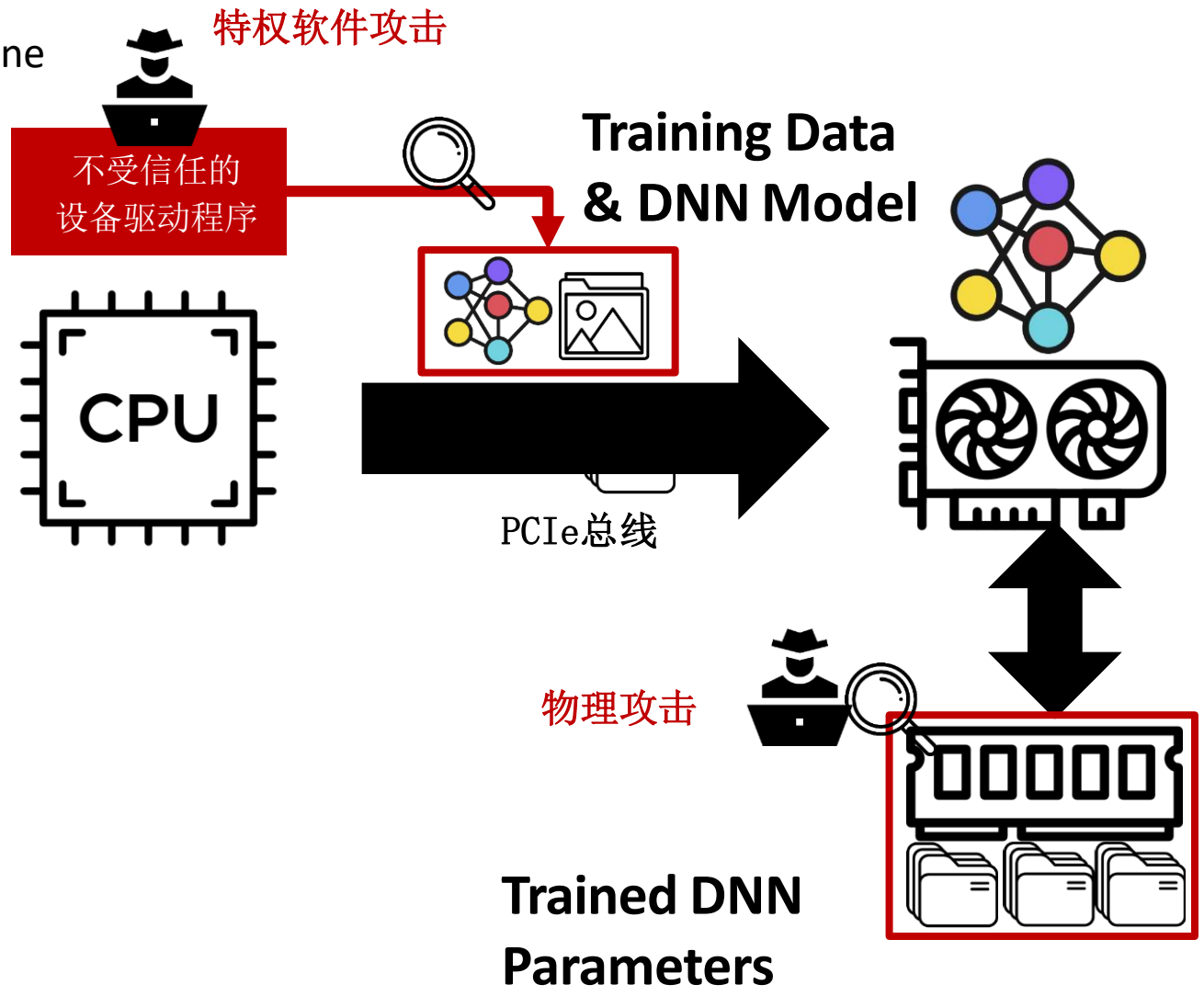
Common Counters: Compressed Encryption Counters for Secure GPU Memory

汇报人：王道宇

華中科技大學
Huazhong University of Science and Technology

GPU计算的安全性需求

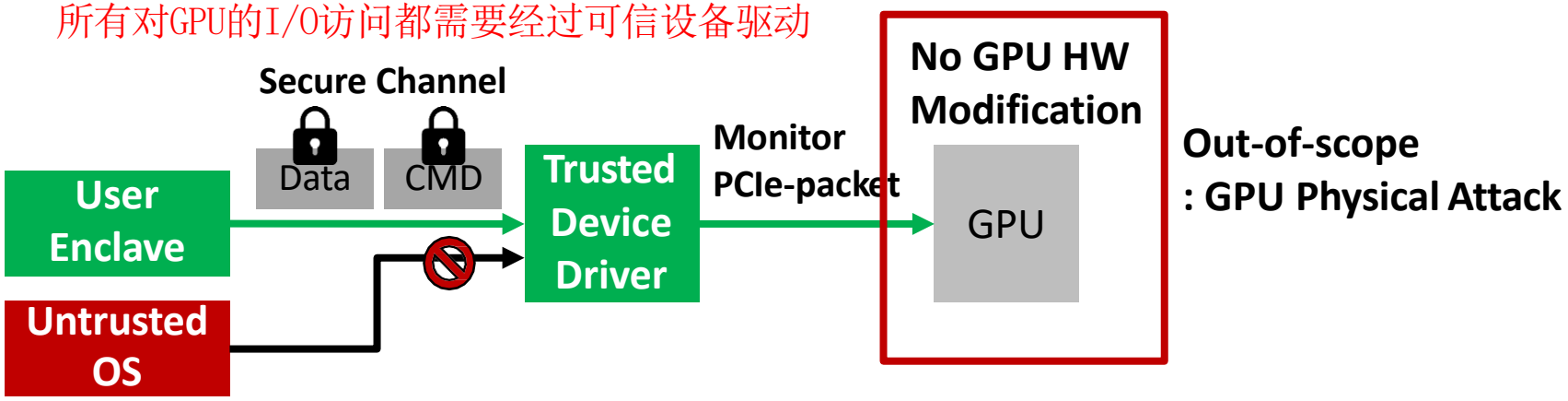
- 可信执行环境（TEE）
  - Intel SGX, ARM TrustZone
- 现有的可信执行环境没有考虑GPU



之前的工作：HIX & Graviton

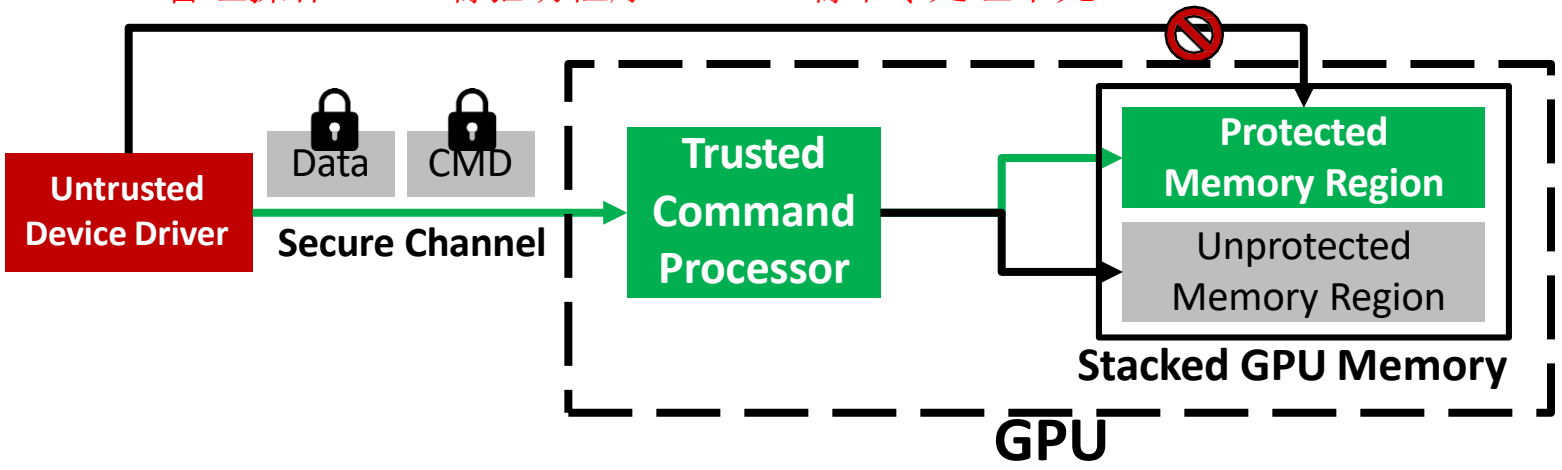
- HIX: 保护从CPU到GPU的I/O通路

所有对GPU的I/O访问都需要经过可信设备驱动

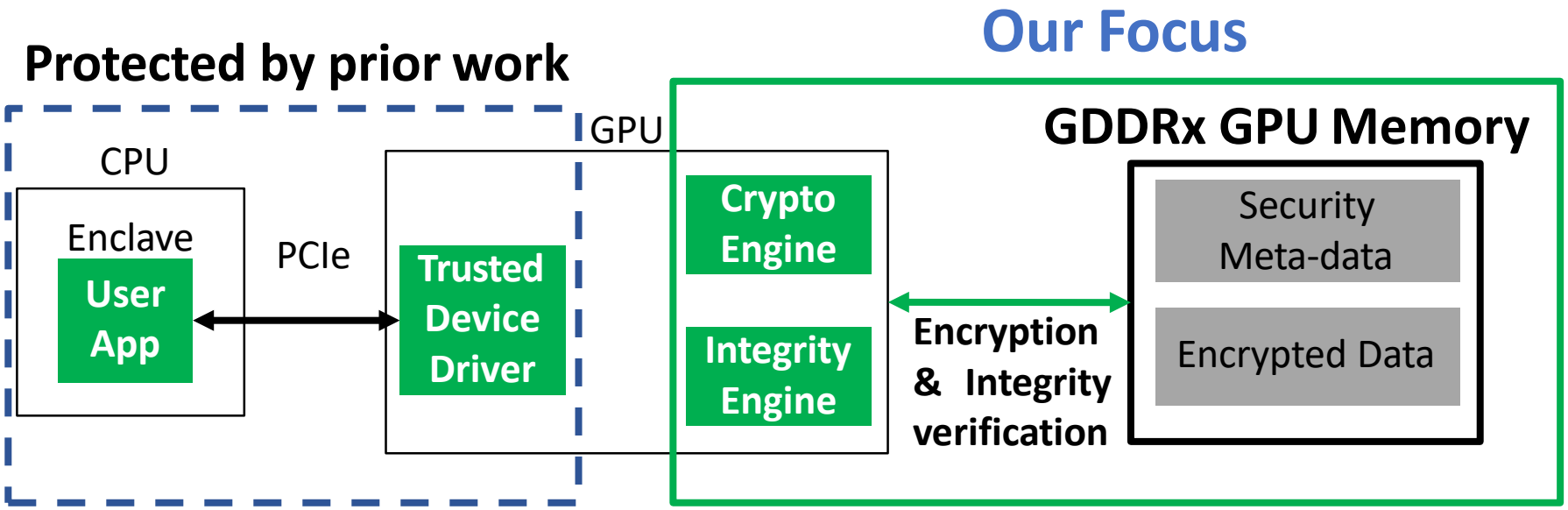


- **Graviton:** 改变GPU硬件

GPU管理操作：CPU端驱动程序 -> GPU端命令处理单元



目标：GPU内存安全



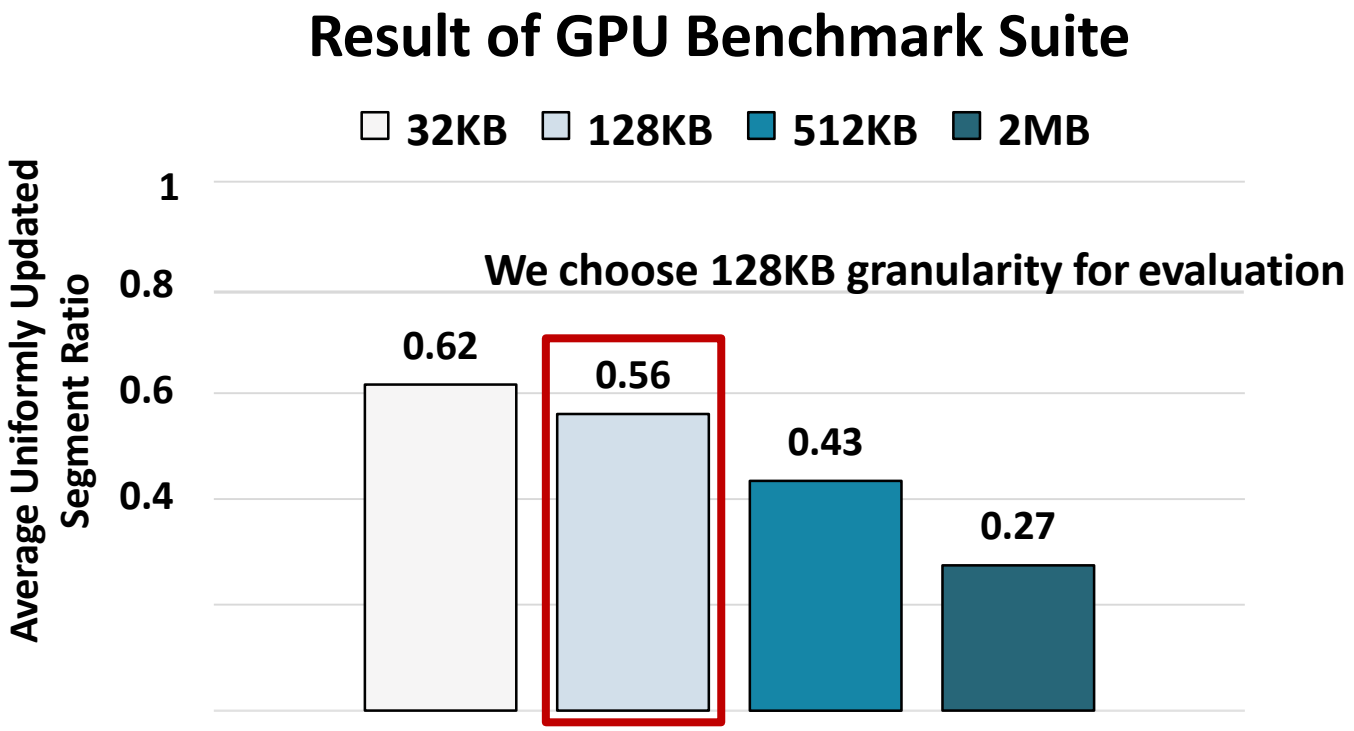
主要贡献：

- 以较低的性能开销实现GPU内存安全
- 利用了GPU应用独特的内存更新行为
- 将平均性能开销降低到2.9%

威胁模型与假设

- 威胁模型
  - 攻击者可以完全控制操作系统和其他特权软件
  - 攻击者可以对暴露的系统组件进行物理攻击
- 可信计算前提
  - GPU软件运行在GPU上
  - 用户应用程序运行在CPU Enclave中

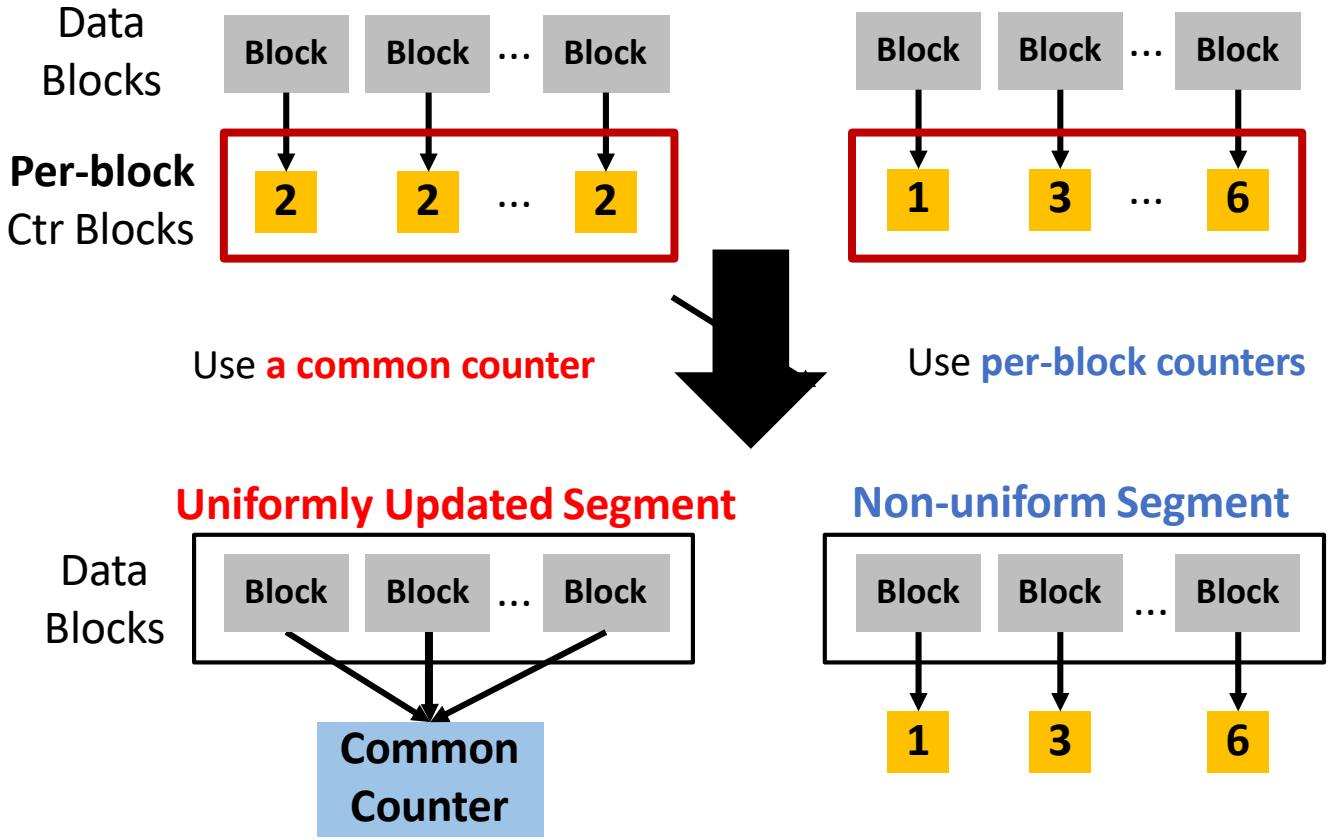
观察：GPU应用写特性



观察1：GPU应用倾向于统一更新内存
观察2：有不同计数器值的块数量很少

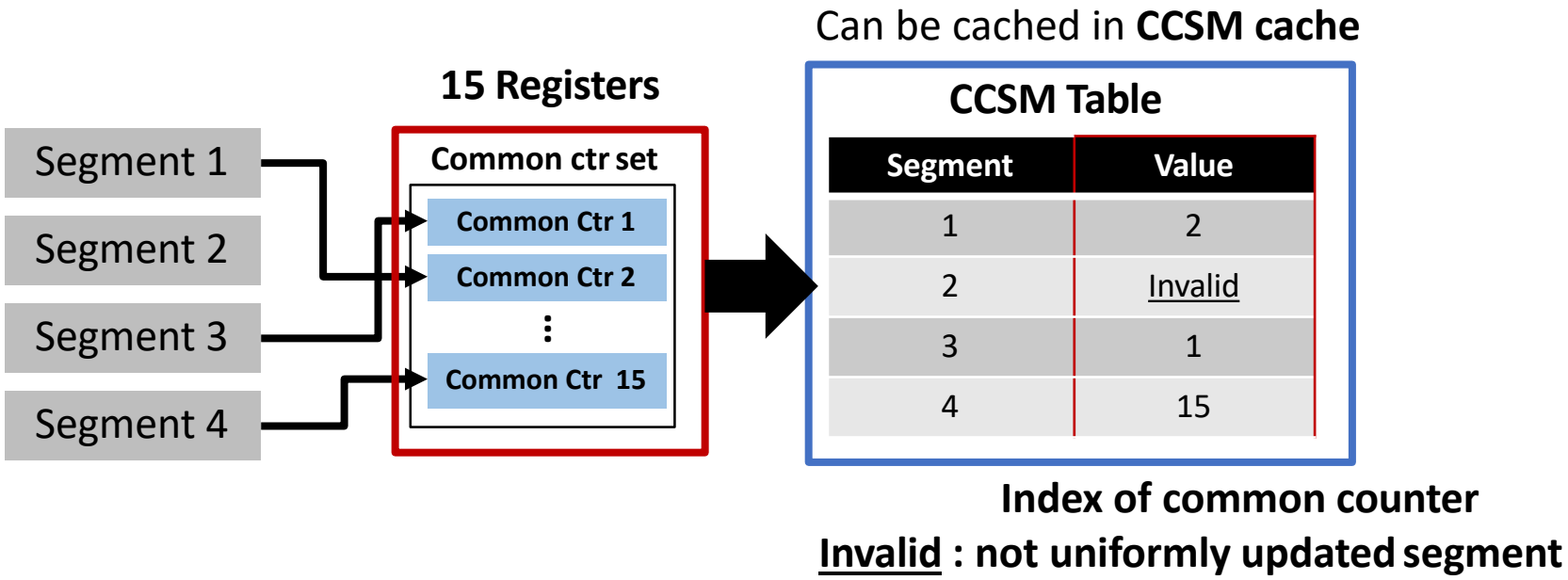
主要思想

- 为一致更新的段使用粗粒度计数器

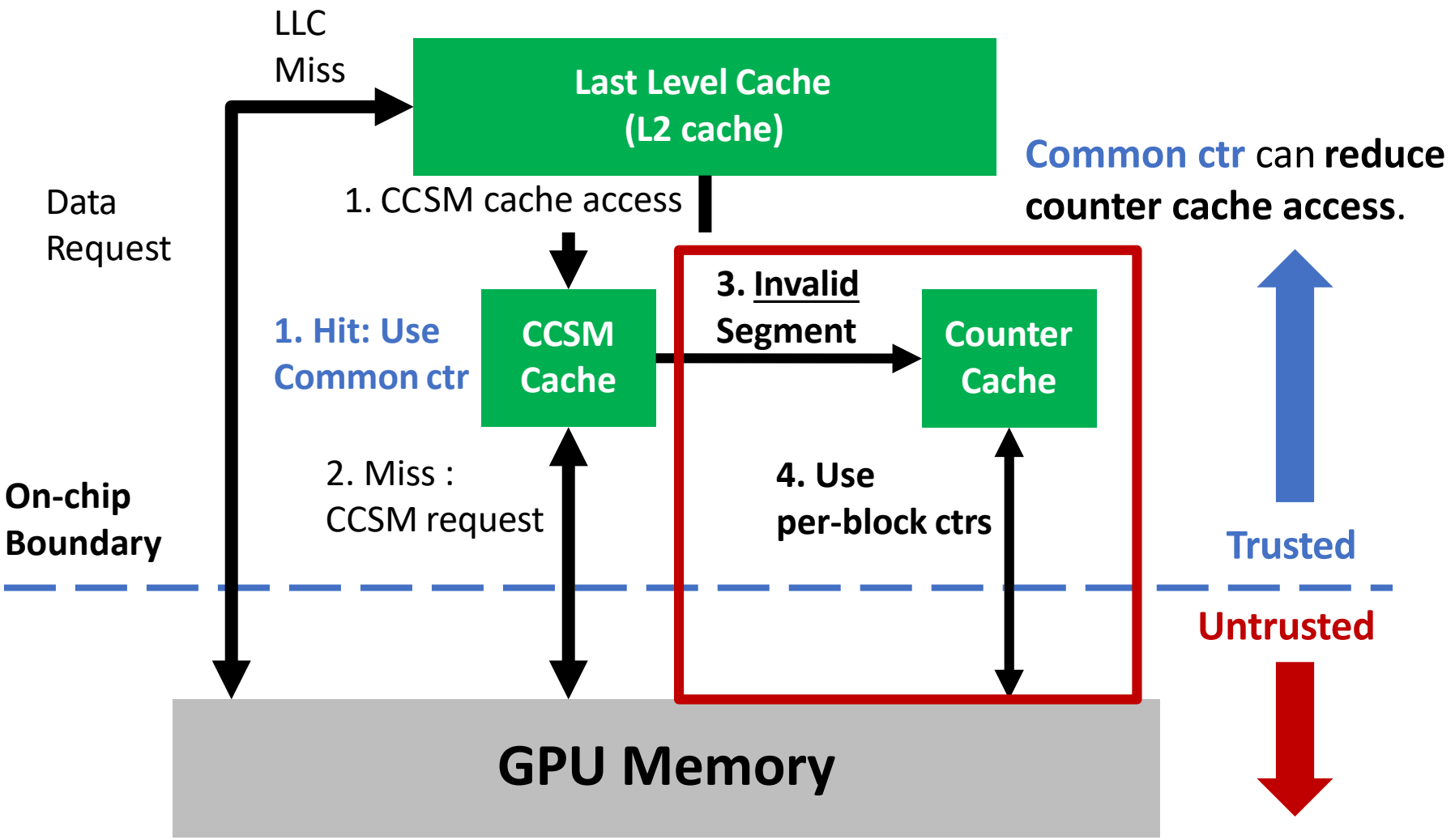


Finding Uniformly Updated Segments

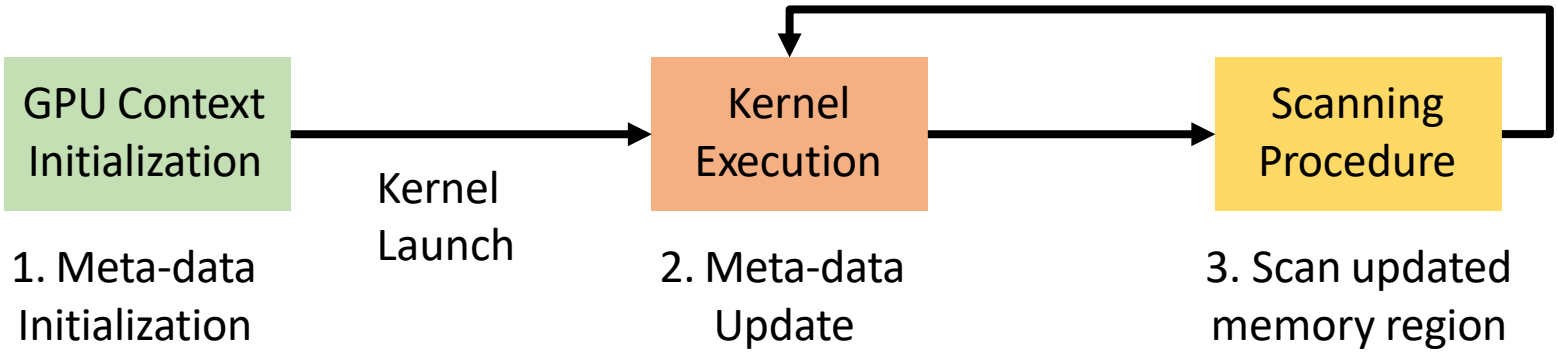
- 公共计数器状态映射(CCSM)
  - 检查内存段是否使用了公共计数器

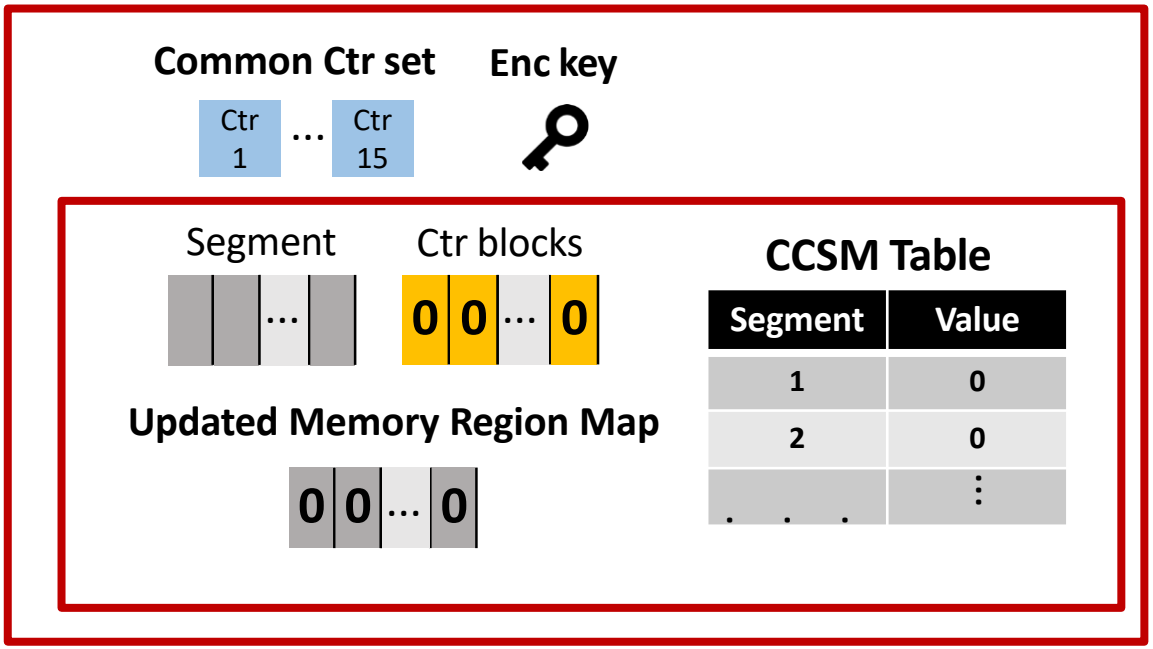


上级缓存缺失处理


LLC
Miss
Last Level Cache
(L2 cache)
Common ctr can reduce
counter cache access.
Data
Request
1. CCSM cache access
3. Invalid
Segment
1. Hit: Use
Common ctr
CCSM
Cache
Counter
Cache
2. Miss :
CCSM request
4. Use
per-block ctrs
On-chip
Boundary
Trusted
Untrusted
GPU Memory

GPU Execution with Common Counter





结论

- 结果
  - Common Counter将平均性能开销降低到2.9%
- 问题
  - Memory encryption 是GPU内存安全的关键瓶颈之一