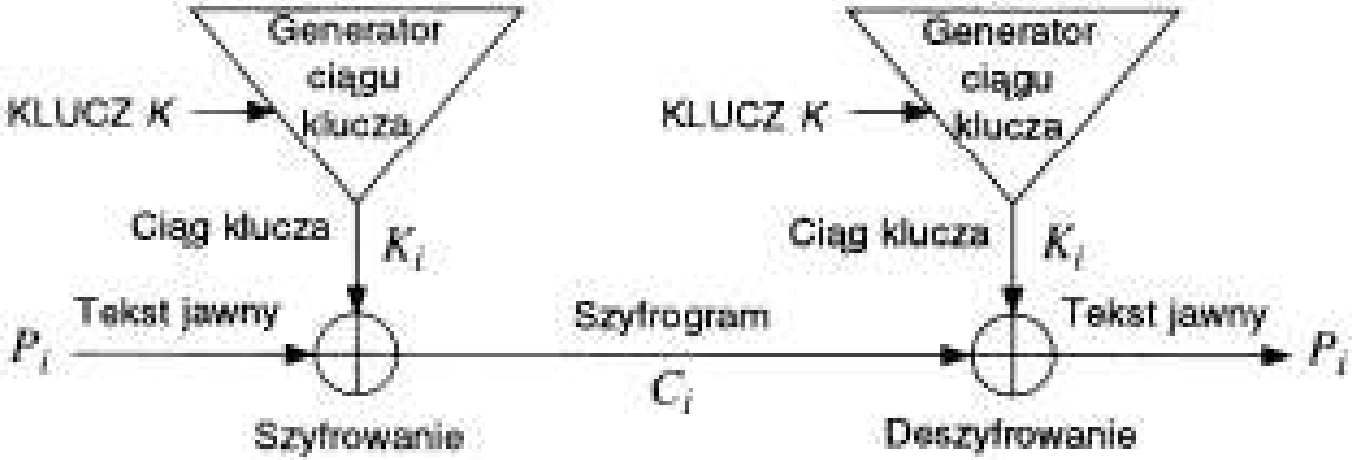
Szyfry strumieniowe w układach programowalnych FPGA

Marcin Rogawski
rogawskim@prokom.pl

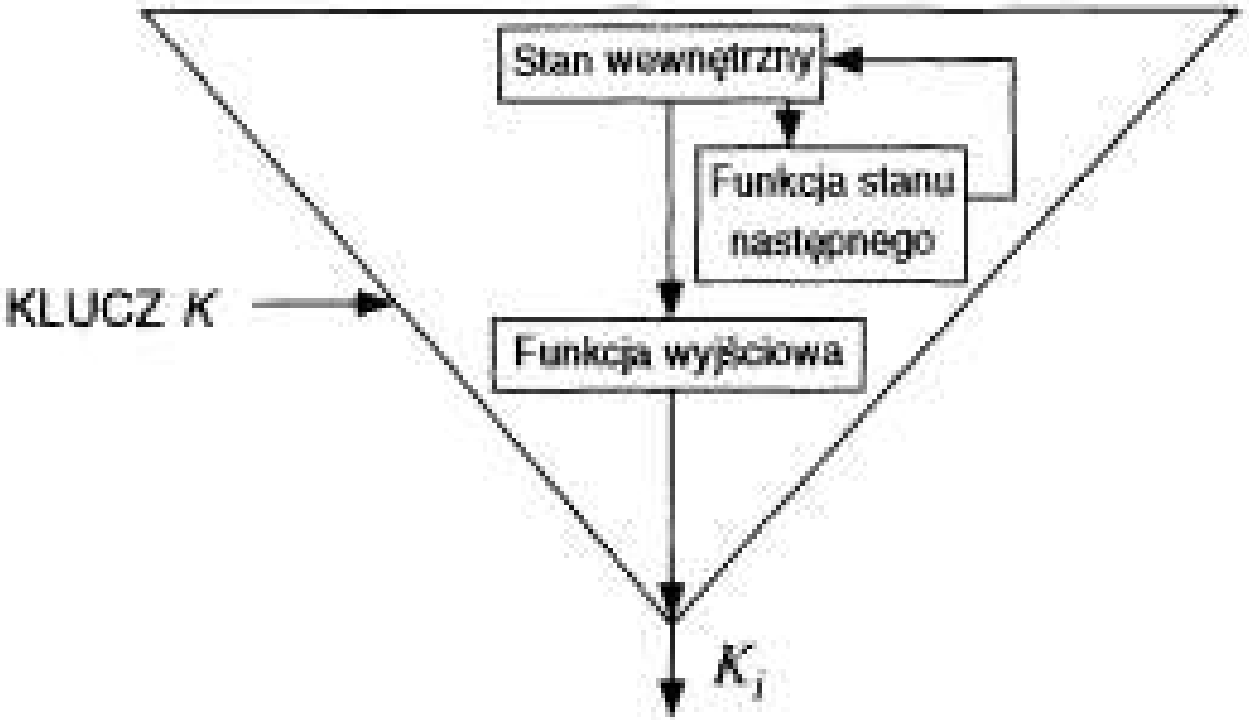
Plan referatu

- Szyfry strumieniowe,
- Wybór tematu,
- Struktury programowalne – element fizyczny,
- Architektury akceleratorów kryptograficznych – element logiczny,
- Szyfry strumieniowe – implementacje w FPGA,
- Podsumowanie.

Szyfry strumieniowe



Szyfry strumieniowe



Wybór tematu

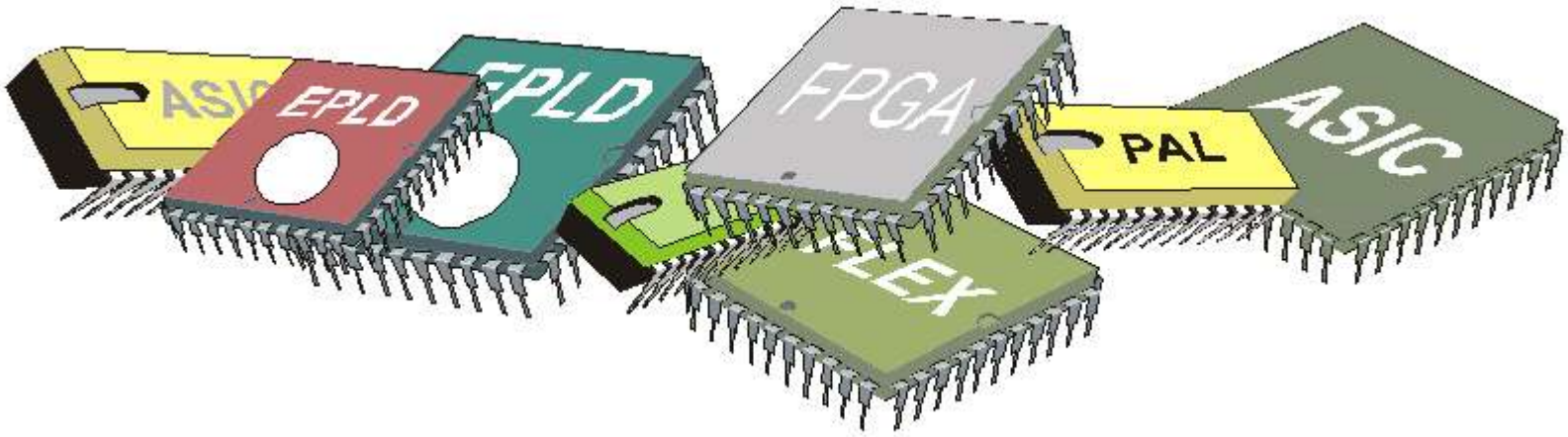
- Konkurs AES,
- Konkurs NESSIE,
- Szyfry strumieniowe – „art of state”,
- Zastosowanie szyfrów strumieniowych,
- Układy FPGA.

Akceleratory kryptograficzne w FPGA

- Założenia funkcjonalne,
- Założenia wydajnościowe,
- Cena układu,
- Współpraca z innymi układami scalonymi.

Układy programowalne – warstwa fizyczna

- Zasoby:
  - liczba wyprowadzeń;
  - bloki logiczne;
  - bloki pamięci wbudowanej;
  - bloki DSP;



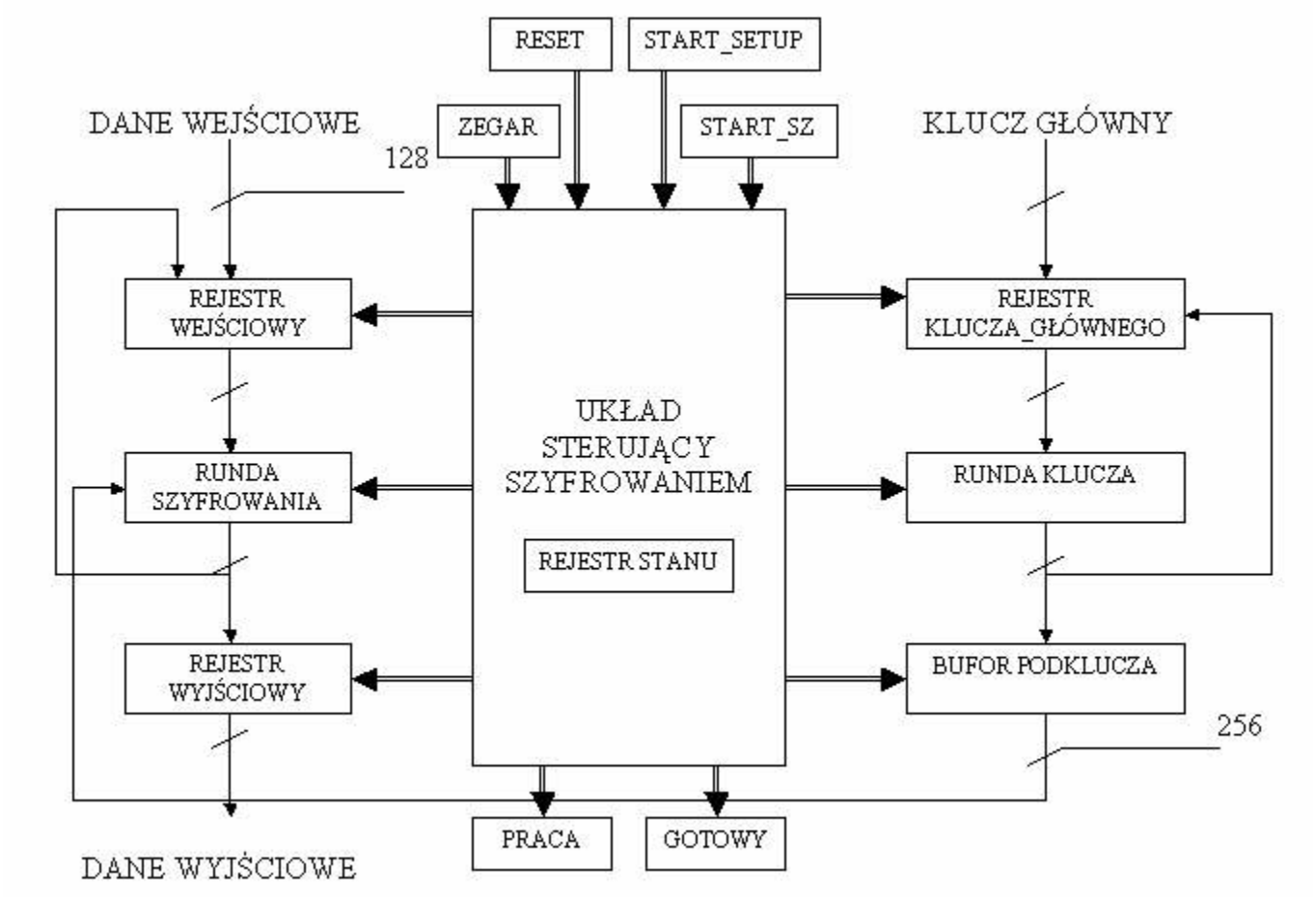
Cykl rozkazowy

- Pobranie instrukcji,
- Dekodowanie instrukcji,
- Pobranie argumentów,
- Wykonanie operacji,
- Zapis wyniku.

Architektury modułów kryptograficznych – warstwa logiczna

- Architektura ITERACYJNA (L);
- Architektura KOMBINACYJNA (U);
- Architektura POTOKOWA (P);
- Architektura HYBRYDOWA (…);

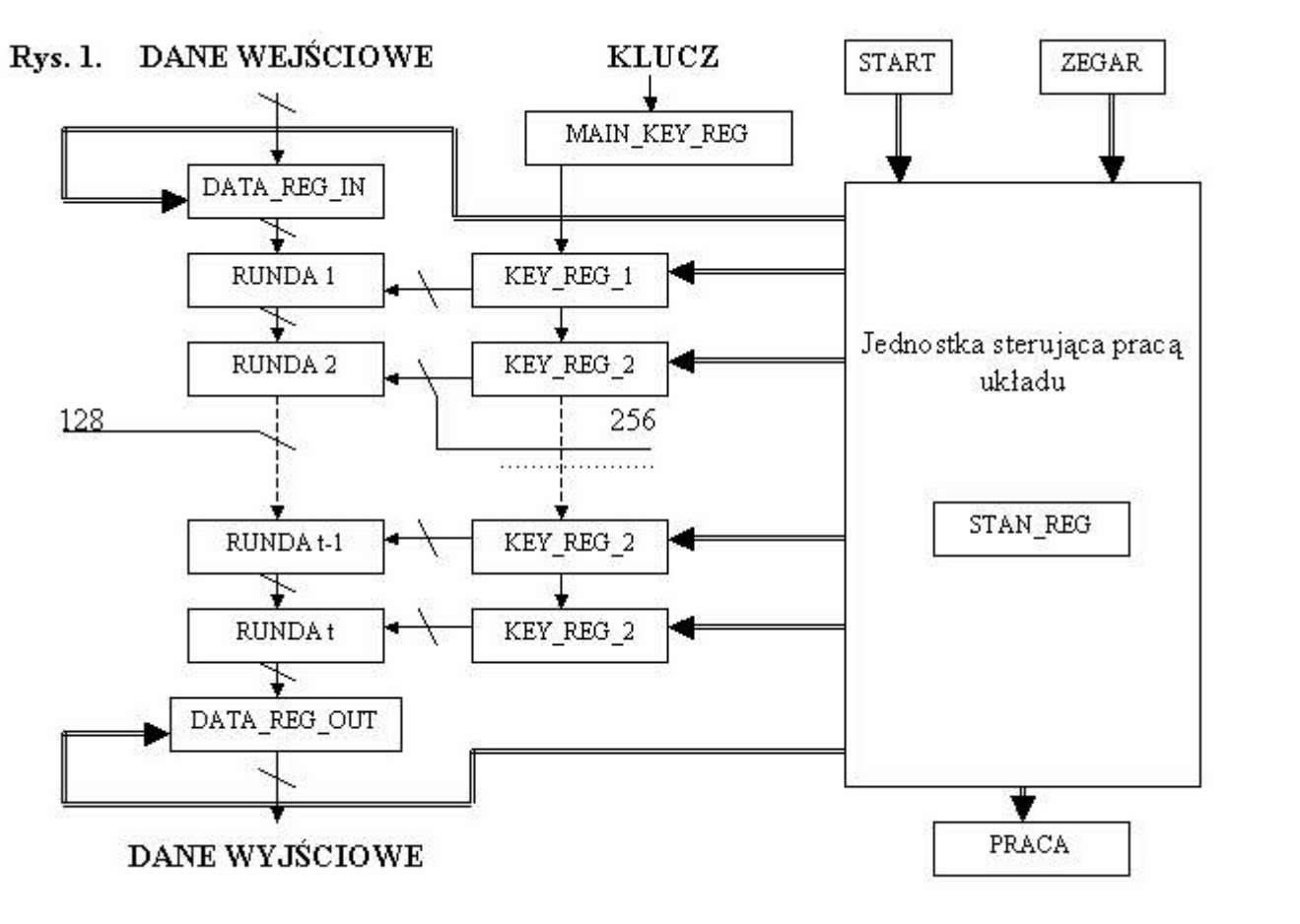
Architektura ITERACYJNA



Architektura ITERACYJNA

- Naturalna dla algorytmów kryptograficznych;
- Duża efektywność;
- Możliwość realizacji pełnej funkcjonalności algorytmu (różne tryby pracy);
- Najmniejsza przepustowość;

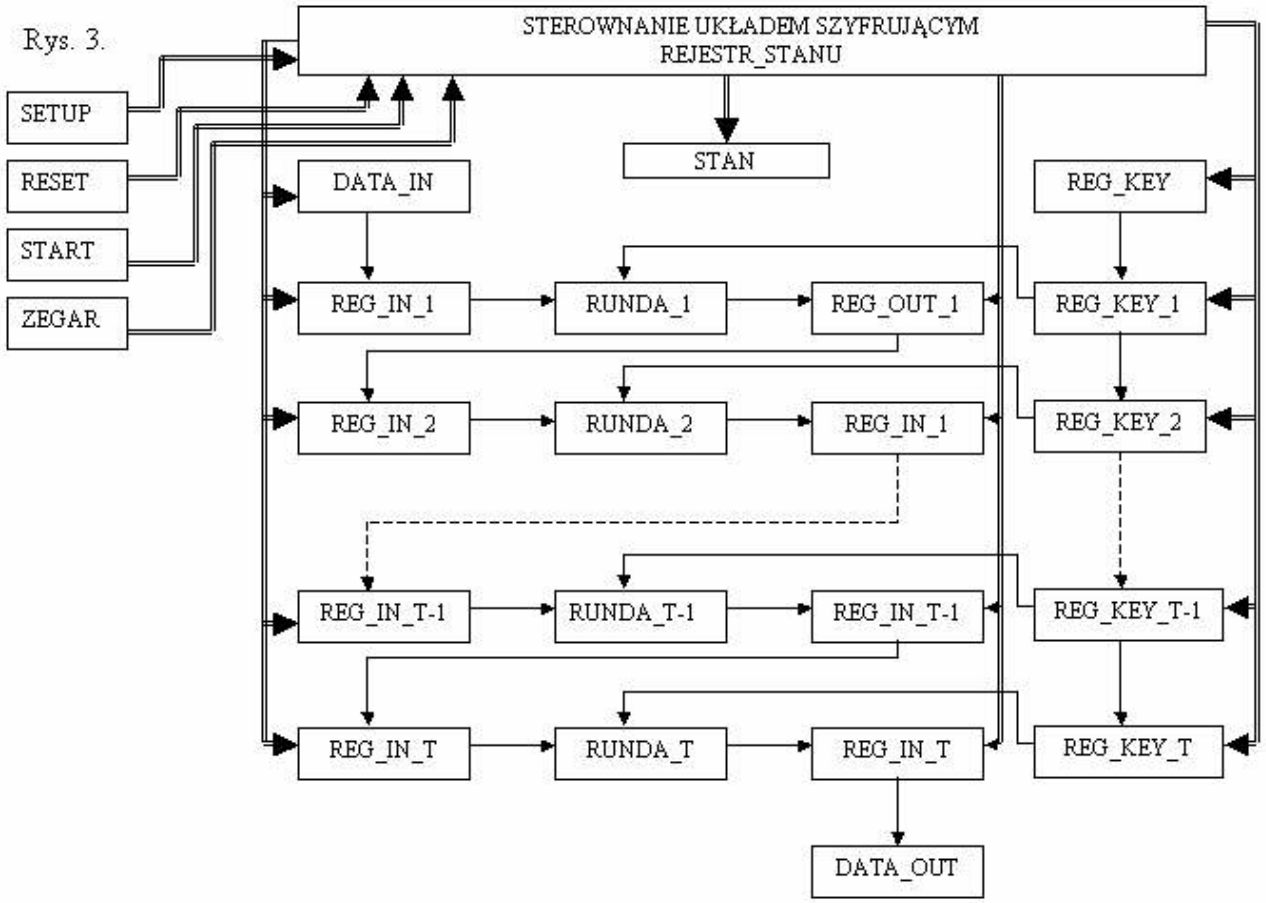
Architektura KOMBINACYJNA



Architektura KOMBINACYJNA

- realizacja podstawowej operacji algorytmu w ciągu jednego taktu zegarowego;
- niska efektywność;
- układ sterujący – nieskomplikowany;
- ograniczona możliwość realizacji większości algorytmów kryptograficznych

Architektura POTOKOWA



Architektura POTOKOWA

- Natura procesorów o potokowej architekturze;
- Duża efektywność;
- Największa szybkość przetwarzania;
- Możliwość realizacji każdego algorytmu blokowego;
- WADA: architektura tylko dla ECB;
- WADA: brak wsparcia dla funkcji skrótu, szyfrów strumieniowych

Algorytmy kryptograficzne i Architektury

	Algorytmy blokowe	Algorytmy strumieniowe	Funkcje skrótu
architektura interacyjna	Każdy algorytm	Każdy algorytm	Każdy algorytm
architektura kombinacyjna	Każdy algorytm, ale czasami niezbędny jest Key Setup	Większość algorytmów, z którymi się zetknął autor można zrealizować używając tej architektury	Większość algorytmów, z którymi się zetknął autor można zrealizować używając tej architektury
architektura potokowa	Praca w trybie ECB, lub prostym licznikowym	____	____
architektura hybrydowa	Dowolne kombinacje	Kombinacyjno-iteracyjne	Kombinacyjno-iteracyjne

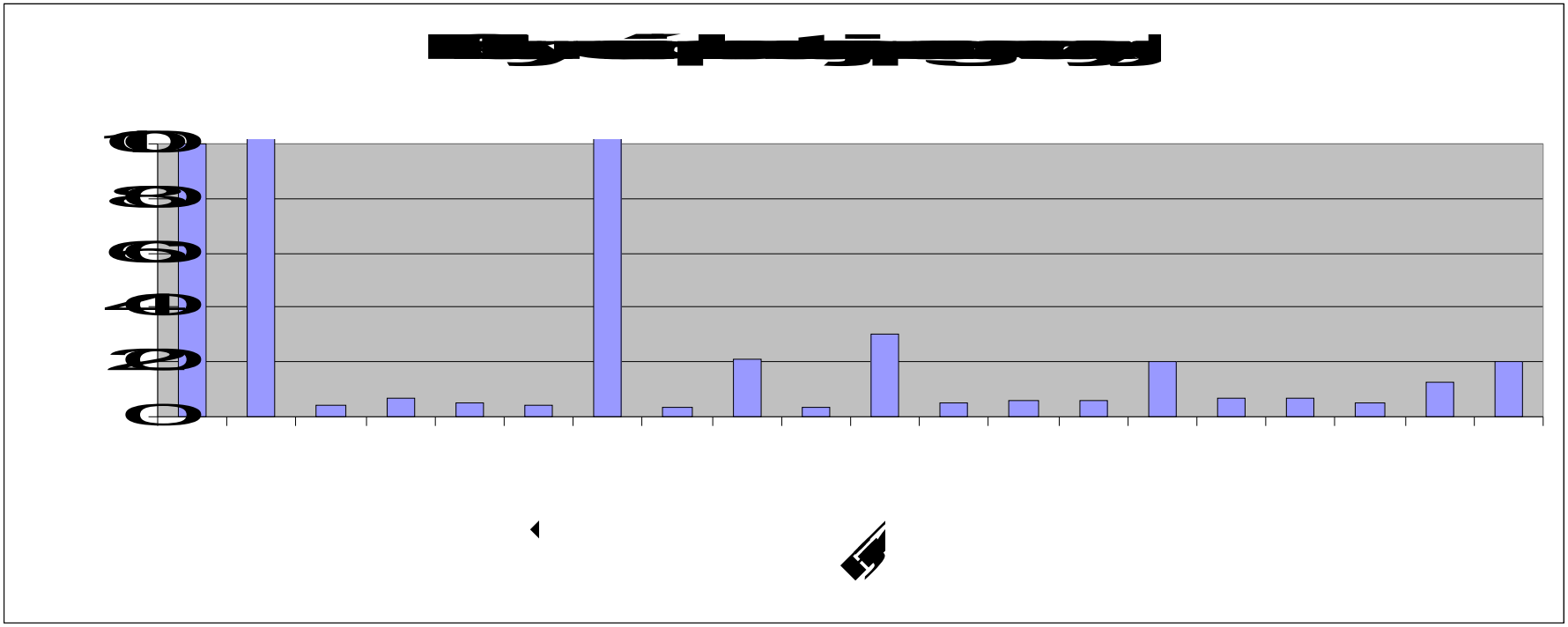
Wybrane szyfry strumieniowe

- A5,
- BGML (Hastad J., Naslund M.- Szwecja),
- E0,
- Helix (Schneier B. - USA),
- Leviathan (Cisco Systems - USA),
- Lili-128 (Queensland University of Technology, Golic J. Australia/Serbia),
- Mir-1 (Alexander Maximov - Rosja),
- Mugi (Hitachi),
- Rabbit (Cryptico A/S - Dania),
- RC4 (Rivest R. - USA),
- Sober-t16 (Qualcomm - Australia),
- VMPC (Żółtak B. - Polska),
- W7 (Wave7 Optics, Anagram Laboratories, University of Waterloo -- Belgia),
- F8 (Matsui M. - Japonia),
- Rijnadael – OFB (J.Deamen, V.Rijmen - Belgia).

Dalsze badania …

- HC-256,
- Henkos,
- ISAAC,
- Panama,
- Seal,
- Scream,
- Snow,
- Turing,
- Wake.

Wyniki implementacji programowych



Założenia implementacyjne

- Układ Flex 10KE,
- AHDL,
- Wybrane szyfry – wersja podstawowa,
- Biblioteka funkcji,
- Największa szybkość,

Przepustowość

$$\frac{\text{(długość słowa)}}{\text{(ilość cykli) * (czas trwania cyklu)}}$$

Długość słowa / stan wewnętrzny

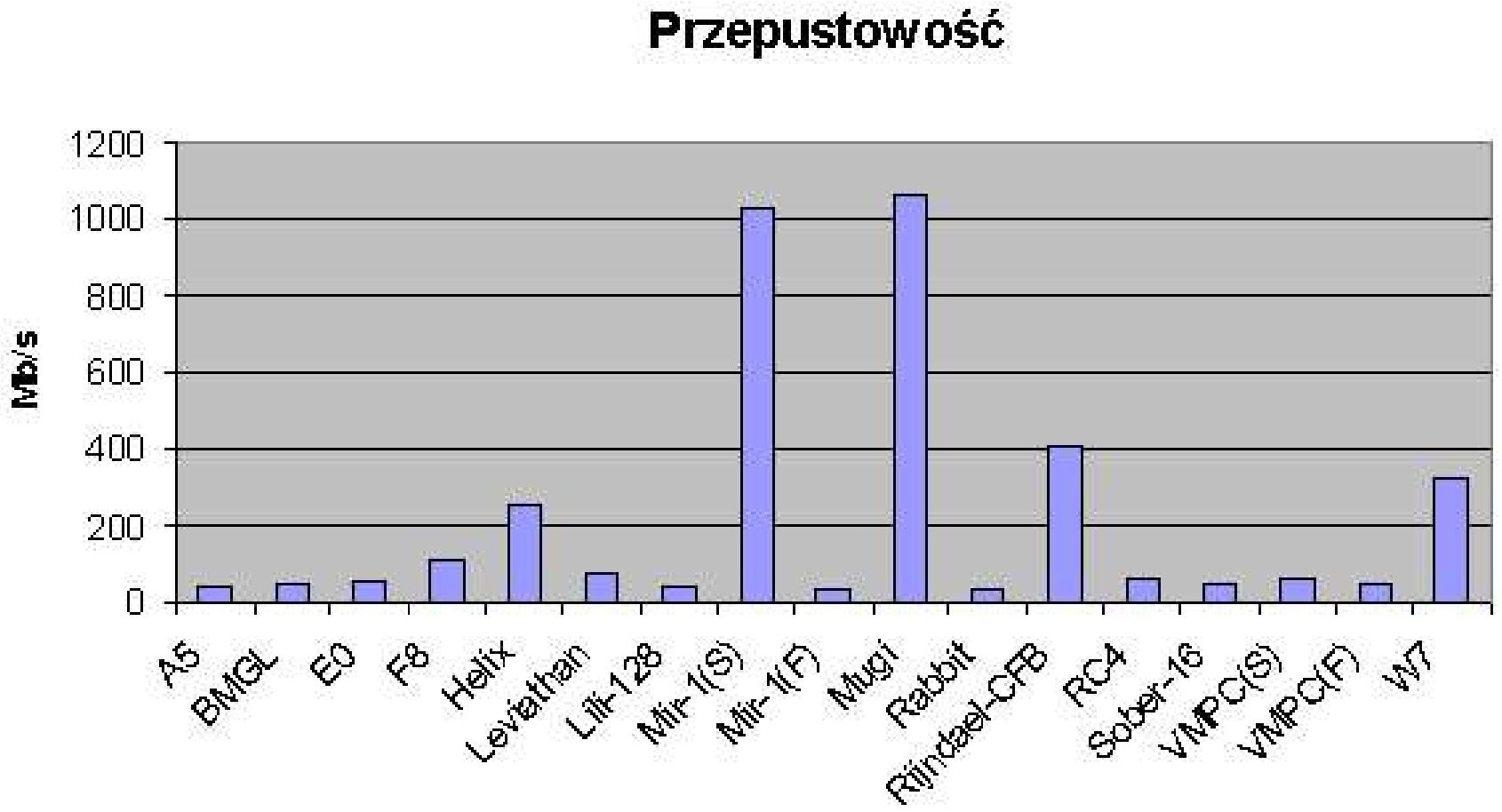
algorytm strumieniowy	długość strumienia klucza	wielkość stanu wewnętrzngo
A5	1	64
BMGL	16	17*128 (2176)
E0	1	128+2 (130)
Helix	32	128
Leviathan	32	128
Lili-128	1	128
Mir-1	64	2*64 + 4*64 (384)
Mugi	64	3*64 + 16*64 (1216)
Rabbit	128	8*32+8*32+1 (513)
RC4	8	(8*256) 2048
Sober-16	8	128
VMPC	8	(8*256) 2048
W7	8	8*128
F8	64	128
Rijndael – OFB	128	128

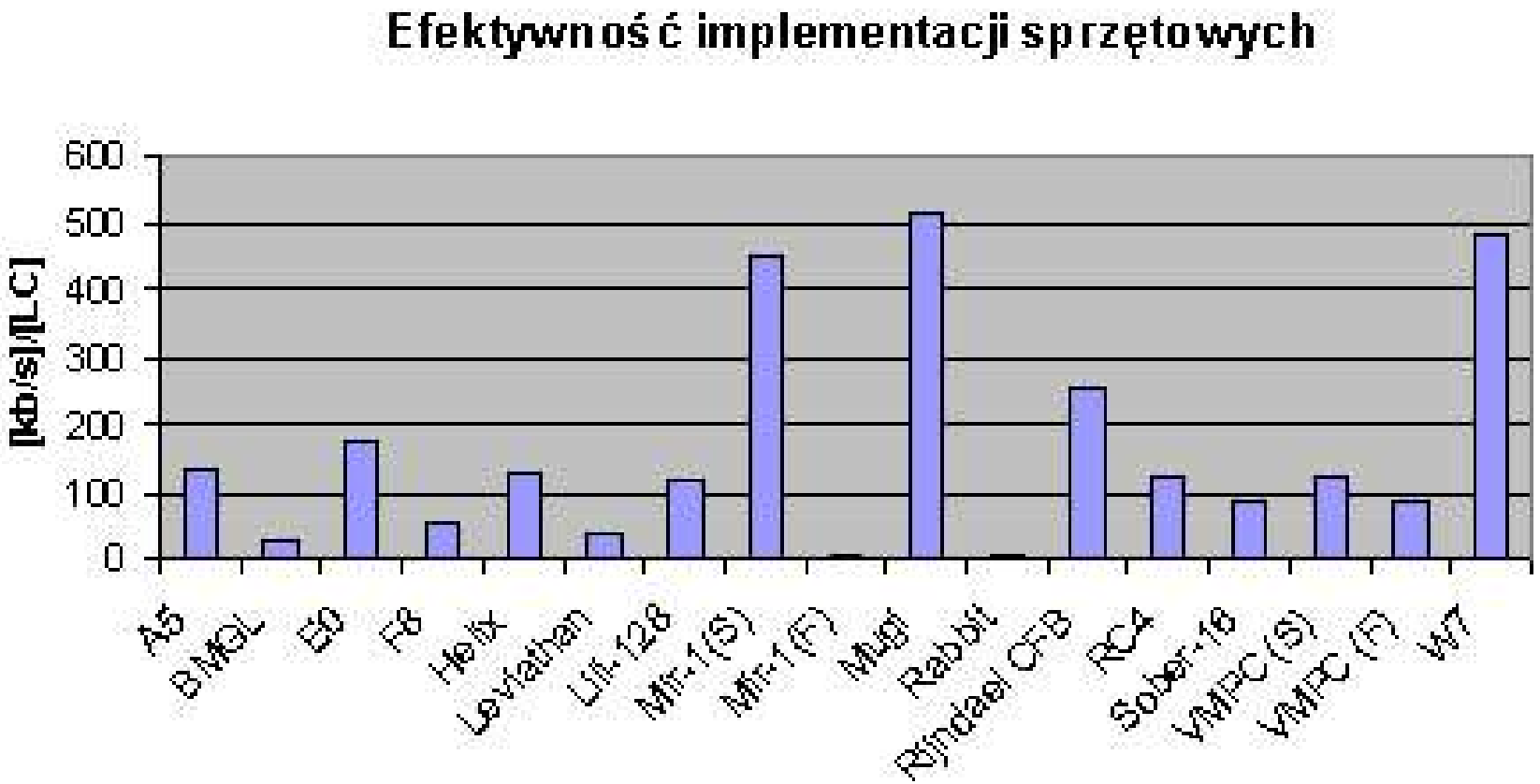
Operacje składowe

	operacje arytmetyczne	operacje logiczne	Przesunięcia	LFSR	Podstawienia sbox	tablice	Mnożenie przez macierz
	* / +	and / or	shift / rot	reg./niereg.			
A5	- / -	- / -	- / -	- / t	-	-	-
BMGL	t / -	- / -	t / -	- / -	t	-	t
E0	- / t	- / -	t / -	t / -	-	-	-
Helix	- / t	- / -	t / -	- / -	-	-	-
Leviathan	- / t	- / -	- / -	- / -	t	-	-
Lili-128	- / -	- / -	- / -	- / t	t	-	-
Mir-1	t / t	t / t	t / -	- / -	t	-	-
Mugi	- / -	- / -	- / t	- /-	t	-	t
Rabbit	t / t	- / -	t / t	- / -	-	-	-
Rc4	- / t	- / -	- / -	- / -	-	t	-
Sober-t16	- / t	t / -	- / -	- / t	-	-	-
VMPC	- / t	- / -	- / -	- / -	-	t	-
W7	- / -	t / t	- / -	- / t	-	-	-
F8	- / -	t / t	- / -	-/ -	t	-	-
Rijndael - OFB	- / -	- / -	t / t	- / -	t	-	t

Wyniki implementacji - FPGA

	Częstotliwość max.	Zajętość struktury	Przepustowość / zajętość	Przepustowość
	[Mhz]	[LC/mem. bits]	[kb/LC]	[Mb/s]
A5	158,7	299	132,7	39,7
BMGL	166,7	1620 / 40960	26,6	43,1
E0	250	280	178,8	50,0
F8	50	2031	54,3	110,3
Helix	65	2003	126,9	254,2
Leviathan	35	1978	37,9	75,0
Lili-128	204,8	339	114,7	38,9
Mir-1	37,3	4521 / 49152	8,1	36,73
Mir-1 (S)	32	2,294 / 49152 / 96	449,8	1032
Mugi	33,3	2075 / 32768	513,7	1066
Rabbit	16,7	4809	7,4	35,6
Rijndael OFB	90	1610 / 40960	254,7	410,0
RC4	70,4	459 / 4096	122,7	56,3
Sober-16	25,18	525	85,3	44,8
VMPC	71,9	514 / 12228	86,3	44,4
VMPC (S)	100,0	498/ 12228	124,0	61,75
W7	161,3	674	478,6	322,6


Przepustowość
Mb/s
1200
1000
800
600
400
200
0
A5
BMGL
E0
F8
Helix
Leviathan
Lili-128
Mir-1(S)
Mir-1(F)
Mugi
Rabbit
Rijndael-CFB
RC4
Sober-16
VMPC(S)
VMPC(F)
W7


Efektywność implementacji sprzętowych
[Mb/s]/[LC]
600
500
400
300
200
100
0
A5
BMGL
E0
F8
Helix
Leviathan
Lili-128
Mir-1(S)
Mir-1(F)
Mugi
Rabbit
Rijndael CFB
RC4
Sober-16
VMPC(S)
VMPC (F)
W7

Podsumowanie

- Implementacje sprzętowe a algorytmy kryptograficzne,
- Elastyczność rozwiązań,
- Rozwój szyfrów strumieniowych,
- Rozwój technologii,
- Wyniki prac ECRYPT.

Dziekuję za uwagę.

rogawskim@prokom.pl