Efektywność szyfrów strumieniowych w układach programowalnych

Marcin Rogawski

Plan referatu

- eSTREAM: 2004-2008,
- Implementacje sprzętowe finalistów eSTREAM,
- Porównanie wyników prac z ośrodkami naukowymi,
- Podsumowanie prac z lat 2004-2007,
- Podsumowanie,

eSTREAM

- http://www.ecrypt.eu.org/stream/
- 2 profile – sprzętowy i programowy,
- III faza (finał): 2007 kwiecień – 2008 marzec,
- implementacje w środowiskach z bardzo mała bateria zasilająca (np. RFID)
- implementacje przy ograniczonej ilości zasobów (np. Smard Card)
- implementacje w specyficznych architekturach (8-bit)
- implementacje w środowiskach o bardzo dużej przepustowości (wiele Gigabitów na sekundę)
- duża elastyczność implementacji: od bardzo małych i wolniejszych, po większe i bardzo szybkie,
- jakość specyfikacji – elegancja i prostota zapisu.

eSTREAM – profil sprzętowy

Achterbahn, Decim, Edon80, F-FCSR,

Grain, Hermes, LEX, MAG, MICKEY, Moustique,

NLS, Phelix, Polar Bear, Pomaranch,

Rabbit, Salsa20, Sfinks, SSS, TRBDK3 YAEA,

Trivium, TSC-3, Yamb, VEST, WG, Zk-Crypt

Pochodzenie algorytmów zgłoszonych do konkursu eSTREAM

Profil sprzętowy – po pierwszej fazie

Achterbahn, Decim, Edon80, F-FCSR,

Grain, Hermes, LEX, MAG, MICKEY, Moustique,

NLS, Phelix, Polar Bear, Pomaranch,

Rabbit, Salsa20, Sfinks, SSS, TRBDK3 YAEA,

Trivium, TSC-3, Yamb, VEST, WG, Zk-Crypt

SASC2007 – wyniki głosowania

Profil sprzętowy					
	Na pewno tak	**Raczej tak**	**Raczej nie**	**Zupełnie nie**	**punkty**
Grain	**39**	**7**	**1**	**2**	**1,63**
Trivium	**39**	**6**	**3**	**2**	**1,54**
Salsa20	20	12	7	2	1,00
Mickey128	18	7	8	5	0,66
Rabbit	11	13	11	6	0,29
F-FCSR	**5**	**16**	**10**	**3**	**0,29**
Lex	9	14	8	8	0,21
Phelix	11	11	10	8	0,18
Mickey	**11**	**9**	**7**	**10**	**0,11**
Edon80	**2**	**19**	**11**	**6**	**0,00**
Pomaranch	**3**	**12**	**12**	**10**	**-0,38**
Decim	**0**	**13**	**11**	**7**	**-0,39**
Moustique	**1**	**9**	**15**	**9**	**-0,65**
Vest	7	4	12	18	-0,73
WG	0	9	11	13	-0,85
ZK-Crypt	2	6	9	17	-0,97
NLS	0	8	10	16	-1,00
Polar Bear	0	6	10	15	-1,10
Hermes8	0	6	14	18	-1,16
TSC-4	0	6	7	19	-1,22
Achterbahn	1	2	8	35	-1,61

Finaliści eSTREAM – profil sprzętowy

Achterbahn, Decim, Edon80, F-FCSR,

Grain, Hermes, LEX, MAG, MICKEY, Moustique,

NLS, Phelix, Polar Bear, Pomaranch,

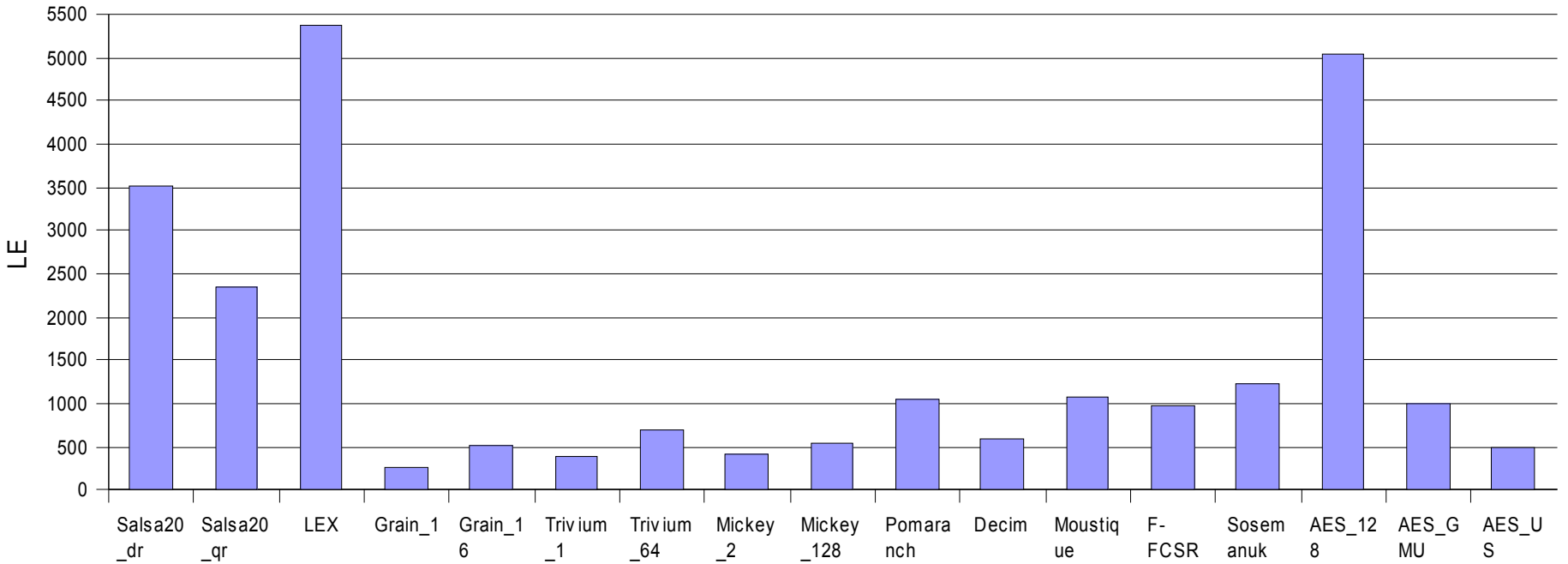
Rabbit, Salsa20, Sfinks, SSS, TRBDK3 YAEA,

Trivium, TSC-3, Yamb, VEST, WG, Zk-Crypt

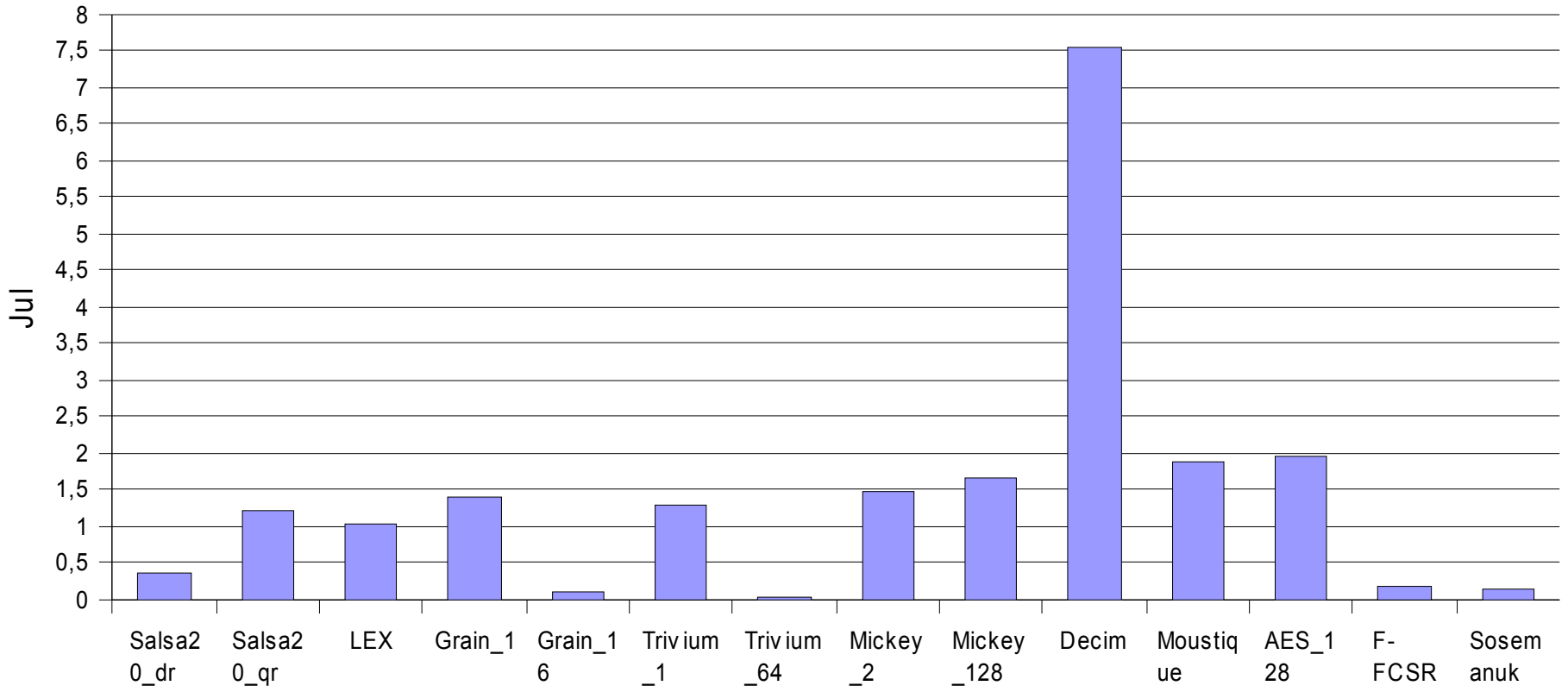
Założenia implementacyjne

- Architektura iteracyjna,
- Quartus II 6.0, Altera Cyclone EP1C12, AHDL (VHDL),
- Biblioteka funkcji,
- Standardowa logika,
- Bez metod autoryzacji,
- FSM: „one hot”
- Benchmark: *“Testing Framework for eSTREAM Profile II candidates”:*
- ***GMU**: ~1000LE, 174Mb/s*
- ***US**:~500LE, 2,2Mb/s*
- ***autorskie**: 5053LE, 611Mb/s*

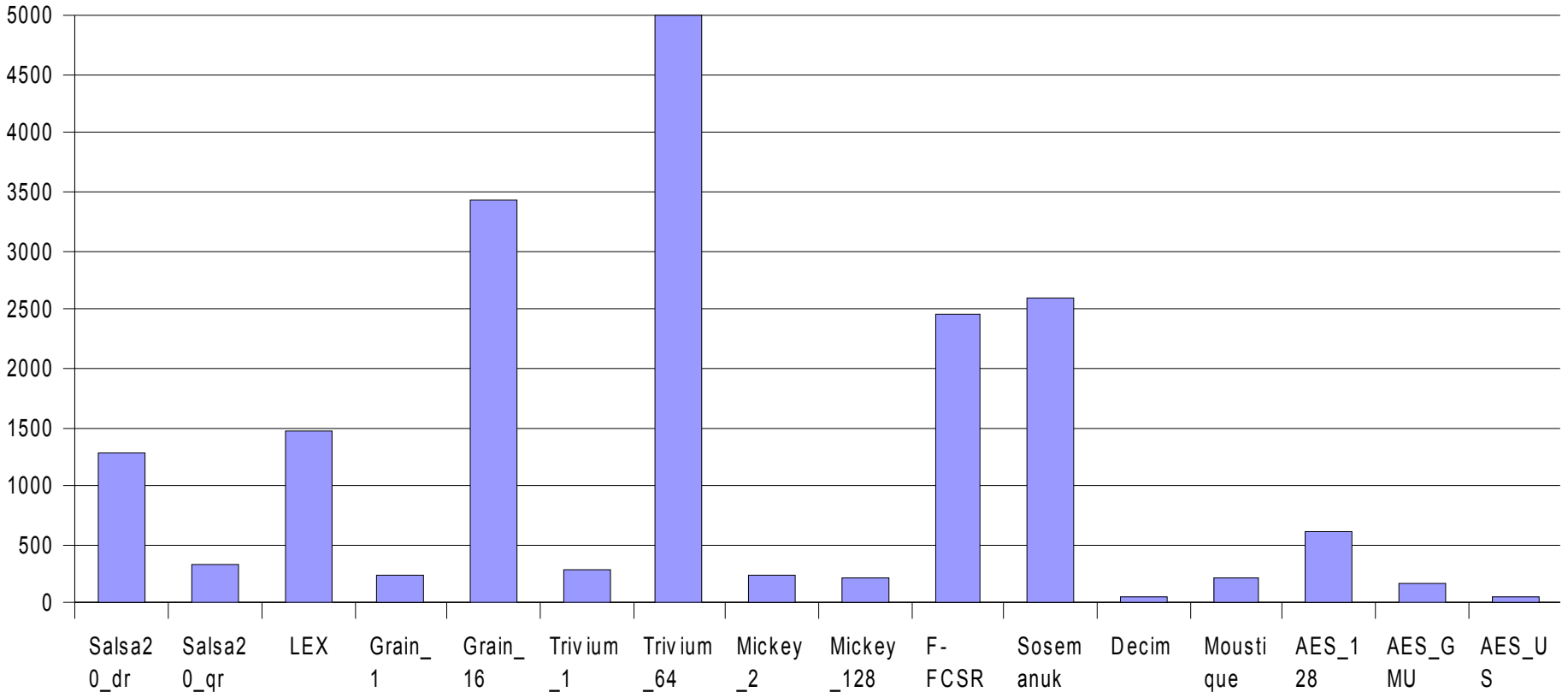
Wyniki implementacji - Zajętość struktury



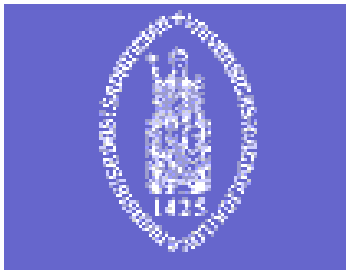
Energia do wygenerowania 1Gb strumienia klucza



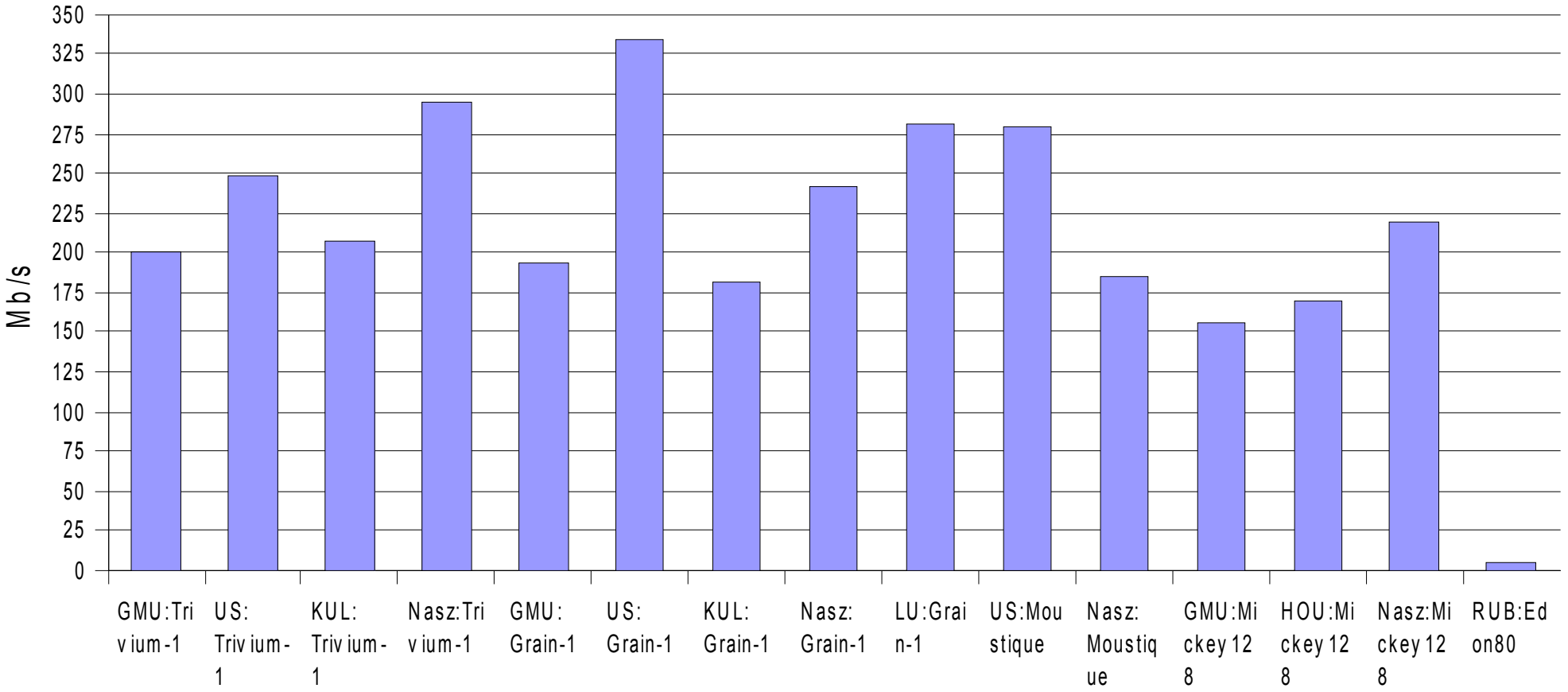
Przepustowość



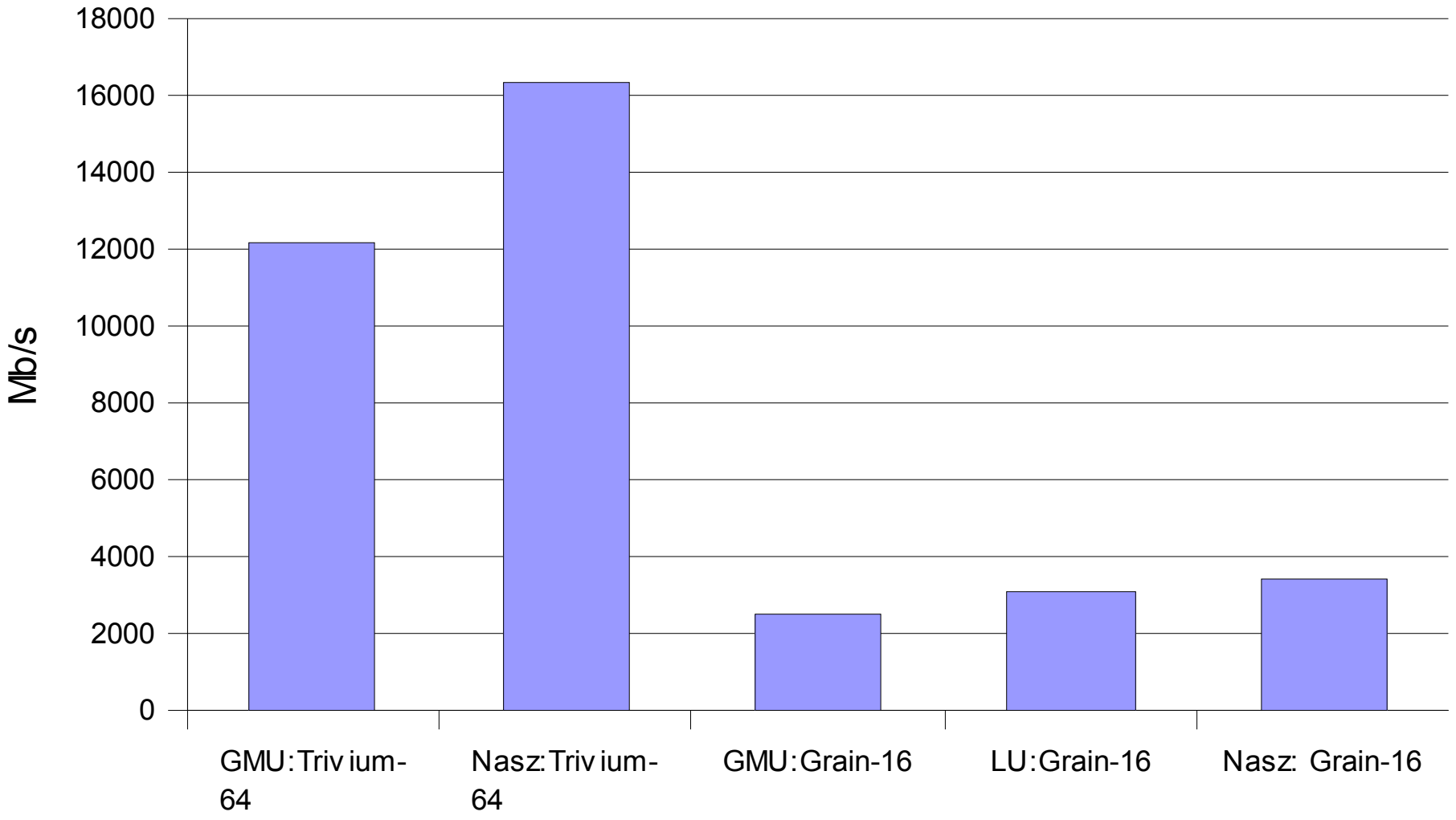
Oceny implementacji sprzętowych



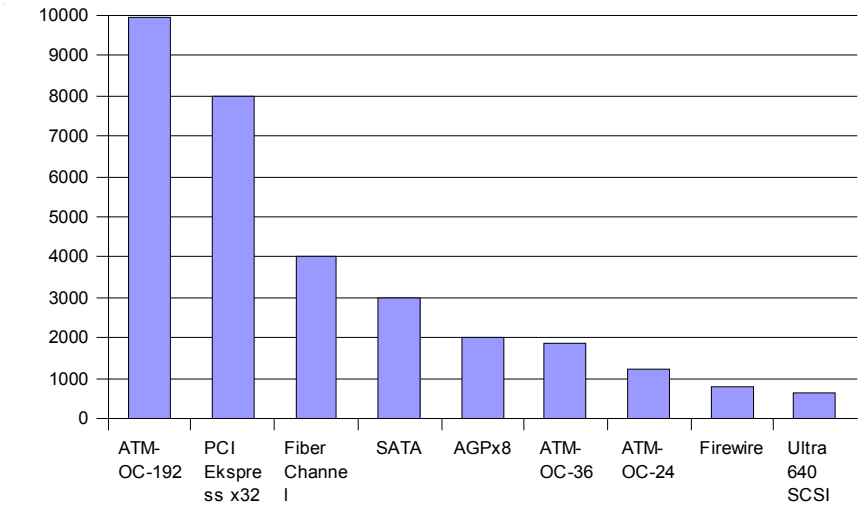
Wyniki implementacji różnych ośrodków naukowych – rozwiązania kompaktowe

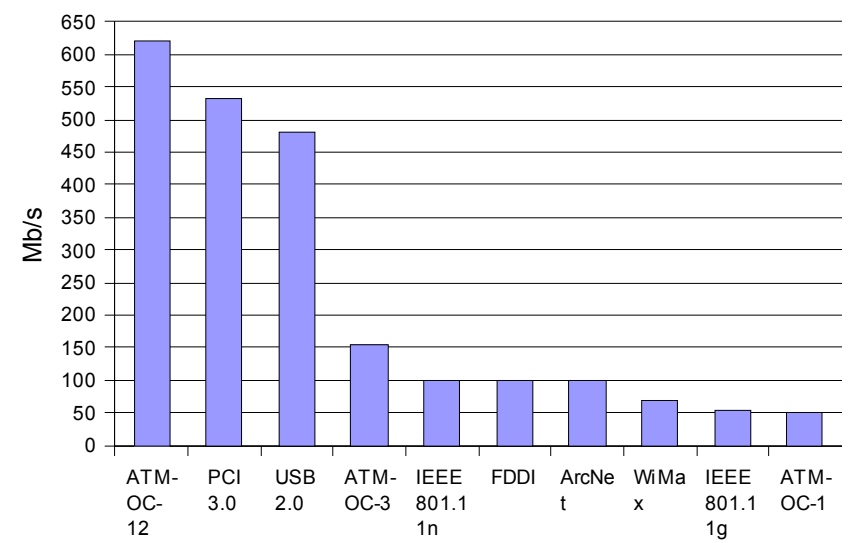


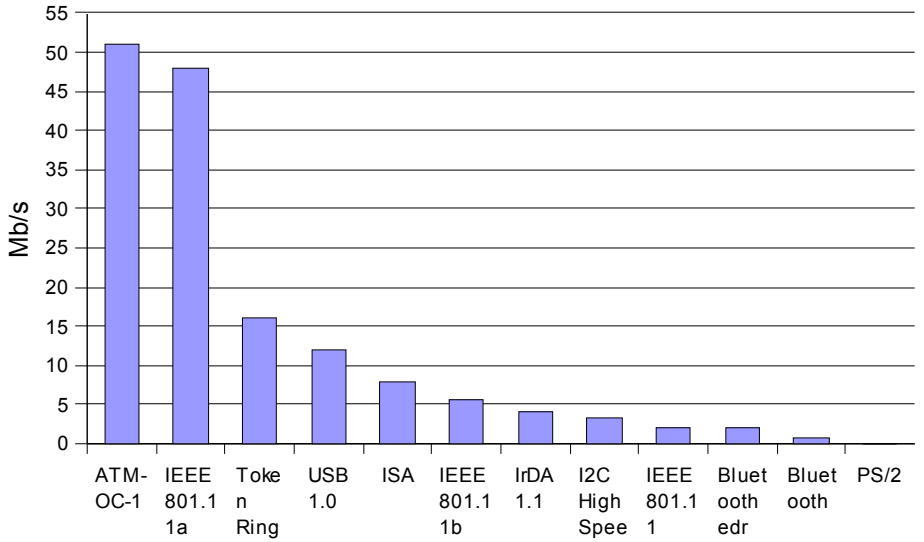
Wyniki implementacji różnych ośrodków naukowych – „szybkie”



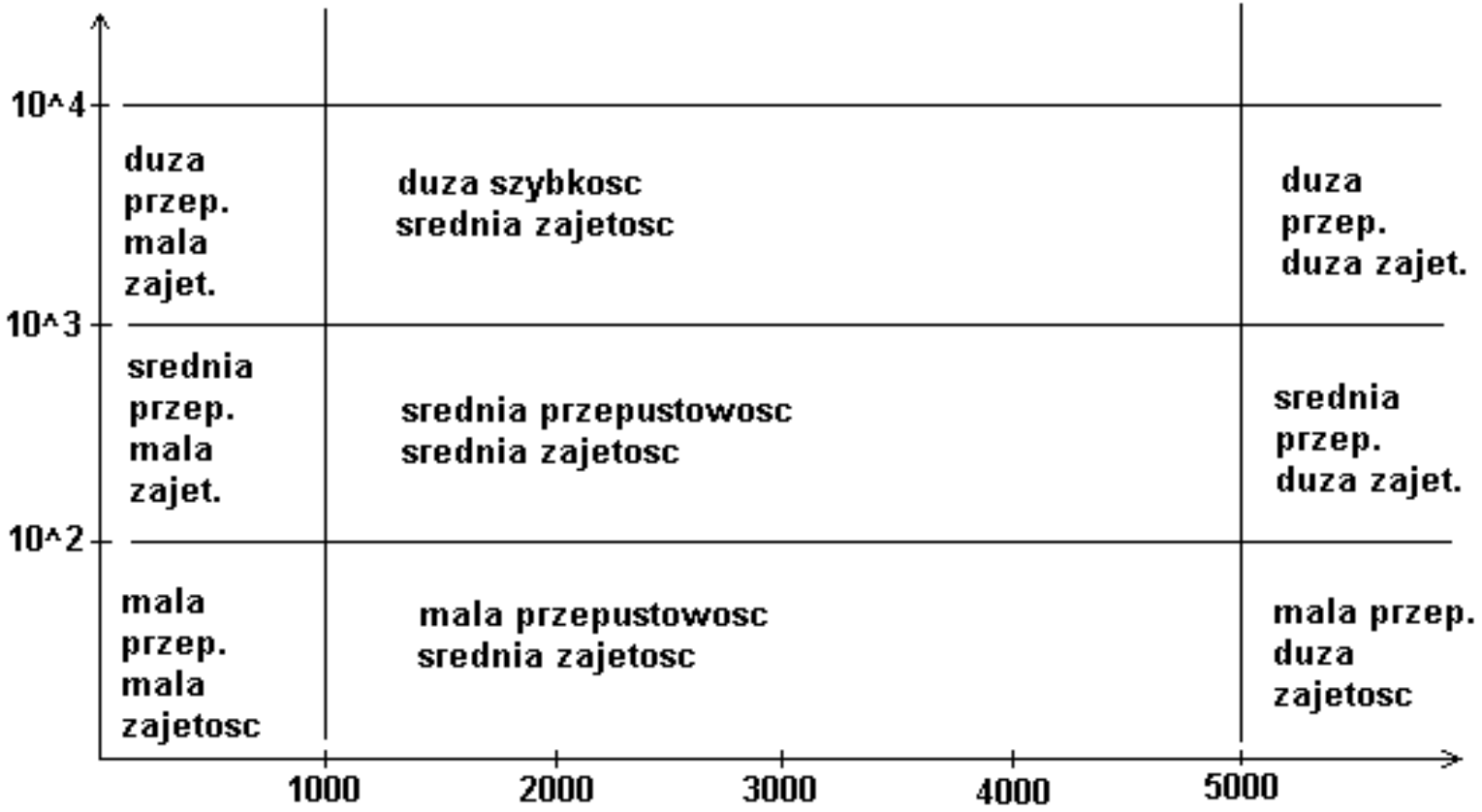
Technologie - przepustowości



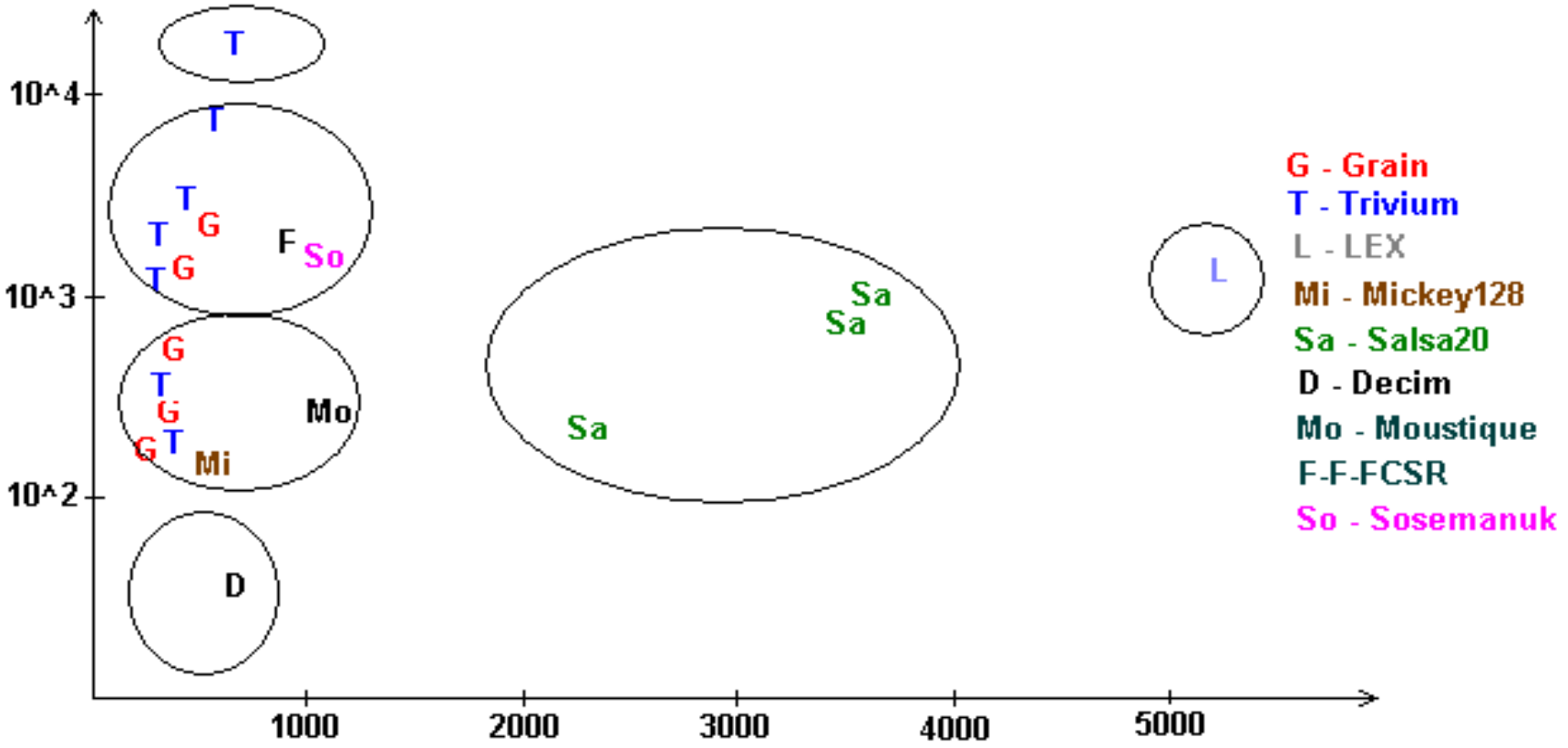




Implementacje - profile



eSTREAM - profile



Podsumowanie prac 2004-2007

- Enigma 2005: “Szyfry strumieniowe w układach programowalnych FPGA” {*A5, BGML, E0, Helix, Leviathan, Lili-128, Mir-1, Mugi, Rabbit, RC-4, Sober-t16, VMPC, W7, F8, AES OFB Mode*}
- Enigma 2006: “Sprzętowo-zorientowane konstrukcje szyfrów strumieniowych” {*A5, Grain, Trivium*}
- Enigma 2007: “Efektywność szyfrów strumieniowych w układach programowalnych” {*AES, Grain, LEX, Mickey, Salsa20, Trivium, Pomaranch, Moustique, F-FCSR Decim*}
- Zajętość: 1560LE (2005) -> 1425LE (2007),
- Przepustowość: 218Mb/s (2005) -> 2045Mb/s (2007),

Podsumowanie

- Zajętość – Grain,
- Pobór mocy – Trivium,
- Przepustowość - Trivium,
- Elastyczność – Trivium, Grain,
- wyniki potwierdzone na znanych uniwersytetach,
- eSTREAM – ogłoszenie wyników konkursu

Dziękuję za uwagę ...