无线传感器网络中公钥机制研究综述

何炎祥[1)] 孙发军[1)] 李清安[1)] 何 静[2)] 汪吕蒙[1)]

[1)](武汉大学计算机学院 武汉 430072)

[2)](肯尼索州立大学计算机科学系 玛丽埃塔 30060 美国)

摘 要 物联网是当前学术界和产业界的研究热点,作为物联网主要构成部分之一的无线传感器网络(Wireless Sensor Networks,WSNs),其安全与人们的生活安全及隐私息息相关.过去近二十年来 WSNs 安全得到了广泛深入的研究,其中公钥机制从最初的不可行认知到现今的广泛研究应用,在 WSNs 中的可行性正逐渐被认可.然而公钥机制是否可以在 WSNs 中全面展开、其被引入到 WSNs 后会带来哪些问题、还有哪些尚未解决,这些都有待进一步探究.本文梳理了 WSNs 中公钥机制研究的高质量文献并将其归结为原语类、密钥管理类、认证与访问控制类、其他应用类,对比分析了各类文献中的经典研究工作,总结了 WSNs 中引入公钥机制的必要性、可行性及相关问题与挑战,针对这些挑战分析了其现有解决情况,最后对研究方向及可能的解决方案进行了展望.

关键词 传感器网络;安全;综述;密码学原语;密钥协商;密钥管理;物联网

中图法分类号 TP393 **DOI 号** 10.11897/SP.J.1016.2020.00381

A Survey on Public Key Mechanism in Wireless Sensor Networks

HE Yan-Xiang[1)] SUN Fa-Jun[1)] LI Qing-An[1)] HE Jing(Selena)[2)] WANG Lv-Meng[1)]

[1)](*School of Computer Science, Wuhan University, Wuhan* 430072)

[2)](*Department of Computer Science, Kennesaw State University, Marietta* 30060, *USA*)

Abstract Internet of Things (IoT) is a research hotspot in academia and industry. As one of the main components of IoT, the security of WSNs (Wireless Sensor Networks) is closely related to people's life security and privacy. In the past nearly 20 years, the security of WSNs has been studied extensively and deeply. From the initial infeasible consciousness to the present extensive researches and applications, the feasibility of public key mechanism in WSNs has been recognized gradually by scholars. However, there are still many problems that need to be further explored, such as whether the public key mechanism can be fully deployed in WSNs, what problems it brings after being introduced into WSNs, and what remains unresolved. In this paper, the high-quality literature on public key mechanism researches in WSNs have been collected and classified into four categories: Primitive, Key Management, Authentication and Access Control, and other applications. The necessity, feasibility, and related issues and challenges of introducing public key mechanism into WSNs have been summarized. Moreover, the existing feasible solutions addressing the aforementioned challenges have been analyzed comprehensively in this paper. According to the existing researches we find that: (1) Considering key length, speed, security, etc. the most suitable public key mechanism for WSNs is ECC (Elliptic Curve Cryptography). The fastest scalar multiplication in the existing implementation schemes of ECC primitives only

收稿日期:2018-10-26;在线出版日期:2019-06-25.本课题得到国家自然科学基金(91118003,61373039,61502346)资助.**何炎祥**(通信作者),博士,教授,博士生导师,中国计算机学会(CCF)会士,主要研究领域为分布式并行处理、可信软件、数据分析和软件工程.E-mail:yxhe@whu.edu.cn.**孙发军**,博士研究生,副教授,中国计算机学会(CCF)会员,主要研究方向为可信传感器网络及软件、分布式计算.**李清安**,博士,副教授,中国计算机学会(CCF)会员,主要研究方向为编译优化及嵌入式系统.**何 静**,博士,副教授,主要研究方向为无线网络与移动计算、社会网络分析、云大数据分析.**汪吕蒙**,博士研究生,主要研究方向为 GPGPU 并行计算与低功耗.

takes 0.29 s on MCAz platform with security level ECC163, which was achieved by Aranha et al. of Oliveira project team in 2010. (2) As for the WSN applications with high security requirements, it is necessary to employee a public key mechanism for key agreement. AKA (Authenticated Key Agreement) scheme based on pairing-free certificateless public key mechanism is the most promising scheme. And the CL-EKM scheme recently proposed by Seo et al. has comprehensive advantages among the existing AKA schemes for WSNs. (3) Among the authentication and access control schemes, Ke et al.'s external authentication scheme, Jiang et al.'s three-factor authentication scheme, and Ren, Shim et al.'s external user broadcast authentication scheme are the most representative. Finally, the research directions and probable solutions are prospected. (1) NTRU with high efficiency, anti-quantum attack and lattice-based theory may become the most important public key primitive in WSNs in the future after solving the problem of high storage and communication load caused by the long keys. (2) AKA scheme based on certificateless public key mechanism without pairing operation is becoming a hot topic in the current low-cost and high-efficiency AKA research. (3) In the public key mechanisms of authentication and access control, AKA is the basis of authentication mechanism for internal nodes. While in the access control of external users, access control technologies based on three or even multiple factors such as passwords, memory cards, biometrics and other factors are becoming a research hotspot. Furthermore, broadcast authentication is also an important research direction in this field. (4) In addition, public key-based schemes have also received widespread attention in the field of security research in medical and healthcare applications. In summary, with the deepening of security researches, public key mechanism is increasingly becoming an important fundamental tool to ensuring security in WSNs, especially in the case of high security requirements.

Keywords sensor networks; security; review; cryptographic primitive; key agreement; key management; Internet of Things

1 引 言

自 2005 年物联网概念提出以来,随着物联网产业规模的逐步扩大,其安全问题日益得到广泛的关注[1].在安全问题未能得到有效解决前,将物联网广泛应用于大众生活是比较困难的.其困难之处在于,当人们将随身物品联网之后,可能面临严峻的人身安全和隐私暴露等问题.因此无论学术界还是产业界都视安全研究为物联网研究之首[2].

无线传感器网络(Wireless Sensor Networks, WSNs)是构成物联网的核心,其安全问题自 WSNs 在学术界被研究以来就得到了广泛的关注[3].早在 2000 年前后,研究者们就考虑到传感器节点资源配置极为苛刻及非对称加密机制的高计算量,所以早期都集中于 WSNs 中对称密钥机制的研究[4-5],在密钥管理方面提出了一系列有代表性的方案,如 SPINS[6]、LEAP[7]、TinySec[8]、EG 方案[9]、RKPS[10]等.然而基于对称密钥技术的方案都存在自身无法克服的缺陷,如有安全时限假设[7]、物理上是邻居且链路可靠的情况下(指相互之间能无误码地收到对方消息)不能建立直接安全链接[11]、少量节点捕获会暴露部分对密钥(pairwise key)而适量节点捕获可能暴露整个密钥池[12]等.这些安全缺陷对于安全性要求不高的应用场合或许可忽略,但对于军事应用、反恐、安防等安全性要求高的应用场合需要引入公钥机制才能弥补.公钥机制的引入可以使得一个节点密钥的泄漏仅影响该节点本身及直接相关联的链路,并且可确保物理上的邻居在信号可靠的情况下建立直接安全链接.此外,在 WSNs 中部署公钥机制也有它独特的优势,由于安全资料(包括安全系统公用参数、公/私钥对等)可在部署前统一预装,WSNs 用公钥机制进行密钥协商等操作时可以省去传统网络中自己创建密钥对及协商前发送大量附加安全参数的需要[13],只是需要把它用在密钥管理、认证等关键场合[14].根据崔莉等人[15]的研究,增加安全机制后可以构建出如图 1 所示的 WSNs 安全体系结构图.其中,链路层邻居发现时点到点会话密钥的建立、传

输层用户到传感器节点的端到端会话密钥的建立以及消息认证和身份认证的模块都更适合使用非对称的公钥技术，而当节点高配时应用层的加密签名、网络层的安全路由控制也可采用公钥技术. 这些功能模块中，最重要的是链路层建立点到点间的会话密钥和传输层建立用户与传感器节点间的端到端的会话密钥以构建安全接连，这些安全连接是其他各通信模块得以安全的基础. 如前所述，会话密钥的建立(即密钥交换/协商)目前来说只有通过公钥机制才能得以完善解决，所以我们认为公钥机制在安全性要求高的场合是必要的.

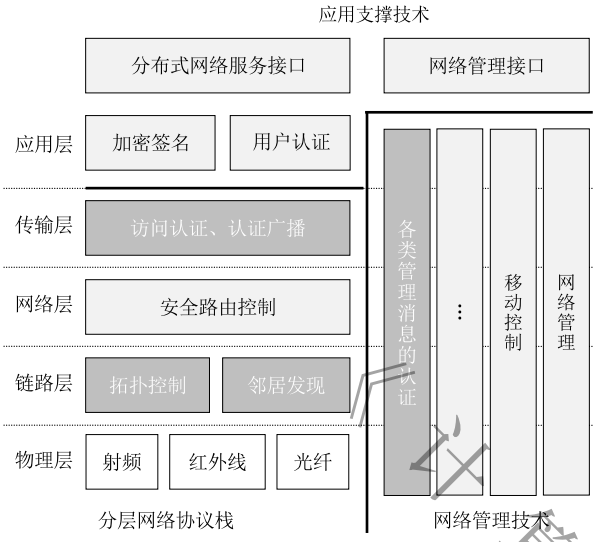
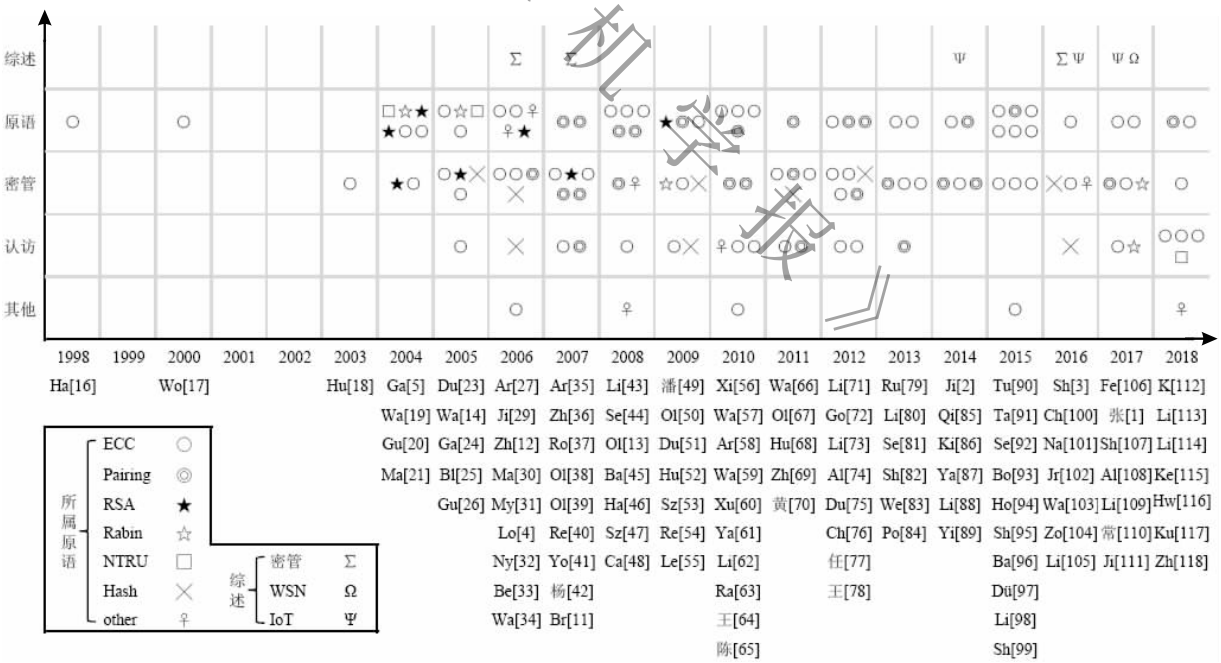


图 1　WSNs 安全体系结构

为了更好地研究公钥机制在 WSNs 中的应用情况，本文梳理了 WSNs 研究以来其公钥机制相关的文献，以英文检索词“sensor network、public key、WSN、key agreement、key management、Internet of Thing(IoT)”和中文检索词“WSN、传感器网络、物联网、公钥”等利用 WoS、dblp、中国知网、百度文库等检索工具对国内外重要期刊会议进行检索，通过人工审查方式移除掉与研究问题无关的论文，并利用追溯法通过查阅相关论文的参考文献和相关研究人员发表的论文列表来进一步识别出遗漏的论文，最终，我们选择出与该研究问题直接相关的高质量文献共 110 篇(截至 2018 年 12 月). 按研究层次大体可以将其 132 个研究点分成五类：综述、原语类、密钥管理类、认证访问类、其他应用类，其分布如图 2 所示.



注：坐标系中符号表示研究点的类别（按所用公钥原语或综述来划分），而综述分为密钥管理(密管)、物联网(IoT)、无线传感器网络(WSN)三大类，纵轴表示类别，横轴表示年份，横轴下是按年分列的参考文献编号. 此外文献[22]与[21]、[28]与[27]的工作相近未再计入统计数据中.

图 2　传感器网络中公钥机制主要研究成果分布

由图可知目前主要集中在原语类和密钥管理类且多数集中于椭圆曲线密码学(Elliptic Curve Cryptography，ECC)研究[119]. 原语类主要讨论 WSNs 中公钥原语[37]的可行性、可优化性；密钥管理类主要研究公钥机制在 WSNs 中密钥管理方面的应用，其中讨论得最多的主题就是如何安全有效地利用公钥机制来建立供会话使用的对称密钥；访问认证类主要讨论如何利用公钥技术进行网外用户访问控制及认证广播；其他应用类主要讨论了抗特殊攻击的公钥机制及如何利用公钥机制来增强 WSNs 应用

中数据传递的安全性.

接下来的内容是这样安排的,我们首先在第 2 节分析公钥机制引入 WSNs 后带来的挑战,介绍评判解决这些挑战的方法;第 3 节综合分析在 WSNs 中实现公钥原语的可行性及相关优化方法;第 4 节综合分析应用公钥机制于密钥管理的研究工作;第 5 节综合分析公钥机制在 WSNs 的认证与访问控制中的应用情况;第 6 节综合分析公钥机制在 WSNs 中的其他应用研究;最后在第 7 节总结全文并对今后的研究方向进行了展望.

2 挑战与评估

2.1 问题及挑战

首先,WSNs 安全有一个共有挑战,即低成本高集成度要求导致的计算、存储、通信、能量等资源限制与无线未照料情况下高安全需求的矛盾,如何在这二者之间根据应用需求进行折中是 WSNs 安全所要考虑的主要问题.

其次,这一挑战在公钥机制引入后显得更加严峻,公钥密码体制要求的计算强度通常为对称密码体制的成百上千倍,多数公钥机制密钥较长,加密的块较大,使用证书机制时有额外的证书开销,这些因素导致的计算、存储、通信、能量等开销往往为低配置 WSNs 所不能承受.如何选择合适的公钥方案以及在相应公钥原语中选用合适的参数对原语中的基本操作进行优化、如何用较低代价来确认一枚公钥是否是内部节点的公钥、确认实体是否拥有与公钥对应的私钥以及如何在引入公钥机制后高效地利用它为 WSNs 安全服务等都是公钥机制引入后要深入研究的问题.

我们认为公钥机制引入 WSNs 后主要带来了以下 4 类挑战:

挑战 1. 高开销公钥原语的可行性——其可行性已被多次验证但有待进一步优化;

挑战 2. 公钥认证——即认证一个公钥是否的确为某个合法节点所有,这在传统网络中通常通过证书和 PKI 来解决,但在资源受限的 WSNs 中,显然不能或不宜直接采用这类高开销的方式;

挑战 3. 如何设计公钥机制使之达语义安全并有效地使用形式化方法证明它,一般考虑的是使设计的公钥机制达到可证明安全并在标准模型或随机 Oracle 模型下有效证明其确实具有可证明安全性,但即使在 Oracle 模型下证明也是一大挑战;

挑战 4. 如何抵抗各类特殊攻击,主要有如何抵抗节点捕获带来的一系列攻击,如女巫攻击、SinkHole 攻击、虫洞攻击、吸血鬼攻击等;如何抵抗无节点捕获的能量耗尽等 DoS 攻击,如干扰(jamming)攻击,因公钥机制计算量大,这类攻击会导致配有公钥机制的节点消耗更多的能量.

以上 4 类挑战中最后一类挑战是无线传感器网络的普遍性挑战,但在有公钥机制的节点中,这类攻击的效果会被放大,所以引入公钥机制后其引发的安全问题会更加突出.

2.2 评估指标及方法

现有 WSNs 公钥领域的研究总体上从安全性和开销两个方面来进行评估.

2.2.1 安全性

安全性的总体评估指标可以是安全属性、抗各类攻击的能力、语义安全[120].其中语义安全是最强的一类安全指标.

安全属性通常有:机密性(Confidentiality)、完整性(Integrity,常用于对称密钥机制)、不可否认性(Non-repudiation,常用于公钥签名机制)、认证(Authentication)、新鲜性(Freshness)等.其中机密性还包括一般保密性、前向保密性、完美前向保密性、后向保密性等.

无线传感器网络中主要要考虑抵抗以下攻击:伪造攻击、假冒攻击、重放攻击、虫洞攻击、SinkHole 攻击、女巫攻击、吸血鬼攻击、DoS 攻击等,对于认证的密钥协商协议需要考虑抵抗密钥泄漏伪装攻击(PCI 攻击)、未知密钥共享攻击(UKS)、已知会话密钥攻击(KSK)等[106].

语义安全中一般需要证明加/解密方案的不可区分性(Indistinguishability)是否达到 IND-CPA、IND-CCA、IND-CCA2(适应性选择密文攻击下的不可区分性)安全,证明签名/解签方案的不可伪造性(Unforgeability)是否达到 EUF-CMA 或 EUF-ACMA(适应性选择消息攻击下的存在性不可伪造)安全.其中不可区分性用于刻画保密性,而不可伪造性用于刻画完整性、不可否认性、认证等.

常用的评估方法有非形式化启发式分析方法和形式化分析方法[121].

在启发式分析方法中,先定义安全目标、攻击模型,设计安全方案,最后启发式分析检验是否能抵抗攻击模型所定义的攻击、是否达到相关安全目标.这类方法过程简单、工作量小、效率高,但仅限于对已知攻击的分析,会受分析者知识面和经验的限制且

分析推理过程常常不够严谨，有存在安全漏洞的可能，比较适合于分析将已在传统网络中形式化证明过的方案移植到 WSNs 后对安全的影响.

形式化分析方法有基于符号的形式化方法和基于计算复杂性的形式化方法[122]，其中前者还包括基于逻辑、基于模型检测、基于定理证明的三类方法. 目前多数主要是采用基于逻辑的形式化方法和基于计算复杂性的形式化方法. 基于逻辑的形式化方法是采用逻辑推理的方式推导出方案具有某些安全属性，如 BAN 逻辑[108]、CSN 逻辑[80]等. 基于计算复杂性的形式化方法(即通常所说的可证明安全性，一般通过不可区分性、不可伪造性、eCK 模型来衡量)采用归约的方式，利用计算复杂性理论将方案的破解归约到一个困难问题的求解如 CDH、DDH 等或归约到密码本原如大数分解难题(Integer Factorization Problem，IFP[3])、离散对数问题(Discrete Logarithm Problem，DLP)等. 因计算机在多项式时间内求解这些困难问题的优势是可忽略的，从而证明攻击者破解方案的可能性是可忽略的，如 Liu[62]、Li[73]、Yin[89]、Seo[92]等人的工作. 也有少部分采用定理证明方法并使用 ProVerif、AVISPA 等定理证明工具进行形式化证明，如 Jiang[111]、Gope[123]等人的工作. 相较于非形式化的启发式方法，形式化方法以类似数学语言描述使问题和模型更准确、精确和严谨，严格意义上的形式化模型可以证明方案在假设的前提下没有安全问题，但证明一般比较复杂，一些难于形式化的问题只能采用启发式分析方法.

2.2.2　开　销

安全性和开销通常是正相关关系，即随着安全性的提高开销一般是增加的，实际应用中的方案需要根据具体实情在各性能和代价中进行折中：应用需求、资源配置、安全性、计算量、存储量、通信量、能耗等. 我们这里考虑的开销主要有计算量、通信量、存储占用，因为能耗通常与这三个量正相关，所以本文随后比较研究中未再进行各方案能耗的比较，具体可参考各方案相应文献及 Wander 等人的工作[14]. 根据现有研究，可以得到以下能耗关系：公钥操作(前四类)＞通信＞对称密钥操作＞Hash 操作＞除＞乘＞加减，而公钥操作中则有：对运算＞模幂＞标量乘①(Scalar Multiplication)＞点映射(MapToPoint)＞模平方根＞求逆＞模乘＞模平方.

计算量可以用时间(单位：s)、时钟周期数(单位：cycle)、关键操作个数来衡量. 时间一般是通过实际实验测得[14,20]或由现有相关实验研究推算得到[18]，而时钟周期数[72,97-98,105,109,112]通常是通过仿真平台获得. 为便于各方案脱离硬件平台来比较，通常安全协议的计算量以占用时间长、难度大的关键操作的个数来衡量[41,73,79,89,107]，这类操作通常有双线性对运算、标量乘、模幂、模乘、求逆、模平方、模平方根、点映射等.

通信量一般以包数、每包字节数来衡量且要考虑接收方/发送方、单播/广播等因素. 原语研究通常只需要考察节点有限的通信资源对其影响，不需要像密钥管理等安全协议一样考虑网络所需要的通信总量，可适当考虑密文和签名的长度对通信量的影响. 而密钥管理协议除了需要考虑节点本身限制以外还需要兼顾网络，密钥协商宜先按链路计算总开销(但当前众多方案只考虑了一对节点间的通信量)，最后平均到每个节点. 即若整个网络一次密钥协商后一条链路的发送量为 QC_s、接收量为 QC_r、网络链路数为 e、节点数为 n，则平均每节点发送、接收通信量分别为 QC_s*e/n、QC_r*e/n，因通常节点的度 $d=2e/n$，也即分别为 $QC_s*d/2$、$QC_r*d/2$.

存储开销主要是指密钥等安全资料占用的存储，但实际还应该包括程序占用的 Flash ROM 和运行程序时使用的 RAM，因与具体硬件平台有关，目前只有少数原语研究的方案[5,20-21]给出了相关数据，本文也只考虑了安全资料占用的 RAM，各类开销指标及衡量方法如表 1 所示.

表 1　开销研究的衡量指标及方法

类别	密码原语	安全协议
计算	时间、时钟周期数	时钟周期数、操作数量、时间
通信	适当考察密文及签名长度对通信量的影响	以节点或单次会话来衡量或以链路来衡量
存储	公钥、私钥	公/私钥、会话密钥、证书
衡量	至少给出关键操作的各类开销	一般以关键操作数量评估，可进一步实验验证

2.2.3　实验/仿真评估平台

用作 WSNs 公钥机制的实验/仿真平台通常是：Contiki、TinyOS 与 RELIC[87]、TinyECC[92]的组合，多数组合成 Contiki＋RELIC 或 TinyOS＋TinyECC[43]，也有直接使用通用密码学 C 函数库 MIRACL(Multi-precision Integer and Rational Arithmetic Cryptographic Library)[47,50,108]或优化后的 MIRACL[53]，Oliveira 等人在他们的 TinyPBC07 中也使用 MIRACL[13]，但后来认为它并非专为资源受限设备配置的库，所以在后期 TinyPBC11 版中更

① 本文标量乘和点乘都指椭圆曲线群上的同一操作，即常数 k 乘某点 Q 的操作 $k\cdot Q$.

换成 RELIC[67]，还有很多学者使用自己设计的密码函数库，如 WM-ECC[66]、MoTE-ECC[88] 等，而对于 WSNs 协议的仿真也有方案使用 NS2、OMNet++ 等工具.

2.3 符号约定及假设

2.3.1 符号约定

为了便于本文叙述，依据现有文献[89,107]的符号约定，提议使用如表 2 所示的符号表示规范.

表 2 符号表

符号	含义	符号	含义
BP	双线性对运算	FP	固定点乘运算
MM	模乘运算	H	Map-to-Point 函数
MR	模逆运算	h	Hash 到一个比特串
SM	标量乘运算	n	传感器节点总数
PA	点加运算	d	节点的邻居数或度
MP	Map-to-Point 操作	e	网络拓扑中的边数
ME	模幂运算	ID	节点身份号
MQ	模平方根运算	Nonce	随机新鲜值
RP	随机点乘运算	T	时间

2.3.2 假 设

为方便各方案的描述比较，我们对相关参数作如下假设：

假设 ID 长 2 字节，时间 t、Nonce 和位置长 4 字节，Hash 值和点长度均为 20 字节，MAC 值、对称密钥为 80 位，每个包数据以外的附加开销为 17 字节(首尾及前导码分别按 9 字节和 8 字节计算).

假设密钥协商中每对节点间只进行一次协商，计算量、通信量等为整个网络各安全链路建立后，按每条链路计算并平均到每个节点，如通信量为所有操作所有包的收/发总字节数的每节点均值.

因 Hash 等对称密钥操作时间比公钥操作时间低几个数量级，故假设 Hash 及相关对称密钥操作时间为 0 秒；假设同一程序在同主频同核数的 CISC 和 RISC 机器上执行后时间相当、但 RISC 机器上功耗较低，同一程序运行时间与字长和频率成反比.

3 公钥原语研究

3.1 总 概

密码学原语(Cryptographic Primitive)是指在信息安全领域中为实现信息的保密性/不可区分性和不可伪造性而设计的一些最基本密码操作，主要包括加/解密、签名/验签、消息摘要生成/验证等，加/解密用于确保保密性，签名/验签用于确保不可伪造性和不可否认性，而消息摘要通常用于确保完整性. 公钥原语就是指在这些操作中使用了公钥技术的密码学原语. WSNs 公钥原语研究主要包括加/解密和签名/验签等原语操作在 WSNs 中的可行性研究以及构成这些原语的基本操作如模幂(Modular Exponentiation)、点乘(Point Multiplication)、双线性对(Bilinear Pairing)运算、卷积等的优化研究，优化方向主要包括：域上运算(模幂、模约减、求逆、平方根、乘、平方、双倍)、群上运算(点加、倍点、标量乘)、曲线选择(Koblitz 曲线)、域的选择(素域、二元域、三元域)、双线性对的选择、格基选择等.

现有 WSNs 中公钥原语研究按所基于的难题主要可以分为五类[3]：基于 IFP 的 RSA[124] 和 Rabin；基于椭圆曲线上离散对数难题(Elliptic Curve Discrete Logarithm Problem，ECDLP)的 ECC；基于双线性对(Pairing)难题[125] 的 PBC(Pairing-Based Cryptography)；基于格上难题的 NTRU(Number Theory Research Unit)[126]；基于有限域上的多变量二次多项式方程组的难解问题的 MQ(Mutivariate Quadratic equations). 我们就其主要的 RSA、Rabin、ECC、NTRU、PBC 在 80 位安全级下对比分析[4,20] 如表 3 所示，并就现有 WSNs 中的原语研究按原语类别分成 ECC、PBC、RSA、包括 Rabin 和 NTRU 在内的其他原语四类分别比较如下.

表 3 主要公钥原语特点对照表

原语类别	理论基础	基础难题	速度	公私钥长度	明文块长	密文长度	特点	安全性	主要运算	研究代表
RSA	大数模余环	大数分解	慢	1024/1024	1024	1倍明文长	单一数学原语和少量操作	亚指数算法破解；不抗量子攻击	模幂、模乘	[14,20]
ECC	椭圆曲线群	ECDLP	快	320/160	320	1～2倍明文长	复杂的数学原语，许多临时操作	指数算法破解；不抗量子攻击	标量乘、点映射	[14,18,20,22]
Rabin	大数模余环	大数分解	加密快	1024/1024	1024	1倍明文长	简单的数学原语，解密与 RSA 相当	亚指数算法破解；不抗量子攻击	模平方(根)运算	[4]
NTRU	格理论	SVP 问题[3]	最快	1841/834	417	1倍公钥长	更简单的数学原语，需并行单元	解密可能会失败；抗量子攻击	卷积	[3-4]
PBC	双线性对映射	BBCDH[3]	最慢	320/320	320	1～2倍明文长	便于构建基于身份的无证书公钥机制	指数算法破解；不抗量子攻击	对运算、点映射	[12-13]

注：其中研究代表的范围是指传感器网络领域内，其他未声明的都默认为传感器网络领域.

3.2　基于 ECC 的公钥原语研究

一般认为，适用于 WSNs 的公钥原语研究起始于2004年Gura等人的工作[20]，他们在早期 Hasegawa 等人[16]16 位微处理器和 Woodbury 等人（其实验表明二元扩域 F_2^p 上的点乘是最慢的）[17]8 位微处理器上实现椭圆曲线密码算法的基础上，对 ECC 和 RSA 两类公钥原语的能耗、速度、代码大小、内存占用等进行了比较研究，发现随字长减小，性能上 ECC 更加优于 RSA. 在 ECC 优化方面，他们提出的一个新的乘算法——混合乘（Hybrid Multiplication）明显减少了内存使用量且在 Atmel AVR 平台上有25%的性能提升，此外对 ECC 还使用结合仿射坐标（Affine coordinate）和雅可比坐标（Jacobian coordinate）构成的混合射影坐标系统（Projective Coordinate Systems）、非相邻形式 NAFs（Non-Adjacent Forms）编码、伪梅森（Mersenne）素域进行优化，并通过指令集扩展（Instruction Set Extensions）方式扩展出乘加指令（MULACC）以提高乘加组合运算的速度，他们认为素域比二元域更有效. 同年，美国哈佛大学的 Malan 等人[21]给出了 TinyOS 中第一个二元扩域上的 ECC 原语实现，他们的研究进一步表明了 WSNs 中使用公钥原语特别是应用 ECC 的可能性. 随后，德国 Karlsruhe 大学的 Blaß 等人[25]提出使用预计算并存储基点的倍数以便以后使用存储换速度的方式来提高效率，他们只选择了 113 位作为 ECC 的密钥参数，所以虽然他们获得了比 Malan 方案快的点乘速度但却降低了方案的安全等级.

此后，宁鹏等人[43]基于 ECDSA、ECIES、ECDH 构建了一个可以配置的密码操作原语库——TinyECC且提供了可选的 Barrett 约减（Barrett Reduction）、混合乘、混合平方（Hybrid Squaring）三个大整数操作优化及射影坐标系统、曲线优化（Curve Optimization）、滑动窗口（Sliding Window）、Shamir 技法（Shamir's Trick）四个 ECC 操作优化方法. 他们的研究表明，开启优化开关虽然会不同程度的加快密钥原语操作的速度，但也会增加存储消耗. 根据其优化实验数据，我们认为比较合适的方案是，在存储允许的情况下逐步开启：射影坐标（较耗 ROM）＞曲线优化＞混合乘＞混合平方＞滑动窗口（非常耗 RAM）＞Barrett 约减，以使性能达到最佳. Wang 等人[34]也以汇编语言实现 Gura 等人提出的混合乘方法，实验表明混合乘至少比通常以 C 实现的乘快 7 倍以上，模余在模数是伪梅森数时能优化得比传统长除方法快 10 倍. 除了大整数操作优化外，可通过混合射影坐标系来减少乘和平方中的求逆和约减操作次数，从而达到加速 ECC 指数操作的目的.

2008 年，Oliveira 项目组的 Szczechowiak 等人在 Gura 等人优化方法的基础上提出了 NanoECC 方案[47]，其分析研究发现能利用寄存器较好地进行混合乘加速，使用素域利于模约减（Modular Reduction）运算，分治方法利于提高乘的速度，射影坐标比仿射坐标更有效，也使用 Comb 方法来提高固定点乘的速度. 其实验体现出素域上的点乘要快于二元扩域. Seo 等人[44]发现已有 $GF(2^m)$ 域上的乘法有大量冗余内存访问而导致效率不高，所以他们提出了一些减少冗余的内存访问的方法，基于以上优化以及对 Koblitz 曲线是 ATmega128L 上基于 $GF(2^m)$ 实现 ECC 最快的一类曲线的认识，他们提出了使用 Koblitz 曲线的 TinyECC 即 TinyECCK，并通过选用 Lopez-Dahab 坐标系统以减少标量乘中的求逆操作，利用 NAFs 编码提高群上操作的速度. 他们的实验却表明二元域上的乘要比素域快.

相对之前研究，Lederer 等人[55]基于更高安全级 ECC192，域操作优化方面考虑了素域上加/减、乘和平方、模约减等运算的优化，如采用优化后的 Gura 等人的混合乘方法、用梅森素域的方式来优化模约减等. 群操作方面通过混合坐标系减少点乘中的求逆操作，通过 NAFs、窗口方法（Window method）、结合查找表并使用 Comb 方法来减少固定点乘中加和倍点的次数，他们实验得到的点乘时间有明显缩小.

2010 年，Aranha 等人[58]发现早期 ECC 实现研究似乎表明素域上的点乘运算比二元域上的点乘运算快. 他们选用二元域，对其上的乘法用优化后的 Karatsuba 算法分治，并用 Lopez-Dahab 二元域乘法、循环移位寄存器窗口、预计算窗口分块、结果缓存、后嵌模约减等操作进行优化，就不同安全级提出模约减优化方法，对平方、求逆运算用扩展的欧几里得等算法进行优化. 群上运算选用 Koblitz 曲线和 Solinas 的 4-TNAF（τ-adic Non-adjacent Form）编码方法优化随机点乘，用 Comb 方法优化固定点乘，并发现使用 Koblitz 曲线的确比常规曲线快一倍左右. 他们的工作表明，二元域上的 ECC 操作实现比素域上的更有效.

而王潮等人[64]提出了基于 Montgomery 曲线（简称为 M 曲线）对 ECDSA 算法进行改进研究，他们着重于其中异步点乘（实指一个固定点乘加一个随机点乘）进行优化，使异步点乘由 2 个 SM 减少为 1.2 个 SM. Liu 等人[62]提出将签名过程分成在线

和离线签名两部分并分别优化，在其比较的 IBOOS 方案 ST、XMS 及非 IBOOS 方案 HS、CC、GQ 等方案中，他们的方案最优. 随后 Wang 等人[66]在域运算上优化了混合乘、模除、模约减，ECC 群操作上优化了加、双倍、模约减，在点乘中尽量以点双替代点加，并使用 NAFs，他们基于 MICAz、TelosB、iPAQ 平台对 ECC 原语进行了实现.

2012 年，巴西 Oliveira 项目组的 Gouvêa 等人[72]分别讨论了素域和二元域上的优化，对于素域，选用 Karatsuba 算法优化乘、用 Montgomery 算法优化模约减，对于二元域，利用 Lopez-Dahab 算法结合 Karatsuba 算法来优化乘，用扩展的欧几里德算法优化求逆. 而点群操作上，主要采用 Comb 或 wTNAF 对素域或二元域的固定点乘运算进行优化，此外也发现用 GLV(Gallant-Lambert-Vanstone)方法能提高 ECDSA 和 ZSS 的效率. 其实验亦表明二元域上的乘要快于素域. 随后，Seo 等人[81]使用操作数据缓冲和暂存部分积的方式来解决 TinyECC 中混合乘技术不适宜于 16 位 MSP430 这一问题，和 Seo[44]、Aranha[58]一样发现了 TinyECC2.0 中的大量冗余内存访问操作，其中混合乘的作用没有显现，却因循环控制分支和条件操作导致过多的执行时间而产生性能下降，comba-MAC 中没有集中考虑操作数访问数量的优化和增量地址方式，从而导致过多的内存操作，针对这些问题他们提出了改进方法，特别是提高乘加指令(MAC)的效率，并使 ECC 的核心操作多项式乘的延迟比已知的方法降低了 6%.

2014 年，Liu 等人[88]给出了一个高度优化且可扩展的 ECC 库——MoTE-ECC，支持不同参数大小的优化素域上(Optimal Prime Fields，OPFs)M 曲线和 Twisted Edwards 曲线(TE 曲线)的标量乘操作，M 曲线有利于随机点乘，而 TE 曲线可使固定点乘更迅速，并采用基于 Fermat 小定理的求逆方式、曲线参数优化、对 Comb 算法优化等方法来提高速度. 当取 ECC160 安全级时，M 曲线上的加和双倍运算比 TinyECC 库快 3 倍，而 TE 曲线上的加和双倍运算比 TinyECC 库快 2.1 和 1.9 倍. 随后，Liu 等人在 MoTE-ECC 上进行了进一步改进，为了适用点压缩他们采用了利于模约减运算的伪梅森素域来替代 OPFs，并引入了一个 Z 形迂回技术来计算平方，从而得到了一个基于 16 位 MSP430 MCU 高度优化的 ECDH 方案[98]，他们这一方案是现有基于素域 ECC 方案中最快的. 同年，Düll 等人[97]则基于 128 位安全级的 Diffie-Hellman(DH)密钥交换协议[127]在三个不同主流微控制器体系结构上展开实验研究. 主要针对于各平台从乘和平方上进行了不同的优化，使用 3 级 Karatsuba 算法和 Montgomery 算法优化乘，以 2 级 Karatsuba 技术优化平方，并第一次给出素域 X25519(p 为 $2^{255}-19$)在 Cortex-M0 上的实验数据.

2016 年，Liu 等人[105]基于 IoT 背景对 ECC 原语进行了进一步研究，他们对伪梅森素域上的模加/减、乘、平方、约减、求逆进一步优化，使之参数化、模块化，从而使实现更加可扩展也更安全，他们实验分析表明虽然其方案比 Düll 等人的方案[97]要慢，但 Düll 方案的占用空间是他们的 3 倍. 随后，他们在 MSP430 工作的基础上为 MICAz 和 Tmote 设计了一个可扩展、规范、高度优化的 ECC 库[109]，其工作仍基于 MoTE 曲线，因为它利于计算热 ECDH 密钥，并对域上的加/减、乘、多精度乘、平方、求逆、模约减等运算进行优化，群上运算主要考虑用基于 twisted Edwards 坐标和仿射坐标的混合点加、用 Comb 方法计算固定点乘、用 Montgomery 阶梯法计算随机点乘、并使用 Shamir 技巧进行双基标量乘等优化操作. 其椭圆曲线群的参数化实现支持伪梅森有限素域，并以高速版、内存有效版支持多个安全级别.

最近，北京交通大学的 Li 等人[113]则应用无证书公钥机制于车联传感网(Vehicular Sensor Networks)的车载信息的认证传输之中，他们也给出了双线性对、标量乘、MapToPoint、ECC 签名、ECC 验签等公钥操作时间，体现出了公钥操作中 ECC 的效率，但从实验环境来看并非在实际传感器节点上取得数据. Hwajeong[116]等人考虑到以前的 ECC255 方案仅考虑速度的提升而忽略了存储空间的节约，所以他们从节约存储的角度设计了一个既有较高速度又节约存储的 ECC255 实现方案，他们在具有 32 位乘法器的 16 位 MSP430X 处理器上测得标量点乘为 6666895 个时钟周期且仅需要 4054B ROM，相对于当时最好的 Düll 方案速度上损失了 20.5%，但存储上节约了 59.8%.

为了对以上众多 ECC 原语研究工作从字长、频率、安全级数等方面对标量乘时间进行归一化比较，我们取归一化平台的安全级为 80 位(即 ECC160)、硬件为 8 位字长 8MHz 的 MICAz、设待计算方案的 ECC 安全级为 S_0 位、其实验平台字长为 B_0、主频为 F_0、测得的标量乘时间为 T_0，根据 Wang 等人的调研[57]，对 ECC 原语来说 ECC 公钥操作运算量与安

全级的立方成比例，由之前假设，则归一化后标量乘时间 T 可计算为

$$T=k_0\times T_0\times\frac{B_0}{8}\times\frac{F_0}{8}\times\frac{160^3}{S_0^3} \quad (1)$$

而据 Gura[20]、Liu[88]等人实际实验结果分析，可取比例系数为

$$k_0=1-0.001641\times(160-S_0) \quad (2)$$

由式(1)可根据各方案实验数据计算出各 ECC 实现方案的标量乘折合时间如表 4 所示. 由表 4 可知，经过学者们十多年的不懈努力，其中的关键运算标量乘(折合时间)从早期的 31.52 s 减少为后来的 0.28 s，目前最好的研究结果是由 Oliveira 项目组的 Aranha 等人[58]于 2010 年在 MICAz 平台上基于 ECC163 取得. 用这一评估方法我们对众多研究的实验数据进行了折合比较，发现同一方案在 MICAz 上运行效率要高于其他节点，可能主要是 MICAz 中 RISC 架构的 ATmeta128L 寄存器配比高的缘故.

表 4　基于 ECC 原语实现情况比较

年份	方案	原语	域	实现	平台配置	标量乘/s	折合/s
1998	Hasegawa[16]	ECC160	素域	汇	16-10-M16C	0.13/0.48	0.33/1.20
2000	Woodbury[17]	ECC134	伪梅素	C、汇	8-12-8051	1.95/8.37	4.77/20.46
2004	Gura[20]	ECC160	素域	汇	8-8-Atmega128	0.81	0.81
2004	Malan[21]	ECC160	二元扩	nesC、C	8-7.38-MICA2	34.16	31.52
2005	Blaß[25]	ECC113	二元扩	n/a	8-8-ATmega128	6.74	17.66
2006	Arazi[27]	ECC160	素域	nesC、TinyECC	8-7.37-MICAz	2.33/4.67	2.15/4.30
2006	Wang[34]	ECC160	伪梅素	necC、C、汇	8-8-MICAz	1.24/1.35	1.24/1.35
2008	Liu[43]	ECC160	素域	necC、C、汇、TinyECC	8-8-MICAz	1.88	1.85
2008	Szczechowiak[47]	ECC160	素域	necC、C、汇、NanoECC	8-7.38-MICA2	1.27	1.172
2008	Seo[44]	ECC160	二元扩	C、汇	8-8-MICAz	1.14	1.14
2009	Lederer[55]	ECC192	素域	necC、C	8-8-MICAz	0.71/1.67	0.43/1.02
2010	Liu[62]	ECC160	素域	necC、C	8-8-MICAz	0.896	0.896
2010	Aranha[58]	ECC163	二元扩	C、汇	8-8-MICAz	0.29/0.32	0.28/0.30
2011	Wang[66]	ECC160	素域	nesC、汇、WM-ECC	8-8-MICAz	1.24	1.24
2012	Gouvêa[72]	ECC160	二元扩	C、汇	16-8-Tmote	0.26/0.58	0.52/1.16
2013	Seo[81]	ECC160	素域	基于 TinyECC	16-8.91-MSP430	优化乘	提高 6%
2014	Liu[88]	ECC160	素域	汇、C、MoTE-ECC	8-7.37-ATmega128	0.37/0.85	0.34/0.78
2015	Liu[98]	ECC160	伪梅素	IAR 仿真	16-8-MSP430F1611	0.20/0.41	0.41/0.81
2015	Düll[97]	ECC255	素域	汇编、C、仿真	8-8-ATmega	1.74	0.50
2016	Liu[105]	ECC159	伪梅素	汇、C	16-8-MSP430	0.24/0.48	0.49/0.98
2017	Liu[109]	ECC159	伪梅素	AVR 仿真	8-8-MICAz	0.32/0.68	0.33/0.69
2018	Hwajeong[116]	ECC255	素域	汇编	16-8-MSP430	0.833	0.476

注：实现中 C、汇、nesC、硬分别表示 C 语言、汇编语言、nesC 语言、硬件；平台配置 aa-bb-ccc 中 aa 代表字长(位)、bb 代表频率/MHz、ccc 为平台或 MCU 型号，标量乘和折合栏分别代表该方案相应配置下进行标量乘运算的时间，折合栏为按归一化方法折合后的时间，当有两个时间以 tt/ss 标注时，tt 代表固定标量乘时间，ss 代表随机标量乘时间，当只有一个时间时表示未分类测试，一般指随机标量乘时间；伪梅素表示伪梅森素域，二元扩表示二元扩域.

3.3　基于双线性对运算的公钥原语

最早基于 WSNs 应用双线性对运算进行安全方案设计的是 2006 年 Zhang 等人的工作[12]，但他们只是在密钥建立中应用对运算，并没有在传感器节点实现对运算，其方案评估是参照一个 32 位 ST22 智能卡上的实验数据基于 32 位的 Startgate 传感器节点来估算的. 2007 年巴西 Oliveira 等人则首先用双线性对运算提出了一个基于身份的密钥协商方案[38]，但其只是基于 ATmega128 微控制器测量了模乘的成本并运用 Barreto 等人已有的研究估算了双线性对的计算时间. 他们的评估表明，使用 Affine 坐标系或 Projective 坐标系、有预计算或无预计算、梅森素数或非梅森素数，前者均比后者效果好约 1/3. 随后他们在基于 7.3828 MHz 的 ATmega128L 微控制器(MICA2/z 系列传感器使用)的传感器上第一次实现了对运算——TinyTate[39]，他们选取的安全参数中有限素域阶 q 的位数为 256，而椭圆曲线点群阶的位数为 128(文献[56]评估为 40 位安全级). 他们的工作第一次用实验表明在资源有限节点(如字长限制为 8 位时)进行对运算是可行的.

此后，Oliveira 项目组的 Szczechowiak 等人[47]利用他们的 NanoECC 库第一个在二元扩域上实现双线性对操作. 因考虑到有限域乘法在双线性对运算中的重要性，他们在 NanoECC 的基础上，在其基于双线性对的密钥交换方案 TinyPBC 中[13]进一步使用 Lopez 等人的 Lopez-Dahab(LD)方法对有限域上乘法进行了优化，实验表明其对运算只要不到

NanoECC 一半的时间. 随后 Oliveira 团队的 Scott 等人所在的爱尔兰研究组[53]在 Oliveira 等人工作的基础上对 WSNs 中基于双线性对的运算进一步扩展到 Tmote、Imote2 等节点上,他们的实验表明:整体来说 η_T 对是所有 Tate 对中最快的双线性对. 而香港城市大学 Xiong 等人[56]指出之前的方案主要集中于提高速度而较少考虑节约内存消耗,所以他们提出了一套既提高速度又节省内存的 Tate 对计算方案——TinyPairing[56],为考虑加速的同时节省内存,该套方案分别在求立方、模约减、多项式乘(Polynomial Multiplication)上提出了三个优化算法以提高速度,他们的椭圆曲线构建在三元有限域之上,比二元有限域上元素占用的存储小,建立了一个安全级达 1024 位 RSA 级的 Eta(η_T)对操作软件库,从速度和内存两类指标来说,它在当时所有基于 nesC[128]实现中是最有效的.

2011 年,Oliveira 项目组继续在之前工作的基础上把双线性对运算扩展到 8 位、16 位、32 位三类传感器节点上[67],并进一步提高了双线性对运算的速度,他们把在 8 位 ATmega128L、16 位 MSP430、32 位 PXA27x 上的 η_T 对运算速度分别提高到 1.9 s、1.27 s、0.14 s,从而使得基于对运算的密钥机制甚至可与基于标量乘运算的密钥机制媲美. 随后 Li 等人在 Liu 等人[62]工作的基础上提出了一个基于身份、使用对运算、无 MaptoPoint 操作的离线+在线组合签名方案[73],并形式化证明了方案可以达 EUF-CMA 安全,与当时最新的基于双线性对的方案相比他们的方案是性能最好的,但与 Liu 等人的工作相比在离线签名和存储上都要多出不少开销. 同年,巴西 Oliveira 项目组的 Gouvêa 等人[72]提出了一个 160 位素域和 256 位素域乘提高 12% 和 18% 的方法——即利用 MSP430X 模块 32 位硬件乘法器中的稀疏素数约减(Sparse Prime Reduction),他们的有效实现也使双线性对运算能提升 25%～30% 的速度,并发现该方法也能应用到其他的 8 位和 16 位平台,其实验表明二元域上实现的 Eta 对运算要快于素域上的 Ate 对运算.

2015 年,Yin 等人[89]构建了一个利用双线性对和对称加密的混合签密算法,并在随机 Oracle 模型中对方案进行了形式化证明,他们的分析表明其混合签密方案要优于现有同类方案,签密只需要 1 个双线性对和 2 个标量乘操作,而解签只需 1 个双线性对和 3 个标量乘操作. 最近,Kwon 等人[112]指出 TinyPBC 没有做扩域级算法优化,而该文同时做域和扩域算法优化,优化了域约减的性能,并进行了 Miller 循环优化和双线性对运算算法优化. 与 TinyPBC 相比,约减性能提高了 29.1%,而扩域稀疏乘提高了 12.22% 的性能,Eta 对计算只需要 1.224 s,与 TinyPBC 相比,速度要快 5.88% 而内存可节约 19.2%.

与 ECC 原语方案一样,为了便于各方案的比较我们按 8 位 8 MHz 的硬件平台对双线性对运算结果进行了归一化,但因尚未见较统一的双线性对安全级的界定及等价转化研究,这里没再按安全级归一化到 80 位安全级,结果如表 5 所示. 一般认为素域 $\mathbf{F}_{q_{256}^4}$ 的 Ate 对和二元域 $\mathbf{F}_{2^{4\times 271}}$ 上的 η_T 对提供的是 80 位安全级,但后来 Gouvêa 等人[72]分析 $\mathbf{F}_{2^{4\times 271}}$ 只提供了 70 位安全级,$\mathbf{F}_{2^{4\times 353}}$ 才达到 80 位安全级[3],我们可参考 ECC 不同安全级间运算量转化的方法进行估算比较. 从表 5 结果可知,目前最有效的是 2011 年 Oliveira 等人的工作,他们在 8 位 7.37 MHz 的 ATmega128L 上实现 η_T 对运算耗时 1.9 s.

表 5 基于双线性对运算的公钥原语研究

年份	方案	域	对	安全级	实现工具	平台配置	对运算/s	折合/s
2007	Oliveira[39]	$\mathbf{F}_{q_{256}^2}$	Tate	40 位	nesC/TinyECC	8-7.38-MICAz	30.21	32.74
2008	Szczechowiak[47]	$\mathbf{F}_{2^{4\times 271}}$	η_T	70 位	necC、C、汇/MIRACL	8-7.38-MICA2	10.96	10.11
2008	Szczechowiak[47]	$\mathbf{F}_{q_{256}^4}$	Ate	80 位	necC、C、汇/MIRACL	8-7.38-MICA2	17.93	16.54
2008	Oliveira[13]	$\mathbf{F}_{2^{4\times 271}}$	η_T	70 位	C、汇、MIRACL	8-7.37-MICAz	5.45	5.02
2009	Szczechowiak[53]	$\mathbf{F}_{2^{4\times 271}}$	η_T	70 位	necC、C、汇/MIRACL	8-8-Atmega128	2.66	2.66
2009	Szczechowiak[53]	$\mathbf{F}_{q_{160}^4}$	Tate	50 位	necC、C、汇/MIRACL	8-8-Atmega128	7.43	7.43
2010	Xiong[56]	$\mathbf{F}_{3^{6\times 97}}$	η_T	70 位	nesC	8-7.37-MICAz	5.30	4.89
2011	Oliveira[67]	$\mathbf{F}_{2^{4\times 271}}$	η_T	70 位	C、汇/RELIC	8-7.37-MICAz	1.90	1.75
2012	Gouvêa[72]	$\mathbf{F}_{2^{4\times 353}}$	η_T	80 位	C、汇	16-8-Tmote	2.59	5.17
2012	Gouvêa[72]	$\mathbf{F}_{q_{160}^{12}}$	Ate	80 位	C、汇	16-8-Tmote	3.79	7.58
2012	Gouvêa[72]	$\mathbf{F}_{q_{256}^{12}}$	Ate	128 位	C、汇	16-8-Tmote	9.93	19.86
2018	Kwon[112]	$\mathbf{F}_{2^{4\times 271}}$	η_T	80 位	C	16-8-MSP430	1.22	2.45

注:除安全级别外,归一化平台与 ECC 一致(8 位 8MHz),相关同类参数意义可参考表 4,q_{256}^4 表示嵌入度(Embedding degree)为 4、q 是 256 位长的素数.

3.4　基于 RSA 的原语

相比于 ECC，RSA 开销大、密钥及加密块过长，因此较少被考虑应用于 WSNs 的安全机制中. 目前基于 RSA 的应用研究集中于早期公钥原语可行性研究阶段，主要代表性研究有 Gura[20]、TinyPK[19]、Wang[34]、secFleck[52]，其中前三个方案是软件实现，最后一个依赖于硬件实现. 最早 Gura 等人的 RSA 研究以 Montgomery 乘作为 RSA 的模乘，用中国剩余定理 CRT 来加速模幂操作，同时对其模平方等操作进行优化，他们的研究表明，当加密取小指数时，RSA-1024 公钥操作相对较快(0.43 s)，可与 ECC 操作媲美，但 RSA-1024 私钥操作(10.99 s)却要慢 20 多倍. 同年 Watro 等人设计和实现了 TinyPK，其小指数 RSA 指数操作在 MICA1 平台上当采用 1024 位密钥时耗时 14.5 s. Wang 等人[34]也基于大整数操作优化的思想，利用蒙哥马利(Montgomery)约减有效计算 RSA 指数运算，并以中国剩余定理来减少指数大小使 RSA 指数操作加速到 4 倍，RSA 公、私钥操作分别只需要 0.79 s 和 21.5 s. 与之前基于软件实现的研究不同，Hu 等人基于 TPM(Trusted Platform Module)技术提出了一个硬件实现的 secFleck[52]，该平台包括一个标准的 TPM 芯片和一套软件加密原语，支持 WSNs 中的公钥操作，采用 RSA 公钥机制，私钥为 2048 位，他们测得硬件加密只需 0.055 s，而同样安全级的软件实现需要 450 s，基于软件的方法耗能是基于硬件方法的 1300 倍之多，所以他们也建议，应该用对称加密于常规安全通信，而用非对称加密于关键任务. 各方案比较如表 6 所示.

表 6　基于 RSA 原语实现情况比较

年份	方案	密钥长度	实现	平台配置	公钥 e	加/解密/s	折合/s
2004	Gura[20]	1024 位	汇	8-8-Atmega128	32769	0.43/10.99	0.43/10.99
2004	TinyPK[19]	1024 位	C	8-4-MICA1	3	14.5	7.25
2006	Wang[34]	1024 位	necC、C、汇	8-8-MICAz	65537	0.79/21.5	0.79/21.50
2009	secFleck[52]	2048 位	C、硬	8-8-ATmega128L	65537	0.06/0.75	0.03/0.38

注：表中实现和配置数据含义与表 4 相同，折合栏中只有一个时间时表示模幂运算的时间.

3.5　其他公钥原语研究

除了以上三类主要的公钥原语研究外，早期美国 Worcester 理工学院的 Gaubatz 等人[5]就 Rabin 和 NTRU 进行了分析、优化设计，使用不到 17000 个门电路耗 148.18 uW 实现了 Rabin 方案，用不到 3000 个门电路低于 20 uW 的耗能实现了 NTRU 加密，而且分别达到了 60 位和 57 位安全级. 随后对 Rabin、NTRU、ECC(ECMV)在加/解密和签名/验签等公钥操作方面进行了比较[24]，他们的实验表明：Rabin 具有明显的非对称性、加/解密(或验签/签名)速度上相差近 400(1.089 s/2.88 ms)倍、无并行时 Rabin 加密速度是三者中最快的，而有 84 路并行时 NTRU 是运算速度最快的公钥方案.

与传统公钥机制研究不同，Bellare 等人提出的有状态 PKC(Public Key Cryptography)方案的发送方都在加密操作后会记录加密状态以供下一次加密操作使用，从而能将原来分别需要 2 个和 3 个指数操作的 DHIES 和 Kurosawa- Desmedt 方案改进成有状态版后只需要 1 个指数操作，且实验表明平均无状态加密协议耗能是有状态加密协议的 8.5 倍. 而 Bo 等人[93]的工作也表明有状态加密机制比无状态加密机制要快约一个量级. Baek 等人将 Bellare 等人提出的有状态 PKC 方案[33]在 WSNs 的 MICAz 平台上基于 TinyECC 库用 nesC 语言进行了实现[45]，并对 TinyECC 库按方案要求进行了修改.

此外，最近一些学者开始关注 WSNs 中基于公钥的聚合签名与环签名的研究，如 Horng 等人的无证书聚合签名机制[94]及 Sharma 等人的无对无证书的环签名研究[95]，为 WSNs 中公钥原语的研究注入了新的要素.

3.6　公钥原语能耗研究

为了更准确的衡量公钥机制所引入的能耗是否为传感器节点可承受，美国加州大学 Wander 和太阳微系统实验室 Gura 等人[20]就公钥加密的认证密钥交换协议的能耗基于一个 8 位 CPU 的硬件平台量化比较 RSA 和 ECC 两类公钥原语，在能耗方面进行了可行性分析. 他们针对于 Berkeley/Crossbow 的 Mica2dots 平台测量和评估得到了通信、对称密钥操作的基本能耗数据，并基于 RSA 与 ECC 的数字签名与密钥交换测得了计算能耗相关数据. 其研究表明：

(1)一个 RSA1024 签名能耗相当于发送 5132 字节数据，而一个 ECDSA-160 签名相当于发送 385 字节数据，一个 160 位 ECC 公钥生成相当于一次密钥交换的能耗即 22.3 mJ；

(2)计算占能耗的主要部分，分别达 82%和 72%，通信能耗第二，相对而言随机数生成及 Hash 运算的

能耗可以忽略. RSA-1024 计算能耗是 ECC-160 能耗的 4.9 倍,通信能耗是其 2.7 倍;RSA-1024 的密钥交换总能耗是 ECC-160 的 4.2 倍;

(3) ECC-160 点乘操作要比 RSA-1024 私钥模幂操作快一个数量级且只需要不到 1/3 的存储,在 4 MHz 的 CPU 上 ECC-160 点乘操作仅花 1.61 s 282 字节数据存储而 RSA-1024 私钥模幂操作需要花 22 s 930 字节存储;

(4) 与空闲时传感节点省电模式下的耗能相比,不频繁密钥协商操作的能耗是可忽略的,故在小的无线设备上将公钥应用于这类操作是可行的.

而 Targhetta 等人[91]评估了 ECC 在不同软硬件配置情况下实现的不同安全级别的能耗代价,着重探索了 ECC 在素域/二元扩域上指令集扩展、使用指令 Cache、配备 Monte/Billie 优化协处理器的优化效果,对素域/二元扩域的能耗和性能在 RISC 处理器 Pete 上对六种搭配进行了评估比较,实验结果表明开发的改进二元扩域 $GF(2^m)$ 协处理器比之前研究加速 2 倍以上,而增加 4 kB 指令 cache 能减少 ECC30%的能耗. 实验结果也证明二元扩域比素域上有 1.31 至 2.11 倍的能效提高,同时使用二元扩域 $GF(2^m)$ 协处理器与仅使用扩展指令集的方法相比能效上可提高 2.8 到 3.61 倍.

此外, Zhang[12]、Arazi[27-28]、Baek[45]、Liu[62]、Liu[43]等人的研究工作中也对公钥原语相关的能耗进行了分析研究.

3.7 公钥原语研究小结

计算量方面,公钥原语中同等安全级下最快的是 NTRU[24],但需要使用并行单元,而近二十余年的研究表明,从各方面综合衡量公钥原语中最适合低配 WSNs 的是 ECC[61,109]. 虽然多数认为双线性对运算量大,但经过 Oliveira 等人的努力,基于双线性对的原语几乎可与 ECC 媲美. 现有实验表明双线性对中 Tate 对要快于 Weil 对,而后来基于 Tate 对改进出的 Ate 对和 Eta(η_T)对中后者是最快的[87],所以目前多数研究都集中于 Eta 对的优化. 对于低配置的 WSNs 来说,RSA 因加解密速度太慢、应用成本太高,一般认为不适宜应用于 WSNs 中[20,52],宜采用轻型的 Rabin 或取小指数的方法[35],在低配传感端用低复杂度的模平方或小指数运算,其速度甚至比 ECC 还快[20].

安全性方面,RSA 和 PBC 的安全性分别建立在大数分解和 DLP 难题的基础上,目前已知有亚指数算法能解这些难题,而 ECC 所基于的 ECDLP 目前还只有指数级算法可解[129]. 在抗特殊攻击方面,Rabin 和基于小指数的 RSA 所具有的非对称特点可起到一定抗 DoS 攻击的作用,NTRU 是这些方案中暂时没有量子破解算法的公钥机制. 使用 ECC 能以较短密钥和较高效率达到 RSA 同样的安全级别.

在最适合于 WSNs 也是目前被广大学者研究得最多的 ECC 原语中,优化效果好的特性有:使用 Koblitz 曲线、射影坐标系、伪梅森素域、Montgomery 乘、Comb 方法、混合曲线、混合乘等. 因二元域有利于平方、平方根、加、约减等,而素域便于利用硬件平台的乘指令[50],所以使用素域还是二元域一直是目前研究争议的焦点,目前暂时是二元域上的标量乘比素域上的要快,最近 Liu 等人[109]取得了素域上的最好结果,而 Aranha 等人[58]于 2010 年取得了二元域上的最好结果.

4 应用于密钥管理的公钥机制研究

多数学者[14,21,52]认为,虽然公钥机制在 WSNs 中可行,但因其占用资源多,仅适合应用于不频繁的一些操作如密钥管理特别是密钥协商中[14],所以自公钥技术在 WSNs 中的可行性得到确认以来,应用公钥机制于对称密钥管理是目前 WSNs 中公钥机制研究又一热点. 同时对于自组织无人照料的 WSNs 来说,因其通常采用开放的无线传输,为了使节点间通信处于保密状态,首要问题是如何利用公钥技术来为随机部署的两个邻居节点建立会话用的对称密钥,以便为节点间构建保密通信信道. 所以 WSNs 中公钥机制在密钥管理方面的应用通常围绕会话密钥建立机制来展开,故本节重点调研密钥建立.

4.1 密钥建立概述

依据 Krawczyk、Diffie 等人的提议[130-131],密钥建立可以分成密钥传输和密钥协商两类,而结合认证还有认证的密钥传输(Authenticated Key Transport, AKT)和认证的密钥协商(Authenticated Key Agreement, AKA),统称为认证的密钥建立(Authenticated Key Established, AKE).

密钥传输是指会话密钥以加密传输的方式从一方传递给另一方的过程. 认证的密钥传输通常使用公钥加密来实现会话密钥的保密传输,并使用数字签名方式来对传输实体及传递的消息进行认证,但这类方式的公钥一般需要通过昂贵的证书操作来认

证，如 TinyPK[19]、uSSL-RSA[14]. 密钥传输方式中，在互认证了对方公钥后只需要一个包(1Pass)即可建立会话对密钥，但会话密钥的保密依赖于发送节点私钥的保密，因此无前向保密性.

密钥协商是指实体双方通过交换秘密信息并用两方的秘密信息计算出会话密钥的过程. 早期 WSNs 领域的密钥协商多是基于 DH 协议，但因为纯 DH 协议未经认证，存在中间人攻击(Man-In-The-Middle，MITM). 如 Malan 等人给出的协议 EPKI[21]就是这类无认证的密钥协商协议，他们指出使用 Diffie 等人于 1992 年提出的 STS 方案[130]可实现一个认证的密钥协商机制，所以随后学者们提出了一系列认证的密钥协商方案. 在公钥认证后密钥协商方式需要两个消息(2Pass)才能利用收到的秘密信息建立会话用对密钥，在通信上比密钥传输多一次通信，但具有前向保密性.

通常把与对密钥建立相关的所有方案都称为密钥协商，有时也称为密钥交换(Key Exchange)，下边文献归类中我们仍按照常规做法，把与密钥建立相关的方案，包括密钥传输、协商等方式，都统称为密钥协商，因此本文 AKA 实指 AKE，也包括 AKT.

4.2　WSNs 中基于公钥的密钥协商研究

早期 Malan[21]和 Liu[43]等人就利用基于 ECC 的 DH 协议——ECDH 在 WSNs 以非对称密钥机制实现了对称对密钥的建立，考虑到认证安全需要后，学者们提出了一系列认证的密钥协商方案，按先后发展主要包括基于证书、基于 Hash 认证技术、基于身份和对运算、无双线性对非传统证书机制四类方法，其在 WSNs 中对应的经典方案分别是 uSSL[14]、Merkle 树[23]、TinyPBC[67]、CL-EKM[92]，我们分别就这四类机制在 WSNs 中的研究现状进行分析.

4.2.1　基于证书认证的 AKA

在公钥机制被证明可行后首先提出的是基于证书的机制，如 Watro 等人提出的 TinyPK[19]采用如表 7 所示的最简证书，利用数字签名进行进行认证，但 Das 等人[132]指出方案中的传感器节点可以被假冒. 而 Wander、Gura 等人[14]在其基于公钥机制的能耗评估研究中也提出了轻型公钥证书的方案，使用精简后的轻型证书{ID＋公钥＋签名}(多数方案采用，所以我们称之为标准型)，但 Wander 等人基于 ECC 的协议中未给出明确认证的协商步骤. 2006 年，Zhou 等人[36]提出为防止恶意节点接入攻击应该完成节点认证和密钥建立两步，也即进行认证的密钥建立，他们使用 ECDSA 和 ECDH 结合的方式实现了一个认证的固定会话密钥协商协议，其采用的公钥认证方法其实就是使用基于证书的 ECDSA 签名认证方式，他们在 Wander 等人证书基础上增加了建立时间及时长.

表 7　基于证书认证的 AKA 比较(80 位安全级)

方案	证书形式	原语	长/B
TinyPK[19]	{EP 公钥}$_{CA私钥}$	RSA	128
Wander[14]	标准型	RSA/ECC	262/82
Zhou[36]	标准型＋建立时长	ECDSA	110
Ren[54]	标准型＋有效期	ECDSA	86
Brown[11]	标准型	ECC	82
潘耘[49]	{Hash(n,ID)^d}	RSA	20

Ren 等人的工作[54]中也提到了基于轻型证书的方式并设计了如表 7 所示的轻型证书，他们也指出 CAS(Certificate-Based Authentication Scheme)方式有两个显著的不足：一是需要增加额外的通信量；二是需要进行包括证书验证在内的两个昂贵的签名验证. 此外 Brown[11]和潘耘[49]等人的公钥方案中也使用证书来认证公钥，但前者方案结合了自证明机制[77]，后者采用的是轻型证书的方式，并基于二次剩余理论使用类似 Huang 等人[18]方案中的 MSR(Modular Square Root)机制来进行密钥传输以建立会话密钥.

4.2.2　基于 Hash 认证的 AKA

考虑到用证书等方式认证公钥的高代价，早期学者们提出了一些轻型的基于 Hash 的认证技术，这其中有 1970 年 Bloom 等人提出的布隆过滤器(Bloom Filter)和 1979 年 Merkle 等人提出的一个 Hash 树结构——Merkle 树[23]. WSNs 中早期 Perrig 等人曾在 SPINS 中应用 Hash 链技术实现了一个延迟认证的广播消息认证方法——μTESLA[6]. 随后 Du 等人在其基础上提出使用 Merkle 树来认证公钥[23]，他们提出了基本的 Merkle 树、Merkle 森林、结合部署信息的 Merkle 森林三个方案. 他们指出，虽然基本的 Merkle 树方案能以 $\log(n)$ 的存储量、通信量和计算量来实现公钥认证，但其可扩展性仍不够理想，当节点数较多时，通信量 $\log(n)$ 仍比较大. 随后他们给出剪修后的 Merkle 森林方案，但考虑到存储的根 Hash 量随修剪层数呈指数增长，他们提出了基于节点部署信息来构建 Merkle 森林的方案，其研究表明在同等存储的情况下，使用布置信息比不用布置信息的方案能节约通信量约 3.5 个 Hash 值. 复旦大学 Ma 等人[30]则在 Du 等人的基础上把 Merkle 树技术应用于无线传感器执行器网络中，

与之不同的是他们在证据生成中使用了节点实际的位置,这样可以抵抗移动攻击者的攻击,但要求网络部署前提前获得节点预部署位置且要求准确部署,并针对布置时少数误放节点提出了依据新的位置及组信息重新生成证据的算法,从而部分弥补了这种对位置要求苛刻的不足. Nyang 等人[32]则提出了将节点的公钥证据随机分布于网络中的部分节点中,并通过协同认证的方式来认证公钥,但该方法易招至假冒节点所带来的 DoS 攻击.

随后基于 Hash 的公钥认证方法在 Ren 等人[54]的工作中得到了比较好的综合,他们总结了公钥认证中的四个方法并就优缺点进行了深入分析:基于证书的方案(CAS)因计算和通信代价需要高能耗、基于直接存储的方案(Direct storage based Authentication Scheme,DAS)不易扩展、基于布隆过滤器的方法(Bloom filter based Authetication Scheme,BAS)能进一步减少直接存储方法的内存. 最后他们利用 Merkle Hash 树提出了一种混合方法(Hybrid Authentication Scheme,HAS). 他们的方案中考虑了节点被俘获、DoS 等能量耗尽攻击问题,并给出了量化分析及证明. 而后 Qin 等人[85]指出 Ren 等人仅将布隆过滤器应用于用户的认证而未用于节点的认证,提出会话密钥协商完后再根据簇头收到的周边邻居节点公钥信息建立公钥认证需要的布隆过滤器,然后用之前协商的会话密钥加密后传给簇内各节点,这样使簇内各节点日后以公钥机制通信时便于互认证公钥. 但他们给出的方案中密钥协商时未认证公钥,这容易导致假冒攻击.

最近 Nadir 等人[101]提出了使用掩码的 Hash 认证公钥的方法,他们将网络中所有节点的 Hash 掩码及公钥对应的掩码 Hash 值存储在一张表中,并为每个节点预装这张表来实现对公钥的认证,这与 Du、Ren 等人提到的 DAS 方法相似,只是他们使用掩码的方式来缩短需要存储的 Hash 值的位数,相当于使用了一个生成短 Hash 值的 Hash 函数,所以是以降低安全性换取 Hash 值存储空间的节约.

几种基于 Hash 技术的公钥认证技术中 Merkle 树/森林是安全性最好的一类方案,但可扩展性不高,主要体现在:随节点总数的增加,通信量的增加对 WSNs 来说是不可承受的且部署后节点新增困难,与布隆过滤器结合的 HAS 方案虽然可一定程度增加节点总数,但降低了安全性,节点新增问题也依旧存在. 基于 Hash 认证的各 AKA 方案对比如表 8 所示.

表 8 基于 Hash 认证的 AKA 比较

类别	计算量	通信量	存储	安全性	相关研究
纯 Hash	1	1	n	易构成假冒/伪造攻击	[32,101]
Bloom Filter(BF)	k	1	m 位	存在假阳性	[54,85]
计数型 BF	k	1	m 位	存在假阳性,元素可删	[54]
Merkle 树	$\log(n)$	$\log(n)$	$\log(n)+1$	较高,低扩展性	[23,30]
Merkle 森林	$\log(n)+2^r-r$	$\log(n)-r$	$\log(n)+2^r-r+1$	较高	[23,30]
MF+BF(HAS)	$\log(n)+k-r$	$\log(n)-r$	$\log(n)+m-r+1$	存在假阳性	[54]

注:未标明单位的为 Hash 操作个数,m 为 BF 的长度,k 为 Hash 函数个数,n 为总传感器节点数,r 为由树构建森林削减去的顶部层数,表中都只考虑与证据相关的消耗,而略去共有部分如公钥的传递、存储等.

4.2.3 基于对运算和身份认证的 AKA

基于身份的公钥密码体制是 Shamir 等人最先于 1984 年提出[42],其基本思想是使用公共可识别的与实体身份相关的信息做为公钥,如 e-mail 地址、身份证号或其他唯一标识信息,这样就不再需要证书来证明公钥,可省去 PKI 系统的证书管理操作,但直到 2001 年 CRYPTO 会议上 Boneh 和 Franklin 才给出了一个可实际应用的实现方法. 而在 WSNs 中,Zhang 等人[12]基于身份和位置信息及双线性对运算提出了一个抗俘获的安全机制,他们首先提出了基于位置的密钥(Location- Based Key,LBK)这一概念,将节点私钥绑定到其位置和 ID,使用共享主钥的方式生成私钥,并基于双线性对运算提出了一个基于 LBK 的邻居认证方案,该方案也表明了 LBK 在抗节点捕获攻击方面的性能. 最后使用了门限密钥的原理提出一个基于位置的担保门槛方案 LTE(Location-based Threshold-Endorsement)来抵抗伪造数据注入攻击. 2007 年,国内杨庚等人[42]和巴西 Oliveira 等人[13]分别提出了 WSNs 中基于身份加密的密钥分配方法,他们都是在 Boneh 和 Franklin 工作基础上的进一步完善,其中杨庚等人是以结合 BF-IBE 加密算法和 DH 协议的优点来实现会话密钥建立,而 Oliveira 等人却将他们设计的 TinyPBC 方案在实际的传感器节点上进行了实现并实验评估. 他们假设建立会话密钥的节点双方事先知晓对方的 ID,并有公钥 $P_A=H(ID_A)$、$P_B=$

$H(ID_B)$及私钥 $S_A=sP_A$、$S_B=sP_B$，则可用双线性对运算

$$\hat{e}(S_A,P_B)=\hat{e}(sP_A,P_B)=\hat{e}(P_A,P_B)^s=\hat{e}(P_A,sP_B)$$
$$=\hat{e}(P_A,S_B)=\hat{e}(S_B,P_A)$$

生成两方共享的对密钥：

$$k_{A,B}=\hat{e}(S_A,P_B)=\hat{e}(S_B,P_A)=k_{B,A}.$$

但该方案缺乏对节点身份的认证措施.

与此同时，韩国 Kim 等人[41]也基于身份和双线性对运算提出了一个认证的密钥协商方案，他们主要通过双线性对运算来减轻通信量，因为使用双性对映射后不再需要传递证书，他们的方案也与 TinyPBC 一样实现了无证书协商的方式.

近来，Yang 等人[87]针对之前杨庚等人的工作进行改进，将使用模幂操作的 DH 协议替换成基于 ECC 的 ECDH，并在消息中引入 ID 及 Nonce 挑战响应机制抗重放攻击，使用 KDF 来生成会话密钥，此外还考虑了密钥更新及节点新增等操作，与之前方案相比，时间和能耗分别节省 16.1% 和 19.7%.

基于双线性对运算和身份认证的密钥协商协议（如表 9）虽然密钥协商过程简单且可完全做到不用证书，但计算上需要 MaptoPoint 操作和双线性对运算，一般认为双线性对运算要比点乘运算复杂至少一个数量级且存在密钥托管问题[92,113]，即服务器私钥泄露会导致全网各节点私钥泄露，所以随后学者们提出使用无对无证书的认证方式.

表 9　基于对运算和身份认证的 AKA 比较

方案	计算量	通信量/B	存储/B	安全性
LBK-LTE[12]	1BP+1MP	发：27+42d；收：69d	40+10d	优点：抗虫洞、重放、伪造多种攻击；缺点：位置泄露、共享主密钥
TinyPBC[67]	1BP+1MP	发：2d；收：2d	40+10d	优点：几乎零交互 缺点：缺乏确认认证
IBE-DH[42]	2BP+3ME+1FP+1MP	发：19+77d；收：96d	40+10d	优点：结合 BF-IBE 和 DH 的优点；缺点：两方案结合不够紧密
Kim[41]	2BP+2ME+2RP+2FP+1MM	发：19+86.5d；收：105.5d	80+10d	优点：公钥可由 ID 计算出，不用传输；缺点：计算比通信代价高时不占优势
Yang[87]	2BP+2RP+2FP+1MP	发：19+77d；收：96d	40+10d	优点：结合 BF-IBE 和 DH 的优点；缺点：传递的消息未认证

注：计算量指每次协商单方实体的计算总量，通信量是指整个网络各安全链路建立后平均每个节点的通信量，每个包的首尾及前导码分别按 9B 和 8B 计算，即每个包的附加开销为 17B. 设计当为广播时，周边邻居都会收到包，而为单播时只有具有相应目的地址的节点才能收到包.

4.2.4　无双线性对非传统证书认证的 AKA

我们这里非传统证书机制指与开销大的传统证书认证机制相区别的一类开销小、适合于低配置网络使用的认证方式，主要指包含隐式证书、轻型证书、无证书在内的非传统证书认证方式. 事实上最早的无证书思想中给出的公钥为两个椭圆曲线点，相当于普通的公钥加证书大小，本质上也是隐式证书的一种形式. 鉴于基于身份的公钥机制（ID-PKC）存储密钥托管上的安全问题，2003 年 Al-Riyami 和 Paterson 在亚密会上提出了无证书公钥机制[133]（Certificateless PKC，CL-PKC），它结合了基于身份的公钥机制与自证明公钥（Self- certified，1991）、隐式证书（Implicit certificate，1989）机制等思想的特点，利用身份信息及 Schnorr 等签名模式将证书尽可能地隐藏在公钥中，使之既起到公钥和自证明的作用，又不会导致像 ID-PKC 机制那样因私钥完全被服务器托管而致恶意 KGC 伪造攻击. 在这些非传统证书机制中，通常使用 Schnorr 签名模式：$a+hb \bmod q$，其中 a,b 一般为实体的长期秘密和临时秘密，而 h 是用与实体身份相关的信息经 Hash 函数生成的 Hash 值，假设长期秘密为 x，临时秘密为 r，则可采取如下两种形式之一：

（1）Schnorr 标准模式[92,96,102]：$r+hx \bmod q$；

（2）Schnorr 变形[18,27,66]：$x+hr \bmod q$.

但不可采取 $h+rx \bmod q$ 的形式，因为这样实体可以根据 h 提取出 rx，利用该 rx 即可仿造出任意实体的认证信息.

CL-PKC 其实是 WSNs 中最早引入的基于公钥的密钥协商机制. 早在 2003 年，普林斯顿大学的 Huang 等人[18]在 WSNA2003 上提出了相似的机制，他们将其称为隐式证书机制，和同年 Al-Riyami 提出的无证书公钥机制思路相似，他们方案中先由用户产生自己的部分私钥 g_U 和部分公钥 G_U，再由 CA 产生其另一部分私钥 s_U、隐式证书 IC_U 和全部公钥 Q_U，最后用户在拿到部分私钥及隐式证书后即可构建自己的全部私钥/公钥对并校验证书及密钥的正确性. 但潘耘等人[49]指出 Huang 等人方案中存在语义矛盾，认为既然隐式证书 IC_U 是公开的，则预分配阶段没必要使用安全信道传输 G_U，我们认为虽然用户最终收到隐式证书并能验证它，为确保 G_U 未被攻击者所替代而导致重复生成工作，若有安全信道可使用时也可选择安全通道. 同时分析中也发现该方案的设计有些冗余，可进一步对其精简，这在后续研究中得以验证. 2006 年前后，Arazi 等人利用类

Schnorr 签名思路构建了一个自证明公钥机制[27]，在他们方案中，将 Huang 等人的隐式证书替换成了公钥，而对公钥的签名则利用 Schnorr 签名方式融入到私钥中，这样真正持有私钥的实体则可用它既认证公钥又认证了私钥，但这一方案安全的关键是协商之后需要一个密钥确认环节，或许因为确认环节实现简单，该文只是提到并未对确认环节进行分析. 若通过密钥确认阶段确保认证，我们认为其达到了认证 DH 协议的安全性水平，但因为认证是最后完成，故存在延迟认证. 随后 Brown、Du 等人发现随机密钥预分发方案的一些不足，他们认为采用公钥机制可弥补这些不足，所以他们结合 Du 等人之前提出的基于异构传感器网络（Heterogeneous Sensor Networks，HSN）的方案和 Arazi 等人的自证明公钥机制的优点，提出了一个基于 HSN 的自证明公钥机制[11]，但他们方案中仍冗余地使用轻型证书来认证公钥且位置信息未进行保密传输.

2011 年 Wang[66] 在 WSNs 中实现原语 WM-ECC 之后，利用自证明公钥的原理，结合对称密钥与非对称密钥机制的特点构建了一个认证的密钥协商协议，但他们的方案存在伪造攻击. 随后，Porambage 等人[84] 利用椭圆曲线 QV 隐式证书标准——ECQV 构建了一个密钥协商协议，他们协议中使用了基于公钥的证书和基于对称密钥的 MAC 认证两种方式，而且 MAC 认证使用共享主密钥方式，并未有对证书进行校验的环节，需等以后用会话密钥通信中才能确认安全，故也存在延迟认证.

2015 年，Seo 等人在其无对无证书混合签密方案 CL-HSC 可证明安全性论证的基础上[134]，针对于异构动态无线传感器网络提出了一个基于无证书公钥机制的密钥管理方案——CL-EKM[92]. 他们针对耐俘获性、抗克隆与假冒攻击、前后向安全、抗已知密钥攻击来设计密钥管理方案，其方案由 7 个部分构成：系统建立、对密钥生成、簇格式化、密钥更新、密钥撤销、节点移动、节点新增，在系统建立阶段首先依据无证书密钥机制的方法为基站 BS 生成私/公钥对(x, P_{pub})，为各传感器节点生成部分和全部公/私钥对(R_{L_i}, d_{L_i})、$(P_{L_i}, R_{L_i})/(d_{L_i}, x_{L_i})$，在节点部署后开始进行对密钥生成，生成具体过程如图 3 所示，由该方案协商过程可知，H 节点和 L 节点需要的计算量分别为 1FP＋5RP 和 1FP＋3RP，且 H 节点要发送两个大小分别为 42B 和 44B 的包，而 L 节点需要发送一个 106B 的协商包. 该方案是基于具有可证明安全性的 CL-PKC[134]，所以具有较好的安全性，但其计算量大，和其他同类方案一样存在延迟认证.

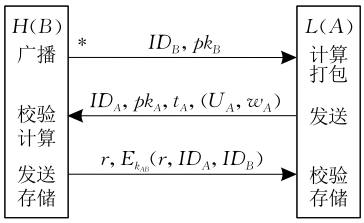


图 3 CL-EKM 协议

同年，Bala 等人[96] 分析发现，为确保两实体间进行安全通信，认证的密钥协商是主要的机制，他们利用 Schnorr 签名模式构建了一个基于身份的无对两方密钥协商协议——PF-ID-2PAKA，并将方案在 TinyOS 下基于 RELIC 库进行了实现. 用该方案建立会话密钥，每方实体需要将公钥的隐式证书传递给对方，故需要一个 82B 的包，而每端需要进行 3 次随机点乘和 1 次固定点乘运算. 随后，Jr[102] 结合 SMQV 及隐式证书的特点基于物联网环境提出了一个轻型无托管的认证的密钥协商协议，该协议分成两个阶段：预布置阶段和密钥协商阶段，在预布置阶段，一个可信赖的 KGC 为所有节点生成公/私钥对，并利用 Schnorr 签名模式构造隐式证书，最后在密钥协商阶段利用类似 DH 协议的方法来生成两节点的对密钥.

最近，随着物联网及车联网的不断发展，车载传感器网络得到了广泛应用，北京交通大学的 Li 等人[113] 则应用无（隐式）证书公钥机制于车联传感网（Vehicular Sensor Networks）的车载信息的认证传输之中，他们在车辆和 TA（Trusted Authority）、车辆和 PKG（Private Key Generator）以及车辆和 RSU（RoadSide Unit）间多次应用 Schnorr 签名模式构建认证的信息传输，并利用分叉引理证明了他们的方案是抗适应性选择消息攻击下的伪造攻击. 他们的实验也体现出无证书机制的良好性能.

此外，北京大学 Jing 等人[29] 利用组合密钥的思想构建了组合公钥方案，并结合 DH 协议构建了一个密钥协商协议. 他们的方案实现了公钥的无证书认证，但对每个节点来说公钥池的存储是个较大的负担，而公钥池的大小也受映射函数 F_{map} 值位数的限制，因 WSNs 中节点的身份 ID 可被任意冒用，只有在最后通过私钥认证后才能确定当前请求是否假冒，所以也存在延迟认证.

总之，在基于隐式证书、轻型证书、无证书的密钥协商方案中，通常都会采用 Schnorr 签名模式或

其变体，而且多数存在延迟认证，从而容易招致 DoS 攻击，这是今后研究中将要考虑解决的一个问题. 此类密钥建立方案比较分析如表 10 所示. 此外，其他基于公钥的密钥管理机制研究还有：结合公钥机制与特殊网络结构[51,63,78,107]（如 HSN）、与 Hash 技术和对称密钥机制结合构成混合密钥管理机制[69-70,74-75,80-90]、密钥更新[76]、组密钥管理[65]、基于拉格朗日插值方法的密钥管理[103]等研究.

表 10　无双线性对非传统证书认证的 AKA 比较

方案	计算量	通信量/B	存储/B	安全性
Huang[18]	2FP+2RP	发：103+85d；收：188d	106+10d	启发式分析：依赖于对称密钥机制的实现模式
Arazi[27]	2FP+2RP	发：99+37d；收：136d	60+10d	优点：安全性较高；缺点：需确认环节，存在延迟认证
Jing[29]	1RP+kPA	发：19+38d；收：57d	3220+10d	缺点：r 未保密，公钥池大小难折中
Brown[11]	2FP+2RP	发：99d；收：99d	60+10d	优点：HSN+自证明；缺点：无密钥确认，需传验证书
Wang[66]	1FP+1RP	发：142d；收：142d	60+10d	优点：对称加密、挑战响应；缺点：假冒、MITM 攻击
Poram[84]	2RP	发：73d；收：73d	60+10d	缺点：使用共享主密钥方式，未构成安全认证
Seo[92]	1FP+4RP	发：59+92d；收：151d	60+10d	优点：具有可证明安全性；缺点：计算量大，延迟认证
Bala[96]	3RP+1FP	发：99d；收：99d	80+10d	缺点：存在伪造攻击，其中 R_A，T_A 都可被伪造
Jr[102]	3RP+1FP	发：183d；收：183d	100+10d	优点：隐式证书+SMQV；缺点：存在伪造攻击

注：计算量和通信量的计算及数据依之前假设进行. 假设当为广播时，周边邻居都会收到包，而为单播时只有具有相应目的地址的节点才能收到包. Seo[92]中设 r 为 20B，计算时为统一假设其应用于分布式网络结构，即任意节点间需要建立连接，Jing[29] 中设 r 长度为 20B，Huang[18]方案中设 $k=80$ 则 cv 为 10B，其中 Wang[66]、Jr[102]因包过大需要进行切割. 随机标量为 20B，以上数据以一次协商收发双方的为准. 假设文献[29]方案中 Fmask 的输出为 80 位，Arazi 等人[27]方案中确认包长为 20B，对称密钥加密密文与明文等长，而存储量上除 Jing 等人方案[29]外每个节点还需要存储 KGC 或 CA 的公钥 40B.

5　认证与访问控制

认证与访问控制是现代计算机系统中一种必要的安全控制机制，通常认证是访问控制的手段，而访问控制使得不同用户有不同访问权限的结果则是认证的最终目标，即将欲访问用户认证为不同权限级别的合法用户或者非法用户，从而给不同用户以不同的访问权限. 从接收认证消息的对象个数可将认证分为广播认证①和单播认证，按认证的对象可分为实体认证和消息认证等，按通信范围又可分网内节点间和对外部访问用户的认证，而按认证所使用的凭证类别数可分为单因素认证（一般认证）、双因素认证[132]（two-Factor Authentication，2FA）、三因素认证[111]（three-Factor Authentication，3FA）、多因素认证（Multi-Factor- Authentication，MFA）等，目前常用的凭证类别有口令、身份、智能卡、生物信息等，我们可据 Jiang 等人的研究[111]得到一般外部用户访问 WSNs 的模型如图 4 所示. 网内节点间的单播认证已经在密钥协商部分进行了讨论，除了基于公钥的单播认证以外，还可以利用协商好的对称密钥基于消息摘要机制、Hash 技术等[100,123,132]进行认证（这不在本文的讨论范围之内），因网内传感器节点的广播需求少，所以网内节点的广播认证主要是指 Sink 节点的广播认证. 我们这里主要讨论广播认证（含外部用户的广播和 Sink 节点的广播认证）和对外部访问用户的认证（含向外单播和多播或单用户和多用户）两个方面.

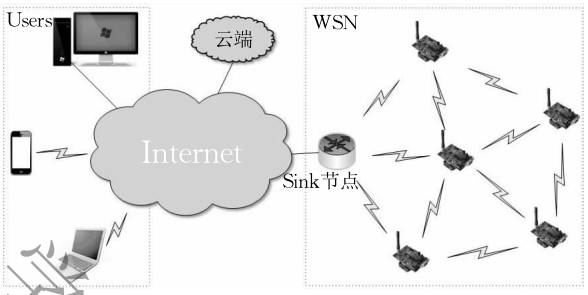


图 4　外部用户访问 WSNs 模型

5.1　对外部用户的访问认证

2005 年，太阳微系统实验室 Gupta 等人在公钥原语研究[14,20]的基础上，针对用户通过互联网访问 WSNs 数据的需求，首次提出了 WSNs 中端到端传输的要求，基于 SSL 结合 ECDH、ECDSA 提出了第一个可运行于 WSNs 中的微 SSL——端到端安全访问 WSNs 的 Sizzle[26]，远程用户端和传感器服务端通过 ECDSA 协议进行相互认证，并通过 ECDH 协议协商会话密钥，最后以会话密钥来保密传输数据，并进行了可靠性传输实验，为网外用户认证访问传感器节点的研究跨出了第一步，但他们实现的仅为点到点的单播认证，即一个节点认证一个用户，不便于实现数据共享[50]. 随后，Zhou 等人[36]也基于 ECDSA 及 ECDH 实现了一个节点间认证的密钥协

① 本文的广播认证和认证广播都是指同一个概念，即一个实体广播认证包，有多个实体接收并能对其真实性进行认证. 众多文献表述成广播认证（Broadcast Authentication），但我们认为实际应该是指认证（的）广播（Authenticated Broadcast），当然可以在强调广播时用“认证广播”，强调认证时用“广播认证”.

商协议,但其存在拒捕时间假设且新老节点协议更适合合并设计.

2009 年,Leonardo 等人指出,相比 MAC 而言,在多用户与传感器结点通信中使用数字签名机制可有以下优势:易认证、少存储和管理、利于多播.他们的 Secure-TWS 方案[50] 和 Sizzle 一样提供了一个微 Web 服务框架,但他们没有使用只能单播的 SSL,而是仅用数字签名,即传感器节点对数字签名后方可多播给多个需要的用户,他们的实现使用"证书+数字签名"的方式,为选取一种好的数字签名方法,基于当时常用的 MSP 和 AVR 平台对几种常用签名算法进行了比较,在他们比较的 ZSS、BLS、ECDSA、Schnorr 四种算法中,Schnorr 算法性能最佳,而与 Schnorr 相当的 ECDSA 位居其次.次年,Yasmin 等人提出的认证框架[61] 把认证分成三类:基站传感器间的、传感器间的、认证外部用户,并分析了广播认证和外部用户认证两类实例,对 IBS 和 IBOOS 进行了较形式化的定义,并将其分别用于传感器认证用户和用户认证传感器之中.他们实验分析表明,以 2% 的能量广播消息用第一类 IBOOS 可签 24021 个消息,第二类 IBOOS 可签 2778 个消息,而 IDS 方案只能签 1550 个消息,IMBAS[48] 只能签 1852 个消息.

2011 年,Wang 等人[66] 针对于传感器网内节点间的认证密钥协商问题,结合隐式证书机制和对称密钥的优势,利用 Hash 函数的特点设计了一个抗重放的节点间认证协议,但我们上边的分析表明该方案存在替换公钥攻击的安全漏洞.同年,Hur 等人[68] 设计了一个基于属性加密(KP-ABE)的访问控制方案.最近,Al-Turjman[108] 也提出了一个认证的密钥协商框架,Ke 等人[115] 则基于 ECC 提出了一个两因素认证的方案,在用户与网关间使用 Schnorr 签名模式进行认证,而网关与传感器节点间使用预共享密钥方式认证.此外 Jiang[111]、Li[114] 等人针对目前对外部用户认证的研究热点——三因素认证方案展开了研究,Jiang 等人的方案在用户与网关间使用 Rabin 加密传递会话密钥构建信息,而 Li 等人的方案则使用类似 ECDH 的密钥协商方式,但二者在网关与传感器间均使用预共享密钥方式来传递会话密钥构建信息.以上对外部用户的访问认证方案对比如表 11 所示.

表 11 对外部用户的访问认证方案对比

年份	方案	原语	认证类别	认证方式	密钥协商	安全性
2005	Sizzle[26]	ECC	SSL 集成单用户认证	ECDSA	ECDH	传感器节点向 Sink 节点认证代价大
2006	Zhou[36]	ECC	节点间认证	ECDSA	ECDH	有拒捕时间假设,且新老节点协议应该合并设计
2009	STWS[50]	ECC	对外多用户认证	ECDSA 等四种	仅认证	比较了签名方案,数据未保密传输
2010	Yasmin[61]	ECC	用户和传感器节点间双认证	IBOOS、IBS	IOAKE	IBOOS 达可证明安全,IBS 仅依赖于 ECDLP
2011	Wang[66]	ECC	节点间及用户与节点间认证	隐式证书及门限	ECDH	存在伪造攻击
2011	Hur[68]	PBC	多用户分层次认证	访问树	KP-ABE	精细地多用户分级访问控制
2017	Al-T[108]	PBC	外部用户/Sink 认证	Pairing	Pairing	协商的会话密钥未保密
2018	Ke[115]	ECC	外部用户认证	Schnorr 签名	ECDH	宣称安全性达可证明安全
2018	Jiang[111]	Rabin	外部用户认证	三因素认证	密钥传递	安全性获 ProVerif 验证
2018	Li[114]	ECC	外部用户认证	三因素认证	ECDH	安全性依赖于 ID 的匿名性

5.2 广播认证

广播认证按广播的来源可分为基站 Sink 节点广播和(多)用户广播,而按所采用的密码技术可分为基于对称密钥技术的广播认证(如 μTESLA[6])和基于公钥机制的广播认证.本文我们仅关注基于公钥机制的广播认证,所以随后所提广播认证都是指的这一类.2007 年 Ren 等人最先提出了 WSNs 中对外部用户基于公钥的广播认证问题,在分析现有基于对称密钥技术的广播认证 μTESLA 的延迟认证等不足后,指出可以采用基于证书、Merkle 树、基于身份和双线性对[40]、布隆过滤器[54] 等这些基本方法进行认证,并重点提出了将 Merkle 树与布隆过滤器相结合(HAS)[54] 的方法,从而避免了单纯 Merkle 树方法的高通信量问题和 Merkle 森林方法的高存储需求问题,因布隆过滤器和 Merkle 树都是基于 Hash 技术,所以 HAS 具有计算开销非常低的特点.但随后 Cao 等人提出 HAS 等利用 Hash 技术的方案可扩展性差,需要待老用户退出后才可增加新用户,所以他们提出了一个基于身份的认证广播方案 IMBAS[48] 以解决这一可扩展性问题,他们将广播分成用户广播和 Sink 广播两类,提出一个基于 BNN-IBS 的变体方案 vBNN-IBS 用于用户广播,使用带部分消息恢复的 Schnorr 签名用于 Sink 广播.

而 Wang 等人[57] 却认为公钥机制对于 WSNs 来说太昂贵,直接将其应用于 WSNs 实现认证广播是不现实的,所以他们提出了"短期短公钥"(Short-Term Short Public Key)方案的思想,即针对认证广播的短期时效性和 WSNs 低资源配置的特点,采用

较短的公/私钥对并使之在短期内有效的方式，但这样需要大量的短公/私钥对，他们提出了基本的和提高的两个方案来分发这些密钥对，相对于对称密码技术而言，这种频繁的公钥操作开销还是很大，至少是对称密钥技术的十倍. 同样，鉴于 μTESLA 的延迟认证和公钥认证的高计算量，Liu 等人[71]提出了一种结合 Hash 和公钥签名机制的分摊签名方案，该方案结合了公钥认证和 Hash 认证的优点，让一组信息的第 0 条信息传送的是下一条信息的 Hash 值，而这个 Hash 值需要用公钥进行签名认证，此后每条消息都包括本身需要传送的内容和下一条消息的 Hash 值，直到最后一条消息为本身内容加一段随机填充值. 这解决了 μTESLA 协议延迟认证和公钥认证大计算量的问题，但发送前一条消息需要知道后边 $n-1$ 条消息的内容，容易被攻击者利用其洪泛广播方式而发起 DoS 攻击.

2013 年，Shim 等人提出了一个带消息恢复的认证广播方案——EIBAS[82]，取得了最小的通信负荷，相比之前的基于身份的广播认证方案减少了消息长度，从而减少了 48.5% 的消耗. 他们使用了一个没有 MapToPoint 操作、具有消息恢复功能的对优化的 IBS，并参考 Barreto 等人的研究(作为 IEEE P1363.3 的提案)、借用 Tso 等人的消息恢复方法去除了消息的传送，从而减少了通信量. 随后，他们考虑到现有基于身份的认证广播方案虽然去除了传统基于证书机制证书传递的需要，但需要昂贵的双线性对运算，所以他们提出了一类新的基于身份的签名方案，这类签名方案具有消息恢复功能且无对运算需要，并提供可证明安全性. 他们提出了两种消息恢复签名方法：全部消息恢复(MR-IBS)和部分消息恢复(PMR-IBS)，并由此构建了一个基于身份的多用户认证广播方案——BASIS[107]，基于 MICAz 和 Tmote Sky 两类常用硬件平台评估了其计算、通信及能耗等性能指标，实验表明他们的方案与 BAS[54] 和 IMBAS[48] 相比分别节能 66% 和 16% 以上.

如表 12 所示，我们就这些广播认证方案进行了比较. 此外，近来国内常芬等人[110]提出了匿名认证方案，他们结合椭圆曲线和环签名机制在保护身份信息隐私的同时实现了对恶意节点的可追踪性，为 WSNs 中的认证提出了适合应用的新要求.

表 12　各广播认证方案对比

年份	方案	类别	特点
2007	Ren[40]	外部用户广播认证	设计了 Merkle 树、基于证书、基于身份和双线性对三类方法，其计算量依次升高，而通信和存储量依次降低
2008	Cao[48]	外部多用户及 Sink 广播认证	IMBAS，提出一个基于 BNN-IBS 的变体 vBNN-IBS 用于用户广播；使用带部分消息恢复的 Schnorr 签名于 Sink 广播
2009	Ren[54]	外部用户广播认证	在 Ren[40] 基础上设计了基于证书、布隆过滤器、Merkle 树、HAS 四类方法，但 HAS 的可扩展性仍不够好[48]
2010	Wang[57]	Sink 节点广播认证	提出使用短期短长度公钥的 Short-PK，使计算量在确保安全时降低一个量级，但不适于间歇性无规律广播认证
2012	Liu[71]	Sink 节点广播认证	结合 Hash 链技术实现了多消息分摊一个公钥认证的认证方式，需要提前知道紧随其后广播消息的 Hash 值
2013	Shim[82]	多用户及节点间互广播认证	提出了一个带消息恢复的认证广播方案——EIBAS，使用了一个没有 MapToPoint 操作、具有消息恢复功能和对优化的 IBS，进行了安全分析但未进行形式化证明
2017	Shim[107]	外部多用户广播认证	提出完全消息恢复的 MR-IBS、部分消息恢复的 PMR-IBS 签名方案和基于身份的广播认证方案BASIS，并对其进行形式化证明，达到 EUF-CMA 可证明安全性

6　其他应用研究

6.1　抗特殊攻击的公钥机制

在无线传感器网络中引入公钥机制是一把双刃剑，PKC 具有好的耐抗性、可扩展性和去中心化管理等特性[35]，但在弥补对称密钥机制缺陷、提供强安全性的同时，也引入了耗能耗时的公钥操作，所以学者们在考虑应用公钥机制于 WSNs 的同时也努力去克服引入公钥机制带来的影响，如有些学者提出了抗 DoS 攻击[35,48,54,59,123]、抗侧信道(Side Channel Attack，SCA)攻击[3,83,88,109]、抗节点捕获攻击[12,53,74,79,86-87,101]、抗虫洞攻击[35,40]、抗量子攻击[4-5,24,37]等公钥机制研究.

Arazi 等人的工作[35]讨论了抗 DoS 的方案，他们借用 Huang、Aydos 等人快速认证、模平方根实现不对称认证的思想及 Girault 等人提出的自认证公钥技术[77]提出了一个新的基于 RSA 的抗 DoS 攻击的安全框架，通过该安全框架，可使得密钥建立时，发起者将比响应者明显消耗多很多的能量. 在其分成的两个阶段中，第一阶段，采用小指数 RSA 的不对称方式，可使传感器端只需要花费 4 个模乘运算、2 次接收和 1 次发送即可实现对 Sink 节点的认证. 第二阶段，他们提供了三种不同的认证方式：

RSA 密钥传输、ECDSA、基于 ECC 的自证明固定密钥生成.但这两个阶段的设计还不够完善,如在第一阶段存在伪装攻击而第二阶段中的设计有些笔误.

Wang 等人[59]提出了因节点被捕导致的 DoS 攻击问题,因为攻击者可以捕获一个传感器节点,然后用它向网络注入大量的伪造数据包,从而因数据包在整个网络传播而耗尽整个网络的能量,所以他们基于 Shamir 的门限技术及 ECPVS 签名方案提出了一个伪造数据过滤方案——PDF(Public-key based false Data Filtering),能 100%地杜绝伪造数据包且抗节点捕获攻击.但由该文评估可知,这一方案的通信代价比较大,而且需要以一组传感器节点做为签名者,我们认为不太适用于 WSNs.

在抗侧信道攻击研究方面,Lederer 等人[55]基于更高安全级 ECC192 探讨了 ECDH 中如何采用窗口法和 Comb 方法防 SCA 攻击的问题.Liu 等人[88]则发现 Montgomery 曲线中一个很大的优点是存在只用 x 坐标的点加规则,可优化成规则执行的算法以抗 SPA、时序分析等 SCA 攻击,并在后来的密码操作库研究[109]中采用 Montgomery 阶梯法来实现抵抗这类 SCA 攻击.同时,Düll 等人[97]通过避免私密数据依赖分支和保密索引存储访问来避免时序分析、能量分析等 SCA 攻击.而 Shim 等人则在他们的综述[3]中专门论述了 SCA 这一类比较容易发生于易被攻击者靠近的、低配置的传感器节点中的重要安全问题.

6.2 数据安全性保护中的应用

虽然 Gura 等建议尽量将公钥机制用于 WSNs 中的关键功能,但公钥机制除了应用于密钥管理、认证访问研究以外,也被部分学者直接应用于数据的安全保护研究上,公钥操作开销很大,但在一些配置稍高的网络如 HSN 中的高层部分,或结合对称密钥机制构成前头所述的混合方式还是可行的,特别是在有线供电或即时收集能量的 WSNs[135]中.这方面的研究主要有 Mykletun[31]、Shim[99]等人在数据聚集方面的工作、韩国 Haque[46]、Xuan[60]等人在医疗应用上的工作以及印度 Kumar 等人和国内 Wei 等人将无证书数据聚集签名应用于医疗上的工作[117].

7 总结与展望

7.1 总 结

随着物联网的研究与应用逐渐深入,作为物联网的主要组成部分之一——WSNs 的安全影响着物联网的普及应用,没有安全甚至是不够安全的物联网都将不能得到广大用户的青睐,因此 WSNs 中安全问题的彻底解决成为了物联网技术能否被广泛应用的关键,早期基于对称密钥机制方案的众多安全缺陷使得我们不得不再次将目光投向曾被认为不适合于 WSNs 的公钥机制,后来公钥机制在传感器节点上的可行性研究发现,若只将其用于网络中不频繁使用的关键操作以确保安全也是可行的.而随着过去十多年对 ECC 在 WSNs 中实现上的不断优化,其速度也提高了十余倍,这使得 WSNs 中应用公钥机制变得更加可行,特别适合应用于网络建立初期安全的邻居发现中.据现有研究表明,ECC 是现有公钥原语中性能开销比最佳的一类原语,不过效率高、抗量子攻击、基于格理论的 NTRU 在解决了长密钥等带来的高存储与高通信负荷问题后或许能成为今后 WSNs 中最重要的一种公钥原语;而密钥建立中最适合使用无证书/隐式证书机制,但应该选用无双线性对运算的方案,因为就目前研究来看,双线性对运算所耗时间是 ECC 原语操作的 6 倍以上(比较同一安全级下最佳方案);同时无证书/隐式证书机制也适合应用于网内网外的各类认证操作中,但一般适宜使用 Schnorr 模式的签名机制;此外,在医疗保健等应用领域的安全性研究上,基于公钥机制的方案也得到了广泛的关注;最后,引入公钥机制所带来的一系列新的挑战如 DoS 攻击、量子攻击、SCA 攻击、捕获节点攻击、能量耗尽攻击等值得我们进一步去研究探讨.

7.2 待解决的挑战与展望

接下来我们就 WSNs 中的公钥机制研究尚待解决的挑战和可能的解决途径从原语、密钥管理、认证、抗各类攻击等方面进行分析与展望.

(1)原语方面.我们认为有现有原语的测定与提升以及新原语的开发两大研究方向.前者可着重于各类原语的优化提速方面,如对 ECC 进一步进行域上和群上操作的优化、加快模乘、标量乘运算部件的速度,以硬件实现的提速(可考虑将 secFleck 由 RSA 扩展到 ECC)等,此外新的传感器设备中这些原语相关实验数据的获取目前没有很多可参考的依据,多数研究仍建立在早期研究工作之上,如能耗数据多以 Gura 等人工作作为评估基础,因此可在 TI 等公司的新传感器设备上对现有原语进行进一步实验研究,为新设备能耗等性能评估提供参考依据.而

新原语的发掘方面，鉴于现有公钥操作仍属重量级操作，所以诸如不对称运算等新的抗 DoS 攻击的原语思想有待于进一步发掘，而随着量子计算技术的飞跃发展，抗量子攻击的公钥原语研究迫在眉睫，当然这也是整个公钥领域亟待解决的问题，多数学者认为基于格的密码值得深入研究.

(2) 密钥管理. 目前 WSNs 中基于公钥的密钥管理研究主要集中于密钥协商，除此以外，公钥的更新、撤销、节点增加删除也是需要解决的问题，特别是如何在泄露私钥时安全更新 Sink/PKG/KGC/TA/CA 中心的公钥，又如何在更新公钥后更新所有证书，这些方面仍存在许多可研究的问题待我们去探索，事实上，密钥更新、撤销、节点新增删除等也是之前 WSNs 中对称密钥机制研究者们涉足较少的领域. 而在目前研究得比较多的密钥协商方面，考虑链路可靠性的密钥协商、认证的密钥协商方面还有许多可值得研究的，特别是考虑链路可靠性的密钥协商目前涉足的工作比较少，就我们所知，仅有 ShortPK 中[57]比较全面地考虑了可靠性问题，而基于 Merkle 树等 Hash 技术及无证书认证等轻型机制也具有很好的研究前景，因为这些技术更利于抗 DoS 攻击，特别是非常轻的基于 Hash 的认证技术. 此外，WSNs 中 PKI 等较完整的公钥基础设施机制仍未得到较深入全面的研究，目前涉足的仅有 Kim[86]和 Misra[136]等人的工作.

(3) 认证与访问控制方面. 我们说认证包括认证的密钥协商协议、内部实体认证、对外部用户的认证以及广播认证，这一直是 WSNs 中的研究热点，但目前主要集中于 WSNs 对外部用户的认证，特别是基于口令、存储卡、生物特征等三因素甚至多因素访问控制方法的研究. 同时认证是否需要经过 Sink 节点仍是值得讨论的问题，不经过 Sink 节点时可防单点故障、DoS 攻击，但安全仅依赖于配置较低的传感器节点而更容易被成功攻击，而经过 Sink 节点进行认证时又容易导致 DoS 攻击和单点故障等安全问题，我们认为结合这两种方式的混合认证可以扬长避短，因此可能是今后主要的研究方向. 此外，现有 WSNs 中认证与访问控制机制多数仍保持在合法与非法用户的辨识层面，以后应该需要向权限控制方向纵深发展，以适合于对不同层级用户进行访问控制的需要.

(4) 抗各类特殊攻击方面. Shor 的研究[137]表明，在一台量子计算上，大数分解和离散对数问题可以在多项式时间内解决，而对 ECDLP 小嵌入度攻击也有一些新进展[129]，因此寻找抗量子攻击等新公钥原语是目前后量子时代整个公钥安全领域的一大挑战. 在既要求抗量子计算攻击，又要求硬件资源限制为传感器节点之上的情况下，如何设计一种满足这两方面特点的公钥机制极具挑战性. 在 NIST 的后量子密码报告中，除了前面提到的无线传感器网络安全者所关注的基于格和基于多变量两类密码外，还有基于编码和基于哈希的密码，目前密码界公认格密码是最有力的竞争者，并在近期得到了广泛的关注[138]. 而多数研究也表明基于格的 NTRU 是能抗量子攻击的一类轻快的公钥原语，比较可能适用于 WSNs[3]. 虽然已有基于 WSNs 的格密码应用研究[4,24,118]，但这类机制的密钥长度或处理的数据长度很长[3,138]，对于短包通信的 WSNs 是一个阻碍，所以基于格的公钥机制是否确实适合 WSNs 还有待进一步考究. 此外，还有学者提出基于超奇异椭圆曲线上的同源问题、共轭搜索问题以及辫群(braid groups)中相关问题来设计抗量子的密码系统[138]，这些后量子时代的新密码方案是否适合 WSNs 也是值得研究的课题.

而抗 DoS 攻击方面我们除了可以通过提高速度降低开销从而减轻 DoS 攻击被检测到前造成的影响外，采用基于信誉(Reputation-based[139])或临时信任值(Temporal-credential-based[140])的机制等或许是一个好的思路. 但信誉如何表示，如何认定节点身份，节点身份最终是否仍要通过数字签名来解决，这些都是有待于研究的问题. 此外，通过去特征法抗侧信道攻击、在现有基于公钥的密钥协商协议中集成抗资源消耗、节点捕获、虫洞、吸血鬼、女巫、重放、侧信道等各类攻击[90]的能力亦仍有可研究的空间.

(5) 其他方面. 在公钥机制的安全目标方面，WSNs 密钥协商协议应该达可证明安全甚至是语义安全，目前仍只少数协议达到了这一点. 而利用物理层的特点设计安全机制[141]也是值得探究的方向，因为它可以从最底层来防范 DoS 等攻击，如近年来 Zou 等人[104]分析因无线网络开放的广播特性而更易受到各种攻击，他们重点提到了物理层存在的各种干扰攻击，指出虽然可以一定程度上通过跳频如 FHSS 等技术进行防范，但物理层的抗干扰攻击仍具有很大的挑战性. 最后，在安全机制的评估方面，以上安全方案研究中多是分安全性和开销两大块来

评估的,但我们认为对于安全协议的评估还可进一步考虑可靠性和可扩展性.

致 谢 在此,我们向对本文提出宝贵建议的审稿专家及参与本文内容讨论的所有老师和同学表示衷心的感谢,特别感谢张晓瞳同学提的修改建议!

参 考 文 献

[1] Zhang Yu-Qing, Zhou Wei, Peng An-Ni. Survey of Internet of Things security. Journal of Computer Research and Development, 2017, 54(10): 2130-2143(in Chinese)
(张玉清, 周威, 彭安妮. 物联网安全综述. 计算机研究与发展, 2017, 54(10): 2130-2143)

[2] Jing Q, Vasilakos A V, Wan J, et al. Security of the Internet of Things: Perspectives and challenges. Wireless Networks, 2014, 20(8): 2481-2501

[3] Shim K A. A survey of public-key cryptographic primitives in wireless sensor networks. IEEE Communication Surveys & Tutorials, 2016, 18(1): 577-601

[4] Lopez J. Unleashing public-key cryptography in wireless sensor networks. Journal of Computer Security, 2006, 14(5): 469-482

[5] Gaubatz G, Kaps J P, Sunar B. Public key cryptography in sensor networks—Revisited//Proceedings of the European Conference on Security in Ad-Hoc and Sensor Networks. Heidelberg, Germany, 2004: 2-18

[6] Perrig A, Szewczyk R, Wen V, et al. SPINS: Security protocols for sensor networks//Proceedings of the 7th Annual International Conference on Mobile Computing and Networking. Rome, Italy, 2001: 189-199

[7] Zhu S, Setia S, Jajodia S. LEAP: Efficient security mechanisms for large-scale distributed sensor networks//Proceedings of the 10th ACM Conference on Computer and Communications Security. Washington, USA, 2003: 62-72

[8] Karlof C, Saatry N, Wagner D. TinySec: A link layer security architecture for wireless sensor networks//Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems. Baltimore, USA, 2004: 162-175

[9] Eschenauer L, Gligor D V. A key-management scheme for distributed sensor networks//Proceedings of the 9th ACM Conference on Computer and Communications Security. Washington, USA, 2002: 41-47

[10] Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks//Proceedings of the IEEE Symposium on Security and Privacy. Berkeley, USA, 2003: 197-213

[11] Brown J, Du X, Nygard K. An efficient public-key-based heterogeneous sensor network key distribution scheme//Proceedings of the 2007 IEEE Global Communications Conference. Washington, USA, 2007: 991-995

[12] Zhang Y, Liu W, Lou W, et al. Location-based compromise tolerant security mechanisms for wireless sensor networks. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 247-260

[13] Oliveira L B, Scott M, Lopez J, et al. TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks//Proceedings of the International Conference on Networked Sensing Systems. Kanazawa, Japan, 2008: 173-180

[14] Wander A S, Gura N, Eberle H, et al. Energy analysis of public-key cryptography for wireless sensor networks//Proceedings of the IEEE International Conference on Pervasive Computing and Communications. Koloa, USA, 2005: 324-328

[15] Cui Li, Ju Hai-Ling, Miao Yong, et al. Overview of wireless sensor networks. Journal of Computer Research and Development, 2005, 42(1): 163-174(in Chinese)
(崔莉, 鞠海玲, 苗勇等. 无线传感器网络研究进展. 计算机研究与发展, 2005, 42(1): 163-174)

[16] Hasegawa T, Nakajima J, Matsui M. A practical implementation of elliptic curve cryptosystems over $GF(p)$ on a 16-bit microcomputer//Proceedings of the International Workshop on Public Key Cryptography. Pacifico Yokohama, Japan, 1998: 182-194

[17] Woodbury A D, Bailey D V, Paar C. Elliptic curve cryptography on smart cards without coprocessors//Proceedings of the 4th Smart Card Research and Advanced Application Conference. Bristol, UK, 2000: 71-92

[18] Huang Q, Cukier J, Kobayashi H, et al. Fast authenticated key establishment protocols for self-organizing sensor networks//Proceedings of the ACM International Conference on Wireless Sensor Networks and Applications. San Diego, USA, 2003: 141-150

[19] Watro R, Kong D, Cuti S F, et al. TinyPK: Securing sensor networks with public key technology//Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks. Washington, USA, 2004: 59-64

[20] Gura N, Patel A, Wander A, et al. Comparing elliptic curve cryptography and RSA on 8-bit CPUs//Proceedings of the 6th International Workshop on Cryptographic Hardware and Embedded Systems. Cambridge, USA, 2004: 119-132

[21] Malan D J, Welsh M, Smith M D. A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography//Proceedings of the 1st IEEE Conference on Sensor and Ad Hoc Communications and Networks. Santa Clara, USA, 2004: 71-80

[22] Malan D J, Welsh M, Smith M D. Implementing public-key infrastructure for sensor networks. ACM Transactions on Sensor Networks, 2008, 4(4): 1-23

[23] Du W, Wang R, Ning P. An efficient scheme for authenticating public keys in sensor networks//Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing. Urbana, USA, 2005: 58-67

[24] Gaubatz G, Kaps J P, Ozturk E, et al. State of the art in ultra-low power public key cryptography for wireless sensor networks//Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops. Koloa, USA, 2005: 146-150

[25] Blaß E, Zitterbart M. Towards acceptable public-key encryption in sensor networks//Proceedings of the 2nd International Workshop on Ubiquitous Computing. Miami, USA, 2005: 88-93

[26] Gupta V, Millard M, Fung S, et al. Sizzle: A standards-based end-to-end security architecture for the embedded Internet. Pervasive & Mobile Computing, 2005, 1(4): 425-445

[27] Arazi O, Elhanany I, Rose D, et al. Self-certified public key generation on the Intel Mote 2 sensor network platform//Proceedings of the IEEE Workshop on Wireless Mesh Networks. Reston, USA, 2006: 118-120

[28] Arazi O, Qi H. Self-certified group key generation for ad hoc clusters in wireless sensor networks//Proceedings of the International Conference on Computer Communications and Networks. Saint Thomas, USA, 2008: 359-364

[29] Jing Q, Hu J, Chen Z. C4W: An energy efficient public key cryptosystem for large-scale wireless sensor networks//Proceedings of the 3rd IEEE International Conference on Mobile Adhoc and Sensor Systems. Vancouver, Canada, 2006: 827-832

[30] Ma J, Zhang S, Zhong Y, et al. PEAN: A public key authentication scheme in wireless sensor and actor network//Proceedings of the IEEE International Conference on Computer and Information Technology. Seoul, Korea, 2006: 230-235

[31] Mykletun E, Girao J, Westhoff D. Public key based cryptoschemes for data concealment in wireless sensor networks//Proceedings of the IEEE International Conference on Communications. Istanbul, Turkey, 2006: 2288-2295

[32] Nyang D H, Mohaisen A. Cooperative public key authentication protocol in wireless sensor network//Proceedings of the International Conference on Ubiquitous Intelligence and Computing. Wuhan, China, 2006: 864-873

[33] Bellare M, Kohno T, Shoup V. Stateful public-key cryptosystems: How to encrypt with one 160-bit exponentiation//Proceedings of the ACM Conference on Computer and Communications Security. Alexandria, USA, 2006: 380-389

[34] Wang H, Li Q. Efficient implementation of public key cryptosystems on mote sensors//Proceedings of the International Conference on Information and Communications Security. Raleigh, USA, 2006: 519-528

[35] Arazi O, Qi H, Rose D. A public key cryptographic method for denial of service mitigation in wireless sensor networks//Proceedings of the 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. San Diego, USA, 2007: 51-59

[36] Zhou Y, Zhang Y, Fang Y. Access control in wireless sensor networks. Ad Hoc Networks, 2007, 5(1): 3-13

[37] Roman R, Alcaraz C. Applicability of public key infrastructures in wireless sensor networks//Proceedings of the 4th European Conference on Public Key Infrastructure: Theory and Practice. Palma de Mallorca, Spain, 2007: 313-320

[38] Oliveira L B, Dahab R, Lopez J, et al. Identity-based encryption for sensor networks//Proceedings of the 5th IEEE International Conference on Pervasive Computing and Communications Workshops. White Plains, USA, 2007: 290-294

[39] Oliveira L B, Aranha D F, Morais E, et al. TinyTate: Computing the Tate Pairing in resource-constrained sensor nodes//Proceedings of the 6th IEEE International Symposium on Network Computing and Applications. Cambridge, USA, 2007: 318-323

[40] Ren K, Zeng K, Lou W, et al. On broadcast authentication in wireless sensor networks. IEEE Transactions on Wireless Communications, 2007, 6(11): 4136-4144

[41] Kim Y H, Lee H, Park J H, et al. Key establishment scheme for sensor networks with low communication cost//Proceedings of the International Conference on Autonomic and Trusted Computing. Hong Kong, China, 2007: 441-448

[42] Yang Geng, Wang Jiang-Tao, Cheng Hong-Bing, et al. A key establish scheme for WSN based on IBE and Diffie-Hellman algorithms. Acta Electronica Sinica, 2007, 35(1): 180-184(in Chinese)
(杨庚，王江涛，程宏兵等. 基于身份加密的无线传感器网络密钥分配方法. 电子学报，2007，35(1)：180-184)

[43] Liu A, Ning P. TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks//Proceedings of the International Conference on Information Processing in Sensor Networks. St. Louis, USA, 2008: 245-256

[44] Seo S C, Han D G, Kim H C, et al. TinyECCK: Efficient elliptic curve cryptography implementation over $GF(2^m)$ on 8-bit Micaz mote. IEICE Transactions on Information and Systems, 2008, E91-D(5): 1338-1347

[45] Baek J, Tan H C, Zhou J, et al. Realizing stateful public key encryption in wireless sensor network//Proceedings of the IFIP TC-11 23rd International Information Security Conference. Milano, Italy, 2008: 95-107

[46] Haque M M, Pathan A S K, Hong C S. Securing U-healthcare sensor networks using public key based scheme//Proceedings of the 10th International Conference on Advanced Communication Technology. Phoenix Park, Korea, 2008: 1108-1111

[47] Szczechowiak P, Oliveira L B, Scott M, et al. NanoECC: Testing the limits of Elliptic Curve Cryptography in sensor

networks//Proceedings of the 5th European Conference on Wireless Sensor Networks. Bologna, Italy, 2008: 305-320

[48] Cao X, Kou W, Dang L, et al. IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks. Computer Communications, 2008, 31(4): 659-667

[49] Pan Yun, Wang Li-Cheng, Cao Zhen-Fu, et al. Lite-CA based key pre-distribution scheme in wireless sensor network. Journal on Communications, 2009, 30(3): 130-134(in Chinese)
(潘耘, 王励成, 曹珍富等. 基于轻量级 CA 的无线传感器网络密钥预分配方案. 通信学报, 2009, 30(3): 130-134)

[50] Oliveira L B, Kansal A, Priyantha B, et al. Secure-TWS: Authenticating node to multi-user communication in shared sensor networks//Proceedings of the IEEE International Conference on Information Processing in Sensor Networks. San Francisco, USA, 2009: 289-300

[51] Du X, Guizani M, Xiao Y, et al. A routing-driven Elliptic Curve Cryptography based key management scheme for heterogeneous sensor networks. IEEE Transactions on Wireless Communications, 2009, 8(3): 1223-1229

[52] Hu W, Corke P, Wen C S, et al. secFleck: A public key technology platform for wireless sensor networks//Proceedings of the European Conference on Wireless Sensor Networks. Cork, Ireland, 2009: 296-311

[53] Szczechowiak P, Kargl A, Scott M, et al. On the application of pairing based cryptography to wireless sensor networks//Proceedings of the 2nd ACM Conference on Wireless Network Security. Zurich, Switzerland, 2009: 1-12

[54] Ren K, Yu S, Lou W, et al. Multi-user broadcast authentication in wireless sensor networks. IEEE Transactions on Vehicular Technology, 2009, 58(8): 4554-4564

[55] Lederer C, Mader R, Koschuch M, et al. Energy-efficient implementation of ECDH key exchange for wireless sensor networks//Proceedings of the 3rd IFIP WG 11.2 International Workshop on Information Security Theory and Practice: Smart Devices, Pervasive Systems, and Ubiquitous Networks. Brussels, Belgium, 2009: 112-127

[56] Xiong X, Wong D S, Deng X. TinyPairing: A fast and light-weight Pairing-based cryptographic library for wireless sensor networks//Proceedings of the Wireless Communications and Networking Conference. Sydney, Australia, 2010: 1-6

[57] Wang R, Du W, Liu X, et al. ShortPK: A short-term public key scheme for broadcast authentication in sensor networks. ACM Transactions on Sensor Networks, 2010, 6(1): 1-29

[58] Aranha D F, Dahab R, Pez J, et al. Efficient implementation of elliptic curve cryptography in wireless sensors. Advances in Mathematics of Communications, 2010, 4(2): 169-187

[59] Wang H, Li Q. Achieving robust message authentication in sensor networks: A public-key based approach. Wireless Networks, 2010, 16(4): 999-1009

[60] Xuan H L, Sankar R, Khalid M, et al. Public key cryptography-based security scheme for wireless sensor networks in healthcare//Proceedings of the International Conference on Ubiquitous Information Management and Communication. Suwon, Korea, 2010: 1-7

[61] Yasmin R, Ritter E, Wang G. An authentication framework for wireless sensor networks using identity-based signatures //Proceedings of the 10th IEEE International Conference on Computer and Information Technology. Bradford, UK, 2010: 882-889

[62] Liu J K, Baek J, Zhou J, et al. Efficient online/offline identity-based signature for wireless sensor network. International Journal of Information Security, 2010, 9(4): 287-296

[63] Rahman S M M, El-Khatib K. Private key agreement and secure communication for heterogeneous sensor networks. Journal of Parallel & Distributed Computing, 2010, 70(8): 858-870

[64] Wang Chao, Shi Xiang-Yong, Niu Zhi-Hua. The research of the promotion for ECDSA algorithm based on Montgomery-form ECC. Journal on Communications, 2010, 31(1): 9-13 (in Chinese)
(王潮, 时向勇, 牛志华. 基于 Montgomery 曲线改进 ECDSA 算法的研究. 通信学报, 2010, 31(1):9-13)

[65] Chen Yan-Li, Yang Geng. Hybrid group key management scheme for wireless sensor networks. Journal on Communications, 2010, 31(11): 56-64(in Chinese)
(陈燕俐, 杨庚. 适合于无线传感器网络的混合式组密钥管理方案. 通信学报, 2010, 31(11): 56-64)

[66] Wang H, Sheng B, Tan C C, et al. Public-key based access control in sensornet. Wireless Networks, 2011, 17(5): 1217-1234

[67] Oliveira L B, Aranha D F, Gouvêa C P L, et al. TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. Computer Communications, 2011, 34(3): 485-493

[68] Hur J. Fine-grained data access control for distributed sensor networks. Wireless Networks, 2011, 17(5): 1235-1249

[69] Zhang X, He J, Wei Q. EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks. EURASIP Journal on Wireless Communications & Networking, 2011, 2011(1): 1-11

[70] Huang Jie, Huang Bei. Public key based key distribution scheme for wireless sensor networks. Journal on Communications, 2011, 32(10): 52-58(in Chinese)
(黄杰, 黄蓓. 无线传感器网络中一种基于公钥的密钥分配方案. 通信学报, 2011, 32(10): 52-58)

[71] Liu Y, Li J, Guizani M. PKC based broadcast authentication using signature amortization for WSNs. IEEE Transactions on Wireless Communications, 2012, 11(6): 2106-2115

[72] Gouvêa C P L, Oliveira L B, López J. Efficient software implementation of public-key cryptography on sensor networks using the MSP430X microcontroller. Journal of Cryptographic Engineering, 2012, 2(1): 19-29

[73] Li F, Zhong D, Takagi T. Practical identity-based signature for wireless sensor networks. IEEE Wireless Communications Letters, 2012, 1(6): 637-640

[74] Alagheband M R, Aref M R. Dynamic and secure key management model for hierarchical heterogeneous sensor networks. Information Security Iet, 2012, 6(4): 271-280

[75] Du D, Xiong H, Wang H. An efficient key management scheme for wireless sensor networks. International Journal of Distributed Sensor Networks, 2012, 2012(1): 141-149

[76] Chang S Y, Lin Y H, Sun H M, et al. Practical RSA signature scheme based on periodical rekeying for wireless sensor networks. ACM Transactions on Sensor Networks, 2012, 8(2): 13

[77] Ren Yong-Jun, Wang Jian-Dong, Xu Da-Zhuan, et al. Key agreement protocol for wireless sensor networks using self-certified public key system. Journal of Computer Research and Development, 2012, 49(2): 304-311(in Chinese)
(任勇军，王建东，徐大专等. 自认证公钥的无线传感器网络密钥协商协议. 计算机研究与发展，2012，49(2)：304-311)

[78] Wang Chao, Hu Guang-Yue, Zhang Huan-Guo. Lightweight security architecture design for wireless sensor network. Journal on Communications, 2012, 33(2): 30-35(in Chinese)
(王潮，胡广跃，张焕国. 无线传感器网络的轻量级安全体系研究. 通信学报，2012，33(2)：30-35)

[79] Ruj S, Sakurai K. Secure and privacy preserving hierarchical wireless sensor networks using hybrid key management technique //Proceedings of the Global Communications Conference. Atlanta, USA, 2013: 402-407

[80] Li Y, Li W, Wang G, et al. A hybrid authenticated group key agreement protocol in wireless sensor networks. International Journal of Distributed Sensor Networks, 2013, 2013(6): 69-72

[81] Seo H, Shim K A, Kim H. Performance enhancement of TinyECC based on multiplication optimizations. Security & Communication Networks, 2013, 6(2): 151-160

[82] Shim K A, Lee Y R, Park C M. EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks. Ad Hoc Networks, 2013, 11(1): 182-189

[83] Wenger E. Hardware architectures for MSP430-based wireless sensor nodes performing elliptic curve cryptography// Proceedings of the 11th International Conference on Applied Cryptography and Network Security. Banff, Canada, 2013: 290-306

[84] Porambage P, Kumar P, Schmitt C, et al. Certificate-based pairwise key establishment protocol for wireless sensor networks//Proceedings of the IEEE International Conference on Computational Science and Engineering. Sydney, Australia, 2013: 667-674

[85] Qin Z, Zhang X, Feng K, et al. An efficient identity-based key management scheme for wireless sensor networks using the Bloom filter. Sensors, 2014, 14(10): 17937

[86] Kim D, An S. Efficient and scalable public key infrastructure for wireless sensor networks//Proceedings of the International Symposium on Networks, Computers and Communications. Hammamet, Tunisia, 2014: 1-5

[87] Yang L, Ding C, Wu M. Establishing authenticated pairwise key using pairing-based cryptography for sensor networks// Proceedings of the 8th International Conference on Communications and Networking in China. Guilin, China, 2014: 517-522

[88] Liu Z, Wenger E, Großschädl J. MoTE-ECC: Energy-scalable elliptic curve cryptography for wireless sensor networks// Proceedings of the 12th International Conference on Applied Cryptography and Network Security. Lausanne, Switzerland, 2014: 361-379

[89] Yin A, Liang H. Certificateless hybrid signcryption scheme for secure communication of wireless sensor networks. Wireless Personal Communications, 2015, 80(3): 1049-1062

[90] Tufail A, Khan A M, Kim K H. A reliable and secure hybrid key management scheme for WSNs. Journal of Internet Technology, 2015, 16(4): 629-642

[91] Targhetta A D, Owen D E, Israel F L, et al. Energy-efficient implementations of $GF(p)$ and $GF(2^m)$ elliptic curve cryptography//Proceedings of the 33rd IEEE International Conference on Computer Design. New York City, USA, 2015: 704-711

[92] Seo S H, Won J, Sultana S, et al. Effective key management in dynamic wireless sensor networks. IEEE Transactions on Information Forensics & Security, 2015, 10(2): 371-383

[93] Boudia O R M, Senouci S M, Feham M. A novel secure aggregation scheme for wireless sensor networks using stateful public key cryptography. Elsevier Science Publishers B.V., 2015, 32(C): 98-113

[94] Horng S J, Tzeng S F, Huang P H, et al. An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks. Information Sciences, 2015, 317(C): 48-66

[95] Sharma G, Bala S, Verma A K. Pairing-free certificateless ring signcryption (PF-CLRSC) scheme for wireless sensor networks. Wireless Personal Communications, 2015, 84(2): 1-17

[96] Bala S, Sharma G, Verma A K. PF-ID-2PAKA: Pairing free identity-based two-party authenticated key agreement protocol for wireless sensor networks. Wireless Personal Communications, 2015, 87(3): 1-18

[97] Düll M, Haase B, Hinterwälder G, et al. High-speed Curve25519 on 8-bit, 16-bit, and 32-bit microcontrollers. Designs Codes & Cryptography, 2015, 77(2-3): 493-514

[98] Liu Z, Seo H, Hu Z, et al. Efficient implementation of ECDH key exchange for MSP430-based wireless sensor networks//Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. Singapore, 2015: 145-153

[99] Shim K A, Park C M. A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks. IEEE Transactions on Parallel & Distributed Systems, 2015, 26(8): 2128-2139

[100] Chang C C, Le H D. A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. IEEE Transactions on Wireless Communications, 2016, 15(1): 357-366

[101] Nadir I, Zegeye W K, Moazzami F, et al. Establishing symmetric pairwise-keys using public-key cryptography in Wireless Sensor Networks (WSN)//Proceedings of the IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference. New York, USA, 2016: 1-6

[102] Simplicio Jr M A, Silva M V M, Alves R C A, et al. Lightweight and escrow-less authenticated key agreement for the Internet of Things. Computer Communications, 2016, 98(2017): 43-51

[103] Wan C, Zhang J. Identity-based key management for wireless sensor networks using Lagrange interpolation. Security & Communication Networks, 2016, 9(16): 3713-3723

[104] Zou Y, Zhu J, Wang X, et al. A survey on wireless security: Technical challenges, recent advances, and future trends. Proceedings of the IEEE, 2016, 104(9): 1727-1765

[105] Liu Z, Großschädl J, Li L, Xu Q. Energy-efficient elliptic curve cryptography for MSP430-based wireless sensor nodes//Proceedings of the 21st Australasian Conference on Information Security and Privacy. Melbourne, Australia, 2016(9722): 94-112

[106] Ferrag M A, Maglaras L A, Janicke H, et al. Authentication protocols for Internet of Things: A comprehensive survey. Security & Communication Networks, 2017, 2017(4): 1-41

[107] Shim K A. BASIS: A practical multi-user broadcast authentication scheme in wireless sensor networks. IEEE Transactions on Information Forensics and Security, 2017, 12(7): 1545-1554

[108] Al-Turjman F, Ever Y K, Ever E, et al. Seamless key agreement framework for mobile-sink in IoT based cloud-centric secured public safety sensor networks. IEEE Access, 2017, PP(99): 1

[109] Liu Z, Huang X, Hu Z, et al. On emerging family of elliptic curves to secure Internet of Things: ECC comes of age. IEEE Transactions on Dependable & Secure Computing, 2017, 14(3): 237-248

[110] Chang Fen, Cui Jie, Wang Liang-Min. A traceable and anonymous authentication scheme based on elliptic curve for wireless sensor network. Journal of Computer Research and Development, 2017, 54(9): 2011-2020(in Chinese)
(常芬, 崔杰, 王良民. WSN 中基于椭圆曲线的可追踪匿名认证方案. 计算机研究与发展, 2017, 54(9): 2011-2020)

[111] Jiang Q, Zeadally S, Ma J, et al. Lightweight three-factor authentication and key agreement protocol for Internet-integrated wireless sensor networks. IEEE Access, 2017, 5: 3376-3392

[112] Kwon J, Seo S C, Hong S. An efficient implementation of Pairing-based cryptography on MSP430 processor. Journal of Supercomputing, 2018, 74(5): 1-24

[113] Li C, Zhang X, Wang H, et al. An enhanced secure identity-based certificateless public key authentication scheme for vehicular sensor networks. Sensors, 2018, 18(1): 194

[114] Li X, Niu J, Kumari S, et al. A three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things environments. Journal of Network and Computer Applications, 2018, 103: 194-204

[115] Ke Z, Kai X, Fushan W. A provably secure anonymous authenticated key exchange protocol based on ECC for wireless sensor networks. Wireless Communications and Mobile Computing, 2018, 2018(Special Issue): 1-9

[116] Hwajeong S. Compact software implementation of public-key cryptography on MSP430X. ACM Transactions on Embedded Computing Systems, 2018, 17(3): 1-12

[117] Kumar P, Kumari S, Sharma V, et al. A certificateless aggregate signature scheme for healthcare wireless sensor network. Sustainable Computing: Informatics and Systems, 2018, 18: 80-89

[118] Zhu H, Tan Y, Zhu L, et al. An identity-based anti-quantum privacy-preserving blind authentication in wireless sensor networks. Sensors, 2018, 18(5): 1663

[119] Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation, 1987, 48: 203-209

[120] Shannon C E. Communication theory of secrecy systems. Bell System Technical Journal, 2014, 28(4): 656-715

[121] Li Xiao-Wei. Research on Provably Secure Authentcated Key Agreement Protocol [Ph. D. dissertation]. Xidian University, Xi'an, 2013(in Chinese)
(李晓伟. 可证明安全的认证与密钥协商协议研究[博士学位论文]. 西安电子科技大学, 西安, 2012)

[122] Lu Lai-Feng. Study on Theory and Applications of Security Protocols Formal Analysis [Ph. D. dissertation]. Xidian University, Xi'an, 2012(in Chinese)
(鲁来凤. 安全协议形式化分析理论与应用研究[博士学位论文]. 西安电子科技大学, 西安, 2012)

[123] Gope P, Hwang T. A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. IEEE Transactions on Industrial Electronics, 2016, 63(11): 7124-7132

[124] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978, 32(2): 126-130

[125] Galbraith S D, Paterson K G, Smart N P. Pairings for cryptographers. Discrete Applied Mathematics, 2008, 156(16): 3113-3121

[126] Hoffstein J, Pipher J, Silverman J H. NTRU: A ring-based public key cryptosystem. Algorithmic Number Theory, 1998, (1423): 267-288

[127] Diffie W, Hellman M E. New directions in cryptography. IEEE Transactions on Information Theory, 1976, IT-22(6): 644-654

[128] Gay D, Levis P, Behren R V, et al. The nesC language: A holistic approach to networked embedded systems//Proceedings of the ACM Sigplan 2003 Conference on Programming Language Design and Implementation. San Diego, USA, 2003: 1-11

[129] Joux A, Vitse V. Elliptic curve discrete logarithm problem over small degree extension fields. Journal of Cryptology, 2013, 26(1): 119-143

[130] Diffie W, Oorschot P C V, Wiener M J. Authentication and authenticated key exchanges. Designs Codes & Cryptography, 1992, 2(2): 107-125

[131] Law L, Menezes A, Qu M, et al. An efficient protocol for authenticated key agreement. Designs Codes & Cryptography, 2003, 28(2): 119-134

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

[133] Al-Riyami S S, Paterson K G. Certificateless public key cryptography. ASIACRYPT 2003, 2003, 2894(2): 452-473

[134] Seo S, Bertino E. Elliptic curve cryptography based certificateless hybrid signcryption scheme without pairing. CERIAS of Purdue University, West Lafayette, USA: Technical Report: TR 2013-10, 2013

[135] He S, Chen J, Jiang F, et al. Energy provisioning in wireless rechargeable sensor networks. IEEE Transactions on Mobile Computing, 12(10): 1931-1942, 2013

[136] Misra S, Goswami S, Taneja C, et al. Design and implementation analysis of a public key infrastructure-enabled security framework for ZigBee sensor networks. International Journal of Communication Systems, 2016, 29(13): 1992-2014

[137] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. Society for Industrial and Applied Mathematics Review, 1999, 41(2): 303-332

[138] Zhang Ping-Yuan, Jiang Han, Cai Jie, et al. Recent advances in Lattice-based Cryptography. Journal of Computer Research and Development, 2017, 54(10): 2121-2129(in Chinese)
(张平原，蒋瀚，蔡杰等. 格密码技术近期研究进展. 计算机研究与发展，2017, 54(10): 2121-2129)

[139] Ganeriwal S, Balzano L K, Srivastava M B. Reputation-based framework for high integrity sensor networks. ACM Transactions on Sensor Networks, 2008, 4(3): 1-37

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

[141] Zenger C T, Pietersz M, Zimmer J, et al. Authenticated key establishment for low-resource devices exploiting correlated random channels. Computer Networks, 2016, 109: 105-123

HE Yan-Xiang, Ph. D., professor, Ph. D. supervisor. His research interests include distributed parallel processing, trusted software, data analysis and software engineering.

SUN Fa-Jun, Ph. D. candidate, associate professor. His research interests include trusted sensor network and software, distributed computing.

LI Qing-An, Ph. D., associate professor. His research interests include compilation optimization and embedded systems.

HE Jing (Selena), Ph. D., associate professor. Her research interests include wireless networking and mobile computing, social network analysis and big data analysis on clouds.

WANG Lv-Meng, Ph. D. candidate. His research interests include GPGPU parallel computing and low power consumption.

Background

Security is an important issue to WSNs especially in the context of IoT. Because of their inherent characteristics, the mechanisms based on symmetric-key all have their own insurmountable shortcomings that can be perfectly solved in the public key mechanisms. In the same time, the deployment of public key mechanisms in sensor networks has its own unique advantage that security data can be preloaded before deployment. The existing literatures mainly focus on the three fields: public key primitives, pairwise key establishment, authentication and access control. The feasibility of public

key primitives and the authentication problems of public key and node identity have been solved preliminarily, but there is still room for optimization in these two aspects. In addition, the introduction of public key mechanism enhances the effect of some special attacks, such as attacks with nodes captured, DoS attack and quantum attack. In this paper, the necessity, feasibility, related problems, challenges and existing solutions of introducing public key mechanism into sensor networks are summarized. And some research directions and possible approaches are prospected.

Our research group mainly study how to construct trusted sensor network, especially how to construct the trusted protocols and softwares in the WSNs. We had ever researched on "Impact of Link Status on Key Negotiation in WSNs" and proposed some coping approaches. This research

is funded by the National Natural Science Foundation of China (NSFC) project "Research on Theories and Methods of Trusted Software Construction" under Grant No. 91118003 which aims at a series of theories and methods for constructing trusted software by combining theoretical research with empirical research. This paper is supported by the NSFC project "Research on Theory and Methods of Green Compiler for Green Embedded Systems" under Grant No. 61373039 as well which focuses on power optimization of embedded systems via a special green compiler framework. This paper is supported by the NSFC project "Wear Leveling Method for Phase-change Memory Based on Compiler Technology" under Grant No. 61502346 which mainly solves the issues on calling transformation and dispersion transformation of spilling code to ease the uneven writes on stack.