_1, s_1, t_1, T_1\}$是加密后的密文，敌手$\mathcal{A}$不知道认证网关密钥$\mathrm{sk}_{\mathrm{ID_{AG}}}$就无法从该密文中获取关于用户口令$\mathrm{PW}_{\mathrm{UE}}$的有效信息。同理，在不知道传感器节点的密钥$\mathrm{sk}_{\mathrm{ID_{SN}}}$或者用户密钥$\mathrm{sk}_{\mathrm{ID_{UE}}}$时，敌手$\mathcal{A}$无法从$\mathrm{CT}_4=\{c_4, s_4, t_4, T_4\}$，$\mathrm{CT}_5=\{c_5, s_5, t_5, T_5\}$，$\mathrm{CT}_2=\{c_2, s_2, t_2, T_2\}$得到任何信息。

仿冒攻击　本文所提出的MFAS-SM9方案在数据传输过程中为每个消息M_i产生签名σ_i，若敌手$\mathcal{A}$尝试伪装成合法用户，$\mathcal{A}$必须获得用户的密钥$\mathrm{sk}_{\mathrm{ID_{UE}}}$才能成功伪造消息的签名；否则，在不知道密钥$\mathrm{sk}_{\mathrm{ID_{UE}}}$时，敌手$\mathcal{A}$无法生成有效签名而无法伪装成用户。同理，敌手$\mathcal{A}$无法伪装成认证网关或传感器节点。

消息重放攻击　由于使用公开信道，任何敌手$\mathcal{A}$都能够截取传输的数据并尝试发起消息重放攻击。在MFAS-SM9方案中，通过将时间戳T_i引入到消息M_i中，再通过加密算法生成密文CT_i，即$c_1=(M_i||T_i)\oplus H_3(t_i||w_i||\mathrm{ID})$，将$\mathrm{CT}_i=\{c_i, s_i, t_i, T_i\}$。接收者可以在解密后验证时间戳是否满足$|T_i^{'}-T_i|\le\Delta T$，从而抵抗消息重放攻击。

匿名性　在MFAS-SM9方案中，用户在注册阶段计算$\mathrm{MID}_{\mathrm{UE}}=H_1(\mathrm{ID}_{\mathrm{UE}}||r_1)$，隐藏了真实标识信息$\mathrm{ID}_{\mathrm{UE}}$，并且每一次会话都重新选取随机数$r_1$，确保每次会话能产生动态的随机标识，从而具有不可追踪性。

前向安全性　假设认证网关的密钥$\mathrm{sk}_{\mathrm{ID_{AG}}}$被泄露，但随机值$r_5$对认证网关保持机密，敌手$\mathcal{A}$在不知道用户密钥$\mathrm{sk}_{\mathrm{ID_{UE}}}$时无法通过公开信息$\mathrm{CT}_5$恢复$r_5$。因此，认证网关的密钥$\mathrm{sk}_{\mathrm{ID_{AG}}}$泄露无法使敌手$\mathcal{A}$重构会话密钥。

口令更新　当用户需要更新口令时，MFAS – SM9方案能够实现在不需要与远程认证网关交互的前提下，在本地自主地更新口令$\mathrm{PW}_{\mathrm{UE}}\rightarrow\mathrm{PW}_{\mathrm{UE}}^{\mathrm{new}}$。

5　方案分析

本节将MFAS-SM9方案与近几年基于椭圆曲线密码体系设计的认证方案相比较，分别给出在安全性、计算开销和通信开销上的比较结果。

文献[22]提出了一个基于区块链的匿名认证方案并且具有用户审计功能；文献[23]提出了在数据采集传感器网络中安全的认证方案，并提供数据完整性保护；文献[24]提出一种用于无线体域网安全通信的有效匿名身份验证方案，同时提供消息机密性；文献[25]提出一种用于车联网的匿名认证方案并具有批处理能力；文献[26]设计了一种用于空天信息网络并具有快速路由的匿名认证方案；文献[27, 28]提出用于无线体域网的身份认证方案。文献[29]提出了一种具有本地数据隐私保护的匿名认证方案。文献[30]提出了一种具有隐私保护的多因素认证方案，并在标准模型下分析了方案的安全性。文献[3]提出一种面向多网关的多因素认证方案，该方案可以用于分布式系统。表1给出了方案的安全性比较。根据预备知识中给出的敌手模型和评价指标，可以发现本文相比较其他文献具有良好的安全性。

表2给出了方案的计算开销比较。其中T_{H}表示哈希运算，T_{C}表示群元素乘法运算，T_{M}表示MapToPoint运算，T_{E}表示群元素幂运算，T_{P}表示配对运算，T_{S}表示对称加密/解密运算。表3给出了方案的通信开销比较。其中$|\mathbb{G}_1|$表示群$\mathbb{G}_1$中元素的大小，$|\mathbb{G}_2|$表示群$\mathbb{G}_2$中元素的大小，$|\mathbb{G}_{\mathrm{T}}|$表示群$\mathbb{G}_{\mathrm{T}}$中元素的大小，$|\mathbb{Z}_p^*|$表示群$\mathbb{Z}_p^*$中元素的大小。计算开销和通信开销的对比结果表明MFAS-SM9方案适用于无线传感器设备。

本文使用Intel(R) Core(TM) i5-12500H 2.50 GHz性能计算机，并基于PBC (Pairing-Based Cryptography) 密码学库测试相关密码学运算开销。其中，哈希运算约为1.381 ms；群元素的乘运算约为2.653 ms；幂运算约为3.443 ms；对称加密运算约为2.251 ms；MapToPoint运算约为2.923 ms；配对运算约为6.274 ms。本文选取BN曲线进行通信开销测试，其中$|\mathbb{G}_1|=256$ bit，$|\mathbb{G}_2|=512$ bit，$|\mathbb{G}_{\mathrm{T}}|=3\,072$ bit，$|\mathbb{Z}_p^*|=256$ bit。

图4和图5分别给出了本文与相关方案的计算开销对比和通信开销对比结果，从图4和图5可以看

表 1 方案的敌手模型和系统评价指标对比

文献	敌手模型						系统评价指标											
	1	2	3	4	5	6	1	2	3	4	5	6	7	8	9	10	11	12
文献[22]	√	√	√	×	×	√	√	×	√	√	×	√	√	√	√	√	√	√
文献[23]	√	√	√	×	×	√	√	√	√	×	×	√	√	√	√	√	×	×
文献[24]	√	√	√	√	×	√	√	×	√	√	×	√	√	×	√	√	×	√
文献[25]	√	√	√	×	×	√	√	×	√	√	×	√	√	√	√	√	√	×
文献[26]	√	√	√	√	×	√	√	√	√	√	×	√	√	√	√	√	√	√
文献[27]	√	√	√	×	×	√	√	×	√	√	×	√	√	×	√	√	×	×
文献[28]	√	√	√	×	×	√	√	×	√	√	×	√	√	√	√	√	√	×
文献[29]	√	√	√	×	√	√	√	×	√	√	×	√	√	×	√	√	×	×
文献[30]	√	√	√	√	×	√	√	×	√	√	×	√	√	√	√	√	×	×
文献[3]	√	√	×	√	√	√	√	×	√	√	√	√	√	√	√	√	√	√
MFAS-SM9	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√

其中，“√”表示满足该条件；“×”表示不满足该条件。

表 2 方案的计算开销对比

文献	用户	认证网关	传感器节点
文献[22]	$4T_{\mathrm{H}}+6T_{\mathrm{C}}+4T_{\mathrm{M}}+2T_{\mathrm{P}}$	$5T_{\mathrm{H}}+4T_{\mathrm{M}}+3T_{\mathrm{E}}+4T_{\mathrm{P}}$	$9T_{\mathrm{H}}+2T_{\mathrm{M}}+7T_{\mathrm{E}}+4T_{\mathrm{P}}$
文献[23]	$21T_{\mathrm{H}}+2T_{\mathrm{C}}+4T_{\mathrm{M}}+2T_{\mathrm{s}}+2T_{\mathrm{P}}$	$13T_{\mathrm{H}}+6T_{\mathrm{c}}+4T_{\mathrm{M}}+6T_{\mathrm{S}}+2T_{\mathrm{P}}$	$6T_{\mathrm{H}}+2T_{\mathrm{M}}+2T_{\mathrm{S}}+2T_{\mathrm{P}}$
文献[24]	$5T_{\mathrm{H}}+11T_{\mathrm{C}}+2T_{\mathrm{M}}+2T_{\mathrm{s}}$	—	$7T_{\mathrm{H}}+12T_{\mathrm{C}}+4T_{\mathrm{M}}+2T_{\mathrm{s}}+4T_{\mathrm{P}}$
文献[25]	$T_{\mathrm{H}}+3T_{\mathrm{E}}+T_{\mathrm{P}}$	—	$T_{\mathrm{H}}+2T_{\mathrm{E}}+T_{\mathrm{M}}+T_{\mathrm{P}}$
文献[26]	$2T_{\mathrm{H}}+4T_{\mathrm{E}}+19T_{\mathrm{C}}+2T_{\mathrm{P}}$	$2T_{\mathrm{H}}+5T_{\mathrm{E}}+14T_{\mathrm{C}}+5T_{\mathrm{P}}$	$T_{\mathrm{H}}+4T_{\mathrm{E}}+4T_{\mathrm{C}}$
文献[27]	$8T_{\mathrm{H}}+2T_{\mathrm{E}}+9T_{\mathrm{C}}+4T_{\mathrm{M}}+2T_{\mathrm{s}}+3T_{\mathrm{P}}$	—	$7T_{\mathrm{H}}+2T_{\mathrm{E}}+4T_{\mathrm{C}}+4T_{\mathrm{M}}+2T_{\mathrm{s}}+4T_{\mathrm{P}}$
文献[28]	$6T_{\mathrm{H}}+4T_{\mathrm{E}}+3T_{\mathrm{C}}+T_{\mathrm{S}}$	—	$3T_{\mathrm{H}}+4T_{\mathrm{E}}+2T_{\mathrm{C}}+T_{\mathrm{S}}+T_{\mathrm{P}}$
文献[29]	$12T_{\mathrm{H}}+4T_{\mathrm{C}}$	$18T_{\mathrm{H}}+5T_{\mathrm{C}}$	$7T_{\mathrm{H}}+2T_{\mathrm{C}}$
文献[30]	$2T_{\mathrm{H}}+2T_{\mathrm{B}}+T_{\mathrm{C}}+4T_{\mathrm{E}}+6T_{\mathrm{PRF}}+T_{\mathrm{S}}+T_{\mathrm{Sig}}$	—	$2T_{\mathrm{H}}+3T_{\mathrm{C}}+5T_{\mathrm{E}}+6T_{\mathrm{PRF}}+T_{\mathrm{S}}+2T_{\mathrm{Sig}}$
文献[3]	$17T_{\mathrm{H}}+2T_{\mathrm{B}}+3T_{\mathrm{C}}$	$15T_{\mathrm{H}}+T_{\mathrm{C}}$	$4T_{\mathrm{H}}+2T_{\mathrm{C}}$
MFAS-SM9	$12T_{\mathrm{H}}+4T_{\mathrm{C}}+2T_{\mathrm{E}}+2T_{\mathrm{P}}$	$6T_{\mathrm{H}}+3T_{\mathrm{C}}+2T_{\mathrm{E}}+T_{\mathrm{P}}$	$7T_{\mathrm{H}}+5T_{\mathrm{C}}+2T_{\mathrm{E}}+2T_{\mathrm{P}}$

表 3 方案的通信开销对比

文献	用户	认证网关	传感器节点
文献[22]	$\lvert\mathbb{G}_1\rvert+2\lvert\mathbb{G}_2\rvert+5\lvert\mathbb{G}_{\mathrm{T}}\rvert+5\lvert\mathbb{Z}_p^*\rvert$	$4\lvert\mathbb{G}_1\rvert+3\lvert\mathbb{G}_2\rvert+6\lvert\mathbb{G}_{\mathrm{T}}\rvert+6\lvert\mathbb{Z}_p^*\rvert$	$\lvert\mathbb{G}_1\rvert+2\lvert\mathbb{G}_2\rvert+3\lvert\mathbb{G}_{\mathrm{T}}\rvert+5\lvert\mathbb{Z}_p^*\rvert$
文献[23]	$\lvert\mathbb{G}_1\rvert+2\lvert\mathbb{G}_2\rvert+\lvert\mathbb{G}_{\mathrm{T}}\rvert+6\lvert\lvert\mathbb{Z}_p^*\rvert$	$\lvert\mathbb{G}_1\rvert+2\lvert\mathbb{G}_2\rvert+2\lvert\mathbb{G}_{\mathrm{T}}\rvert+15\lvert\mathbb{Z}_p^*\rvert$	$\lvert\mathbb{G}_{\mathrm{T}}\rvert+5\lvert\mathbb{Z}_p^*\rvert$
文献[24]	$2\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert+3\lvert\mathbb{Z}_p^*\rvert$	—	$2\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert+2\lvert\mathbb{Z}_p^*\rvert$
文献[25]	$\lvert\mathbb{G}_1\rvert+2\lvert\mathbb{G}_2\rvert+5\lvert\mathbb{Z}_p^*\rvert$	—	$2\lvert\mathbb{G}_1\rvert+2\lvert\mathbb{G}_2\rvert+3\lvert\mathbb{Z}_p^*\rvert$
文献[26]	$5\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert+4\lvert\mathbb{Z}_p^*\rvert$	$4\lvert\mathbb{G}_1\rvert+2\lvert\mathbb{G}_2\rvert+8\lvert\mathbb{Z}_p^*\rvert$	$\lvert\mathbb{G}_1\rvert+\lvert\mathbb{Z}_p^*\rvert$
文献[27]	$3\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert+5\lvert\mathbb{Z}_p^*\rvert$	—	$\lvert\mathbb{G}_1\rvert+\lvert\mathbb{Z}_p^*\rvert$
文献[28]	$2\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert+3\lvert\mathbb{Z}_p^*\rvert$	—	$\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert+3\lvert\mathbb{Z}_p^*\rvert$
文献[29]	$2\lvert\mathbb{G}_1\rvert+9\lvert\mathbb{Z}_p^*\rvert$	$\lvert\mathbb{G}_1\rvert+13\lvert\mathbb{Z}_p^*\rvert$	$\lvert\mathbb{G}_1\rvert+10\lvert\mathbb{Z}_p^*\rvert$
文献[30]	$2\lvert\mathbb{G}_1\rvert+3\lvert\mathbb{Z}_p^*\rvert$	—	$\lvert\mathbb{G}_1\rvert+4\lvert\mathbb{Z}_p^*\rvert$
文献[3]	$2\lvert\mathbb{G}_1\rvert+5\lvert\mathbb{Z}_p^*\rvert$	$2\lvert\mathbb{G}_1\rvert+8\lvert\mathbb{Z}_p^*\rvert$	$\lvert\mathbb{G}_1\rvert+\lvert\mathbb{Z}_p^*\rvert$
MFAS-SM9	$2\lvert\mathbb{G}_1\rvert+3\lvert\mathbb{Z}_p^*\rvert$	$2\lvert\mathbb{G}_1\rvert+2\lvert\mathbb{Z}_p^*\rvert$	$2\lvert\mathbb{G}_1\rvert+2\lvert\mathbb{Z}_p^*\rvert$

出， MFAS-SM9方案的计算开销和通信开销居于第2位，高于文献[3]所提方案。

6 结束语

身份认证方案为无线传感器系统建立了网络安

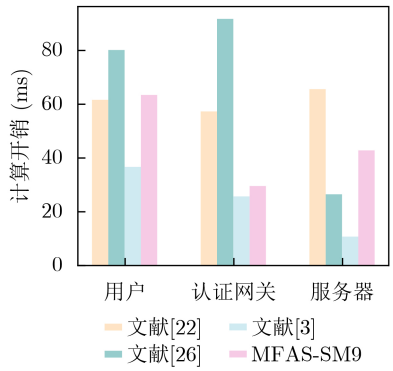

图 4 方案的计算开销对比

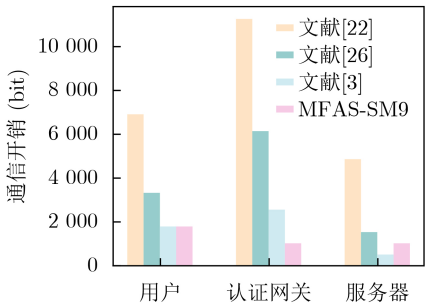

图 5 方案的通信开销对比

全的第一道防线，能有效阻止恶意攻击者的非法访问，保护了传感器中敏感数据的安全。本文在商密SM9标识密码算法框架下提出一种多因素认证方案，使用口令、生物特征以及智能卡作为认证因素，既提供了安全高效的认证方式，也符合国家网络空间安全核心技术自主可控的发展战略。与现有方案相比，本文提出的MFAS-SM9方案在保证安全性的前提下，也适用于无线传感器系统。物理不可克隆函数可以提高本地硬件安全性，因此我们将进一步研究在商密SM9密码算法框架下设计基于物理不可克隆函数的多因素认证方案 。

参 考 文 献

[1] 李文婷, 汪定, 王平. 无线传感器网络下多因素身份认证协议的内部人员攻击[J]. 软件学报, 2019, 30(8): 2375–2391. doi: 10.13328/j.cnki.jos.005766.
LI Wenting, WANG Ding, and WANG Ping. Insider attacks against multi-factor authentication protocols for wireless sensor networks[J]. *Journal of Software*, 2019, 30(8): 2375–2391. doi: 10.13328/j.cnki.jos.005766.

[2] SON S, LEE J, PARK Y, *et al*. Design of blockchain-based lightweight V2I handover authentication protocol for VANET[J]. *IEEE Transactions on Network Science and Engineering*, 2022, 9(3): 1346–1358. doi: 10.1109/TNSE.2022.3142287.

[3] 王晨宇, 汪定, 王菲菲, 等. 面向多网关的无线传感器网络多因素认证协议[J]. 计算机学报, 2020, 43(4): 683–700. doi: 10.11897/SP.J.1016.2020.00683.
WANG Chenyu, WANG Ding, WANG Feifei, *et al*. Multi-factor user authentication scheme for multi-gateway wireless sensor networks[J]. *Chinese Journal of Computers*, 2020, 43(4): 683–700. doi: 10.11897/SP.J.1016.2020.00683.

[4] 汪定, 王平, 雷鸣. 基于RSA的网关口令认证密钥交换协议的分析与改进[J]. 电子学报, 2015, 43(1): 176–184. doi: 10.3969/j.issn.0372-2112.2015.01.028.
WANG Ding, WANG Ping, and LEI Ming. Cryptanalysis and improvement of gateway-oriented password authenticated key exchange protocol based on RSA[J]. *Acta Electronica Sinica*, 2015, 43(1): 176–184. doi: 10.3969/j.issn.0372-2112.2015.01.028.

[5] YU S and PARK Y. A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions[J]. *IEEE Internet of Things Journal*, 2022, 9(20): 20214–20228. doi: 10.1109/JIOT.2022.3171791.

[6] WATRO R, KONG D, CUTI S F, *et al*. TinyPK: Securing sensor networks with public key technology[C]. Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, Washington, USA, 2004: 59–64. doi: 10.1145/1029102.1029113.

[7] DAS M L. Two-factor user authentication in wireless sensor networks[J]. *IEEE Transactions on Wireless Communications*, 2009, 8(3): 1086–1090. doi: 10.1109/TWC.2008.080128.

[8] HUANG Huifeng, CHANG Yafen, and LIU Chunhung. Enhancement of two-factor user authentication in wireless sensor networks[C]. Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Darmstadt, Germany, 2010: 27–30. doi: 10.1109/IIHMSP.2010.14.

[9] WANG Ding and WANG Ping. On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions[J]. *Computer Networks*, 2014, 73: 41–57. doi: 10.1016/j.comnet.2014.07.010.

[10] SADRI M J and ASAAR M R. An anonymous two-factor authentication protocol for IoT-based applications[J]. *Computer Networks*, 2021, 199: 108460. doi: 10.1016/j.comnet.2021.108460.

[11] ALLADI T, CHAMOLA V, and NAREN N. HARCI: A two-way authentication protocol for three entity healthcare IoT networks[J]. *IEEE Journal on Selected Areas in Communications*, 2021, 39(2): 361–369. doi: 10.1109/JSAC.2020.3020605.

[12] JIANG Jingwei, WANG Ding, ZHANG Guoyin, *et al*. Quantum-resistant password-based threshold single-sign-on authentication with updatable server private key[C]. 27th

European Symposium on Research in Computer Security, Copenhagen, Denmark, , 2022: 295–316. doi: 10.1007/978-3-031-17146-8_15.

[13] WANG Qingxuan, WANG Ding, CHENG Chi, *et al*. Quantum2FA: Efficient quantum-resistant two-factor authentication scheme for mobile devices[J]. *IEEE Transactions on Dependable and Secure Computing*, 2023, 20(1): 193–208. doi: 10.1109/TDSC.2021.3129512.

[14] WANG Ding and WANG Ping. Two birds with one stone: Two-factor authentication with security beyond conventional bound[J]. *IEEE Transactions on Dependable and Secure Computing*, 2018, 15(4): 708–722. doi: 10.1109/TDSC.2016.2605087.

[15] WANG Qingxuan and WANG Ding. Understanding failures in security proofs of multi-factor authentication for mobile devices[J]. *IEEE Transactions on Information Forensics and Security*, 2023, 18: 597–612. doi: 10.1109/TIFS.2022.3227753.

[16] CHENG Zhaohui. Security analysis of SM9 key agreement and encryption[C]. 14th International Conference on Information Security and Cryptology, Fuzhou, China, 2019: 3–25. doi: 10.1007/978-3-030-14234-6_1.

[17] 赖建昌, 黄欣沂, 何德彪, 等. 国密SM9数字签名和密钥封装算法的安全性分析[J]. 中国科学:信息科学, 2021, 51(11): 1900–1913. doi: 10.1360/SSI-2021-0049.

LAI Jianchang, HUANG Xinyi, HE Debiao, *et al*. Security analysis of SM9 digital signature and key encapsulation[J]. *SCIENTIA SINICA Informationis*, 2021, 51(11): 1900–1913. doi: 10.1360/SSI-2021-0049.

[18] LAI Jianchang, HUANG Xinyi, HE Debiao, *et al*. Provably secure online/offline identity-based signature scheme based on SM9[J]. *The Computer Journal*, 2022, 65(7): 1692–1701. doi: 10.1093/comjnl/bxab009.

[19] 赖建昌, 黄欣沂, 何德彪, 等. 基于SM9的CCA安全广播加密方案[J]. 软件学报, 2023, 34(7): 3354–3364. doi: 10.13328/j.cnki.jos.006531.

LAI Jianchang, HUANG Xinyi, HE Debiao, *et al*. CCA secure broadcast encryption based on SM9[J]. *Journal of Software*, 2023, 34(7): 3354–3364. doi: 10.13328/j.cnki.jos.006531.

[20] LI Nan, GUO Fuchun, MU Yi, *et al*. Fuzzy extractors for biometric identification[C]. 37th International Conference on Distributed Computing Systems, Atlanta, USA, 2017: 667–677. doi: 10.1109/ICDCS.2017.107.

[21] BELLARE M, POINTCHEVAL D, and ROGAWAY P. Authenticated key exchange secure against dictionary attacks[C]. International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, 2000: 139–155. doi: 10.1007/3-540-45539-6_11.

[22] LYU Qiuyun, LI Hao, DENG Zhining, *et al*. A2UA: An auditable anonymous user authentication protocol based on blockchain for cloud services[J]. *IEEE Transactions on Cloud Computing*, 2023, 11(3): 2546–2561. doi: 10.1109/TCC.2022.3216580.

[23] ZHOU Quan, TANG Chunming, ZHEN Xianghan, *et al*. A secure user authentication protocol for sensor network in data capturing[J]. *Journal of Cloud Computing*, 2015, 4(1): 6. doi: 10.1186/s13677-015-0030-z.

[24] AZEES M, VIJAYAKUMAR P, KARUPPIAH M, *et al*. An efficient anonymous authentication and confidentiality preservation schemes for secure communications in wireless body area networks[J]. *Wireless Networks*, 2021, 27(3): 2119–2130. doi: 10.1007/s11276-021-02560-y.

[25] VIJAYAKUMAR P, AZEES M, KOZLOV S A, *et al*. An anonymous batch authentication and key exchange protocols for 6G enabled VANETs[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2022, 23(2): 1630–1638. doi: 10.1109/TITS.2021.3099488.

[26] YANG Qingyou, XUE Kaiping, XU Jie, *et al*. AnFRA: Anonymous and fast roaming authentication for space information network[J]. *IEEE Transactions on Information Forensics and Security*, 2019, 14(2): 486–497. doi: 10.1109/TIFS.2018.2854740.

[27] ARFAOUI A, BOUDIA O R M, KRIBÈCHE A, *et al*. Context-aware access control and anonymous authentication in WBAN[J]. *Computers & Security*, 2020, 88: 101496. doi: 10.1016/j.cose.2019.03.017.

[28] ODELU V, SAHA S, PRASATH R, *et al*. Efficient privacy preserving device authentication in WBANs for industrial e-health applications[J]. *Computers & Security*, 2019, 83: 300–312. doi: 10.1016/j.cose.2019.03.002.

[29] VIJAYAKUMAR P, OBAIDAT M S, AZEES M, *et al*. Efficient and secure anonymous authentication with location privacy for IoT-based WBANs[J]. *IEEE Transactions on Industrial Informatics*, 2020, 16(4): 2603–2611. doi: 10.1109/TII.2019.2925071.

[30] 魏福山, 张刚, 马建峰, 等. 标准模型下隐私保护的多因素密钥交换协议[J]. 软件学报, 2016, 27(6): 1511–1522. doi: 10.13328/j.cnki.jos.005001.

WEI Fushan, ZHANG Gang, MA Jianfeng, *et al*. Privacy-preserving multi-factor key exchange protocol in the standard model[J]. *Journal of Software*, 2016, 27(6): 1511–1522. doi: 10.13328/j.cnki.jos.005001.

朱留富：博士生，研究方向为公钥密码学、密码安全协议.

汪 定：教授，博士生导师，研究方向为公钥密码学、信息安全.

责任编辑：陈 倩