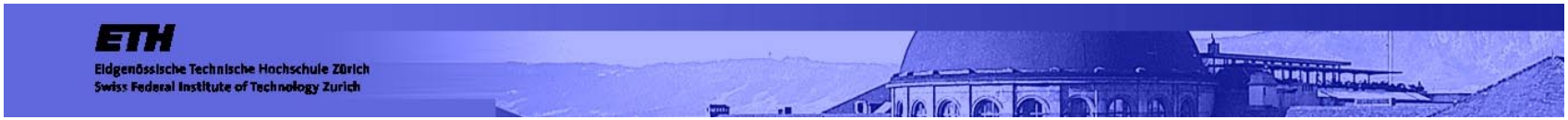


Hardware Evaluation of eSTREAM Candidates

Frank K. Gürkaynak, Peter Luethi, Nico Bernold,
René Blattmann,Victoria Goode, Marcel Marghitola,
Hubert Kaeslin, Norbert Felber, Wolfgang Fichtner

Integrated Systems Laboratory
ETH Zurich

2. February 2006

Table of Contents

Implementing eSTREAM Candidates

eSTREAM candidates (34)

ABC Achterbahn CryptMT/Fubuki DECIM DICING DRAGON Edon80 F-FCSR Frogbit Grain HC-256 Hermes8 LEX MAG MICKEY Mir-1 MOSQUITO NLS Phelix Polar Bear POMARANCH Py Rabbit Salsa20 SFINKS SOSEMANUK SSS TRBDK3 YAEA Trivium TSC-3 VEST WG Yamb ZK-Crypt

Implementing eSTREAM Candidates

eSTREAM candidates (12)

ABC Achterbahn CryptMT/Fubuki DECIM DICING DRAGON
Edon80 F-FCSR Frogbit Grain HC-256 Hermes8 LEX MAG
MICKEY Mir-1 MOSQUITO NLS Phelix Polar Bear
POMARANCH Py Rabbit Salsa20 SFINKS SOSEMANUK SSS
TRBDK3 YAEA Trivium TSC-3 VEST WG Yamb ZK-Crypt

- Algorithms that support only Profile-II

Implementing eSTREAM Candidates

eSTREAM candidates (10)

ABC Achterbahn CryptMT/Fubuki DECIM DICING DRAGON
Edon80 F-FCSR Frogbit Grain HC-256 Hermes8 LEX MAG
MICKEY Mir-1 MOSQUITO NLS Phelix Polar Bear
POMARANCH Py Rabbit Salsa20 SFINKS SOSEMANUK SSS
TRBDK3 YAEA Trivium TSC-3 VEST WG Yamb ZK-Crypt

- Algorithms that support only Profile-II
- Algorithms without any cryptological issues

Implementing eSTREAM Candidates

eSTREAM candidates (7)

ABC Achterbahn CryptMT/Fubuki DECIM DICING DRAGON Edon80 F-FCSR Frogbit Grain HC-256 Hermes8 LEX MAG MICKEY Mir-1 MOSQUITO NLS Phelix Polar Bear POMARANCH Py Rabbit Salsa20 SFINKS SOSEMANUK SSS TRBDK3 YAEA Trivium TSC-3 VEST WG Yamb ZK-Crypt

- Algorithms that support only Profile-II
- Algorithms without any cryptological issues
- Algorithms which are not likely to get updates

Implementing eSTREAM Candidates

eSTREAM candidates (8)

ABC Achterbahn CryptMT/Fubuki DECIM DICING DRAGON Edon80 F-FCSR Frogbit Grain HC-256 Hermes8 LEX MAG MICKEY Mir-1 MOSQUITO NLS Phelix Polar Bear POMARANCH Py Rabbit Salsa20 SFINKS SOSEMANUK SSS TRBDK3 YAEA Trivium TSC-3 VEST WG Yamb ZK-Crypt

- Algorithms that support only Profile-II
- Algorithms without any cryptological issues
- Algorithms which are not likely to get updates
- Once these are completed, look for additional algorithms that seem easy to implement.

Implementing eSTREAM Candidates

eSTREAM candidates (8)

ABC Achterbahn CryptMT/Fubuki DECIM DICING DRAGON Edon80 F-FCSR Frogbit Grain HC-256 Hermes8 LEX MAG MICKEY Mir-1 MOSQUITO NLS Phelix Polar Bear POMARANCH Py Rabbit Salsa20 SFINKS SOSEMANUK SSS TRBDK3 YAEA Trivium TSC-3 VEST WG Yamb ZK-Crypt

- Algorithms that support only Profile-II
- Algorithms without any cryptological issues
- Algorithms which are not likely to get updates
- Once these are completed, look for additional algorithms that seem easy to implement.

Compare against an AES core running in OFB mode

Fair Comparison

The following factors may have significant effect on the outcome of a hardware design:

- **The experience of the designer**

Fair Comparison

The following factors may have significant effect on the outcome of a hardware design:

- **The experience of the designer**
- **Implementation platform/technology**
  FPGA (which device?, how are the resources used?),
  ASIC (which technology?)

Fair Comparison

The following factors may have significant effect on the outcome of a hardware design:

- **The experience of the designer**
- **Implementation platform/technology**
  FPGA (which device?, how are the resources used?),
  ASIC (which technology?)
- **Project schedule**

Fair Comparison

The following factors may have significant effect on the outcome of a hardware design:

- **The experience of the designer**
- **Implementation platform/technology**
  FPGA (which device?, how are the resources used?),
  ASIC (which technology?)
- **Project schedule**

In this project

All designs were implemented by a group of 4 students:

- with equal experience
- using a standard cell based ASIC design flow
- within 14 weeks

Methodology

Tools

Description:	Code written in VHDL
Simulation:	Mentor Graphics Modelsim 6.0c
Logic Synthesis:	Synopsys Design Vision-2004.12
Physical Design:	Cadence SoC Encounter 4.1-usr4
Technology:	UMC 0.25 µm 5-Metal CMOS

Methodology

Tools

Description: Code written in VHDL

Simulation: Mentor Graphics Modelsim 6.0c

Logic Synthesis: Synopsys Design Vision-2004.12

Physical Design: Cadence SoC Encounter 4.1-usr4

Technology: UMC 0.25 µm 5-Metal CMOS

Guidelines for design

- The provided C code has been used as a reference
- All synthesized algorithms include test structures
- No ROM macros were used
- Optional MAC support is not included
- All algorithms accept plaintext and deliver ciphertext

The Team

Sherlock

Nico Bernold
René Blattmann

Watson

Victoria Goode
Marcel Marghitola

7^{th} semester students of the Information Technologies and Electronics Department of the ETH Zurich.

Performance Metrics

Circuit performance will be measured by:

A	Total circuit area after synthesis in μm^2
f	Maximum clock rate in MHz
P	Power consumption in mW
Radix	Generated output bits per clock cycle

Performance Metrics

Circuit performance will be measured by:

A	Total circuit area after synthesis in μm^2
f	Maximum clock rate in MHz
P	Power consumption in mW
Radix	Generated output bits per clock cycle
T	Throughput in Gbits/s
TpA	Throughput per area in Gbits/s·mm^2
E	Energy per data item mJ/Gbits

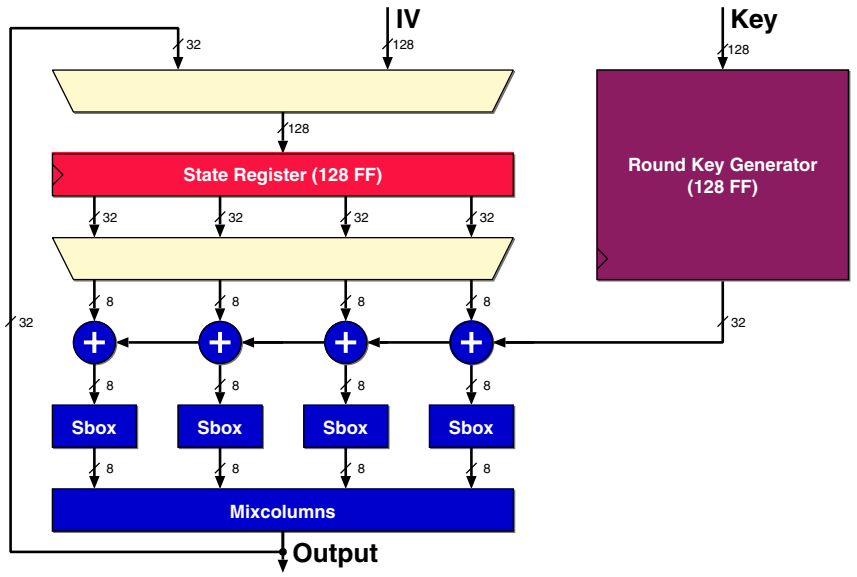
AES

Radix 3.12

FFs 265

A 300k μm^2

T 0.665 Gb/s



Advanced Encryption Standard

- More experience with implementing AES
  Highly optimized
- 32-bit datapath
- on-the-fly key generation

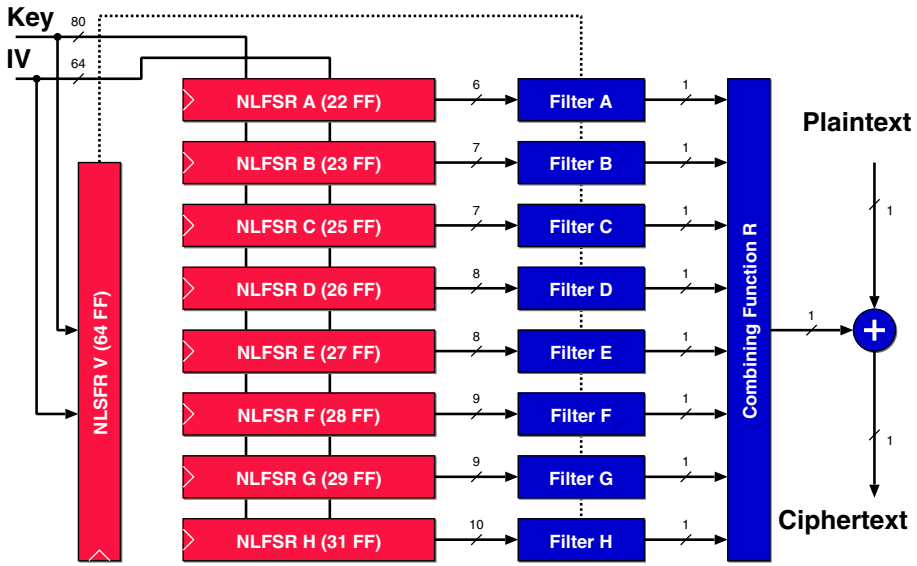
Achterbahn

Radix 1-16

FFs 285

A 191k-480k μm^2

T 0.310-1.423 Gb/s



Pro

✓ Very good documentation and reference code

✓ Good performance trade-off

Con

x Low throughput

x Large area

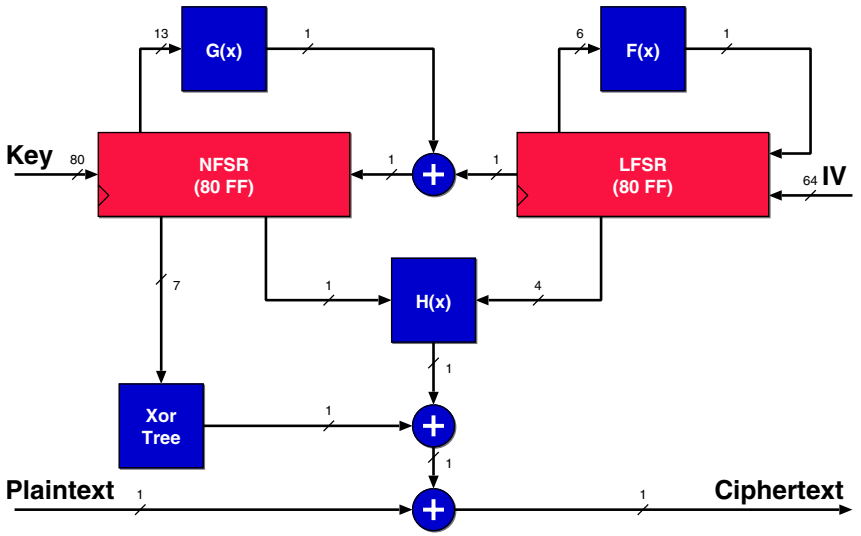
Grain

Radix 1-16

FFs 166

A 65k-135k μm^2

T 0.280-4.00 Gb/s



Pro

- ✓ Small area
- ✓ High throughput
- ✓ Very simple and straightforward architecture

Con

- x Only moderate performance trade-off

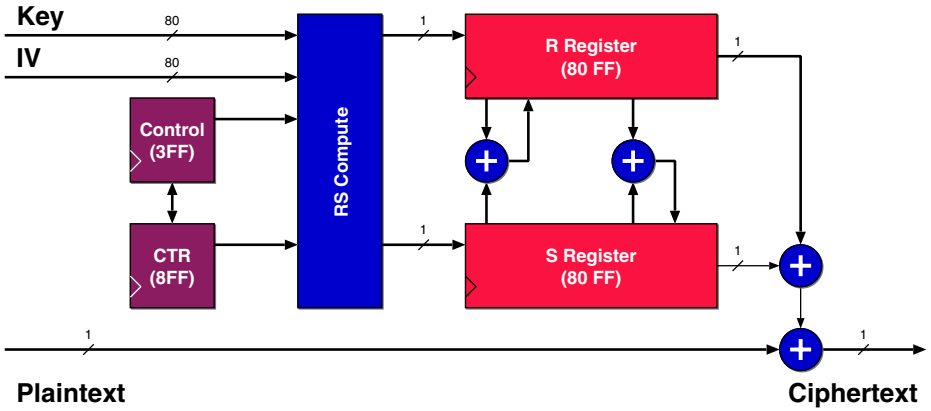
Mickey

Radix 1

FFs 170

A 87k μm^2

T 0.307 Gb/s



Pro

✓ Very 'hardware friendly' documentation

✓ Very compact

Con

x Low throughput

x Difficult to parallelize/increase radix

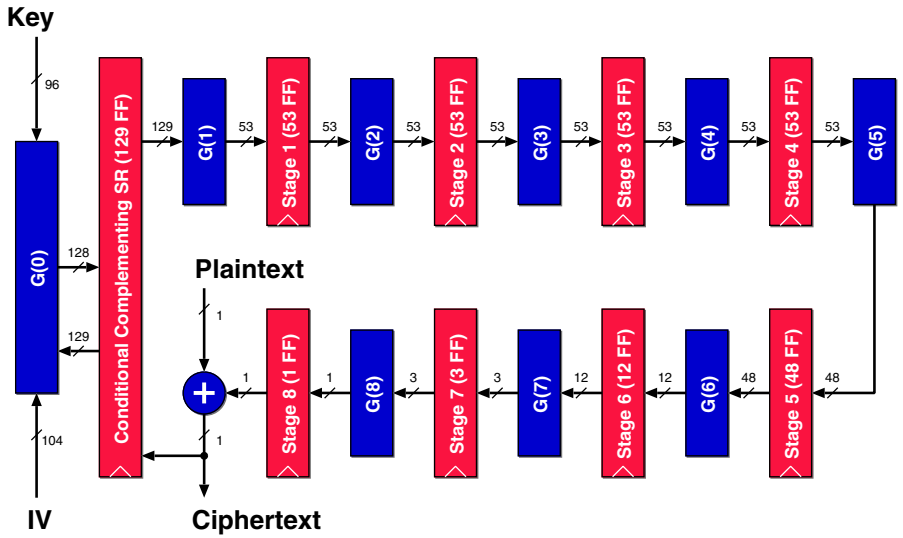
Mosquito

Radix 1,3

FFs 411

A 222k-377k μm^2

T 0.300-0.870 Gb/s



Pro

✓ Simple logic structure

Con

x Difficult to parallelize

x Low throughput

x Large area

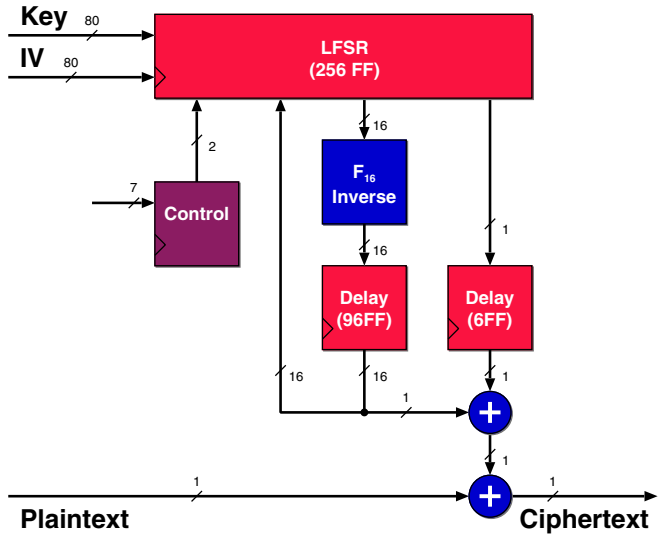
Sfinks

Radix 1-16

FFs 289-754

A 123k-696k μm^2

T 0.180-2.500 Gb/s



Pro

✓ Easy to follow documentation

Con

x Additional hardware for initialization

x Complex inverse function, not well described in documentation

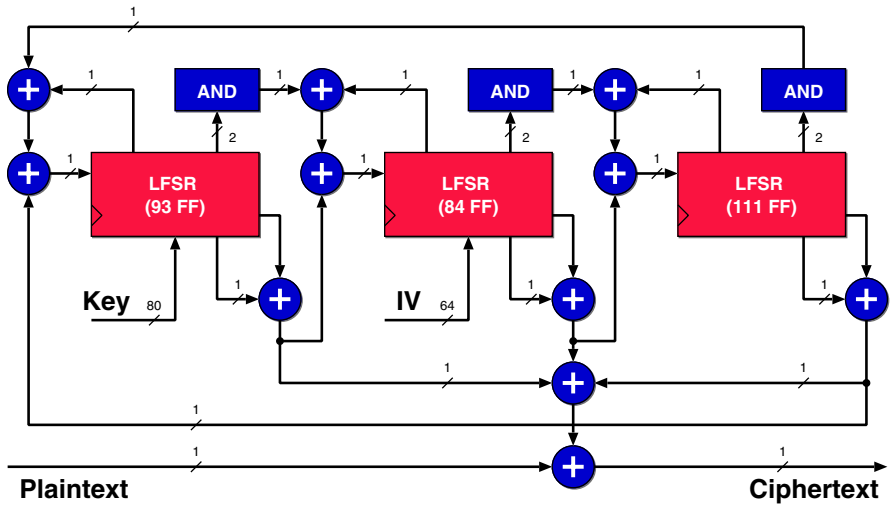
Trivium

Radix 1-64

FFs 295

A 90k-150k μm^2

T 0.313-26.600 Gb/s



Pro

✓ Very high throughput

✓ Small area

Con

x Bad performance/area trade-off

x Reference C code has no comments, difficult to understand

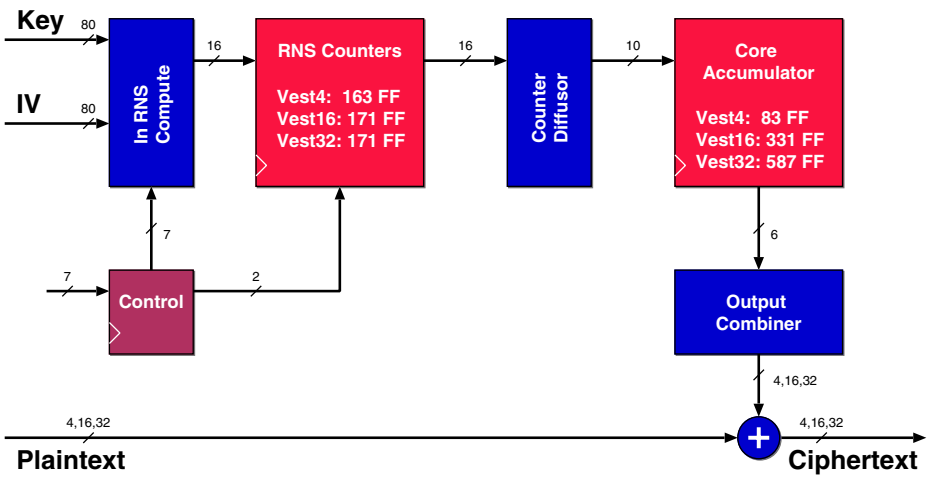
Vest

Radix 4-32

FFs 266-778

A 214k-620k μm^2

T 1.250-10.000 Gb/s



Pro

✓ High throughput

Con

x Complex algorithm, difficult to write VHDL code

x Better suited to FPGAs, many look-up tables

x Large area

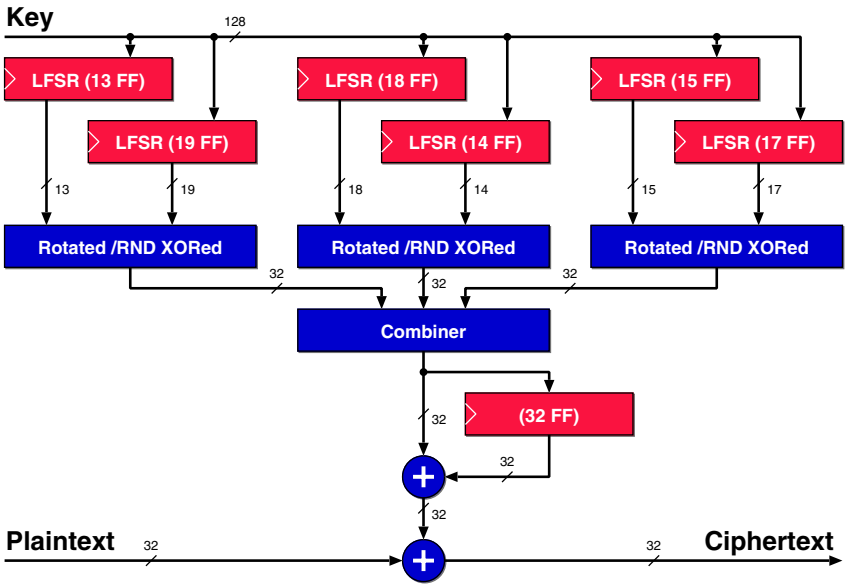
ZK-Crypt

Radix 32

FFs 189

A 135k μm^2

T 7.451 Gb/s



Pro

✓ Very good performance

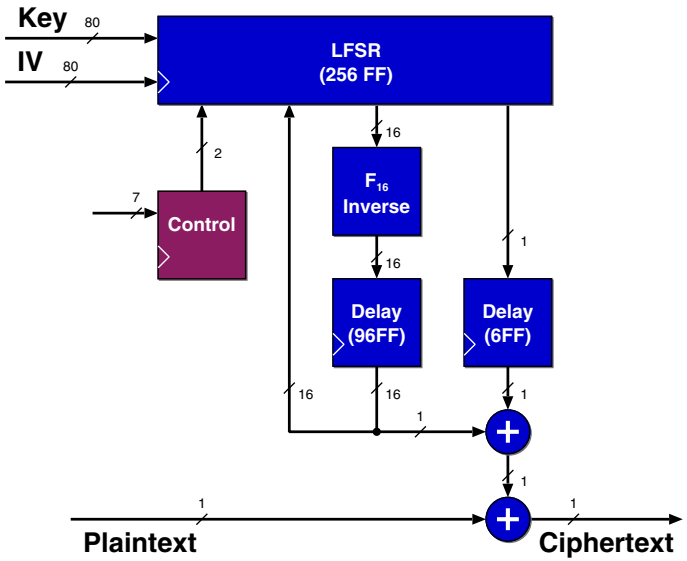
✓ No initialization sequence

Con

x Unacceptable documentation

x Difficult to implement

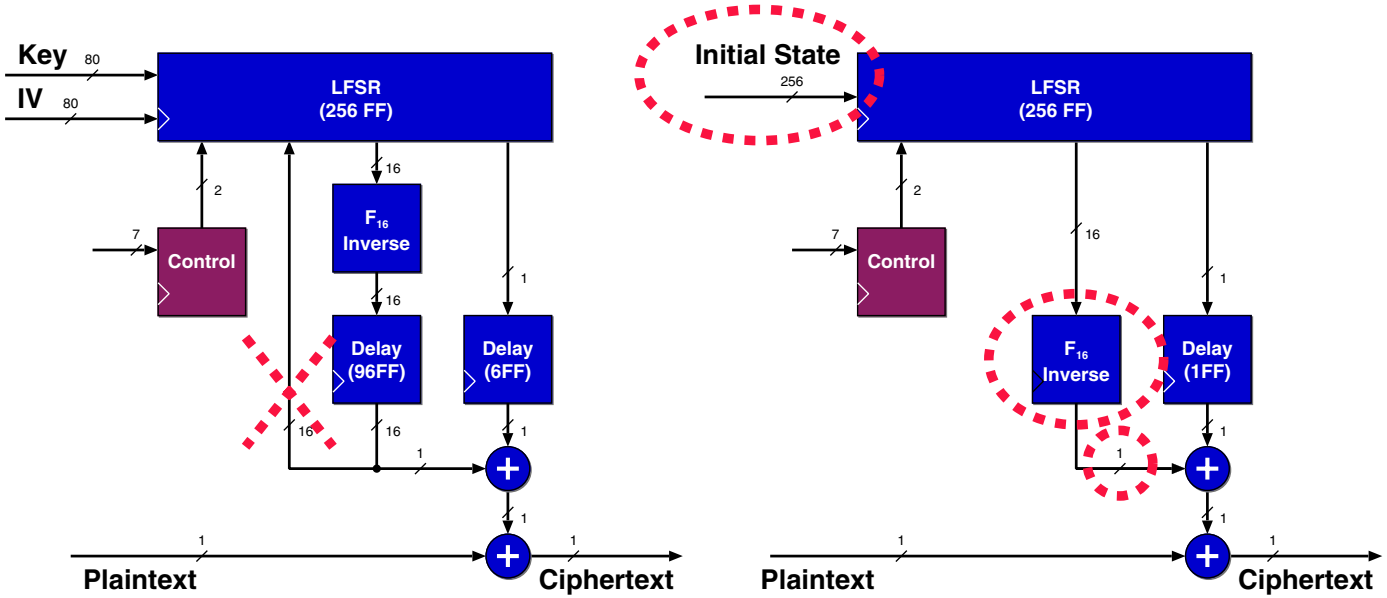
Initialization



Example Sfinks

- 15 out of 16 outputs of the inverse is not used for cipher
- The output of the inverse needs to be delayed by 6 cycles

Initialization



Example Sfinks

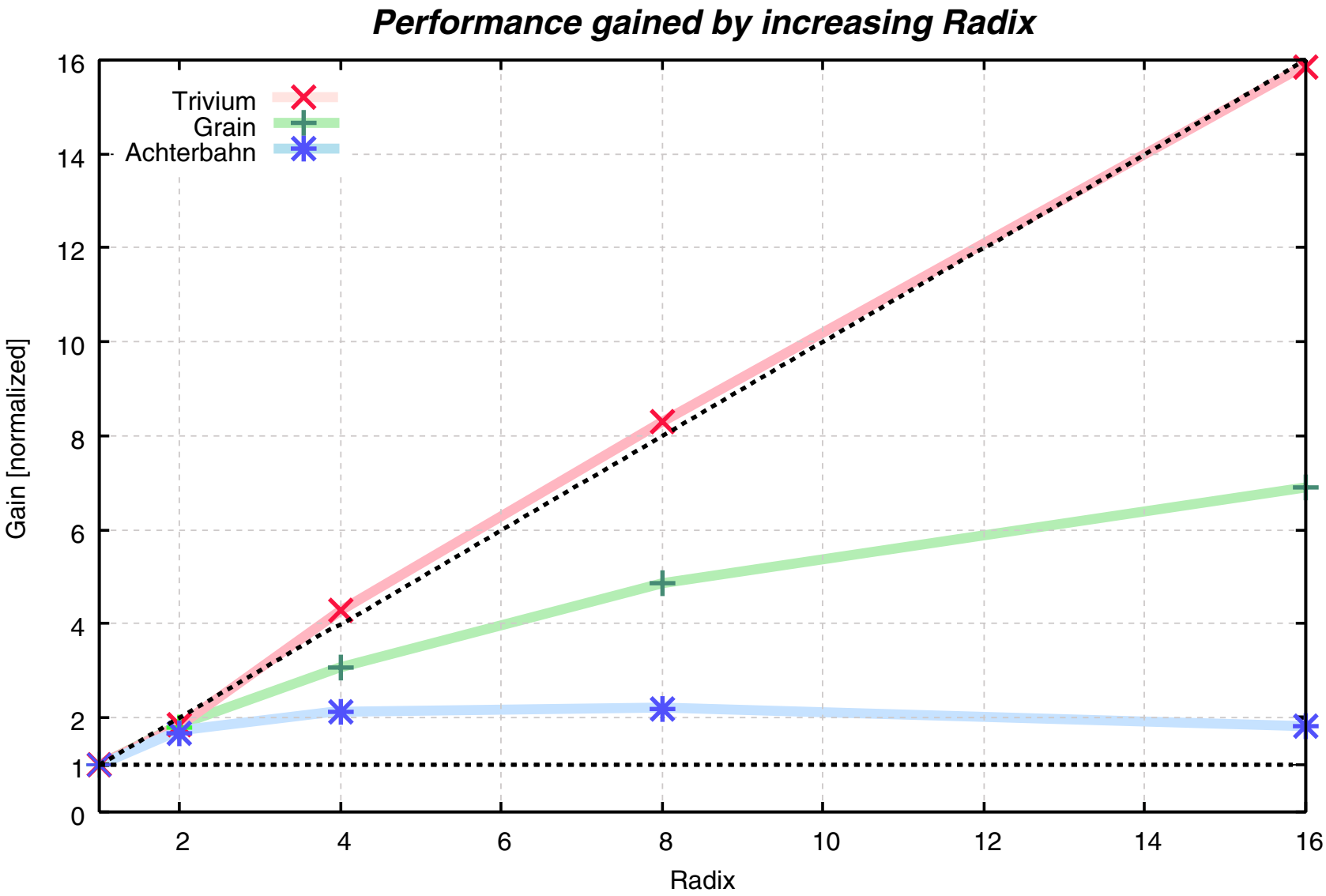
- 15 out of 16 outputs of the inverse is not used for cipher
- The output of the inverse needs to be delayed by 6 cycles
- The initial state of the registers can be loaded directly
- This increases efficiency by 30%

Stage Delay

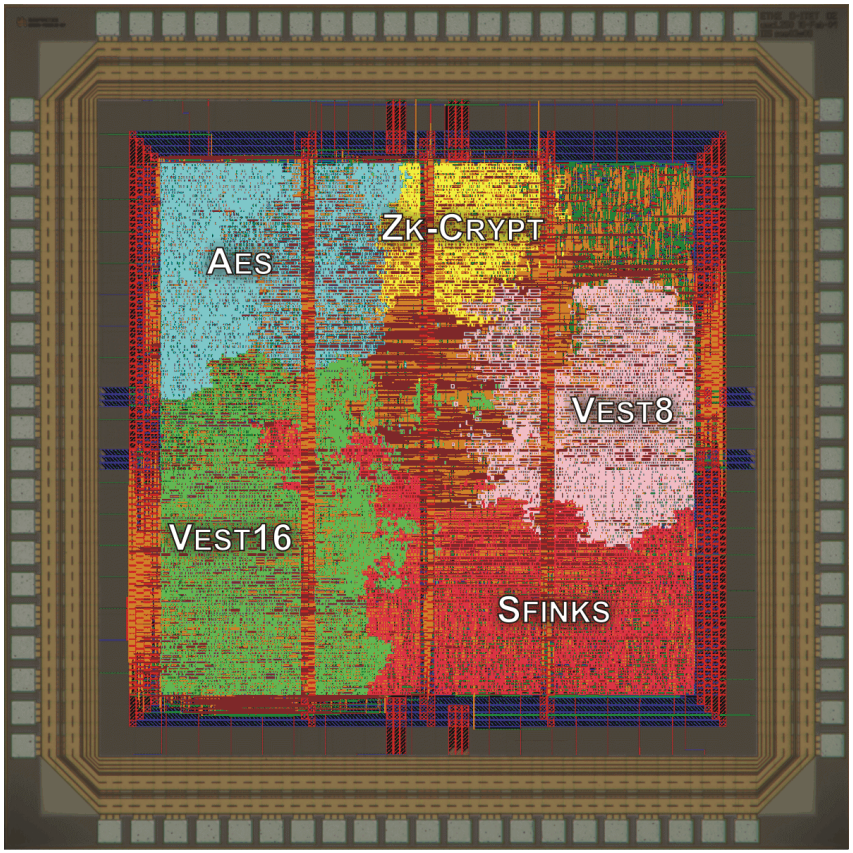
FO4 delay	UMC 0.25 µm	Design Style	Difficulty
10-20	1GHz-500MHz	Custom ASIC	State of the art
20-50	500MHz-200MHz	Custom/Std. Cell	Very challenging
50-100	200MHz-100MHz	Fast Std. Cell	Involved
100-500	100MHz-20MHz	Basic Std. Cell	Standard
500+	$\leq$ 20MHz	Basic Std. Cell	Easy

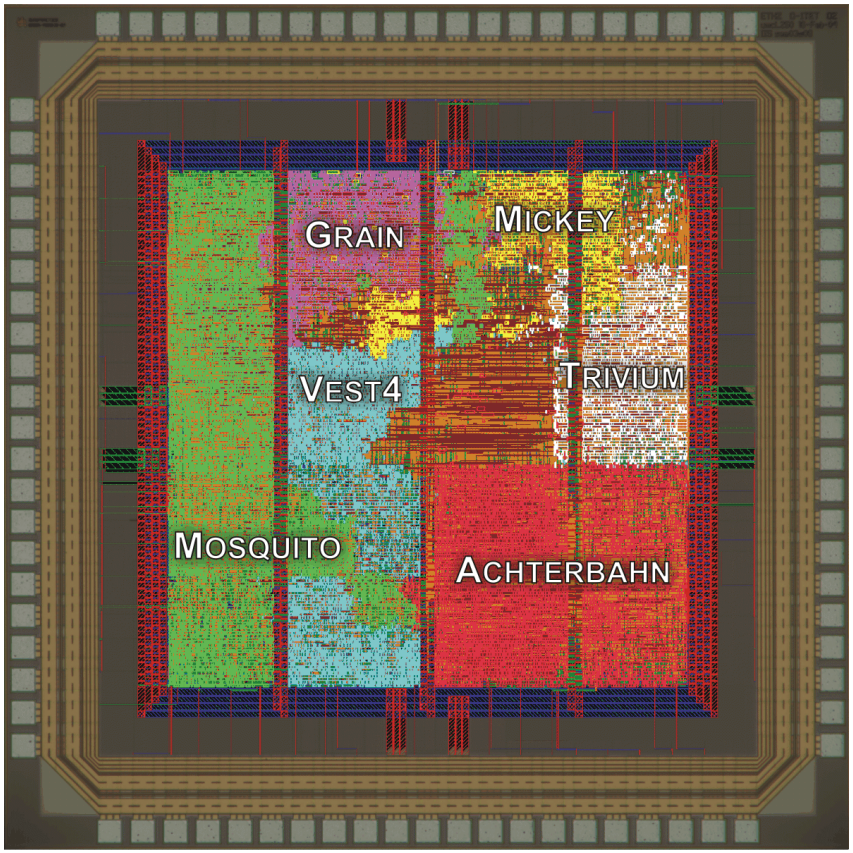
- Each technology has a **comfort zone** for clock frequency
- Physical design effort for **fast** designs becomes disproportionately high
- For UMC 0.25 µm, FO4 delay is 0.1 ns.
  Clock frequency should not exceed 200 MHz by much.

Radix


Performance gained by increasing Radix
Trivium
Grain
Achterbahn
Gain [normalized]
Radix
0
1
2
4
6
8
10
12
14
16

Sherlock and Watson





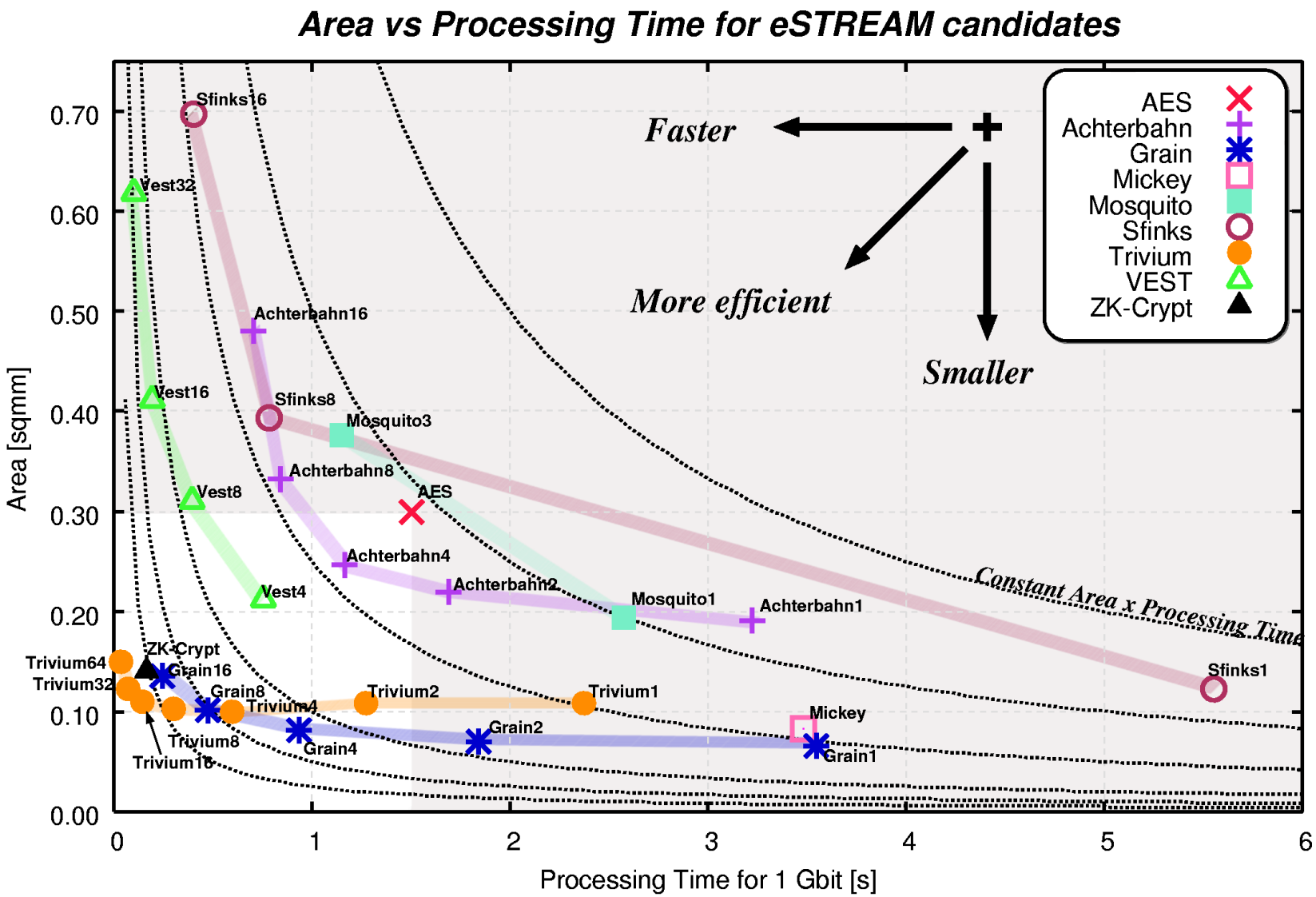
Sherlock

AES, Sfinks, Vest8, Vest16, ZK-Crypt

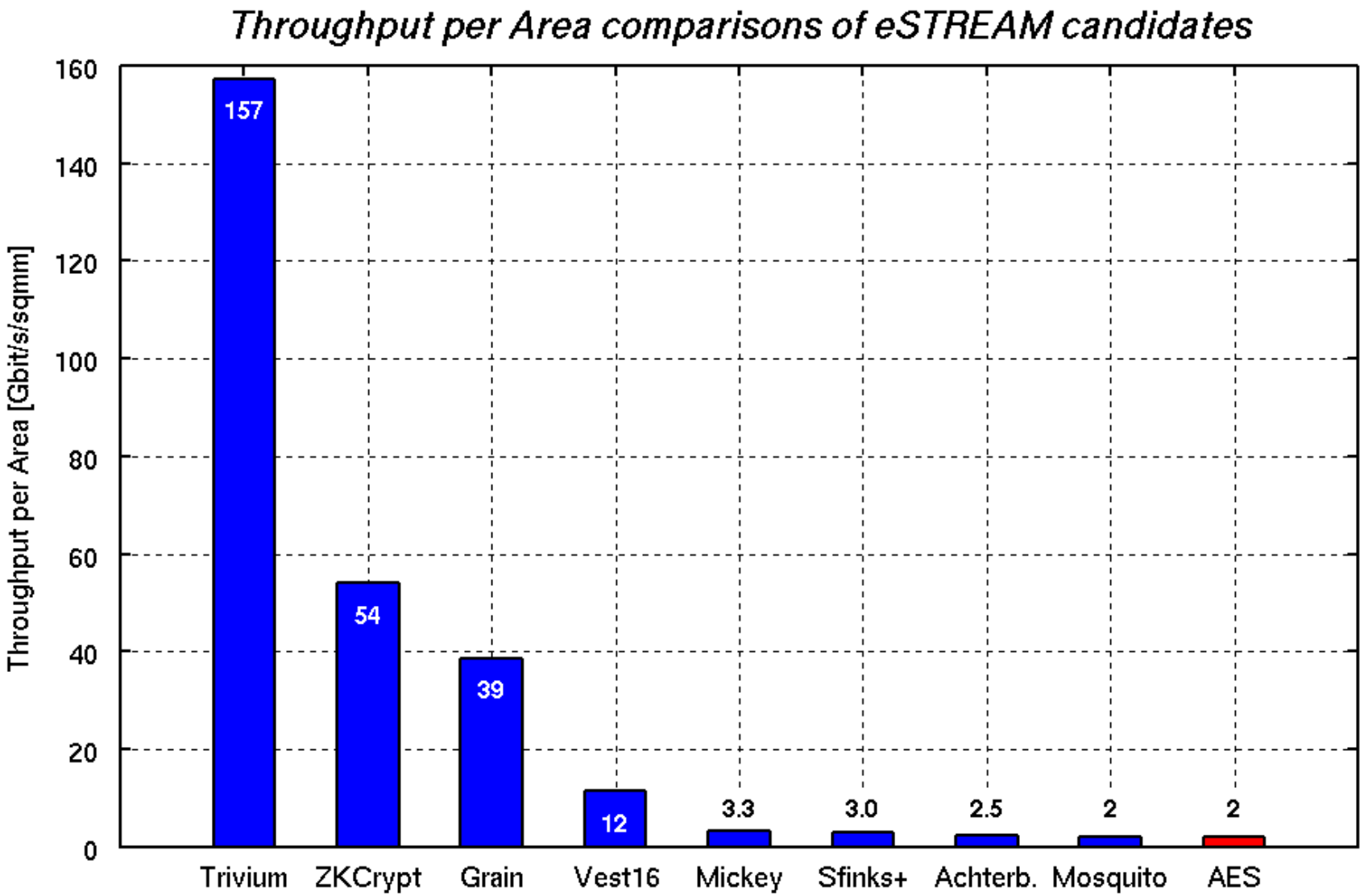
Watson

Achterbahn, Grain, Mickey, Mosquito, Vest4, Trivium

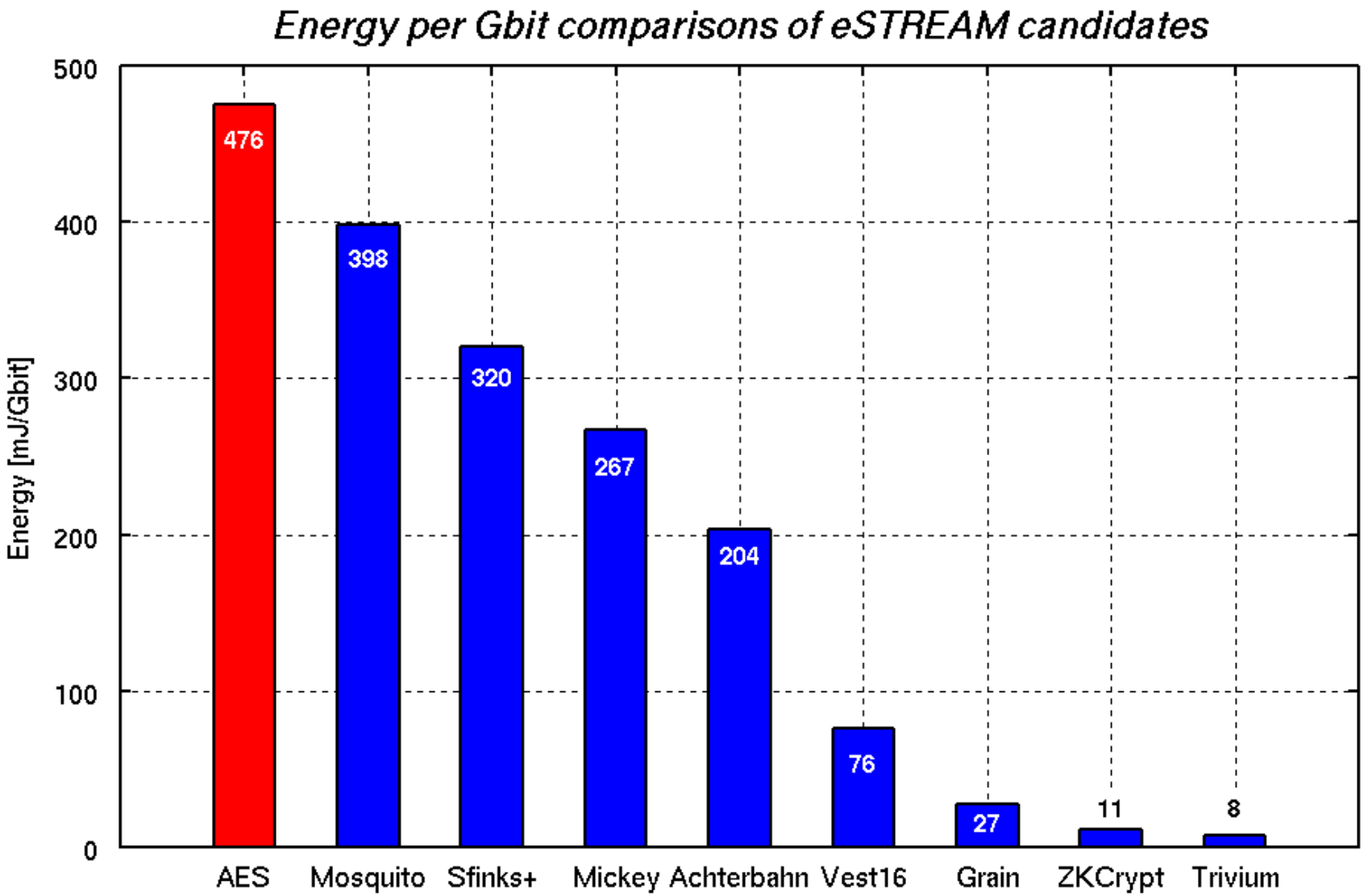
Area vs Time required to process 1 Gbit



Throughput per Area



Energy required to process 1 Gbit



Concluding Remarks

Final words

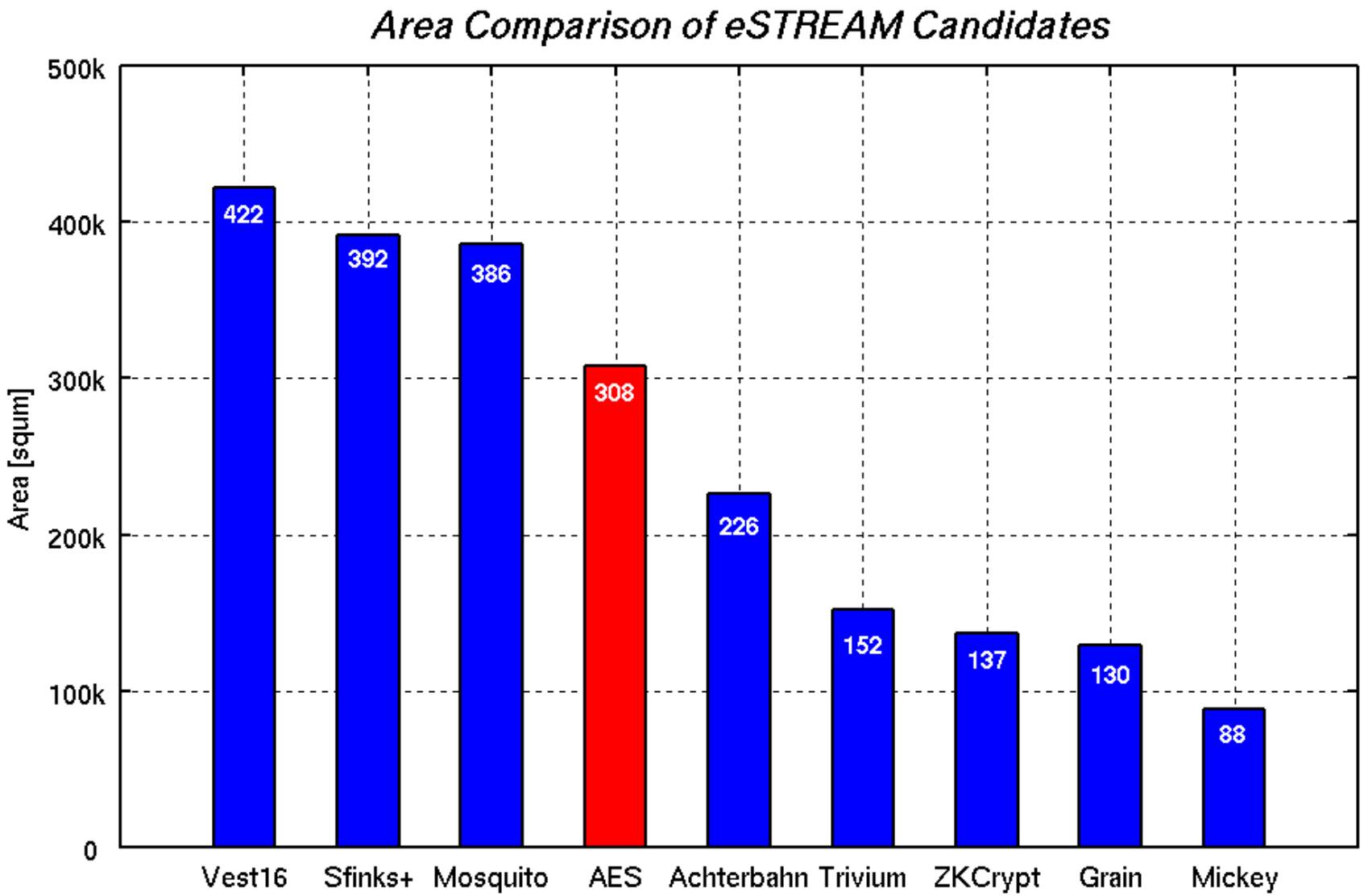
- There are several eSTREAM candidates which are **smaller**, have a **higher throughput** and consume **less power** than AES.
- Without knowing their cryptographic qualities, it is inappropriate to rate the algorithms solely based on their hardware performance.
- As hardware designers, we favor designs which offer a broad range of **trade-offs between area and throughput**.
- Sherlock and Watson are expected back from manufacturing May 2006.
- This presentation and additional results are available at:

http://asic.ethz.ch/estream

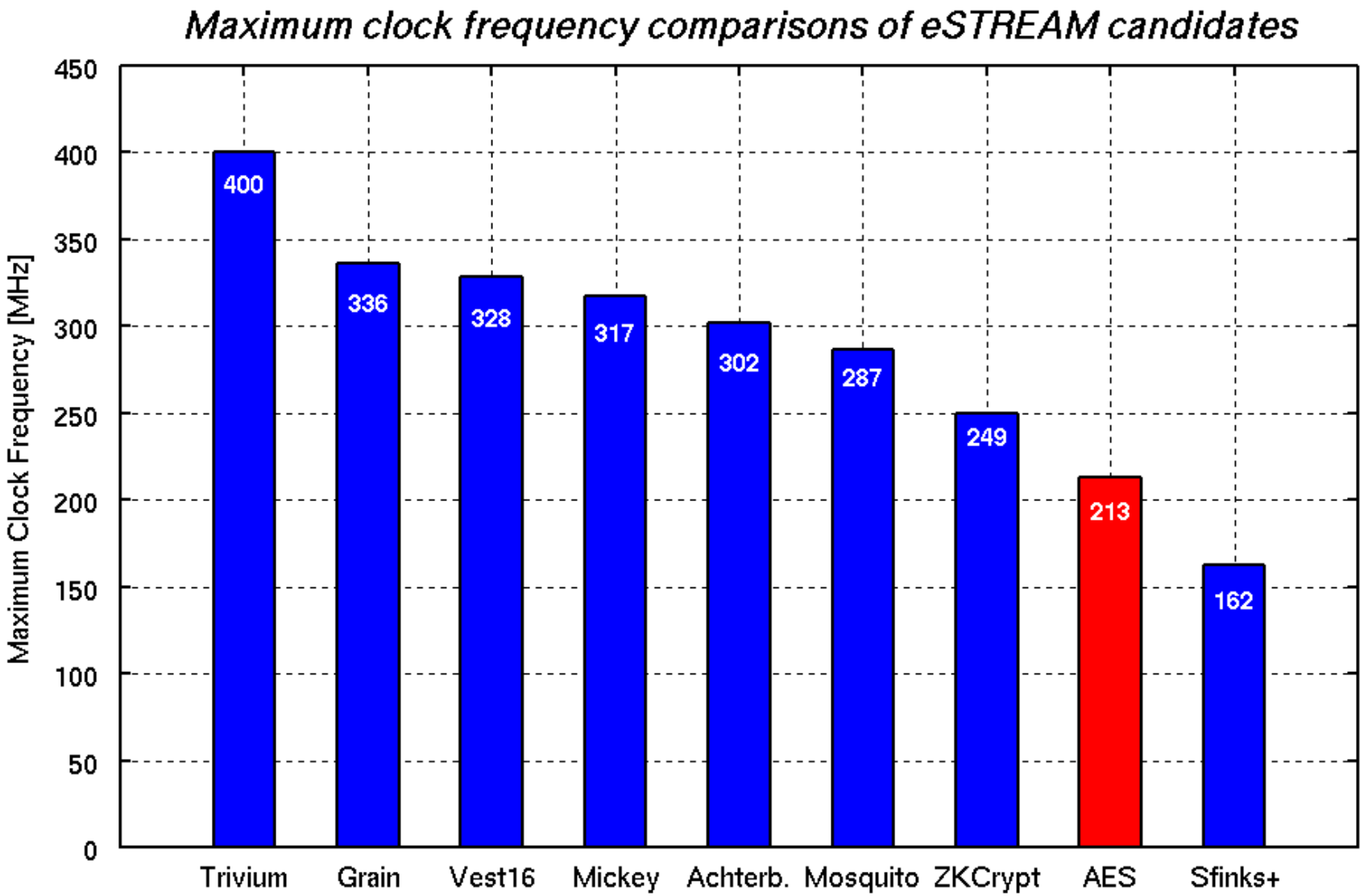
Post-layout Results

Algorithm	**A** (μm^2)	**f** (MHz)	**T** (Gb/s)	**TpA** (Gb/s·mm^2)	**P** (mW)	**E** (mJ/Gb)
AES (Ofb)	308,286	213	0.620	2.010	294	476
Achterbahn	225,966	302	0.562	2.487	114	204
Grain	129,579	336	5.007	38.641	136	27
Mickey	88,118	317	0.296	3.357	79	267
Mosquito	385,752	287	0.802	2.079	319	398
Sfinks	391,850	162	1.209	3.086	387	320
Trivium	151,628	400	23.842	157.239	189	8
Vest	421,811	328	4.892	11.598	372	76
ZK-Crypt	137,182	250	7.434	54.190	82	11

Area


Area Comparison of eSTREAM Candidates
Area [squm]
500k
400k
300k
200k
100k
0
422
392
386
308
226
152
137
130
88
Vest16
Sfinks+
Mosquito
AES
Achterbahn
Trivium
ZKCrypt
Grain
Mickey

Maximum clock frequency



Power consumption