2022年 CCF-华为胡杨林基金

可信计算领域专项

申报方向与课题

CCF-华为胡杨林基金可信计算技术委员会

二零二二 年 四 月 十五 日

下一代可信计算的技术体系

项目背景

随着计算技术的快速发展和网络、个人通信等深度渗透，越来越多的信息（包括涉及安全和隐私的敏感信息）正在从独立的甚至是物理隔离的计算环境迁移到边缘侧和云端。如何保护数据的全生命周期安全成了巨大的挑战，特别是如何保护数据在使用阶段的安全更是成为边缘侧和云端计算面临的安全挑战。基于硬件的可信执行环境（又称机密计算）是解决该挑战的一条可行路径，产业界和学术界在不同的体系架构下，提出了一系列的可信执行环境的框架，包括最初的ARM TrustZone、Intel SGX、AMD SEV乃至最新的RISC-V Keystone等，但是除了TrustZone在移动领域的广泛普及外，在云计算/数据中心领域，以Intel SGX技术为代表的可信执行环境并未得到大规模的普及和应用，即使是移动领域的TrustZone，也只能保护特定高安应用中用户隐私数据的使用（比如指纹、支付等等），无法满足丰富多样的应用及其海量用户数据处理的安全和隐私需求，从技术角度看，限制目前可信执行环境大规模普及的主要技术瓶颈有（1）机密计算软件开发模型；（2）机密计算硬件基础原语；和（3）机密计算信任模型等。

针对这些挑战，需要构建下一代可信计算的技术体系，包含下一代可信执行环境的仿真、硬件实现、新应用以及安全分析等，研究内容包含但不限于以下方向：

研究内容

方向一：下一代机密计算硬件模型、软件开发模型及基础原语设计

在这个方向，我们鼓励申请人抓住开源硬件以及开源芯片设计的大趋势，利用较为成熟的开源硬件项目，实现下一代可信执行环境在硬件平台（比如FPGA平台等）进行实现。同时，我们希望申请人能够面向下一代云/数据中心的计算场景，结合计算架构的演进趋势（比如异构、以数据为中心等），设计下一代机密计算所需的基础硬件原语。

同时，我们鼓励申请人能够面向下一代云/数据中心的计算场景，机密计算的硬件模型，结合机密计算软件模型逐步以应用为中心的趋势，设计下一代机密计算所需的软件开发模型、基础可信软件栈和接口。

方向二：下一代可信执行环境的安全分析和安全增强

可信执行环境本身也面临这各类安全挑战，比如侧信道攻击和错误注入等，目前很多主流的可信执行环境并不具备防御侧信道攻击的能力。那么下一代可信执行环境是否也天然会有这类安全挑战，如何在硬件尚不具备或者只是部分具备地情况下系统性地分析下一代可信执行环境的安全隐患就成了重要的研究方向。同时，在分析安全隐患的基础上，如何进行结构性改进，从软件、硬件、软硬件角度增强可信执行环境的安全性也是这一方向的关注点。

方向三：下一代机密计算的其他基础能力建设

我们鼓励申请人结合自身的研究背景以及学术发展的趋势，提出其他具有创新性的下一代机密计算技术，共同领引机密计算的发展。

异构可信执行环境的交互验证和边界拓展

项目背景：

随着可信执行环境的推广，以及AI等大运算量的应用出现，单一的可信执行环境已经无法满足计算场景所需要的计算资源。虽然增加运算资源本身并不难，但是如何把新增加的计算资源纳入到可信执行环境的安全边界中就成了一项重要任务。面对不断增长的用户计算需求，可信执行环境边界的拓展其重要性甚至高于可信执行环境本身，如何安全可信地拓展这一边界就成为了研究的一个重点。

此领域针对跨平台可信执行环境交互验证和边界拓展，包含不同可信执行环境的交互验证、异构计算场景下的可信执行环境边界拓展等，研究内容包含但不限于以下方向：

研究内容：

方向一：同构和异构可信执行环境的交互验证与拓展

当前不同的厂商和学术界研究人员提出了不同的可信执行环境及其运行平台，如何让运行在不同可信执行环境中的应用能够互相信任，并在这层信任的基础上构建可信的互联互通协议，保证数据在可信执行环境中的安全防护和不同可信执行环境之间的可信传输。在这个技术之上，我们也鼓励申请人考虑对如何对高资源需求、分布式的任务进行划分，优化算法并高效分配到不同的可信执行环境中。

方向二：异构平台上的可信执行环境边界拓展

随着异构算力的普遍化，越来越多的计算，比如AI运算等，都依赖于加速芯片的使用，而这些加速芯片，无论是GPU还是NPU、TPU、FPGA等，并不在可信执行环境的保护范围内。如何将这些算力资源纳入到可信执行环境的边界中，并且能够对异构计算的算力细粒度划分，对故障隔离，保证QoS，学术界已经在开始思考这些问题，也开始提出了一些解决方案。我们鼓励申请人深入这个领域，从任务的角度重新思考这个问题，提出高效的可信执行环境边界拓展方案。

方向三：构建异构可信计算的其他创新技术

在这一方向，我们鼓励申请人结合其自身研究背景和研究兴趣，同时结合产业发展的大趋势，提出新型的异构可信模式，应用于不同的场景，保护从个人隐私到AI模型等的数据安全。

从数据的视角研究下一代可信计算

项目背景

随着社会信息化程度的不断提高，数据正在成为越来越重要的资产，对数据的控制也称为企业的核心竞争力之一。但是数据的广泛采集和使用，也带来了对用户隐私的关注，为了保护数据安全和用户隐私，大量的法律法规在最近一段时间里被颁布出来，从欧洲的GDPR，到中国的个人信息保护法，这些都体现了各国政府对数据安全和用户隐私的重视，同时也对企业如何安全高效地处理海量的用户数据提出了挑战。虽然已经有了各类安全和可信技术，包括可信执行环境，软件沙箱，也包括各类传统的和新兴的密码技术，从普通的加解密，到同态计算、多方计算等。但是这些技术中并没有一个单一的技术能从性能、安全、可信等角度都满足企业的需求，在很多场景下，企业往往要在众多技术中做出选择。如何对这些技术进行拼接和整合，利用各项技术自身的长处，同时避免其弱项，就成了研究的热点。

此领域以应用场景为导向，在符合安全模型的前提下，对不同的信息安全保护方法、算法和技术进行深度融合，实现信息的安全可信处理，研究内容包含但不限于以下方向：

研究内容

方向一：利用密码学拓展可信执行环境的边界

密码学方案已经在信息安全和隐私领域展现了极大的应用潜力，但是目前的主流密码学方案，比如同态计算和多方计算等往往性能受限。基于此，我们鼓励申请人去考虑利用密码学方案拓展可信执行环境的安全边界，保证数据的运算（无论是以明文形式在可信执行环境内部还是以密文形式在密码学框架内部）始终处在受保护的状态下，同时又充分利用各类密码学方案以及可信执行环境的安全能力。

方向二：面向未来非单一信息安全保护的计算环境

在这个方向上，我们鼓励申请人结合其自身研究背景和所处领域，考虑可能的应用场景，可以是现实中存在的场景，也可以是未来很可能会出现的新运算场景。在这些场景中，对受保护信息和受保护运算的安全需求进行梳理，同时选择合适的安全运算场景进行任务分配，都是研究人员需要面对的新挑战。

方向三：传统机密计算和隐私计算技术痛点分析

基于密码学的隐私计算等相关技术已经发展了很多年，但是离实用还有一定距离，特别是性能一直跟不上计算发展的大趋势，从这一个角度出发，我们鼓励申请人针对传统的基于密码学的算法，从实用性角度入手，分析现有算法在各个应用场景下的痛点，深度分析这类痛点的可能解决方法。

硬件安全的新型方法与技术

项目背景

考虑到硬件安全本身是一个很广泛的概念，其主要包括两个方面，一方面是硬件本身的安全性（Security for Hardware），另一方面是用于安全目的的密码硬件设计（hardware for security）。例如，以“幽灵”和“熔断”为代表的一系列利用预测执行和乱序执行的漏洞，给处理器安全敲响了警钟。各类新型的硬件安全隐患也层出不穷，从硬件木马，物理侧信道，调试端口暴露，到硬件的知识产权和芯片全产业链安全等问题，都需要研究人员提出新型的硬件安全方法进行应对。此外，密码原语是硬件安全的基础，然而密码原语的高能效硬件实现面临严重挑战，尤其是后量子时代的密码硬件的高能效实现需要研究人员提出新型硬件加速方法。本项目从security for hardware和hardware for security两个角度关注芯片的安全性问题，尤其关注特别是处理器芯片的自身硬件安全。

研究内容

方向一：片上系统和处理器的硬件形式化验证、安全规范及工具

目前硬件形式化验证工具缺乏系统的安全规范，且存在性能上的瓶颈，无法快速自动对复杂硬件系统进行整体的形式化验证。我们希望申请人能对复杂硬件系统进行建模，提出或利用新型的建模方式保证准确性和有效性并降低形式化分析的开销，实现对整体硬件设计的安全验证与分析；或在开源工具的基础上，开发和迭代适用于硬件设计的形式化验证框架与工具，提高验证的自动化程度；或针对现有不同类别的形式化验证框架，系统化地整理硬件安全形式化验证所需要的安全规范，清晰的定义这些规范的保护范围，为多种框架的横向比较以及芯片安全的等级划分做铺垫。

方向二：非传统密码的计算加速

非传统密码，比如后量子密码、同态算法等，正受到越来越多的关注。而传统硬件实现方法，受制于存算分离的冯·诺伊曼架构，难以显著降低大规模数据搬运带来的巨大功耗与性能开销，不能满足资源受限情况下的加解密计算需求，新型的硬件加速方法，比如数字存内计算、专用硬件等方式目前仍具有较高计算复杂度。基于此，我们鼓励申请人开展对非传统密码的计算硬件加速的研究，提出高能效的密码算法、软件或硬件的加速方法，为物联网、大数据时代的网络空间安全保驾护航。