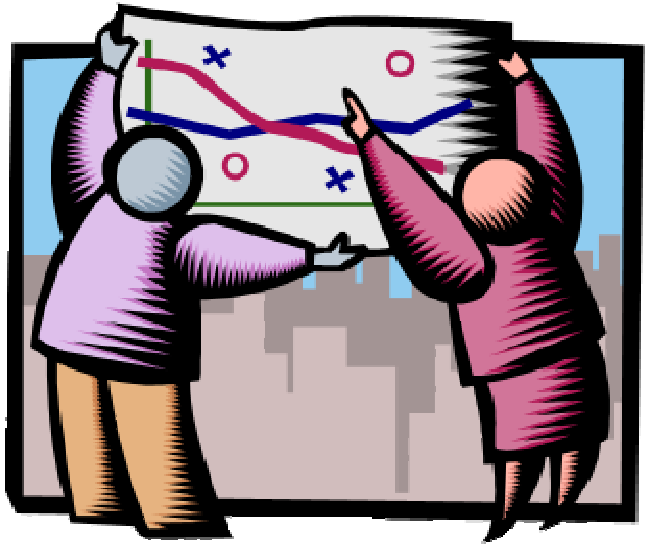
CHES 2009 Panel: Benchmarking of Cryptographic Hardware

Patrick Schaumont
Virginia Tech
September 2009



Benchmarking Crypto-Hardware

- There are **60** tables in the 27 papers from CHES 2008
- **34** of these 60 tables compare hardware implementations
- **11** of these 34 tables compare results from different publications

- Clearly, the CHES community likes to compare (=benchmark)

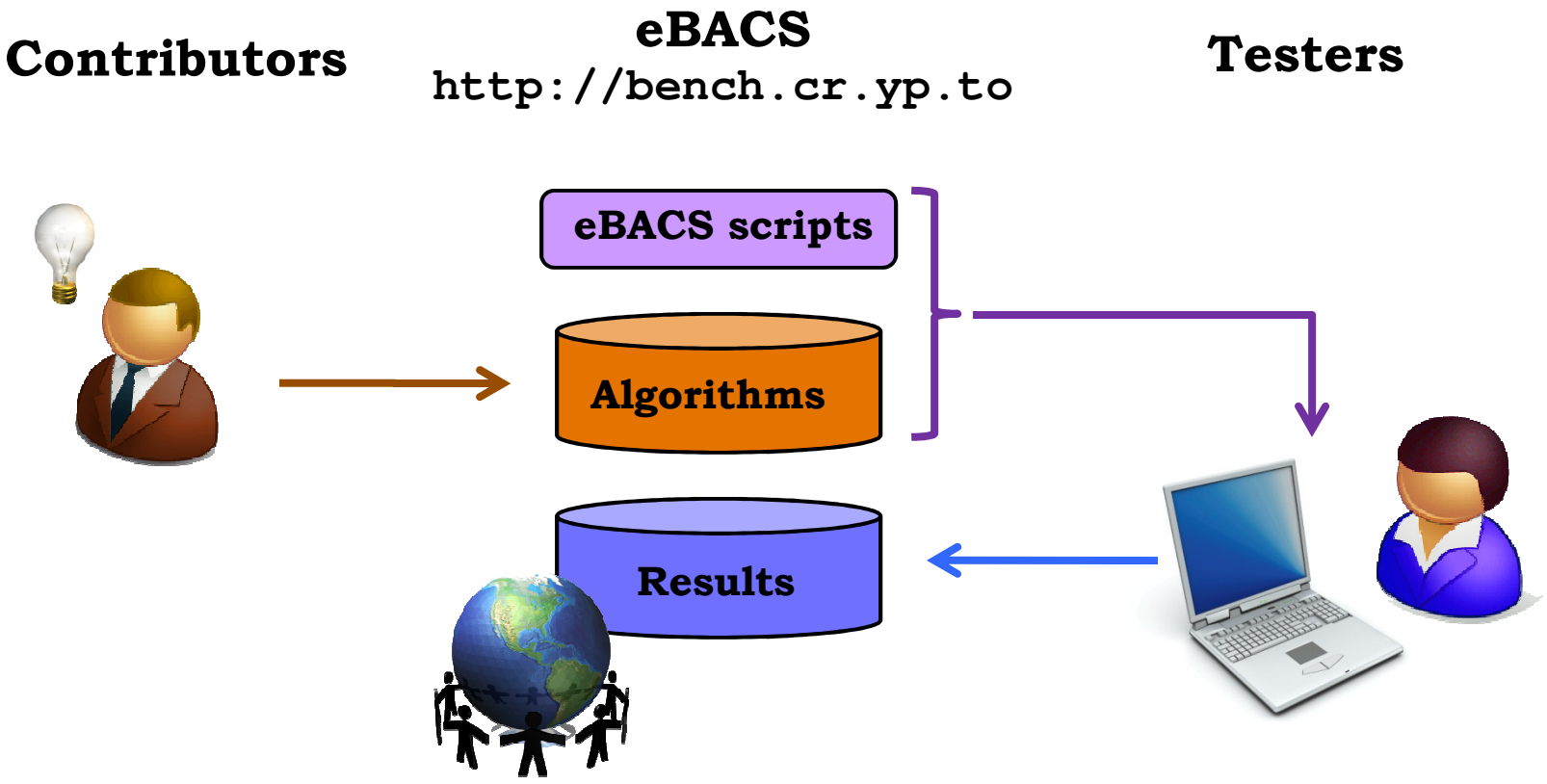
The common ground is vague

- **Hardware Cost**: Slices, Slices Occupied, LUTs, 4-input LUTs, FFs, FDS, Gate Equivalent GE, Size on ASIC, DSP Blocks, BRAMS, Number of Cores, CLB, LS, µP, MUL, XOR, NOT, AND
- **Hardware Performance**: cycles per block, cycles per byte, Modexp/s, PointMul/s, Latency (cycles), t_{delay}, F_{Max}, Time-Area product (clock-cycles slices), Critical Path, Throughput at 100 KHz
- **Hardware efficiency**: Kbps/gate

Ergo:

1. **Everybody's using a metric that makes his/her design look "better" ?**
2. **Nobody really knows how to measure security, power, energy**

Benchmarking Crypto-Software



Question 1

- Is it possible to create a standard method to benchmark cryptographic hardware?
  - If yes, how?
  - If no, why not?

Question 2

- How do we collect and report hardware metrics of cryptographic hardware?
  - How do we define "better"? power? energy? area-time? ..?

Panelists

- **Saar Drimer** (Cambridge, UK)
  - http://www.cl.cam.ac.uk/~sd410/papers/fpga_survey.pdf
- **Daniel J. Bernstein** (UIC, IL)
  - eBACS author (with Tanja Lange)
- **Peter Alfke** (as himself / Xilinx)
  - Notorious comp.arch.fpga educator
- **Kris Gaj** (GMU, VA)
  - FPGA Crypto-benchmarks for AES, eSTREAM
- **Frank K. Gürkaynak** (ETHZ, CH)
  - ASIC Crypto-benchmarks for eSTREAM