BEN GRAS, MICHAEL KURTH,
HERBERT BOS, KAVEH RAZAVI, CRISTIANO GIUFFRIDA
VRIJE UNIVERSITEIT AMSTERDAM

ABSYNTHE: AUTOMATIC BLACKBOX SIDE-CHANNEL SYNTHESIS ON BLACK BOXES

VUSec

BEN GRAS, MICHAEL KURTH,
HERBERT BOS, KAVEH RAZAVI, CRISTIANO GIUFFRIDA
VRIJE UNIVERSITEIT AMSTERDAM

AS TO THE OPINIONS AND POSITIONS EXPRESSED IN THIS PRESENTATION, THEY ARE THOSE OF THE SPEAKERS AND DO NOT REPRESENT THE VIEWS OF ANY CURRENT OR PREVIOUS EMPLOYER, INCLUDING INTEL CORPORATION OR ITS AFFILIATES

VUSec

SIDE CHANNELS

Observation: Shared resources often give rise to side channels

- L1, L2, LLC caches
- TLB
- Branch predictor state
- Store-to-Load forwarding
- Many others

SIDE CHANNELS

Most side channels are eviction based

- Original: cache attack and many variants
- Cache directory attack
- TLBleed (TLB)
- Many branch prediction based attacks (PHT, BTB)

Each can have

- Complex addressing function
- Complex structure (sets, ways, levels, inclusivity)

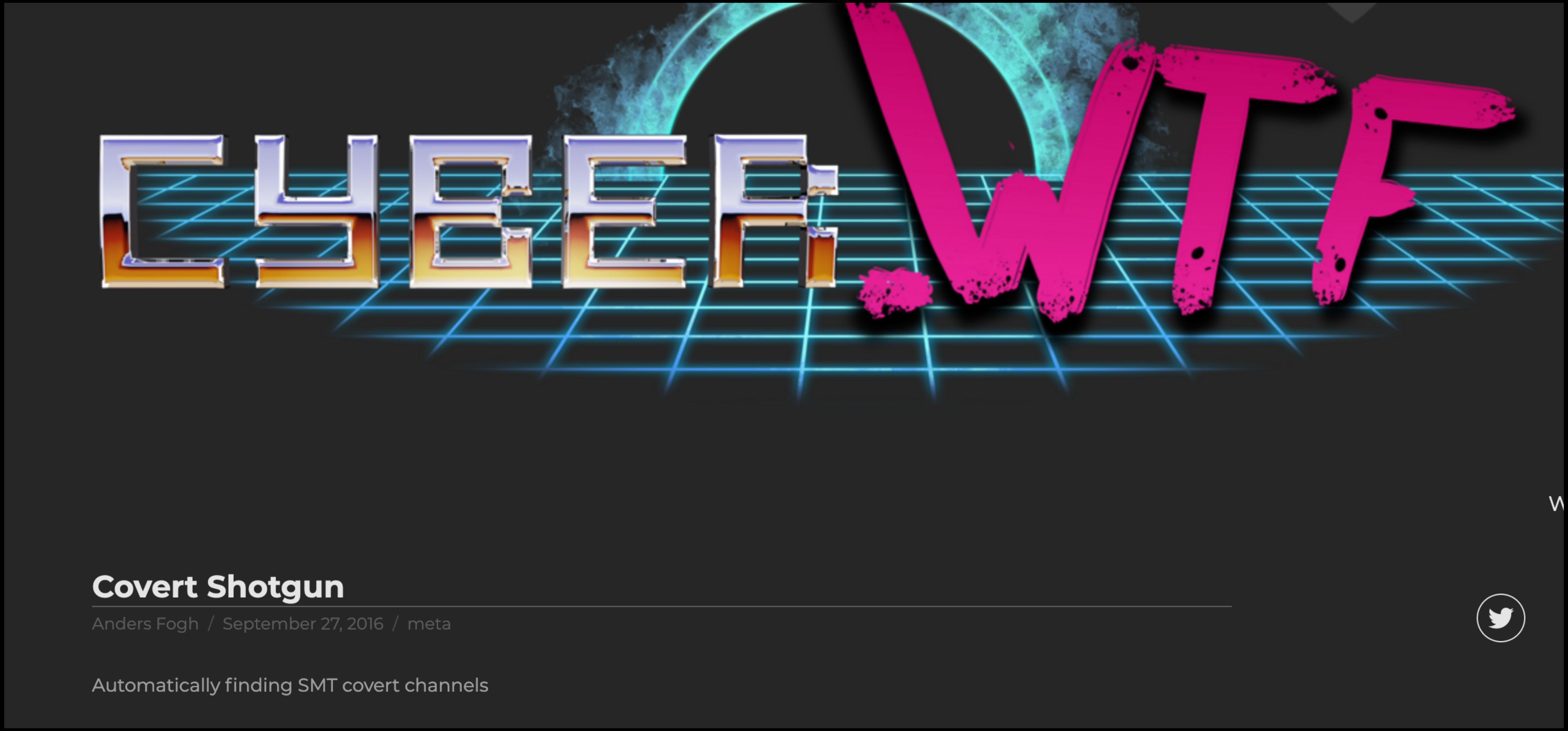
LESS REVERSE ENGINEERING

- Lifetimes have been spent in reverse engineering uarch structures
- Let’s just target stateless resources? No eviction.
- Examples: execution unit contention, execution port contention
- Let’s do a full multi-arch NxN covert shotgun & upgrade to side channel

ABSYNTHE: THE VISION

- Given: target code, architecture
- Automatically find secret-dependent code paths in target code
- Mix side channel primitives to improve signal strength
- Include inter-VM signal
- Upgrade synchronized secret classification to unsynchronised key recovery

ABSYNTHE: THE VISION

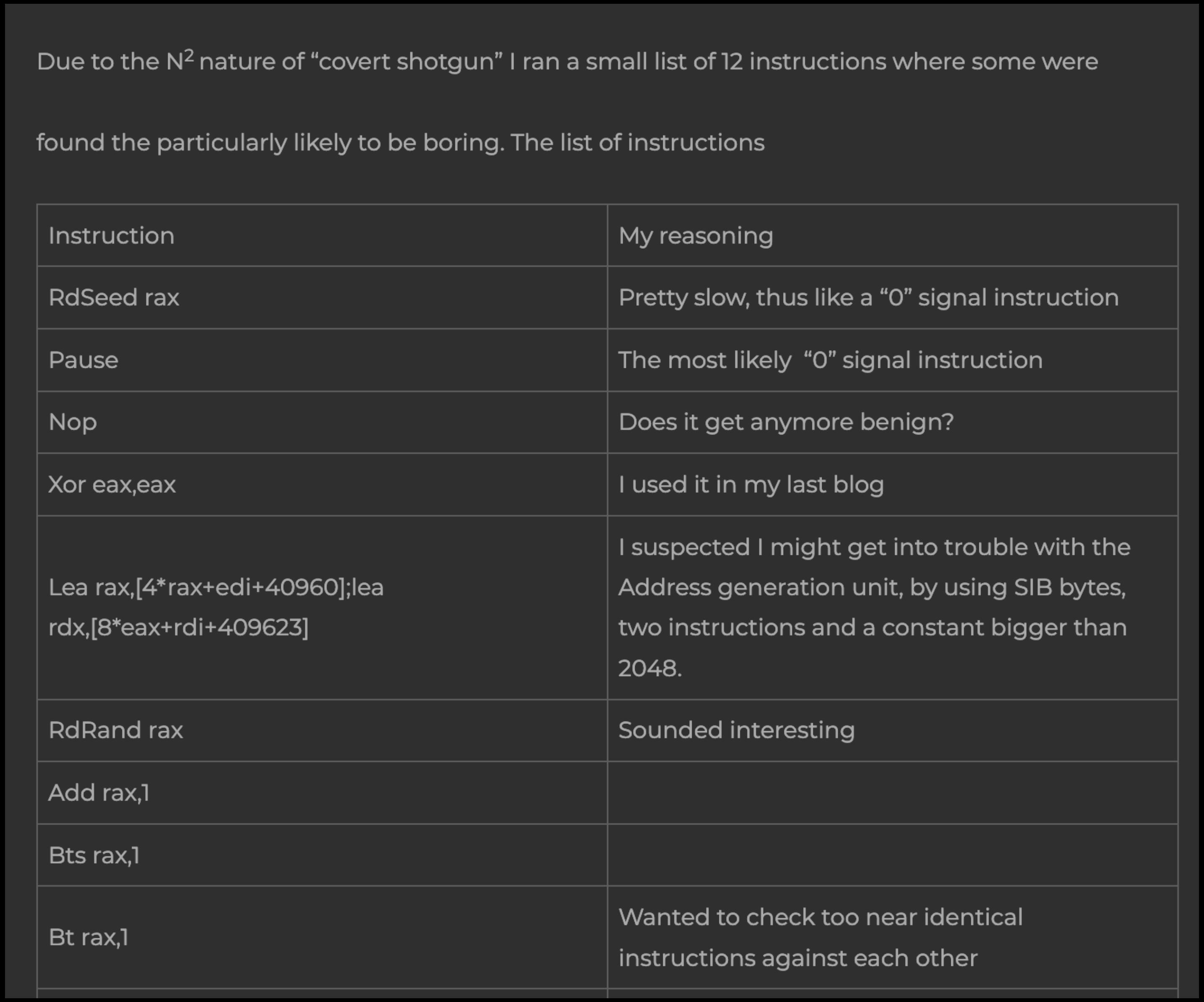


Covert Shotgun

Anders Fogh / September 27, 2016 / meta

Automatically finding SMT covert channels

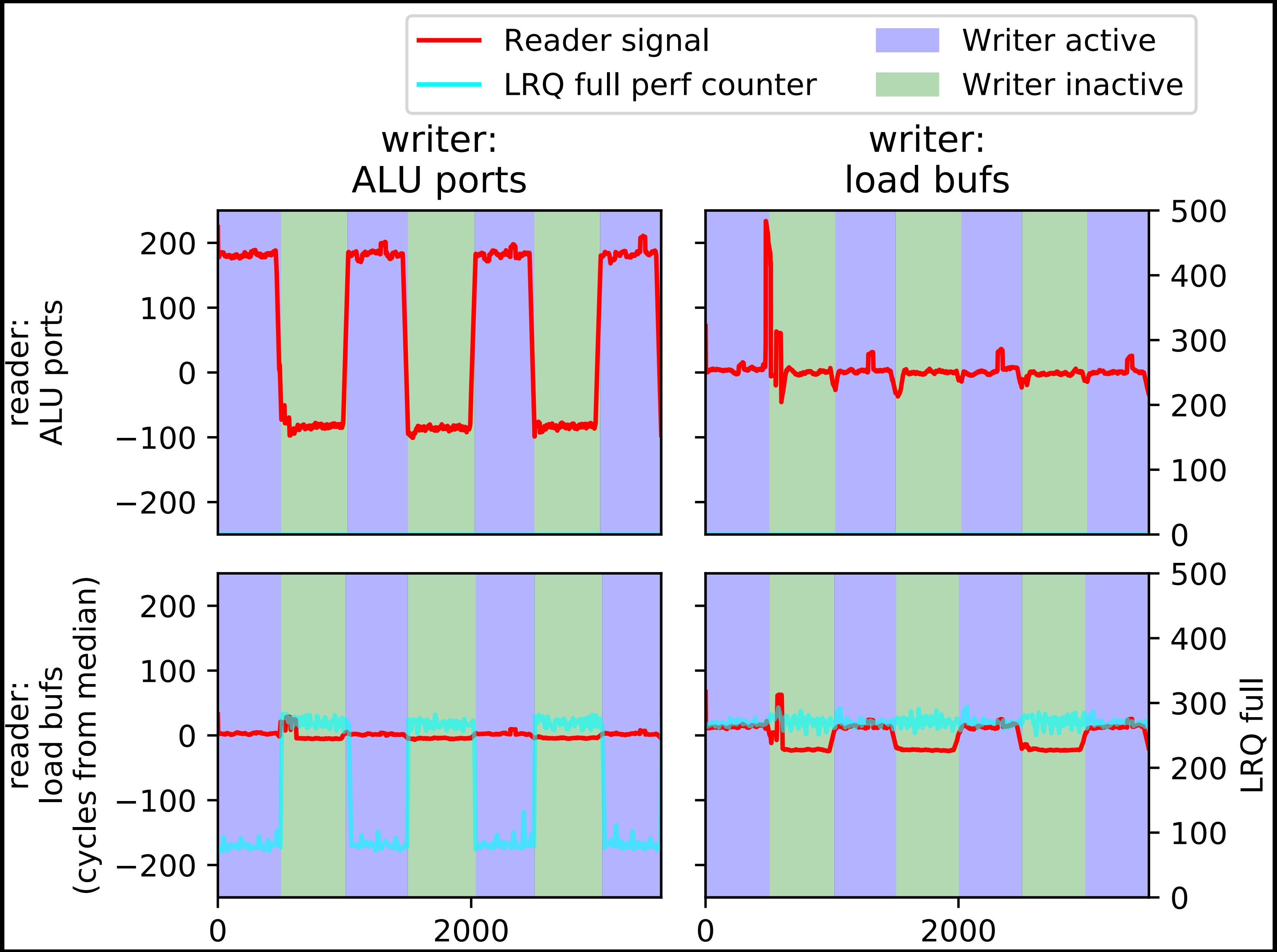
ABSYNTHE: THE VISION



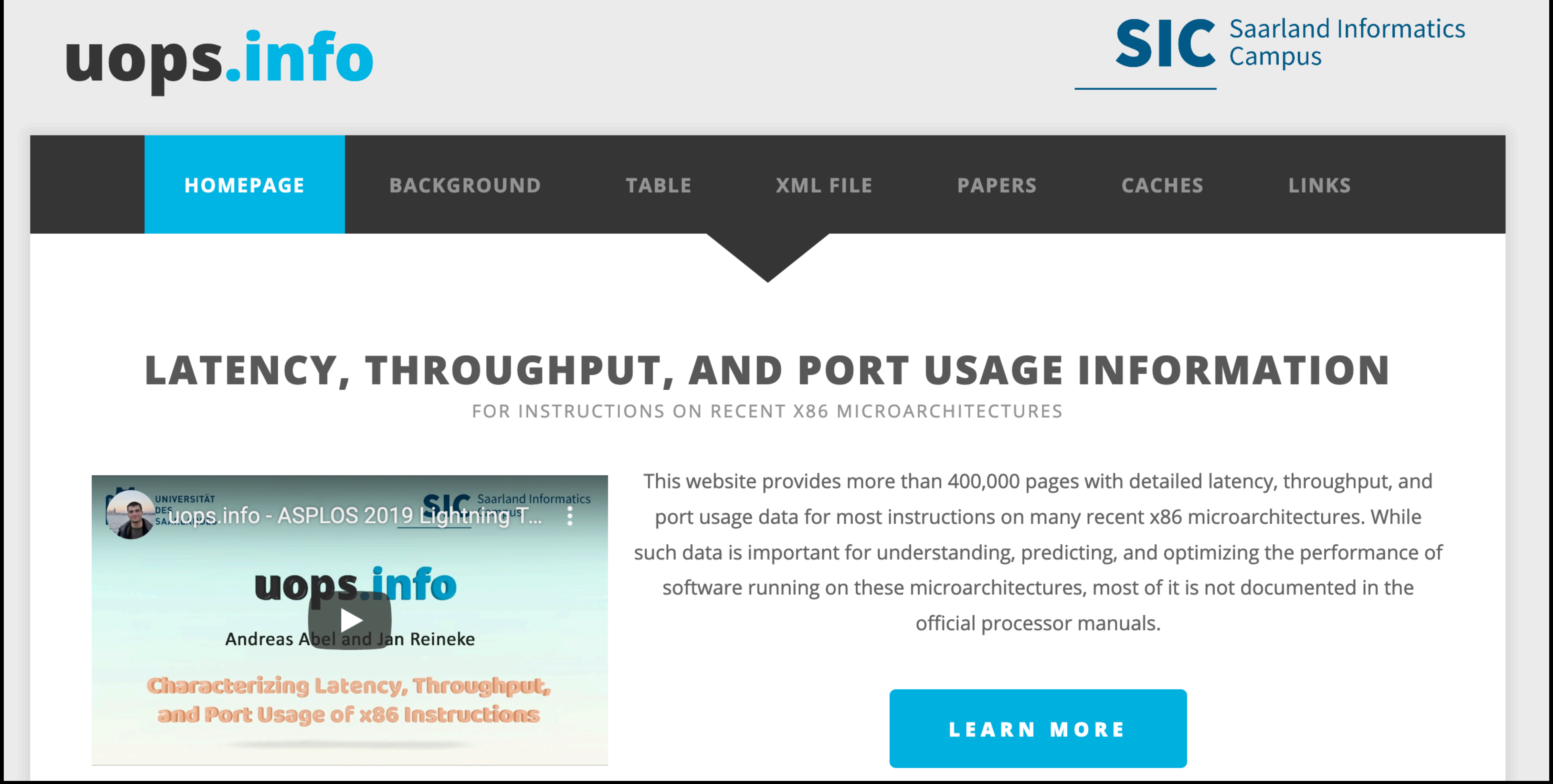
Due to the N^2 nature of “covert shotgun” I ran a small list of 12 instructions where some were found the particularly likely to be boring. The list of instructions

Instruction	My reasoning
RdSeed rax	Pretty slow, thus like a “0” signal instruction
Pause	The most likely “0” signal instruction
Nop	Does it get anymore benign?
Xor eax,eax	I used it in my last blog
Lea rax,[4*rax+edi+40960];lea rdx,[8*eax+rdi+409623]	I suspected I might get into trouble with the Address generation unit, by using SIB bytes, two instructions and a constant bigger than 2048.
RdRand rax	Sounded interesting
Add rax,1	
Bts rax,1	
Bt rax,1	Wanted to check too near identical instructions against each other

OUR COVERT SHOTGUN: PRIMITIVES ON ARM VULCAN



ALL X86 INSTRUCTIONS?

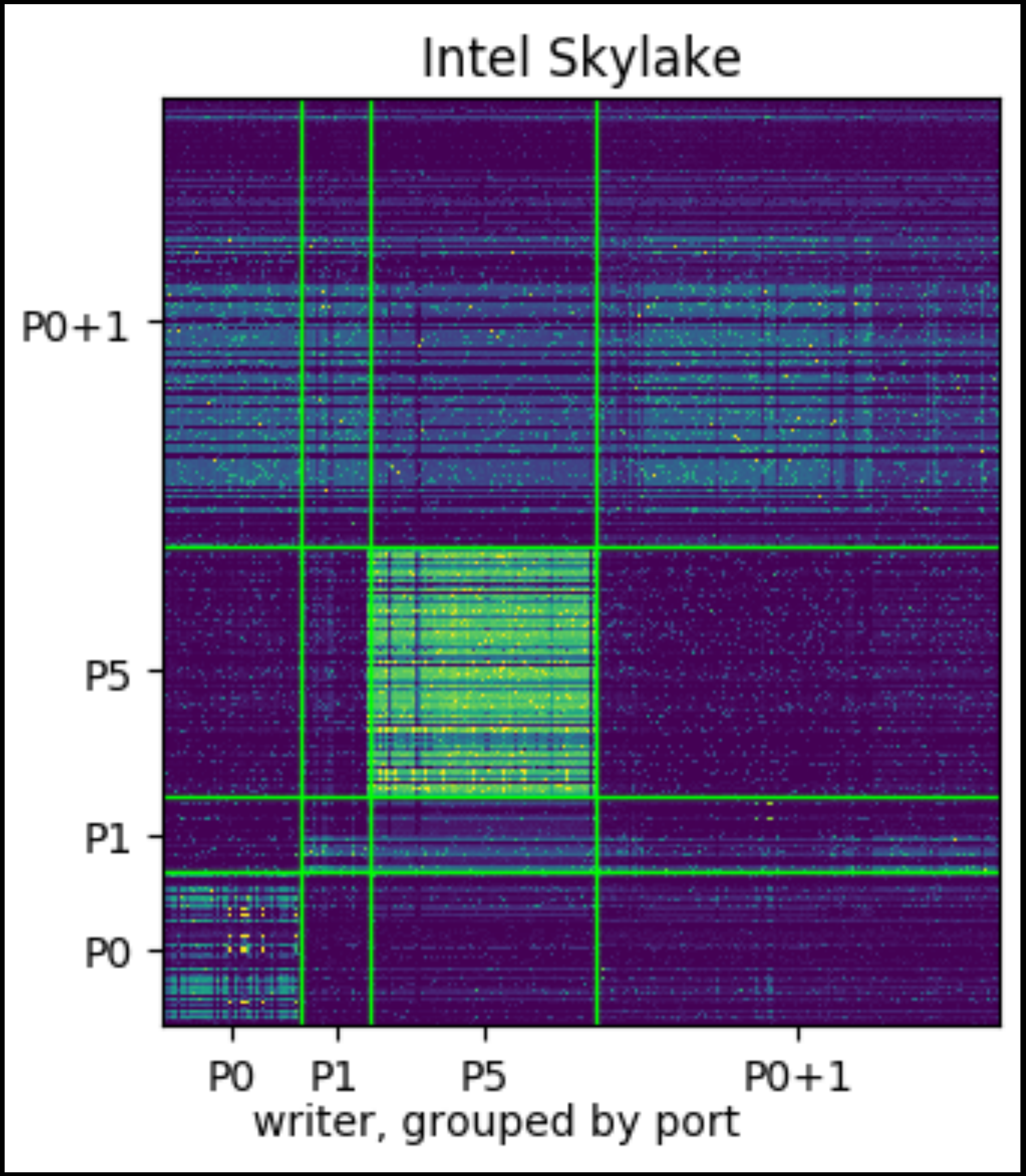

uops.info
SIC Saarland Informatics Campus
HOMEPAGE
BACKGROUND
TABLE
XML FILE
PAPERS
CACHES
LINKS
uops.info - ASPLOS 2019 Lightning T...
uops.info
Andreas Abel and Jan Reineke
Characterizing Latency, Throughput, and Port Usage of x86 Instructions
LEARN MORE

LATENCY, THROUGHPUT, AND PORT USAGE INFORMATION

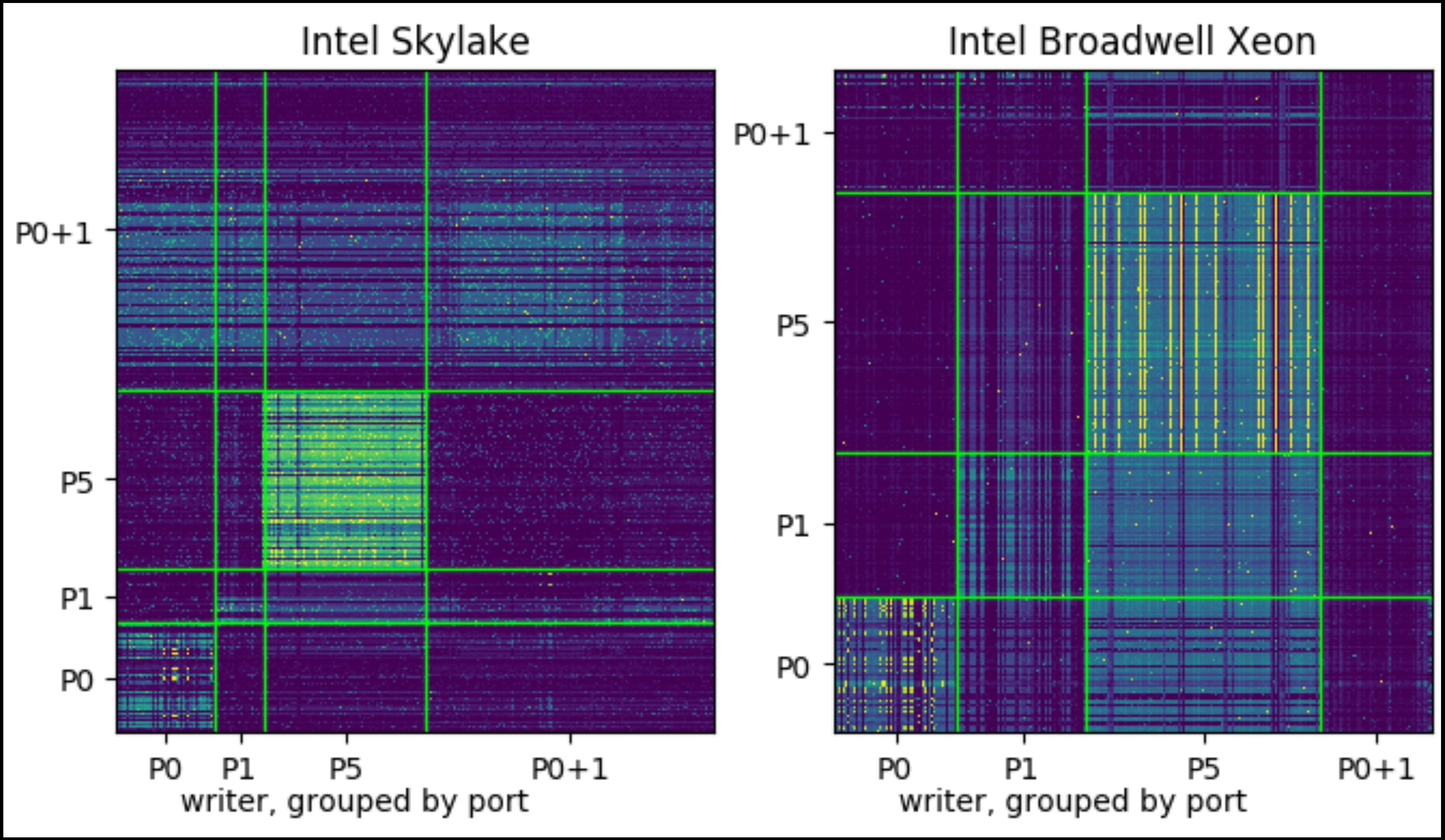
FOR INSTRUCTIONS ON RECENT X86 MICROARCHITECTURES

This website provides more than 400,000 pages with detailed latency, throughput, and port usage data for most instructions on many recent x86 microarchitectures. While such data is important for understanding, predicting, and optimizing the performance of software running on these microarchitectures, most of it is not documented in the official processor manuals.

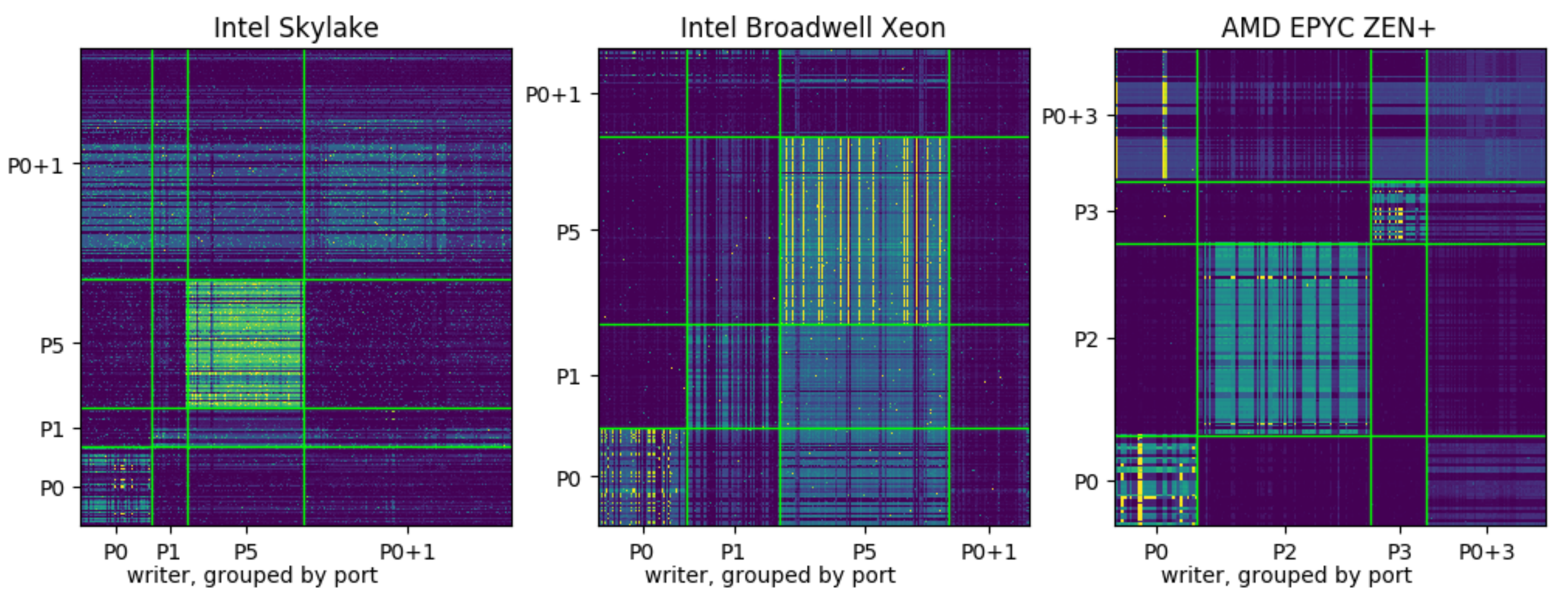
ALL ON SKYLAKE



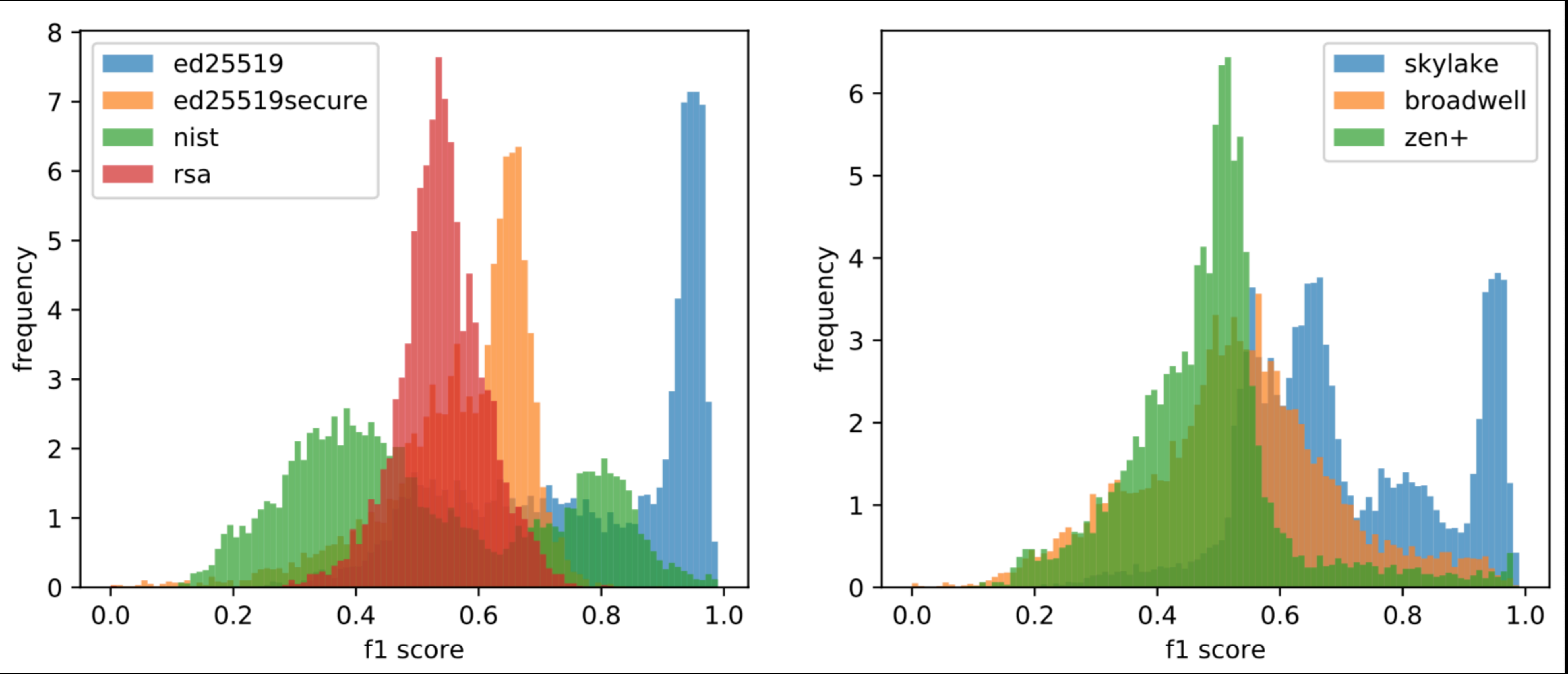
AND BROADWELL



AND ZEN


Intel Skylake
P0+1
P5
P1
P0
P0
P1
P5
P0+1
writer, grouped by port
Intel Broadwell Xeon
P0+1
P5
P1
P0
P0
P1
P5
P0+1
writer, grouped by port
AMD EPYC ZEN+
P0+3
P3
P2
P0
P0
P2
P3
P0+3
writer, grouped by port

TRY ALL INSTRUCTIONS AS SIDE CHANNELS ON VULNERABLE LIBGCRYPT TARGETS

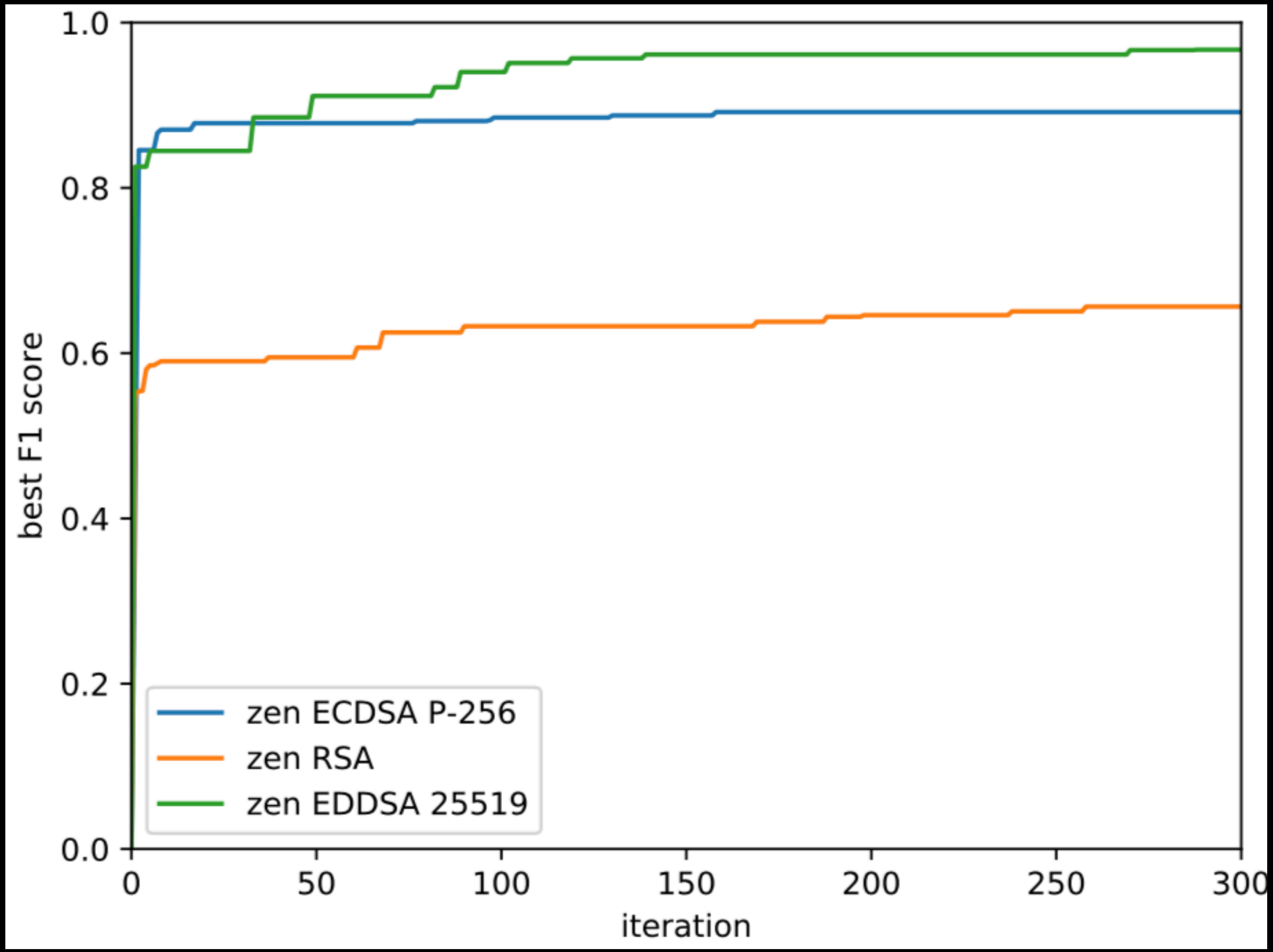


AUTOMATICALLY TUNE

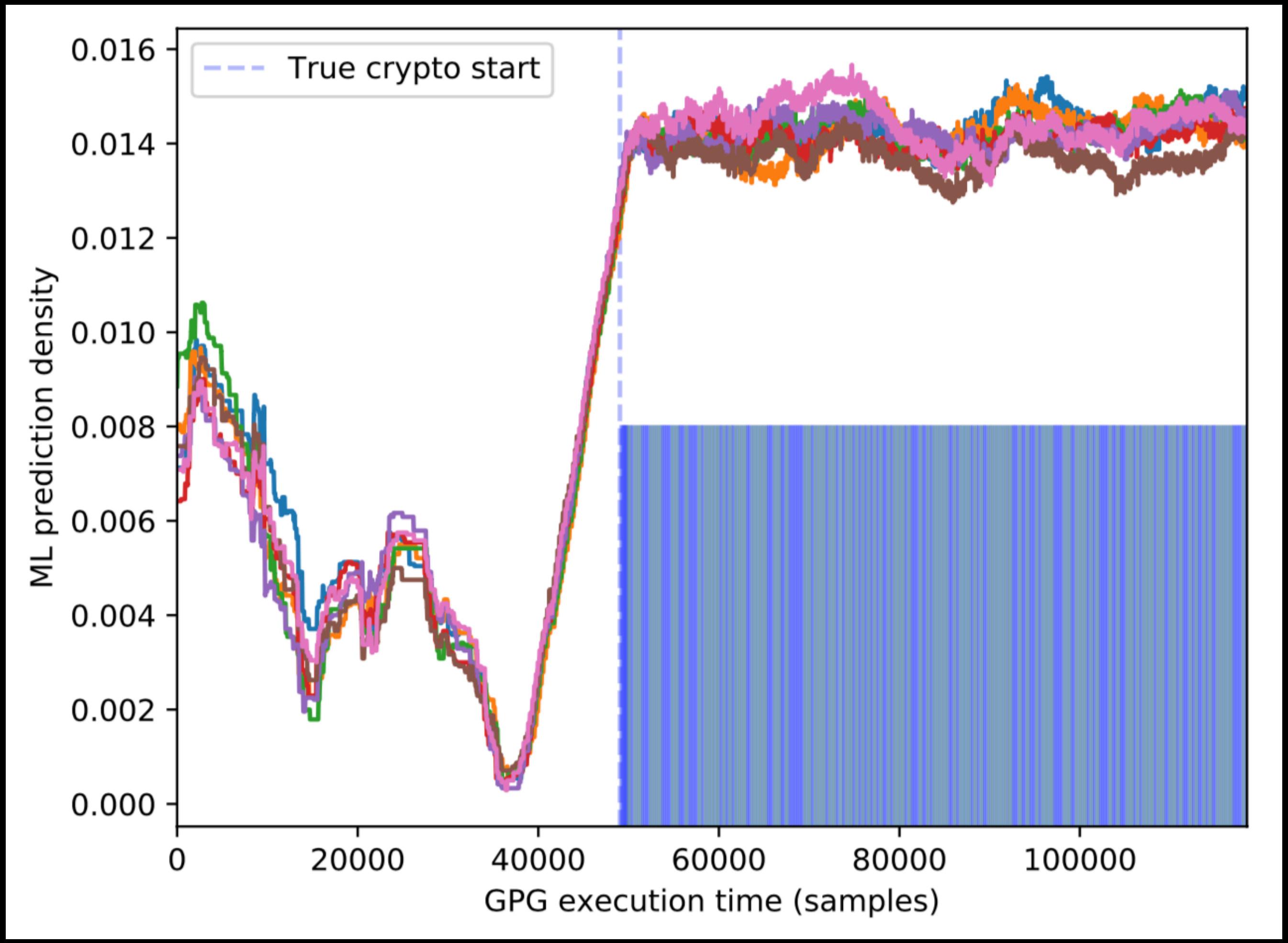
- We can differentiate secrets using these side channels
- Can we do better if we mix them?

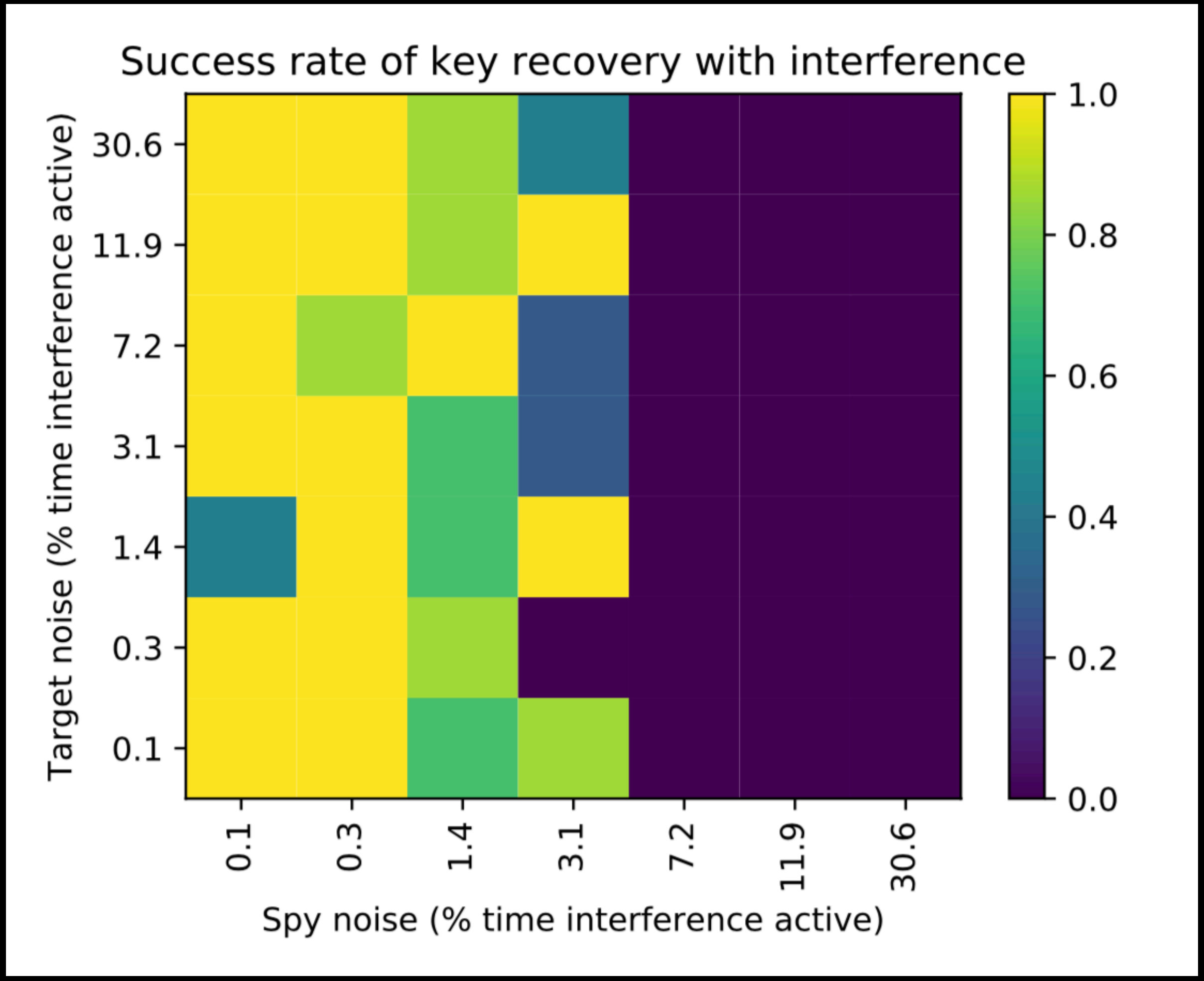
AUTOMATICALLY TUNE

- We can differentiate secrets using these side channels
- Can we do better if we mix them?

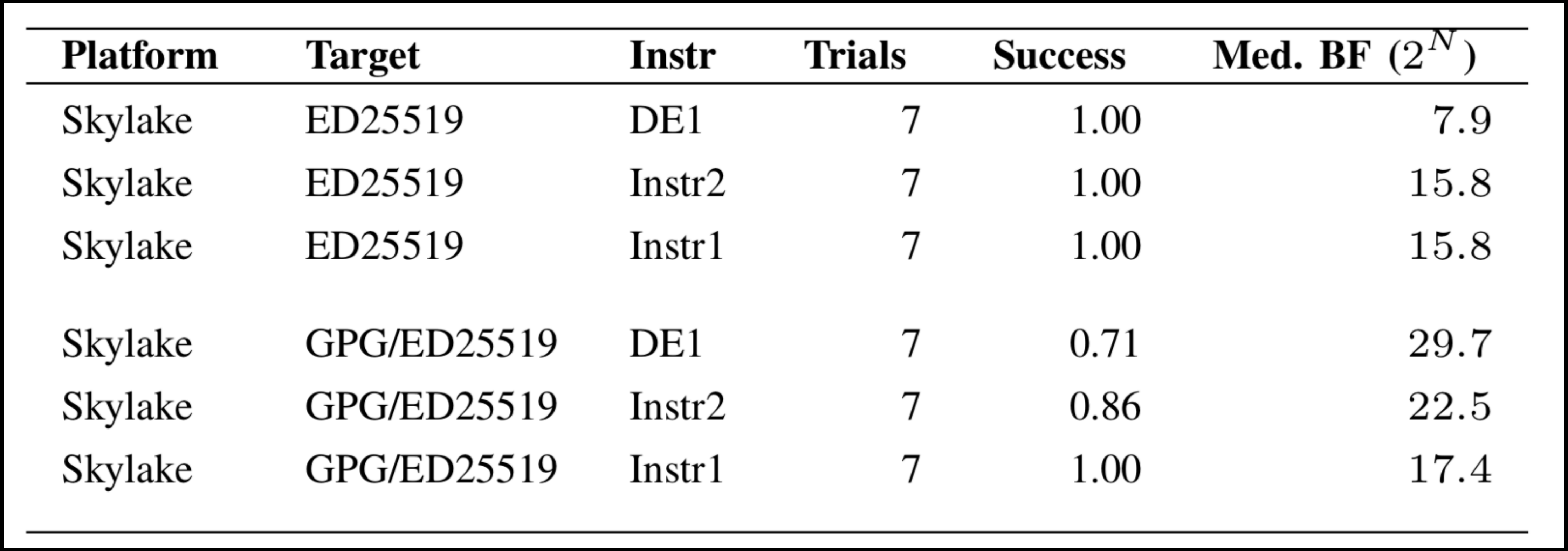


NOISE RESISTANCE



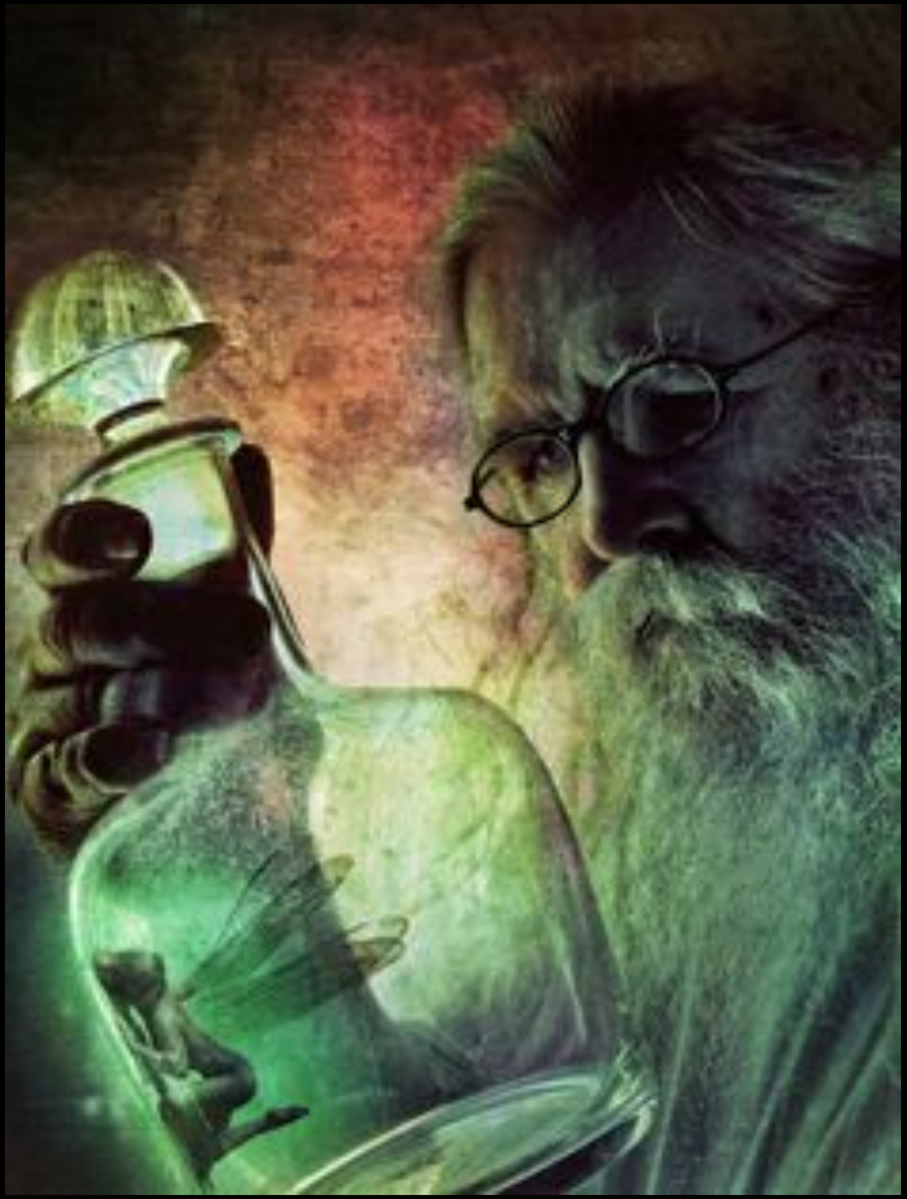


RESULTS: FULL KEY RECOVERY, PLAIN AND GPG



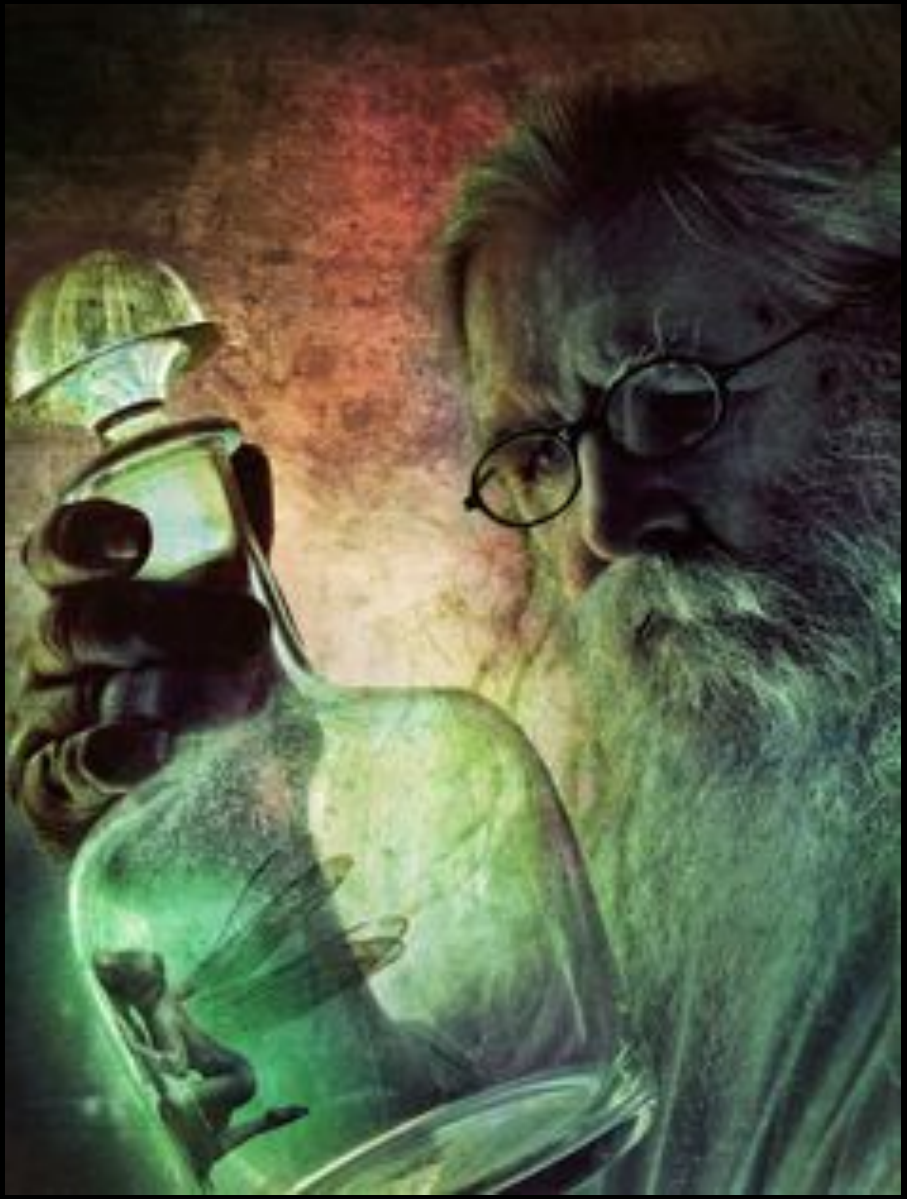
Platform	Target	Instr	Trials	Success	Med. BF (2^N)
Skylake	ED25519	DE1	7	1.00	7.9
Skylake	ED25519	Instr2	7	1.00	15.8
Skylake	ED25519	Instr1	7	1.00	15.8
Skylake	GPG/ED25519	DE1	7	0.71	29.7
Skylake	GPG/ED25519	Instr2	7	0.86	22.5
Skylake	GPG/ED25519	Instr1	7	1.00	17.4

CONCLUSION



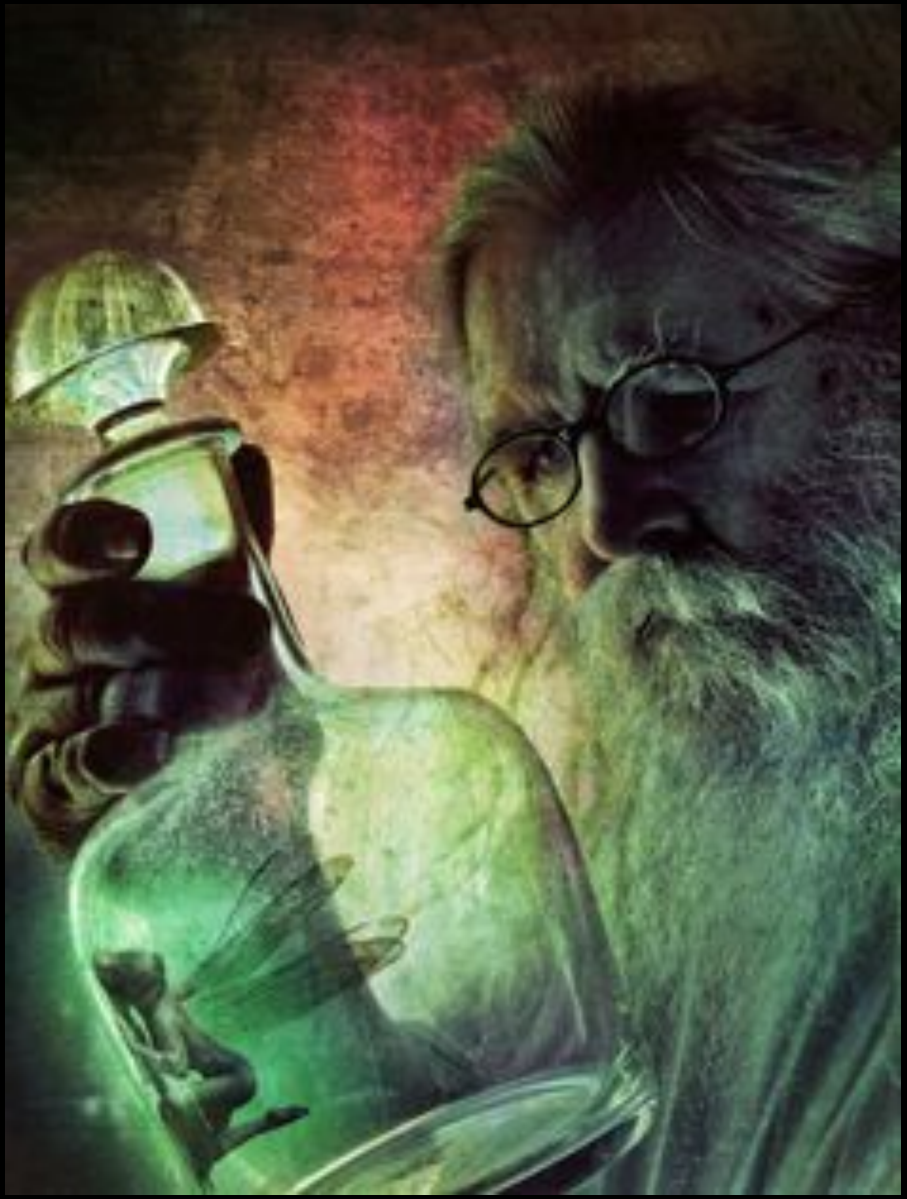
CONCLUSION

- ABSynthe is a useful side channel analysis kit



CONCLUSION

- ABSynthe is a useful side channel analysis kit
- New, multi-arch side channel results



CONCLUSION

- ABSynthe is a useful side channel analysis kit
- New, multi-arch side channel results
- Thank you for listening