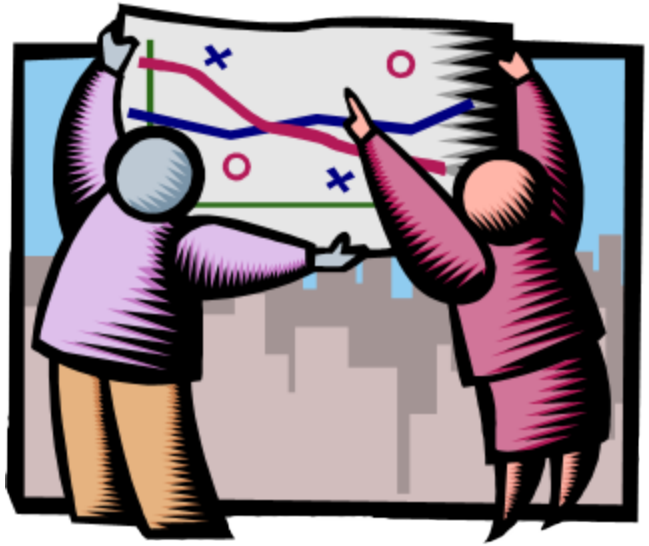
Post Layout Results are Required

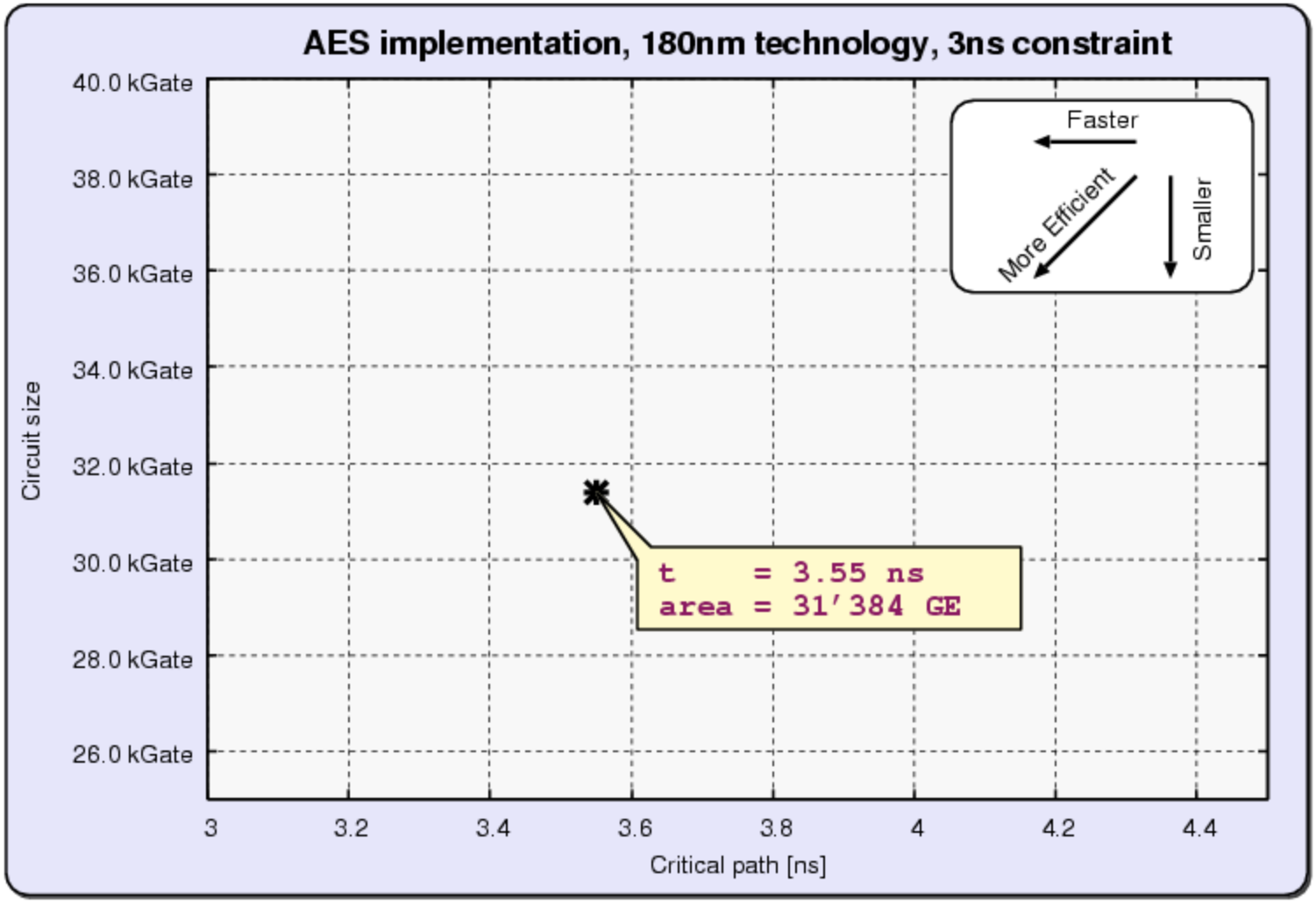
Frank K Gurkaynak
ETHZ
September 2009



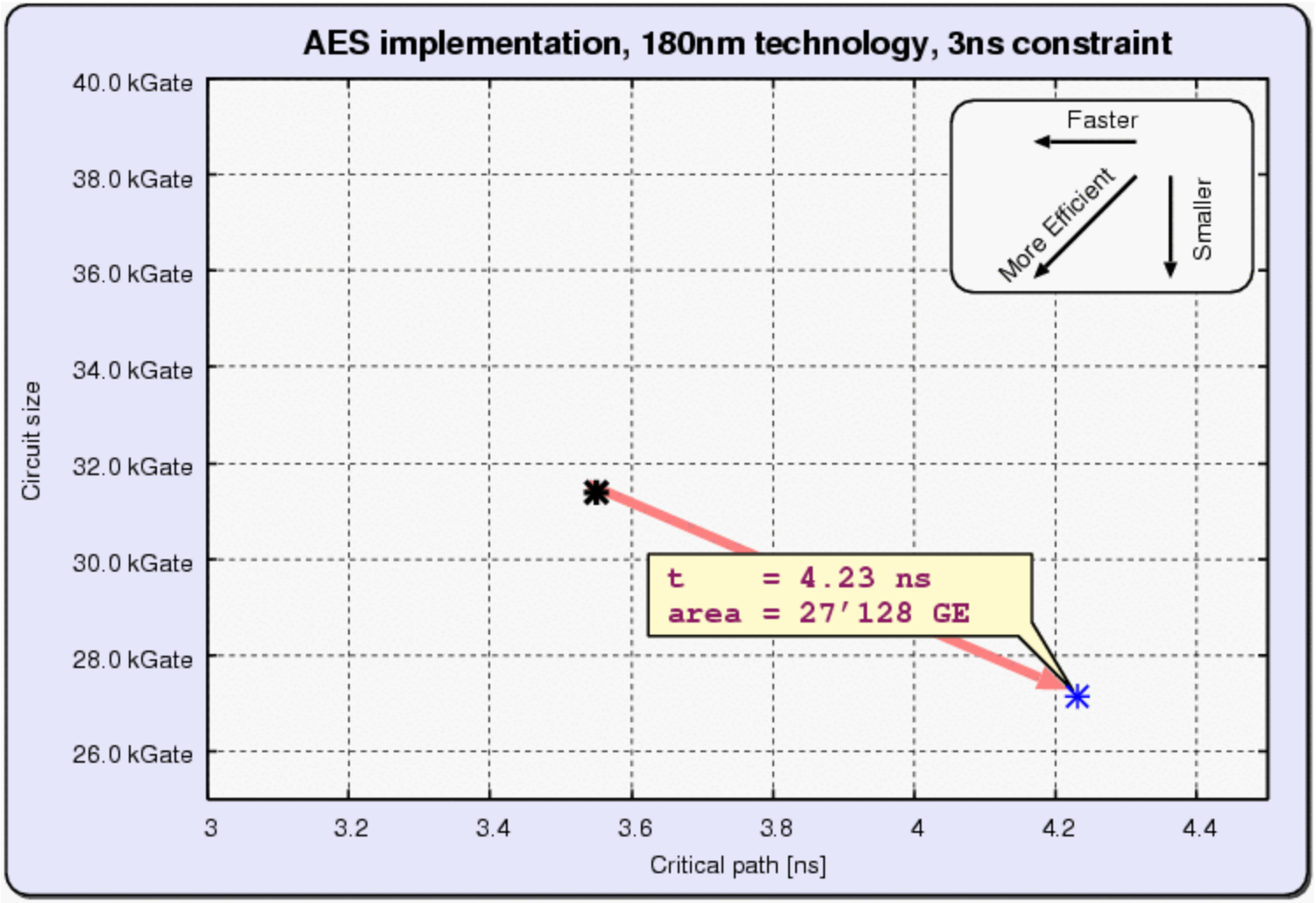
Post-layout results are required

- For some (not all) designs, post-layout results **can deviate significantly** from synthesis results. Can't live without them!
- There is no recipe for getting post-layout results:
  - Standard EDA tools are designed to '**fulfill given constraints**' and not to find the 'best possible solution'
  - Most EDA tools employ **proprietary algorithms**, essentially users do not know how exactly the program works.
  - Tools rely on heuristic algorithms which show **large variations**.
  - Results **depend on many factors**: the technology used, the standard cell library, the synthesis tool, synthesis constraints, the floorplan, placement algorithm, routing algorithm, .. etc

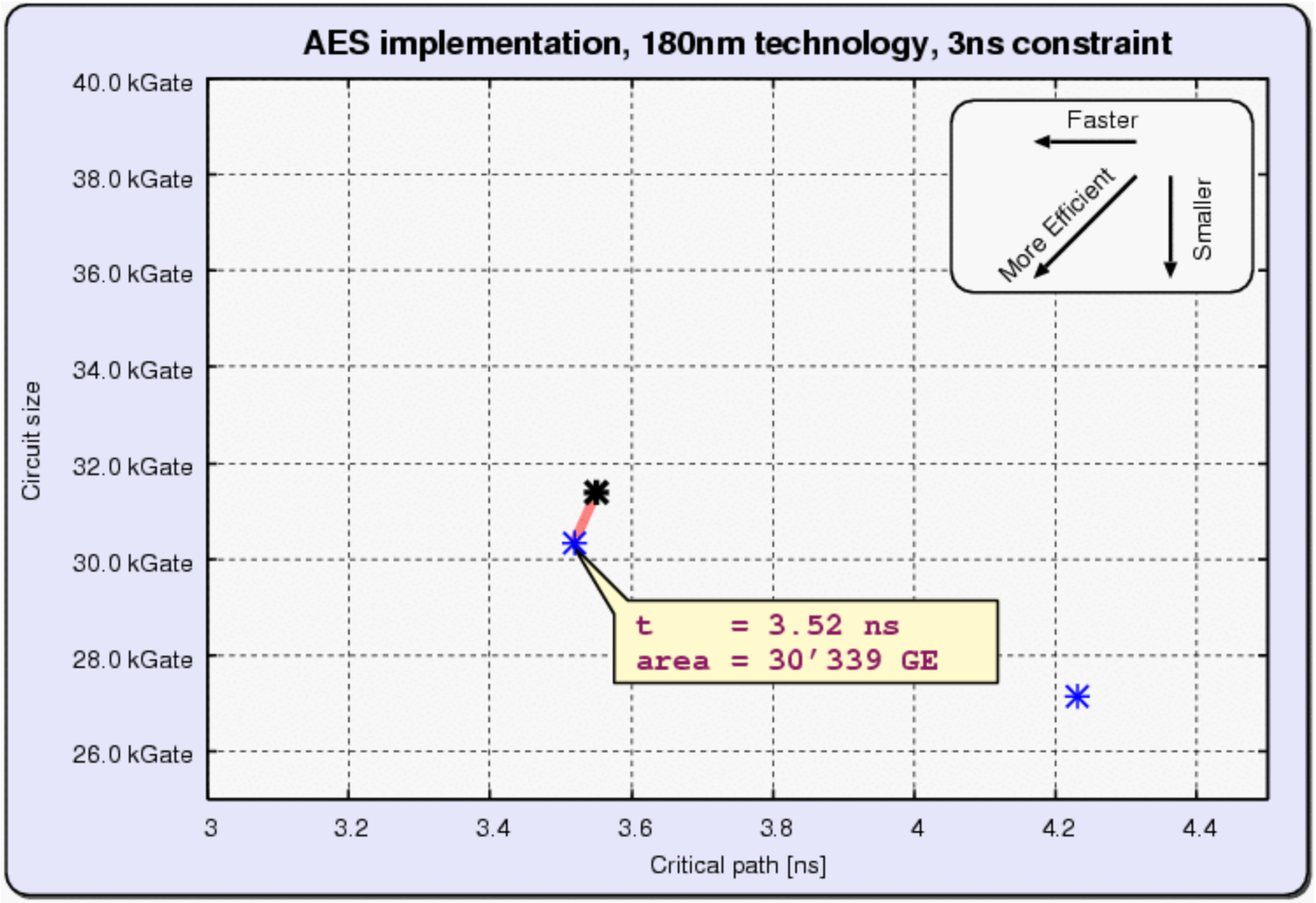
Results can be deceiving



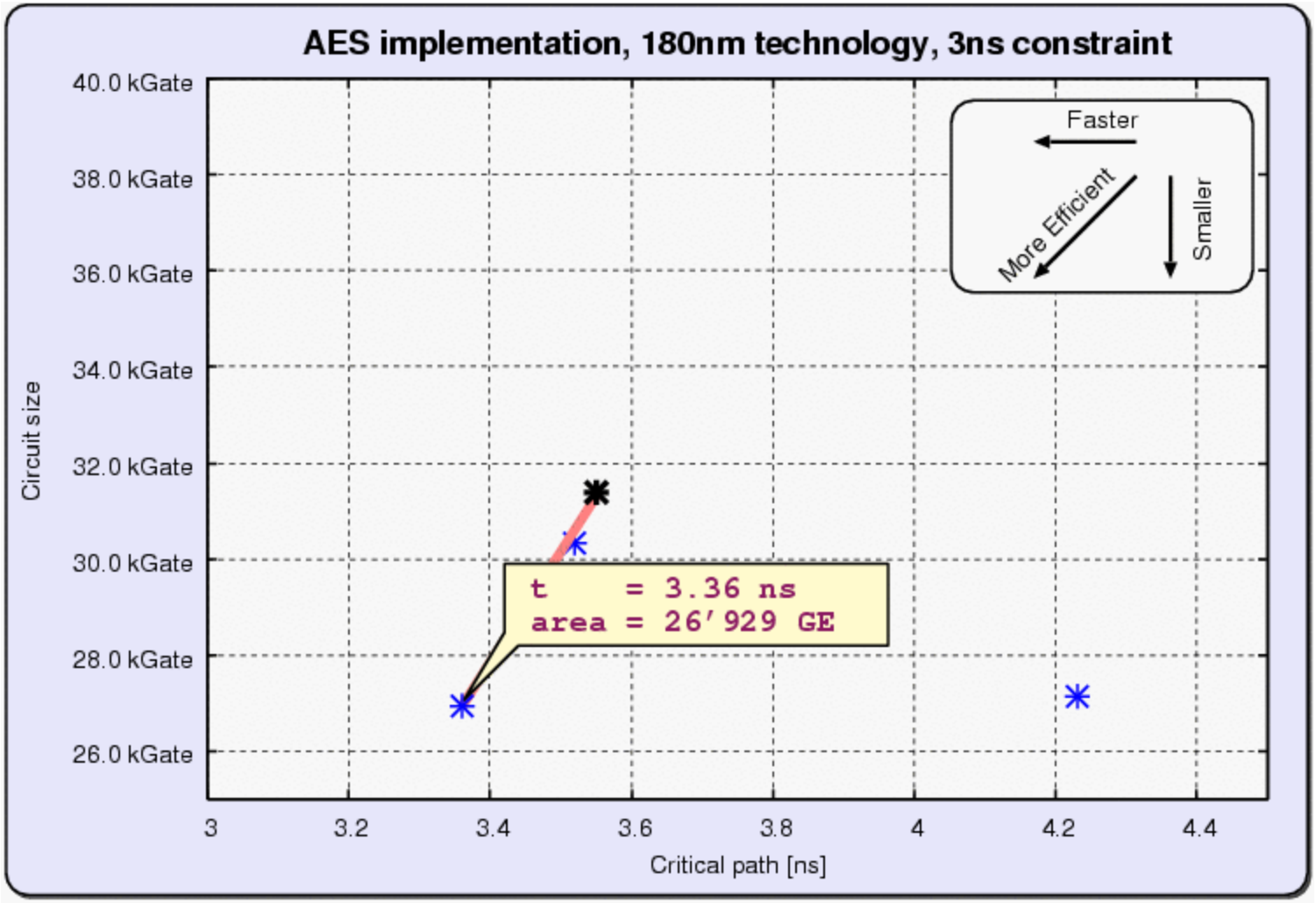
Different standard cell library



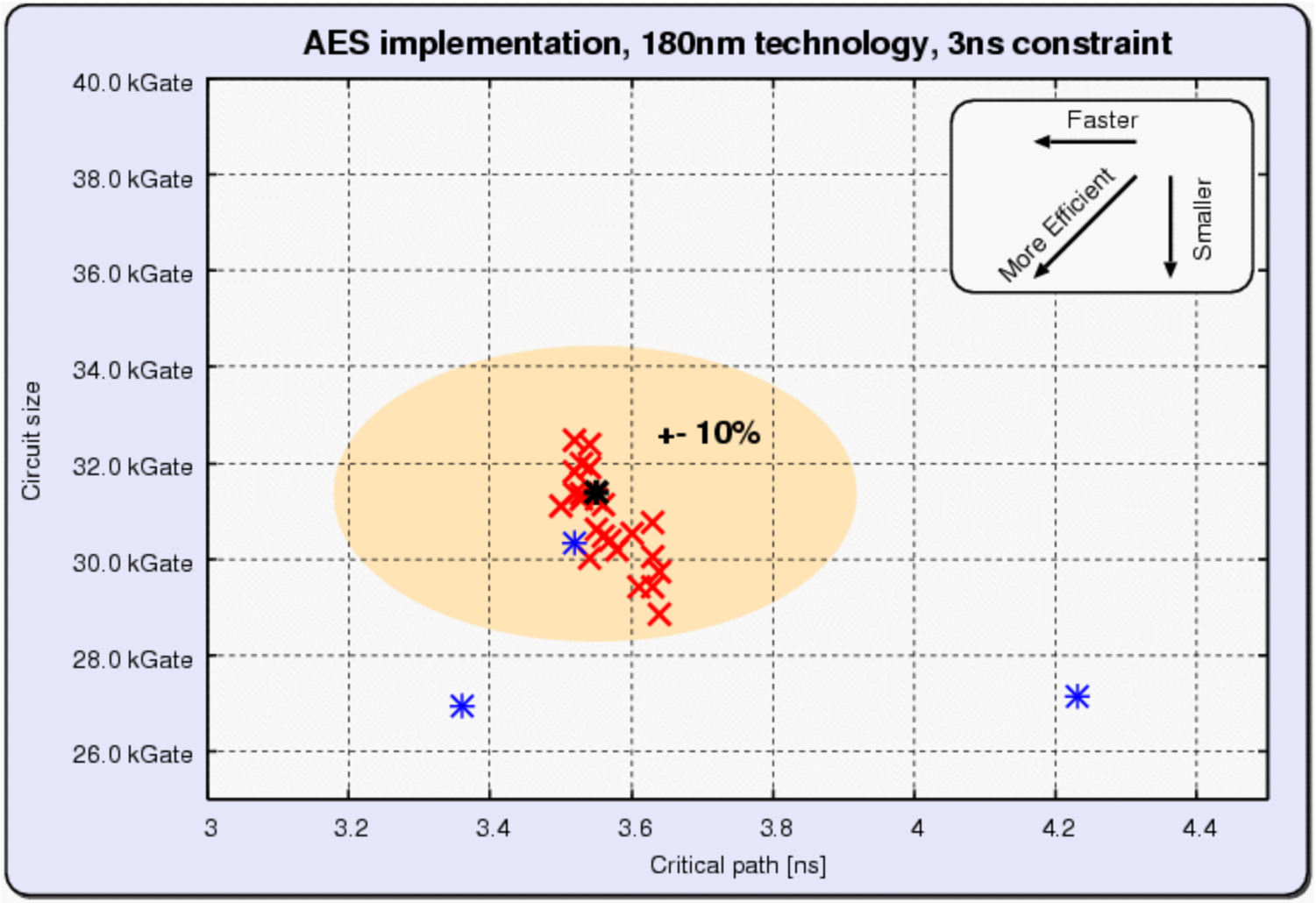
Different version of synthesis program



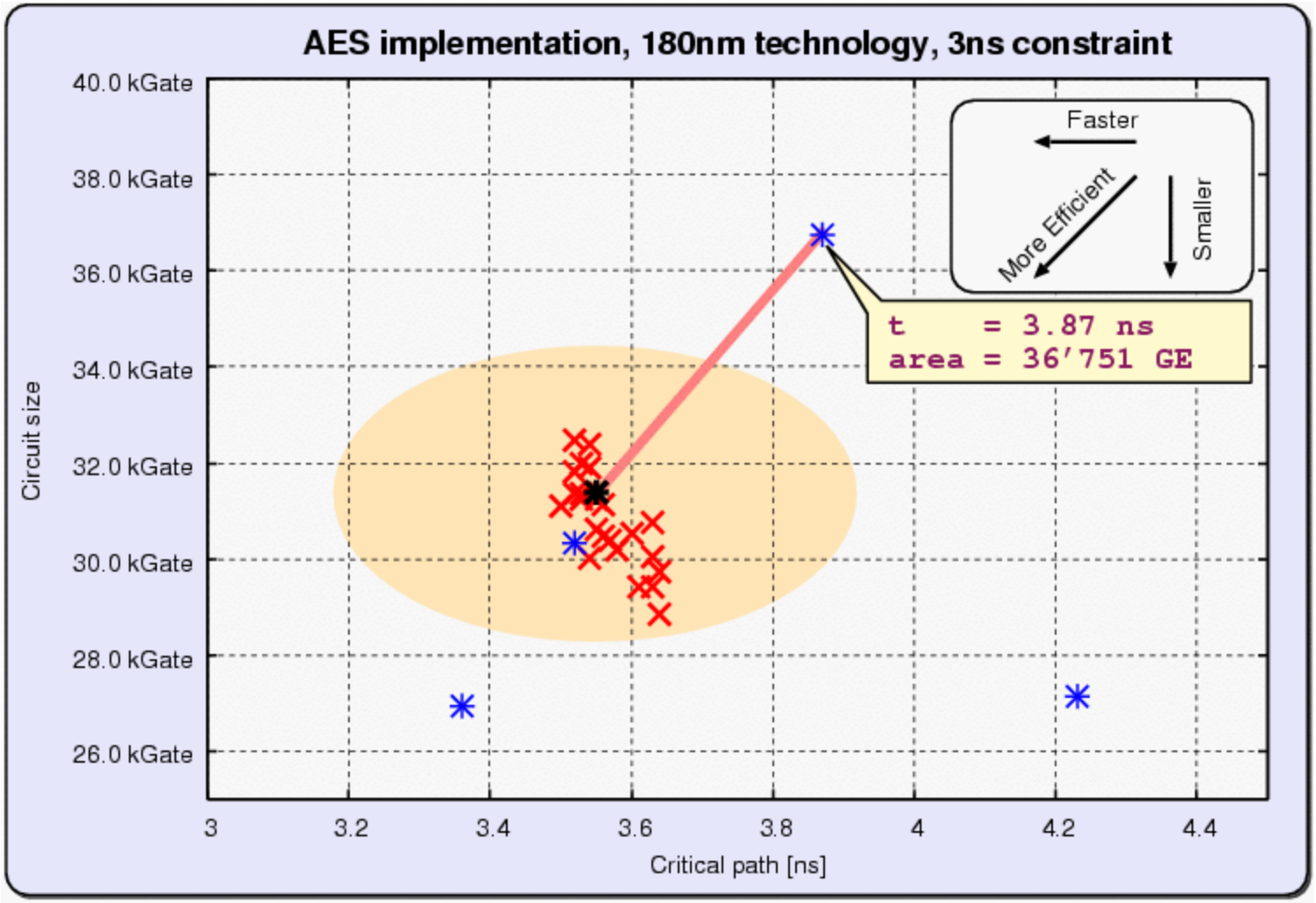
Different compile option



Different timing constraints (<3ns)

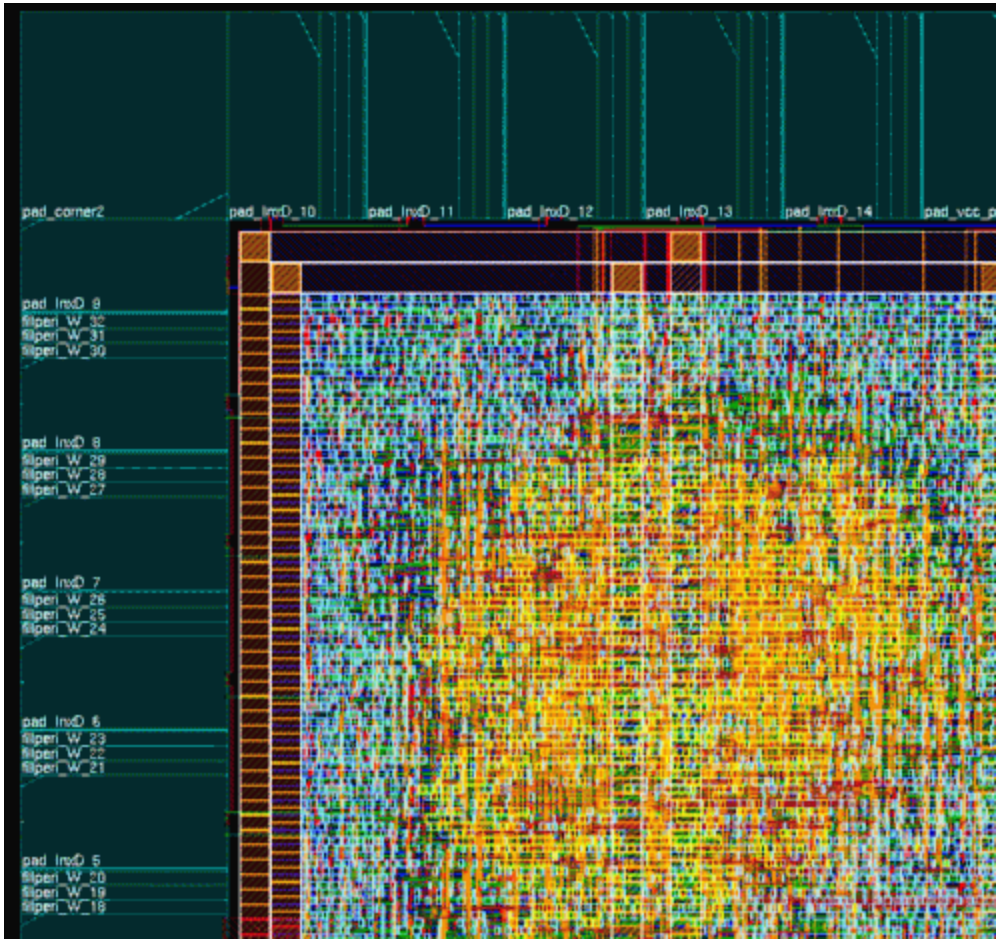


Post-layout result, total core area



Post-layout has significant overhead

- I/O pads
- Power routing
- Clock Trees
- Additional area for routing
- Filler cells for decoupling
- Scan/Test overhead
- I/O Interface



Difficult to separate overhead from actual circuit

10 years of AES papers

What were the most interesting results:

- Basic implementation. (how fast, large)
- Cost of implementing options of the algorithm. (encoding/decoding, 128/192/256 bit)
- Tradeoffs between Area and Speed. (datapath width 8bit – 128 bit)
- Interesting architectural alternatives
  - Implementing SubBytes (Lookup table or decomposition)
  - Shared inverse multiplication between encoding and decoding
  - Subkey generation (stored, on the fly)

What to avoid

- Reporting on performance of ASICs you can not realistically manufacture or test; your designs may not be practical.

  Very advanced technologies (45nm or less), predictive technology models, excessively high (>1 GHz) clock rates, exotic heterogeneous manufacturing technologies.

- Stating area in absolute numbers (mm^2)

  It is not easy to compare to known quantities.

- Basing a paper on improvements less than 10% in performance.

  Can be due to variations in design flow.

- Making very fine grained optimizations.

  i.e. removing the reset input of several FFs to save 10 gate equivalents in the overall design.

What can be done?

- IACR could **publish a set guidelines** and or requirements for reporting performance.

  i.e. state technology, metal options, library vendors, tool versions. Report area taking the core area of placed and routed design using kgate equivalents etc.

- IACR could **publish base HDL** implementations of algorithms, including testbenches.

  Submissions would be required to compare against these implementations.

- IACR could **advocate a specific ASIC technology**, FPGA platform for HW comparisons, and update these every 3/5 years.

  Submissions could include other technologies as well.