计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2015.20150764
52(10):2341-2352,2015

物联网隐私保护研究进展

董晓蕾
(华东师范大学上海市高可信计算重点实验室 上海 200062)
(dongxiaolei@sei.ecnu.edu.cn)

Advances of Privacy Preservation in Internet of Things

Dong Xiaolei
(*Shanghai Key Laboratory for Trustworthy Computing*, *East China Normal University*, *Shanghai* 200062)

Abstract Internet of things (IoT) has been increasingly applied to kinds of new network environments. In the ciphertext access control of IoT, it is required to achieve fine-grained access control policy on the authorized entities. Unfortunately, the traditional communication channel security cannot well satisfy the security and privacy requirements from the "one-to-many" and "many-to-many" scenarios such as resisting the secret key sharing attack. Privacy preserving outsourced computation in IoT can realize secure data aggregation and signal processing in the encrypted domain, protect the individual data privacy and the aggregation result privacy, and verify the correctness of computation. However, most of the existing work exploited (fully) homomorphic encryption directly on data themselves, incurring inefficiency and significantly deviating from the principle of hybrid encryption. To address the issues outlined above, in this paper, we introduce recent concrete solutions exploiting cryptographic techniques, especially presenting the following two results proposed by our research team: a new mechanism of traceable and revocable attribute-based encryption and a new method of lightweight privacy preserving aggregating n data by executing the public key encryption only once. On the meanwhile, we also give a survey on the privacy preserving techniques in popular network services such as smart grid, wireless body area network and wireless vehicular ad hoc network, and suggest the recent advances and results with respect to the challenging open problems in this research field all over the world.

Key words Internet of things (IoT); privacy preserving; ciphertext access control; secure outsource computation; traceable; revocable; lightweight

摘 要 物联网被越来越广泛地应用于各种不同的新型网络环境中.在物联网密文数据访问控制方面,要求对授权方实现细粒度的密文访问控制策略.然而,传统的信道安全无法满足"一对多"、"多对多"环境下抵抗密钥共享攻击等基于应用的安全与隐私保护需求.物联网隐私保护外包计算可在加密域上,保护单个数据隐私及外包计算结果隐私的前提下实现对数据的聚合和信号处理等运算,并验证其正确性.但现有工作多基于(全)同态加密技术来实现,效率低下,且不符合混合加密的基本原则.针对上述2方面问题,介绍了国际上近年来利用密码学技术的具体的解决方案,特别是阐述了该团队提出的同时满足可追踪与可撤销性的多机构属性基加密方法和在不得不使用公钥加密进行数据隐私保护的前提下,仅使用一次公钥加密来高效实现对n个数据轻量级隐私保护外包聚合的新方法.同时,对当前热门的智能电网、无线体域网和无线车载网等中的隐私保护研究进展进行了综述,给出了国内外在该领域的最新

收稿日期:2015-06-15;**修回日期**:2015-08-19
基金项目:国家"九七三"重点基础研究发展计划基金项目(2012CB723401);国家自然科学基金创新群体项目(61321064);国家自然科学基金项目(61373154);国家自然科学基金A3前瞻计划项目(61411146001)

研究进展和对该领域具有挑战性的公开问题的研究情况.

关键词 物联网;隐私保护;密文数据访问控制;安全外包计算;可追踪;可撤销;轻量化

中图法分类号 TP309

物联网隐私保护有密码学技术和非密码学技术2类,本文主要介绍密码学技术实现隐私保护的研究进展.物联网是指利用局部网络或互联网等通信技术把传感器、控制器、机器、人员和物等通过新的方式联在一起,形成人与物、物与物相联,实现信息化、远程管理控制和智能化的网络[1-2].物联网是互联网的延伸,它包括互联网及互联网上所有的资源,兼容互联网所有的应用.与普通互联网不同的是由于物联网是通过射频识别(radio frequency identification, RFID)装置、红外感应器等信息传感设备把物品与互联网相连接的,因此其主要节点的运算、传输等资源都受到极大的制约,可以说资源受限是物联网的一个重要特点.如何在资源受限的物联网中,保护用户的数据隐私、身份隐私与位置隐私等将直接影响物联网的发展与普及.

在资源受限的物联网中,最常用的保护各类隐私的方法是加密(通常是同态加密),设计轻量化加密方案成为物联网隐私保护中最重要的方法之一.我们认为,在不得不使用公钥加密的时候,除了轻量化加密方案外,减少使用公钥加密/解密的次数是更为重要的方法,尤其是只使用一次公钥加密的方法.2006年为了减少使用CA的认证次数我们提出了轻量化CA的加密方法[3].2011年我们给出了利用陷门单向置换构造CCA2安全的轻量级CA加密方案的一般方法[4],并应用这个方法,采用Onion Routing数据转发协议,加密了车载网(vehicular ad-hoc network, VANET)用户申请服务的内容与传输路径,保证了服务内容与用户信息的隐私.这个工作近年来已被作为一种基本方法被国内外学者大量应用于车载网络、传感网络等安全和隐私保护研究[5-8].

物联网中所有的元素(设备、资源及通信等)都是个性化和私有化的.因此,从用户的角度来说,如何实现物联网通信中的各类隐私保护显得尤为重要.物联网根据实际应用背景主要包括无线体域网、智能电网、车载网和无线射频网(RFID)等.由于物联网节点具有存储、计算和通信资源受限的特点,因此除了满足互联网中一般的隐私保护需求外,还需特别注重设计的高效性与轻量性.以无线体域网为例,利用生物特征设计轻量级的、无需密钥材料预分配的密钥协商协议,以满足人体传感器节点资源受限的特点.另一方面,正是由于物联网节点资源受限,我们还考虑如何在资源分配不对称的环境中,研究基于云计算物联网系统中的隐私保护问题.由于云服务器通常被认为拥有充足的存储和计算资源,因此物联网节点可以把存储开销较大的数据外包存储在云服务器上;或将计算开销较大的运算外包给云服务器,完成外包聚合、外包计算等工作.然而,云服务器通常被认为在半可信模式或恶意模式下工作.前者是指云服务器严格执行协议的规定,但通过与用户的交互最大程度地提取有关用户隐私的秘密信息;后者是指云服务器可以任意破坏协议的执行.因此,外包存储的数据必须以加密的形式存储在云服务器上,外包计算也必须在加密域上进行.如何保证云存储密文数据的细粒度访问控制及外包计算中用户的个人数据隐私、外包计算结果隐私及实现外包计算结果的正确性验证具有重要的理论意义与实际应用价值.

在外包存储密文数据访问控制方面,国内外研究进展逐渐从传统的只针对信道攻击来研究能抵抗选择明文攻击(chosen ciphertext attack, CPA)和适应性选择密文攻击(CCA2)的属性基加密(attribute-based encryption, ABE)来保证细粒度的密文数据访问控制,过渡到研究能抵抗私钥共享攻击的可追踪、可撤销、多机构的属性基加密技术.在隐私保护外包计算方面,国内外研究进展逐渐从传统的依赖(全)同态加密技术来实现安全外包聚合、外包计算,过渡到不依赖于(全)同态加密技术实现轻量级的隐私保护外包聚合与外包计算.本文主要针对基于云的物联网系统密文数据访问控制和隐私保护外包计算两方面的国内外最新研究进展进行综述.

1 物联网密文数据访问控制

分布式移动医疗云计算系统已经越来越广泛地被包括欧盟和北美在内的众多国家政府与医疗机构采纳,用于提供高质量且高效的医疗卫生服务.由于人体传感器和病人手持终端设备存储于计算资源受限,因此通常需要将病人个人健康信息外包存储在

云服务器中,属于典型的物联网体结构.只有被授权的医生才能对相应病人的个人健康信息解密,获得相应明文的访问控制权限并给出及时准确的诊疗反馈.在移动医疗社交网络中,个人健康信息(personal health information)经常共享于同一个社交群体,即患有同种疾病的病人间以提供病情交流与精神支持;或共享于多个不同医疗机构的云服务器间以提供高效的医疗会诊服务.然而,同时也带来了一系列安全与隐私保护的巨大挑战,尤其是如何保证隶属于病人极端隐私的个人健康信息在无线信道传输时,免遭包括窃听攻击与篡改攻击在内的各种威胁.

在安全方面,最为重要的是密文医疗数据的访问控制问题,即仅被授权的医生或医疗服务机构才能正确恢复病人的个人健康信息.在实际中,由于未经授权的个人健康信息采集与泄露会给病人带来极大的麻烦,因此病人都非常关注自身个人健康数据的机密性.在分布式移动电子医疗云计算系统中,病人的哪部分个人健康信息应当被分享,且应当分享给哪些医疗服务人员是两个亟待解决的、具有挑战性的安全与隐私保护问题.近年来,在医疗密文数据访问控制方面已有一系列研究成果.Dillema 等人[9]提出了一个基于物理位置的访问控制方案,保证只有在现实世界中与病人同处于某一个地理范围内的医生对其个人健康信息具有访问控制权限.然而,该方案不适用于 E-health 系统中的远程医疗服务需求.为解决该问题,Yu 等人[10]利用属性基加密技术提出了一个无线体域网中的密文医疗数据分布式细粒度访问控制方案 FDAC,只有属性集满足特定访问控制结构的医疗服务人员才能成功解密相应的个人健康信息.

近年来,Li 等人[11]在基于云的电子医疗系统中,利用多权威机构的属性基加密技术,提出了一个以病人为中心的、细粒度的密文医疗数据访问控制方案.但是,该方案仅考虑了单个云服务器用于密文医疗数据外包存储访问控制的情形,并未对 E-health 移动社交网络中,密文医疗数据在多个云服务器间共享时的安全与隐私保护问题给出相应的解决方案.近年来,除了在病人密文医疗数据访问控制方面有一系列研究工作外,利用假名和其他隐私保护技术来构造匿名认证方案也有许多相关成果.Lin 等人[12]在 E-health 系统中,针对全局敌手提出了可同时满足内容隐私与上下文隐私保护的方案 SAGE.Sun 等人[13]利用匿名凭据、伪随机数发生器和基于知识的零知识证明提出了一个 E-health 系统中隐私保护的应急反馈机制.Lu 等人[14]基于零知识证明在匿名 P2P 网络中提出了一个隐私保护的认证方案.然而,零知识证明所需的巨大计算开销使得这些方案无法直接应用于分布式移动电子医疗云计算系统中资源受限的病人终端设备.为了解决该问题,Riedl 等人[15]提出了一个新的假名体系 PIPE 用于 E-health 系统中的隐私保护.Slamanig 等人[16]将医疗数据假名、身份管理、多元数据的模糊处理与匿名认证技术相结合,来抵抗泄露攻击与统计分析攻击;并提出能保证个人健康信息传输与存储匿名性与隐私性的安全机制.Schechter 等人[17]也在动态群中提出了一个匿名认证方案.但是,上述方案均基于公钥基础设施(PKI)提出,需要在线证书机构(CA)的实时参与;且需为每一个群成员生成一个用于加密数据的对称密钥,因此其开销与群大小成线性关系.

需要指出的是,Goyal 等人[18]提出的传统的属性基加密方案就其安全模型而言,仍然是针对“一对一”情形,即一个用户发送方和一个数据接收方(称为“一对一”)的应用场景提出了解决方案.在“一对一”的应用场景中,由于加密数据只能有单一用户解密,因此解密的数据接收方没有动机将自己的私钥共享给其他用户,使得其他用户能够访问原本是其独自享受访问控制权力的机密数据(并且在这种情形下,一旦用户私钥泄露,很容易追踪到泄漏源).然而,在“一对多”的应用场景中(“多对多”、“多对一”情形类推),原本各用户只能访问自己属性集合满足的那些访问结构对应的加密数据,这些用户间存在共享各自私钥的动机,以获得解密最大范围的加密数据,使自身利益最大化.换句话说,在“一对多”的场景下,只考虑“信道”上的敌手显然是不完全的.所以,必须至少考虑可追踪、可撤销或者多机构等的安全模型需求之一才算是关于多方密码学的安全模型[19].然而,仅具有可追踪性的 ABE 方案还未能满足加密数据在“一对多”情形下的加密数据访问控制安全需求.因为,可追踪性并不能消除已泄露私钥造成加密文件非法读取的负面影响,即获得泄露私钥的非法用户仍能使用该私钥,继续享有对未授权加密数据访问能力.更严重的是,一旦用户私钥泄露,得到泄露私钥的用户还可以将该私钥继续泄露给其他用户.在这种私钥多级泄露情形下,现有的具有白盒可追踪能力与黑盒可追踪能力的 ABE 方案,都只能将泄露源定位到最初对该私钥具有合法拥有权的用户.对中间的二级、三级等私钥泄漏源并不具备可追踪性.此外,访问控制结构随时间和外部客观条件的

变化,会发生动态改变与更新,即原来享有对特定加密数据访问能力的用户,随后可能会被撤销.因此,还需要提出具有撤销访问权限能力的 ABE 安全模型、安全方案及其安全性证明[19].

为了解决上述问题,我们团队[20]首次提出了机会存储(opportunistic storage)的概念,给出了基于属性的多级隐私保护模型(attribute-based athorized multi-level privacy-reserving model, AAPM),并在移动医疗云计算系统中提出了一个病人可控的、具有多级隐私保护能力的认证与密文医疗数据访问控制方案(patient self-controllable multi-level privacy-preseving authentication and encrypted medical record access control, PSMPA).合作认证是指病人的个人健康信息由于医疗会诊和研究的目的,在多个医疗服务机构或多个医药研究中心共享.因此,在不同机构中的用户可分为以下 3 种类型:病人直接授权的主治医生、病人间接授权的医生和非授权人员.1)病人直接授权的主治医生不仅能访问病人的个人健康信息,还能获得其真实身份;2)病人间接授权的医生,由于其通常从事于医疗会诊、医药研究和教学等无需知道病人真实身份信息的工作,因此他们只能访问病人的个人健康信息;3)非授权人员无法获得有关病人的任何信息.通过设计一个基于属性的指定验证人签名(attribute-based designated verifier signature, ABDVS),直接授权的医生能获得认证密钥和解密密钥,从而访问病人的个人健康信息和真实身份.同时,他们还能生成与原始 ABDVS 无法区分的副本,用于在间接授权医务人员间共享.

具体地说,通过设计属性基指定验证人签名,直接授权的主治医生能获得如下认证密钥与解密密钥:

$$K_{\mathrm{Decp}}=e(g_1^{q_{\mathrm{R}}(0)},g^b)=e(g,g)^b,$$

$$K_{\mathrm{Dec}}=H_2(K_{\mathrm{Decp}}),$$

并通过下式验证病人的真实身份:

$$H_1(D_{K_{\mathrm{Dec}}}(C)\|K_{\mathrm{Decp}}e(g_1,g_2)^{hc})=H_1(m\|K_{\mathrm{Sig}})=\sigma,$$

其中,$q_{\mathrm{R}}(0)$,$e(\cdot,\cdot)$,$D(\cdot)$,hc,σ,$H_1:\{0,1\}^*\rightarrow\mathbb{Z}_p^*$,$H_2:G_1\rightarrow\{0,1\}^{|K_{\mathrm{Dec}}|}$分别代表访问控制树的根秘密、双线性配对运算、安全对称加密机制、医疗服务机构的私钥、由病人生成的属性基指定验证人签名和密码学 Hash 函数.此外,直接授权的主治医生还能生成以下签名副本:

$$\sigma_{\mathrm{T}}=H_1(m\|K_{\mathrm{Decp}}e(g_1,g_2)^{hc})=H_1(m\|K_{\mathrm{Sig}}).$$

该签名副本与原始签名 σ 具有概率多项式时间不可区分性.因此,病人的真实身份信息能对间接授权的医务人员进行有效保护.无法获得认证密钥与解密密钥的非授权人员不能获得有关病人的任何信息.

为了进一步解决直接授权的主治医生与间接授权的医务人员、非授权人员间的密钥共享攻击,我们团队[21]还首次提出了一个能同时实现可追踪、可撤销功能的多机构属性基加密方案 TR-MABE.在分布式移动医疗云计算系统中的密钥共享攻击是指直接授权的主治医生将其私钥恶意泄露给间接授权人员(如医药研究公司的工作人员),使其非法获得能同时访问病人个人健康信息及其真实身份的权利,从而得知病人身份与其所患疾病之间的对应关系,进行有效的针对性广告推送等业务.直接授权的主治医生从中获利,而病人的身份隐私遭到暴露.

具体地说,多权威机构表现在各中央权威机构 CA_i 根据其管辖的授权医生身份,为其生成相应的身份公钥 $pcpk_{gid,i}=(gid,L_{gid,i},L'_{gid,i},\{\Gamma_{gid,k,i}\},\sigma_{gid,i})$ 和私钥($pcsk_{gid,i}$, $pcsk'_{gid,i}$).各属性权威机构 AA_i 根据授权医生的属性集合 AS_{gid},利用其身份公钥为其生成相应的属性私钥 $pask_{gid,i}=\{pask_{att,gid,i}\mid att\in AS_{gid}\}$.

为了实现可追踪性,我们团队[21]首先提出了一个具有可追踪功能的多权威机构属性基加密方案 PT-MABE.在各中央权利机构 CA_i 为授权医生生成身份私钥时,在表 T_i 中存储如下元组(c_i, gid),在追踪阶段,如果被泄露的私钥通过合法性检验,便能从表 T_i 中搜索到对应泄露私钥的直接授权医生身份 gid.

此外,我们团队[21]还通过存储撤销技术,在所构造方案 PT-MABE 的基础上对非法获得病人个人健康信息或真实身份访问控制权限的间接授权医生和非授权人员的私钥进行撤销;从而构造最终的方案 TR-MABE,极大地降低了病人隐私遭到泄露的风险.其主要思想描述如下:

1) 在加密阶段,对访问控制树中的每一个节点 $y\in\tau_t$,计算:

$$C_y^{(A,\rho),cgy}=PT-MABE.Encrypt(GPAR,$$

$$CAPAR_i,AAPAR_k,K_{cgy},(A,\rho)\vee(B_y,\theta_y)),$$

其中,$cgy\in\{id,data\}$,$(A,\rho)\vee(B_y,\theta_y)$是更新后的访问控制结构.在中央权威机构密钥更新阶段,CA_i 为 $u\in U(rl)$的各节点计算

$$(pcsk^1_{u,s_t,i},pcpk^1_{u,s_t,i})=PT-MABE.CAKeyGen(u,$$

$$GPAR,AAPK_k,CAMSK,\tau=1),$$

其中,$s_t=\{w_{i,t[i]}:i\in\{1,2,\cdots,r\}\}$,$rl$ 是不能访问病人真实身份的间接授权医生撤销列表.在属性权威机构密钥更新阶段,AA_i 根据中央权威机构密钥更新阶段的输出($pcsk^1_{u,s_t,i}$, $pcpk^1_{u,s_t,i}$)和授权医生的属性集合 AS_{gid} 更新其属性私钥:

$$pask^1_{t,i}=\{pask^1_{u,s_t,i}:u\in U(rl)\}.$$

2) 在解密阶段,如果 $t'\geqslant t$,每个 $gid\notin rl$ 的直接授权主治医生可以正确解密:

$$K_{cgy}=PT-MABE.Decrypt(pcsk^0_{u,i},pcpk^0_{u,i},$$
$$pask^0_{u,i},pcsk^1_{u,s_{t'},i},pcpk^1_{u,s_{t'},i},pask^1_{u,s_{t'},i},C_y^{A,\rho}),$$

从而进一步解密病人的密文健康信息和真实身份信息.

$$ID_{\text{pat}}=D_{K_{id}}(CT_{ID_{\text{pat}}}),\ m_{\text{pat}}=D_{K_{\text{data}}}(CT_{m_{\text{pat}}}).$$

3) 在密文更新阶段,云服务器在 $t'=t+1$ 时间段计算:

$$C_u^{(A,\rho),id}=PT-MABE.Delegate(GPAR,CAPAR_i,$$
$$AAPAR_k,C_y^{(A,\rho),id},(A,\rho)\vee(B_u,\beta_u)),$$

并将 $C_{t+1}^{(A,\rho),id}=\{C_u^{(A,\rho),id}:u\in\tau_{t+1}\}$ 返回给医生.

2 物联网隐私保护外包计算

由于物联网节点存储、计算资源受限,通常会将计算复杂度较大的运算外包给半可信或恶意的云服务器完成.主要的安全与隐私保护要求如下:

1) 数据隐私.单个数据的内容要对云服务器和数据接收方及其合谋实现隐私保护;

2) 计算隐私.外包数据聚合或外包计算的结果要对云服务器实现隐私保护,仅被授权的数据接收方能利用其私钥对运算结果进行成功解密,获得相应的访问控制权限;

3) 可验证性.当云服务器工作在恶意安全性模型时,数据接收方能成功验证外包计算结果的正确性,即验证云服务器是否严格执行协议规程并返回相应的外包计算结果;

4) 高效性.设计轻量级的隐私保护外包计算协议,使其存储、计算和通信负担适用于物联网存储、计算开销受限的用户端设备.尤其是,用于计算结果正确性验证的计算开销要求小于用户自己进行数据聚合或外包计算的计算开销.

由于物联网设备资源受限,复杂而频繁的数据采集与信息统计分析工作无法仅依靠本地设备完成.因此考虑如何在资源非对称分布的环境下设计安全与隐私保护的外包数据聚合、外包计算也是近年来国内外学者研究的焦点[22-29].全同态加密实现了在密文数据上同时进行加法与乘法操作的功能,从而满足安全外包聚合与外包计算的功能需求.Gentry等人[30]通过设计可重随机化的 Yao's circuit 提出了一个全同态加密和 i-hop 加密方案.Dijk 等人[31]提出了一个基于整数环的全同态加密方案,其中设计了一个仅需基本模(加法和乘法)运算实现的部分同态加密,并结合 Gentry 的技术[32]设计了一个高效的全同态加密方案.但是,Lauter 等人[33]指出即便在为了提高运算效率牺牲一定数量乘法运算的前提下,全同态加密的计算复杂度对物联网设备而言仍然太大而显得不实际.另一方面,随之而来的是无线体域网中隐私保护外包计算的可验证性问题,即要求云服务器向用户证明外包计算结果的正确性.其中一个合理性条件是,用户用于验证的计算复杂性必须小于用户自身计算该目标函数本身.在可验证函数加密方面有一系列研究进展.Gennaro 等人[34]首次提出可验证外包计算的概念,允许计算资源受限的设备将计算复杂性较高的计算外包给远端的半可信或恶意云服务器完成.其次,利用 Yao's garbled circuit 技术和全同态加密技术提出了第 1 个可验证外包计算方案;然而每次验证失败时都要求系统重新初始化.为了提高效率,还提出了一个改进的可验证外包计算方案,每次外包计算的输入由预先设定的输入和本次更新的输入两部分组成.由于预设输入对特定函数运算结果的正确性可预先验证,因此函数计算结果正确性亦能以增量验证的方式进行.从而避免了每次验证失败,都需要维护用户与云服务器间的共享状态来对系统进行初始化的额外负担.近年来,Barbosa 等人[35]以模块化的方式,利用全同态加密技术、函数加密技术和消息认证码技术提出了一个可验证的函数加密方案与可代理的同态加密方案.然而,上述可验证外包计算方案均基于公钥全同态加密技术来实现,其巨大的计算开销无法满足资源受限的物联网设备的性能需求.更重要的是,直接将公钥全同态加密应用于数据本身,违背了混合加密体制中用公钥加密算法来加密较短的对称密钥,用对称密钥来加密较大的数据这一基本原则.最近,我们团队[36]避开全同态公钥加密和零知识证明技术,利用任意单向陷门函数提出了高效的基于单用户时间序列隐私保护数据聚合方案 PPDA,仅需执行一次单向陷门函数运算便能实现对多个数据的隐私保护聚合.该方案的主要工作流程如下:

1) 离线阶段,用任意公钥加密算法作会话密钥协商;

2) 在线阶段,用生成的会话密钥通过简单的加法或乘法运算对数据进行加密;

3) 存储与计算资源充足的第三方在加密域上实现隐私保护的数据聚合;

4) 拥有公钥加密算法对应私钥的授权用户可成功解密聚合结果.

具体而言,首先单向陷门函数 f 作用于随机数 $r\in\mathbb{R}$,其中 $\mathbb{R}$ 是除环.此后,r 用于加密数据拥有者的单个消息 m_i,$i=1,2,\cdots,n$.为了实现单个消息的信息论安全,随机选择加法盲化因子 $r_i\in\mathbb{R}$ ($i=1,2,\cdots,n$)来进一步对单个消息 m_i 进行随机化:

$$C_1=f(r),\ C_{2,i}=m_ir+r_i.$$

当收到来自数据拥有者的加密消息 $C_{2,i}$($i=1,2,\cdots,n$),云服务器执行如下加密域上的聚合操作:

$$C_{\text{add}}=\sum_{i=1}^{n}C_{2,i}=m_{\text{add}}r+r_{\text{add}},$$

其中 $m_{\text{add}}=\sum_{i=1}^{n}m_i$,公开 $r_{\text{add}}=\sum_{i=1}^{n}r_i$,并将聚合结果返回给数据接收方.只有被授权的数据接收方,才能利用单向陷门函数 f 的私钥从密文 C_1 中解密对称加密密钥 r,从而进一步解密聚合结果 m_{add}.为了实现聚合隐私的适应性选择密文安全性,在加密与聚合算法中添加认证项 $C_{\text{ram}}=H_0(r\|r_{\text{add}})$ 和 $C_3=H_1(C_{\text{add}}\|C_{\text{ram}})$,其中 $H_0,H_1:\{0,1\}^*\to\mathbb{R}$ 是密码学 Hash 函数.

单向陷门函数 f 可以根据不同网络环境中特定的安全与隐私保护需求,用公钥加密、身份基加密和属性基加密分别对其进行实例化.尤其需要指出的是,数据接收方与数据拥有者为同一实体的情形是上述一般性构造的特殊形式:为实现此类自外包的隐私保护数据聚合,可以省略密文中的第一项 C_1,仅要求物联网设备秘密保存加密数据的对称密钥 r 用于正确解密聚合结果即可.数据拥有者的个体数据 m_i 的数据隐私可对云服务器和数据接收方完美保护,因为其被对称加密密钥 r 和随机数 r_i 双重盲化.云服务器无法获得 m_i,因为其不具备单向陷门函数的私钥 SK_f 用于解密对称加密密钥 r,也无法获得有关随机盲化因子 r_i 的任何知识;而即便是被授权的数据接收方也只能正确解密 r,无法恢复 r_i.因此,单个数据的隐私具有无条件安全性.聚合隐私建立在一个 CCA2 安全的加密方案基础上,其安全性可归约到单向陷门函数求逆的计算困难性问题上.

性能分析主要从计算开销和通信开销两方面,将所构造方案 PPDA[36] 与利用 Paillier 加法同态加密机制的隐私保护数据聚合方案[37-39] 进行比较.在利用 Paillier 加法同态加密机制实现隐私保护聚合的方案中,为了加密单个数据,要求物联网设备进行群 $\mathbb{Z}_{N^2}$ 中的 2 次模幂运算和 1 次乘法运算.因此,对 n 个数据的隐私保护聚合,要求数据拥有者的物联网设备进行 $2n$ 次相应的模幂运算和 n 次乘法运算.另一方面,如果我们用 RSA 算法实例化所构造聚合方案 PPDA 中的单向陷门函数 f,对 n 个数据实现隐私保护聚合,仅要求数据拥有者的物联网设备进行 1 次单向陷门函数运算(即 1 次群 $\mathbb{Z}_N$ 中的模幂运算)和 n 次群 $\mathbb{Z}_N$ 中的乘法运算即可.对云服务器而言,在 Paillier 加法同态加密隐私保护数据聚合方案中需要进行群 $\mathbb{Z}_{N^2}$ 中的 n 次乘法运算,在所构造方案 PPDA[36] 中需要进行群 $\mathbb{Z}_N$ 中的 n 次加法运算,因此与前者相比,PPDA[36] 的计算开销可以忽略.通信开销方面,在利用 Paillier 加法同态加密的数据聚合[37-39] 与所构造方案 PPDA[36] 中分别要求传输群 $\mathbb{Z}_{N^2}$ 中的 n 个元素和群 $\mathbb{Z}_N$ 中的 $n+1$ 个元素.对云服务器而言,分别要求传输群 $\mathbb{Z}_{N^2}$ 中的 1 个元素和群 $\mathbb{Z}_N$ 中的 2 个元素.

我们在 Linux 平台下利用 2.93 GHz 处理器,调用 PBC[40] 和 Miracle[41] 数据库来研究所构造方案的开销.实验表明,一个群 $\mathbb{Z}_{N^2}$($|N|=1024$)中的模幂运算和乘法运算分别需要 12.6 ms 和 10.4 ms.相应的运算在群 $\mathbb{Z}_N$ 中需要 8.7 ms 和 6.8 ms.如图 1 所示,随着单个数据数目的增长,基于 Paillier 加法同态加密的聚合方案[37-39] 的计算开销明显高于所构造方案 PPDA[36],因为 PPDA 只需要进行一次单向陷门函数计算就能实现对 n 个数据的隐私保护聚合.此外,PPDA[36] 中云服务器的计算开销与现有方案相比也几乎可忽略.如图 2 所示,现有方案[37-39] 中的物联网设备通信开销也大大高于所构造方案 PPDA[36],云服务器的通信开销与现有方案[37-39] 相当.

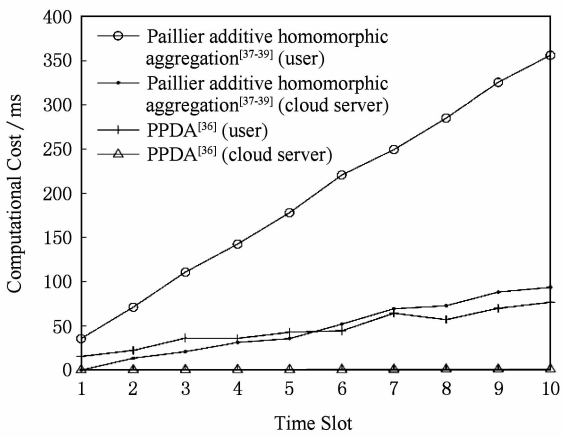

Fig. 1 Computational cost comparion between Paillier's additive homomorphic aggregation and PPDA.

图 1 基于 Paillier 加法同态加密的聚合方案与 PPDA 计算开销比较

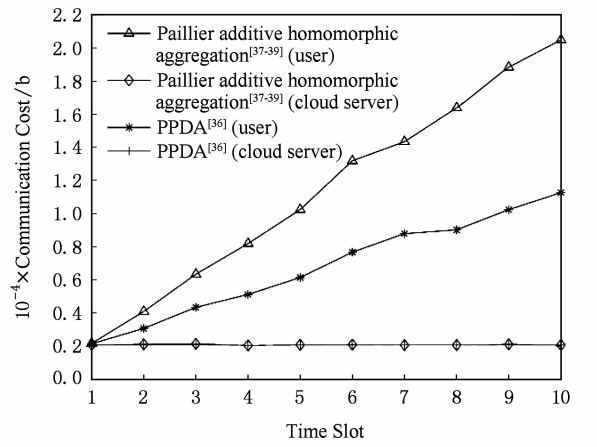

Fig. 2 Communication cost comparion between Paillier's additive homomorphic aggregation and PPDA.

图 2 基于 Paillier 加法同态加密的聚合方案与 PPDA 计算开销比较

2.1 智能电网中的隐私保护数据聚合

国内外大量的研究工作[37-38,42-44]致力于智能电网中隐私保护的数据聚合与动态计费问题. Lu 等人[37]在智能电网通信中提出了一个隐私保护的数据聚合方案 EPPA. 该方案利用超递增向量和 Paillier 同态加密技术对多维数据进行密文聚合. 但是,为验证 n 个加密用电量,即使在采用批量验证技术的前提下,仍需要进行 $n+1$ 次配对运算和 $n-1$ 次模乘运算. 因此,该方案的计算负担随用户数量与用电量采集频率的增加迅速递增,不能满足智能电网中设计轻量的隐私保护数据聚合协议的基本要求. 最近,Erkin 等人[38]利用 Paillier 同态加密技术提出了一个基于时间和空间特性的、隐私保护用电数据聚合方案. Liang 等人[42]提出了一个智能电网中基于实时用电量的、隐私保护的动态计费方案. 该方案在利用全同态加密技术保护用户实时用电量隐私的前提下,以用户个人用电量与用户所在地区用电量为标准来实现动态峰谷计费. 然而,上述国内外现有工作[37-38,42]均利用全同态加密技术作用于每一个实时用电数据,以实现隐私保护的数据聚合,计算开销大,不适于存储、计算及通信资源受限的 smart meters. 为了解决该问题,我们团队[43]在智能电网中,提出了一个高效的隐私保护数据聚合方案. 在该方案中,作者进一步弱化了单向陷门函数的条件,基于两类特殊的单向函数,即满足 $f(x)^y=f(y)^x$ 特性的或切比雪夫多项式函数构造隐私保护数据聚合方案;使得被授权数据接收方,即便不知道相应单向陷门函数的私钥,也可以与数据拥有者协商数据对称加密密钥,从而正确解密聚合结果.

下面我们以第 1 类利用具有 $f(x)^y=f(y)^x$ 性质的单向函数构造隐私保护数据聚合方案为例,来简要介绍其主要思路如下:在加密阶段,每一个用户随机选择 $t,r_i\in_R\mathbb{Z}_p^*$,且计算

$$C_1=f(t),\ s=PK_R^t,\ C_{2,i}=m_{U,i}s+r_i,$$

其中,$m_{U,i}(i=1,2,\cdots,n)$是用户 U 在时间段 t_i 中的实时用电量,$PK_R=f(r)$,$SK_R=r$ 是计费中心的公私钥对. 当 1 个包含 n 个时间段的时间周期 T 结束后,用户 U 公开 $r_T=\sum_{i=1}^{n}r_i$ 并发送 $C_{U,i}=(C_1,C_{2,i})$ 给通信网关. 在聚合阶段,通信网关在密文域上进行聚合运算:

$$C_T=\sum_{i=1}^{n}C_{2,i}=(\sum_{i=1}^{n}m_{U,i})s+\sum_{i=1}^{n}r_i=m_Ts+r_T,$$

其中 $m_T=\sum_{i=1}^{n}m_{U,i}$,并将 $C_A=(C_1,C_T)$ 发送给计费中心. 在解密阶段,计费中心计算并恢复用户在时间周期 T 内的用电量总和:

$$s=C_1^{SK_R},\ m_T=(C_T-r_T)s^{-1}.$$

第 2 类利用切比雪夫多项式构造隐私保护数据聚合方案与第 1 类隐私保护数据聚合方案大致相同,只要在加密阶段进行替换 $C_1=T_t(g)$,$s=T_t(PK_R)$,在解密阶段替换 $s=T_m(C_1)$即可. 该方案的安全性可归约到单向函数求逆的困难性假设.

2.2 无线体域网中的隐私保护密钥协商

在无线体域网的隐私保护方面,国内外研究工作[45-48]多集中在密文医疗数据的访问控制和安全与隐私保护的认证密钥交换协议等方面,后者是前者的基础. Cherukuri 等人[49]首次在无线体域网中,提出基于生物特征的密钥协商协议. 2 个部署于同一人体不同部位的传感器节点对同一生命体征采集到的数据在一定范围内存在误差. 利用 Reed-Solomon 纠错编码技术构造共享密钥机制. 随后,Bao 等人[50]利用脉搏间隙(inter-pulse-interval),基于部署于同一病人不同位置的传感器对同一生命体征采集数据的汉明距离远小于部署于不同病人身体上的传感器对该生命体征采集数据的汉明距离这一观察,构造无线体域网中的会话密钥协商协议. Fuzzy vault 技术[51]被广泛采用,设计无线体域网中的密钥协商协议. 由某一人体传感器节点引入盲化点集合,来混淆从病人人体采集的真实生命体征数据,从而构造

Vault. 另一传感器节点能成功与其建立对密钥，当且仅当该 Vault 与其自身对同一生命体征采集到的数据集的交集的大小满足系统预设的门限值. 然而，Venkatasubramanian 等人[52]在指出 IPI 信号由于其在不同人体间的低差分性不适宜用作无线体域网对密钥建立的同时，提出了一个基于生理信号 PPG 和 ECG 的认证密钥协商协议. OPFKA[53]基于某些特定的生物特征(如：ECG 信号)是有序排列的且只有采集该信号的传感器才能正确识别该序列这一事实，提出了无线体域网中有序生物特征的密钥协商协议. 上述两个方案均利用 Fuzzy vault 技术实现.

然而，Fuzzy vault 技术将无线体域网中的对密钥协商协议陷入两难境地：一方面，通过引入更多的盲化点使 vault 变大，从而增加敌手正确区分真实生物特征采集点与盲化点的难度；但另一方面，由于真实生物特征采集点与盲化点间的碰撞也随之增加，于是在对密钥建立阶段，错误接收率也随之增加，即两个原本生物特征点交集大小没有达到预定门限值的人体传感器节点间也会因为盲化节点与真实点间的碰撞，而错误地建立对密钥. 因此，如何在无线体域网中设计一个安全、高效的，基于生物特征的确定性密钥协商协议是一个亟待解决又极具挑战的公开问题. 我们团队[54]在无线体域网中，提出了一个基于生物特征的、高效的隐私保护确定性密钥协商方案 BDK. 该方案克服了 Fuzzy vault 技术为提高安全性而带来的效率低下问题，并实现了对隶属于对密钥建立双方的生物特征序列实现有效隐私保护. 假定人体传感器节点 A 和 B 具有的生物特征序列为 $\boldsymbol{a}=(a_1,a_2,\cdots,a_n)$ 和 $\boldsymbol{b}=(b_1,b_2,\cdots,b_n)$，其主要思路描述如下.

首先，传感器节点 B 随机选择 $R_B\in_R\mathbb{F}_p$，计算：

$$\boldsymbol{b}^{\mathrm{bld}}=(b_1+R_B,b_2+R_B^2,\cdots,b_n+R_B^n),$$

$$B_0=MAC(ID_B\|ID_A\|\boldsymbol{b}^{\mathrm{bld}})=$$

$$MAC(ID_B\|ID_A\|b_1+R_B\|b_2+R_B^2\|\cdots\|b_n+R_B^n),$$

其中，MAC 是消息认证码. 并将$(ID_B,ID_A,\boldsymbol{b}^{\mathrm{bld}},B_0,N_0)$发送给传感器节点 A，其中 $N_0\in_R\mathbb{F}_P$是为保持消息新鲜性而添加的随机数. 传感器节点 A 随机选择 $R_A\in_R\mathbb{F}_p$，并计算：

$$\boldsymbol{a}^{\mathrm{bld}}=(R_A(b_1^{\mathrm{bld}}-a_1),R_A^2(b_2^{\mathrm{bld}}-a_2),\cdots,$$

$$R_A^n(b_n^{\mathrm{bld}}-a_n)),$$

$$A_0=MAC(ID_A\|ID_B\|\boldsymbol{a}^{\mathrm{bld}})=$$

$$MAC(ID_A\|ID_B\|R_A(b_1^{\mathrm{bld}}-a_1)\|$$

$$R_A^2(b_2^{\mathrm{bld}}-a_2)\|\cdots\|R_A^n(b_n^{\mathrm{bld}}-a_n)),$$

并将$(ID_A,ID_B,\boldsymbol{a}^{\mathrm{bld}},A_0)$发送给传感器节点 B. 最后，传感器节点 B 计算：

$$R_{A,i}=a_i^{\mathrm{bld}}/R_B^i.$$

在生物特征匹配与对密钥生成阶段，如果$\{R_{A,i}\}$满足$\{R_A,R_A^2,\cdots,R_A^{n'}\}$特征且$|\{R_{A,i}\}|\geqslant k$($k$是门限值)，则人体传感器节点 A 和 B 可以成功建立对密钥 $K_{AB}=K_{BA}=H_1(a_1\|a_2\|\cdots\|a_{n'})=H_1(b_1\|b_2\|\cdots\|b_{n'})$. 其中，与集合$\{R_{A,i}\}$中元素对应的生物特征即为传感器节点 A 和 B 的公有生物特征.

该方案的安全性可归约到单向陷门函数求逆的困难性假设. 下面对所构造方案 BDK 的性能作简要分析和比较. 为比较存储开销，假定 ID_B 和 ID_A 分别需要 16 B. 在现有方案 PSKA[52]和 OPFKA[53]中，生物特征点和盲化点分别需要 20 b. 索引需要 1 B. 随机数 N_0 和消息认证码 MAC 分别需要16 B. 因此，所构造方案 BDK 中的传感器节点存储开销为

$$STCOST=2(|ID_B|+|ID_A|)+2.5|M|+$$

$$|Index|+|N_0|+2|MAC|,$$

其中，$|M|$代表生物特征序列的长度. 图 3 表明了所构造方案 BDK 与现有方案 PSKA[52]和 OPFKA[53]的存储开销比较. 观察发现，为传输相同数目的生物特征用户在人体传感器间建立对密钥，方案 BDK[54]的存储开销大大降低，且随着生物特征数目的增长，该种优势表现得越为明显.

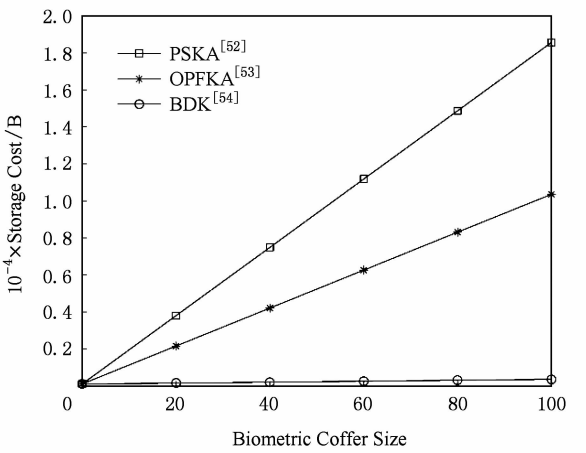

Fig. 3 Storage cost comparison among PSKA[52], OPFKA[53] and BDK[54].

图 3 方案 PSKA[52]，OPFKA[53]和 BDK[54]存储开销比较

在实现相同的安全性要求下，图 4 表明了所构造方案 BDK[54]与现有方案 PSKA[52]和 OPFKA[53]的计算开销比较. 如图 4 所示，方案 PSKA[52]的计算开销随着 Fuzzy vault 的增大而降低. 因为为了达到

相同的安全性,要求在传感器节点间共享更多的生物特征,即在 Fuzzy vault 较小时,要求选择更高次的多项式插值来计算对密钥.在具有相同个数 T_s 的共享生物特征前提下,方案 BDK[54] 的计算开销大为降低,因为其建立对密钥仅需进行 $\mathbb{F}_p$ 上的 T_s-1 个模幂运算和 T_s 个乘法运算即可.此外,与现有方案 PSKA[52] 和 OPFKA[53] 相比,所构造方案 BDK 的错误拒绝率也大大降低,因为确定性对密钥建立方案 BDK[54] 无需引入盲化点集合来保证安全性,在盲化点与真实生物特征点间的碰撞将大为降低.图 5 表明了方案 BDK[54] 与方案 PSKA[52]、方案 OPFKA[53] 间的错误拒绝率比较.

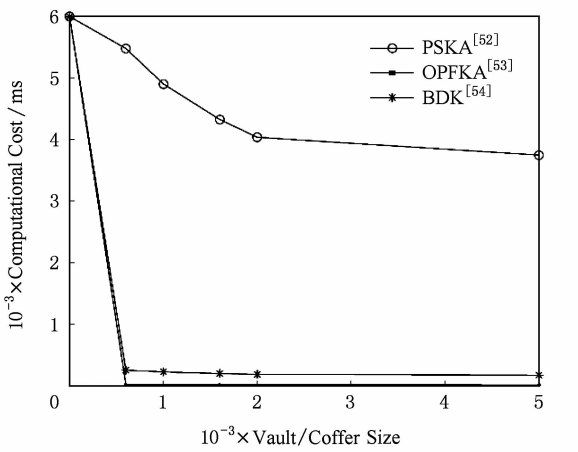

Fig. 4 Computational cost comparison among PSKA[52], OPFKA[53] and BDK[54].

图 4 方案 PSKA[52],OPFKA[53] 和 BDK[54] 计算开销比较

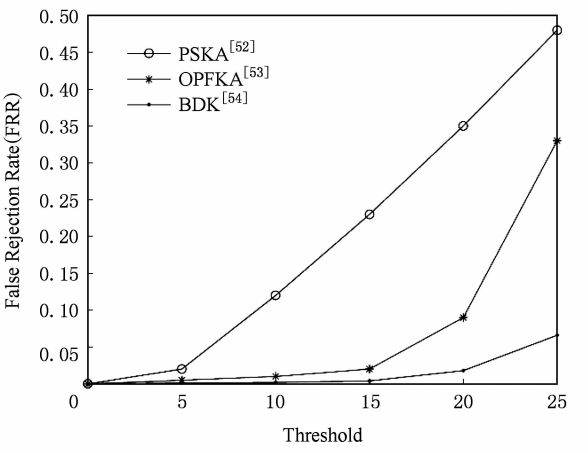

Fig. 5 FRR comparison among PSKA[52], OPFKA[53] and BDK[54].

图 5 方案 PSKA[52],OPFKA[53] 和 BDK[54] 错误拒绝率比较

2.3 无线车载网中的隐私保护数据包传输

国内外大量研究工作[55-60] 致力于车载网络 VANETs 中高效的、隐私保护数据包发送问题.利用传统的基于 PKI 的数字签名技术和群签名技术,可以解决上述问题,但由于签名验证方除验证签名本身外,还需要验证签名方的公钥证书,因此计算、通信开销会随着车载网络中消息数目的增加迅速增大,不适用于资源受限的车载通信设备.Lin 等人[55] 基于 TESLA 提出了一个安全高效的车载通信方案 TSVC.该方案利用消息认证码 MAC 和 Hash 链技术实现对车

载广播消息的快速认证.但为抵抗重放攻击,用户认证的 MAC 密钥释放需要有 β 时间延迟,且该延迟量要求大于消息的传输延迟.因此,该方案不适用于无法预期且需要及时对广播消息验证的紧急情形,如:交通事故与公路犯罪等.另一方面,在公路紧急时间发生的地点,往往有众多车辆聚集,广播消息的数量急剧增加导致消息的传播延迟也随之增加;因此 MAC 密钥释放延迟也要求随之增加,进一步导致无法及时验证紧急情况的广播消息.Zhang 等人[56] 提出了一个基于 RSU 的车载网络消息认证方案 RAISE.Lin 等人[57] 提出了一个车载网络中的消息合作认证方案.该方案分别在车载用户完全合作与自私的前提下,允许用户车载设备可依据剩余资源量对消息进行部分认证,并在一定范围内广播认证结果,从而实现合作认证的目的.然而,该方案并未减少车载网络中广播消息的数目,导致车载设备的通信负担大;其次,系统需要维护一个为用户生成令牌的在线 TA,开销也很大.Lu 等人[58] 在基于车载网络的位置服务中,提出了一个动态隐私保护的密钥管理方案.该方案在车辆动态加入或离开群组时保证前向安全与后向安全.然而,不同于传统网络,车载网络中的车辆由于行驶速度、方向等具有不稳定性和不可预测性,频繁地密钥更新会带来较大的计算和通信开销.之后,Lu 等人[59] 又在车载 DTN 网络中提出了一个高效的、隐私保护数据包过滤发送方案.通过数据包的接收方为其好友设置消息喜好策略,有效避免了垃圾包的传递.最近,我们团队[60] 基于改进的生物种群竞争模型提出了一个基于信誉的门限数据包合作传递激励机制 TCBI,并在此基础上通过外包计算聚合传输证据,提出了能有效抵抗夹层合谋攻击的安全数据包传输协议,为设计无线车载网中隐私保护的冗余消息过滤机制,实现高效数据包认证技术开辟了新的思路.其主要思路描述如下:

假定在时间 TS_S 时刻,从位置 L_S 向 L_1 移动的车载簇 c 中存在 $N_{S,1}^{c,TS_S}$ 个车辆.且沿途共有 $N_{S,1}$ 个路测单元 RSU.每个路测单元 RSU l 随机选择 r_l, $r_{i,l}\in_R\mathbb{F}_p$,并计算

$$C_{l,1}=f(r_l),\ C_{2,i}=V_{L_S\to L_1,TS_S}^{i,l}r_l+r_{i,l},$$

其中,f 是单向陷门函数.假定共有 N_{cf} 个分布式云服务器.RSU l 分别将 $n_k(k=1,2,\cdots,N_{cf})$ 个车辆速度的密文数据发送给车载云服务器 k,满足 $N_{S,1}^{c,TS_S}=\sum_{k=1}^{N_{cf}}n_k$.然后,RSU l 公开 $r_{l,k,T}=\sum_{i=1}^{n_k}r_{i,l}$,计算 $C_{k,\text{ram}}=H_4(r_l\|r_{l,k,T})$,并将 $C_{i,l,k}=(ID_l,ID_k,C_{l,1},C_{2,i},C_{k,\text{ram}})$,发送给车载云服务器 k,其中 $i=1,2,\cdots,n_k$.

车载云服务器 k 计算

$$C_{l,k,T}=\sum_{i=1}^{n_k}C_{2,i}=m_{l,k,T}r_l+r_{l,k,T},$$

$$C_{3,k}=H_5(C_{l,k,T}\|C_{k,\text{ram}}),$$

并将 $C_{l,k,\text{Agg}}=(ID_k,ID_{\text{TM}},C_{l,1},C_{l,k,T},C_{k,\text{ram}},C_{3,k})$ 发送给交通管理部门(traffic mangement, TM).

TM 执行如下解密操作:计算车载簇 c 中的平均速度,并生成聚合传输证据.如果 $C_{k,\text{ram}}=H_4(r_l\|r_{l,k,T})$ 和 $C_{3,k}=H_5(C_{l,k,T}\|C_{k,\text{ram}})$ 验证通过,则计算:

$$r_l=f^{-1}(C_{l,1}),V_{l,T}=\left(\sum_{k=1}^{N_{cf}}C_{l,k,T}-\sum_{k=1}^{N_{cf}}r_{l,kT}\right)r_l^{-1},$$

否则,中止协议运行.其中,$V_{l,T}$ 是计算车辆数据包聚合传输证据,有效抵抗夹层合谋攻击的关键因素.

该方案的安全性可归约到单向陷门函数求逆的困难性假设.图 6 和图 7 表明了其与利用 Paillier 加法同态加密机制的方案 SMART[61] 相比的计算开销与通信开销优势.

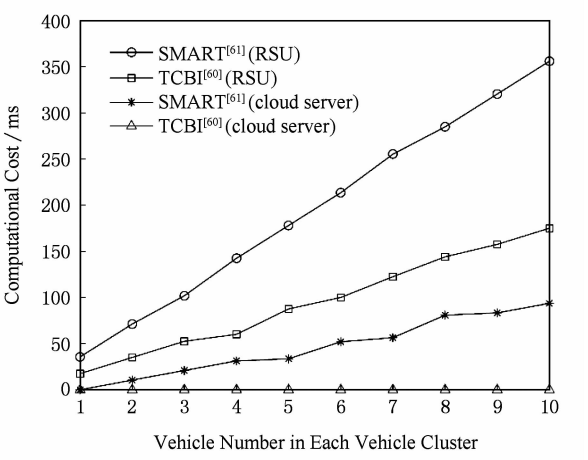

Fig. 6 Computational cost comparison between SMART[61] and TCBI[60].

图 6 方案 SMART[61] 和 TCBI[60] 计算开销比较

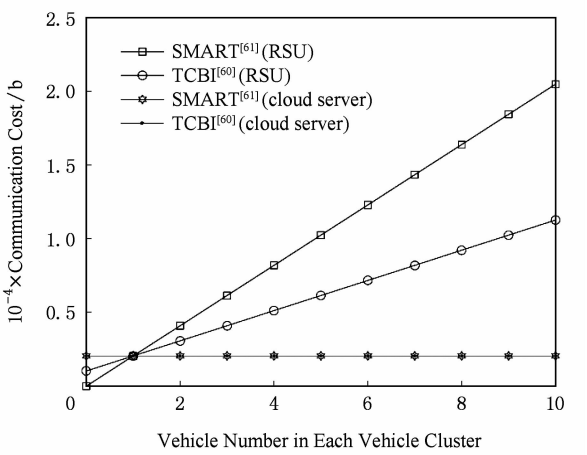

Fig. 7 Communication cost comparison between SMART[61] and TCBI[60].

图 7 方案 SMART[61] 和 TCBI[60] 通信开销比较

3 结束语

本文主要从物联网密文数据访问控制和隐私保护外包计算 2 方面展开,对物联网的隐私保护国内外研究进展进行综述.对物联网(以电子医疗为例)具有多级隐私保护能力的密文数据访问控制,同时具有可追踪、可撤销能力的多机构属性基加密方案,以及物联网中高效的隐私保护外包聚合方案及其在智能电网隐私保护计费、无线体域网隐私保护对密钥建立和无线车载网的隐私保护数据包聚合传输证据生成等方面的应用,给出了其主要研究思路和研究方法.试图让读者理解各种方法的优劣和适用的场景,为进一步从事物联网隐私保护的研究提供新的思路.

参 考 文 献

[1] Li X, Lu R, Liang X, et al. Smart Community: An Internet of Things Application [J]. IEEE Communications Magzine, 2011, 49(11): 68-75

[2] Cao Zhenfu. New Directions of Modern Cryptography [M]. Boca Raton, FL: CRC Press Inc, 2012: 1-400

[3] Mershad K, Artail H, A framework for secure and efficient data acquisition in vehicular ad hoc networks [J]. IEEE Trans on Vehicular Technology, 2013,62(2), 536-551

[4] Dong Xiaolei, Wei L, Zhu H, et al. An efficient privacy-preserving data-forwarding scheme for service-oriented vehicular Ad Hoc networks [J]. IEEE Trans on Vehicular Technology, 2011, 60(2): 580-591

[5] Mershad K, Artail H. A framework for secure and efficient data acquisition in vehicular ad hoc networks [J]. IEEE Trans on Vehicular Technology, 2013, 62(2): 536-551

[6] Jinila Y B, Komathy K. A privacy preserving authentication framework for safety messages in VANET [C] //Proc of SEISCON 2013. Berlin: IET, 2013: 456-461

[7] Guo P, Wang J, Zhu J Z, et al. Intrusion tolerant-based lightweight CA model for wireless mesh networks [J]. International Journal of Multimedia and Ubiquitous Engineering, 2013, 8(6): 19-30

[8] Song Jun, He Chunjiao, Zhang Lei, et al. Toward an RSU-unavailable lightweight certificateless key agreement scheme for VANETs [J]. Communications China, 2014,11(9): 93-103

[9] Dillema F W, Lupetti S. Rendezvous-based Access Control for Medical Records in the Pre-hospital Environment [C] // Proc of HealthNet. New York: ACM, 2007: 1-6

[10] Yu S, Ren K, Lou W. FDAC: Toward fine-grained distributed data access control in wireless sensor networks [C] //Proc of IEEE INFOCOM 2009. Piscataway, NJ: IEEE, 2009: 963-971

[11] Li J, Au M H, Susilo W, et al. Attribute-based signature and its applications [C] //Proc of ASIACCS'10. New York: ACM, 2010: 60-69

[12] Lin X, Lu R, Shen X, et al. SAGE: A strong privacy-preserving scheme against global eavesdropping for ehealth systems [J]. IEEE Journal on Selected Areas in Communications, 2009, 27(4): 365-378

[13] Sun J, Zhu X, Zhang C, et al. HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare [C] //Proc of ICDCS'11. Piscataway, NJ: IEEE, 2011: 373-382

[14] Lu L, Han J, Liu Y, et al. Pseudo trust: Zero-knowledge authentication in anonymous P2Ps [J]. IEEE Trans on Parallel and Distributed Systems, 2008,19(10): 1325-1337

[15] Riedl B, Grascher V, Neubauer T. A secure e-health architecture based on the appliance of pseudonymization [J]. Journal of Software, 2008, 3(2): 23-32

[16] Slamanig D, Stingl C. Privacy aspects of e-health [C] //Proc of the 3rd Int Conf on Availability, Reliability and Security. New York: ACM, 2008: 1226-1233

[17] Schechter S, Parnell T, Hartemink A. Anonymous authentication of membership in dynamic groups [C] //Proc of the 3rd Int Conf on Financial Cryptography. Berlin: Springer, 1999: 184-195

[18] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data [C] //Proc of the ACM Conf on Computer and Communications Security. New York: ACM, 2006: 89-98

[19] Cao Zhenfu. New development of cryptography [J]. Journal of Sichuan University (Engineering Science Edition), 2015, 47(1): 1-12 (in Chinese)
(曹珍富. 密码学的新发展[J]. 四川大学学报(工程科学版), 2015, 47(1): 1-12)

[20] Zhou J, Lin X, Dong X, et al. PSMPA: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributed m-Healthcare cloud computing system [J]. IEEE Trans on Parallel and Distributed Systems, 2015,26(6): 1693-1703

[21] Zhou J, Cao Z, Dong X, et al. TR-MABE: White-Box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-Healthcare cloud computing systems [C] //Proc of IEEE INFOCOM 2015. Pistacaway, NJ: IEEE, 2015: 2398-2406

[22] Lu R, Lin X, Liang X, et al. A secure handshake scheme with symptoms-matching for m-healthcare social network [OL]. [2015-07-20]. http://dx. doi. org/10. 1007/s11036-010-0274-2

[23] Wang H, Fang H, Xing L, et al. An integrated biometric-based security framework using wavelet-domain HMM in wireless body area networks [C] //Proc of ICC 2011. Piscataway, NJ: IEEE, 2011: 1-5

[24] Ren Y, Pazzi R W N, Boukerche A. Monitoring patients via a secure and mobile healthcare system [J]. IEEE Wireless Communications, 2010, 17(1): 59-65

[25] Zhang R, Zhang Y, Sun J. Fine-grained private matching for proximity-based mobile social networking [C] //Proc of IEEE INFOCOM 2012. Piscataway, NJ: IEEE, 2012: 1969-1977

[26] Liang X, Li X, Zhang K, et al. Fully Anonymous profile matching in mobile social networks [J]. IEEE Journal on Selected Areas of Communications (JSAC), 2013, 31(9): 641-655

[27] Li L, Zhao X, Xue G, et al. Privacy preserving group ranking [C] //Proc of IEEE ICDCS 2012. Piscataway, NJ: IEEE, 2012: 214-223

[28] Zhang L, Li X, Liu Y, et al. Verifiable private multi-party computation: Ranging and ranking [C] //Proc of IEEE INFOCOM 2013. Piscataway,NJ: IEEE, 2013: 605-609

[29] Li X, Jung T, Search me if you can: Privacy-preserving location query service [C] //Proc of IEEE INFOCOM 2013. Piscataway, NJ: IEEE, 2013: 2760-2768

[30] Gentry C. Fully homomorphic encryption using ideal lattices [C] //Proc of STOC 2009. Berlin: Springer, 2009: 169-178

[31] Dijk M V, Gentry C, Halevi S, et al. Fully homomorphic encryption over the integers [C] //Proc of EUROCRYPT 2010. Berlin: Spinger, 2010: 24-43

[32] Gentry C, Halevi S, Vaikuntanathan V. i-Hop homomorphic encryption and rerandomizable Yao circuits[G]//LNCS 6223: Proc of CRYPTO2010. Berlin: Springer, 2010: 155-172

[33] Lauter K, Naehrig M, Vaikuntanathan V. Can homomorphic encryption be practical? [C] //Proc of ACM CCS 2011. New York: ACM, 2011: 1-12

[34] Gennaro R, Gentry C, Parno B. Non-interactive verifiable computing: Outsourcing computation to untrusted workers [C] //Proc of CRYPTO 2010. Berlin: Springer, 2010: 465-482

[35] Barbosa M, Farshim P. Delegatable homomorphic encryption with applications to secure outsourcing of computation[G]// LNCS 7178: Proc of CT-RSA 2012. Berlin: Springer, 2012: 296-312

[36] Zhou J, Cao Z, Dong X, et al. Security and privacy in cloud-assisted wireless wearable communications: Challenges, solutions and future directions [J]. IEEE Wireless Communications, 2015, 22(2): 136-144

[37] Lu R, Liang X, Li X, et al. EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications [J]. IEEE Trans on Parallel and Distributed Systems, 2012, 23(9): 1621-1631

[38] Erkin Z, Tsudik G. Private computation of spatial and temporal power consumption with smart meters[G]//LNCS 7341: Proc of ACNS'12. Berlin: Spinger, 2012: 561-577

[39] Shi E, Chan T H H, Rieffel E G, et al. Privacy-preserving aggregation of time-series data [C] //Proc of the 18th Annual Network and Distributed System Security Symp (NDSS 2011). Berlin: Springer, 2011: 111-125

[40] Lynn B. PBC Library [OL]. [2015-07-20] http://crypto.stanford.edu/pbc/

[41] Shamus Software Ltd. Multiprecision integer and rational arithmetic C/C++ library [OL]. [2015-07-20]. http://www.shamus.ie/

[42] Liang X, Li X, Lu R, et al. UDP: Usage based dynamic pricing with privacy preservation for smart grid [J]. IEEE Trans on Smart Grid, 2013, 4(1):141-150

[43] Dong X, Zhou J, Alharbi K, et al. An ElGamal-based efficient and privacy-preserving data aggregation scheme for smart grid [C] //Proc of IEEE GLOBECOM2014. Piscataway, NJ: IEEE, 2014: 4720-4725

[44] Dong X, Zhou J, Cao Z. Efficient privacy-preserving temporal and spacial data aggregation for smart grid communications [J]. Concurrency and Computation: Practice and Experience, 2015, DOI:10.1002/cpe.3570

[45] Eschenauer L, Gligor V. A key management scheme for distributed sensor networks [C] //Proc of the 9th ACM Conf on Computer and Communication Security. New York: ACM, 2002: 41-47

[46] Chan H, Perrig A, Song D. Random key distribution schemes for sensor networks [C] //Proc of the IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2003: 197-213

[47] Liu D, Ning P. Establishing pairwise keys in distributed sensor networks [C] //Proc of the 10th ACM Conf on Computer and Communication Security. New York: ACM, 2003: 41-77

[48] Bresson E, Chevassut O, Pointcheval D, et al. Provably authenticated group Diffie-Hellman key exchange [C] //Proc of ACM CCS'01. New York: ACM, 2001: 255-264

[49] Cherukuri S, Venkatasubramanian K K, Gupta S K S. BioSec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body [C] // Proc of the IEEE Int Conf on Parallel Processing Workshops. Piscataway, NJ: IEEE, 2003: 432-439

[50] Bao S D, Poon C C Y, Zhang Y T, et al. Using the timing information of hearbeats as an entity identifier to secure body sensor network [J]. IEEE Trans on Information Technology in Biomedicine, 2008, 12(6): 772-779

[51] Juels A, Sudan M. A fuzzy vault scheme [C] //Proc of IEEE Int Symp on Information Theory. Piscataway, NJ: IEEE, 2002: 237-257

[52] Venkatasubramanian K K, Banerjee A, Gupta S K S. PSKA: Usable and secure key agreement scheme for body area networks [J]. IEEE Trans on Information Technology in Biomedicine, 2010, 14(1): 60-68

[53] Hu C, Cheng X, Zhang F, et al. OPFKA: Secure and efficient ordered physiological feature-based key agreement for wireless body area networks [C] //Proc of IEEE INFOCOM 2013. Piscataway, NJ: IEEE, 2013: 2274-2282

[54] Zhou J, Cao Z, Dong X. BDK: Secure and efficient biometric based deterministic key agreement in wireless body area networks [C] //Proc of BODYNETS 2013. New York: ACM, 2013: 488-494

[55] Lin X, Sun X, Wang X, et al. TSVC: Timed efficient and secure vehicular communications with privacy preserving [J]. IEEE Trans on Wireless Communication, 2008, 7(12): 4987-4998

[56] Zhang C, Lin X, Lu R, et al. RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks [C] //Proc of IEEE ICC 2008. Piscataway, NJ: IEEE, 2008: 1451-1457

[57] Lin X, Li X. Achieving efficient cooperative message authentication in vehicular ad hoc networks [J]. IEEE Trans on Vehicular Technology, 2013, 62(7): 3339-3348

[58] Lu R, Lin X, Liang X, et al. A dynamic privacy-preserving key management scheme for location based services in VANETs [J]. IEEE Trans on Intelligent Transportation Systems, 2012,13(1): 127-139

[59] Lu R, Lin X, Luan T H, et al. PReFilter: An efficient privacy-preserving relay filtering scheme for delay tolerant networks [C] //Proc of IEEE INFOCOM 2012. Piscataway, NJ: IEEE, 2012: 25-30

[60] Zhou J, Dong X, Cao Z, et al. Secure and privacy preserving protocol for cloud-based vehicular DTNs [J]. IEEE Trans on Information Forensics and Security, 2015,10(6): 1299-1314

[61] Zhu H, Lin X, Lu R, et al. SMART: A secure multilayer credit-based incentive scheme for delay-tolerant networks [J]. IEEE Trans on Vehicular Technology, 2009, 58(8): 4628-2639

Dong Xiaolei, born in 1971. Professor in East China Normal University. Her main research interests include number theory, cryptography, network security, etc.