Emerging New Stream Ciphers vs. AES Comparative Study of Hardware Performance

Kris Gaj
Gabriel Southern
Ramakrishna Bachimanchi
Pawel Chodowiec
&
Fall 2006 GMU ECE 545: Introduction to VHDL class

George Mason University

ECRYPT

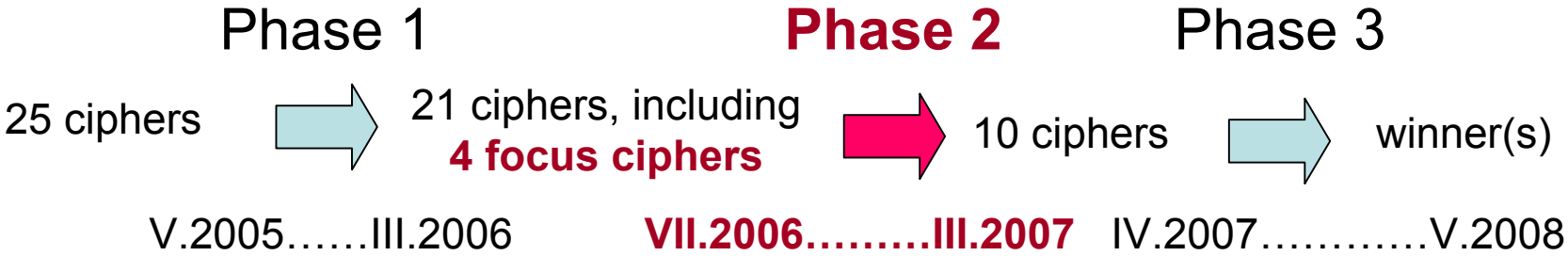
eSTREAM - Contest for a new stream cipher standard, 2004-2008

PROFILE 1

- Stream cipher suitable for **software implementations**

PROFILE 2

- Stream cipher suitable for **hardware implementations** with **limited memory, number of gates, or power supply**
- Key size – minimum 80 bits
- Initialization vector – 32 bits or 64 bits



Goal of Our Project

Comparison of Profile II (hardware) Phase 2 Focus candidates:

- Grain
- Mickey-128
- Phelix
- Trivium

Two additional reference points:

- A5/1 (old & insecure GSM standard)
- AES (compact architecture & basic architecture)

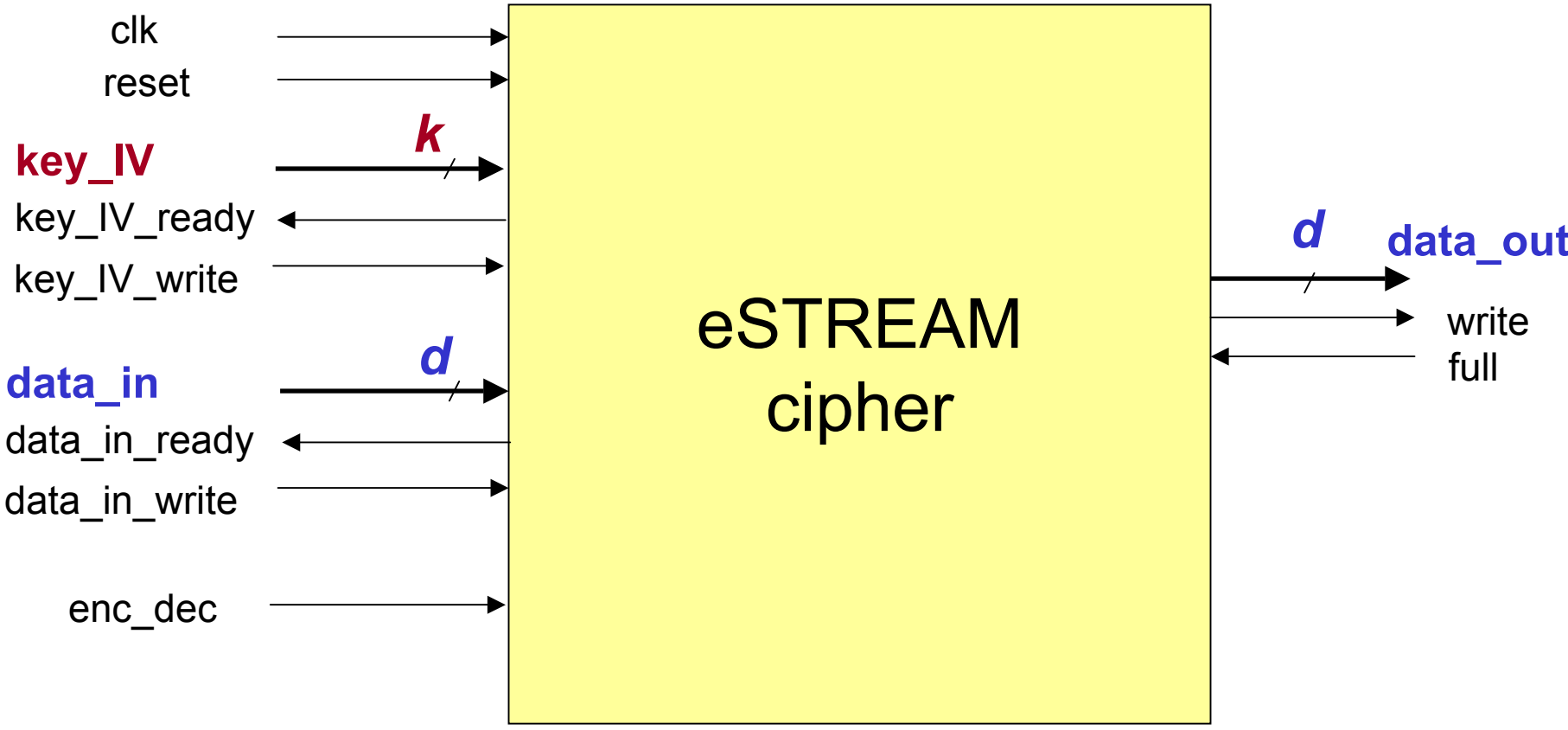
Two hardware technologies:

- Xilinx Spartan 3 FPGAs
- TSMC 90 nm standard-cell library ASICs

Genesis & approach

- Part of GMU Fall 2006 graduate course
  ECE 545 Introduction to VHDL
- Individual 6-week project
- 4 students working independently on each eSTREAM cipher
- best code for each algorithm selected at the end of the semester
- selected designs verified and revised in order to assure
  - correct functionality
  - standard interface & control
  - uniform design & coding style

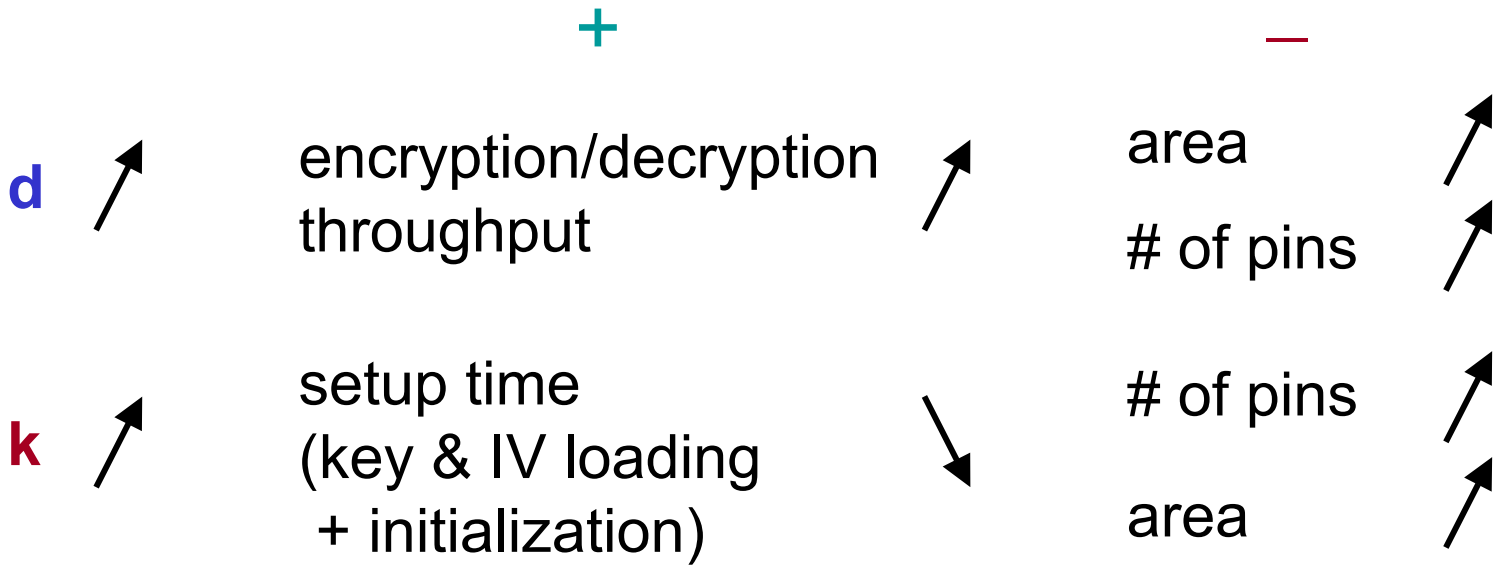
Fixed interface



Two independent parameters

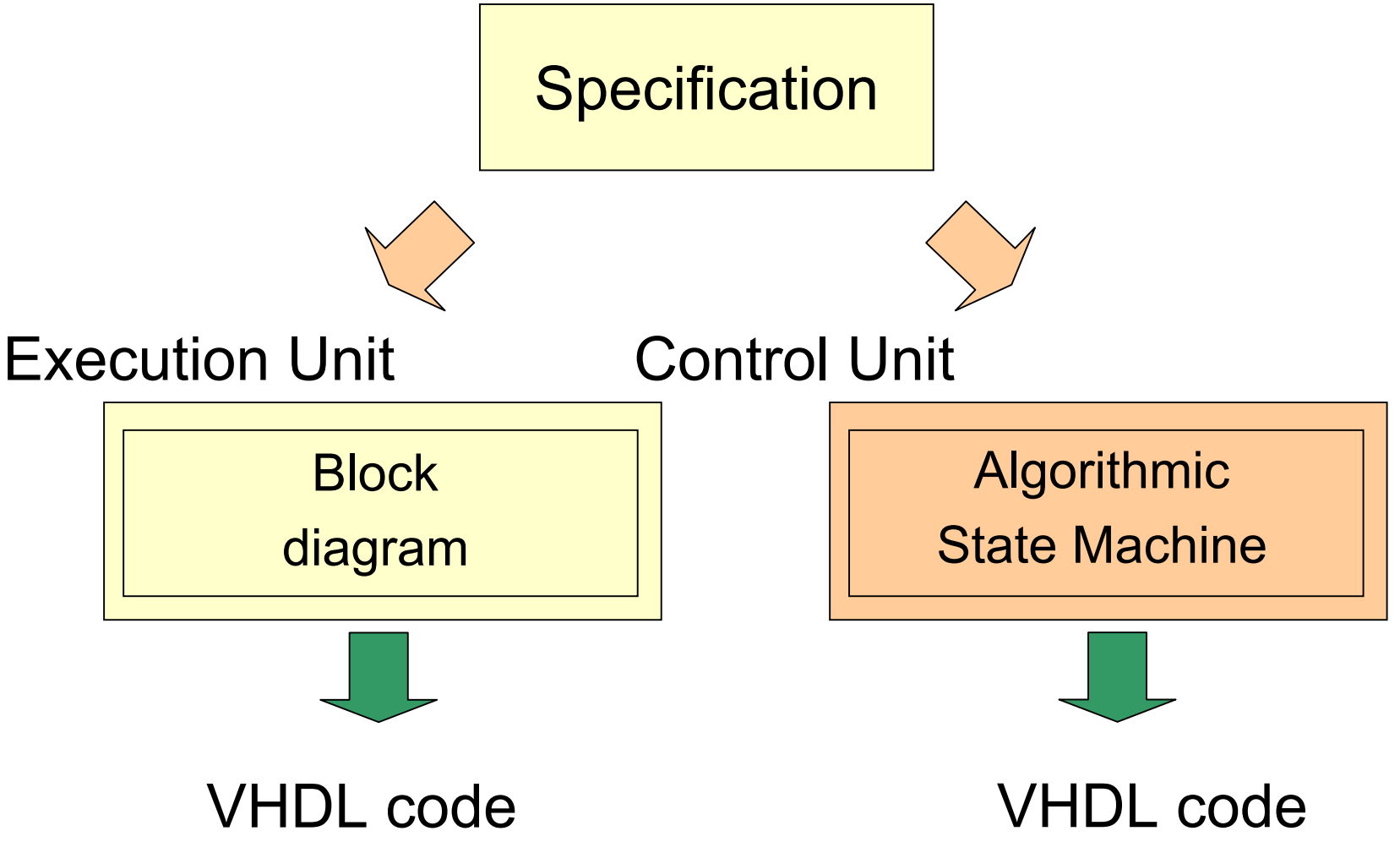
d – number of bits processed per clock cycle (radix)

k – number of bits of key/IV loaded per clock cycle



All results generated with **k = d**

Methodology



Methodology & tools

Technology	FPGA	ASIC
VHDL simulation & debugging	Aldec Active HDL ModelSim Xilinx Edition	
Logic synthesis	Synplicity **Synplify Pro** v. 8.5	Synopsys **Design Analyzer** X-2005.9
Implementation (mapping, placing & routing)	**Xilinx ISE** v. 8.1i	**No physical implementation**

All results **after placing & routing**

All results **after logic synthesis**

Assumptions

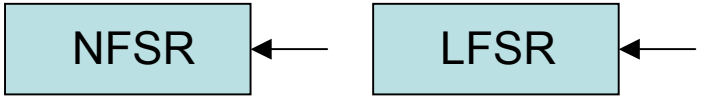
- Only encryption/decryption, **no MAC**
- **Maximum** allowed **key and IV sizes**

Cipher22	Key size	IV size	Internal state size
Grain	80	64	160
Mickey-128	128	**128**	320
Phelix	**256**	128	288
Trivium	80	80	288
A5/1	64	22	64

- **Key and IV need to be reloaded** each time either of them changes
- **No precomputations of internal state** outside of the circuit
- **Registered data output**

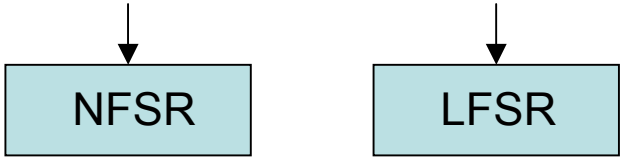
Three categories of stream ciphers represented among those implemented

Based on
LFSRs / NFSRs
with serial inputs



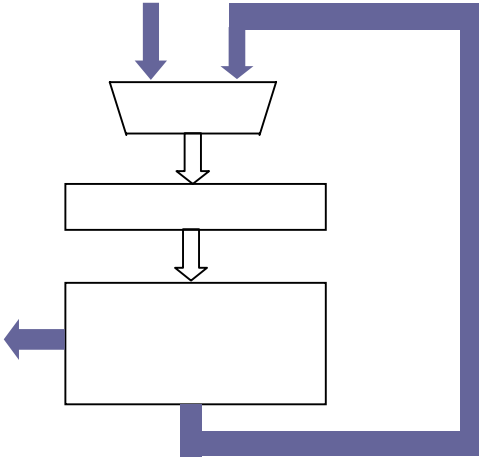
Grain, Trivium, A5/1

Based on
LFSRs / NFSRs
with parallel inputs



Mickey-128

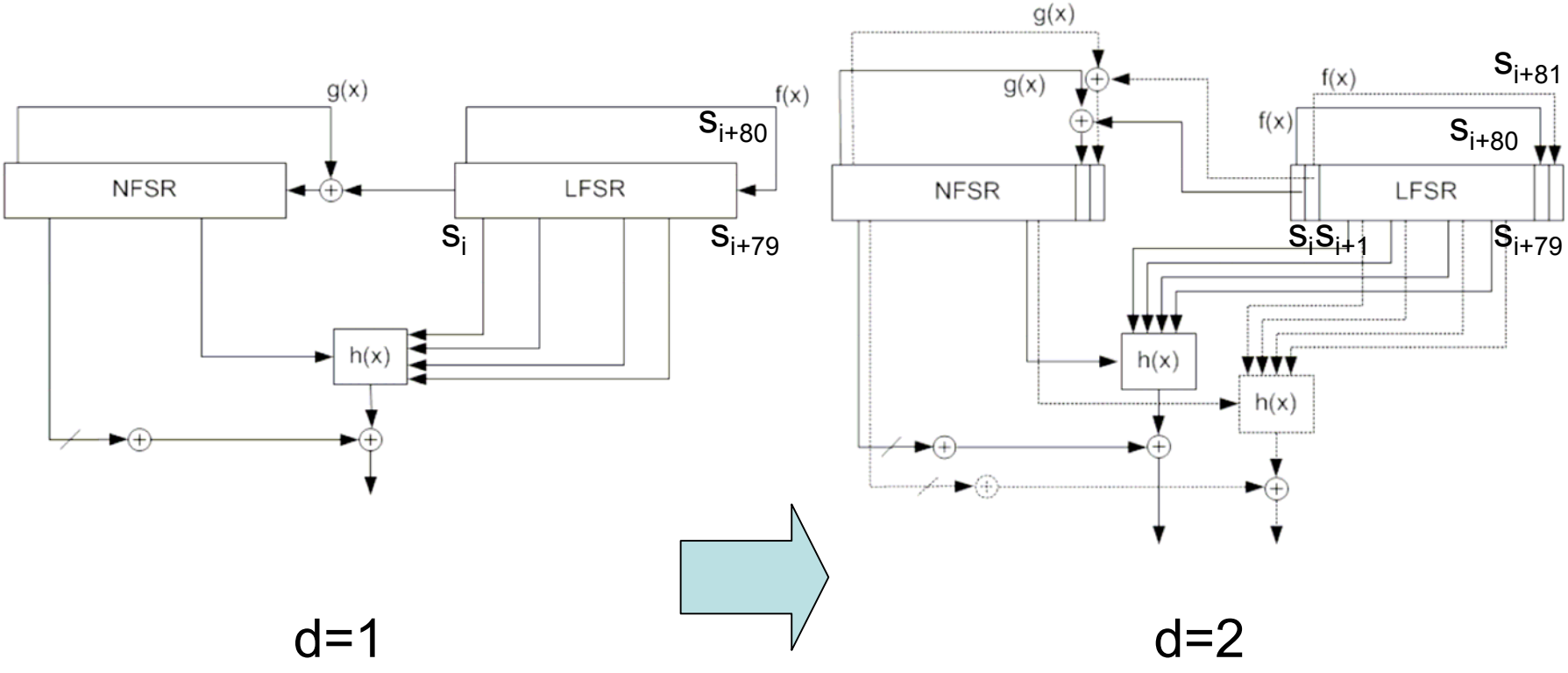
Based on basic iterative architecture and component operations of block ciphers and hash functions



Phelix, AES in OFB or CTR mode

Optimizations for the first group of ciphers

Grain

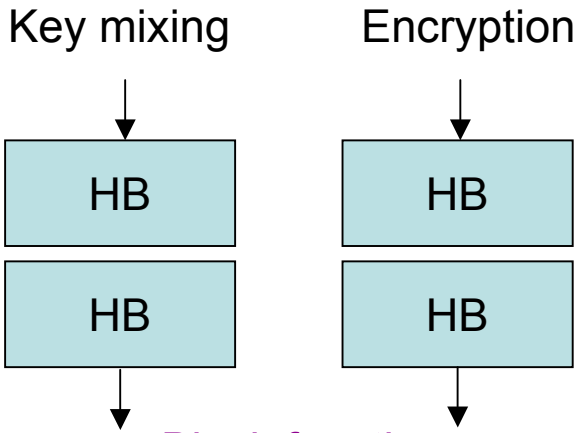


d=1 d=2

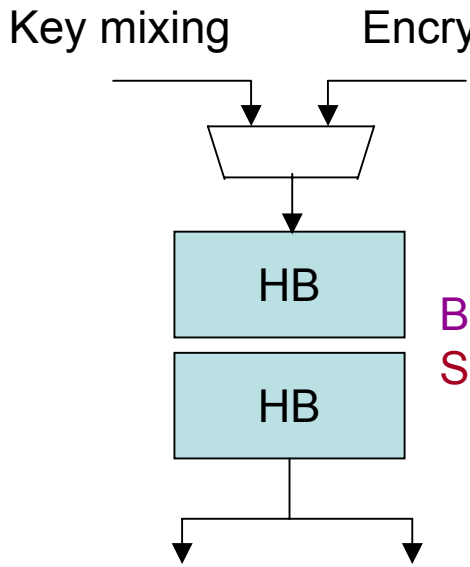
$$S_{i+80}=s_{i+62} + s_{i+52} + s_{i+38} + s_{i+23} + s_{i+13} + s_i$$

$$S_{i+81}=s_{i+63} + s_{i+53} + s_{i+39} + s_{i+24} + s_{i+14} + s_{i+1}$$

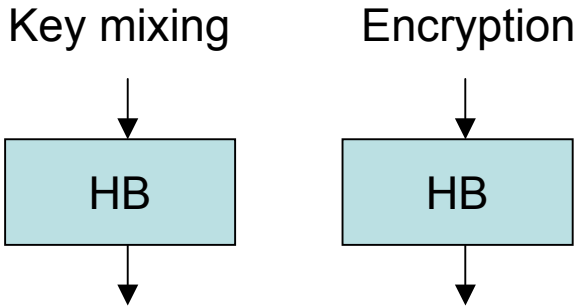
Optimizations for the third group of ciphers
Phelix



Block function,
No sharing

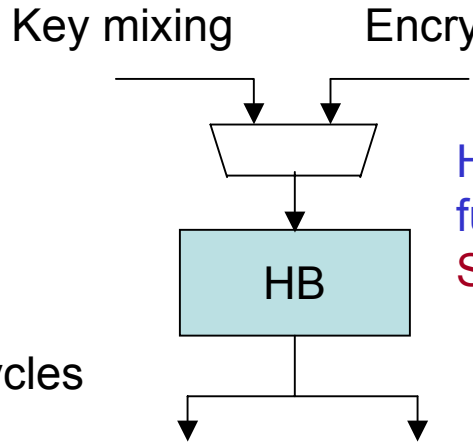


Block function,
Sharing



Half-Block function,
No sharing

2 x number of clock cycles

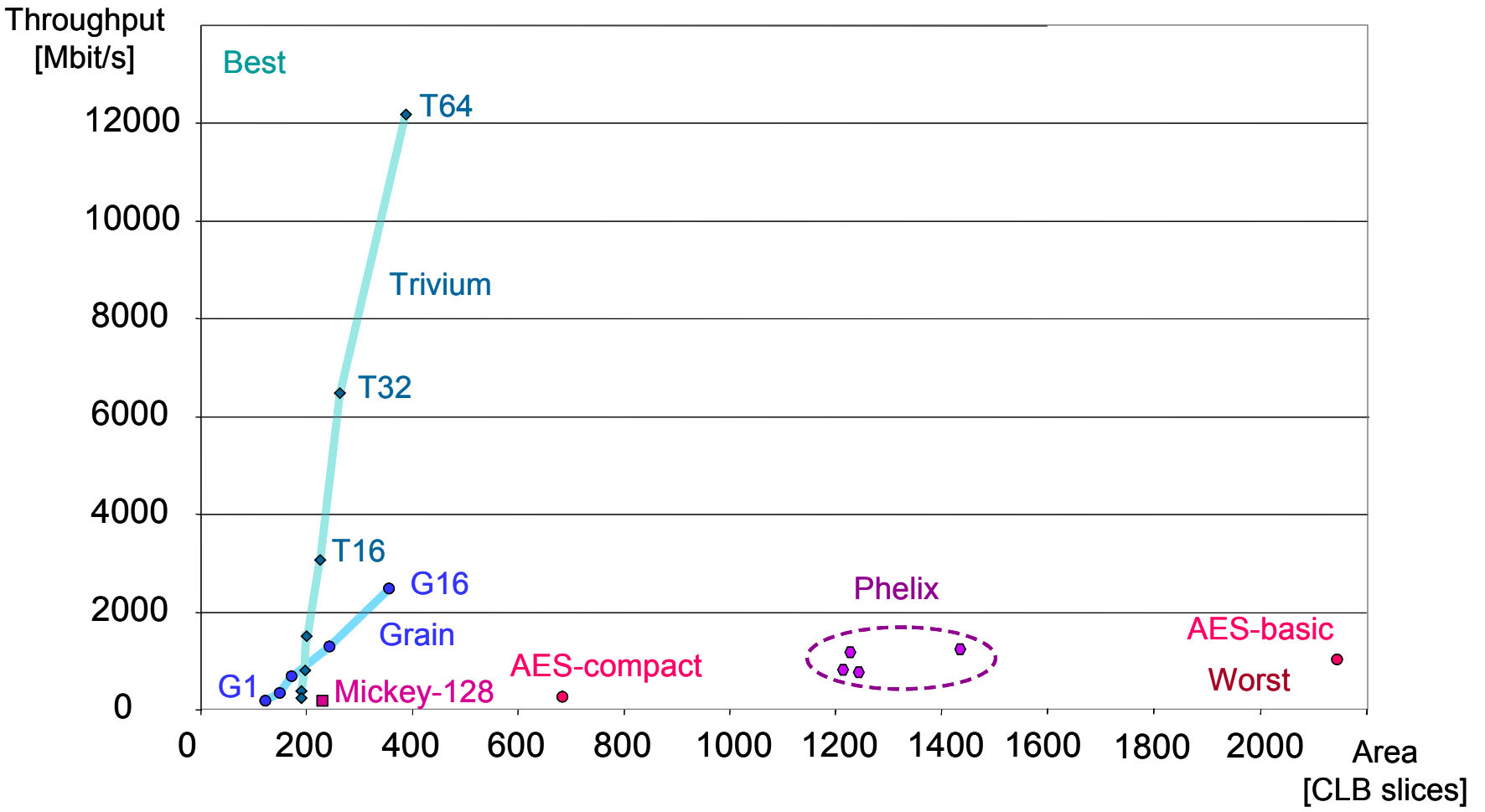


Half-Block
function,
Sharing

Ease of design as perceived by students based on the specification of each cipher

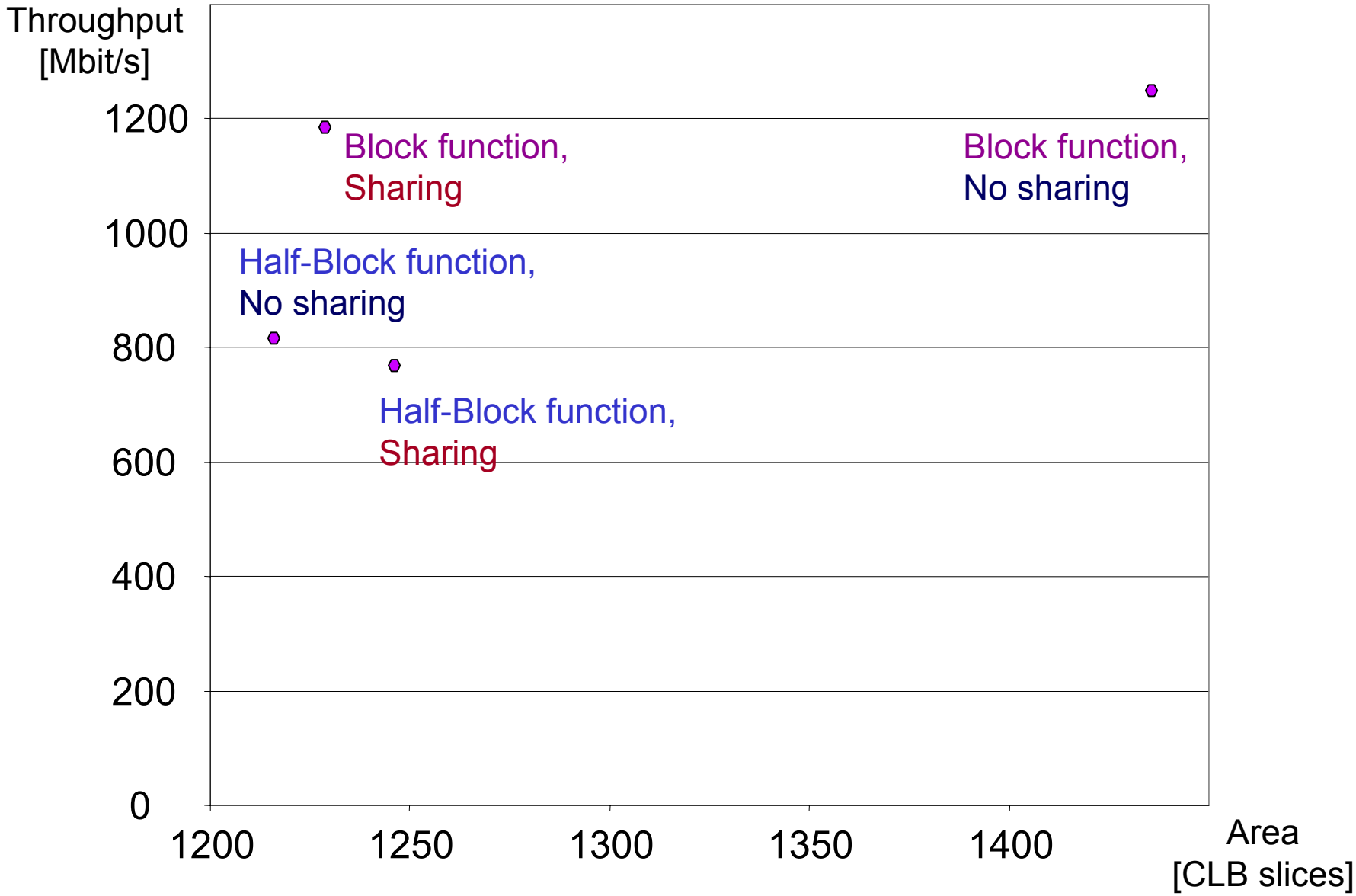
	Average score (5 – very easy, 1 – very difficult)	Number of students who selected the cipher as their first choice
Trivium	**3.36**	**5**
Mickey-128	**3.32**	**3**
Grain	**3.00**	**4**
Phelix	**2.00**	**0**

Throughput vs. area
FPGA: Xilinx Spartan 3 family



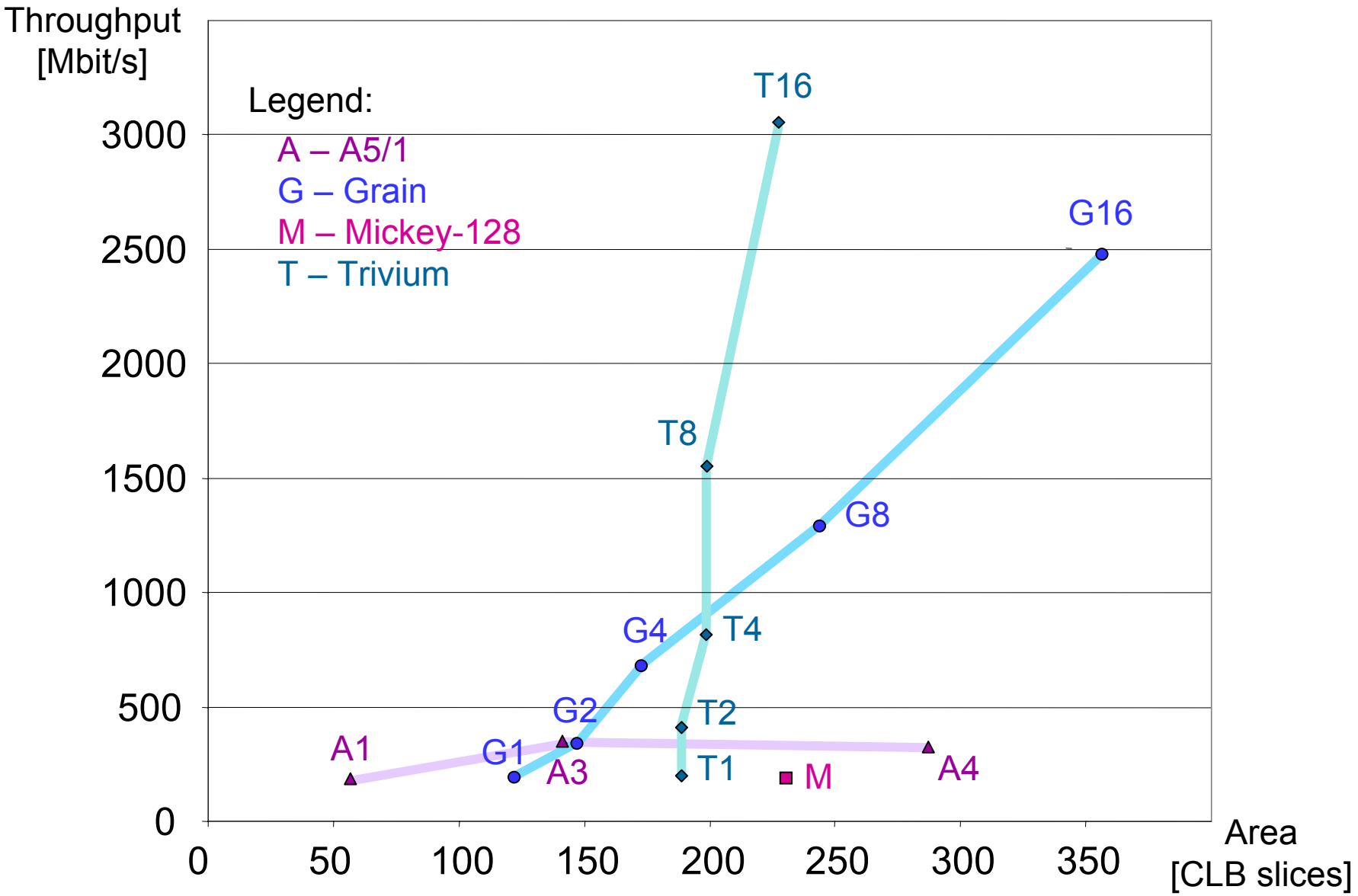
Throughput vs. area: Phelix

FPGA: Xilinx Spartan 3 family

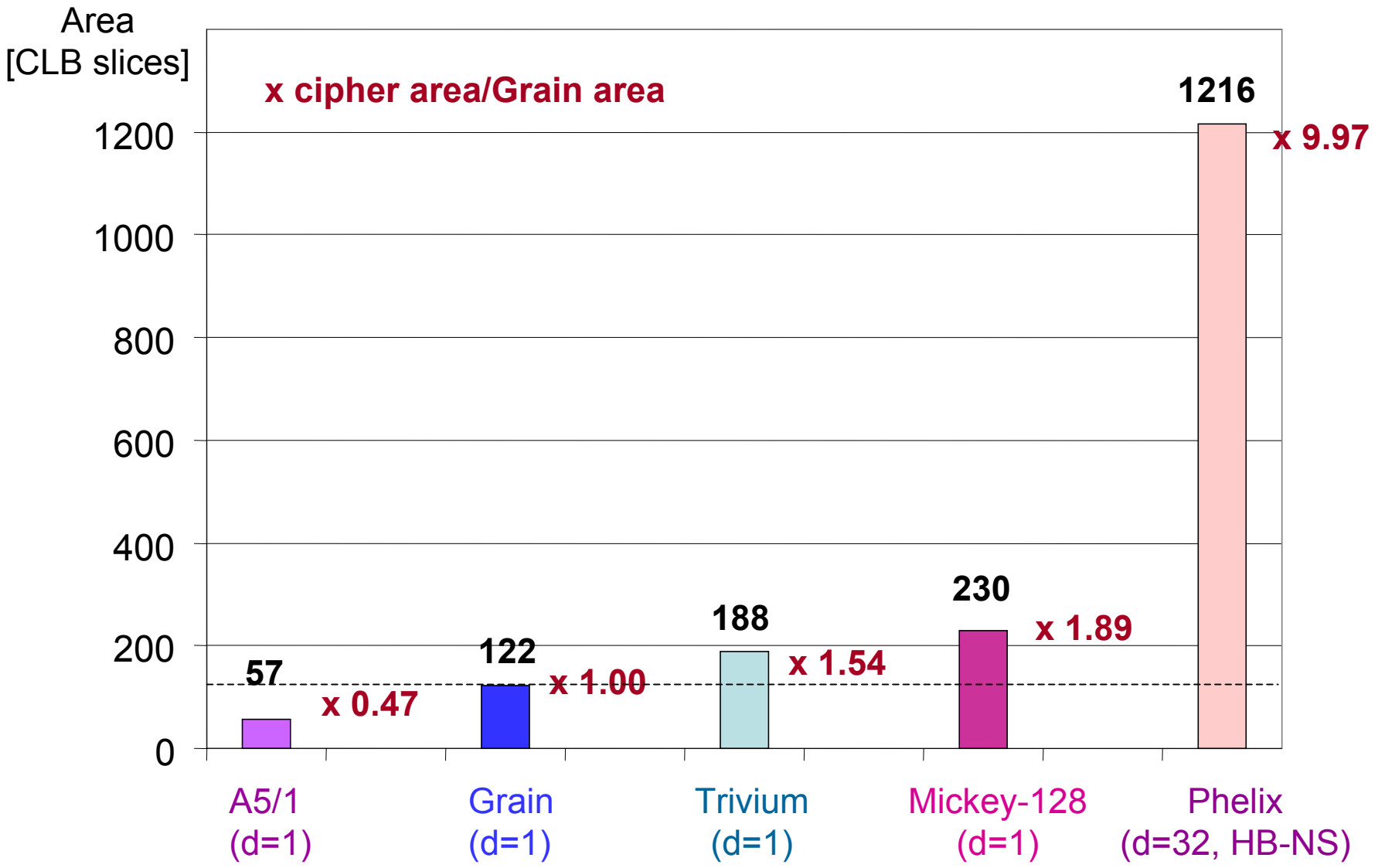


Throughput vs. area: Throughput up to 3 Gbit/s

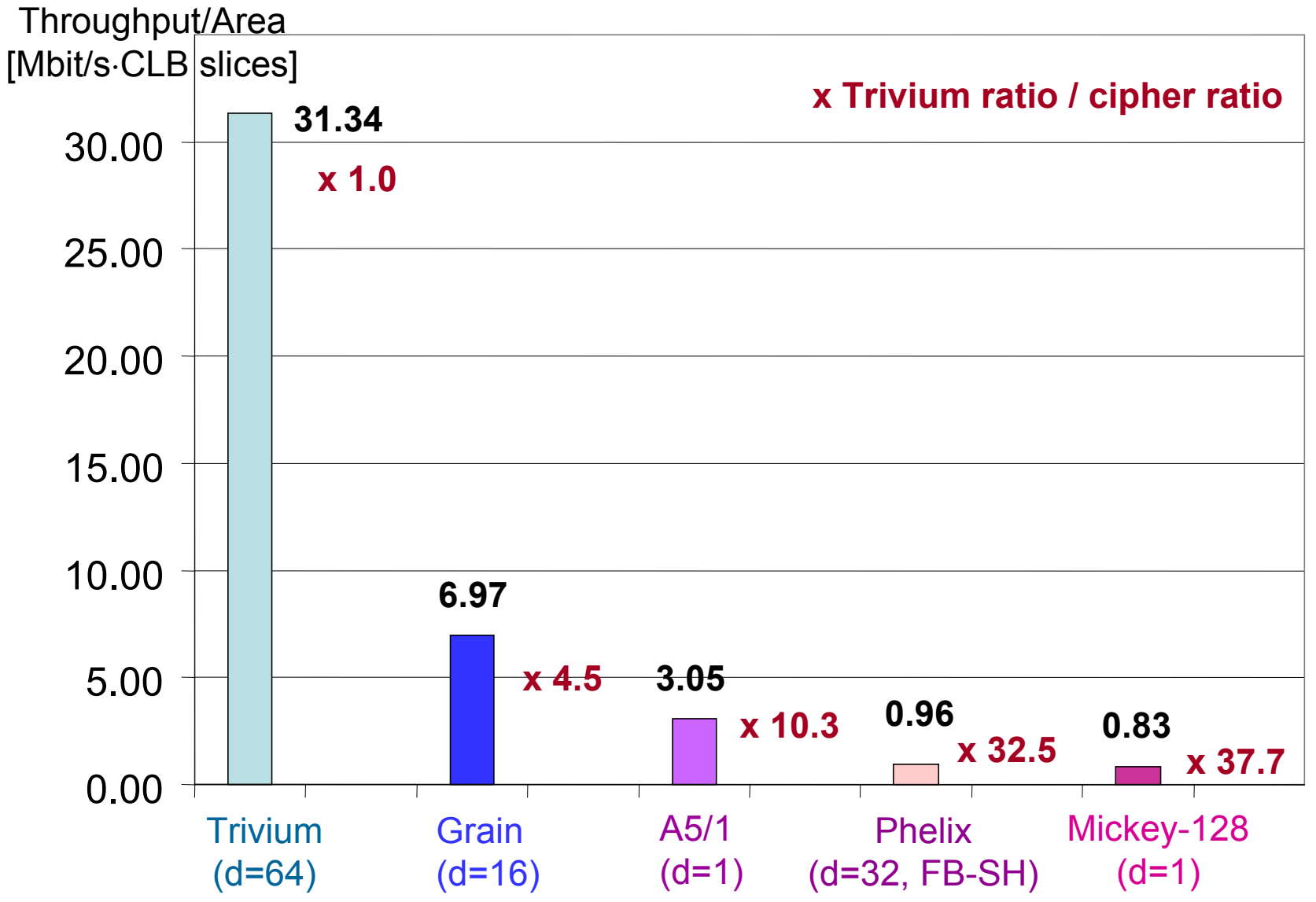
FPGA: Xilinx Spartan 3 family



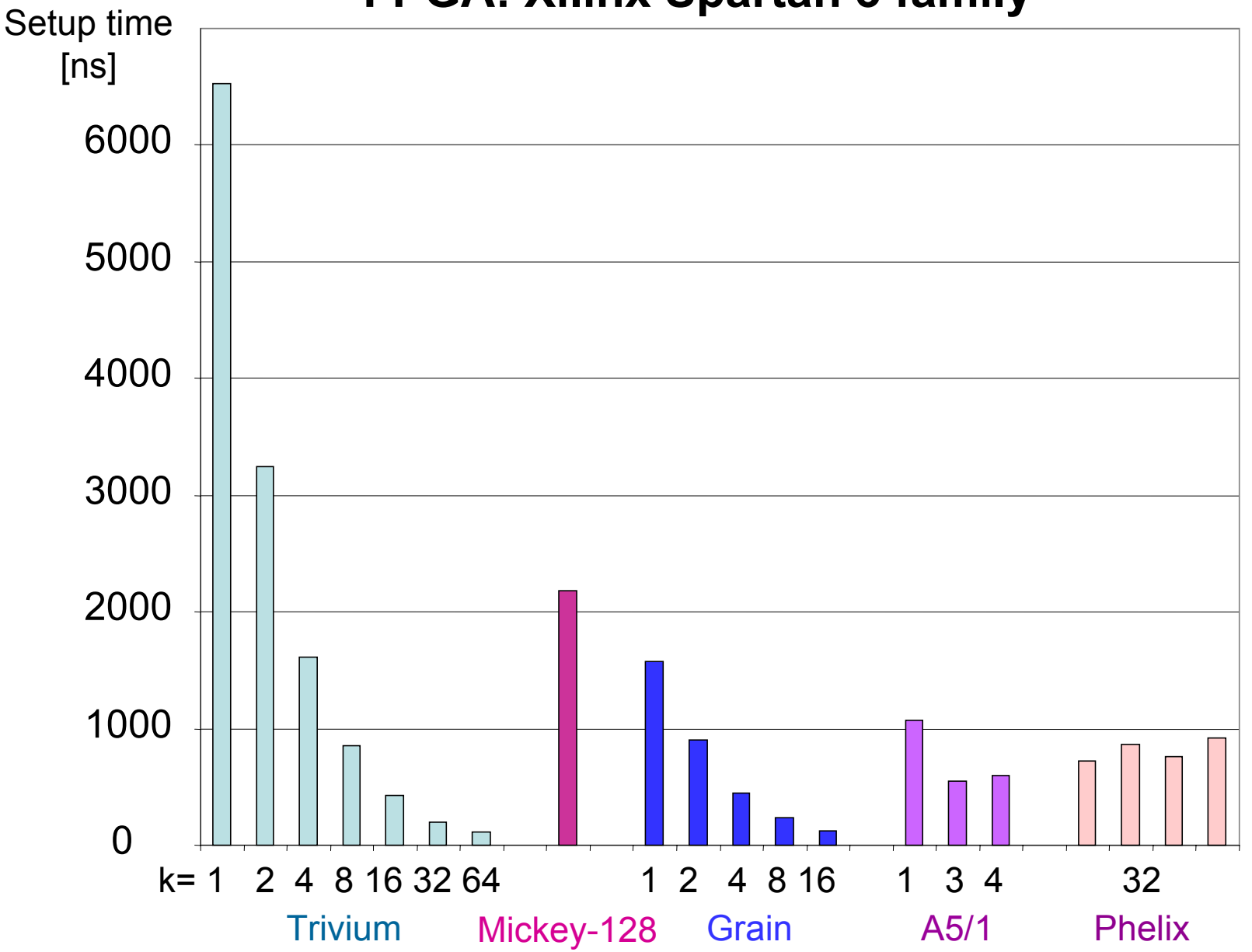
Optimizations for minimum area
FPGA: Xilinx Spartan 3 family



Optimizations for maximum throughput to area ratio
FPGA: Xilinx Spartan 3 family



Setup Time = Key & IV Loading + Initialization Time
FPGA: Xilinx Spartan 3 family



Conclusions

- **Very large differences** among candidate ciphers
  (much larger than for five final candidates in the AES contest)

  Possible reasons:
  - variety of ciphers based on different design principles
  - different internal state, key, and IV sizes
  - early stage of the contest

Trivium and Grain outperform other eSTREAM ciphers
in terms of
- flexibility
- minimum area
- maximum throughput to area ratio.

Once again ciphers based on **LFSR and NFSRs** show their superiority in hardware implementations

Security analysis should **focus first on the most efficient ciphers**