电力大数据密态多源协同安全应用研究*

杨赟博[1,2],胡雪晖[1],洪 晟[3]

(1.上海同态信息科技有限责任公司,上海 200231;2.华东师范大学,上海 200062;
3.北京航空航天大学 网络空间安全学院,北京 100191)

摘 要: 重点介绍了电力大数据在应用过程中存在的主要问题,并结合身份认证、外包计算、全同态加密等新兴技术,给出了电力大数据密态多源协同安全框架,该框架可以让电力大数据安全地流通并实现外包计算,从而构建一个安全的计算环境。随后提出的多方协作安全可信环境体系可完成身份认证,提高安全性的同时简化身份认证流程,提出的电力大数据密态安全计算关键技术可以提高同态加密的运算效率,并提升安全性,同时将该两技术进行结合提出了外包计算密码技术框架及其工作流程。最后通过与常用的同态加密库 SEAL 进行对比,验证了所提出的以"同态构型"加密算法为核心的密态多源协同安全应用框架具有运行效率高、扩展性好的特点,适用于大数据的安全外包计算等场景中。

关键词: 电力大数据;数据安全;外包计算;同态加密;身份认证

中图分类号: TP399 **文献标识码:** A **DOI:** 10.19358/j.issn.2096-5133.2022.04.008

引用格式: 杨赟博,胡雪晖,洪晟. 电力大数据密态多源协同安全应用研究[J].信息技术与网络安全,2022,41(4):52-59.

Research on the security application of encrypted multi-source collaborative for power big data

Yang Yunbo[1,2], Hu Xuehui[1], Hong Sheng[3]

(1.Shanghai Tongtai Information Technology Co., Ltd., Shanghai 200231, China;
2.East China Normal University, Shanghai 200062, China;
3.School of Cyber Science and Technology, Beihang University, Beijing 100091, China)

Abstract: This paper focuses on the main problems in the application of big data in electricity, combines emerging technologies such as identity authentication, outsourced computing and full homomorphic encryption, and proposes an encrypted multi-source collaborative security framework for power big data. It allows power big data to circulate safely and realize outsourced computing, so as to build a secure computing environment. Then the multi-party collaborative security and trustworthy environment system proposed in this paper can complete identity verification. The proposed key technology of cryptographic security computing for power big data can improve the computational efficiency of homomorphic encryption and enhance security, while the two technologies are combined to propose a framework for outsourced computing cryptography and its workflow. Finally, this paper shows that the proposed cryptomorphic multi-source collaborative security application framework with the "homomorphic configuration" encryption algorithm as the core has high operational efficiency and good scalability, and it could be used in scenarios such as outsourced computing of big data.

Key words: power big data; data security; outsourcing computing; homomorphic encryption; identity verification

0 引言

2020 年 3 月 30 日国务院发布的《关于构建更加完善的要素市场化配置体制机制的意见》指出,要加快培育数据要素市场,其中的三个重点分别为:推进政府数据的开放共享,提升社会数据的资源价值,以及对数据资源整合和安全保护的加强。

"十四五"期间,我国进入由工业经济向数字经

* 基金项目:国家重点研发计划(2019YFB1706001)

济大踏步迈进的关键时刻,经济社会数字化转型成为大势所趋,数据已渐渐上升为新的社会生产要素,数据要素价值释放成为重要命题[1]。

在这一背景之下,要求各单位打通数据孤岛,连接产业链中的各个节点,将数据价值转换为实实在在的经济价值。

而电力大数据具有真实性高、时序性强、数据量大的独特优势,深入挖掘电力大数据的应用潜力是目前电网企业应对经济下行,提质增效的重要手段[2]。

近年来,针对大数据的攻击和数据泄露日益严重,国家相继出台了一系列数据安全法规,用以明确与规范大数据安全工作的相关要求[3-4],而这些潜在的数据威胁在电力行业中表现得更为明显[5]。

在电网数字化转型不断推进的当下,电力大数据积累了大量的敏感数据,除身份证号、住址等常见的高价值敏感数据外,还可能涉及政府、军工企业、科研院所等敏感地点的用电分布。通过对用电数据的分析,可以感知到一些敏感区域与机构的工作开展情况。因此,在遵循法律要求,保证电力信息系统中客户的数据和资料保密的前提下[6],需要重点做好电力大数据的安全防护,从根本上规范电力企业信息安全控制问题[7],并亟需解决以电力大数据为代表,数据在超算平台计算环境、第三方平台计算环境以及在应用过程中的隐私保护问题。

1 电力大数据安全应用研究现状

国内外对于电力大数据的安全应用仍然处于应用探索阶段,电力大数据具有数据时效性强、数据链路长、数据类型多等特点,为了解决这些问题,南方电网采用一系列措施逐步推动数据市场释放数据价值[8],其中最关键的一条是强化数据资产管理技术能力,保障数据的安全可用[8],即在保护数据隐私的基础上,同步可以对数据进行运算,以发挥大数据的重要价值。

1.1 全同态加密

在隐私计算场景中,全同态加密和多方安全计算是主流的两大技术,它们都可以应用在电力大数据中,在保证数据安全的基础上,充分发挥大数据在社会和经济上的价值。全同态加密在不对加密数据解密的情况下,完成对密文数据进行任意多次处理[9];而多方安全计算能够在保证数据输入的安全以及数据计算的正确性前提下,在没有第三方的情况下通过协议完成计算[10]。

如表 1 所示,传统加密方法较全同态加密方法和多方安全计算而言,其数据可用性较差,而多方安全计算需要高昂的加解密开销和通信开销,使得其无法直接部署在隐私计算服务中。全同态加密因其加解密开销小、通信开销小等优点而被广泛使用。

外包计算允许计算资源受限的数据拥有者将计算开销较大的本地运算外包给云服务器完成。同态加密技术是外包计算中的一种常用技术,但是传统的同态加密都是基于公钥加密手段进行,经典的全同态加密如 BGV[11]和 CKKS[12]等算法都是对每个明文比特进行运算,造成协议运算效率低下,其巨大的计算开销无法满足资源受限用户终端的性能需求。

1.2 身份认证

电力大数据的信息安全保护措施主要包含身份认证、信息加密及入侵检测等技术,其中首要任务是对用户的身份进行认证,提高电力大数据的安全性,防止非法用户对电力大数据进行访问、使用、修改和删除等操作[13]。

身份认证技术是密码学研究的一项重要内容,可以有效地保证信息安全,在信息系统中有着极其重要的地位[14]。目前主要的身份认证体系由以下三点构成:

(1)基于信息秘密的身份认证

根据用户所知道的信息来证明用户的身份,属于传统的身份认证方式。比如用户设定的用户名、密码,或是安全问题的答案。

(2)基于信任物体的身份认证

根据用户所拥有的信任物体来证明用户的身份。比如校园的一证通、银行的 U 盾等。

(3)基于生物特征的身份认证

根据用户的生物特征值来证明用户的身份。比

表 1 主流技术对比

技术名称	计算开销	通信开销	数据安全性	数据可用性	加解密开销
传统加密	无法计算	低	最高 CCA-2	无	低
全同态加密	极高	低	CPA	高	低
多方安全计算	低	极高	恶意敌手攻击下安全	高	高

如声纹的 Voice ID、指纹解锁、人脸识别等。

传统的身份认证对应的身份认证体系认证要素单一,往往只是依赖于以上三个基础体系当中的一个或多个,不能在现如今复杂的网络环境中保证身份信息的真实有效。用户可以通过伪造的方法通过身份认证,从而对系统进行非法操作或访问。同时传统的身份认证方式不能支持复杂多变的认证需求,具有很大的提升空间。

1.3 安全外包计算

另一方面,云计算技术的飞速发展使大数据面临的安全问题日益凸显,在工业界和学术界都引起了广泛的关注[15]。而在电力大数据场景中,数据一般需要提供给一个强大的计算服务提供方进行计算,但是如果直接将明文数据传输给计算服务提供方,就会造成敏感信息的泄漏,而外包计算允许计算资源受限的数据拥有者将计算开销较大的本地运算外包给云服务器完成,同时保证敏感数据的安全性。

如图 1 所示,传统的安全外包计算模型可以看作是一个一对一模型,即一个数据拥有方和计算服务提供方进行交互后根据计算协议完成运算,但该传统模型受限于特定场景,扩展性较差。

因此,在数据拥有者扩展成多个数据源集合时,传统外包计算中单用户模型无法满足当前其多样的场景需求。为了满足多方参与的需求,本文提出了新型安全外包计算模型,如图 2 所示。该模型可用于多用户场景,且计算服务提供方、数据拥有者和结果需求者相互独立的情况。基于新的模型,数据拥有方的数据隐私可以得到保护,与此同时可以借助计算服务提供方强大的计算资源完成计算,结果需求方也可以得到最终的计算结果,以发挥数据最大效益。

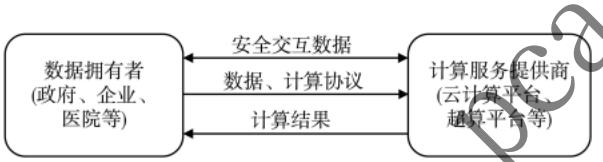

图 1 传统安全外包计算模型

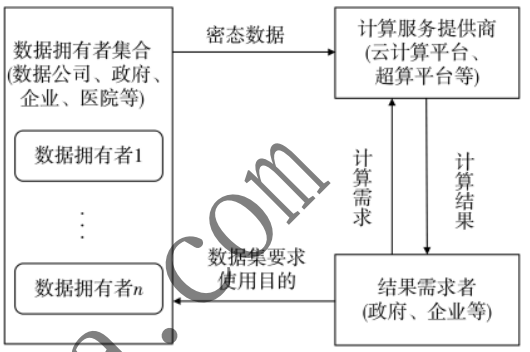

图 2 新型安全外包计算模型

2 电力大数据密态多源协同安全应用研究

2.1 总体框架

电力大数据密态多源协同安全应用的目标是让电力大数据能够安全地流通并实现外包计算,从而构建一个安全的计算环境。图 3 所示是本文提出的电力大数据密态多源协同安全应用的总体研究框架,大体可以分为基于多方协作的安全可信环境研究和电力大数据密态安全计算的研究。

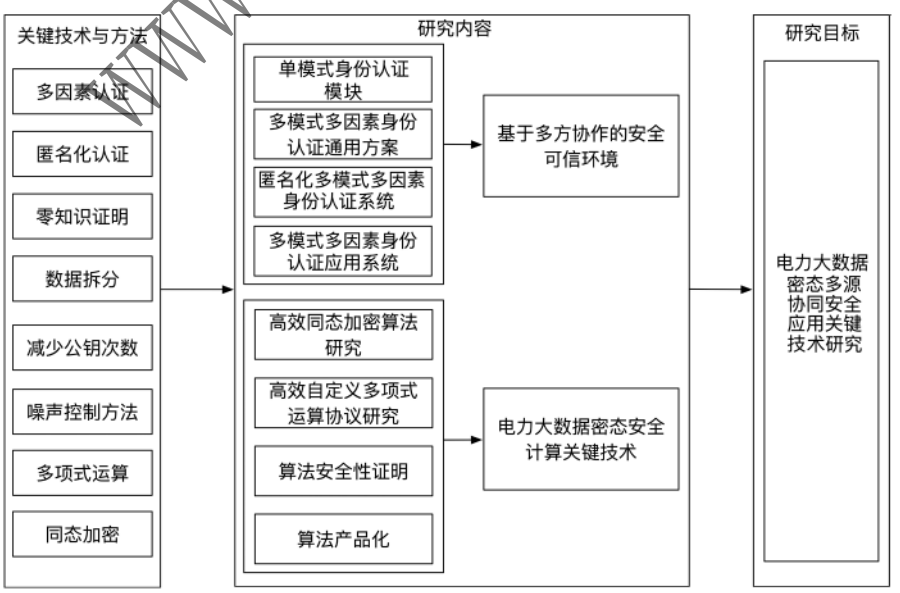

图 3 总体研究框架

2.1.1 基于多方协作的安全可信环境研究

身份安全是数据安全的基石,它可以验证用户的身份是否合法。为了实现电力大数据密态多源协同安全应用中的身份认证,将主要从以下几方面进行研究:

(1)采用一种多因素的认证方法,通过同时对多种难篡改的要素进行认证,提高认证结果的可信程度,解决虚假登录和机器流量的问题。

(2)提出一种多模式的认证方法,使得用户在登录过程中不需要输入账户名与密码,简化登录流程。

(3)使用一种零知识证明的方法,做到在不暴露具体认证要素的情况下,完成对各个因素的认证,从而实现认证过程中的匿名化。防止高权限账户的精准攻击。

2.1.2 电力大数据密态安全计算关键技术研究

电网核心运营大数据具有敏感性强、重要度高等特点,针对电力大数据在第三方平台计算及应用过程中可能存在隐私泄漏等问题,依托国产密码算法并开发密码设备研究在超算平台下基于全同态加密技术的电网大数据安全运算机制,并探索电网的敏感大数据在不被泄漏的前提下的一种安全分析方法。

2.2 多方协作安全可信环境体系

如图 4 所示,多方协作安全可信环境体系研究首先是实现多因素身份认证,主要围绕生物因素、设备因素和网络因素展开,其中生物因素用于系统对人的登录认证,设备因素和网络因素用于系统之间通信时对设备的认证;其次通过零知识证明技术,实现在不校验具体参数的情况下,完成对因子的认证,做到匿名化登录;去除传统认证方式中“用户名+口令”的方式,从而有效规避攻击者通过精准攻击、SQL 注入等方式进行攻击的风险,提升安全性;最后在进行身份认证时,支持手机端动态密码或扫描二维码等多种认证模式,简化认证流程。

图 4 多方协作安全可信环境体系

2.3 电力大数据密态安全计算关键技术

电力大数据密态安全计算关键技术研究如图 5 所示,首先在同态加密中,使用大整数运算替换矩阵运算,将加法时间复杂度降低到 $O(n)$,乘法时间复杂度降低到 $O(n\log n)$,从而提高密文运算效率;其次研究配套的同态加密运算解析器,将用户输入的公式直接映射为对应的密文运算,并且在 RO 模型下构建算法安全模型,刻画攻击者形象,完成安全性证明;最后开发算法对应的电力数据密态协同运算一体设备,满足合规性要求,保障协议执行环境安全。

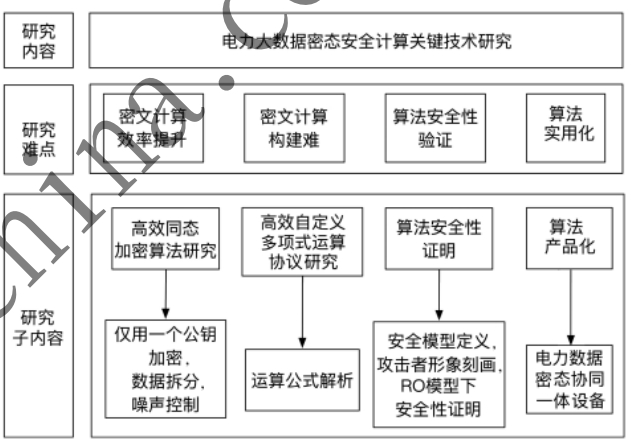

图 5 电力大数据密态安全计算关键技术

2.4 方案介绍

如图 6 所示,在电网数据中心内部需要部署一个身份认证服务以及一个高效同态加密机。身份认证服务用于对数据外包计算平台的操作人员进行访问控制,并在内部留存操作记录,从而保证系统操作者的身份真实有效。在确认操作者身份之后,外包计算平台向计算中心发起数据计算请求。

身份认证服务将通过一种基于匿名化认证的技术完成,该匿名化认证技术首先认证访问者的生物特征,之后认证访问者的操作设备,确保是合法的访问者在授权的设备上发起操作。

如图 7 所示,在实际认证过程中,应用用户的指纹或者人脸信息对用户进行验证。对设备的认证主要是通过采集设备指纹,通过比对完成认证。在制作设备指纹的过程中,也会将设备的网络环境信

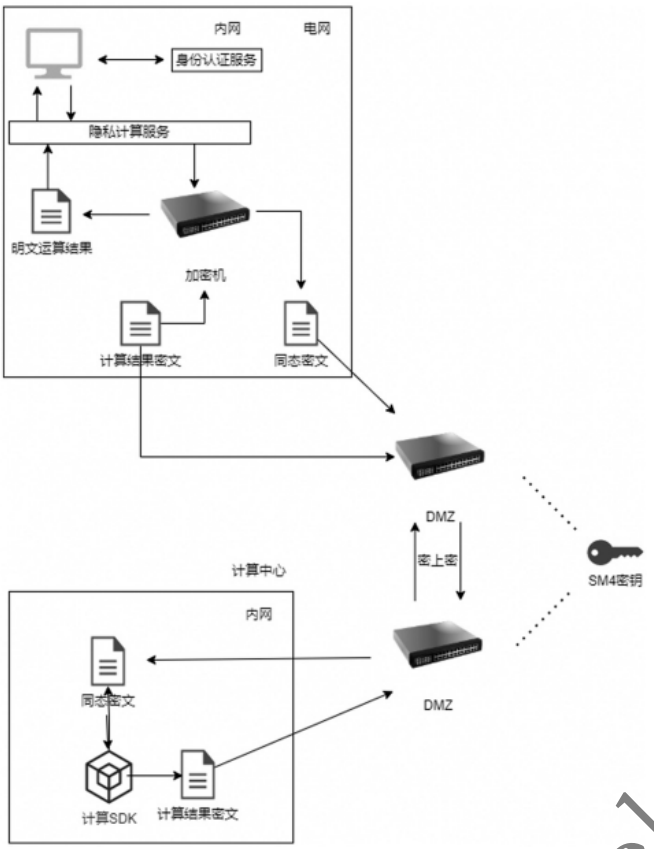

图 6 外包计算密码技术架构图

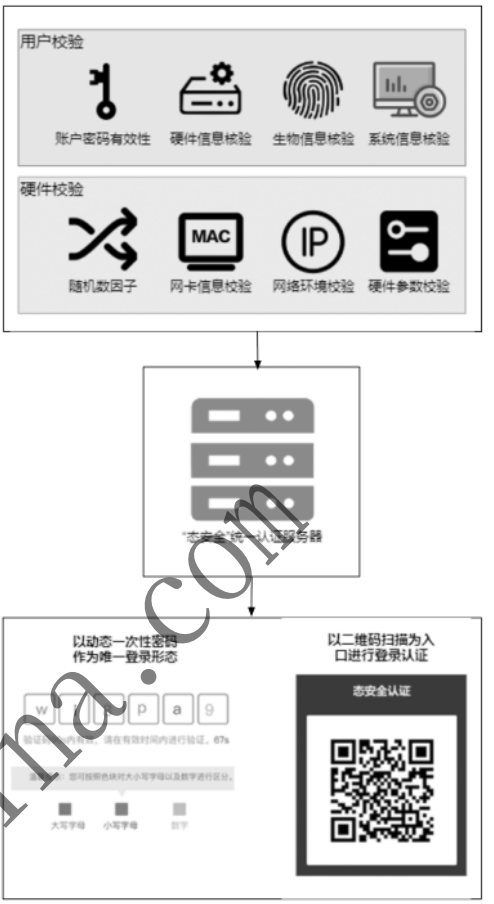

图 7 身份认证服务器组成

息进行采集,一起打包进设备指纹当中,从而保证常用设备在可信的网络环境中运行。

在发送数据的过程中,用户首先在平台上配置计算需求,并配置需要使用同态加密技术进行保护的字段。完成配置之后,系统使用加密机内置的高性能同态加密技术对用户配置的字段进行加密,最后将加密完成之后的数据发送到数据前置机上。

前置机与大数据中心的前置机使用 PAKE 协议(图 8)完成身份认证并且同步生成对称密钥,使用该对称密钥对同态密文进行加密传输,从而加强数据在传输过程中的安全性。

为了能够实现电网和计算中心之间的身份认证,在系统构建时,需要双方使用线下的方式,传递脱敏后的标签信息,用来保证认证过程中的安全性。

在计算中心内部嵌入定制的密文分析业务 SDK,其核心功能为提供基于密文的分析能力,在完成分析计算之后将密文的结果导入前置机当中,计算中心前置机对电网数据中心前置机发起认证请求。在双方进行身份认证之后,会生成会话密钥,该密钥

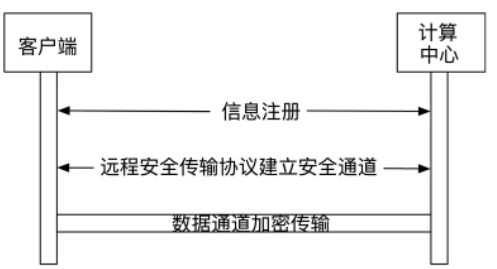

图 8 PAKE 协议交互示意图

用以对计算结果的密文进行加密传输。

电网获取密文计算结果后,首先在前置机中还原出结果的同态密文,再将同态密文导入加密机中进行解密,获得计算结果,计算结果最后发送到有需求的业务系统。

在电网系统当中,除了加密机和身份认证服务之外,还需要部署一个隐私计算服务,该服务主要负责对业务系统提供密码服务,隔离加密机硬件,使得用户业务系统可以通过使用该服务调用加密机,降低系统对接难度。同时,在该服务中附加隐私

策略配置等功能,提升系统的可用性和灵活性。该服务还提供一个 Web 操作界面,用户通过该 Web 界面,使用电力数据外包计算系统。

3 实验和结论

3.1 实验环境搭建

同态构型 V1.0 是由上海同态信息科技有限责任公司(简称“同态科技”)自主研发的一种数据隐私保护加密算法,实现全密文的数学分析,解决数据融合过程中的数据隐私保护以及数据价值稀释问题。

通过使用该算法,数据源能够对外提供可用不可见的数据。需求方能够使用这些可用不可见的数据进行数据分析,获取数据价值。实现在保障数据具体内容不外泄的情况下,完成对于数据计算价值的多方共享。

本文对比测试中采用同态构型 V1.0 算法,代码使用 C++14 进行编译。测试过程中使用的软硬件环境配置如表 2 所示,同时在测试过程中,双方都基于相同的硬件平台,在相同的环境下进行编译与测试。

表 2 软硬件环境配置表

操作系统	处理器	内存
Ubuntu 18.04.1 LTS	Intel Xeon® W-2295@3.0GHz x36	32 GB

3.2 全同态加密算法比较

微软全同态 SEAL 库是目前开源框架下在全同态加密领域的最佳公开实践,在传统的全同态加密算法中具有最高的执行效率。Paillier[16]是目前开源同态加密算法库中执行加法的聚合计算速度最快的算法之一。

本次测试主要通过实际测试对比同态构型 V1.0 算法与微软全同态加密 SEAL 库的加密、解密、加法、乘法以及 Paillier、安全多方计算实际的业务执行效率,同时进行实际运算过程中与明文的对比测试,验证同态构型 V1.0 在性能上的优势。

本次测试共有五个测试项,分别为加密性能对比、解密性能对比、密文加法性能对比、密文乘法性能对比和聚合计算性能对比,以及数据分析总体业务效率对比测试。

3.2.1 加密时间对比测试

对同态构型算法与微软 SEAL 库进行数据加密的用时对比测试,表 3 所示是分别进行 1 000、10 000、100 000 次加密操作的耗时对比。

表 3 加密耗时比较

	耗时/ms	
	同态构型	SEAL
1 000	0.720	1 089.630
10 000	8.129	10 583.800
100 000	80.864	105 990.000

3.2.2 解密时间对比测试

对同态构型算法与微软 SEAL 库进行数据解密的用时对比测试,表 4 是分别进行 1 000、10 000、100 000 次解密操作的用时对比。

表 4 解密耗时比较

	耗时/ms	
	同态构型	SEAL
1 000	0.995	311.887
10 000	9.516	3 078.880
100 000	90.764	30 801.160

3.2.3 加法时间对比测试

对同态构型算法与明文数据加法、微软 SEAL 库进行密态数据加法方面的用时对比测试,表 5 是分别进行 1 000、10 000、100 000 次加法操作的时间对比。

表 5 同态加法耗时比较

	耗时/ms		
	明文	同态构型	SEAL
1 000	0.118	1.546	1 026.09
10 000	1.246	15.577	28 456.8
100 000	11.999	151.473	/

3.2.4 乘法时间对比测试

对同态构型算法与明文数据乘法、微软 SEAL 库进行密态数据乘法方面的用时对比测试,表 6是分别进行 1 000、10 000、100 000 次乘法操作的时间对比。

表 6 同态乘法耗时比较

	耗时/ms		
	明文	同态构型	SEAL
1 000	1.391	40.28	28 092.6
10 000	16.088	415.368	27 777 547
100 000	138.256	4 049.51	/

3.2.5 聚合计算对比测试

检测同态构型、Paillier 的聚合计算效率。分别

运算 1 000、10 000 条数据的加法聚合,整体耗时如表 7 所示。

表 7 聚合计算耗时比较

	耗时/ms		
	明文	同态构型	Paillier
1 000	0.095	1.246	6 376.02
10 000	0.867	13.391	62 249.3

3.3 场景测试

3.3.1 外包计算

使用同态构型、微软全同态加密 SEAL 库分别运算 1 000、10 000 条税后本息和(税后本息和=本金+本金×利率×年份×(1−税率))公式,表 8 为分别统计其整体耗时结果。

表 8 外包计算场景下的耗时比较

	耗时/ms		
	明文	同态构型	SEAL
1 000	0.543	19.011	18 242.7
10 000	5.687	183.878	182 124

3.3.2 大数据量外包计算

使用同态构型和微软全同态加密 SEAL 库分别进行 10 000、20 000、30 000、40 000 次税后本息和公式的外包计算,表 9~表 11 分别为加密、计算、解密的时间比较。

表 9 大数据量外包计算场景下的加密耗时比较

执行次数	加密时间/ms	
	同态构型	SEAL
10 000	29	54 237
20 000	79	103 395
30 000	131	154 901
40 000	182	204 962

表 10 大数据量外包计算场景下的计算耗时比较

执行次数	计算时间/ms	
	同态构型	SEAL
10 000	129	112 725
20 000	255	222 539
30 000	382	333 301
40 000	510	445 552

3.4 电量数据外包计算

本节中分别利用同态构型 V1.0、SEAL 库、Paillier 和文献[17]中的安全多方计算模型对深圳市的峰谷时期电费外包计算进行对比测试。其中电价是明文,电量是密文,表 12 显示了模型中所使用的深圳市峰谷时期电费数据,表 13 为电量数据外包计算总运行时间对比。

表 11 大数据量外包计算场景下的解密耗时比较

执行次数	解密时间/ms	
	同态构型	SEAL
10 000	27	6 399
20 000	53	12 843
30 000	79	19 201
40 000	105	25 624

表 12 深圳市电费(第一档)

用电期	电费
峰期	107.94
平期	65.42
谷期	32.71

表 13 电量数据外包计算总运行时间

数据量	总运行时间/s			
	同态构型	SEAL	Paillier	安全多方计算
10 000	38.857 1	265.546	198.054	5 293.53

表 14~16 分别为同态构型 V1.0、SEAL、Paillier 在各流程中的运行时间,计算的数据量标准均为 10 000 组。

表 14 同态构型各流程运行时间

流程	耗时/s	速度/(次/s)
随机数生成	32.531 8	307.392
加密运算	1.559 56	6 412.08
同态乘法运算	2.904 13	3 443.38
同态加法运算	0.765 355	13 065.8
解密	0.690 503	14 482.2
总时间	38.857 1	257.353

表 15 SEAL 各流程运行时间

流程	耗时/s	速度/(次/s)
加密	64.684 1	154.597
计算	3.451 62	2 897.19
存储	25.702 1	389.073
解密	6.081 01	1 644.46
总时间	265.546	37.658 3

表 16 Paillier 各流程运行时间

流程	耗时/s	速度/(次/s)
计算	2.496 38	4 005.8
解密	194.32	51.461 5
总时间	198.054	50.491 4

4 结论

电力大数据安全是电网数字化安全转型的前提,也是我国在落实新型智能电网方向的重要保障。虽然云端算力可以提升社会资源利用率,然而直接将电力大数据在第三方计算平台中进行应用存在隐私泄漏的可能。因此,在保护电力大数据隐私的情况下将其发挥出最大效益是本课题研究的主要内容。

本文主要研究电力大数据密态多源协同安全应用场景,利用安全外包计算、同态加密、身份认证等手段,构建一个安全的计算环境,能够对数据的全生命周期进行保护,保证电网数据在云上的安全,从而使得电力大数据安全地上云或外包给超算平台等第三方计算服务提供方进行计算,大大降低企业的运营成本,在保护电力大数据隐私安全的同时能够充分发挥电力大数据的经济效益,提升社会生产力。

同时,本文通过对比实验表明了以“同态构型”加密算法为核心的密态多源协同安全应用具有运行效率高、扩展性好的特点,可以用于外包计算等场景中。

参考文献

[1] 张玉清,王晓菲,刘雪峰,等.云计算环境安全综述[J].软件学报,2016,27(6):1328-1348.

[2] 邓恢平.释放电力大数据要素价值[N].中国电力报,2021-12-09(007).

[3] 袁哲.电力大数据应用综述[J].电工技术,2021(11):189-191,195.

[4] 朱洪斌,安龙,杨铭辰.电力大数据安全治理体系研究[J].电信科学,2019,35(11):140-145.

[5] 朱洪斌,安龙,杨铭辰.电力大数据安全治理体系[C]//生态互联 数字电力——2019 电力行业信息化年会论文集,2019:424-425.

[6] 梁霄,梁明.基于身份认证的电力大数据安全技术研究[C]//2018 智能电网新技术发展与应用研讨会论文集,2018:26-27.

[7] 王东斌,王占国,薛闯.大数据背景下电力信息系统安全的研究[J].信息记录材料,2021,22(6):134-136.

[8] 查士加.南方电网陈彬:创新电力数据资产治理,释放电力数据要素价值[EB/OL].[2022-02-09].https://www.sohu.com/a/521554451_121124373.

[9] 陈智罡,宋新霞,郑梦策,等.全同态加密文献计量分析研究[J].计算机工程与应用,2022,58(4):40-51.

[10] 蒋凯元.多方安全计算研究综述[J].信息安全研究,2021,7(12):1161-1165.

[11] BRAKERSKI Z,GENTRY C,VAIKUNTANATHAN V. Fully homomorphic encryption without bootstrapping[J]. ACM Transactions on Computation Theory,2014,6(3):13:1-13:36.

[12] CHEON J H,KIM A,KIM M,et al.Homomorphic encryption for arithmetic of approximate numbers[C]//International Conference on the Theory and Application of Cryptology and Information Security,2017:409-437.

[13] 刘珊,杨华,岳克明.大数据在电力信息安全的研究[J].山西电力,2018(4):45-47.

[14] 张引兵,刘楠楠,张力.身份认证技术综述[J].电脑知识与技术,2011,7(9):2014-2016.

[15] 褚健.解读《工业控制系统信息安全行动计划(2018-2020)》[J].自动化博览,2018,35(7):54-55.

[16] 李丽华.大数据在电力信息安全中的实施对策[J].科技风,2021(2):195-196.

[17] PAILLIER P.Public-key cryptosystems based on composite degree residuosity classes[C]//Proceedings of the 17th International Conference on Theory and Application of Cryptographic Techniques(EUROCRYPT'99). Springer-Verlag,Berlin,Heidelberg,1999:223-238.

(收稿日期:2022-02-24)

作者简介:

杨赟博(1998-),男,博士研究生,主要研究方向:安全多方计算、可搜索加密。

胡雪晖(1995-),通信作者,女,博士,主要研究方向:GDPR、数据隐私。E-mail:rachel@ttaicloud.com。

洪晟(1981-),男,博士,副教授,博士生导师,主要研究方向:工业互联网安全、信息网络安全、复杂系统安全性。

版权声明

经作者授权，本论文版权和信息网络传播权归属于《信息技术与网络安全》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《信息技术与网络安全》编辑部

中国电子信息产业集团有限公司第六研究所