处理器缓存侧信道防御的现状与展望

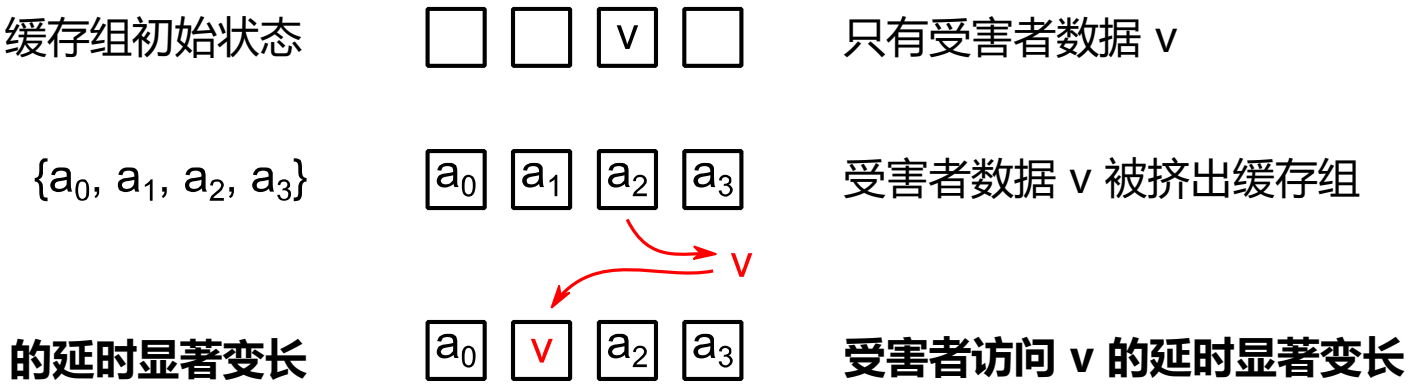
宋 威

北京科技大学
计算机与通信工程学院
网络空间安全系

第五届青年教师学术论坛 2026年10月23日

缓存侧信道攻击

攻击者通过执行看似无害的代码，利用目标缓存上的执行痕迹获得敏感信息的攻击方式即为**缓存侧信道攻击。**



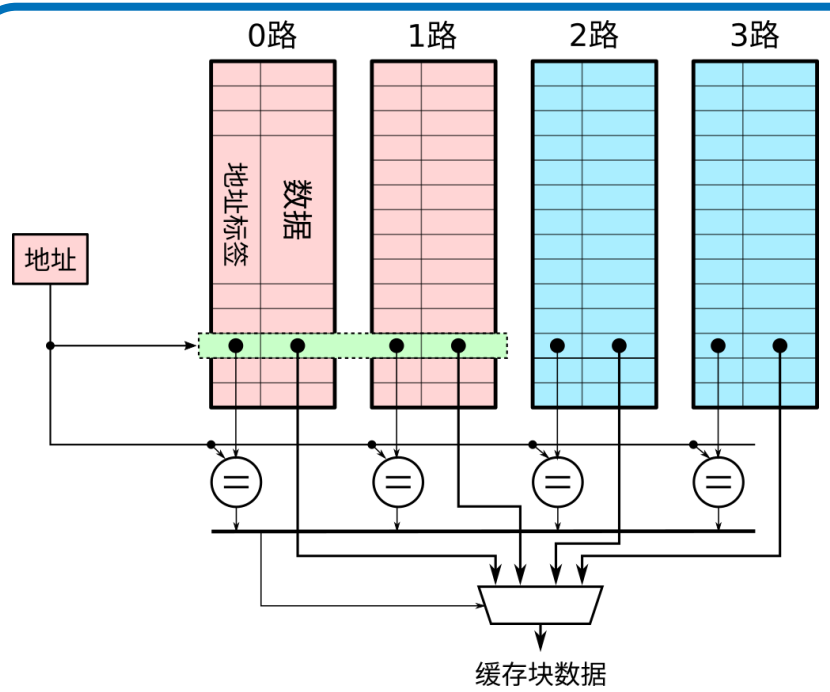
- 正常情况下，受害者的目标数据 v 在缓存命中
- 攻击者通过访问一个驱逐集 $\{a_0, a_1, a_2, a_3\}$，强迫将 v 挤出缓存.
- 如果受害者访问 v ，访问延时变长，攻击者访问驱逐集的时间也变长。

重用型攻击：Flush+Relod，利用冲刷指令直接驱逐目标数据 v 。
冲突型攻击：Prime+Probe，利用驱逐集挤走目标数据 v 。
占用型攻击：没有精确控制，以整个缓存为目标。

- 直接发起攻击泄露信息
- 恶意监控（同驻检测、执行指纹）
- **复杂攻击的关键步骤**（瞬态执行漏洞）
- **架构逆向**（预取、TLB、一致性、总线）

2024-2026 CCF-A类顶会共发表微架构漏洞类文章192篇，其中缓存侧信道相关82篇，占比42.7%。

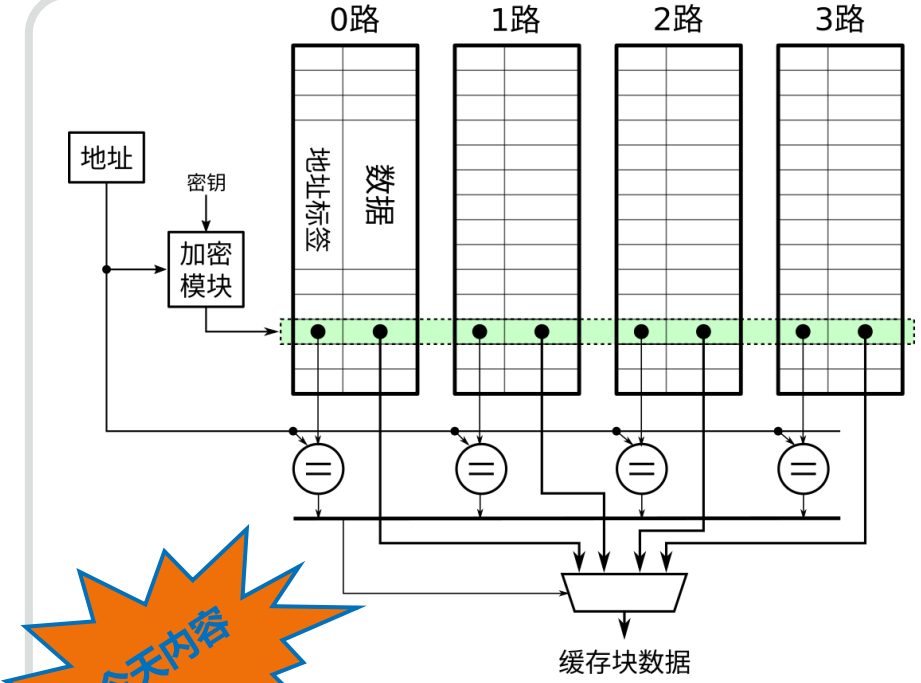
缓存侧信道防御



缓存隔离

将缓存按组或路分区，不同区不冲突，阻止跨区侧信道。

代表设计：Intel CAT (2014)



今天内容

缓存随机化

随机化地址到缓存组的映射，阻挠攻击者控制缓存组，从而阻止侧信道攻击。

代表设计：佐治亚理工
CEASER-S (2019)，MIRAGE (2021)

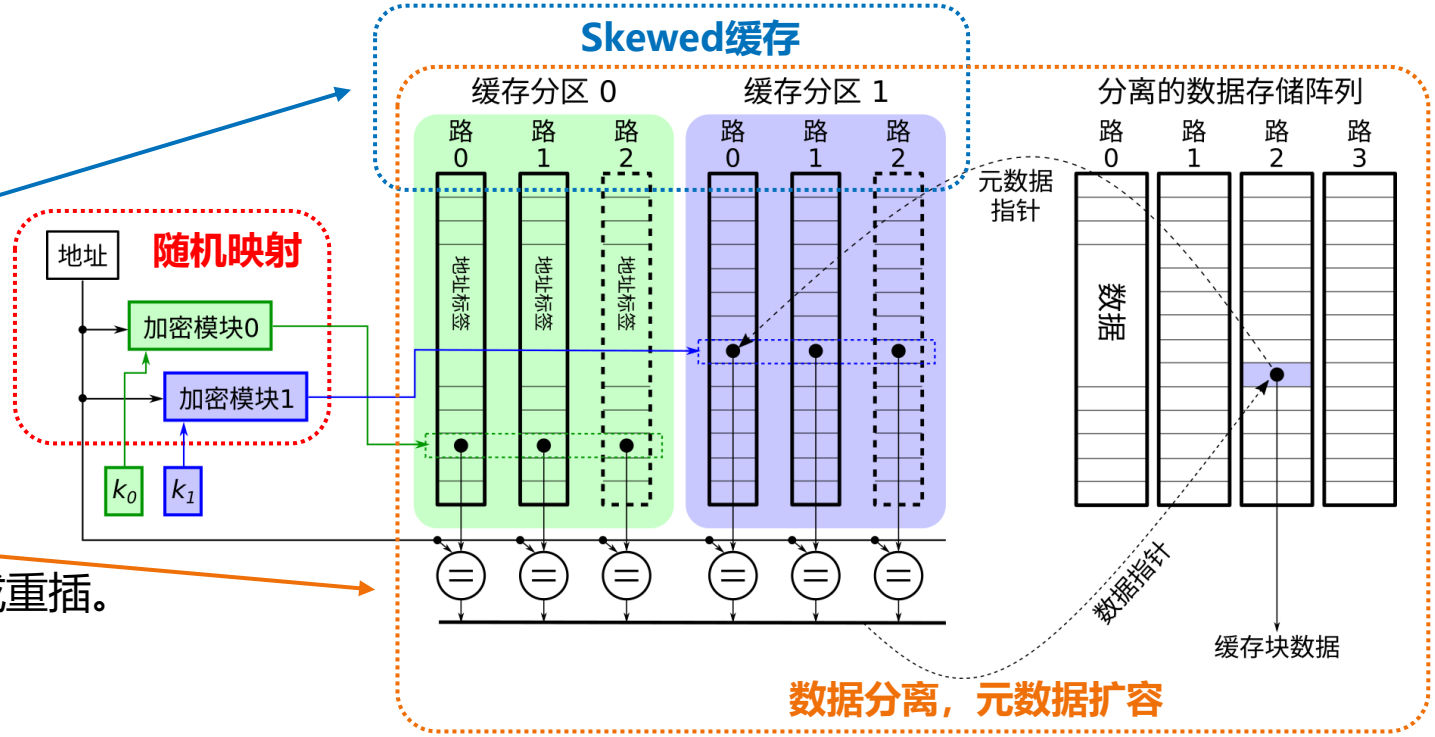
其他辅助防御

- **攻击检测**
在线检测侧信道攻击。
- **数据预取**
关键数据提前预取。
- **物理隔离**
关键程序使用专有硬件、专有缓存或者不适用缓存。

MIRAGE: 缓存随机化的SoTA设计

发展阶段

1. **随机映射** (2007-2019)
   随机化地址到缓存组的映射。
   普林斯顿，佐治亚理工，信工所
2. **随机插入** (2018-2021)
   为新插入缓存块提供多个缓存组。
   佐治亚理工，Graz科技，浙大，信工所
3. **全局随机置换** (2021-2026)
   被驱逐缓存块与冲突缓存组解耦，全局置换或重插。
   佐治亚理工，Intel，维吉尼亚，信工所



完全阻止了冲突型侧信道攻击。

面积上升>20%，功耗上升~20%，缓存命中率下降~3.5%，运行时性能下降>2%。

对现有缓存架构的改动时破坏性的（Skewed缓存，元数据和数据分离）

G. Saileshwar, M. Qureshi. MIRAGE: Mitigating Conflict-Based Cache Attacks with a Practical Fully-Associative Design. USENIX Security, 2021.

我们的贡献（原信工所工作）

坚持使用最基本的多路组相联缓存结构，保安全，降代价。

发展阶段

1. **随机映射**（2007-2019）

   随机化地址到缓存组的映射。

   普林斯顿，佐治亚理工，信工所

RAID-2019:
指出CEASER假设错误

2. **随机插入** (2018-2021)

   为新插入缓存块提供多个缓存组。

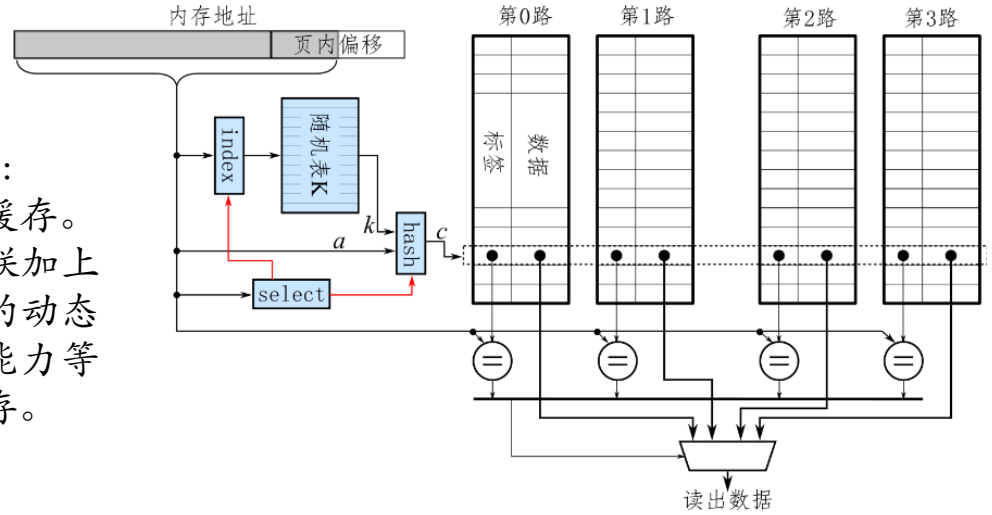
   佐治亚理工，Graz科技，浙大，信工所

3. **全局随机驱逐** (2021-2026)

   被驱逐缓存块与冲突缓存组解耦，全局置换或重插。

   佐治亚理工，Intel，维吉尼亚，信工所

IEEE S&P-2021:
不需要Skewed缓存。
传统多路组相联加上攻击检测驱动的动态重随机，防御能力等同于Skewed缓存。



IEEE TC 2024:
实现于Rocket-Chip处理器，第一个末级缓存随机化的处理器实现。
面积上升2.8%，功耗上升2.5%，缓存命中率下降0.8%，性能下降0.9%

IEEE S&P-2026:
仍然使用传统多路组相联缓存，安全性能略高于MIRAGE.
面积上升3.7%，功耗上升3.4%，**缓存命中率上升~11%（第一次）**

W. Song, P. Liu. Dynamically finding minimal eviction sets can be quicker than you think for side-channel attacks against the LLC. RAID, 2019

W. Song, B. Li, Z. Xue , Z. Li, W. Wang, P. Liu. Randomized last level caches are still vulnerable to cache side-channel attacks! But we can fix it. IEEE S&P, 2021

W. Song, Z. Xue, J. Han, Z. Li, P. Liu. Randomizing set-associative caches against conflict-based cache side-channel attacks. IEEE Transactions on Computers, 2024, 73(4): 1019 – 1033

W. Song, Z. Wang, J. Han, D. Xie, H. Ma, P. Liu. SeqAss: Using sequential associative caches to mitigate conflict-based cache attacks with reduced cache misses and performance overhead. IEEE S&Privacy, 2026

SeqAss: 高安全的串行关联缓存随机化（S&P26）

- 利用**串行关联**实现**负载平衡**的随机插入

  预测器正确率~90%，相比Skewed缓存仅引入10%的访问延时代价；

  基于负载计数器的负载估计和均衡免去了Mirage高达20%的面积。

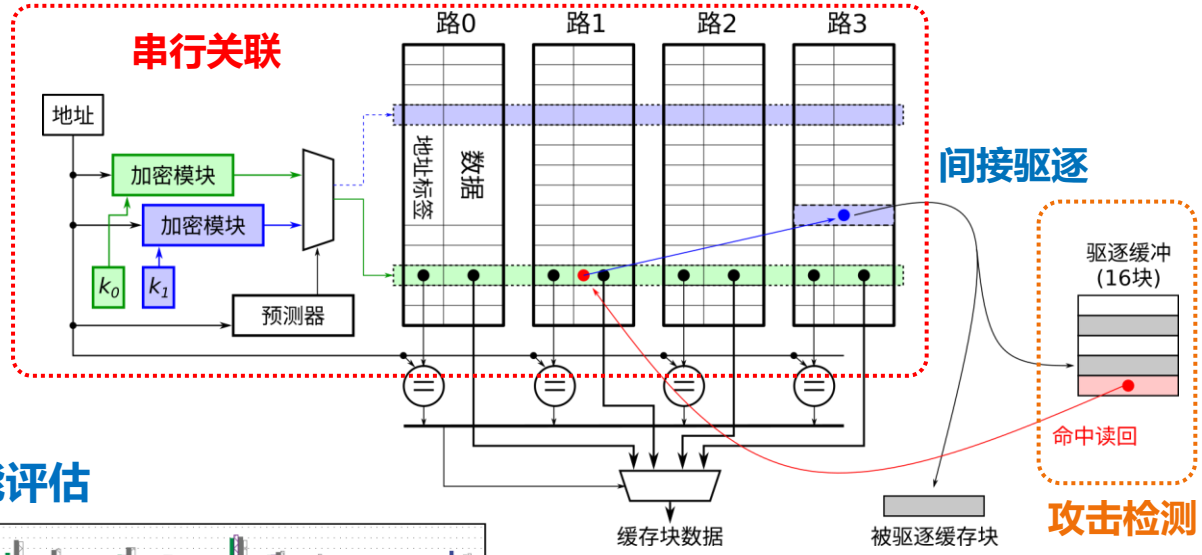
- 利用部分重定位实现**按需间接驱逐**

  盲目支持间接驱逐可导致高达60%的动态功耗增长；

  仅对高负载缓存组进行重定位将动态功耗代价降至26%。

- 提出基于**驱逐缓冲器**的**攻击检测**电路

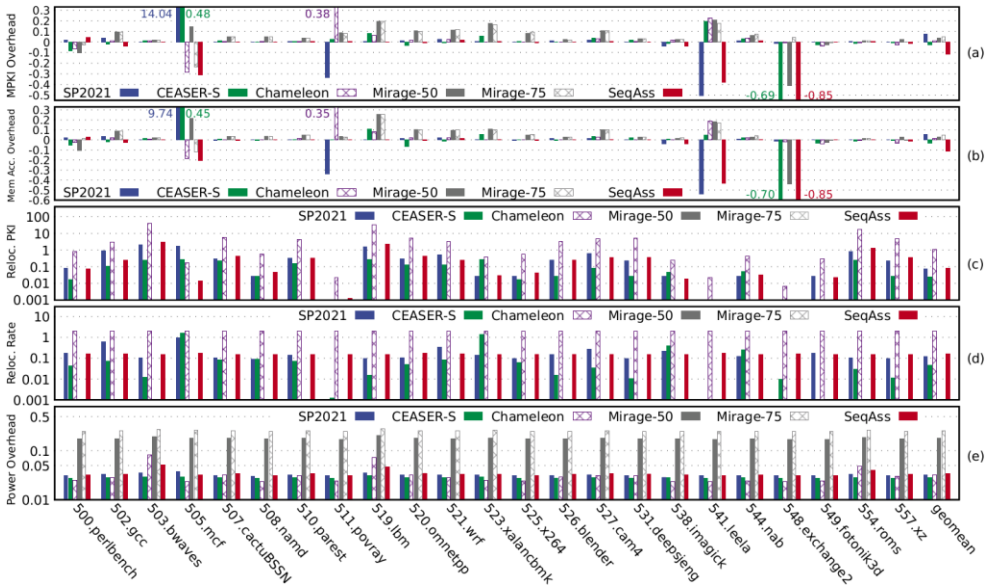
  减少时间差，在受攻击的时候更换加密密钥。

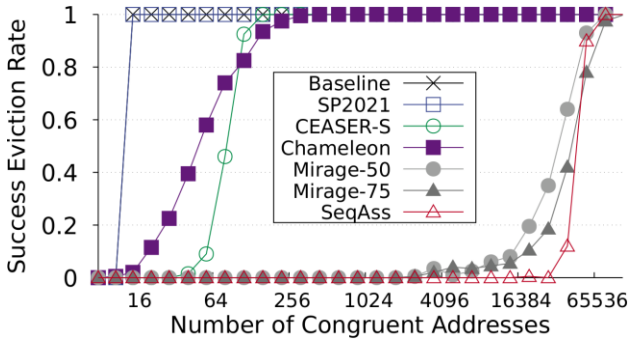


	SeqAss	Mirage
攻击地址数:	48K	30K
存储面积代价:	3.7%	22%
功耗代价:	3.4%	21%
动态功耗代价:	26.1%	61.2%
缓存缺失率:	-11%	2.3%

安全性能提升，
性能全面优于MIRAGE，
缓存缺失率不升反降！

性能评估

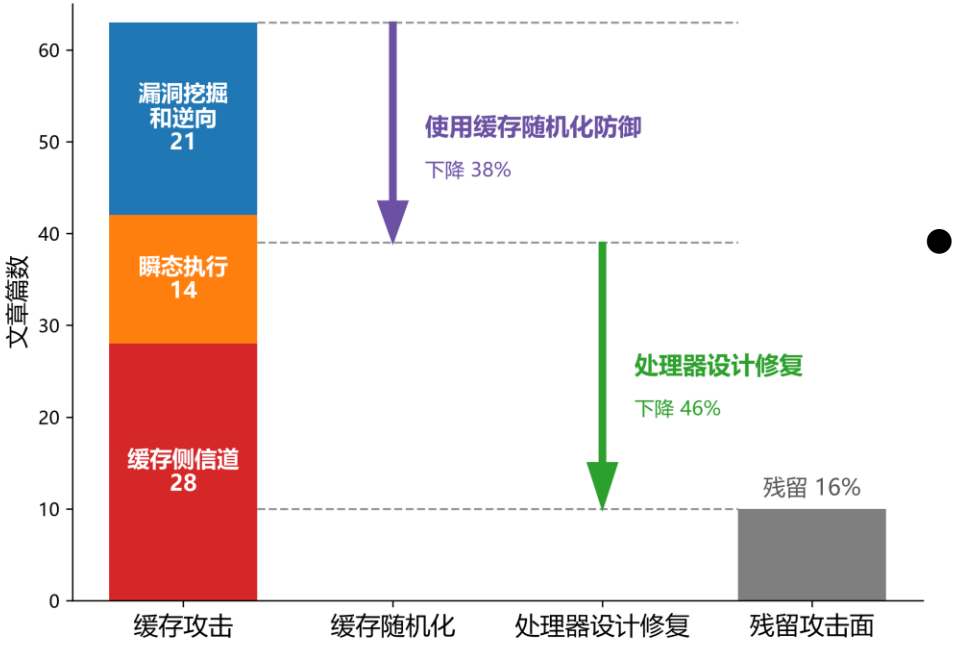


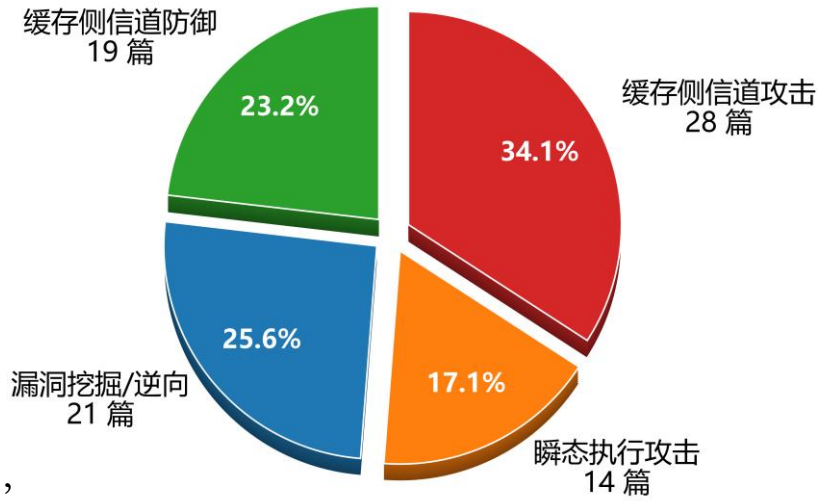


高安全强度略高于Mirage

近年来的研究领域进展（2024至今）

- 统计从2024年到现在安全和体系结构顶会（9个会议）的所有论文（6306篇）
  - 安全(S&P, Security, CCS, NDSS), 体系机构(ISCA, MICRO, HPCA, ASPLOS), 外加DAC
  - 合计缓存安全相关**82篇**，2024：**29篇**，2025：**30篇**，2026：**23篇**（部分）
  - 各类攻击63篇，占比77%，其中传统缓存侧信道攻击占44%，新型攻击占56%。





- 具体分析所有攻击类文章
  - 60%的攻击来源于处理器设计缺陷，可以通过处理器的软硬件简单修复阻止。
  - 大部分的缓存侧信道攻击和一部分的新型攻击在全面使用缓存随机化加固整体缓存架构后失效。
  - **如果全面实施缓存随机化防护，攻击面下降38%，加上处理器的简单漏洞修复，攻击面缩小至16%!**

除了处理器修补漏洞之外，缓存随机化是唯一成建制的防御方案。

- 缓存随机化防御的文章一共5篇，只有一篇来自中国（我们的IEEE S&P 2026）

直至现在的专利情况

- 统计至今为止的所有缓存架构相关专利（201件）
  - 从2018年幽灵和熔断之后猛增，年均20~30件。
  - 大部分为CPU专利（195件），其余皆为GPU（6件）。
  - 缓存硬件防御相关专利共55件，占比27%。

- 缓存硬件防御相关专利（55件）
  - 主要是海外专利（42件），中国专利13件，仅占比24%。
  - 海外专利主体大部分为企业（34件，81%），
    中国大部分为大学和研究机构（12件，92%）。
  - Intel和Microsoft已经成为主要专利所有者，大部分专利已授权，
    部分扩展欧洲和中国覆盖，中国专利基本都为中国独有。

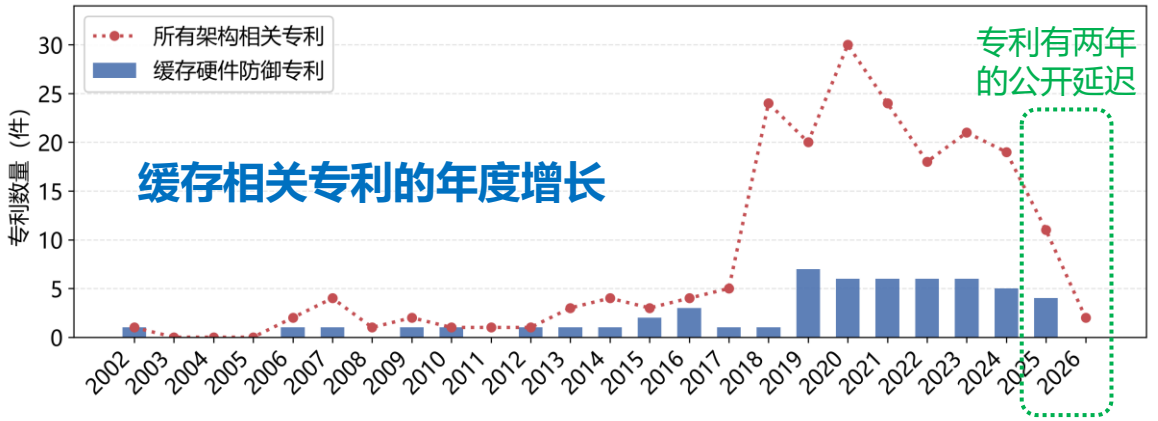
- 缓存随机化相关专利（19件）

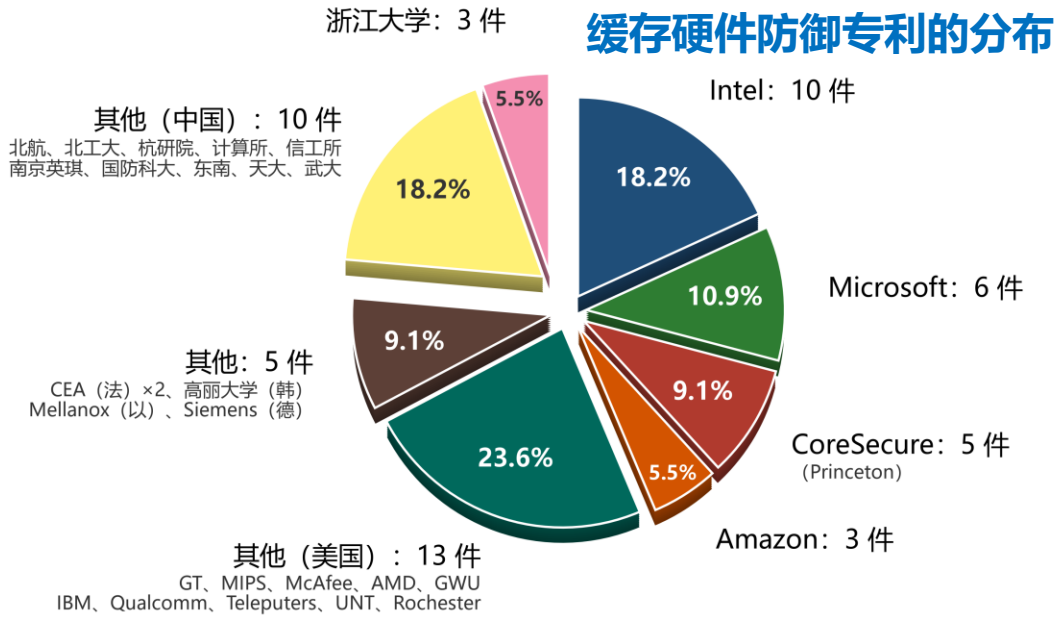
  Intel 6，Amazon 3，**浙大 2**，CEA 2 (法国)，其他6件皆为海外

  US11791978B2, US11620238B2, US20250217295A1, US20250103512A1, US20230350814A1, US12001346B2, CN114647872A, US20170285976A1, US10102375B2, CN110442469B, CN114186226B, EP4180974B1, US12339787B2, US11003594B2, US11550715B2, US20240427884A1, US12229248B1, US9396135B2, US11972034B1

SeqAss的主要技术均不存在专利冲突。

中国企业明显滞后！





未来的研究展望

缓存随机化技术已经可用，Intel已布局，我们拥有较新的技术，但国内企业动力不足。

- 寻找国内企业落地的机会
- 扩展保护到L1和TLB
  - L1和TLB体积较小，直接随机化的安全能力不够，代价不可忍受
  - 考虑将L2联合考虑，建立非包含的随机缓存系统
- 利用现有技术扩展研究范围
  - 已具备缓存分析的能力，可用于缓存安全评估。
  - 内建高速行为级缓存仿真器，可用于缓存一致性相关的硬件漏洞挖掘
- 非常希望能建立合作，扩展研究领域
  - 内存安全防御是我的另外一个主要研究方向。
  - 处理器漏洞的智能挖掘，处理器内存安全防护，面向体系结构研究的智能体，等等。

个人介绍

宋威，9月份刚入职网络空间安全系，教授。处理器安全架构，缓存安全、内存安全。

之前就职于中国科学院信息工程研究所，网络空间安全防御全国重点实验室，研究员，博士生导师。2020年入选中国科学院率先行动“百人计划”青年项目。曼彻斯特大学高级处理器研究小组博士、博士后，剑桥大学处理器架构小组的博后，剑桥lowRISC开源多核RISC-V项目硬件负责人，RISC-V基金会主席Krste教授曾撰写中科院百人推荐信。发表论文50余篇，英文专著一本，CCF和IEEE高级会员，Journal of Computer Security编委会成员。

wsong83@ustb.edu.cn　　13520522084

2026年—至今：　**北京科技大学**，计算机与通信工程学院，网络空间安全系，教授。
2017年—2026年：**中国科学院信息工程研究所**，网络空间安全防御重点实验室，副研究员，研究员。
2014年—2017年：英国**剑桥大学**计算机实验室，博士后副研究员（Research Associate）。
2011年—2014年：英国**曼彻斯特大学**计算机系，博士后副研究员（Research Associate）。
2007年—2011年：英国**曼彻斯特大学**计算机学院，计算机博士（英国EPSRC全奖）。
2005年—2008年：**北京工业大学**自动化系，工学硕士（保送）。
2001年—2005年：**北京工业大学**自动化系，工学学士。



宋威
北京 海淀

扫二维码，添加我为朋友。

感谢各位老师的聆听！