Covert Timing Channels Exploiting Non-Uniform Memory Access based Architectures

Fan Yao, Guru Venkataramani and Miloš Doroslovački

Department of Electrical and Computer Engineering

The George Washington University

Washington, DC, USA

GLSVLSI 2017, Alberta, Canada

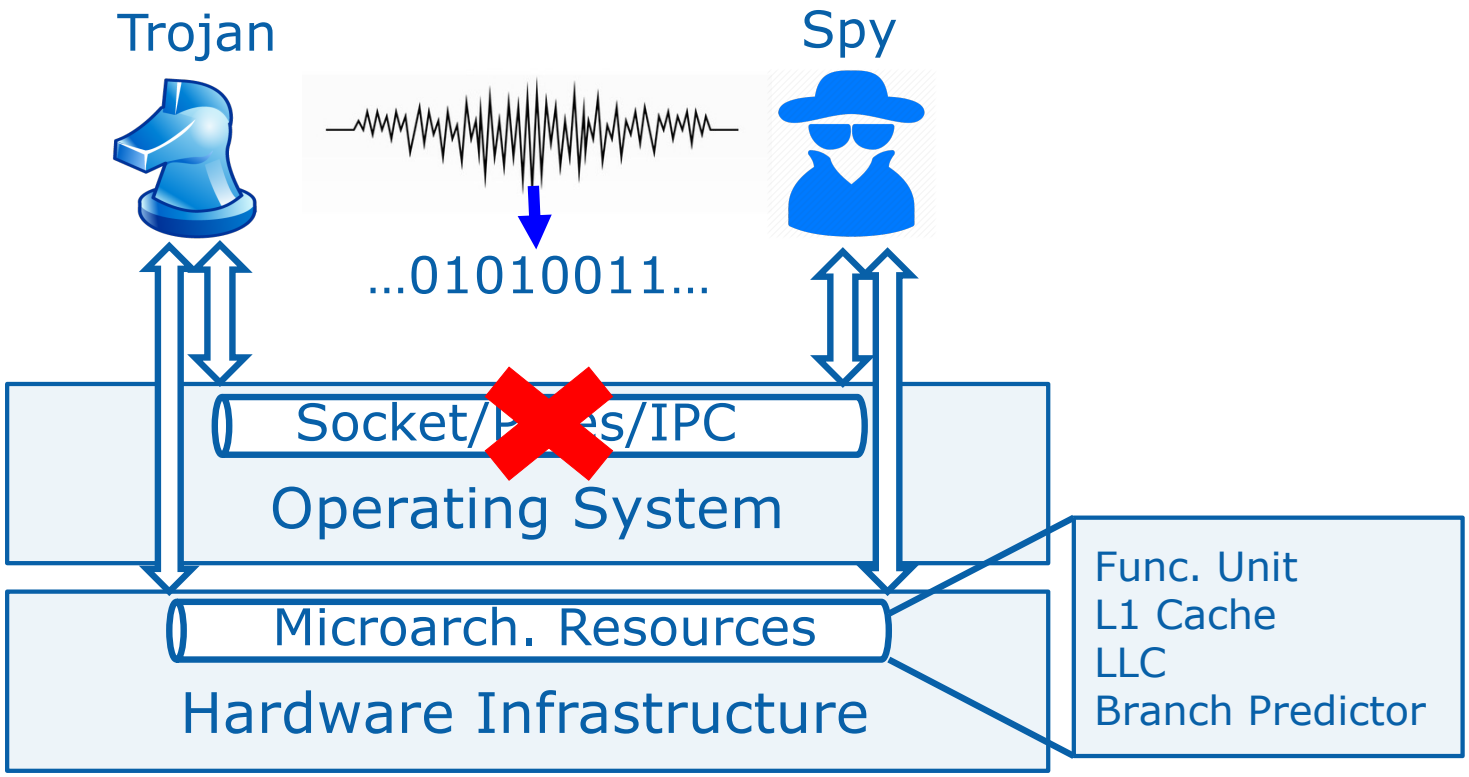
Outline

- Introduction
- NUMA-based Timing Channels
- Demonstration on Real System
- Statistical Quantification
- Conclusion

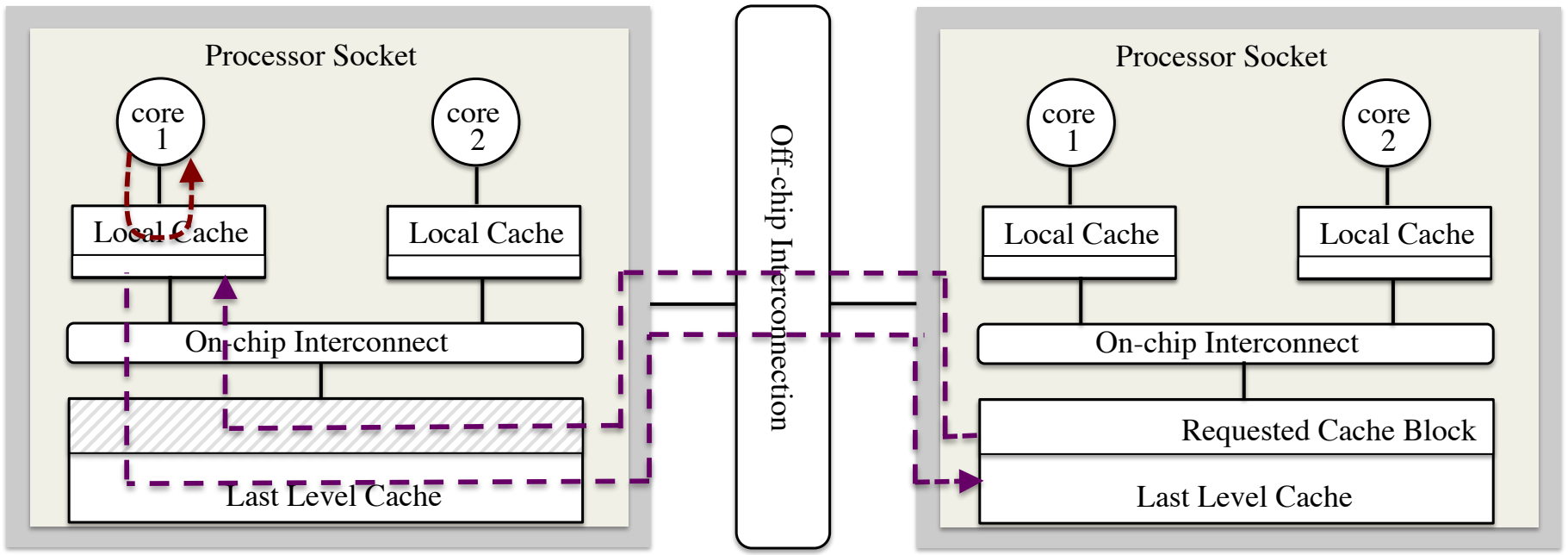
Covert Channels

- **A class of information leakage attacks**
- **Involve two colluding processes**
  - ↗One high privileged, insider process-trojan
  - ↗One low privileged process-spy
- **Covert timing channel**
  - ↗Trojan and spy communicate by modulating timing
- **Different from side channels**
  - ↗Attacker probes the victim to infer secrets in side channel attacks
  - ↗Trojan *intentionally* transmits secrets to spy in covert channel attacks

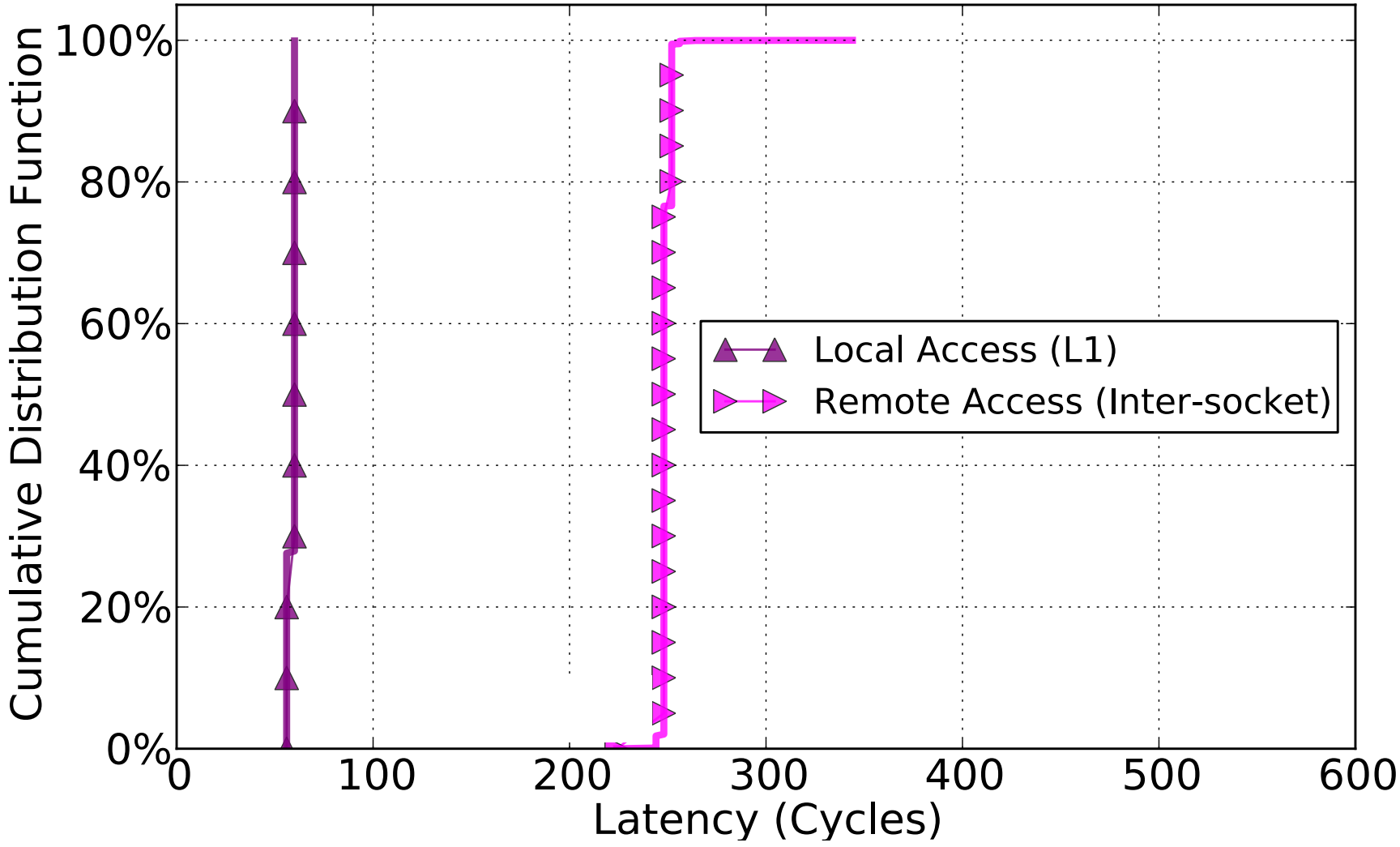
Microarchitecture Covert Timing Channel



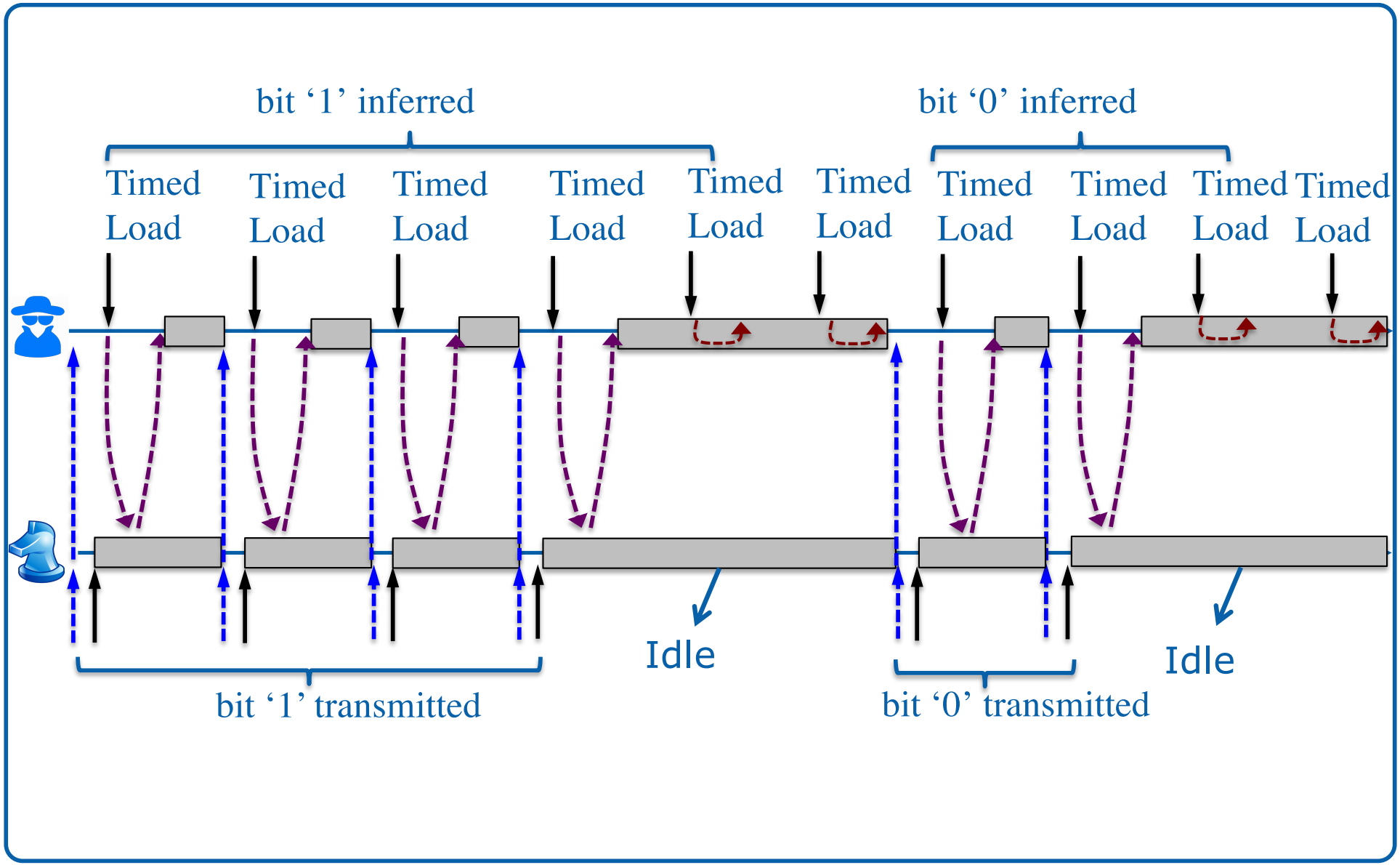
Non-Uniform Memory Access



NUMA Access Latencies Results



Communication Protocol

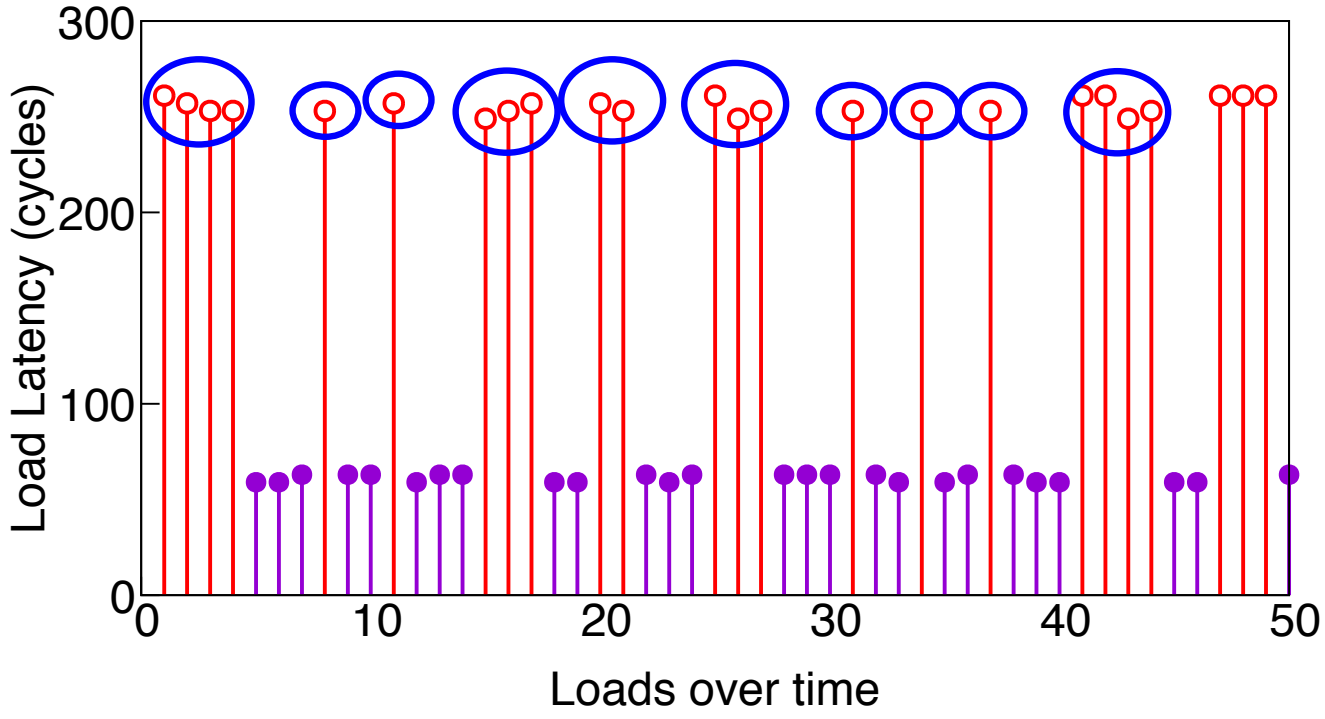


Experimental Setup

- **Hardware Configuration**
  - Dual Socket Xeon X5650 Processor
  - 6 core Processor, 2.67 GHz
  - 32KB L1 Cache, 256KB L2 Cache, 12MB shared L3 cache
- **Software Configuration**
  - Trojan and Spy pinned to distinct sockets (*taskset*)
  - For communication, shared library is used (libgcrypt.so)

Timing Channel Demonstration

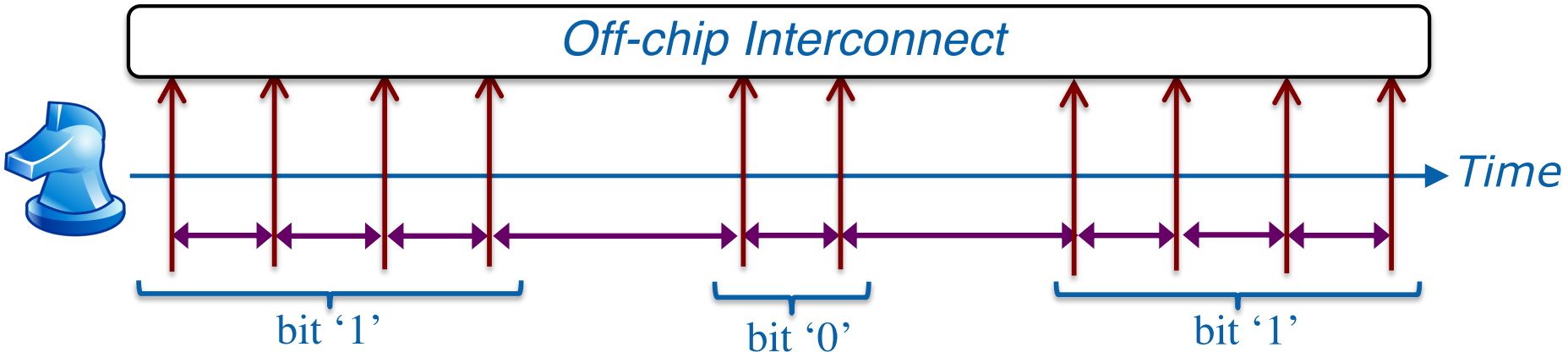
- **Trojan's secrete bits to transmit**
  ↗1001010001
- **Spy's latency reception**



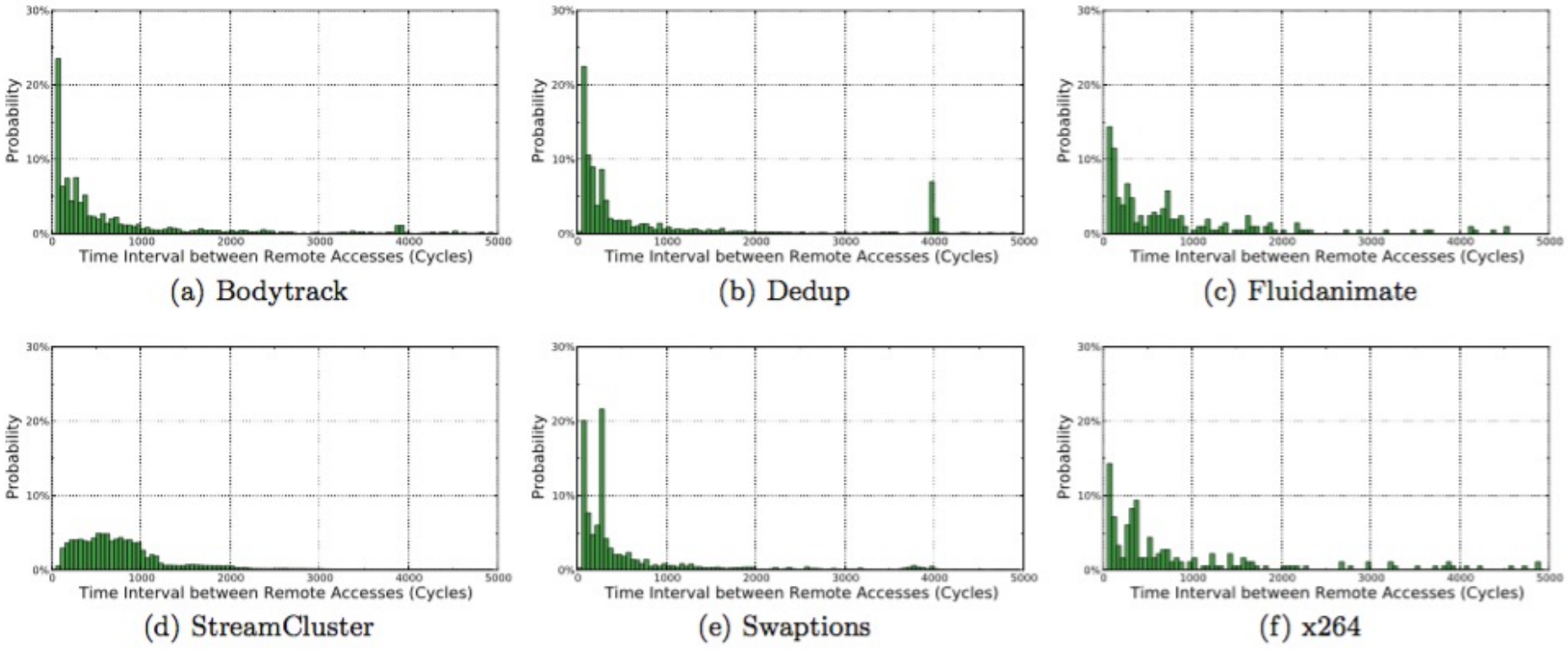
Measured transmission rate:190 Kbps

Timing Channel Analysis

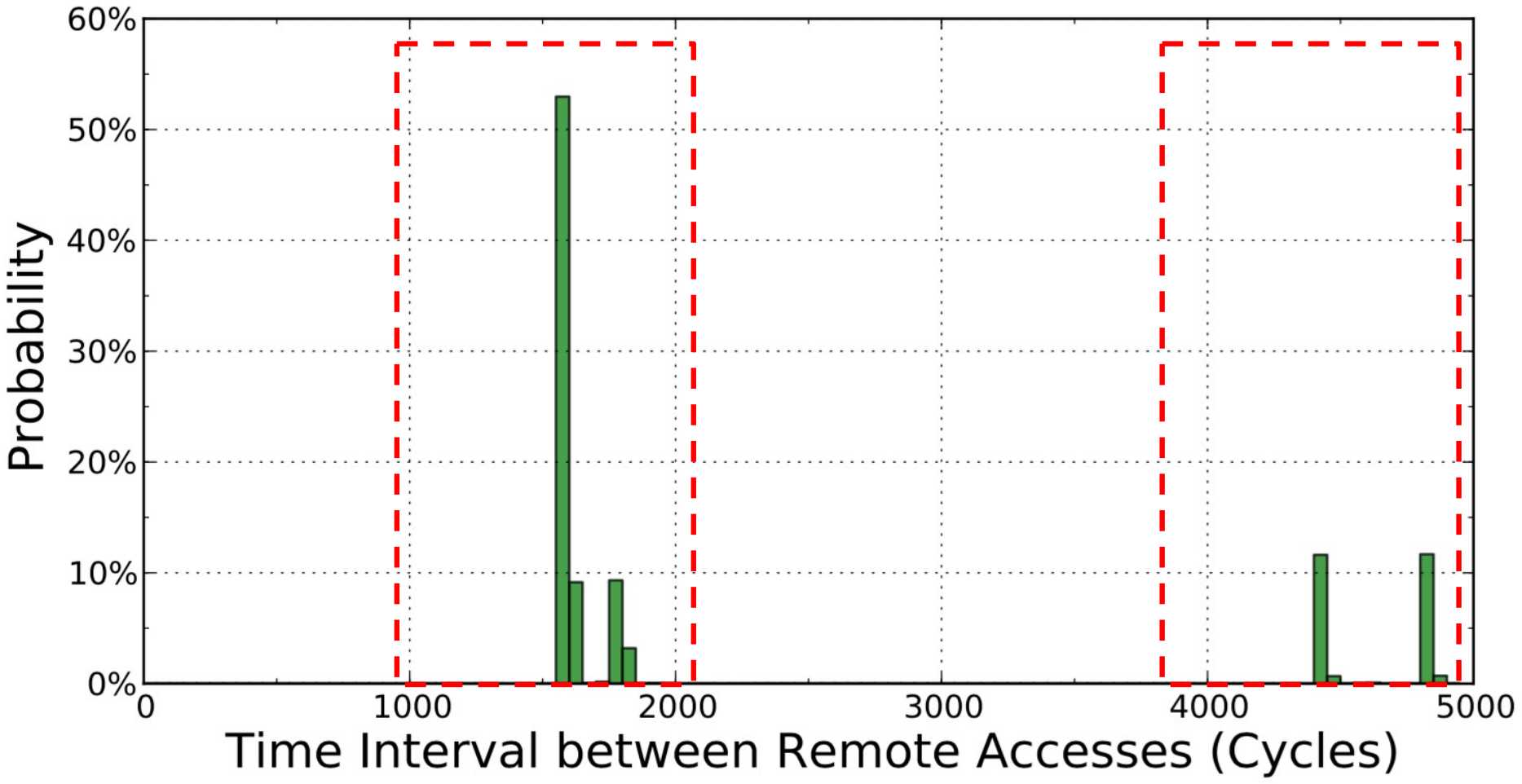
- **Observations**
  - ➚Inter-socket data transfers are manipulated by the Trojan
    - ➔Can we infer timing channels from time interval between two consecutive remote accesses?



Time-Interval – PARSEC Benchmarks



Time-Intervals – NUMA Covert Timing Channels



Quantifying NUMA Covert Channels - Approach

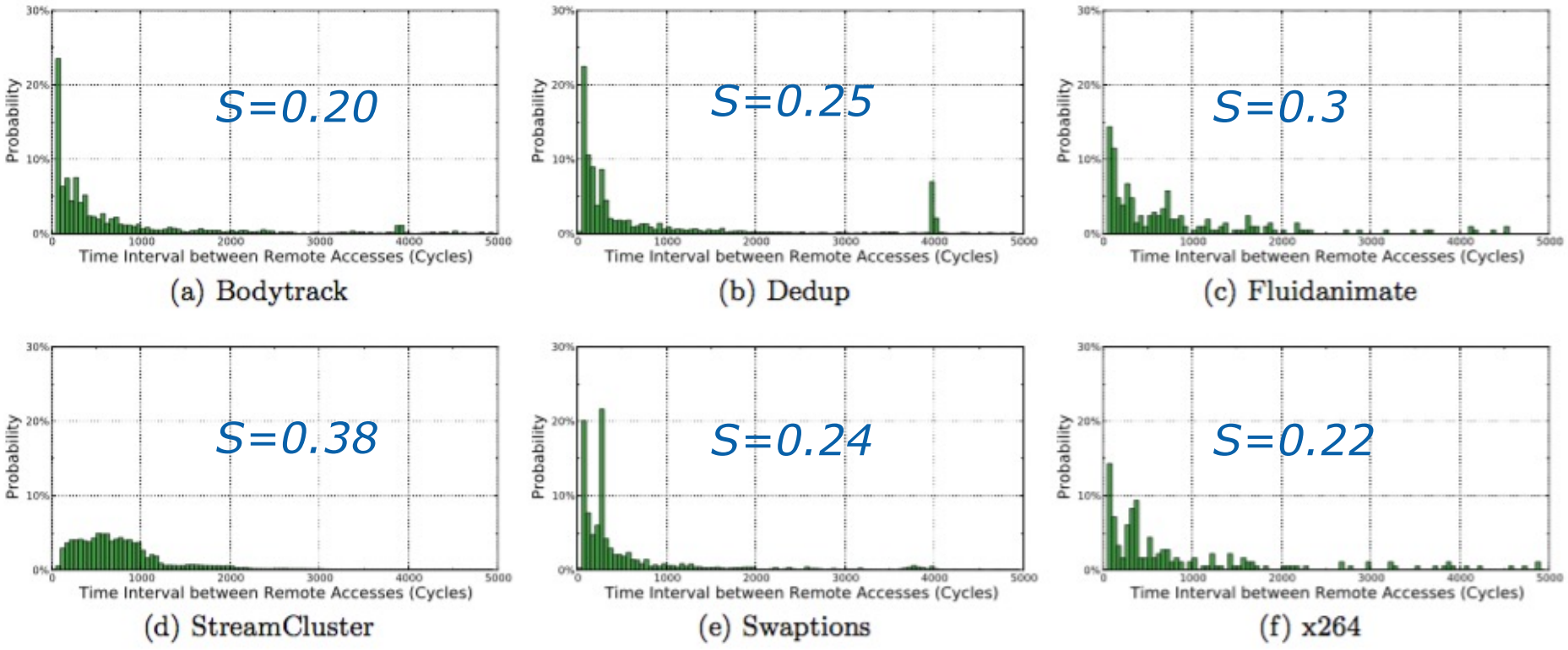
- **Statistically Quantify the Time-Interval Distribution**
  - ↗Legitimate application's time-interval would be more random
  - ↗Use Degree of Sparseness to quantify such character

- **Degree of Sparseness**

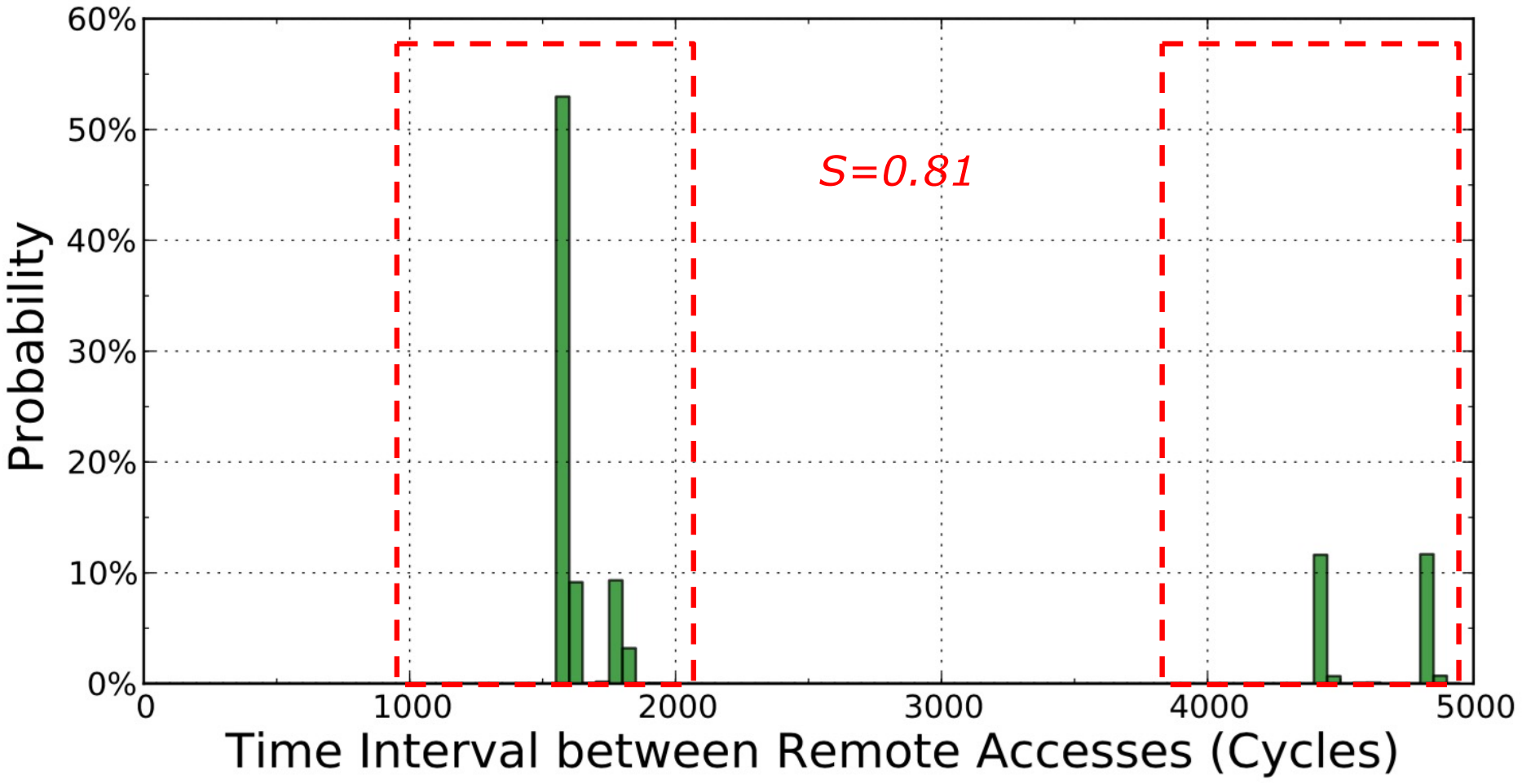
$$S = \frac{M}{M - \sqrt{M}}\left(1 - \frac{\|P\|_1}{\sqrt{M} \times \|P\|_2}\right)$$

  - ↗Where M is the number of samples, P the the sample set
  - ↗$\|P\|_1$ and $\|P\|_2$ are norm1 and norm2 of P respectively.
  - ↗0 means not sparse and 1 means extremely sparse

Time-Interval – PARSEC Benchmarks



Time-Intervals – NUMA Covert Timing Channels



Conclusion

- **We developed a covert timing channel that exploits NUMA latency differences.**

- **We demonstrated an inter-socket multiple cache attack.**

- **We performed statistical analysis to quantify the presence of such attacks.**
  - ↗Can help design defense mechanisms.

- **Acknowledgement**

Email: albertyao@gwu.edu

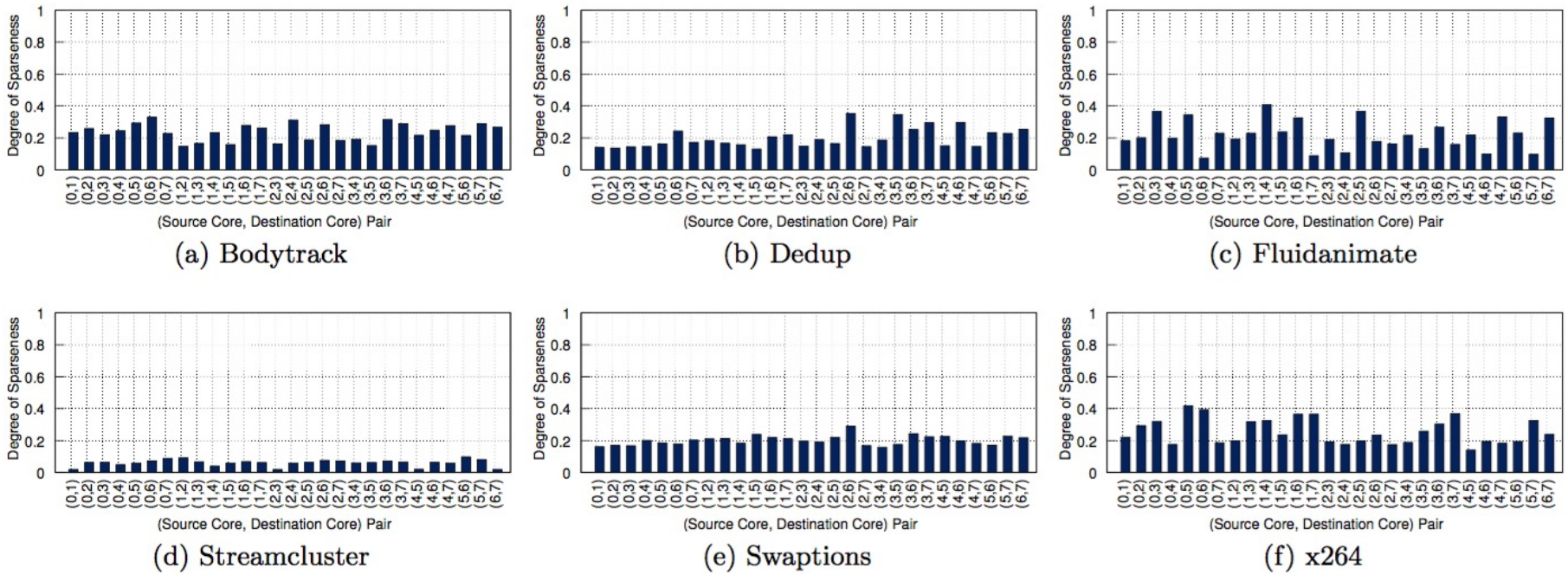
Simulation Setup

- **Gem5 – Cycle accurate full system simulation**
  - 8 CMP Cores
  - Two Level Cache Architectures
  - Minimal Linux distribution with kernel version 2.6.32

- **Benchmark**
  - PARSEC Benchmark 2.1
    - Compiled with 8 threads (pthreads)
  - A prototype implementation of Trojan and Spy
    - Trojan and Spy pinned to different cores

Quantifying NUMA Covert Channels - Results

- **PARSEC Benchmarks**



- **NUMA-based Covert Timing Channels**
  - ↗ 0.81
  - ↗Sufficiently different from the sparseness for normal applications