Tampere University

HyperDegrade: from GHz to MHz Effective CPU Frequencies

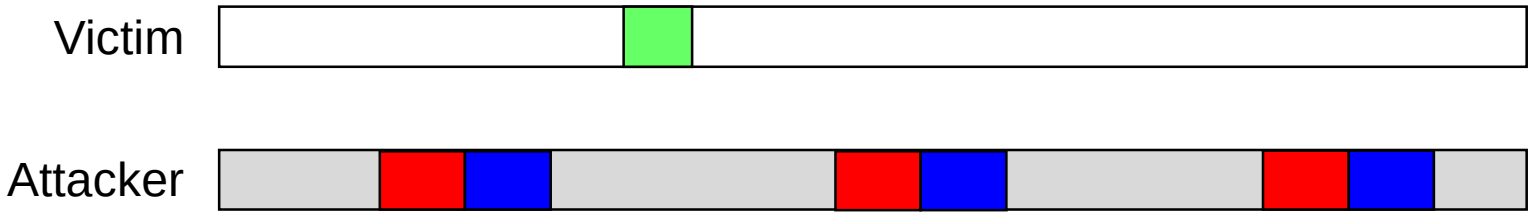
- Alejandro Cabrera Aldaya
  Billy Bob Brumley

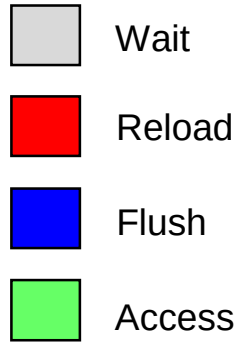
usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Roadmap

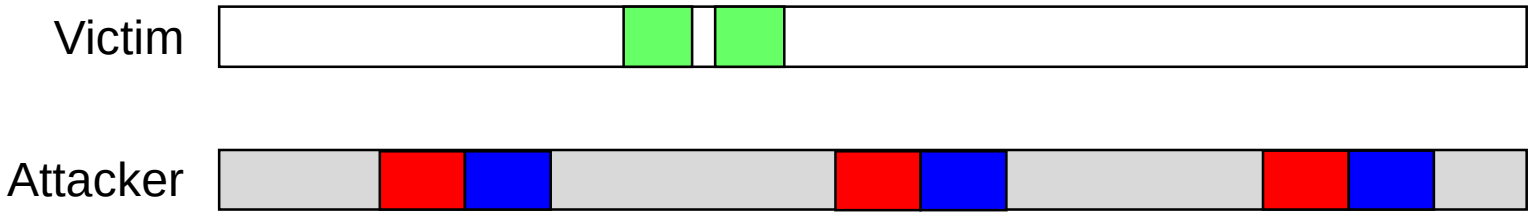
- Flush+Reload and Performance Degradation
- HyperDegrade
- Slowdown estimation and comparison
- HyperDegrade as a *side-channel amplifier*:
  - Comparison with previous approaches
  - Paired with F+R
  - Target: uarch Raccoon Attack leakage on OpenSSL

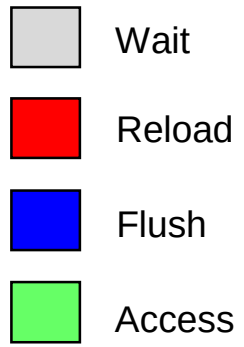
Flush+Reload & Performance Degradation attacks



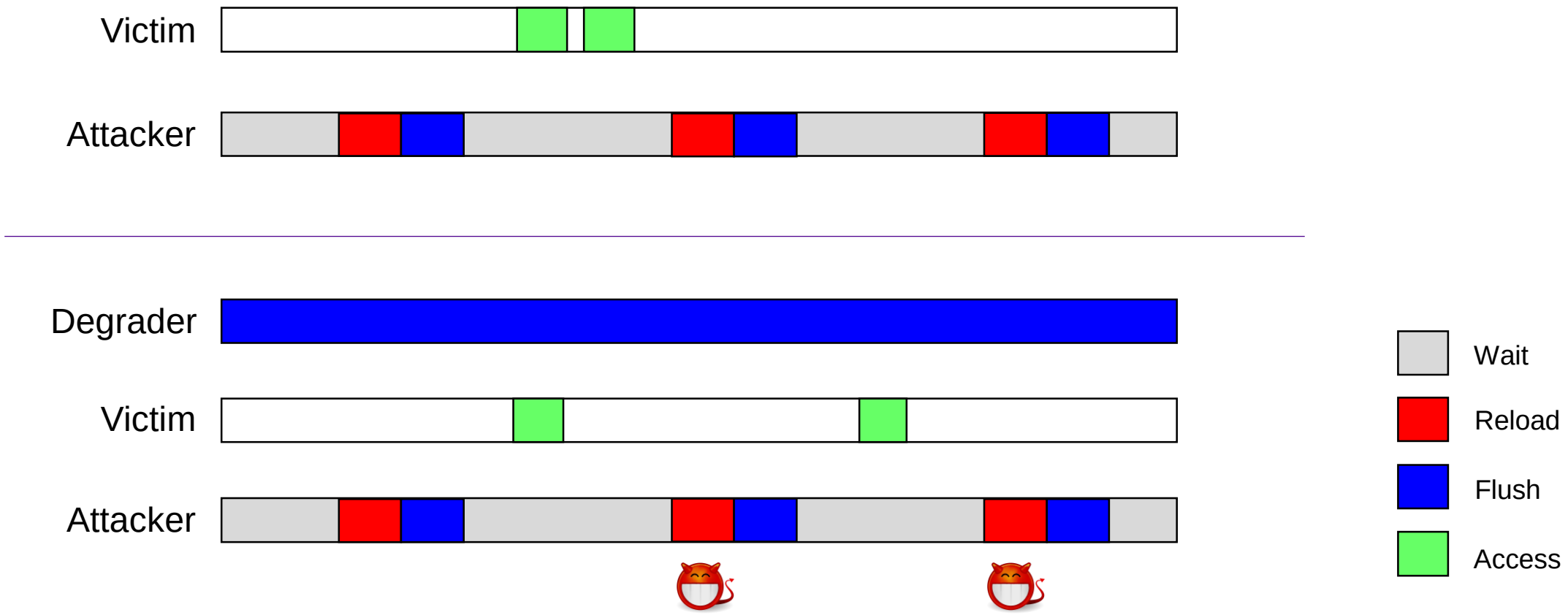


Flush+Reload & Performance Degradation attacks





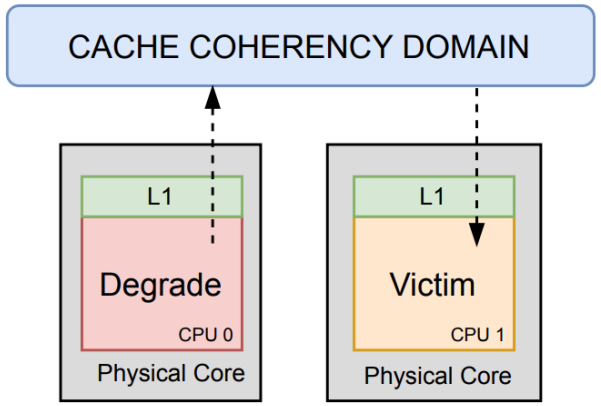
Flush+Reload & Performance Degradation attacks



Performance Degradation Attack

- **Idea:** evicting hot victim cache lines: clflush
- Requires shared memory with the victim (like F+R)
- Requires hot cache line identification
- Targets:
  - RSA [10]
  - ECDSA [8]
  - DSA [51]
  - SM2 [58]
  - AES [18]
  - ECDH [24]

  …

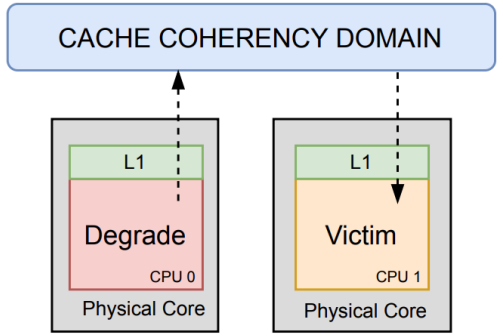


"Amplifying Side Channels Through Performance Degradation", Allan et al., ACSAC'16.

Degrade: revisited

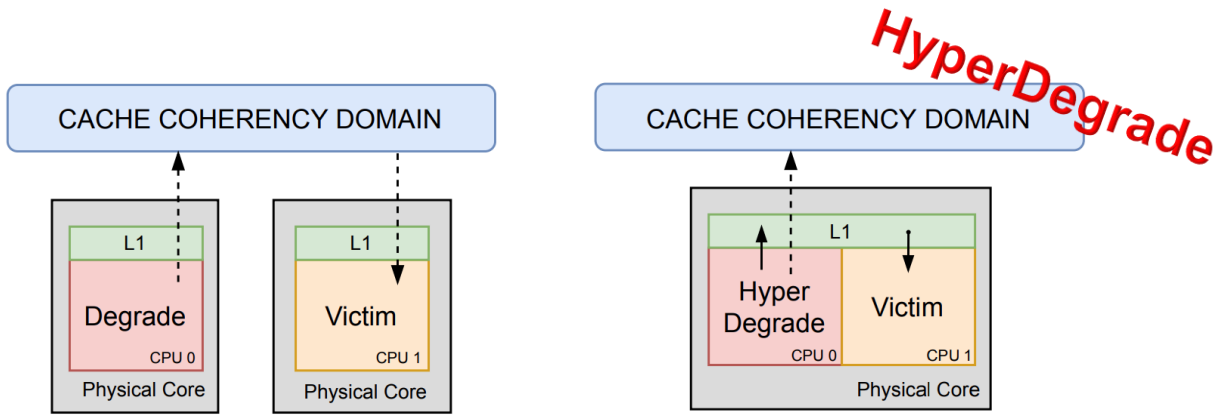
Parameter	NoDegrade	Degrade
inst_retired.any	1.5M	1.5M
L1-icache-load-misses	4,115	33,785
cycles	1,252,211	12,935,389

≪ 1 cache miss / inst
Can we do better?



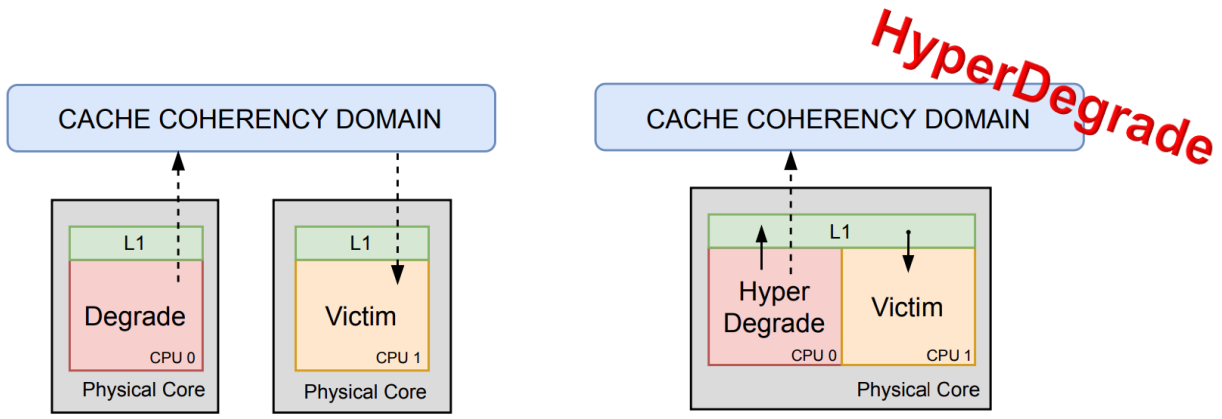
HyperDegrade: Degrade on SMT

Parameter	NoDegrade	Degrade	HyperDegrade
inst_retired.any	1.5M	1.5M	1.5M
L1-icache-load-misses	4,115	33,785	992,074
cycles	1,252,211	12,935,389	504,395,314
machine_clears.smc	<1	28,375	983,348



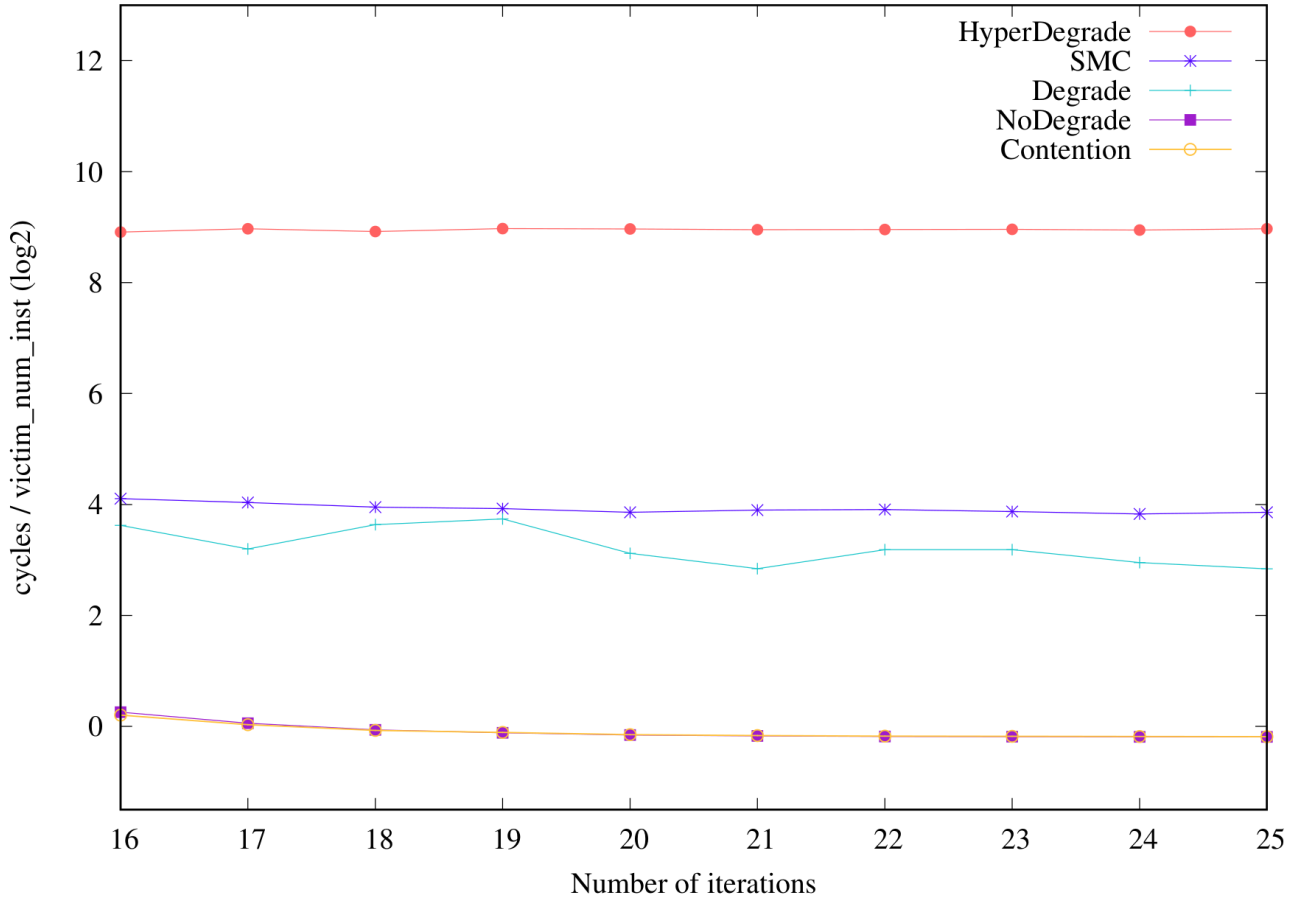
HyperDegrade: Degrade on SMT

Parameter	NoDegrade	Degrade	HyperDegrade
inst_retired.any	1.5M	1.5M	1.5M
L1-icache-load-misses	4,115	33,785	992,074
cycles	1,252,211	12,935,389	504,395,314
machine_clears.smc	<1	28,375	983,348



Slowdown strategies compared

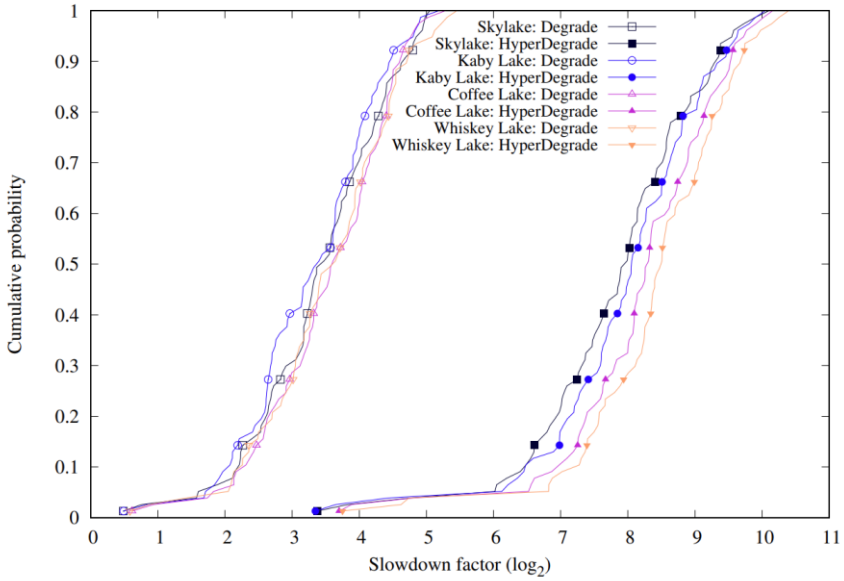
Strategy	Details
NoDegrade	Baseline
Degrade	Allan *et al.* [7]
HyperDegrade	This work
Contention	HyperDegrade @ *cold* CL
SMC	Standalone (no shared memory)



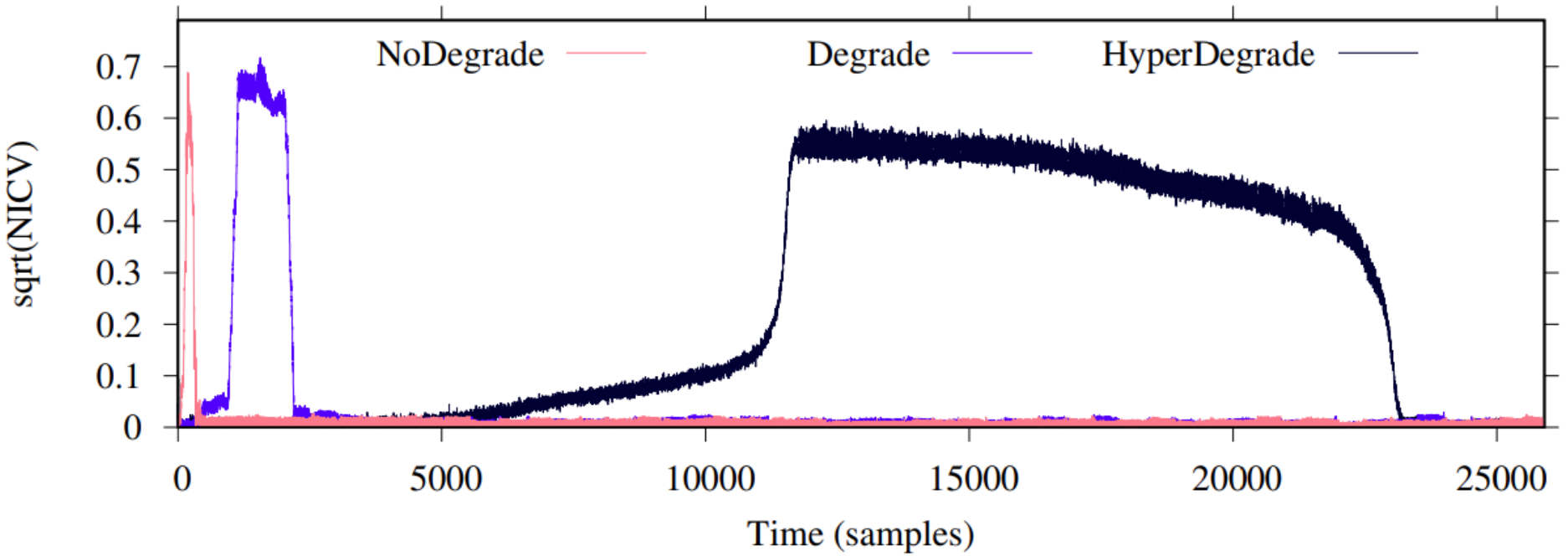
HyperDegrade: benchmarks

BEEBS Suite: 77 microbenchmarks

Family	Method	Min	Mean	Max
Skylake	Degrade	1.4	13.1	33.1
Skylake	HyperDegrade	10.4	306.3	1101.9
Kaby Lake	Degrade	1.4	12.0	36.5
Kaby Lake	HyperDegrade	10.2	330.6	1060.1
Coffee Lake	Degrade	1.5	14.0	39.0
Coffee Lake	HyperDegrade	13.0	382.5	1143.7
Whiskey Lake	Degrade	1.5	14.4	43.9
Whiskey Lake	HyperDegrade	13.5	435.8	1349.3



HyperDegrade as Side-Channel amplifier



HyperDegrade as Side-Channel amplifier

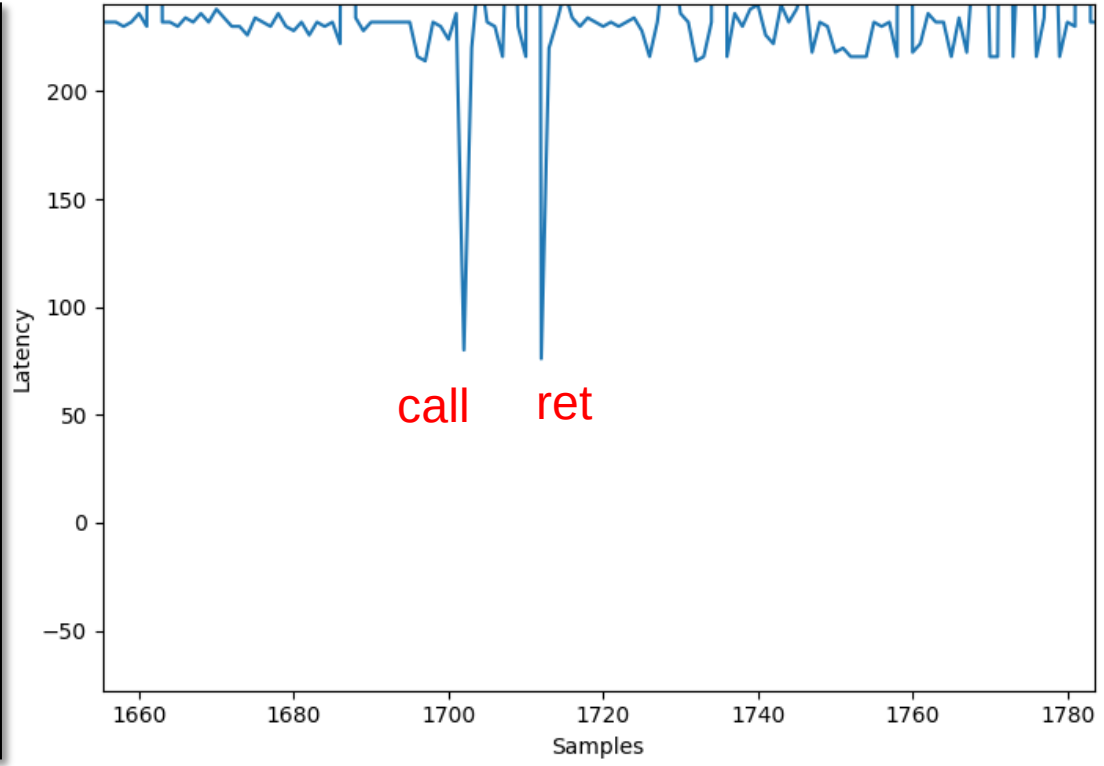
*"**Raccoon Attack**: Finding and Exploiting Most-Significant-Bit-Oracles in TLS-DH(E)", Merget et al., USENIX'21*

The Code

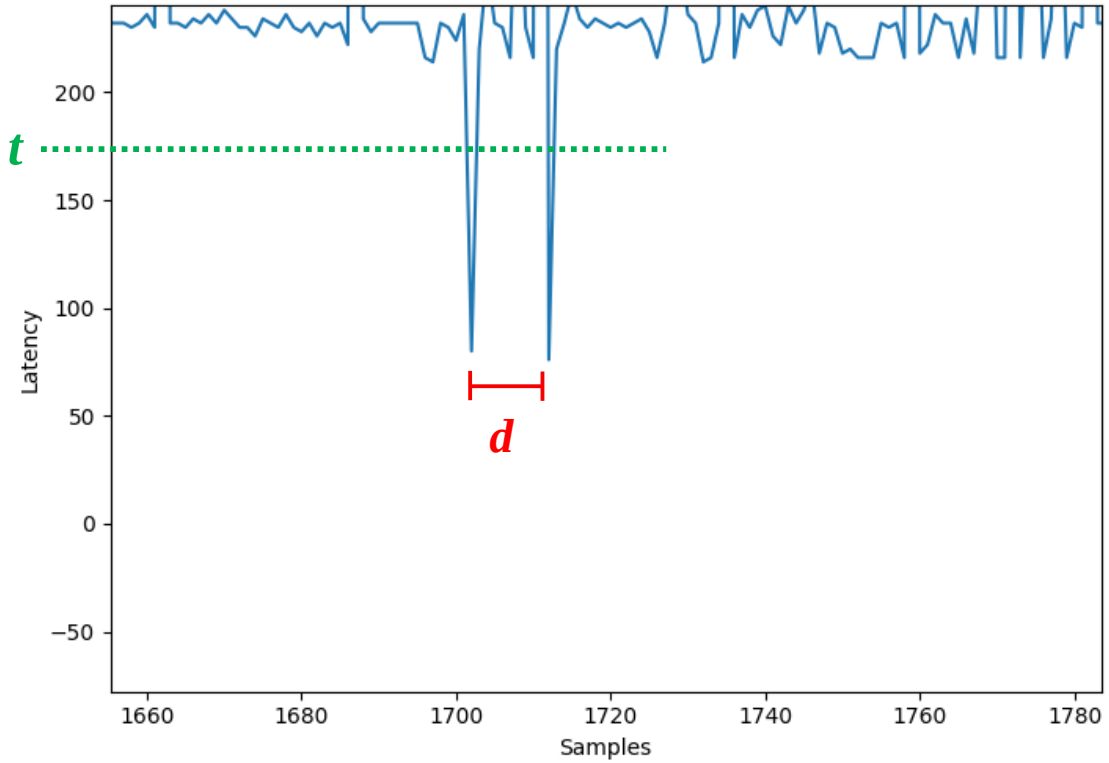
```
33  int DH_compute_key_padded(unsigned char *key,
    ↪   const BIGNUM *pub_key, DH *dh)
34  {
35      int rv, pad;
36      rv = dh->meth->compute_key(key, pub_key, dh);
37      if (rv <= 0)
38          return rv;
39      pad = BN_num_bytes(dh->p) - rv;
40      if (pad > 0) {
41          memmove(key + pad, key, rv);
42          memset(key, 0, pad);
43      }
```

cache line

The Trace



Leakage exploitation approach



Generic attack:

- No optimized per degrade strategy
- Configurable to sweep the parameters set

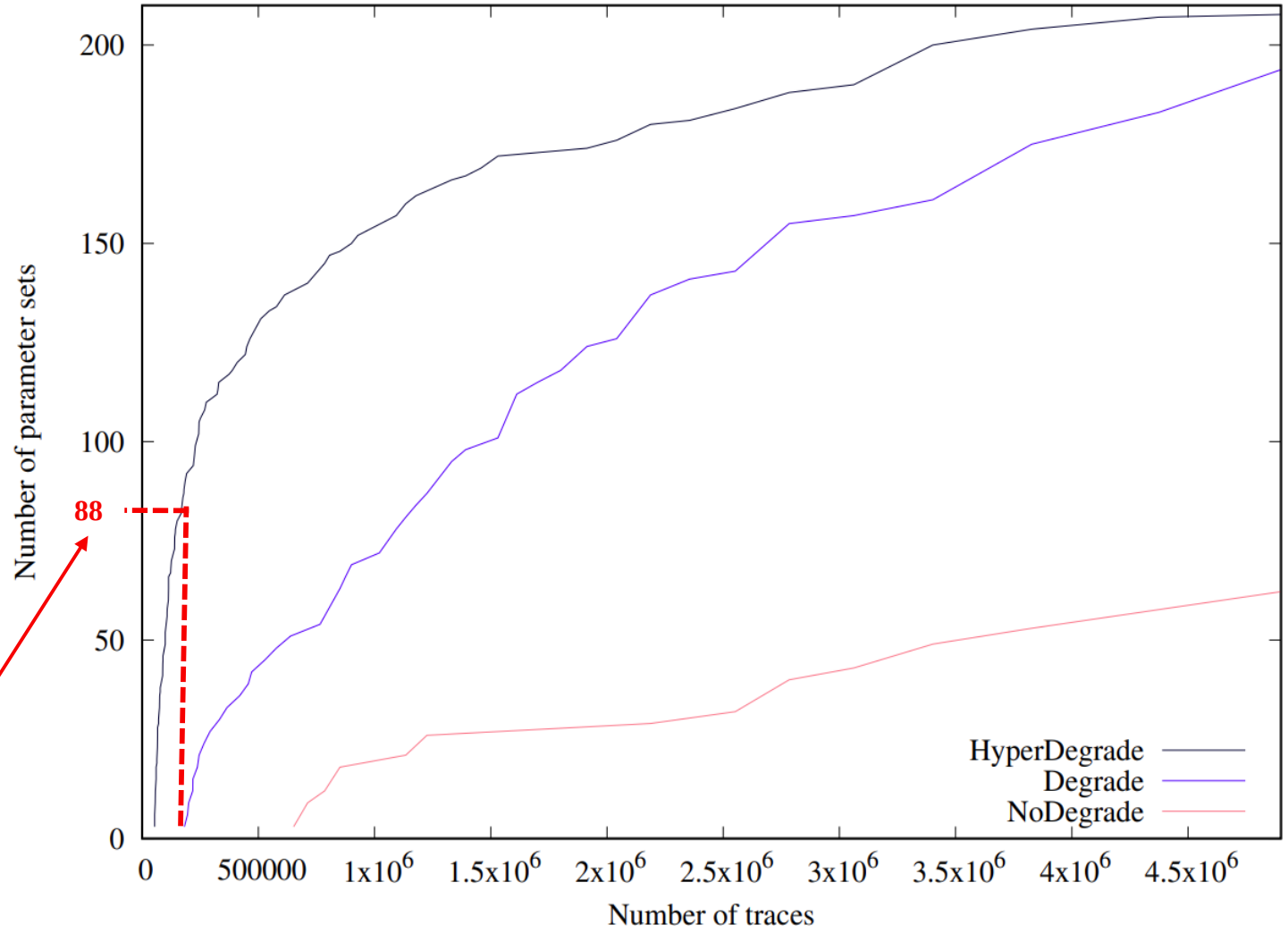
Parameter	Range
Flush+Reload wait time (*r*)	{128, 256}
Cache hit/miss threshold (*t*)	{50, 60,…, 200}
Cache hits distance (*d*)	{1, 5, 10,…, 95}

Experiment results

Best parameter set results:

Strategy	# traces	Reduction
NoDegrade	651,510	1.0x
Degrade	181,189	3.6x
HyperDegrade	53,721	12.1x

HyperDegrade outperforms Degrade in 88 parameters sets



Conclusions

- HyperDegrade requires SMT architectures
- HyperDegrade increases performance degradation
- Machine-clears: additional root cause of original Degrade
- SMC-degrader: slowdown like Degrade w/o its memory requirements
- SMT-contention is not enough
- HyperDegrade reduced # of traces against a Raccoon attack variant

Tampere University

Thank you!

email: alejandro.cabreraaldaya@tuni.fi

artifact: https://zenodo.org/record/5549559

usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION