天津大学大学生创新创业训练计划

项目申报书（创新训练）

|  |  |
| --- | --- |
| 项目名称： | TPCM支撑的可信知识图谱平台 |
| 所属专业名称： | 网络空间安全 |
| 项目负责人： | 王浩宇 |
| 联系电话： | 15864557520 |
| 指导教师： | 许光全 |
| 联系电话： | 18649079119 |
| 申报日期： | 2022年四月三十日 |

天津大学教务处制

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **项目名称** | | | TPCM支撑的可信知识图谱平台 | | | | | | | |
| **项目所属**  **专业类代码** | | | 0809 | | | **申请经费** | | | 10000 | |
| **项目实施时间** | | | 起始时间： 2022 年 5 月 完成时间： 2023 年 5 月 | | | | | | | |
| **申请人或申请团队** |  | 姓名 | | 年级 | 学号 | | 所在院系  /专业 | 联系电话 | | E-mail |
| 负责人 | 王浩宇 | | 2020 | 3020244092 | | 计算机科学与技术 | 15864557520 | | 3020244092@tju.edu.cn |
| 成员 | 高兴 | | 2020 | 3020244135 | | 计算机科学与技术 | 18303835528 | | 3020244135@tju.edu.cn |
| 张思娴 | | 2020 | 3020244255 | | 计算机科学与技术 | 18273226889 | | 3020244255@tju.edu.cn |
| 任家骏 | | 2020 | 3020244396 | | 软件工程 | 16724991935 | | 3020244396@tju.edu.cn |
| 李政睿 | | 2020 | 3020244307 | | 计算机科学与技术 | 15122518453 | | 1260144395@qq.com |
| **指 导 教 师** | 第一指导教师 | 姓名 | | 许光全 | | | 专业技术职务 | 教授 | | |
| 单位 | | 智能与计算学部 | | | 研究方向 | 计算机网络，数据中心安全 | | |
| 联系电话 | | 18649079199 | | | E-mail | binw@tju.edu.cn | | |
| 第二指导教师 | 姓名 | |  | | | 专业技术职务 |  | | |
| 单位 | |  | | | 研究方向 |  | | |
| 联系电话 | |  | | | E-mail |  | | |
| **一、项目简介**（200字以内）  本项目旨在基于TPCM对知识图谱的构建安全、存储安全和融合安全进行保障，利用可信计算技术支撑知识图谱可信融合。可信3.0架构下使用的TPCM，相比TPM2.0架构下的CRTM，可以严格满足主动监控的信任根要求。借助TPCM可同时提供可信度量基点和可信控制基点，保障信任链完整的同时，满足四级可信要求。本项目组提出，面向知识图谱的可信管理平台，基于TPCM实现对系统完整性的保护及对上层应用的加密服务，实现信任链的可靠传递和对该应用场景的契合。 | | | | | | | | | | |
| **二、申请理由**（包括自身具备的知识条件、自己的特长、兴趣、已有的实践创新成果等）  随着云计算技术的广泛使用，云计算的发展速度与相应的网络安全技术之间不协调，不适配的问题日益凸显。网络空间的安全与人民生活、社会秩序和国家安全休戚相关，因此国家对可信计算技术的发展和攻防兼备的网络安全创新人才有着迫切的需求。  项目组成员均来自智能与计算学部，其中四名为计科方向，一名为软件工程方向。成员均有一定的编程经历，掌握多门编程语言，可使用c++/c，java，python等多种编程语言。此次项目的课题方向涉及知识图谱、可信计算、密码学等技术，引起了本项目组成员极大的研究兴趣，我们愿意响应国家网络空间安全人才战略，通过深入的学习了解，掌握更多理论知识和专业技能，竭尽所能完成技术的开发，为国家网络空间安全建设贡献一份力量。  这次项目对我们而言是一次机会，也是一次挑战，面对未来可能遇到的种种技术难题，我们有着自觉性和积极性，借由许老师和学长的指导，我们有信心克服困难，化困难为动力，锻炼自身能力，达到创新训练的目的。  **成员介绍：**  **王浩宇**：具备近两年编程经验，热爱探索，动手能力强。熟练掌握C、C++、Java、Python、Dart等语言，自学Python爬虫、Flutter前端设计和Android基本开发，擅长基于华为弹性云服务器的Linux系统操作和编程，对C# 、MySQL等课外内容有一定了解，对网络安全攻防、知识图谱平台和可信计算研究有浓厚兴趣。积极热情，认真负责，勇于试错。  **任家骏**：具备一年的编程经验和代码经验，精通C++、C语言、java、Python等语言的使用，基本掌握数据库、操作系统等方面的知识，在学校课程的基础上自学过前端编程等课外内容，做事认真，有活力和能动性，责任心强。  **高兴**：具备一年的编程经验，掌握C++、C、Python语言的使用，自学过一些前端编程知识和MATLAB的使用，对嵌入式有一些了解。基本掌握数据结构、操作系统、数据库等方面的知识。对网络安全方面有一定的兴趣，做事认真细心，努力上进，责任心强。  **张思娴**：掌握一定代码基础，具备一年的编程经验。熟练使用c、c++语言，擅长代码的改错和优化。熟悉系统内核开发知识，在算法优化和数据结构方面基础较牢。做事踏实且超前，自学理解能力和动手能力较强  **李政睿**：具备超过一年的编程与代码经验，对C++、C、JAVA等等编程语言有所掌握，能够熟练使用Linux操作系统，并对其架构略有了解；自学云计算、云平台的架构，有云服务器方面的一些知识；掌握部分数学建模知识，能够熟练使用MATLAB、Lingo等等数学工具；对于知识图谱的内容也有所研究。对计算机安全，网络攻防等等内容较为感兴趣，有较强的学习能力和上进心。 | | | | | | | | | | |
| **三、项目方案**  **1、项目研究背景**   * 1. **项目动机**   知识图谱 （Mapping Knowledge Domain）在图书情报界也称为知识域可视化或知识领域映射地图），是显示知识发展进程与结构关系的一系列各种不同的图形“用可视化技术描述知识资源及其载体”挖掘、分析、构建、绘制和显示知识及它们之间的相互联系。简要来说，知识图谱是应用数学、图形学、信息科学等等多领域以及多种方法所构建的，展示学科内容、学科架构、知识关系等功能的一种研究方法，在现代科学研究、教育教学、内容的存储和分析中起着越来越重要的地位。不同知识图谱之间数据支撑不足或者表达不全面的问题，导致实体存在异常或者冗余，知识图谱融合技术应运而生，并给出了针对诸如此的数据层异构问题的解决方案。    图表 1 知识图谱构建过程  而随着信息技术的迅猛发展，互联网的普及，以及移动互联、物联网、大数据、云计算、工业互联网等新型场景的迅速推广，互联网+的模式逐渐深入人心，与之带来的网络安全问题也日益凸显。可信计算（Trusted Computing）则是保证信息安全，构建安全可信网络平台的重要技术。相比于大型机时代对信息简单的隔离，分配用户权限等等方式，当前的互联网环境有着超大的数据量，需要面向超多的终端，面临的安全风险也更加的复杂多样。在此基础上，人们对于可信计算的要求也越来越高。而随着微软、Intel、 IBM等等互联网元老级公司不断深化可信技术，可信计算在当今的热度正在不断攀升。   * 1. **国内外的研究现状**   在知识图谱领域国外的研究起步较早，从万维网，再到W3C建立能够共享数据的语义网，以三元组为数据单元的资源描述框架（RDF）为基石，本体（Ontology）的概念被首次提出并应用，由此诞生了知识图谱的雏形。在全球知识图谱市场上，据Gartner发布的2020年数据与分析领域的十大技术趋势表示，到2022年，知识图谱技术实现100%的快速增长，到2023年，知识图谱技术将促进全球30%的企业机构决策过程的快速情景化。  对比来看，我国对知识图谱的研究起步较晚，缺乏对于知识图谱理论上的系统研究，目前主要以应用为主。2001年至今，我国知识图谱领域共申请专利36572件。特别是在2020年内，知识图谱专利申请量达到峰值，共计7256件。结合国家数字化转型、智能化发展的总体战略，在人工智能技术与应用全面发展的进程中，知识图谱技术将得到更加广泛的研究与应用。  在可信计算领域，目前为止主要是依靠可信平台模块TPM（Trusted Platform Module），通过自身内嵌加密算法保护计算机系统，防止非法用户的数据访问，该标准是由1999年IBM、HP、Intel、微软等著名IT企业发起成立了可信计算平台联盟TCPA (Trusted Computing Platform Alliance）提出的，这个组织后来更名为可信计算组织TCG(Trusted Computing Group)。2013年3月，TCG正式公开发布TPM2.0标准库，从此TPM进入2.0时代。  可信计算在我国，已经形成了完善的理论基础和完备的国家标准体系。我国的可信计算3.0克服了国外TCG对TPM被动挂接的先天缺陷，创造性的提出了运行和防护并存的双体系架构，采用自主创新的对称非对称相结合的密码体制；通过主动度量控制芯片TPCM（Trusted Platform Control Module）植入可信根，在可信密码模块TCM基础上加以信任根控制功能，实现密码与控制相结合，将可信平台控制模块设计为可信计算控制节点，实现了TPCM对整个平台的主动控制。而近年来发生的诸如微软TPM2.0事件，也正是在提示基于可信计算硬件构建新一代安全体系架构已成为必然之路，只有建立自己的防御体系才能避免在关键问题上受制于人。  **3）项目目的**  考虑到当前情况下，安全高效的知识图谱共享平台在经济、教育、科研、商业领域发挥重要作用，本项目考察研究国内外已有的知识图谱安全技术，从构建安全、存储安全、融合安全三方面出发，基于TPCM技术搭建系统性的知识图谱平台保护机制及其加密服务，构建从客户机到服务端、从底层硬件到网络前端的完整信任链传递过程。通过完全信任链的搭建，为用户提供可靠安全的知识图谱创建、存储和融合方案，实现知识图谱在服务平台中的构建安全，互融安全及可信可用。  **4）项目已有基础**  **可信计算体系结构：**可信计算机体系结构是可信计算技术实施的核心，主要为构建具体的可信计算机终端提供总体设计框架，包括可信硬件平台和可信软件平台。可信计算机硬件平台是实现计算机终端安全和网络平台可信的根本保障，其主要包括可信CPU、可信计算机中的安全芯片、BIOS系统及安全外设等，如AMD公司的Opteron处理器、TBD公司的TPM芯片等；可信计算机软件平台的研究表现为计算机硬件平台上各层次软件系统的设计实现与综合集成，相关内容主要包括可信软件栈和可信操作系统的研究，如微软公司开发的支持TPMV1.2芯片和NAP技术的新一代操作系统Windows Vista。  **信任根技术：**信任根是一个不可变的过程或身份，用作信任链中的第一个实体。信任根从系统引导确定授权软件正在系统上运行,以硬件形式构建于整机中，通过建立度量机制，保证系统完整性、身份可信性、安全存储和可信存储，实现主动防御。  **信任链技术：**信任关系逐级传递的方法。具体来说就是计算机接电后开始启动，整个系统运行就会由可信BIOS传递至自检，然后向主引导区进行传递，且向可信操作系统装载器进行传递，之后就是向操作系统内核实行传递，开始系统初始化进程，在这一整个过程中，都是通过可信密码模块实现认证及处理，在经过可信任链相关传递之后，进入可信服务及可信应用。  **可信计算软件栈（TSS）：**TCG提出的方便调用TPM功能的体系结，三层架构（设备驱动程序库、核心服务、服务提供商），TDDL由相应的制造商提供，提供一些系统内核和用户间的接口，通过这些接口可以对不同厂商的TPM进行统一化。其次通过这些接口完成TCS核心服务模块的建立，让TPM的所有功能和原语作为服务可被提供，最后TSP对接TCS并和用户完成交互，TSPI是和C/C++兼容的接口，以此编程使用TPM。  **可信3.0：**我国学者提出的基于TPM实现运算和防御并行的双体系思想，采用自主创新的对称非对称相结合的通过TPCM植入可信源根，在可信密码模块TCM基础上加以信任根控制功能，实现密码与控制相结合制  **TPCM 主动防御可信服务器平台：**建立在可信3.0理念上，基于TPCM搭建的主动防御可信服务器模型，相较于传统的TPM2.0服务器，有明显优势：    图表 2 TPM与TPCM功能比较  **知识图谱融合：**将不同来源和不同结构的知识经过融合操作整合为统一的知识图谱，核心操作在于语义对齐、本体匹配和本体链接。目前流主流的知识融合方法为通过神经网络算法以不同粒度学习实体及其指标的特征。  **5）引用及相关文章**   1. 刘峤,李杨,段宏,刘瑶,秦志光.知识图谱构建技术综述[J].计算机研究与发展,2016,53(03):582-600. 2. 沈昌祥,张焕国,王怀民,王戟,赵波,严飞,余发江,张立强,徐明迪.可信计算的研究与发展[J].中国科学:信息科学,2010,40(02):139-166. 3. 沈昌祥,公备.基于国产密码体系的可信计算体系框架[J].密码学报,2015,2(05):381-389.DOI:10.13868/j.cnki.jcr.000087. 4. 沈昌祥.用可信计算3.0筑牢网络安全防线[J].信息通信技术,2017,11(03):4-6. 5. 沈昌祥,石磊,张辉,刘春,商子豪.可信计算与可信云安全框架[J].科学与管理,2018,38(02):1-6. 6. 冯德尹,吴明念.可信计算技术在网络信息安全中的应用与研究[J].电脑知识与技术,2021,17(13):53-54.DOI:10.14004/j.cnki.ckt.2021.1345. 7. 曹宁.可信计算技术在网络信息安全中的应用[J].信息技术,2021(08):150-155.DOI:10.13274/j.cnki.hdzj.2021.08.028. 8. 安宁钰,赵保华,王志皓.《可信计算体系结构》标准综述[J].信息安全研究,2017,3(04):299-304. 9. Ji S , Pan S , Cambria E , et al. A Survey on Knowledge Graphs: Representation, Acquisition, and Applications[J]. IEEE Transactions on Neural Networks and Learning Systems, 2021, PP(99). 10. Paulheim H , Cimiano P . Knowledge graph refinement: A survey of approaches and evaluation methods[J]. Semantic Web, 2017, 8(3):489-508. 11. Nickel M , Murphy K , Tresp V , et al. A Review of Relational Machine Learning for Knowledge Graphs[J]. Proceedings of the IEEE, 2015, 104(1):11-33. 12. Zhang L , Y Zou, Wang W , et al. Resource allocation and trust computing for blockchain-enabled edge computing system - ScienceDirect[J]. Computers & Security, 2021. 13. TCG . TCG Specification Architecture Overview[EB/OL]. https://www.trustedcomputinggroup.org/downloads/specifications/, 2017. 14. TCG . TNC Architecture Overview[EB/OL]. https://www.trustedcomputinggroup.org/resources/tnc, 2011. 15. TCG . TCG Software Stack (TSS) Specification [R/OL]. https://www.trustedcomputinggroup.org/downloads/specifications/, 2017. 16. Winter J , Dietrich K . A hijacker's guide to communication interfaces of the trusted platform module[J]. Computers & Mathematics with Applications, 2013, 65(5):748-761. 17. Seunghun Han, Wook Shin, Jun-Hyeok Park, and HyoungChun Kim. A bad dream: subverting trusted platform module while you are sleeping. In Proceedings of the 27th USENIX Conference on Security Symposium. USENIX Association, USA, 1229–1246, 2018. 18. U. Chaterjee, D. Mukhopadhyay and R. S. Chakraborty, "3PAA: A Private PUF Protocol for Anonymous Authentication," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 756-769, 2021, doi: 10.1109/TIFS.2020.3021917. 19. K. Yang, L. Chen, Z. Zhang, C. J. P. Newton, B. Yang and L. Xi, "Direct Anonymous Attestation With Optimal TPM Signing Efficiency," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 2260-2275, 2021, doi: 10.1109/TIFS.2021.3051801. 20. Dhiman Chakraborty, Lucjan Hanzlik, and Sven Bugiel. SimTPM: user-centric TPM for mobile devices. In Proceedings of the 28th USENIX Conference on Security Symposium. USENIX Association, USA, 533–550, 2019. 21. A. Hoeller and R. Toegl, "Trusted Platform Modules in Cyber-Physical Systems: On the Interference Between Security and Dependability," 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2018, pp. 136-144, doi: 10.1109/EuroSPW.2018.00026. 22. D. Lu et al., "xTSeH: A Trusted Platform Module Sharing Scheme Towards Smart IoT-eHealth Devices," in IEEE Journal on Selected Areas in Communications, vol. 39, no. 2, pp. 370-383, Feb. 2021, doi: 10.1109/JSAC.2020.3020658. 23. Huajun Chen, Ning Hu, Guilin Qi, Haofen Wang, Zhen Bi, Jie Li, Fan Yang; OpenKG Chain: A Blockchain Infrastructure for Open Knowledge Graphs. Data Intelligence 2021; 3 (2): 205–227. 24. J. Li, J. Wu, J. Li, A. K. Bashir, M. J. Piran and A. Anjum, "Blockchain-Based Trust Edge Knowledge Inference of Multi-Robot Systems for Collaborative Tasks," in IEEE Communications Magazine, vol. 59, no. 7, pp. 94-100, July 2021, doi: 10.1109/MCOM.001.2000419. 25. Ilaria Tiddi, Stefan Schlobach, Knowledge graphs as tools for explainable machine learning: A survey, Artificial Intelligence, Volume 302, 2022, 103627. 26. Qiang Gao, Wei Wang, Kunpeng Zhang, Xin Yang, Congcong Miao, Tianrui Li, Self-supervised representation learning for trip recommendation, Knowledge-Based Systems, 2022, 108791. 27. Wei Jin, Yaxing Li, Han Xu, Yiqi Wang, Shuiwang Ji, Charu Aggarwal, and Jiliang Tang. Adversarial Attacks and Defenses on Graphs. SIGKDD Explor. Newsl. 22, 2, 19–34, 2021. https://doi.org/10.1145/3447556.3447566   **2、项目研究目标及主要内容**  **1）研究目标**：  本项目面向知识图谱共享平台，利用TPCM为系统提供完整性保护及对为上层应用提供加密服务，从而达到使用可信计算技术支撑实现知识图谱融合的目的。该方案能构建面向知识图谱商业级或工业级应用的主动免疫防御系统，来有效解决知识图谱在融合过程中面临的关于知识图谱构建安全、存储安全和融合安全这三大主要问题，并最终实现知识图谱的构建融合与完善。  **2）主要内容：**  在学习了解可信计算技术、TPM/PCR的特点、以及TSS的三层架构体系结后，我们通过TPCM物理芯片和vTPCM虚拟芯片搭建可信知识图谱共享平台。其内容包括：   1. 确定可信根及其实现方式，确定底层TPM和TPCM芯片的使用方法 2. 确定可信根在信任链中的位置 3. 由可信根延长信任链，规定信任链的传递方式 4. 根据设计好的信任链，利用TSS对底层硬件编程，实现其与顶层知识图谱平台的对接     图表 3 项目底层逻辑  构建好可信的知识图谱平台后，我们设计能够安全实现知识图谱融合的算法，将两个以上的同源或者异源知识本体合并为一个知识本体。   * 首先，我们利用语法和数据正规化完成数据预处理。包括：   (1) 检索本体数据库确定上位本体来源；  (2) 基于正则表达式解析本体基本属性；  (3) 根据上述信息用算法估算本体相似度。   * 然后通过属性相似度和实体相似度的计算进行记录连接。该过程中有两种重点应用的映射方法：   (1) 基于搜索引擎的语义相似度计算；  (2) 基于图的拓扑结构计算实体节点相似度。   * 由于数据基数的庞大性，我们对给定的知识库中所有实体对做分块以实现连接。 * 最后完成负载均衡阶段，多次Map-Reduce操作来保证所有块中的实体块数目相当。   根据以上设计，在知识融合过程中语义实现、本体匹配的问题的实现可选用多种可信计算机架构，包括：   1. 基于LT技术的可信计算机框架； 2. 基于NGSCB技术的可信计算机框架 3. 可信PC机实现框架；   在确定核心可信根（安全芯片和CRTM）后，整个系统信任链从信任根开始传递，并更好地契合应用场景。    图表 4 项目内容示意图  **3、项目创新特色概述**   1. **深入知识图谱融合过程**   作为用户知识图谱共享过程的保障，本项目在维护知识图谱的搭建、存储安全之外，注意到了当今社会用户日益增长的知识图谱融合安全需求。通过搭建拥有TPCM主动防御机制的可信服务平台，保证用户在进行知识图谱融合操作时不会出现本体不匹配、语义混乱或失义的情况，有效提高平台进行知识图谱融合的安全性、可靠性、稳定性。   1. **基于可信计算3.0搭建信任链机制**   TCG组织研发的TPM2.0已在生产生活领域广泛应用，但其启动晚于CPU BIOS的特性使得安全性存在不确定性。本项目基于我国沈昌祥院士提出的可信3.0思想，从运算和防御并行的双体系思想出发，将TPCM植入可行根源，加以密码学辅助安全验证，以最大限度保证用户知识图谱操作的安全性。   1. **从硬件到顶层设计的全栈式信任链保护**   本项目兼顾底层硬件基础和顶层网页设计，从用户和服务器平台的TPCM芯片出发设置信任根，基于TPCM和TSS接口延长信任链，直到顶层网页设计中与用户的交互，全面、一站式地保证整个知识图谱共享平台的可靠性和完整性，最大程度地实现用户知识图谱操作全过程的安全。  **4、项目研究技术路线**  我们的项目是面向知识图谱平台，针对管理平台服务器设计基于TPCM的可信平台控制管理方案，利用TPCM对系统完整性的保护及对上层应用的加密服务，构建面向知识图谱商业级或工业级应用的主动免疫防御机制来实现知识图谱的构建安全，互融安全及可信可用。     1. 采用vTPCM虚拟端和少量TPCM物理芯片来实现,需要在vTPCM虚拟端上构建类似于TPCM物理芯片的虚拟模块。 2. 确定核心可信根，构造信任链，并根据不同平台的知识图谱存储和融合的过程来设计出能更好的契合应用场景的信任链的传递方式。 3. 根据TCG提出的方便调用TPM功能的体系结构TSS，进行一部分相关操作系统内核的开发与应用进行交互，构建出类似于TSPI这种和C/C++兼容的接口，以此编程使用TPCM。 4. 根据底层的设计，设计一种架构应用在知识图谱融合过程中，包括语义对齐，本体匹配等问题进行实现，并使应用中的功能可以很好地匹配底层的设计。 5. 可视化模块的设计，为了更形象的表示知识图谱在存储和融合时基于TPCM的可信平台控制管理方案是如何确保安全可信并采取主动免疫防御机制的。运用前后端开发的技术设计一个类似于openKG.CN的网页，提供相关用户的可视界面。通过攻击模型测试和时间效率的对比来进行相关功能的评测   **5、研究进度安排**  **1）准备阶段**  2022.05.01 - 2022.05.31：研读相关文献,与指导教师进行沟通,收集、整理各种资料;  **2）算法设计阶段**  202.06.01 - 2022.07.31：研究设计相关算法，确定可信根，构造可信链和基本信任传递方式;  **3）功能实现阶段**  2022.08.01 - 2022.08.31：使用开发相关工具，搭建知识图谱共享平台，实现TPCM的基本功能。  **4）检验阶段**  2022.09.01 - 2022.11.30：检验基本功能，在此基础上拓展TPCM功能；进行安全性评测验收  **5）结题阶段**  2022.12.01 - 2023.04.20：论文及报告撰写  **6、项目组成员分工** | | | | | | | | | | |
| 总体规划与协调：王浩宇  可信根和信任链设计：王浩宇、任家骏、高兴、张思娴、李政睿  TPCM功能具现化：任家骏、高兴、张思娴  可视化知识图谱共享平台搭建：王浩宇、李政睿、任家骏  平台安全性实证分析: 王浩宇、任家骏、高兴、张思娴、李政睿  结题报告撰写：王浩宇、任家骏、高兴、张思娴、李政睿  **四、预期成果（在对应项目后填写明细）**  A、研究报告： 1 篇；  B、论文发表： 0 篇；  C、专利申请： 0 项；  D、产品设计： 1 个；  E、成果实物： 0 个；  F、其它预期成果：无。 | | | | | | | | | | |
| 1. **经费预算**  |  |  |  | | --- | --- | --- | | **项目** | **预算（元）** | **计算依据** | | 设备费 | 1000 | Linux系云服务器租用费用；可视化知识图谱共享平台搭建费用 | | 材料费 | 4000 | TPM和TPCM实物芯片购买费用 | | 测试化验加工费 |  |  | | 燃料动力费 |  |  | | 差旅费 |  |  | | 会议费 |  |  | | 出版/文献/信息传播/知识产权事务费 | 5000 | 知网、万方等数据库查询费用；专家咨询费用；专业技术咨询培训费用；相关书籍资料购置费用 | | 其他 |  |  | | 合计： 10000 （元） | | | | | | | | | | | | | |
| **六、指导教师意见**  签名：  年 月 日 | | | | | | | | | | |
| **七、学院意见**  学院评审委员会（小组）负责人签名： （学院盖章）  年 月 日 | | | | | | | | | | |
| **八、项目负责人承诺：**  **我保证填报内容的真实性。我已阅知并严格遵守天津大学关于大学生创新创业训练项目管理办法和相关财务管理制度规定。本人将按照申报书的内容负责实施本项目，切实保证学习研究时间，认真开展项目工作，及时报告重大情况变动，按时报送有关材料。**  负责人签名：  2022 年 4 月 30 日 | | | | | | | | | | |
| **九、学校推荐意见**  学校负责人签名： （学校公章）  年 月 日 | | | | | | | | | | |