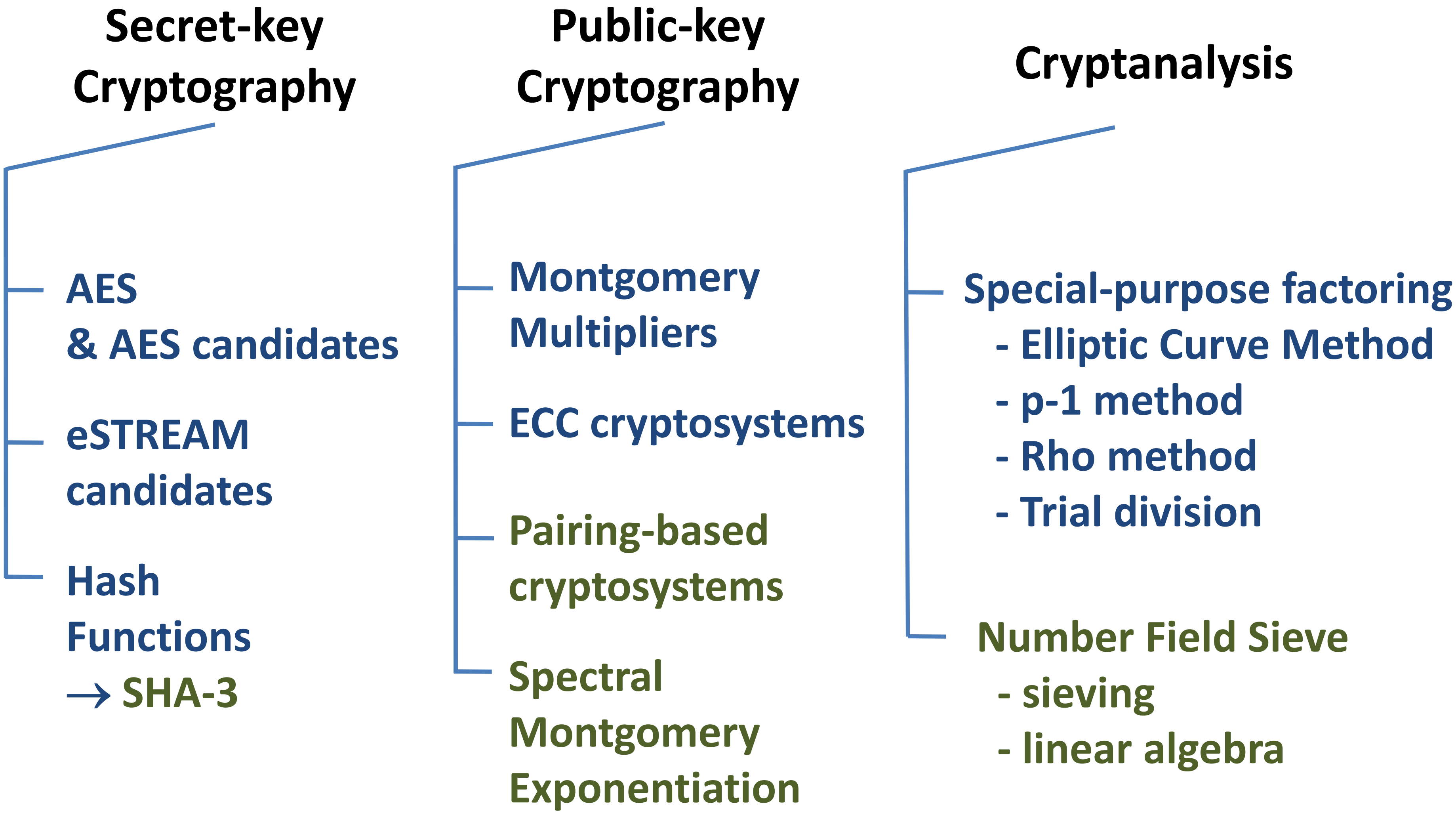
Hardware Architectures



Secret-key Cryptography

- AES & AES candidates
- eSTREAM candidates
- Hash Functions → SHA-3

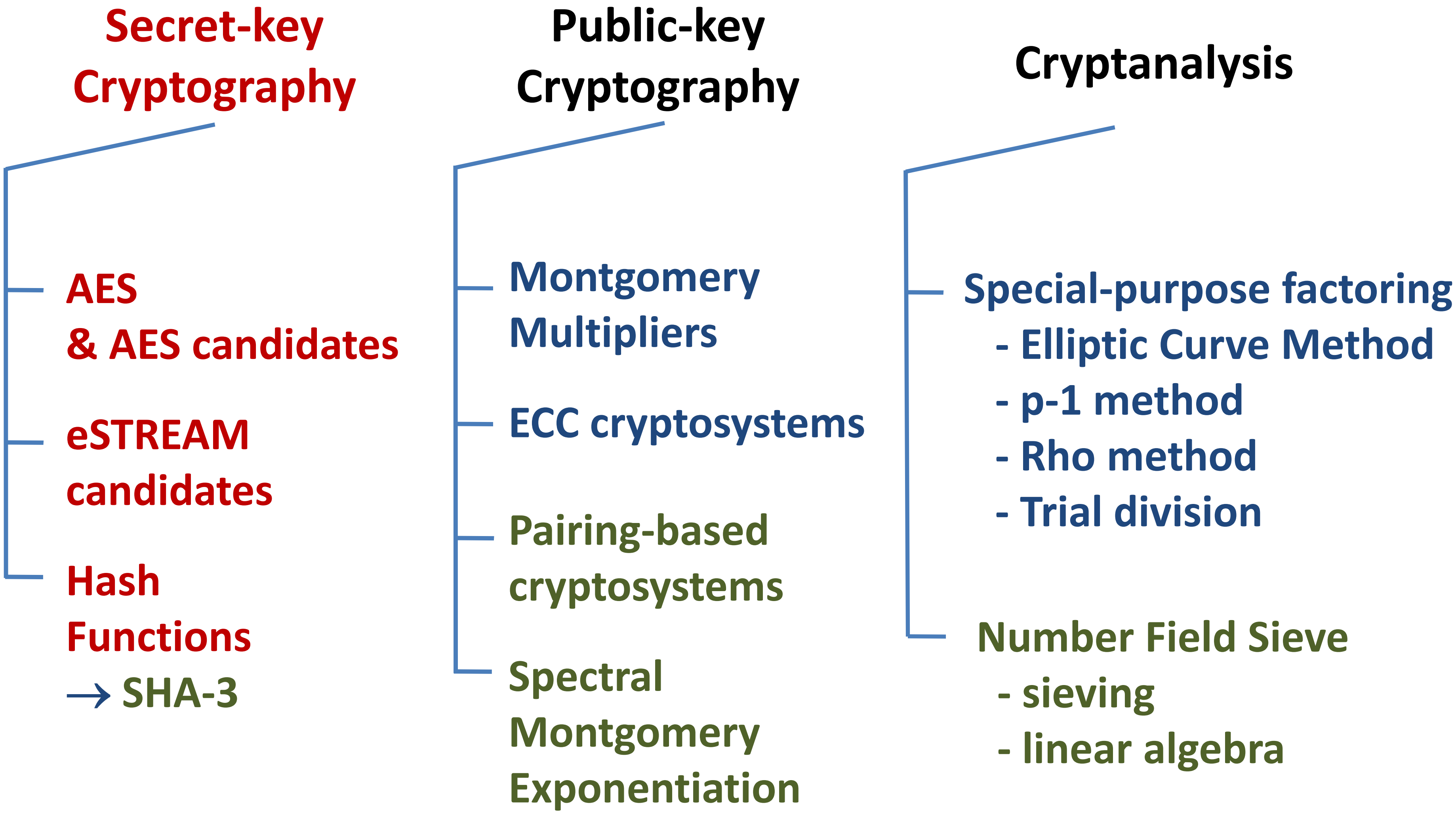
Public-key Cryptography

- Montgomery Multipliers
- ECC cryptosystems
- Pairing-based cryptosystems
- Spectral Montgomery Exponentiation

Cryptanalysis

- Special-purpose factoring
  - Elliptic Curve Method
  - p-1 method
  - Rho method
  - Trial division
- Number Field Sieve
  - sieving
  - linear algebra

Hardware Architectures



Secret-key Cryptography

- AES & AES candidates
- eSTREAM candidates
- Hash Functions → SHA-3

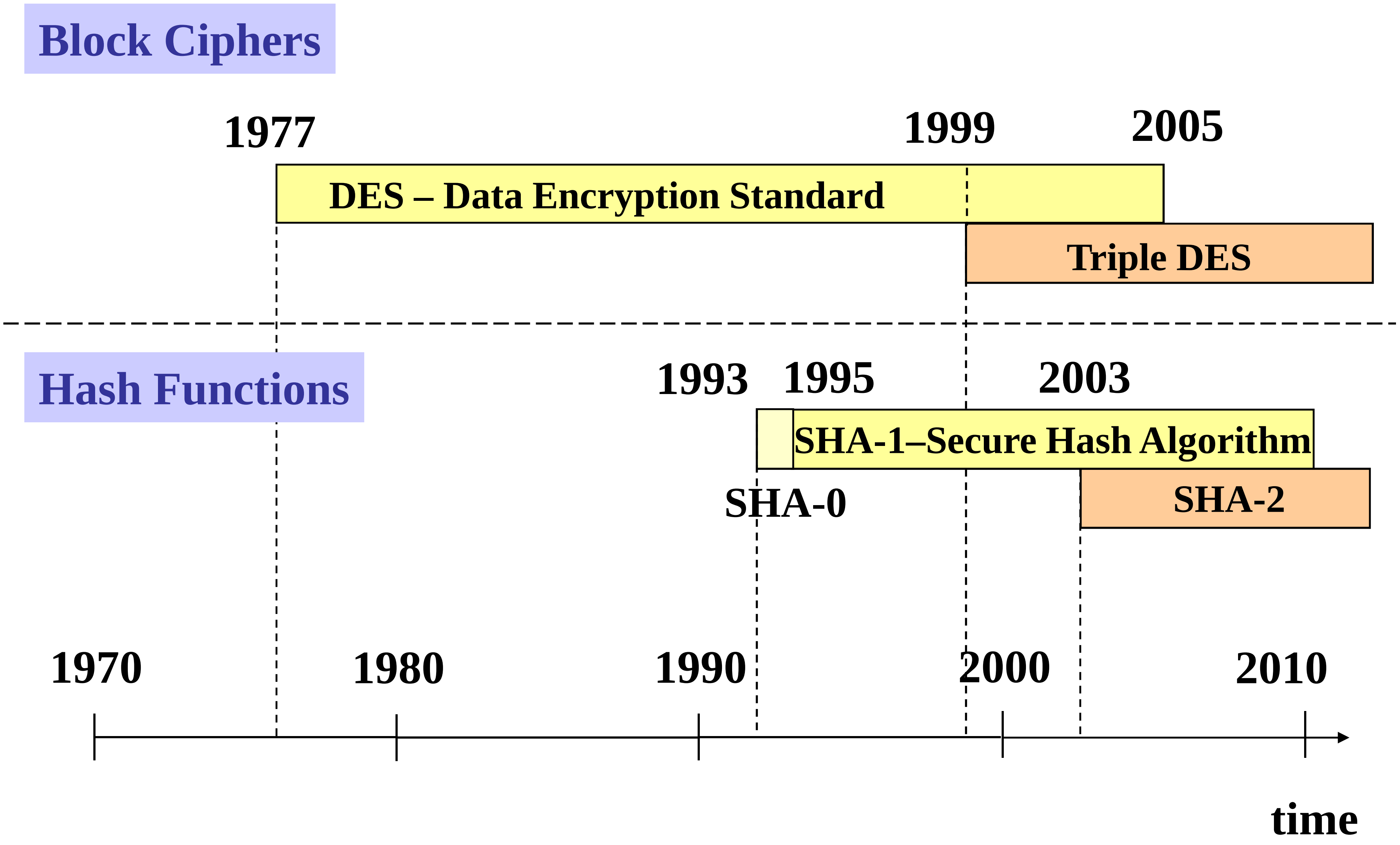
Public-key Cryptography

- Montgomery Multipliers
- ECC cryptosystems
- Pairing-based cryptosystems
- Spectral Montgomery Exponentiation

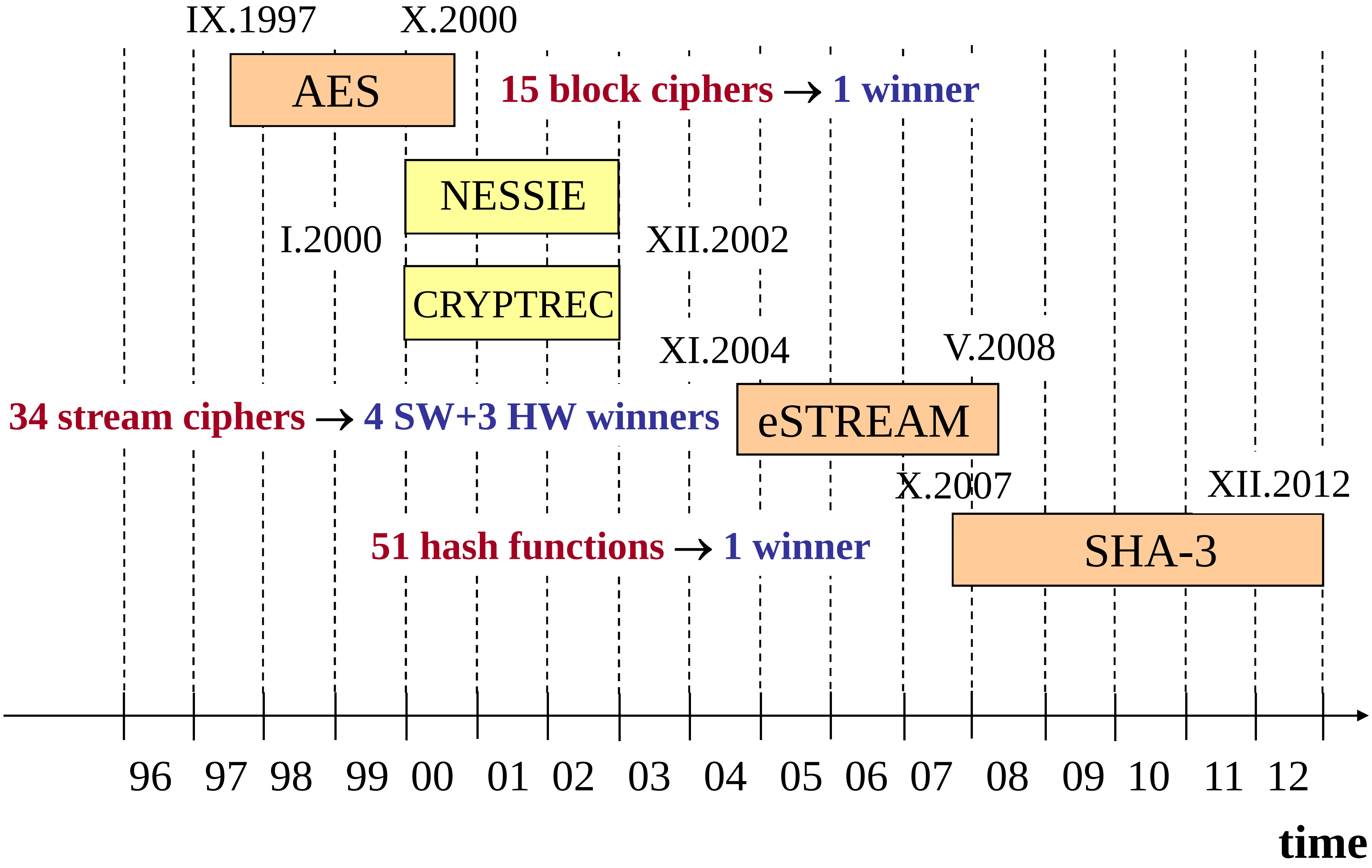
Cryptanalysis

- Special-purpose factoring
  - Elliptic Curve Method
  - p-1 method
  - Rho method
  - Trial division
- Number Field Sieve
  - sieving
  - linear algebra

NSA-developed Cryptographic Standards



Cryptographic Standard Contests



IX.1997 X.2000

AES

15 block ciphers → 1 winner

NESSIE

I.2000 XII.2002

CRYPTREC

XI.2004 V.2008

34 stream ciphers → 4 SW+3 HW winners

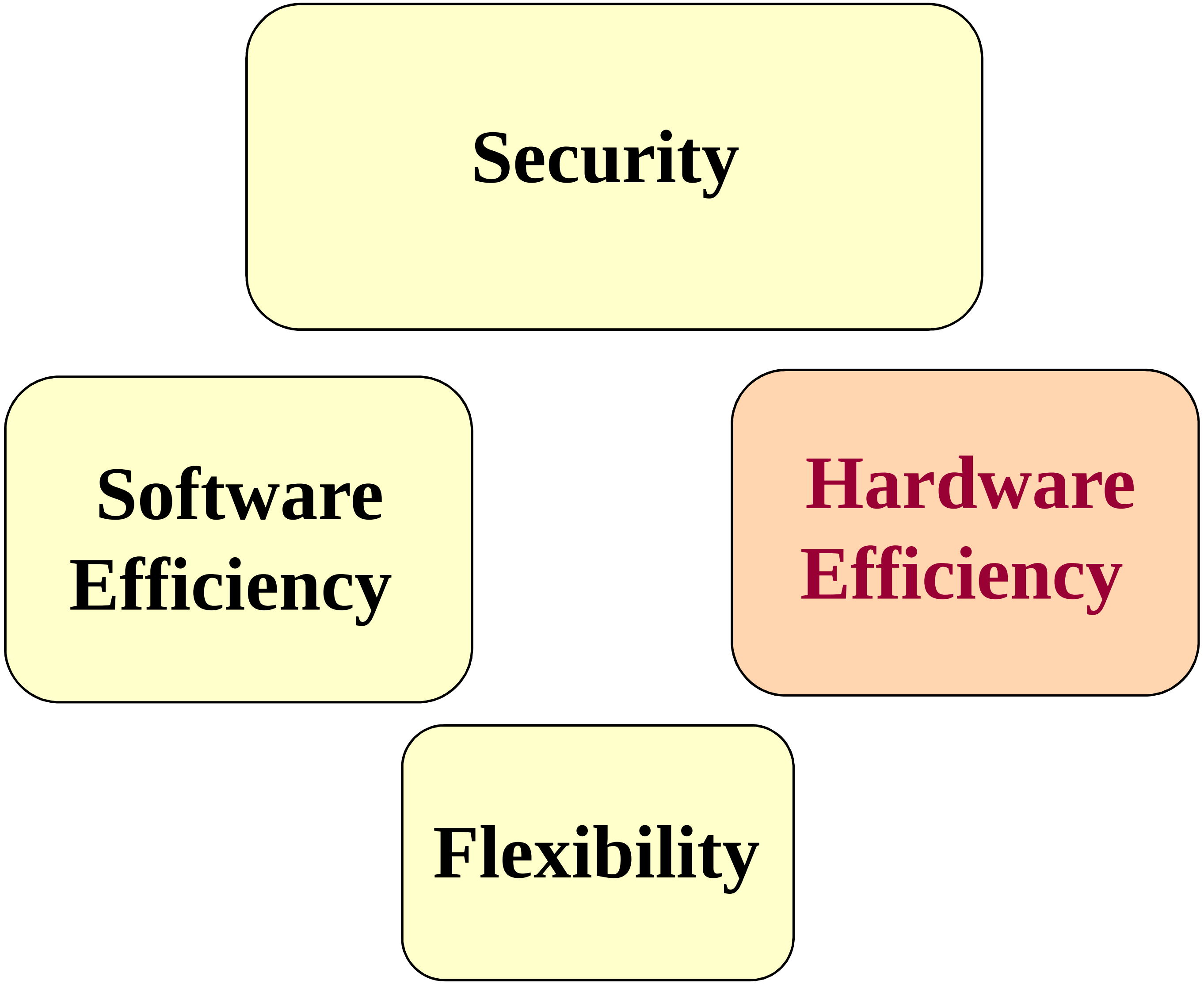
eSTREAM

X.2007 XII.2012

51 hash functions → 1 winner

SHA-3

Criteria used to evaluate cryptographic transformations



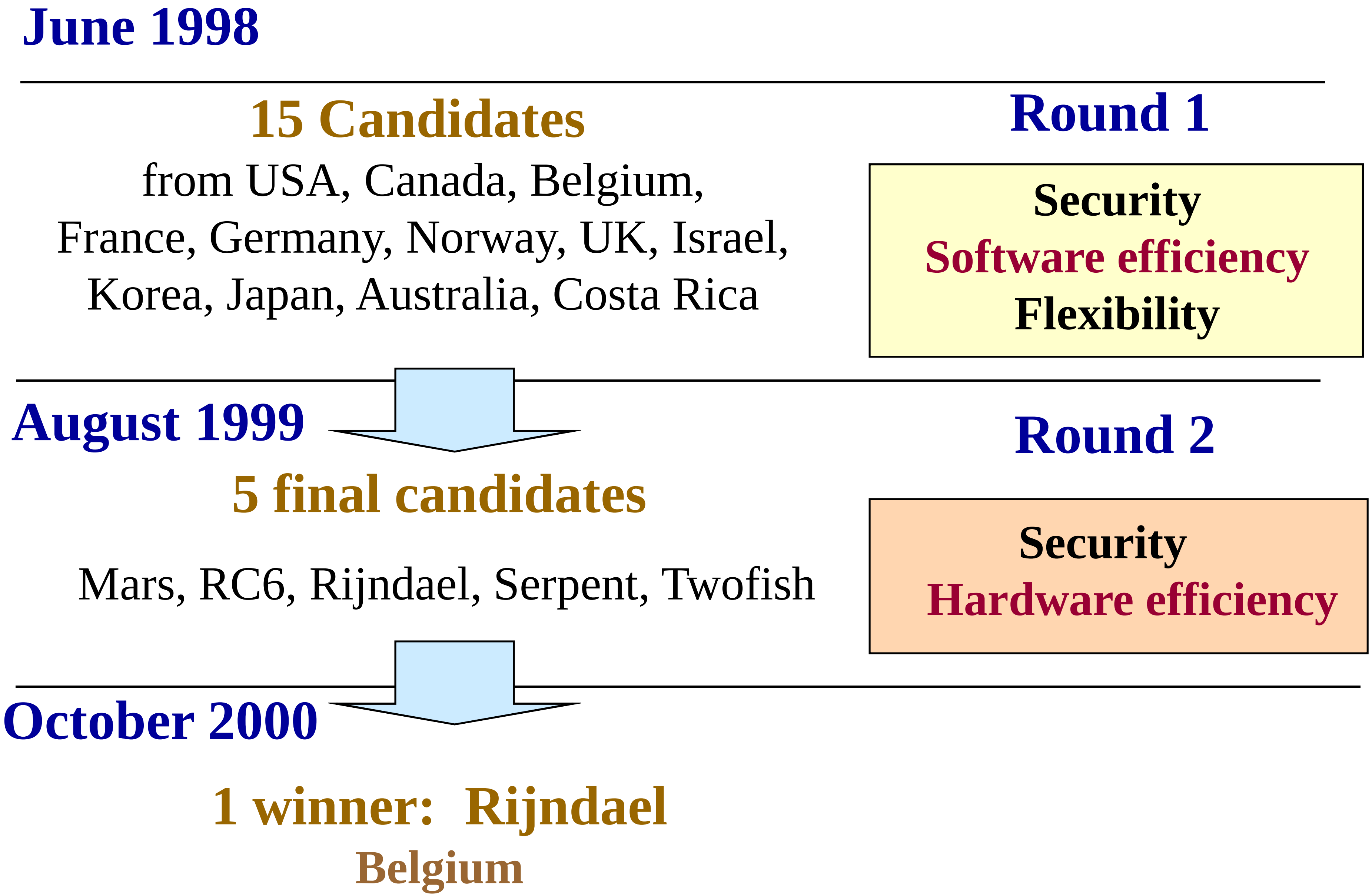
Security

Software Efficiency

Hardware Efficiency

Flexibility

Advanced Encryption Standard (AES) Contest
1997-2001



June 1998

15 Candidates

from USA, Canada, Belgium,
France, Germany, Norway, UK, Israel,
Korea, Japan, Australia, Costa Rica

Round 1

Security
Software efficiency
Flexibility

August 1999

5 final candidates

Mars, RC6, Rijndael, Serpent, Twofish

Round 2

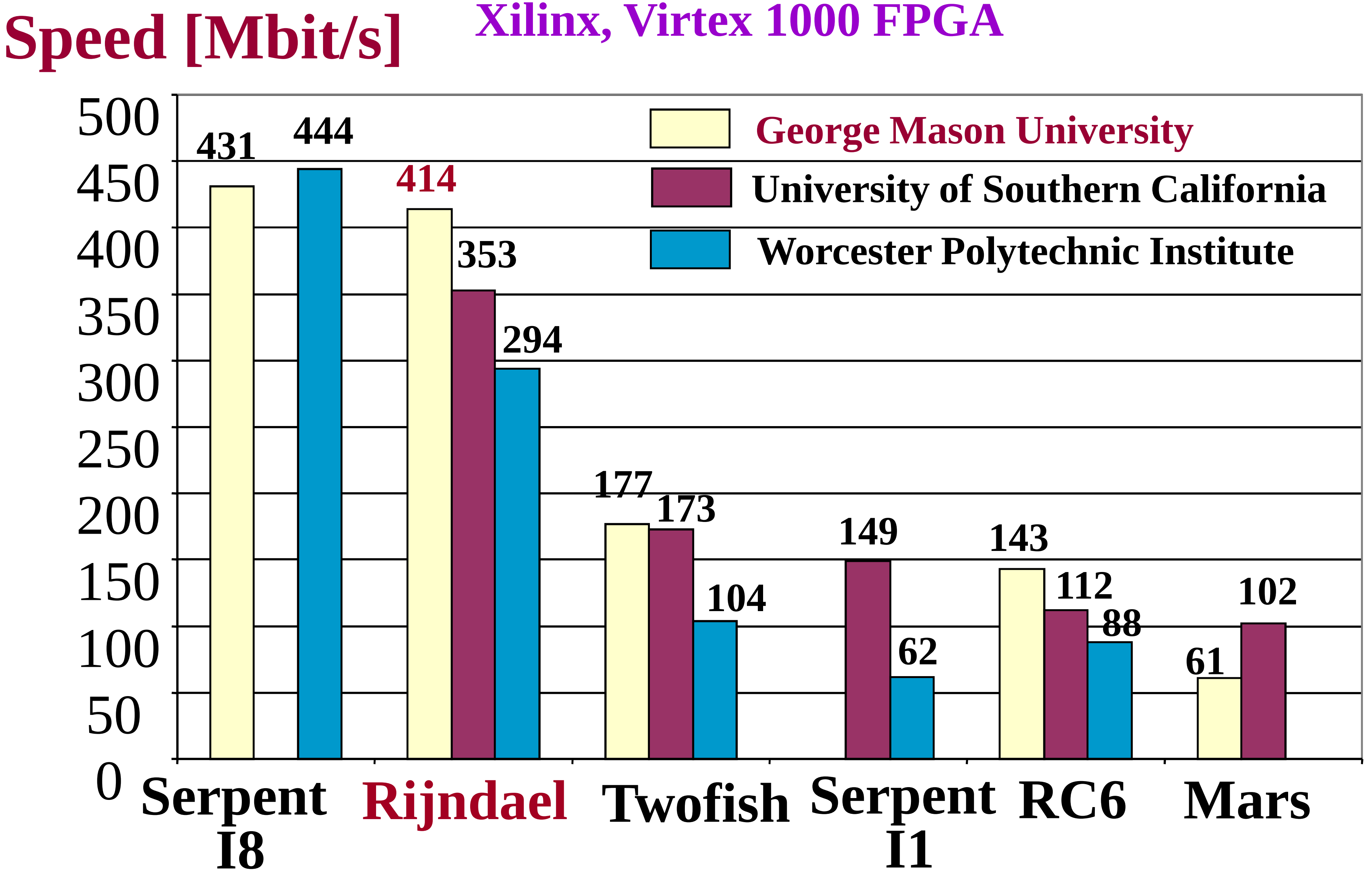
Security
Hardware efficiency

October 2000

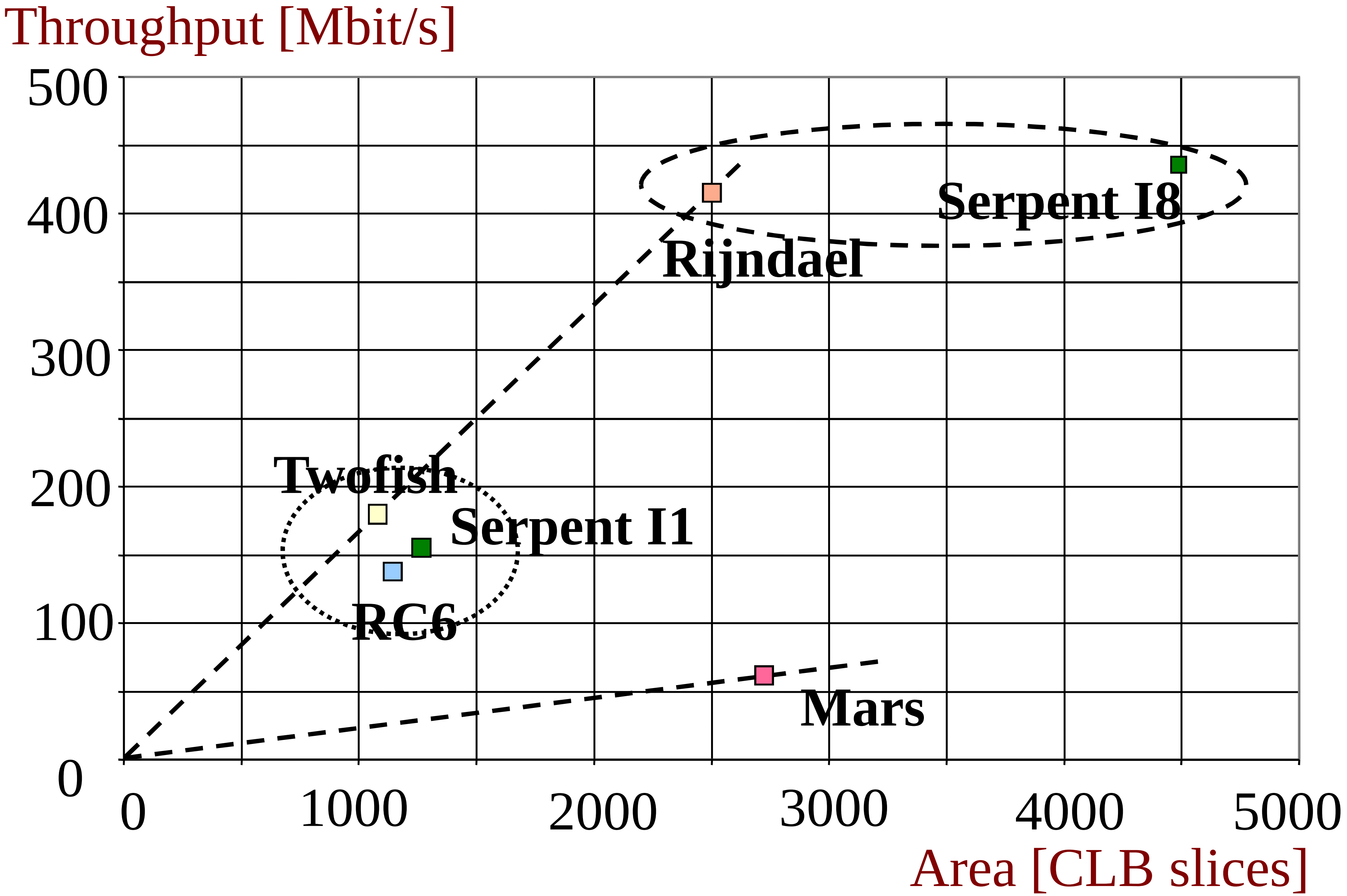
1 winner: Rijndael
Belgium

Implementations of candidates for the new Advanced Encryption Standard (AES)

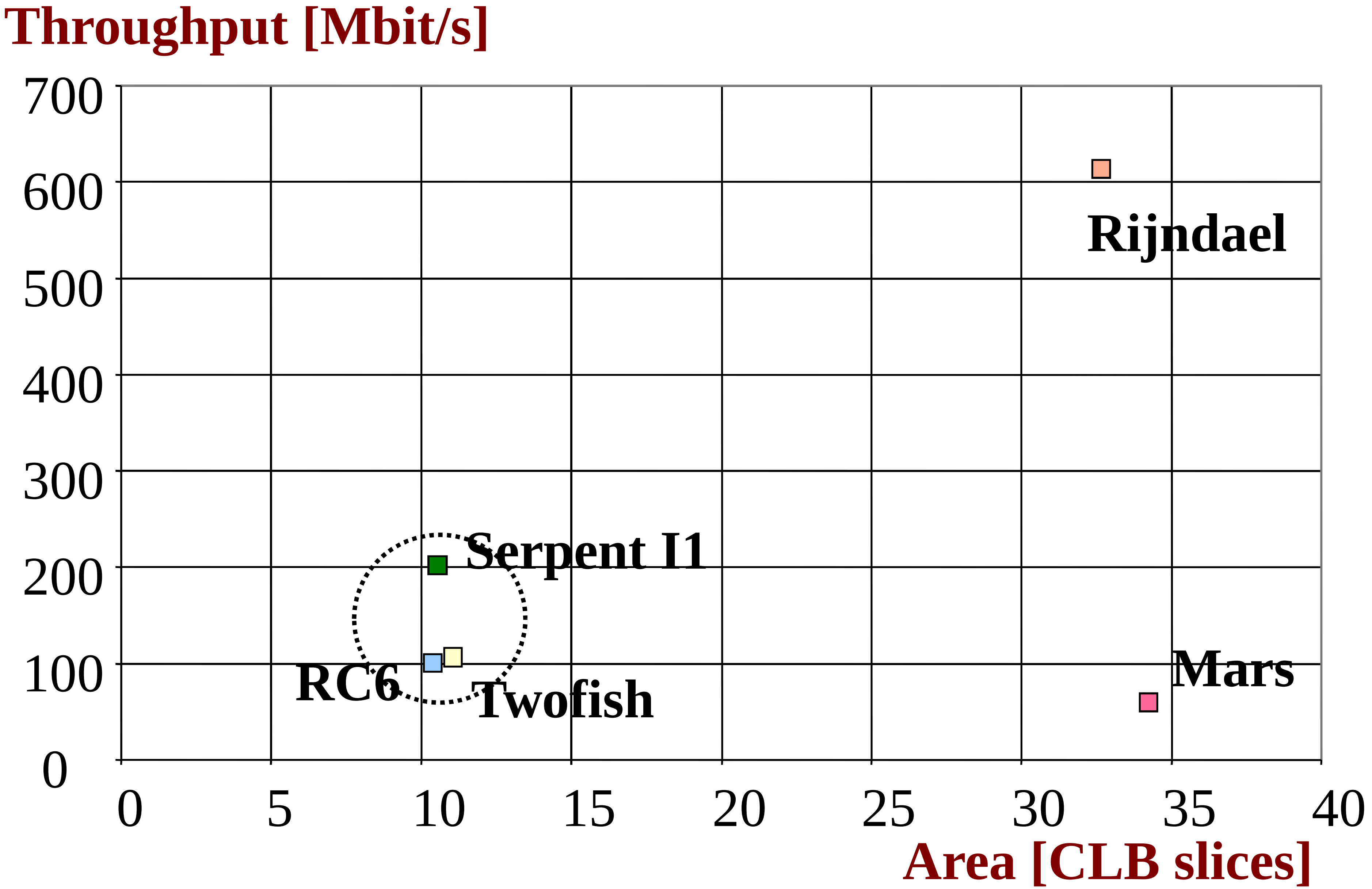
Xilinx, Virtex 1000 FPGA



Our Results: Encryption in cipher feedback modes (CBC, CFB, OFB) - Virtex FPGA

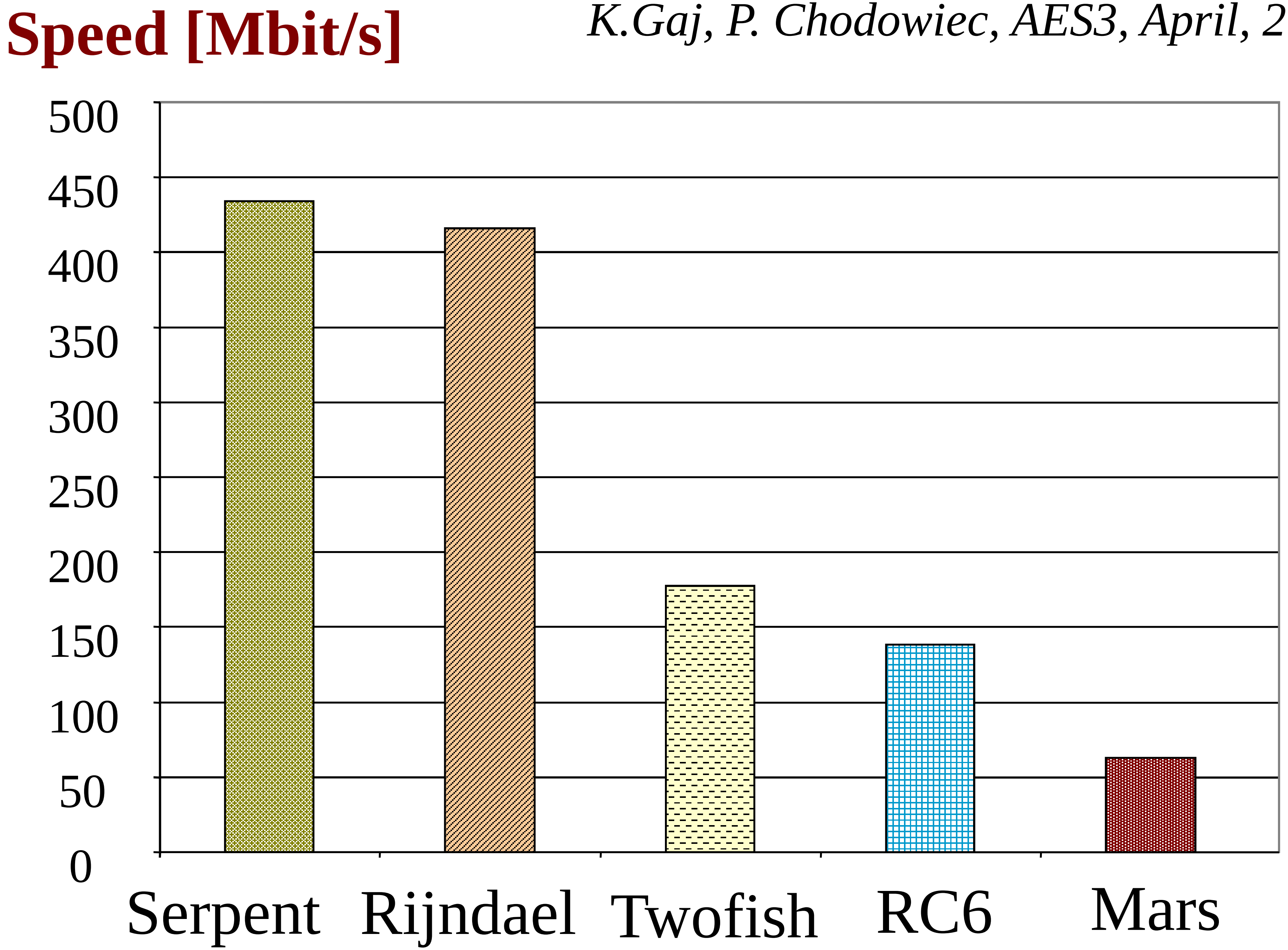


NSA Results: Encryption in cipher feedback modes (CBC, CFB, OFB) - ASIC, 0.5 µm CMOS

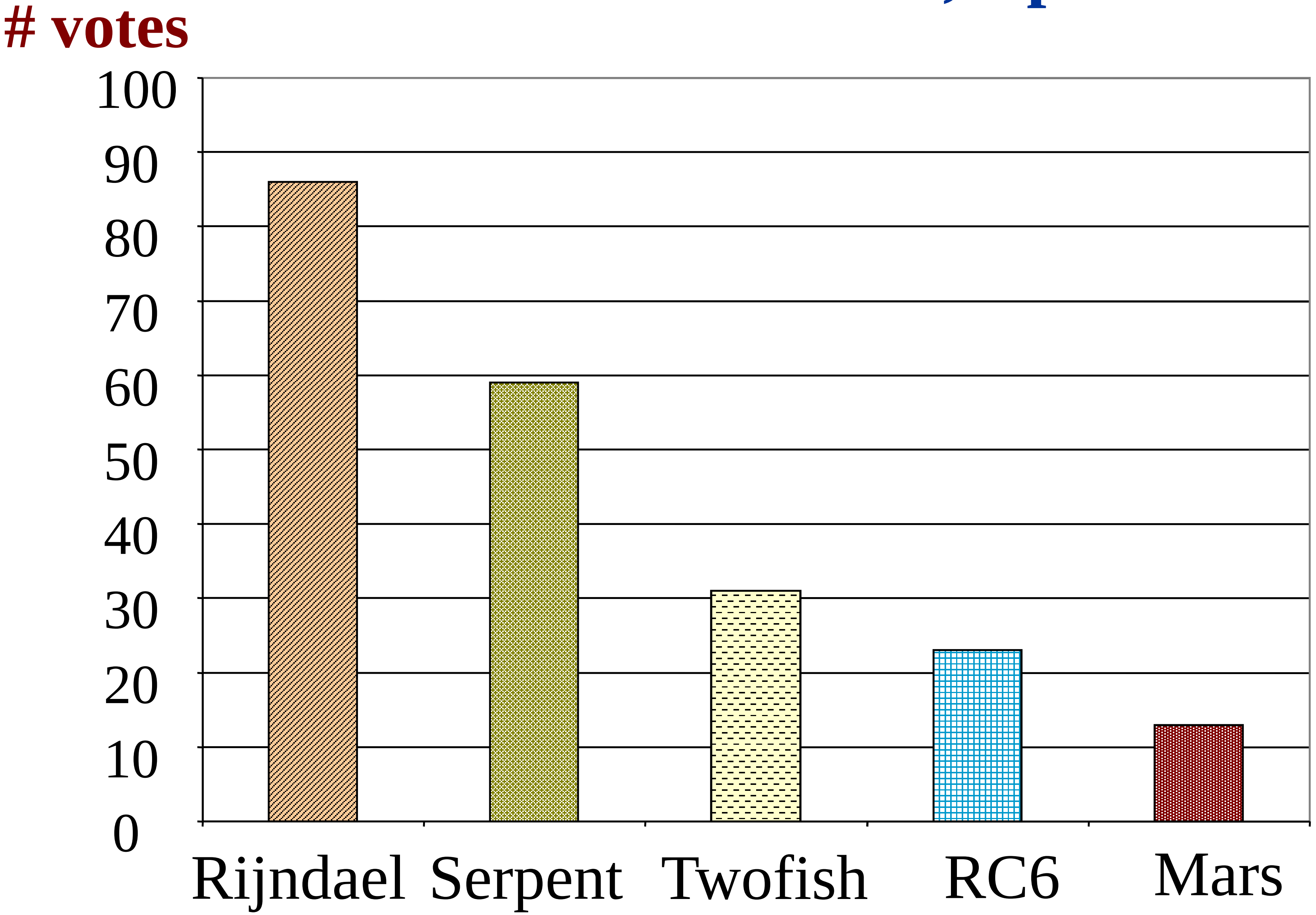


Speed of the final AES candidates in Xilinx FPGAs

K.Gaj, P. Chodowiec, AES3, April, 2000

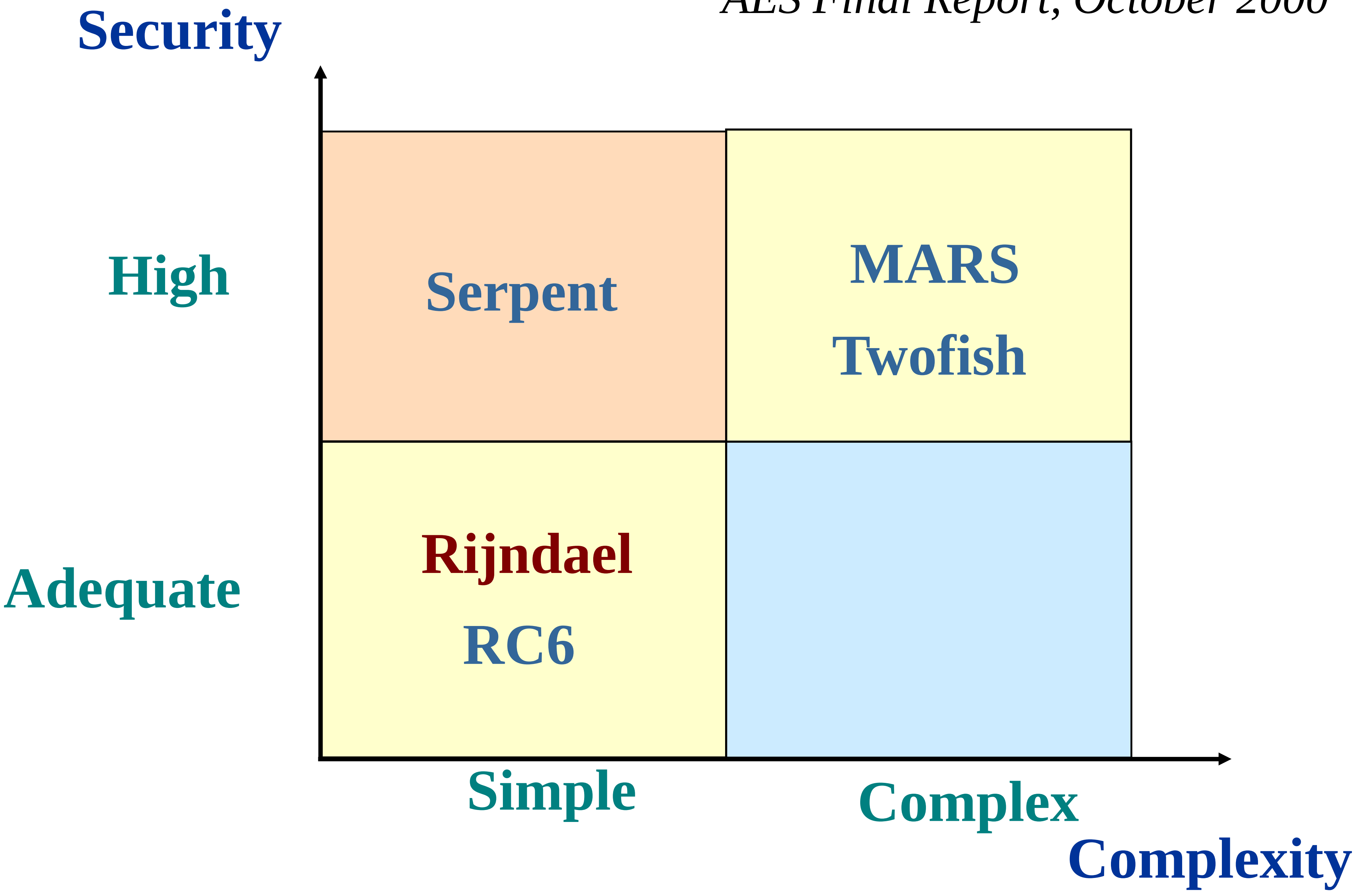


Survey filled by 167 participants of the Third AES Conference, April 2000



NIST Report: Security

AES Final Report, October 2000



Security	Simple	Complex
High	Serpent	MARS Twofish
Adequate	Rijndael RC6	

eSTREAM Stream Cipher Comparison

- Part of the GMU Fall 2006 & Fall 2007 graduate courses
  ECE 545 Introduction to VHDL

- Individual 6-week project

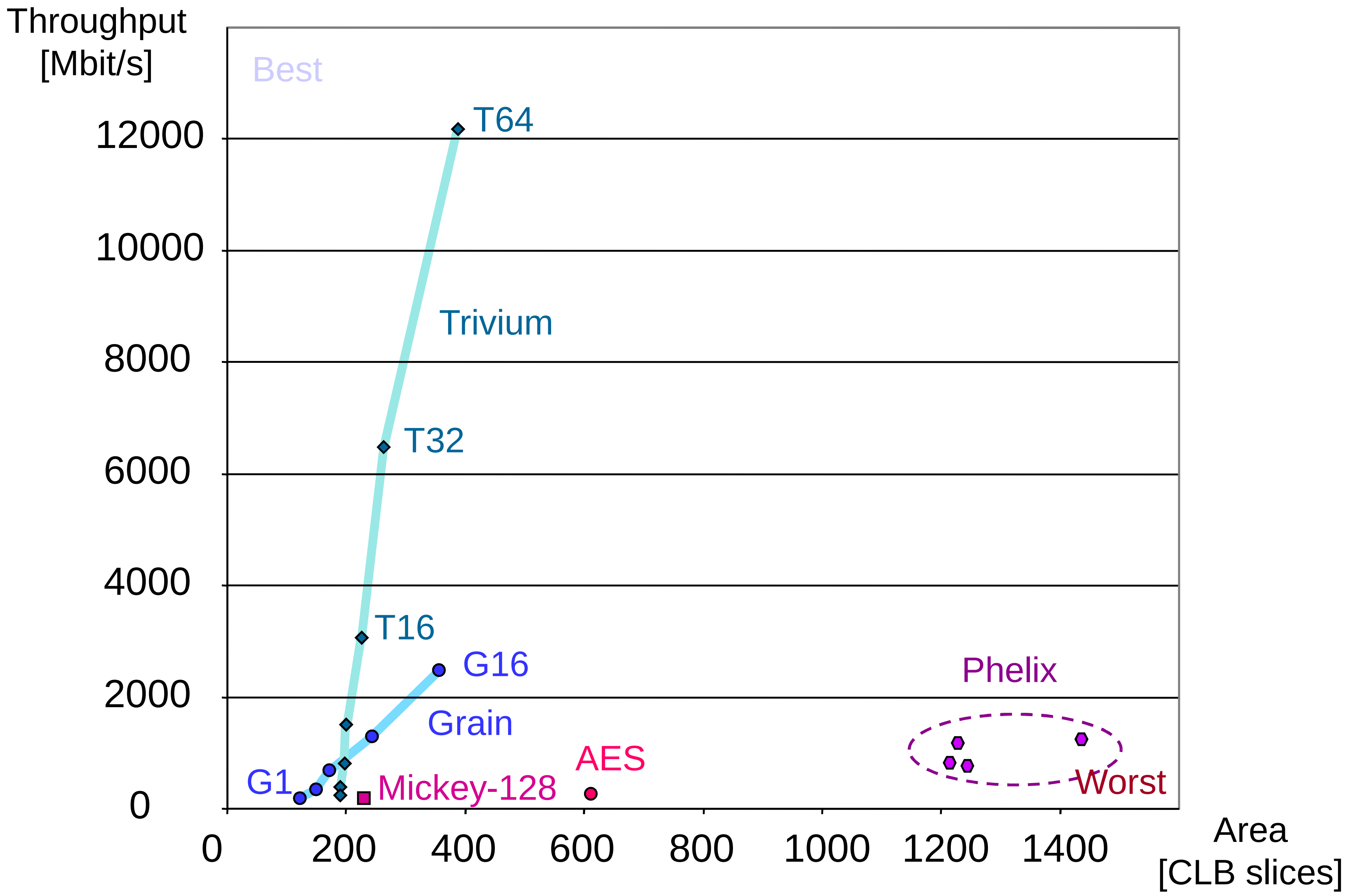
- 4 students working independently on each eSTREAM cipher

- 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
  - possibly uniform design & coding style

Comparison of 4 Focus Hardware-Oriented Stream Ciphers

FPGA: Xilinx Spartan 3 family



Comparison of 8 Final Candidates Sorted by Minimum Area and Maximum Throughput/Area

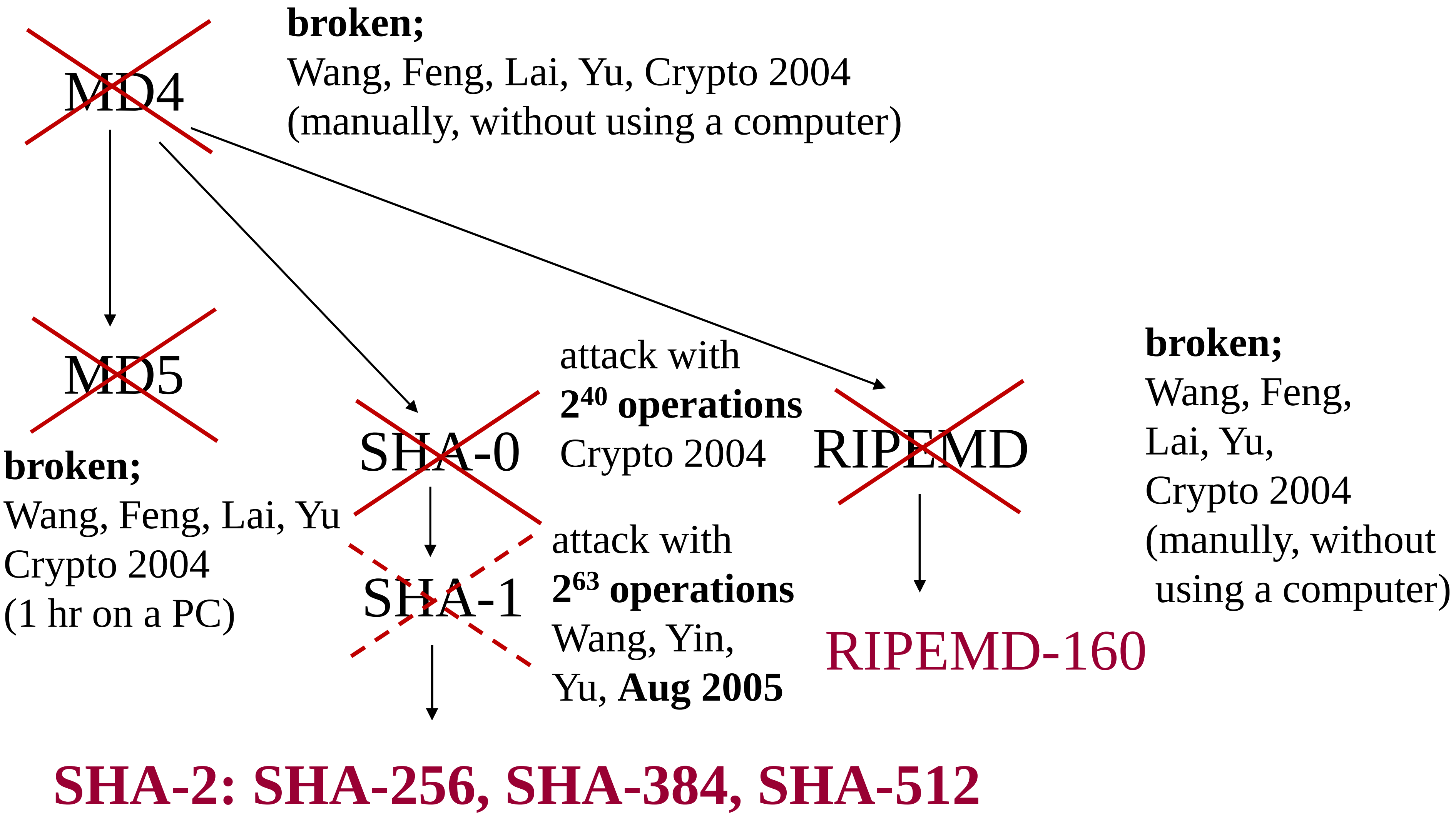
Candidate	Area (slices)	Candidate	Throughput/Area (Mbps/slices)
Grain v1	44	Trivium (x64)	39.26
Grain 128	50	Grain 128 (x32)	7.97
Trivium	50	Grain v1 (x16)	5.98
DECIM v2	80	Trivium	4.80
DECIM 128	89	F-FCSR-16	4.53
MICKEY 2.0	115	Grain v1	4.45
MICKEY 128 2.0	176	Grain 128	3.92
Moustique	278	F-FCSR-H v2	3.23
F-FCSR-H v2	342	MICKEY 2.0	2.03
Trivium (x64)	344	MICKEY 128 2.0	1.27
Grain v1 (x16)	348	Moustique	0.81
F-FCSR-16	473	DECIM v2	0.58
Grain 128 (x32)	534	DECIM 128	0.49
Pomaranch	648	Edon80	0.10
Edon80	1284	Pomaranch	0.08

Conclusions from the Comparison of the eSTREAM Candidates in Hardware

Very large differences among 8 leading candidates:

~30 x	**in terms of area (Grain v1 vs. Edon80)**
~500 x	**in terms of the throughput to area ratio (Trivium (x64) vs. Pomaranch)**

Current State of Security of Major Hash Functions



~~MD4~~

broken;
Wang, Feng, Lai, Yu, Crypto 2004
(manually, without using a computer)

~~MD5~~

broken;
Wang, Feng, Lai, Yu
Crypto 2004
(1 hr on a PC)

~~SHA-0~~

attack with
2^{40} operations
Crypto 2004

~~SHA-1~~

attack with
2^{63} operations
Wang, Yin,
Yu, **Aug 2005**

~~RIPEMD~~

broken;
Wang, Feng,
Lai, Yu,
Crypto 2004
(manully, without
using a computer)

RIPEMD-160

SHA-2: SHA-256, SHA-384, SHA-512

SHA-3 Contest Timeline

2007

- publication of requirements
- 29.X. 2007: request for candidates

2008

- 31.X.2008: deadline for submitting candidates

2009

2 Q – first workshop devoted to the presentation of candidates

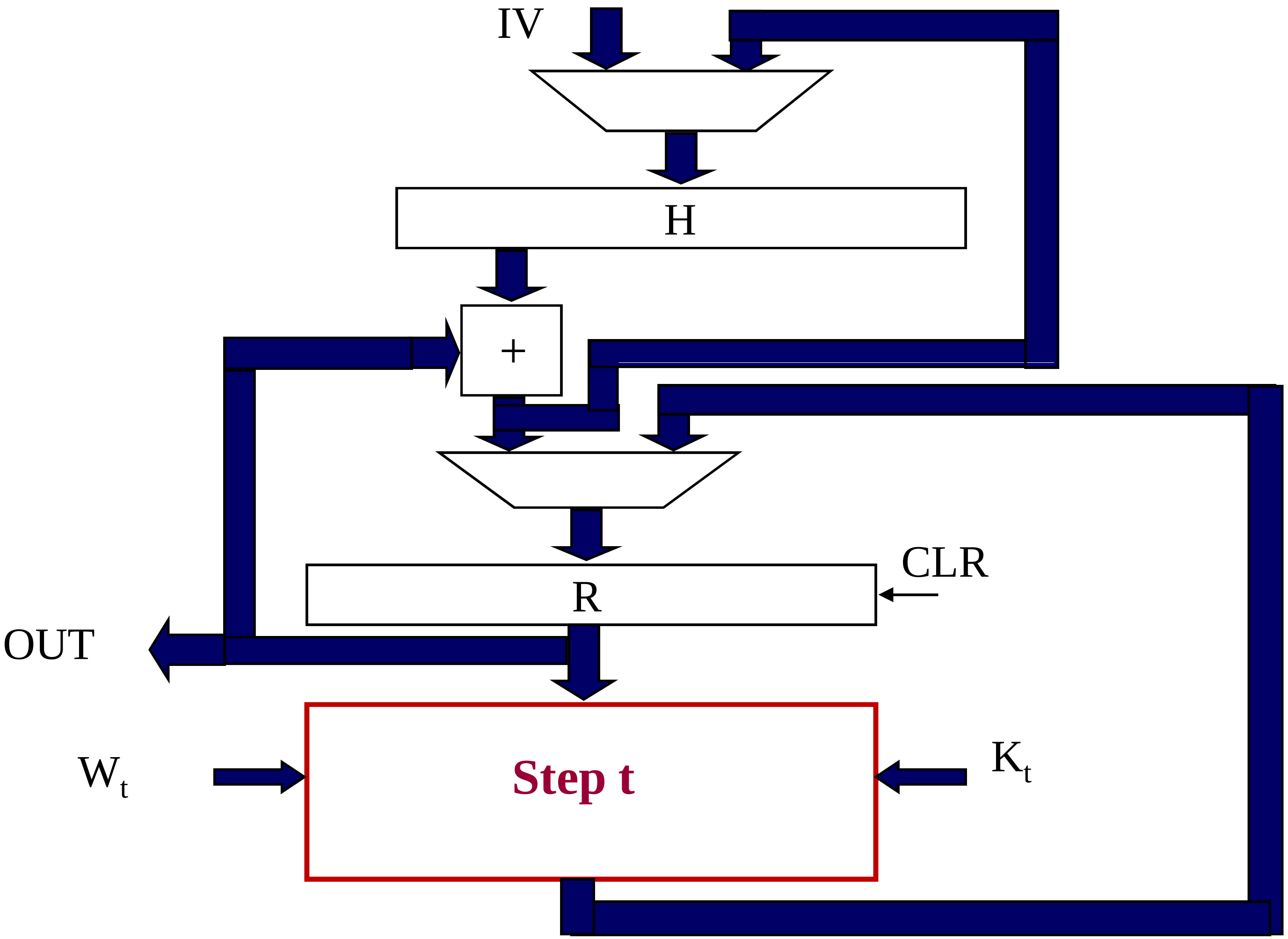
2010

2 Q: second workshop devoted to the analysis of candidates
3 Q: selection of finalists

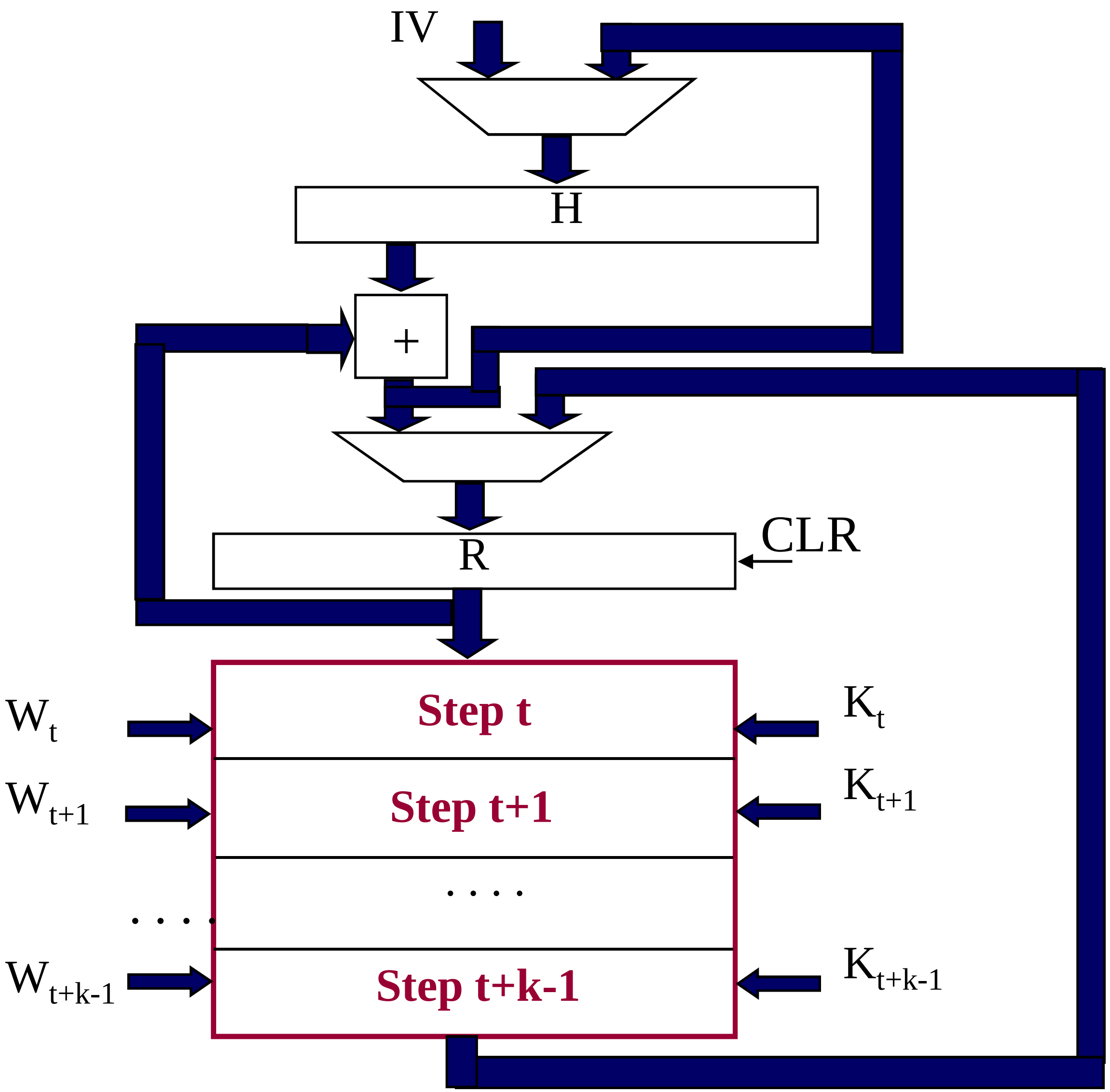
2012

1 Q: last workshop
2 Q: selection of the winner
3 Q: draft version of the standard published
4 Q: final version of the standard published

Basic iterative architecture of a typical hash function



Unrolled architecture



Unrolled Architectures of Hash Functions - Summary

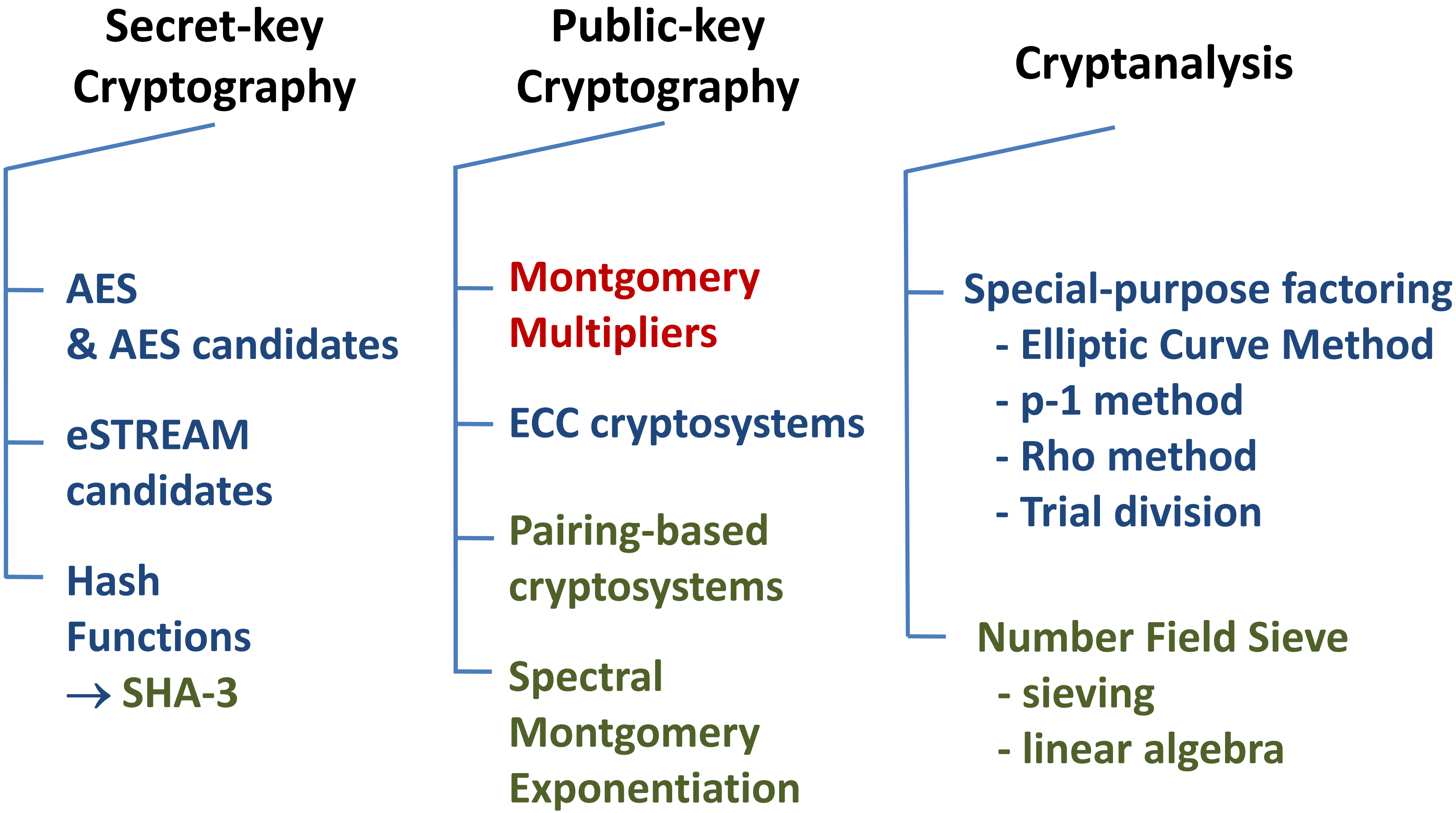
Loop unrolling more suitable for hash algorithms than for symmetric-key ciphers

Speed up compared to the basic iterative architecture:

SHA-1:	**1.9**	(5 rounds unrolled)
SHA-256:	**1.5**	(4 rounds unrolled)
SHA-512:	**1.3**	(5 rounds unrolled)

Speed up is a strong function of data dependencies present in the algorithm

Hardware Architectures



Secret-key Cryptography

- AES & AES candidates
- eSTREAM candidates
- Hash Functions → SHA-3

Public-key Cryptography

- Montgomery Multipliers
- ECC cryptosystems
- Pairing-based cryptosystems
- Spectral Montgomery Exponentiation

Cryptanalysis

- Special-purpose factoring
  - Elliptic Curve Method
  - p-1 method
  - Rho method
  - Trial division
- Number Field Sieve
  - sieving
  - linear algebra

Montgomery Multipliers: Motivation

- Fast modular multiplication required in multiple cryptographic transformations
    - RSA, DSA, Diffie-Hellman
    - Elliptic Curve Cryptosystems
    - ECM, p-1, Pollard's rho methods of factoring, etc.

- Montgomery Multiplication invented by Peter L. Montgomery in 1985 is most frequently used to implement repetitive sequence of modular multiplications in both software and hardware

- Montgomery Multiplication in hardware replaces division by a sequence of simple logic operations, conditional additions and right shifts

Primary Advantage of our New Architectures

- Reduction in the number of clock cycles

  from

  $$\mathbf{2\,n + e - 1}$$

  to

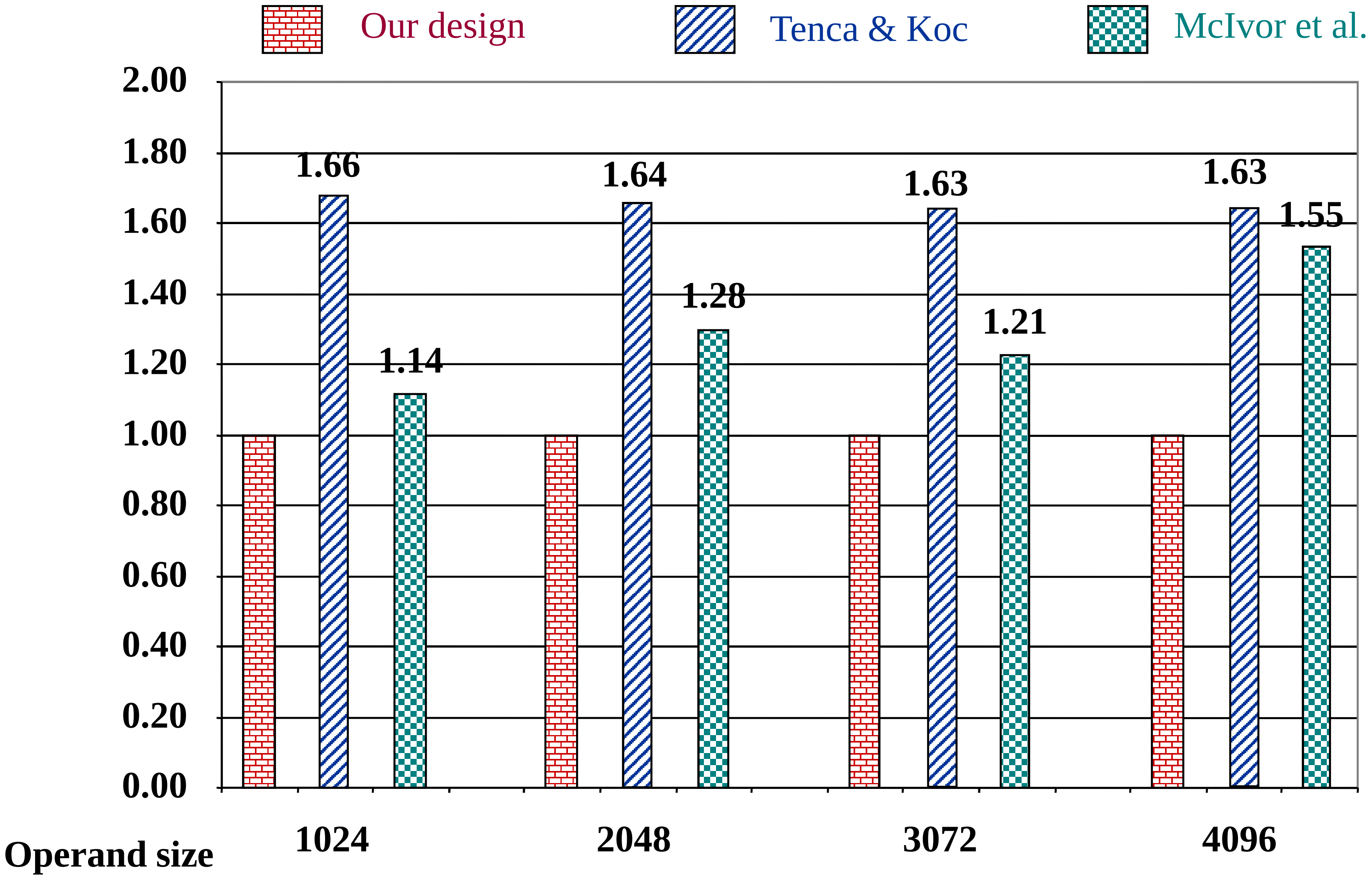
  $$\mathbf{n + e - 1}$$

n – size of operands in bits

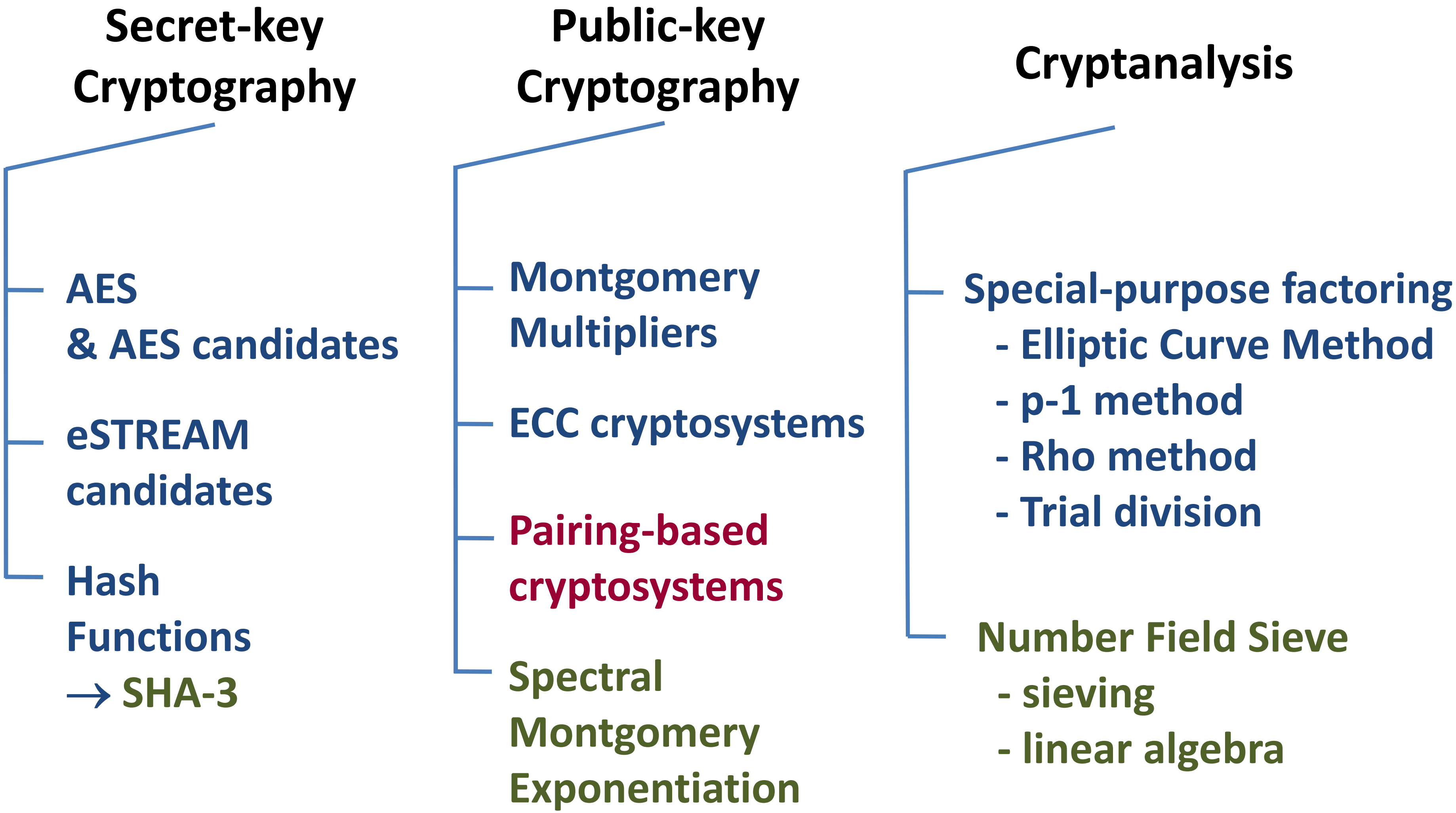
e – size of operands in words

- Minimum penalty in terms of the area and clock period

Normalized Product Latency Times Area
New Architecture vs. Previous Architectures



Hardware Architectures



Secret-key Cryptography

- AES & AES candidates
- eSTREAM candidates
- Hash Functions → SHA-3

Public-key Cryptography

- Montgomery Multipliers
- ECC cryptosystems
- Pairing-based cryptosystems
- Spectral Montgomery Exponentiation

Cryptanalysis

- Special-purpose factoring
  - Elliptic Curve Method
  - p-1 method
  - Rho method
  - Trial division
- Number Field Sieve
  - sieving
  - linear algebra

Pairing Based Cryptography

- New family of public key cryptosystems, first proposed by Menezes, Okamoto, and Vanstone in 1993

- Application to:
  - Identity Based Cryptography
  - One-round 3-way key exchange
  - Short digital signatures
  - Others: Group signatures, batch signatures, threshold cryptography, broadcast encryption, private information retrieval, electronic voting, etc.

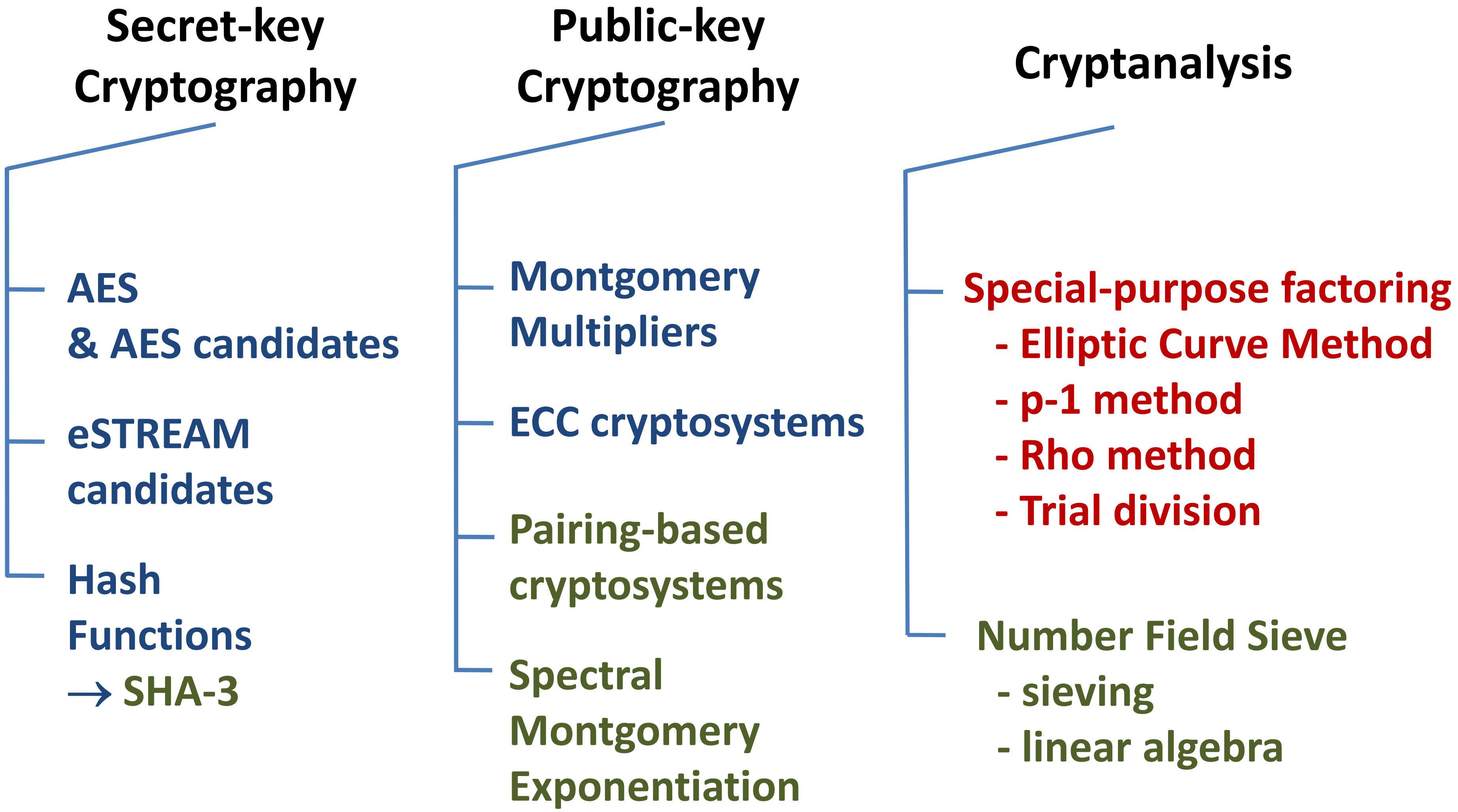
- Not a part of any standard yet

- Very limited number of software and hardware implementations

Spectral Modular Exponentiation

- New method for fast modular exponentiation for very long integers in the range of 10,000-20,000 bits
- First publication in 2007, by Koc and Saldamli
- Intersection of cryptography and Digital Signal Processing
- Better computational complexity than any other algorithm known to date
- No reported software or hardware implementations

Hardware Architectures



Secret-key Cryptography

- AES & AES candidates
- eSTREAM candidates
- Hash Functions → SHA-3

Public-key Cryptography

- Montgomery Multipliers
- ECC cryptosystems
- Pairing-based cryptosystems
- Spectral Montgomery Exponentiation

Cryptanalysis

- Special-purpose factoring
  - Elliptic Curve Method
  - p-1 method
  - Rho method
  - Trial division
- Number Field Sieve
  - sieving
  - linear algebra

Workshop Series

SHARCS - Special-purpose Hardware for Attacking Cryptographic Systems

1st edition:	Paris,	Feb. 24-25,	2005
2nd edition:	Cologne,	Apr. 3-4,	2006
3rd edition:	Vienna,	Sep. 9-10,	2007

See

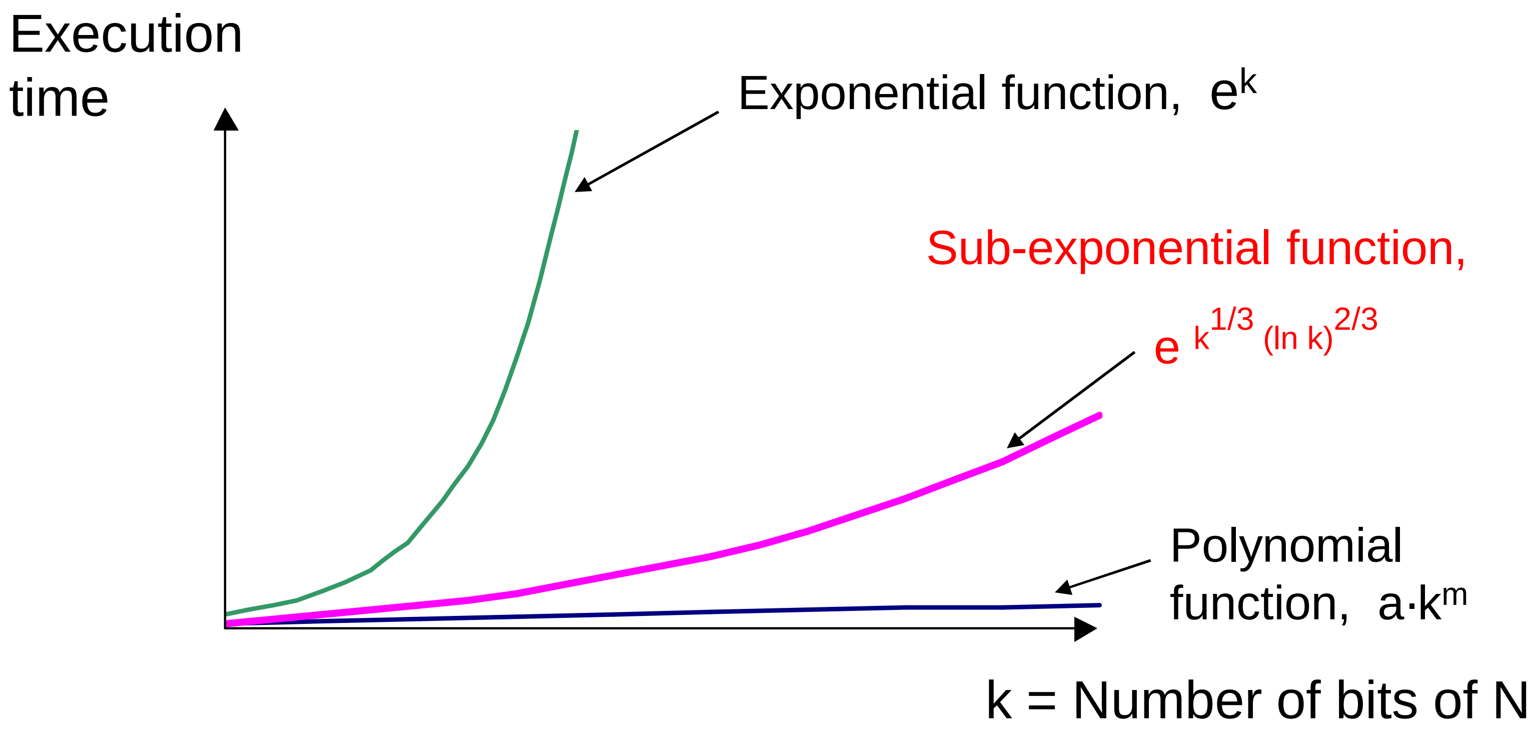
http://www.ruhr-uni-bochum.de/itsc/tanja/SHARCS/

Best Algorithm to Factor Large Numbers

NUMBER FIELD SIEVE

Complexity: Sub-exponential time and memory

N = Number to factor,
k = Number of bits of N



Execution time

Exponential function, e^k

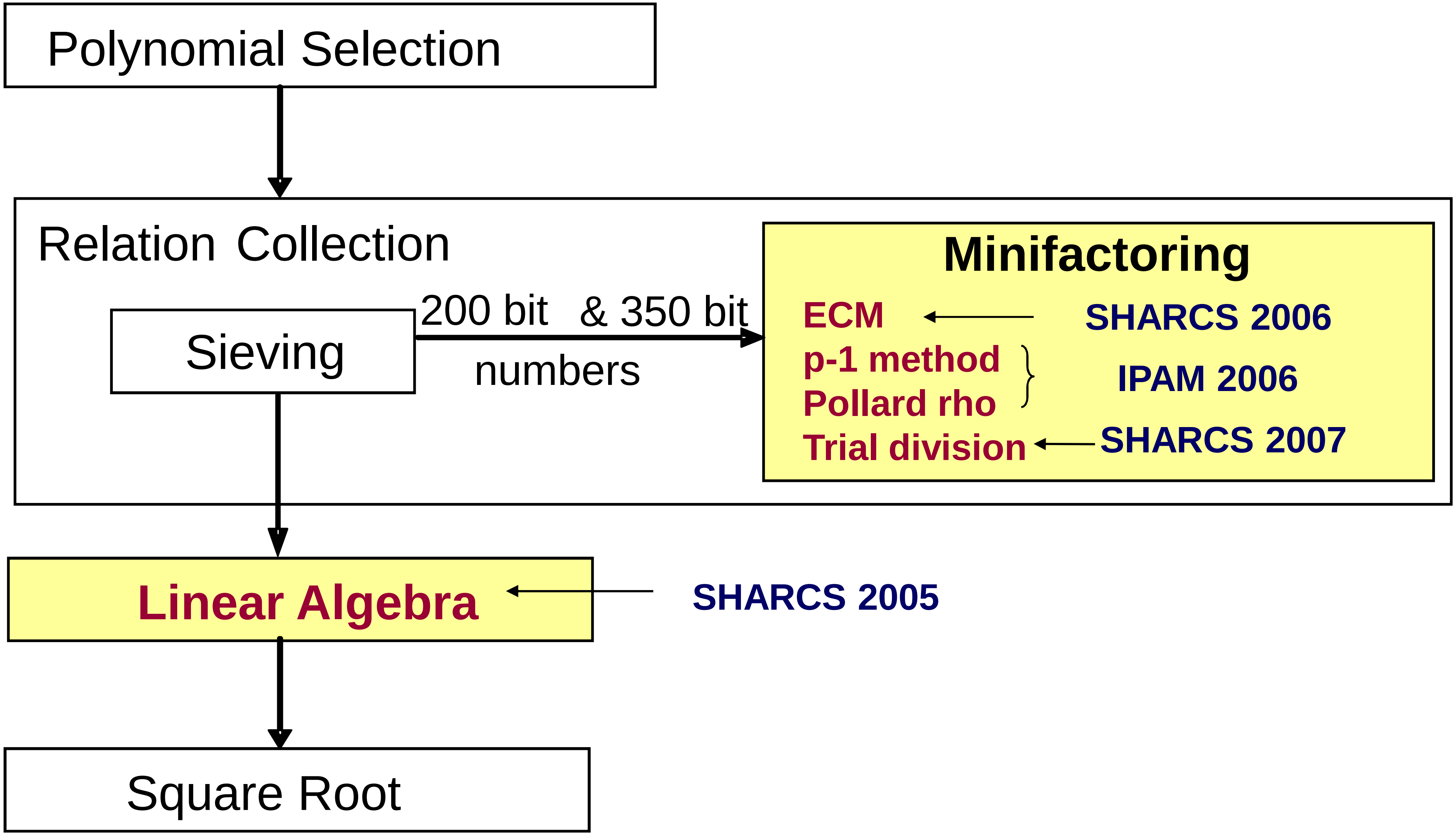
Sub-exponential function,

$e^{k^{1/3} (\ln k)^{2/3}}$

Polynomial function, $a \cdot k^m$

k = Number of bits of N

Factoring 1024-bit RSA keys using Number Field Sieve (NFS)



Polynomial Selection

Relation Collection

Sieving

200 bit & 350 bit numbers

Minifactoring

ECM ← **SHARCS 2006**

p-1 method
Pollard rho } **IPAM 2006**

Trial division ← **SHARCS 2007**

Linear Algebra ← **SHARCS 2005**

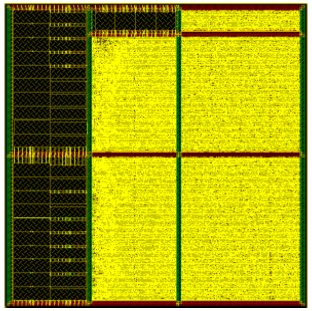
Square Root

Comparison among technologies

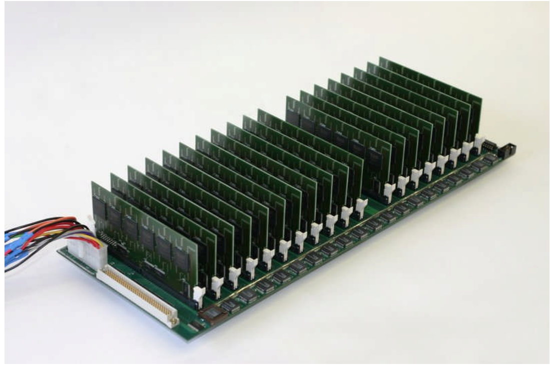
Microprocessors

FPGAs

ASICs



SRC



COPACOBANA

SRC 6
reconfigurable computer

SRC 6 from
SRC Computers

Basic unit:

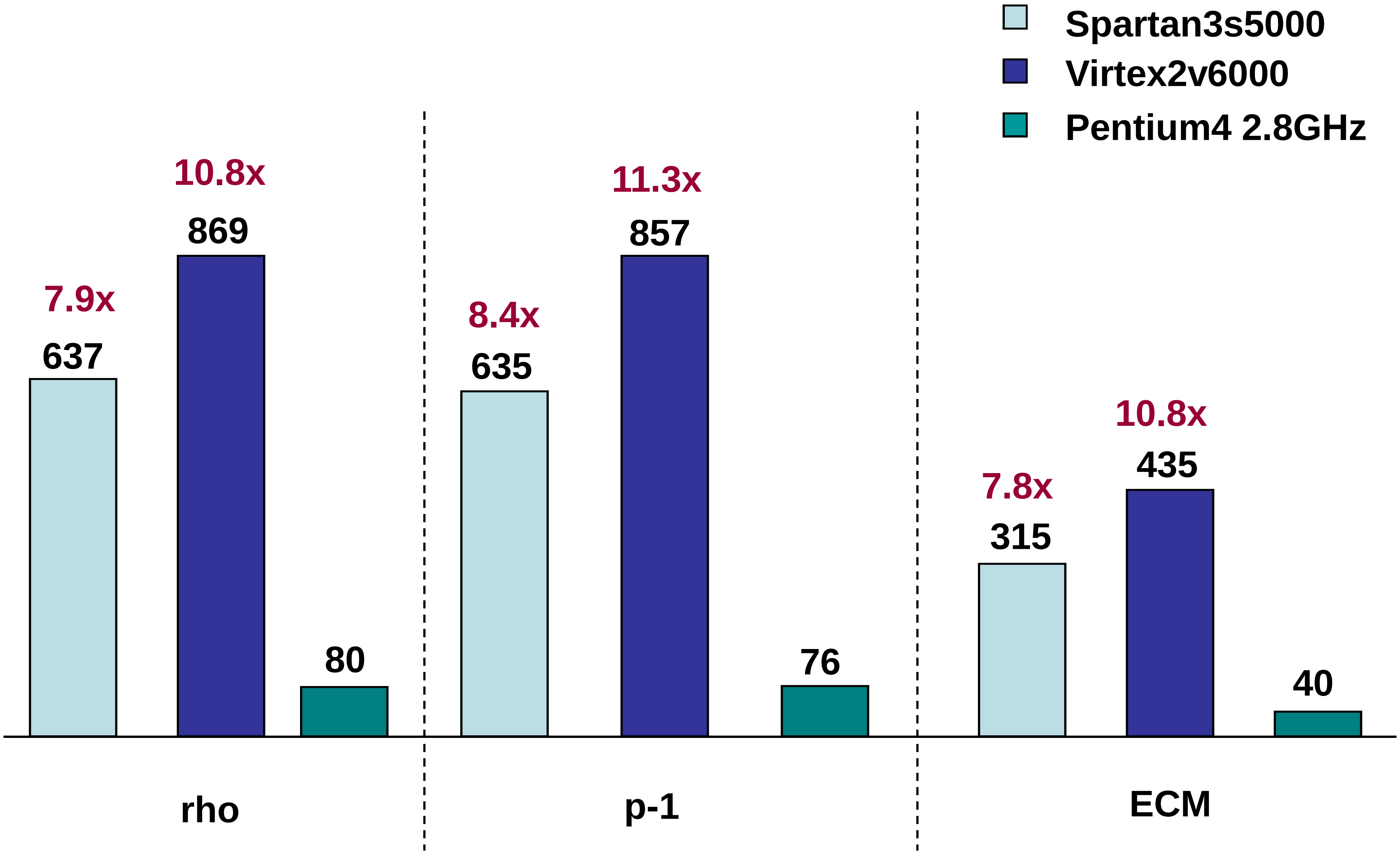
2 x Pentium Xeon 3 GHz

2 x Xilinx Virtex II FPGA
XC2V6000 running at 100 MHz

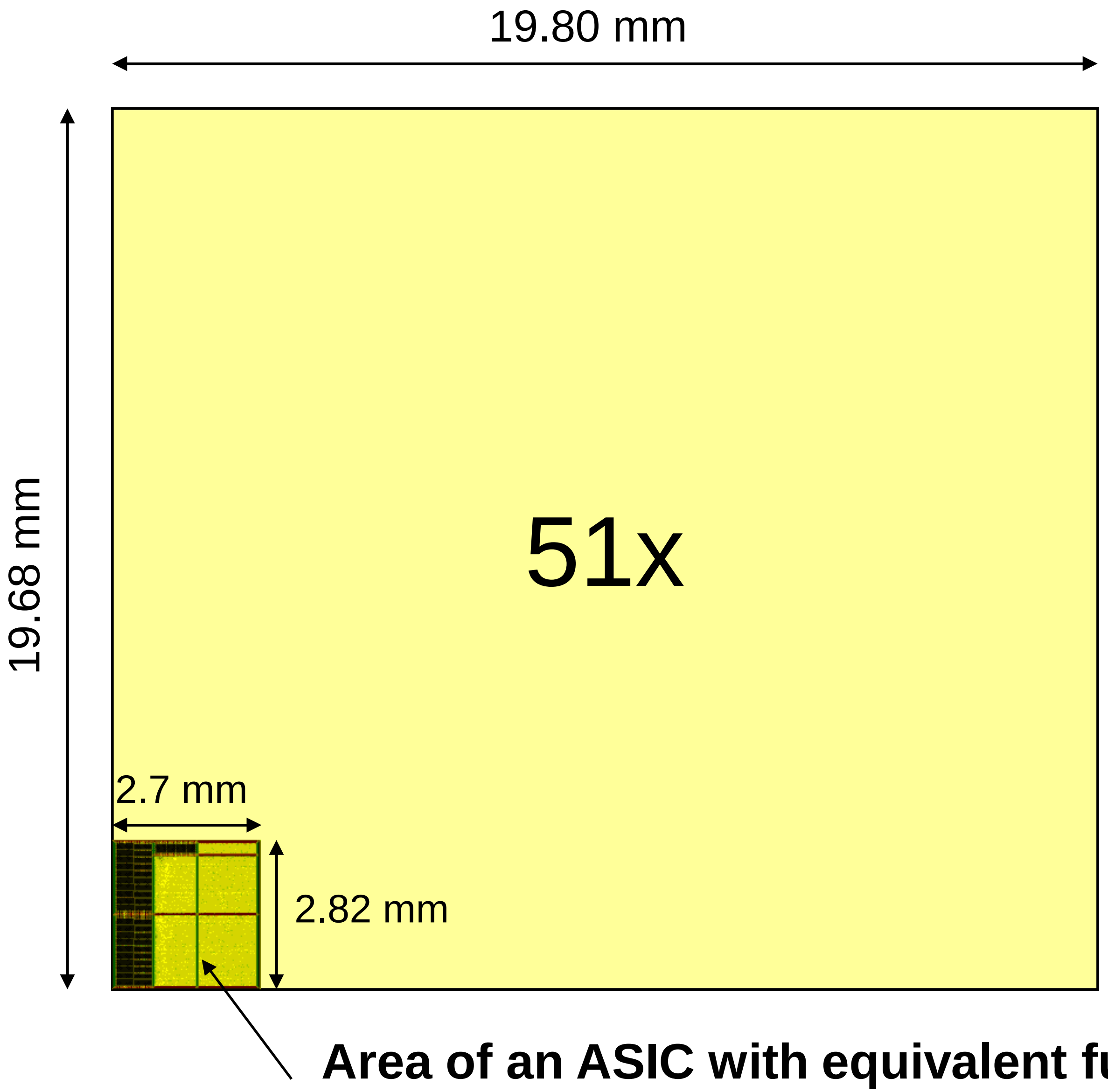
Fast communication interface between the microprocessor board and the FPGA board, 1600 MB/s

Multiple basic units can be connected using Hi-Bar Switch and
Global Common Memory

Factoring Runs per Second



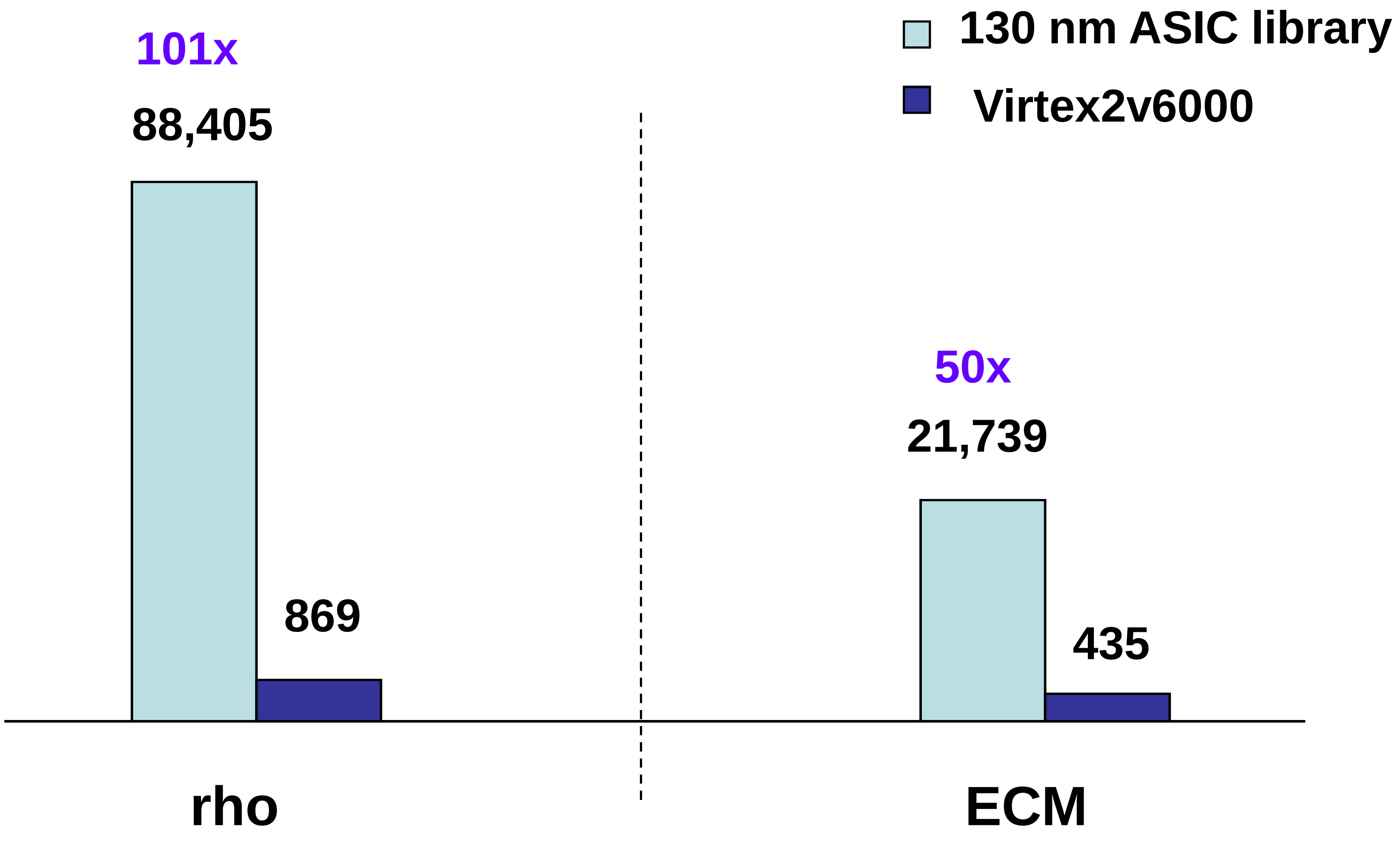
ASIC 130 nm vs. Virtex II 6000 – rho (24 units)



Area of Virtex II 6000
(estimation by R.J. Lim Fong,
MS Thesis, VPI, 2004)

Area of an ASIC with equivalent functionality

Number of rho & ECM computations per second using the same chip area


□ 130 nm ASIC library
■ Virtex2v6000
101x
50x
rho
ECM