

自我体会之创新的难度

宋 威 2023年5月16日 中国科学院大学雁西湖校区

我是谁？

我叫 宋威

中国科学院信息工程研究所 副研究员 博导
研究计算机体系结构安全

教师家庭，父母是大学文科老师

华中师范大学附属小学

华中师范大学第一附属中学 (平行班垫底)

人民大学附属中学

北京工业大学电子信息与控制工程学院 (清华没考上，自动化，本科、硕士)

曼彻斯特大学计算机学院 (计算机，异步电路设计，博士、博后)

剑桥大学计算机实验室 (博后)

2017年回国

讲什么？（讲故事）

收到邀请，可以讲“科研、论文、工作、学校的申请”：

以我自己的真实经历，讲讲我脑中的科研。

自认为的“我”：

- 容易满足的人：不争第一，只争第二。
- 好奇宝宝：什么都想懂，太难学不会，但仍喜欢刨根问底。
- 习惯性动物：一个事情能坚持做很久。
- 固执顽强：打不死的小强。

我不擅长什么：

- 人际关系、挣钱、理论研究

自觉得擅长什么：

- 拓展性的**创新研究**。

创新是什么？

第一个做出一个能够**推动现有科技**的研究工作。

- **新**：第一个
- **创**：推动现有科技
- **推**：被人接受

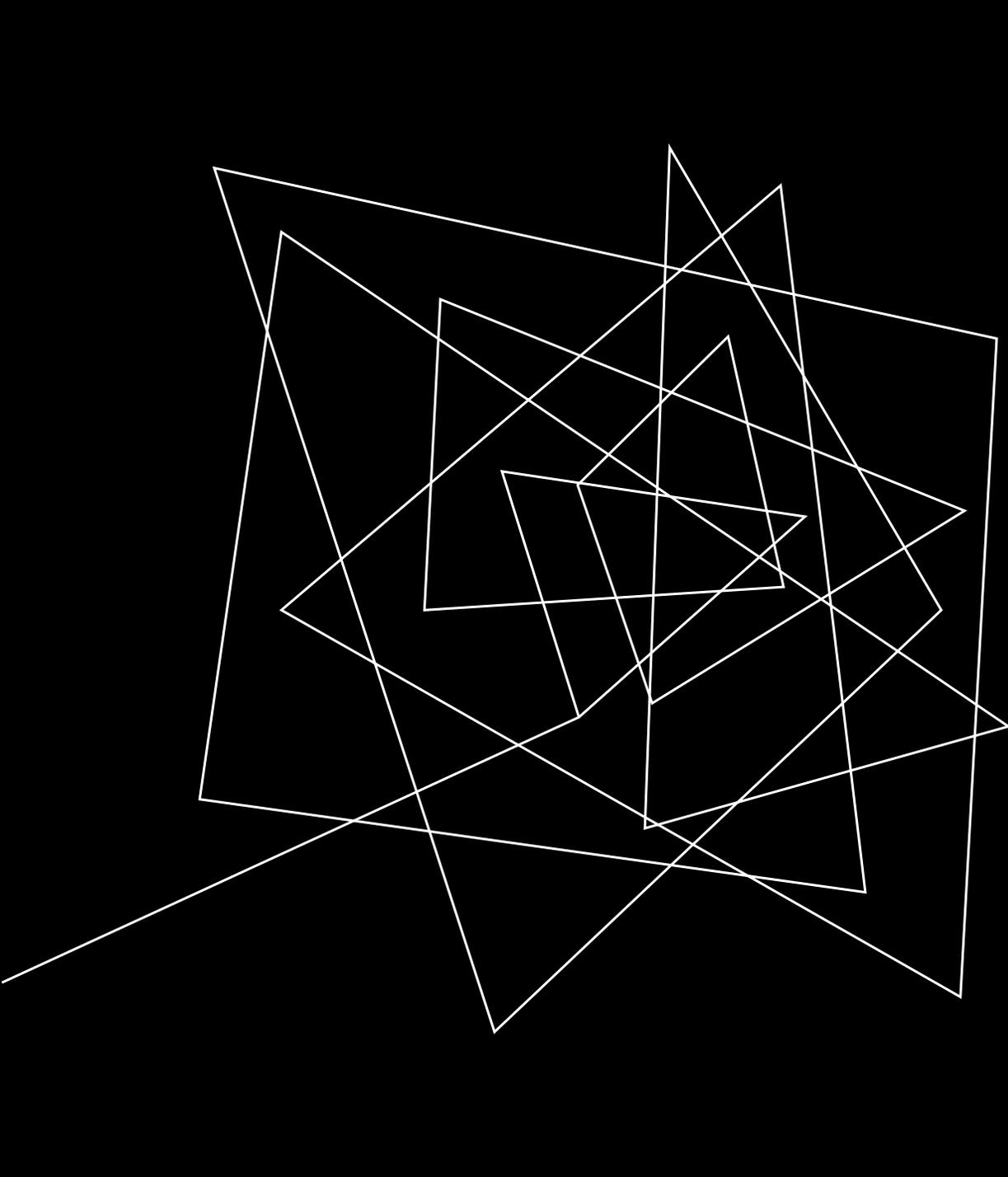
今天我讲两个故事

感谢带我一路走来的人：

硕士生导师，北京工业大学 **方穗明** 副教授，关门弟子。

博士生导师，曼彻斯特大学 **Doug Edwards** 副教授，关门弟子。

宾州法尼亚州立大学的 **Peng Liu** 教授，总是能提出让我郁闷的问题。



第一个故事：

时间：2013年至2016年

地点：英国

事件：基于归并排序算法的
硬件并行排序器设计

初始创新：找到问题

2013年夏天，业余时间参与欧盟AXLE项目，大型数据库的硬件加速。

我尝试解决的问题：**加速排序算法。**

当时的技术水平：**串行归并排序** (FPGA'11 Koch et al. "*FPGASort*")

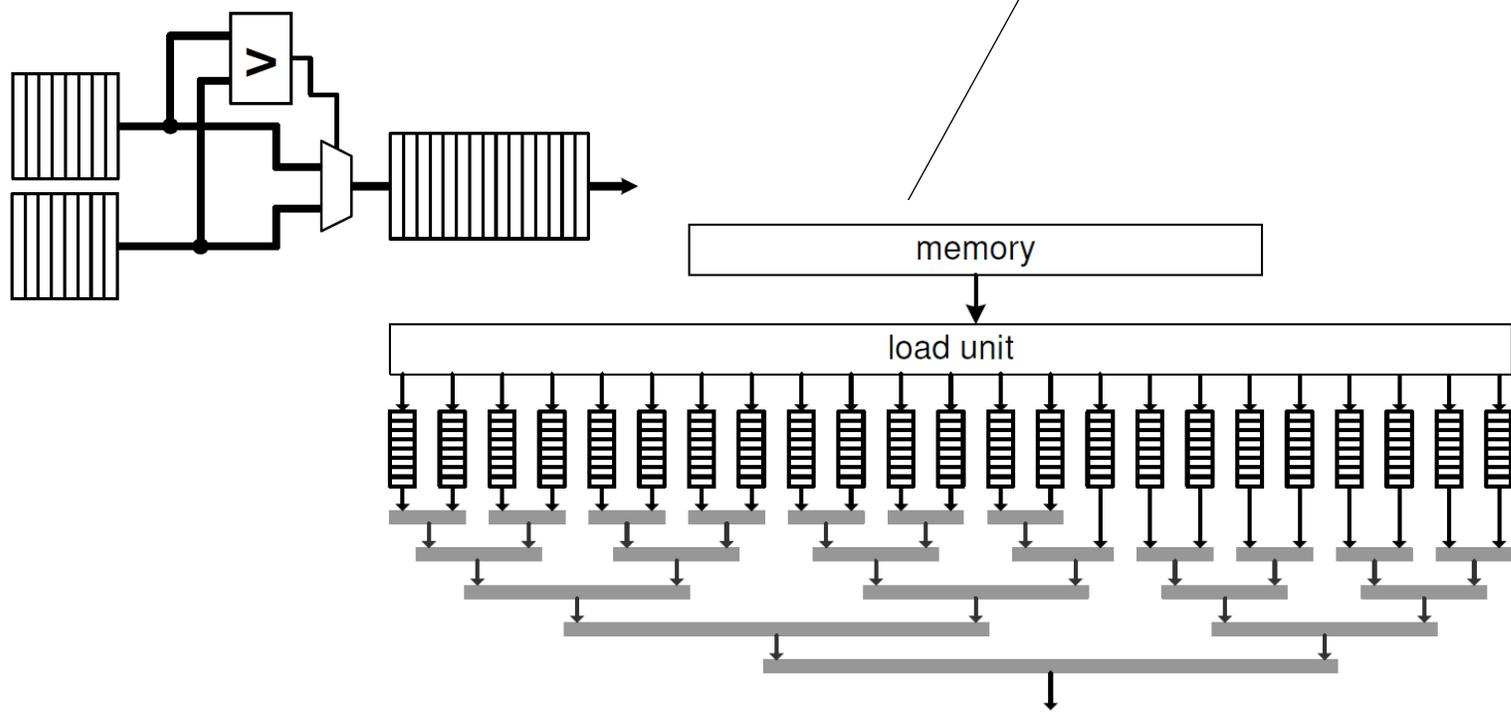
双端口：单个二输入排序器

$$T = f \cdot N \cdot \log_2 N$$

多端口：树形结构多排序器

$$T = f \cdot N \cdot \log_W N$$

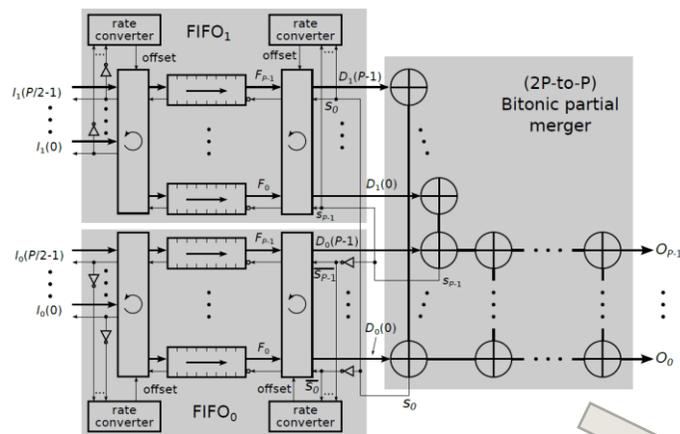
问题：**串行排序器出口带宽受限!**



初始创新：解决问题

解决思路：

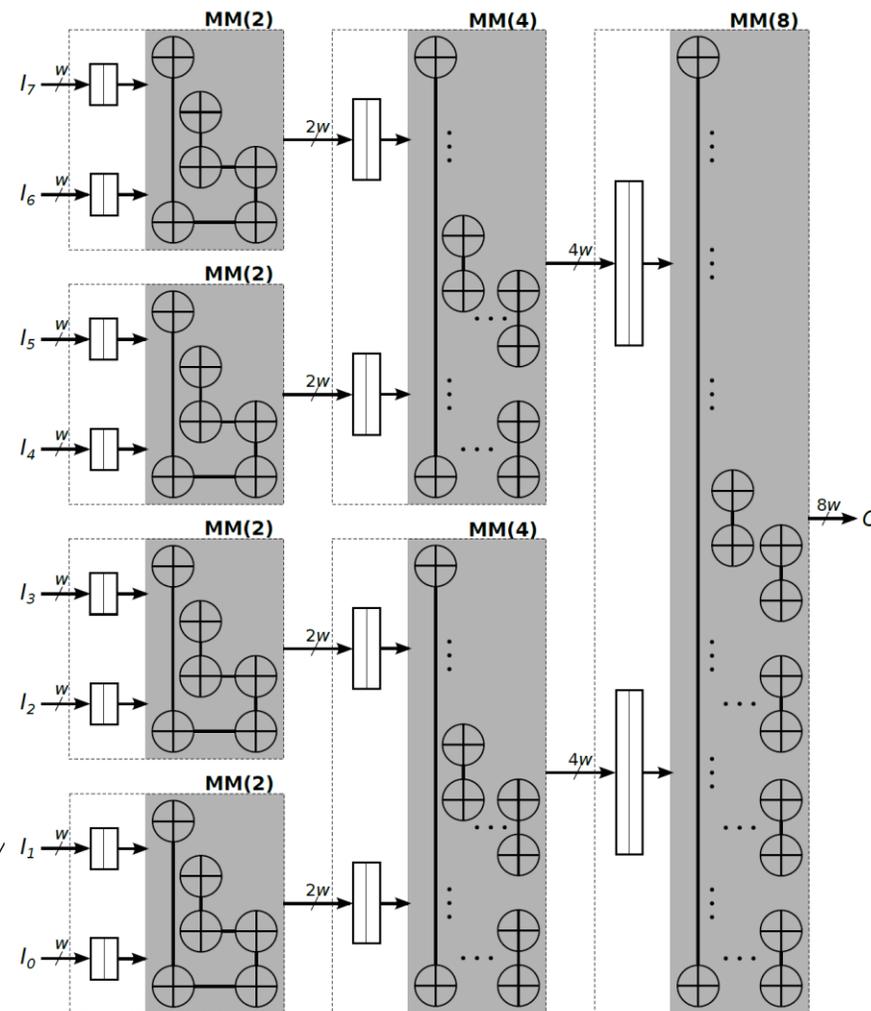
- 整合并行排序网络和串行归并排序器，并行输出。
- 允许排序器堵塞或空闲
(放弃了固定时间性能)



$$T = f \cdot \frac{N}{W} \cdot P \cdot \log_w N$$

$$P > 0.97$$

当W=32时，相比二输入串行归并排序，速度提高160倍！



寻求认同

第一次投稿： IEEE Transactions on Computers

2014年3月投稿： 9月询问， 只找到2个审稿人

2014年12月一审结果： 大修

2015年3月修改稿提交

2015年5月二审结果： 拒稿 两个审稿意见， 一个直接接收， 一个拒稿， AE选择拒稿。 但是， 不公平啊！ ？

The authors emphasize that their design is able to achieve a throughput of 129Gb/s which is greater than that of a 16-lane PCI-E 3.0 interface a modern GPU. However, the FPGA they tested only supports half (8 PCI-E 3.0 lanes) of that interface bandwidth. The reviewer wonders how a such an FPGA sorter would be integrated into a system.

文章说排序器的吞吐已经超过了现有GPU的带宽， 但是也超过了现有FPGA的IO带宽， 所以似乎实现不了啊？

我们谈的是一个新的排序算法， 说的是可以支持的带宽， 离做产品还远着呢， 我至于非要实现一个完整系统了才发篇论文吗？

A quick reimplemention done by this reviewer on a TITAN GPU using the current CUB sorter code can sort the same 459k elements in 745 usec (from and to device memory, ignoring transfers like the authors did). Their design using a full FPGA thus twice as fast as the GPU for the given data set size. However, I would assume the GPU would perform even better for data sets > 3.5 MB as the impact of the GPU launch overhead decreases.

我自己比了比性能， 拿TITAN GPU写了个排序测了一下， 同样排序3.5M数据， 的确FPGA能快50%， 但是， 你这只是小数据量比较， 大量数据的时候GPU的启动时间的影响会缩小（对GPU不公平）。

你至于要拿nVidia最新的GPU和上百号工程师写得GPU排序库的性能跟我这个还在初始创新阶段的FPGA排序加速新算法比较吗？ 还说这么比对GPU不公平？

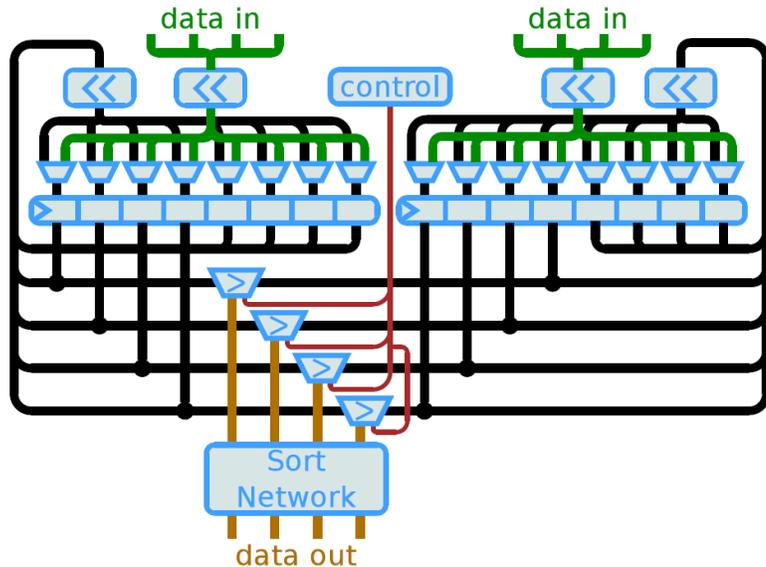
多重打击

第一重打击： IEEE Transactions on Computers 投稿，历时14个月之后拒稿

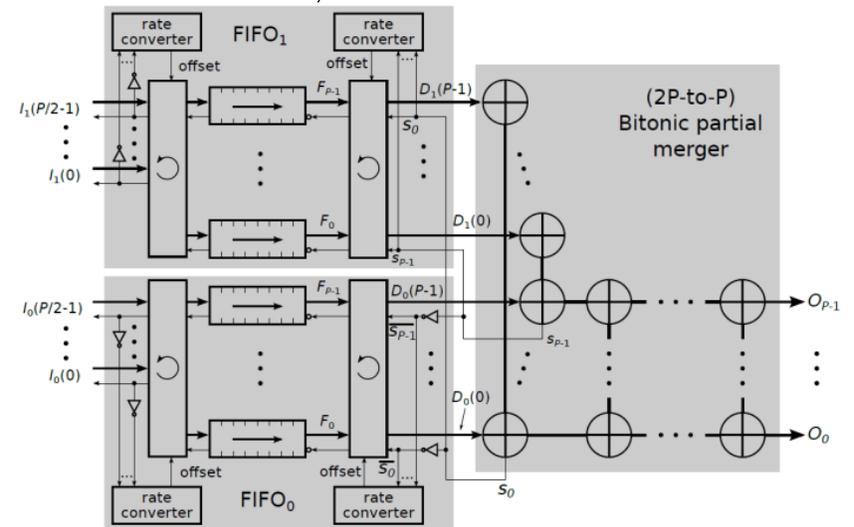
第二重打击：从2014年5月开始，通过曼彻斯特大学技术成果转化部门申请专利。曼大的工作人员将论文送至Xilinx的IP部门评估，没有了下文（估计是评估结果不好），专利申请失败。

第三重打击：2014年的FPGA会议发了篇论文“Hardware Acceleration of Database Operations”

作者：Kunle Olukotun, Professor, Pervasive Parallelism Lab, ECE, Stanford University



= ?



最后一搏

FPGA'14的文章基本已经把并行归并排序器单元的结构发明出来了

但是：树形结构还没有推出来（但是这个已经是顺理成章的下一步），还没有打破固定时间性能（没有推出树形结构的原因）。

2015年12月投稿FCCM'16，来年3月接收。

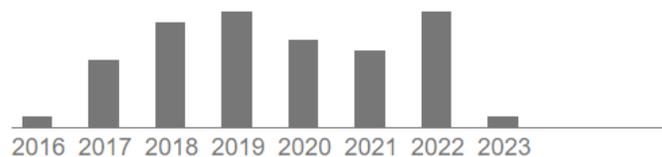
插曲：2016年2月份我找会议主席Matthew French (University of Southern California) 要邀请函（美国签证困难，文章结果未出，我全自费）。主席说，不确定你会不会来，没付钱注册不给写邀请函。等到3月催发邀请函，邀请函上注明“此人全自费哦”

2016年5月，自费去美国，做会议报告，谁也不认识，也无人提问。。。

2017年FCCM最佳论文：

“High-Performance Hardware Merge Sorter,” Susumu Mashimo, Thiem Van Chu, and Kenji Kise
Kenji Kise 东京工业大学

Total citations Cited by 61



FCCM'17最佳论文 53引用



创新难，但是也许获取认同更难

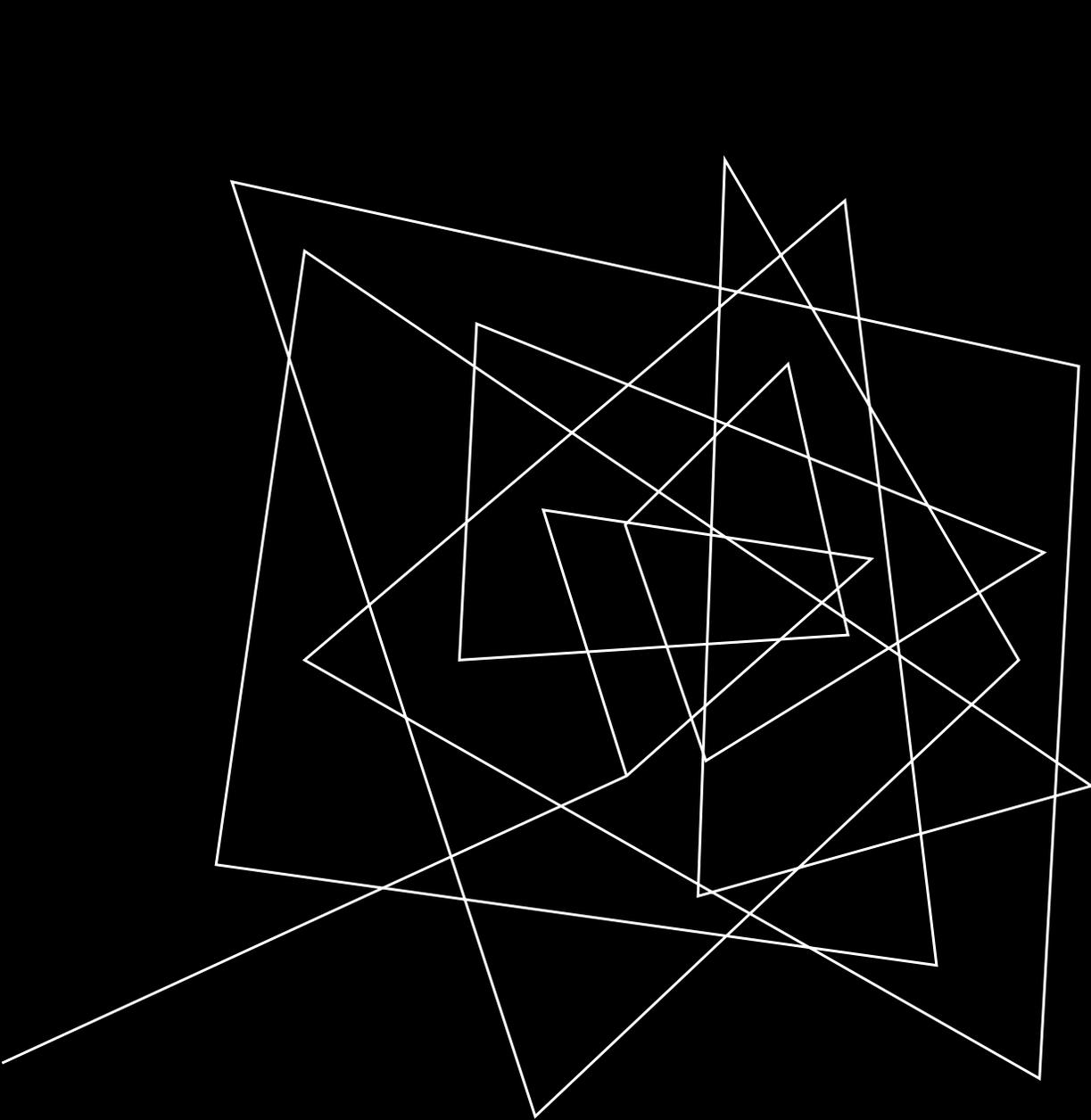
时间长 历时34个月 2013年7月到2016年5月，真正设计时间4个月。

偏见 排序是阻断行为，不是流行为。
没做成产品。
没超越现有的最先进技术。
不认识你。

强大的对手 在真创新上撞车，大概率对方更强，因为我们很弱。

现在回看：

- 开始的时候投TC就是个错误
创新性研究一定要投到一个对这个研究感兴趣的平台！
- 要坚强，不要气馁
因为你在抢别人的饭碗！
- 个人荣誉放低一点，重点在于发出来，是金子还是会发光



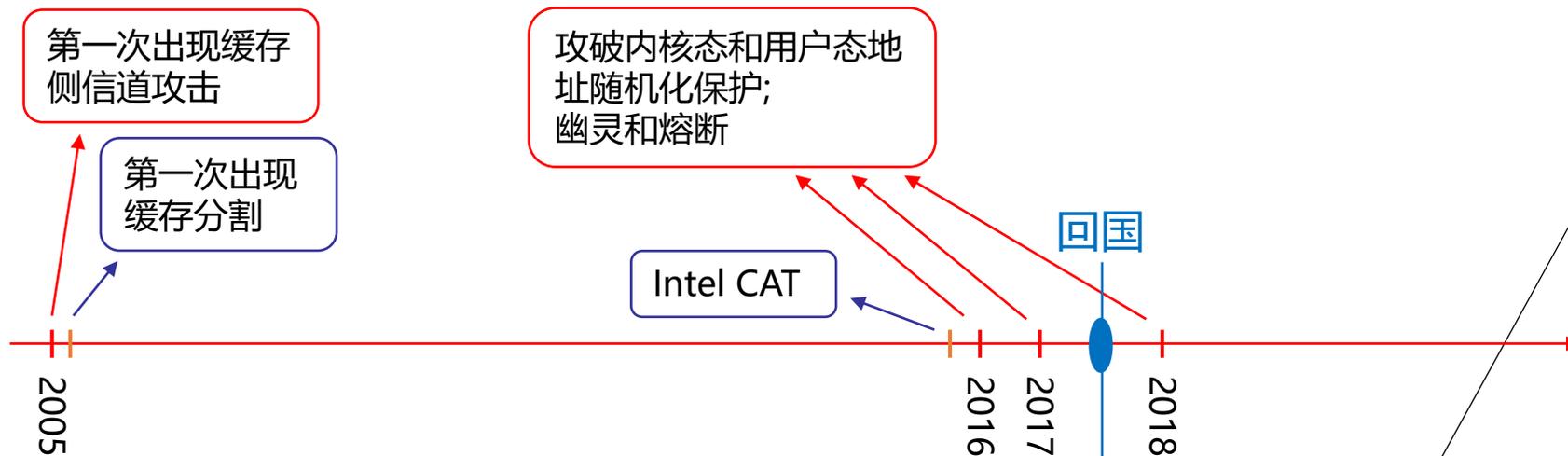
第二个故事：

时间：2017年至2021年

地点：北京

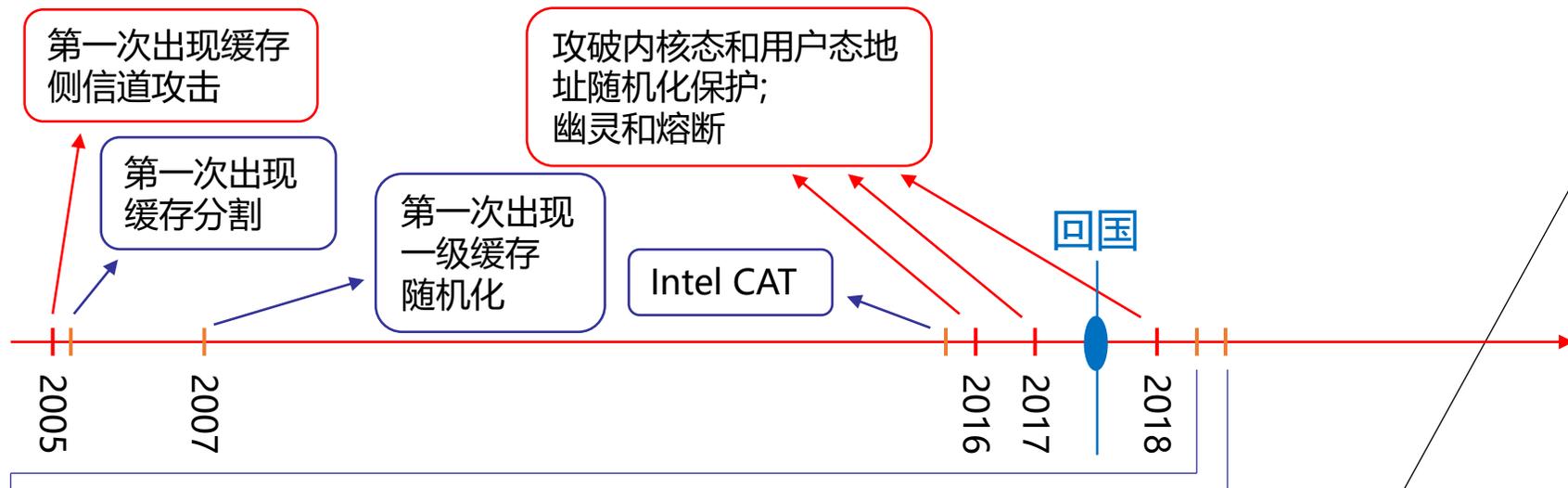
事件：缓存随机化

找到问题：缓存侧信道防御

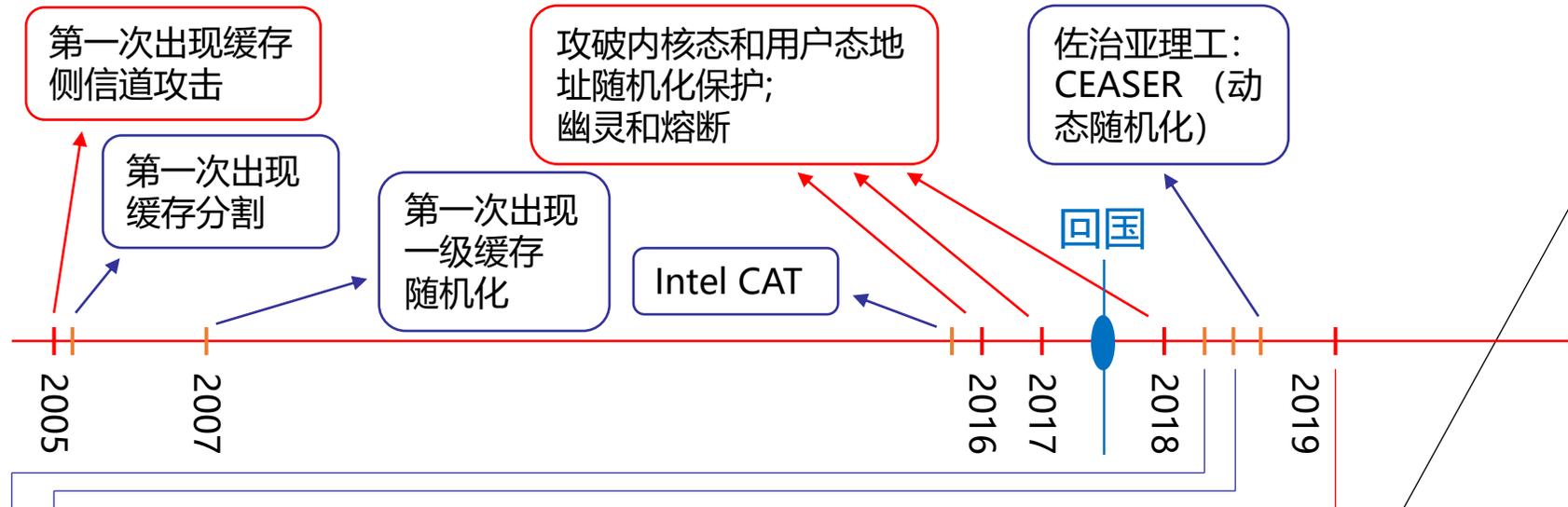


- 缓存分割一直是体系结构领域公认的缓存侧信道的标准防御
2016年Intel的CAT扩展指令集
- 但是缓存分割并不能防御2016-2018年出现的众多侧信道攻击
被打趴下了
- 2017年11月回国，第一次接触缓存侧信道攻击

解决思路：随机化的高速处理缓存（崎岖前行）



趴下了？不，我先证明你错了！



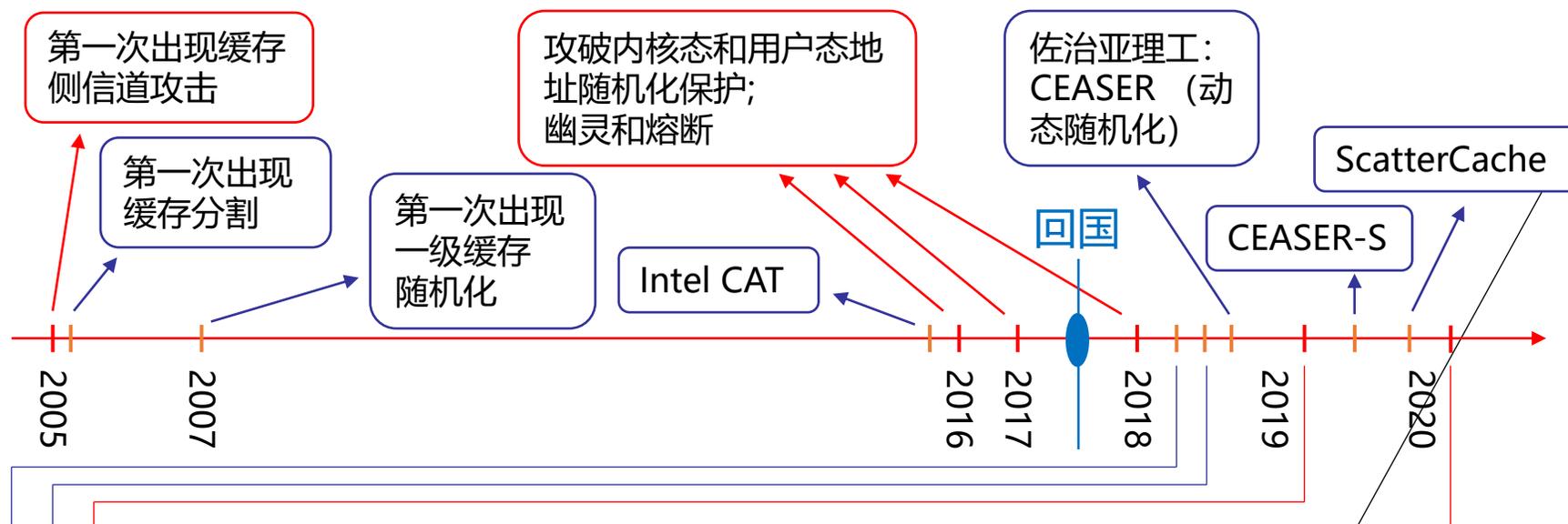
- 第一次提出随机化整个缓存架构 (Security-2018)
- 归纳总结攻击类型 (HPCA-2019)
- CEASER (Micro-2018最佳论文候选): 动态末级缓存随机化
突然一下, 整个学术界似乎一下子都认同缓存随机化了! (慢人一步)
- 用具体实验分析CEASER, 理论/实验证明CEASER的假设错误, 防御无效 (RAID-2019)
接受, 我们的第一篇!

但是只是证明别人错了并不是什么大贡献



作者: **Moinuddin Qureshi**, 佐治亚理工正教授, Yale N. Patt的学生
H因子38, 体系结构名人墙排序19, 仅次于William Dally。

然后，我还要提出我的！



- 第一次提出随机化整个缓存架构 (Security-2018)
- 归纳总结攻击类型 (HPCA-2019)
- 分析CEASER, 理论/实验证明CEASER的假设错误, 防御无效 (RAID-2019)
- 国外学者承认错误, 提出CEASER-S/ScatterCache (skewed缓存), 加固防御
- 分析CEASER-S和ScatterCache, 理论/实验证明他们再一次假设错误了! 并且这一次我们还提出了解决方案, 而且没有任何附加性能损失。 (S&P 2021)



作者: **Daniel Gruss**, 格拉茨技术大学副教授。
2017年博士毕业, H因子26, 幽灵和熔断的发现者之一。

坚持就是胜利，要当打不死的小强！

时间更长 历时42个月 2017年11月到2021年5月。

更强大的对手 神仙打架，我当炮灰。

真的很难：

- 世界变化太快，跟不上
- 无名之辈想去突破现有思维定式很难
- 需要的知识量太大、技术壁垒高
- 队友退缩

现在回看：

- 创新性研究一定要投到一个对这个研究感兴趣的平台！
- 坚持就是胜利：
不怕贼偷，就怕贼惦记。 要当扫地僧。 要当打不死的小强！
- 是金子还是会发光！

感言

- 先当扫地僧，再去摘桃子。
- 在创新这个事情上，只有甘做第二了，才可能获得第一。
- 不要气馁，要当打不死的小强。
- 珍惜给你指路的人。
- 珍惜给你提意见，刁难你的人。



谢谢！

听完了还敢搞创新吗？还感兴趣吗？
我年年博士招不满啊。。。。