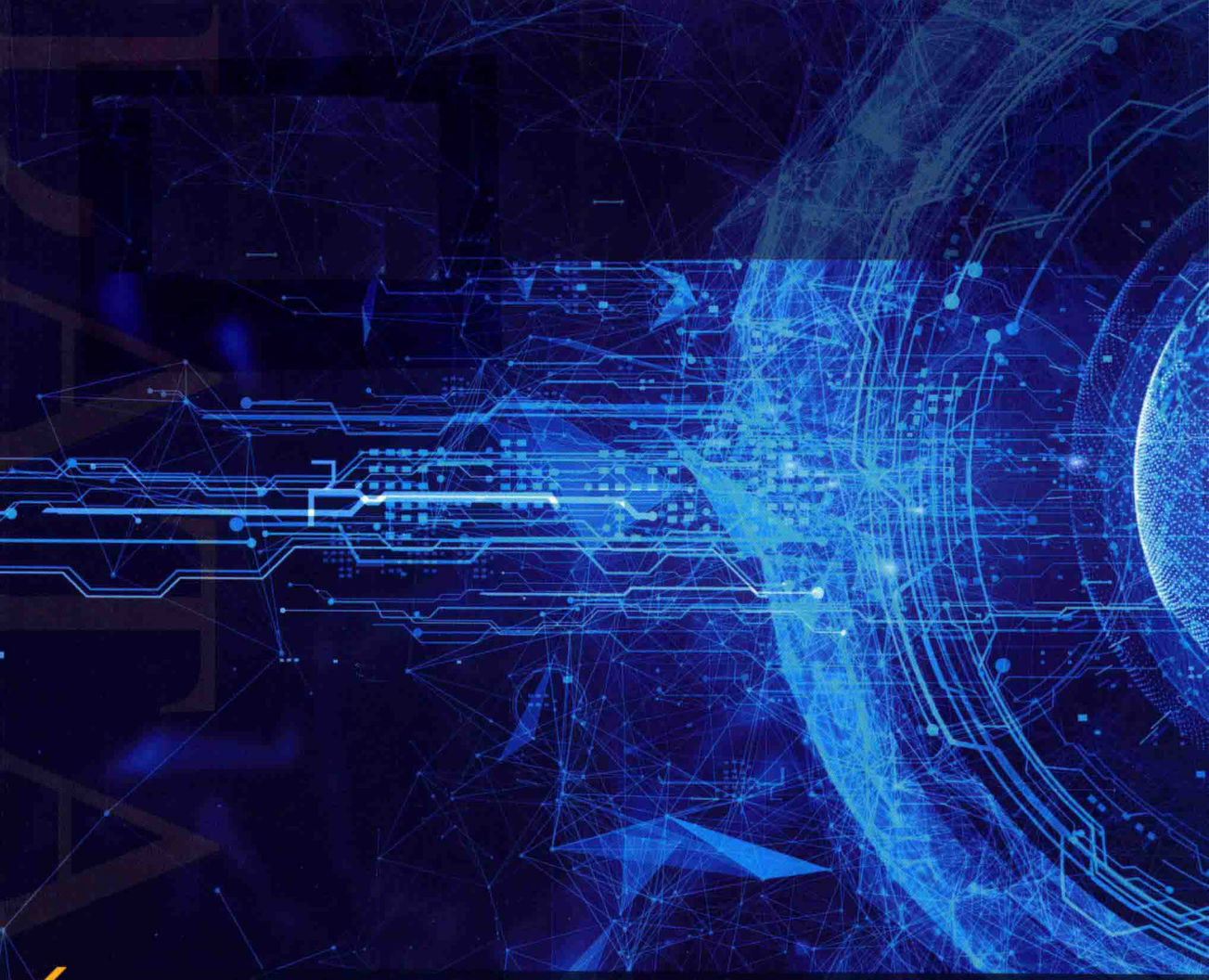

可穿戴设备数据安全及隐私保护

Data Security and Privacy Protection for Wearable Devices

王　俊　朱容波/著

科学出版社

DATA

可穿戴设备数据安全及隐私保护

Data Security and Privacy Protection for Wearable Devices

王 俊 朱容波/著

科学出版社

北 京

内 容 简 介

本书包括6章，全面系统地介绍了可穿戴设备数据安全及隐私保护的基本理论、关键技术及最新成果，主要内容包括基于PUF与IPI的可穿戴设备双因子认证协议、基于平衡D触发器仲裁器的PUF安全性增强、基于FA策略的可穿戴设备空间数据差分隐私发布方案、基于网格划分的空间数据差分隐私发布方案、基于UKF的可穿戴设备流数据差分隐私发布方案等。

本书可供信息安全、网络、通信等专业的科研人员、硕士和博士研究生参考，也可供高等院校相关专业的师生参考。

图书在版编目(CIP)数据

可穿戴设备数据安全及隐私保护 / 王俊，朱容波著.
—北京：科学出版社，2018.9

ISBN 978-7-03-058727-5

Ⅰ.①可… Ⅱ.①王… ②朱… Ⅲ.①移动终端-智能终端-安全技术
Ⅳ.①TN87

中国版本图书馆CIP数据核字（2018）第206956号

责任编辑：李 敏 杨逢渤 / 责任校对：彭 涛
责任印制：肖 兴 / 封面设计：无极书装

科学出版社 出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com

河北鹏润印刷有限公司 印刷
科学出版社发行 各地新华书店经销
*
2018年9月第 一 版 开本：787×1092 1/16
2018年9月第一次印刷 印张：8 1/4
字数：300 000

定价：98.00元
（如有印装质量问题，我社负责调换）

序　言

随着计算机及网络技术的飞速发展，我们迎来了大数据时代。从初始的数据传送基本业务，到当今的大数据驱动经济，我们已经生活在信息的世界里。与此同时，我们的个人痕迹与信息被完全记录，给数据安全和隐私带来重大隐患。数据安全与隐私作为信息技术的重要组成部分，孕育着新的重大突破机遇，正加速向数据业务和数据安全融合方向发展。急速增长的网络用户与数据量，导致数据安全和隐私问题加剧。构建安全防护策略、保护数据隐私已经成为信息安全领域意义重大、亟待解决的研究课题。

针对数据安全和隐私保护这一目的，目前的工作集中在加密、认证、扰动等方面，通过数据加密、身份认证和数据扰动来确保数据安全并保护用户隐私。轻量级身份认证和差分隐私数据发布作为无线体域网环境下可穿戴设备数据安全与隐私保护的关键技术，成为可穿戴设备快速发展的两大技术保障。利用物理不可克隆函数和差分隐私技术，考虑数据安全性和可用性的同时，如何设计轻量级身份认证协议与差分隐私数据发布算法，成为信息安全领域一个新的研究热点。

该书作者长期从事信息安全领域的科学研究与应用开发工作，重点研究轻量级身份认证协议与差分隐私数据发布算法，并取得了一系列重要成果，发表了一批高质量的学术论文，获得了国际同行的广泛关注。该书是这些研究成果的总结，该书的出版将为传播轻量级身份认证协议设计的基础知识、交流差分隐私理论与技术、推进可穿戴设备的发展做出贡献。

作为作者的国际同行，见证了他们的努力学习、刻苦研究及工作后的勤奋与付出。我为他们取得的研究成果和学术著作的出版感到由衷的高兴，并表示由衷祝贺！

马懋德

2018 年 4 月 25 日

前　言

可穿戴设备是指整合到用户衣服，或附于皮肤表面，或直接植入体内的智能化设备。它引导着当今数字化浪潮的发展方向，是未来最有发展前景的技术之一。可穿戴设备与人紧密结合，并以人为载体，主要面向个人服务，提供额外的附加功能，甚至提升人的本能。特别是未来的可穿戴技术，有部分设备非“戴”，而是“种”在人身上，实现治疗疾病、监测状态、改善人体机能，甚至提供人们之前不具备的某种能力等。蓬勃发展的可穿戴设备，给人类带来前所未有生活便利的同时，也会侵犯个人隐私，甚至威胁人身安全。在无线体域网开放式结构下，如何为设备节点和数据中心之间提供一种安全认证机制并保护用户隐私信息，成为信息安全领域一个新的发展趋势和研究热点。

本书包括6章，全面系统地介绍了可穿戴设备数据安全及隐私保护的基本理论、关键技术及最新成果，主要内容包括基于PUF与IPI的可穿戴设备双因子认证协议、基于平衡D触发器仲裁器的PUF安全性增强、基于FA策略的可穿戴设备空间数据差分隐私发布方案、基于网格划分的空间数据差分隐私发布方案、基于UKF的可穿戴设备流数据差分隐私发布方案等。

本书的研究工作得到了国家自然科学基金项目（NO. 61772562，NO. 61272497）、湖北省技术创新专项重大项目（NO. CXZD2018000035）、湖北省自然科学基金杰出青年基金项目（NO. 2017CFA043）、武汉市应用基础研究计划项目（NO. 20170602010101-62）、中央高校基本科研业务费专项基金（NO. 2042017gf0038，2015211020201、YZZ18002）、国家民委中青年英才培养计划项目的支持，同时得到了许多同行和朋友的大力支持，研究生姬美琳参与了部分统稿工作，在此表示感谢。由于水平有限，对一些问题的理解和表述或有不足之处，诚请读者批评指正。

王　俊　朱容波

2018年4月28日

目　录

第1章 绪 论

本章首先介绍了面向健康服务的可穿戴设备安全认证与隐私数据发布的研究背景与意义；其次简要分析了可穿戴设备中安全认证与隐私数据发布的研究现状和存在的问题；再次给出了相关技术路线及关键技术；最后介绍了本书的总体组织结构。

1.1 引 言

可穿戴设备是指整合到用户衣服，或附于皮肤表面，或直接植入体内的智能化设备。它引导着当今数字化浪潮的发展方向，是未来最有发展前景的技术之一[1,2]。可穿戴科技网 WTVOX 指出，2016 年是可穿戴设备蓬勃发展的一年。例如，美国 Empatica 公司推出的 EmbraceWatch，是一款专门为患有癫痫的患者设计的智能腕带，可以帮助预测和防止癫痫发作。Proteus 数字医疗公司研发的可吞服性智能药丸 Helius，它可以在人的体内实时监测人体各种体征数据，以便观察患者病情并针对治疗。医疗科技公司 Medtronic 研发的 MiniMed 530G 人工胰岛系统，该系统监测佩戴者血糖值，若血糖值异常，可控制胰岛素泵注射相应剂量胰岛素，以防止佩戴者异常血糖事件[3]。据全球权威市场研究机构 CCS Insight 预测，到 2021 年，全球可穿戴设备市场可达 1.93 亿台[4]。图 1-1 展示了可穿戴设备市场上升变化趋势。

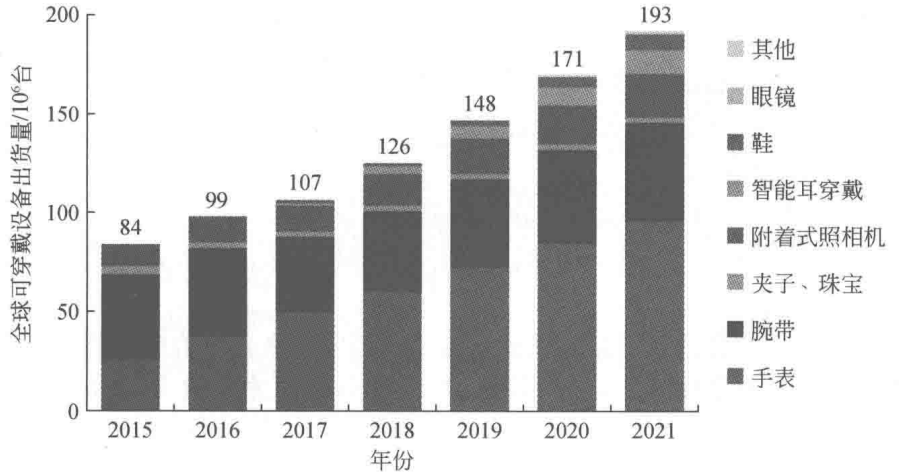

图 1-1 全球可穿戴设备市场预测

可穿戴技术以人为载体，主要面向个人服务，提供额外的附加功能，甚至提升人的本能。特别是未来的可穿戴技术，有部分设备非“戴”，而是“种”在人身上，实现治疗疾

病、监测状态、改善人体机能，甚至提供人们之前不具备的某种能力等[5]。因此，可穿戴设备在社交、健康、日常生活、工作和娱乐等方方面面都能使人兴趣盎然，特别是“互联网+”的普适特性已伸向医疗健康服务界。人体佩戴轻量的传感器进行健康数据监测，如体温、心率、血糖、大脑和肌肉活动等，以实现对患有心脏病、睡觉窒息、帕金森等患者提供必要的治疗；为手术后的患者康复提供监测、自动反馈控制和虚拟现实图像服务等[6]。服务提供商能通过可穿戴设备监测患者的健康状况并提供针对性的诊疗方案，甚至研发新的技术[5]。结合无线体域网（wireless body area network，WBAN）的移动医疗将是席卷全球的浪潮，对“传统医疗”模式将提出挑战。2017 年，在美国年度最大、最重要的健康服务 HIMSS（Healthcare Information and Management Systems Society，医疗卫生信息与管理系统协会）峰会上，“隐私与安全”与前两年一样依旧是频繁出现的热门话题。与会者一致认为，移动医疗涉及的隐私和安全问题必须引起重视。

人们对健康服务更好更快的需求，使得新的可穿戴设备拥有更强大的用户数据收集和处理能力，数据汇聚到后台服务器之后可对数据进一步处理与共享。例如，疾病控制中心，可以根据流感人群的空间位置信息，分析有关区域内流感的扩散趋势，从而有针对性地预警[7,8]。面向健康服务的可穿戴设备虽然应用前景广阔，但是这些设备与人紧密结合。对于用户来说，健康信息都是相对敏感的，任何不恰当的信息暴露都可能泄露用户隐私，导致严重的财产损失，甚至危及人身安全。缺少恰当的安全隐私保护，用户可能不接受可穿戴设备的应用[9]。

安全认证是确保可穿戴设备中用户数据安全的重要手段，但是传统认证机制通常基于密钥和证书[10]。密钥存储空间过大、协商过程复杂且不灵活，在资源受限的可穿戴设备环境下，直接应用传统认证机制不可行。为此，针对可穿戴设备资源受限特点，如何设计一种轻量级安全认证机制，并确保数据安全是值得研究的问题。

匿名化是确保用户隐私的常用方法，传统基于匿名模型的数据隐私保护方案被大量提出。例如，k-anonymity[11]和 l-diversity[12]，这类方案主要是基于限制发布技术。然而，基于匿名的方案也存在隐私泄露的风险，需要不断针对新泄露的风险提出修补方案。例如，de Montjoye 等[13]证明，仅需四条购买记录的时间和位置信息就能识别 110 万匿名信用卡消费数据集中 90% 的用户。

差分隐私（differential privacy）[14]是一种基于数据加噪扰动的隐私保护技术，具有隐私可量化、攻击能力可界定的良好性质，针对用户隐私安全，基于差分隐私的隐私数据发布是值得研究的问题。

良好的数据安全性和严密的隐私保护功能，是面向健康服务的可穿戴设备广泛应用的前提，只有人身安全得到保障，隐私得到保护，这类设备才能被大众接受，走向千家万户，惠及广大百姓。因此，系统地研究和解决可穿戴设备的数据安全与隐私保护问题，能为构建可穿戴设备的健康服务安全体系奠定坚实的安全理论基础，同时，对推动可穿戴设备的普及具有重要应用价值。

1.2　数据安全及隐私保护现状分析

面向健康服务的可穿戴设备与人的结合更紧密，大量涉及个人敏感数据，还可能伴有调节控制功能，如根据设置和测量结果，自动释放药物到体内。这些设备虽然提高了我们的生活质量，但也会涉及更多的个人隐私，对人身安全的威胁也更大。因此，数据安全和隐私保护是摆在我们面前的重要研究课题，需要重点研究安全认证和隐私数据发布问题。

1. 可穿戴设备安全认证

安全认证是确保可穿戴设备用户数据和人身安全的重要手段，可穿戴设备资源受限，直接应用传统认证机制不可行[15]。

WBAN 环境下针对可穿戴设备的认证研究起步较晚，结合可穿戴设备 In-body 和 On-body 易于获取生物特征的应用特点，很多认证采用了新型的生物特征认证方法。生物特征以其私有属性的唯一性，具有较强的安全性，在可穿戴设备安全防护上应用前景广阔[15]。2006 年，Poon 等[16]指出心率的间歇信号（interpulse interval，IPI）是一种良好的用户生物特征，适用于 WBAN 环境下的安全认证。2014 年，Zheng 等[17]提出通过心率特征提取密钥的方法，用于数据安全加密。2015 年，Thang 等[18]从步伐生物特征中模糊提取特征码，通过特征码进行认证。2015 年，Chen 等[19]针对移动设备，提出了一种基于行为节奏特征的认证方案，从用户有节奏的轻敲界面中提取特征与设备中存储的特征进行度量。然而，上述这些认证方案仅考虑了认证方私有属性的唯一性，而没有考虑设备的物理唯一性，易受到假冒攻击。

近年来，由于物理不可克隆函数（physical unclonable function，PUF）具有简便、安全的优势，被广泛应用于资源受限环境下的安全认证[20,21]。早期，基于 PUF 的认证采用存储的激励/响应对（challenge response pair，CRP）实现[22]。此方案需要存储大量 CRP，资源占用多。2012 年，Bassil 等[23]提出了一种基于 PUF 与循环移位操作的射频识别（radio frequency identification，RFID）安全认证方案，该方案也需存储大量的 CRP。2014 年，Rostami 等[24]提出了一种基于多 PUF 并联建模的轻量级认证协议，该方案通过建模进行匹配认证。2015 年，Akgün 和 Cağlayan[25]提出了一种基于 PUF 的可扩展认证协议，此协议能在常数时间复杂度下完成认证。然而，上述认证方案仅考虑了认证方设备物理属性的唯一性，而没有考虑用户私有属性的唯一性，存在假冒、妥协攻击的威胁。

以上方法中，单纯基于生物特征的认证，虽然可以保证私有属性的唯一性，但是容易受到假冒攻击，不能保证节点真实可信；单纯基于 PUF 的认证，虽然能够保证节点的物理唯一性，但不能保证节点一定属于本 WBAN 环境。为了同时保证设备物理属性和用户私有属性双重唯一性，我们认为，结合生物特征与 PUF 技术的认证方法，为 WBAN 环境中设备节点安全认证提供了一种新思路。

2. 健康服务数据隐私保护

面向健康服务可穿戴设备数据的高敏感性，使可穿戴设备从诞生之日起，便遭到用户

隐私泄漏的质疑[26,27]。而随着网络化、信息化的不断深入，用户隐私泄漏的风险越来越大[28]。基于隐私泄露的担忧，研究者提出了一系列隐私保护的用户数据共享方案。

基于传统密码学的隐私保护方案或使用假名 ID 来替换用户记录真实 ID[29]，或使用访问控制策略来确保用户记录仅能被特定用户组访问[30]。这些方法要么被现有去匿名化攻击证明十分脆弱，要么过程复杂[28,31]。

为确保用户信息的安全，提出大量基于 k-anonymity 模型的数据隐私保护方案[32]。这类方案主要是基于限制发布技术，其基本思想是通过对记录数据的准标示符进行泛化或截取处理。将数据集根据不同的泛化标示符进行划分，泛化标识符相同的记录数据归为一个等价类，并且使得每一个等价类中的记录数据不少于 k 个。换句话说，即将某一个用户的记录数据“隐藏”在对应等价类的 k 个记录当中，从而保护用户隐私。然而，基于匿名模型的方法缺乏对隐私保护程度的量化和对攻击者能力的清楚界定，仍然存在隐私泄露风险[12]。

基于概率模型的差分隐私改变了这一局面。差分隐私要求，单个记录数据对数据集查询结果的影响从概率上微小可控。同时差分隐私给出了攻击者的攻击能力上限，即假定在最差情况下，攻击者拥有除当前用户记录以外的所有记录数据，因此，能够抵御差分攻击即表明可以抵御所有已知和未知的隐私攻击。由于差分隐私具有上述隐私可量化、攻击能力可界定的良好性质，它被迅速地引入诸多数据查询与发布应用领域[33]。近年来，已有研究者将差分隐私成功引入智能仪表应用领域[34]和安全位置服务领域[35]，亦有研究者探讨了差分隐私引入健康数据上的可行性[36]。

差分隐私是一种严格证明和安全可控的隐私保护技术，能够保护用户敏感信息不被泄露。发布数据中添加噪声越大，数据越安全，然而，数据可用性越低。差分隐私具有良好的应用前景，但是，如何保护数据隐私的同时提高数据可用性是我们关注的问题[37]。本书分别针对健康服务数据中涉及的空间位置数据和健康状态统计时序数据，研究一种新型的差分隐私保护模型。

1.3 技术路线及关键技术

1.3.1 技术路线

面向健康服务的可穿戴设备的用户数据至关重要，轻则涉及个人隐私，重则关乎人身安危，解决可穿戴设备安全问题迫在眉睫。但可穿戴设备资源受限，在安全认证方面，现有研究成果虽有超轻量化认证机制，但这些机制只针对设备的物理属性进行认证，保证不了用户的私有属性；在隐私保护方面，现有研究成果没有针对可穿戴设备数据特点，在数据安全性与可用性上达不到理想效果。因此，针对可穿戴设备及其数据特点，研究安全认证和隐私保护的新机制，对推动可穿戴设备的深度推广和普及应用具有重要理论意义及应用价值。本书研究内容关系和技术路线分别如图 1-2 和图 1-3 所示。

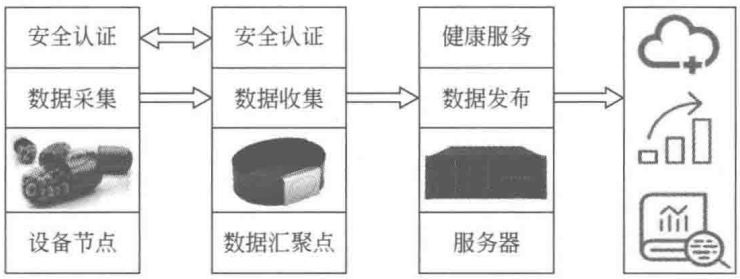

图 1-2　研究内容关系

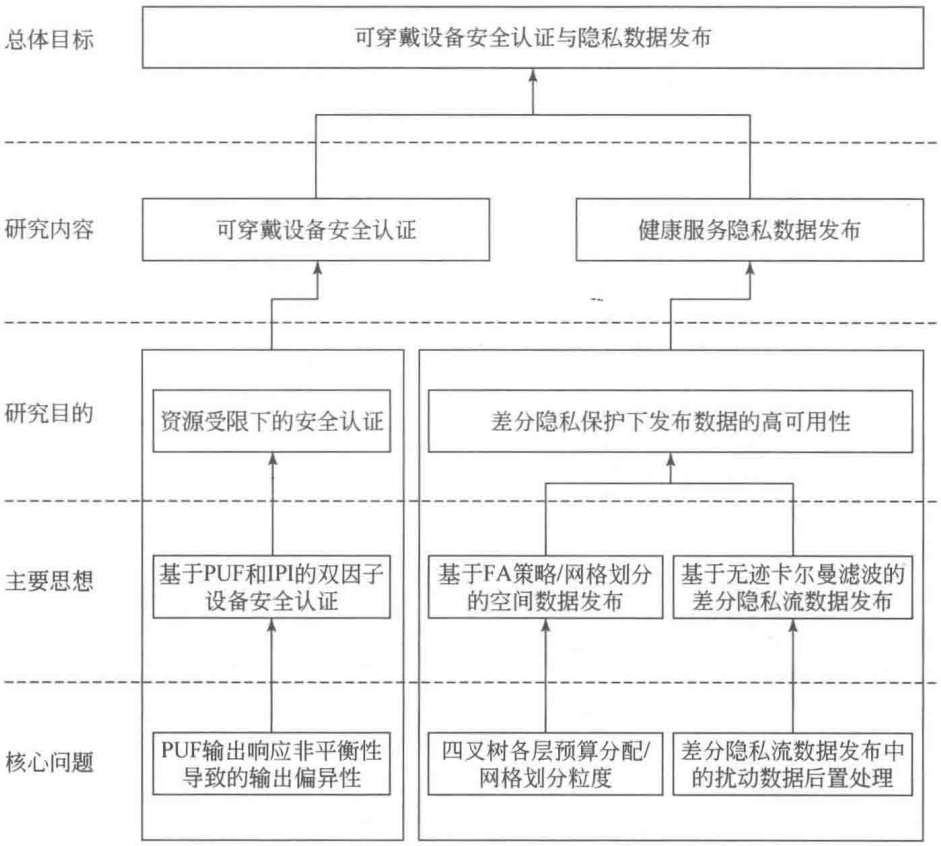

图 1-3　本书研究技术路线

1. 可穿戴设备安全认证

一方面，根据 WBAN 中节点物理特征，针对可穿戴设备自身特点，利用“物理指纹”PUF 技术认证时，结合 IPI 生物特征和 PUF 技术，将人和设备绑定，作为一个整体认证单元，实现设备物理属性和人私有属性的双重唯一性安全认证。另一方面，认证协议中，PUF 安全性事关认证协议安全，PUF 的安全为上层应用提供了安全保障。PUF 的输出响应随机性越高，即其熵测试值越大，PUF 安全性越高。如何实现基于 PUF 和 IPI 的可穿戴设

备双因子认证协议，并进一步提高 PUF 电路的对称性，减少 PUF 电路非对称带来的输出响应偏异性，是本书的研究内容。

2. 健康服务隐私数据发布

1）空间位置数据的差分隐私发布

可穿戴设备服务商发布用户位置统计数据时，需保护用户位置隐私。促进用户共享数据的关键在于保证用户的个人隐私不被攻击者侵犯。但由于数据共享的开放性，攻击者可以开展各类隐私攻击。虽然差分隐私相对传统隐私保护模型具有巨大的优势，但满足差分隐私的同时必须牺牲一定数据可用性。针对健康服务共享发布中静态空间位置数据，本书以同时满足用户数据隐私性和可用性为目标，研究适用于空间位置数据的差分隐私发布方案。

2）流数据的差分隐私发布

健康服务共享发布时序数据主要包括可穿戴设备实时采集的用户生理、健康状态数据，如对血糖、血压、血氧等的检测数据。此类数据具有实时性，如果不考虑数据的实时性，对不同类型数据进行相同的处理，会降低共享发布数据的可用性。针对健康统计动态流数据，研究适用于流数据的差分隐私发布方案，保证数据隐私性的同时，提高数据可用性。

1.3.2 关键技术

面向健康服务的可穿戴设备与人紧密相连，决定了它更有可能面临安全威胁。它自身的资源条件决定了其采取的安全措施是受限的，同时，其健康服务数据既敏感又有公开价值，保证隐私安全前提下的数据发布是必要的。本书研究可穿戴设备安全保护机制中的两个关键技术，包括结合生物特征和物理特征的设备安全认证与可穿戴设备数据安全发布。

本书的关键技术在于以下 3 个方面。

（1）现有基于设备物理特征的认证忽略了用户生物特征的唯一性，使这些协议易受妥协攻击，而基于用户生物特征的认证易受假冒攻击。本书提出一种基于生物特征 IPI 和设备物理特征 PUF 的双因子安全认证机制，使用生物属性 IPI 和设备物理属性 PUF 的双重唯一性进行安全认证，将设备和人绑定为一个整体单元，并通过平衡 D 触发器仲裁器改善 PUF 电路非对称性带来的输出偏向，更好地确保认证安全。

（2）可穿戴设备涉及空间数据和流数据，发布用户位置统计数据时，需保护用户位置隐私。现有基于差分隐私空间分解的数据发布算法常采用均匀隐私预算分配策略，每一个划分单元格分配相同隐私预算，未根据数据查询实际情况进行合理预算分配。本书针对可穿戴设备中空间位置数据，提出一种基于斐波拉契预算分配策略的差分隐私空间数据发布方案。此方案优化了隐私预算的分配，降低了数据发布误差，并通过限制推理和阈值判断

的方法进一步增强扰动数据的可用性，以较小的隐私预算满足较高的发布数据精度。

（3）可穿戴设备流数据发布为数据挖掘分析中的决策制定与疾病预测提供了坚实的基础，然而，流数据直接发布带来了隐私泄露的风险。为解决此问题，差分隐私被应用于流数据发布。扰动数据直接影响挖掘分析的结果，为提高数据可用性，现有差分隐私流数据发布方法常采用卡尔曼滤波进行数据可用性优化，然而，卡尔曼滤波不适应于非线性系统。针对可穿戴设备中的健康时序数据，提出一种基于无迹卡尔曼滤波的差分隐私流数据发布方案。此方案利用抽样的方式近似非线性分布，保护数据隐私的同时增强了数据可用性，既满足用户隐私需求，又保证流数据的高可用性。

1.4　本书结构介绍

本书各章节组织结构如图 1-4 所示，具体如下：

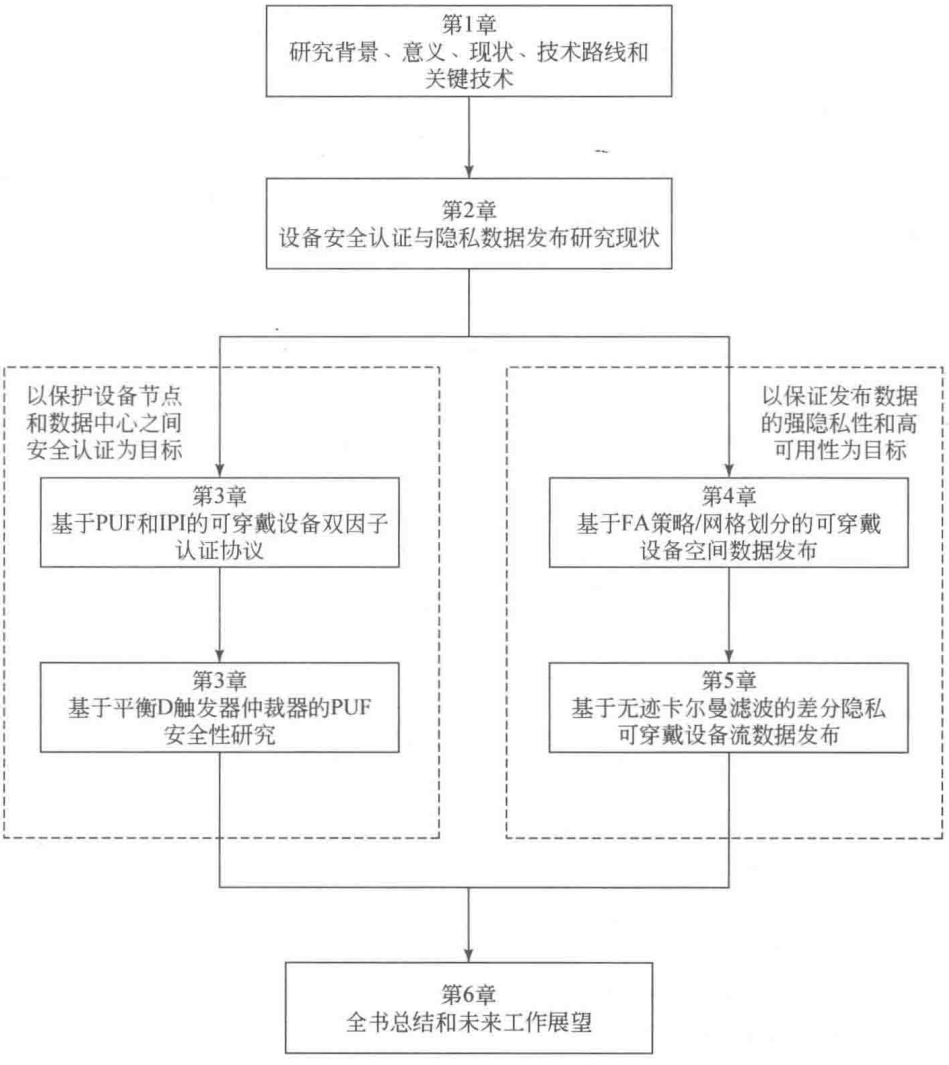

图 1-4　本书组织结构

第 1 章：首先介绍了面向可穿戴设备安全认证与隐私数据发布的研究背景和意义，其次介绍了本书相关研究内容并对其进行了分析，再次给出了本书的技术路线和关键技术，最后介绍了本书的组织结构。

第 2 章：总结了设备安全认证与隐私数据发布方法。设备安全认证主要包括基于 TPM（trusted platform module，可信平台模块）的认证和基于 PUF 的资源受限设备安全认证，用户隐私数据发布主要包括基于差分隐私空间数据发布和时序数据发布。

第 3 章：首先分析了基于物性特征或者生物特征认证方案的不足，提出了一种基于 PUF 和 IPI 的可穿戴设备双因子认证方案，其次对方案进行了安全性分析和性能评估，最后进一步给出了 PUF 安全性增强措施，并通过仿真实验对其进行了验证。

第 4 章：研究了差分隐私空间数据发布，针对已有差分隐私空间分解中均匀隐私预算分配的不足，提出一种斐波拉契预算分布策略，随后分析了不同预算分配策略下数据查询的误差。通过对发布数据噪声误差和均匀假设误差的整体分析，提出一种基于网络划分的空间数据发布方案。上述方案确保数据安全性的同时，提高了数据可用性，并通过数据集对其进行了验证。

第 5 章：首先研究了差分隐私流数据发布，针对基本方案的不足，提出一种基于无迹卡尔曼滤波的差分隐私流数据发布改进方案，其次对两个方案进行了分析，最后对其性能进行了验证和对比。

第 6 章：对本书进行了总结，并展望了未来研究工作。

参 考 文 献

[1] Chen M, Gonzalez S, Vasilakos A, et al. Body area networks: A survey. Mobile Networks & Applications, 2011, 16(2): 171-193.

[2] Movassaghi S, Abolhasan M, Lipman J, et al. Wireless body area networks: A survey. IEEE Communications Surveys & Tutorials, 2014, 16(3): 1658-1686.

[3] Aidan. 10 medical wearables to improve your life in 2016. https://wtvox.com/digital-health/top-10-medical-wearables/. 2016-1-30[2018-5-9].

[4] Insight C. Critical year ahead for smartwatches as big brands join the party. https://www.ccsinsight.com/press/company-news/3161-critical-year-ahead-for-smartwatches-as-big-brands-join-the-party. 2017-8-30[2018-5-9].

[5] Camara C, Peris-Lopez P, Tapiador J E. Security and privacy issues in implantable medical devices: A comprehensive survey. Journal of Biomedical Informatics, 2015, 55(C): 272.

[6] Mukhopadhyay S C. Wearable sensors for human activity monitoring: A review. IEEE Sensors Journal, 2014, 15(3): 1321-1330.

[7] 李静，顾江．个体化医疗和大数据时代的机遇和挑战．医学与哲学(A)，2014，35(1A)：5-10，25.

[8] 喻国明，何睿．健康信息的大数据应用：内容、影响与挑战．编辑之友，2013，(6)：20-22.

[9] Zhang K, Yang K, Liang X, et al. Security and privacy for mobile healthcare networks. IEEE Wireless Communications, 2015, 22(4): 104-112.

[10] 陈炜，龙翔，高小鹏．一种用于移动 ipv6 的混合认证方法．软件学报，2005，16(9)：1617-1624.

[11] Sweeney L. K -anonymity: A model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems, 2002, 10(5): 557-570.

[12] Machanavajjhala A, Gehrke J, Kifer D, et al. L-diversity: Privacy beyond k-anonymity. ACM Transactions on Knowledge Discovery from Data(TKDD), 2007, 1(1): 1-52.

[13] de-Montjoye Y A, Radaelli L, Singh V K, et al. Unique in the shopping mall: On the reidentifiability of credit card metadata. Science, 2015, 347(6221): 536-539.

[14] Dwork C. Differential privacy. Proceedings of the International Colloquium on Automata, Languages, and Programming, 2006, 26(2): 1-12.

[15] Boyen X, Dodis Y, Katz J, et al. Secure remote authentication using biometric data. Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 2005, 494: 147-163.

[16] Poon C C Y, Zhang Y T, Bao S D. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. IEEE Communications Magazine, 2006, 44(4): 73-81.

[17] Zheng G, Fang G, Shankaran R, et al. An ecg-based secret data sharing scheme supporting emergency treatment of implantable medical devices. Proceedings of the International Symposium on Wireless Personal Multimedia Communications, Sydney, Australia, 2014: 624-628.

[18] Hoang T, Choi D, Nguyen T. Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. International Journal of Information Security, 2015, 14(6): 549-560.

[19] Chen Y, Sun J, Zhang R, et al. Your song your way: Rhythm-based two-factor authentication for multi-touch mobile devices. Proceedings of the 2015 IEEE Conference on Computer Communications, Kowloon, Hong Kong, 2015: 2686-2694.

[20] Pappu R. Physical one-way functions. Science, 2002, 297(5589): 2026-2030.

[21] Li B, Chen S. A dynamic PUF anti-aging authentication system based on restrict race code. Science China, 2016, 59(1): 1-12.

[22] Suh G E, Devadas S. Physical unclonable functions for device authentication and secret key generation. Proceedings of the Design Automation Conference, San Diego, CA, USA, 2007: 9-14.

[23] Bassil R, El-Beaino W, Kayssi A, et al. A PUF-based ultra-lightweight mutual-authentication RFID protocol. Proceedings of the Internet Technology and Secured Transactions, Abu Dhabi, United Arab Emirates, 2012: 495 - 499.

[24] Rostami M, Majzoobi M, Koushanfar F, et al. Robust and reverse-engineering resilient PUF authentication and key-exchange by substring matching. IEEE Transactions on Emerging Topics in Computing, 2014, 2(1): 37-49.

[25] Akgün M, Cağlayan M U. Providing destructive privacy and scalability in RFID systems using pufs. Ad Hoc Networks, 2015, 32(C): 32-42.

[26] Barrows R C, Clayton P D. Privacy, confidentiality, and electronic medical records. Journal of the American Medical Informatics Association Jamia, 1996, 3(2): 139.

[27] Safavi S, Shukur Z. Conceptual privacy framework for health information on wearable device. PLoS One, 2014, 9(12): 1-16.

[28] Emam K E, Dankar F K, Neisa A, et al. Evaluating the risk of patient re-identification from adverse drug event reports. Bmc Medical Informatics & Decision Making, 2013, 13(1): 114.

[29] Demuynck L, Decker B D. Privacy-preserving electronic health records. Proceedings of the 9th IFIP TC-6 TC-11 International Conference on Communications and Multimedia Security, Salzburg, Austria, 2005: 150-159.

[30] Caine K, Hanania R. Patients want granular privacy control over health information in electronic medical re-

cords. Journal of the American Medical Informatics Association Jamia,2013,20(1): 7-15.

[31] Benitez K, Loukides G, Malin B. Beyond safe harbor: Automatic discovery of health information de-identification policy alternatives. Proceedings of the 1st ACM International Health Informatics Symposium, Arlington, Virginia,2010: 163-172.

[32] Ye H, Chen E S. Attribute utility motivated k-anonymization of datasets to support the heterogeneous needs of biomedical researchers. Proceedings of the Amia Annual Symposium,2011: 1573-1582.

[33] Wang J, Liu S, Li Y. A review of differential privacy in individual data release. International Journal of Distributed Sensor Networks,2015,11(10): 1-18.

[34] Won J, Ma C Y T, Yau D K Y, et al. Proactive fault-tolerant aggregation protocol for privacy-assured smart metering. Proceedings of the 2014 IEEE INFOCOM Toronto, ON, Canada,2014: 2804-2812.

[35] Fung E, Kellaris G, Papadias D. Combining differential privacy and PIR for efficient strong location privacy. Proceedings of the 14th International Symposium on Spatial and Temporal Databases, Hong Kong,2015: 295-312.

[36] Emam K E, Emam K E. The application of differential privacy to health data. Proceedings of the 2012 Joint EDBT/ICDT Workshops, Berlin, Germany,2012: 158-166.

[37] Zhu T, Xiong P, Li G, et al. Correlated differential privacy: Hiding information in non-IID data set. IEEE Transactions on Information Forensics & Security,2014,10(2): 229-242.