Efektywna implementacja algorytmu kryptograficznego SERPENT w układach programowalnych

Marcin Wójcik

pod opieką dr inż. Mariusza Rawskiego

Spis treści

Cel pracy

- zbadanie możliwości implementacji algorytmu kryptograficznego Serpent w najnowszych układach programowalnych
- zbadanie możliwości zastosowania algorytmu w konfiguracji z równoległą generacją kluczy rundowych

Konkurs AES

- NIST (Narodowy Instytut Standardów i Technologii, 1997)
- Warunki konkursu *AES*
  - symetryczny szyfr blokowy
  - długość klucza 128, 192, 256 bitów
  - długość bloku 128 bitów
  - jawny
  - bez praw autorskich
- Finaliści :

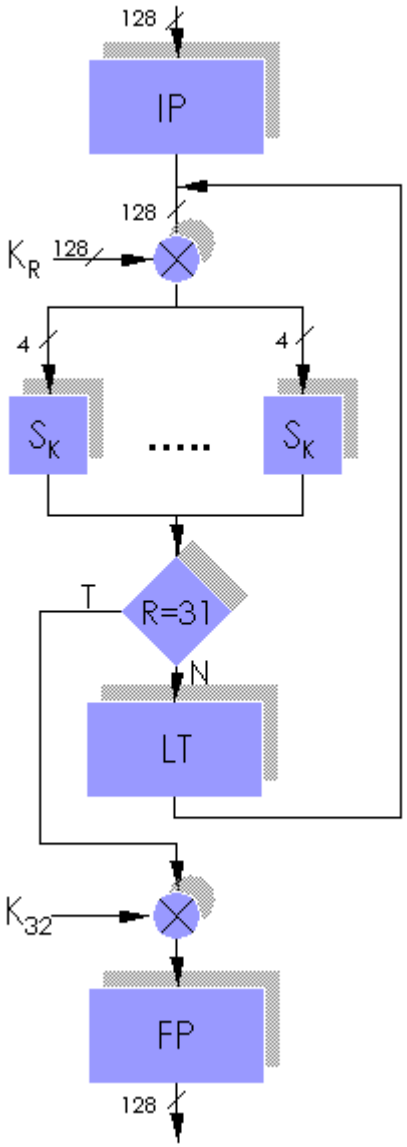
  Rijndael (86), *Serpent* (59), *Twofish* (31), *RC6* (23), *Mars* (13)

Bezpieczeństwo

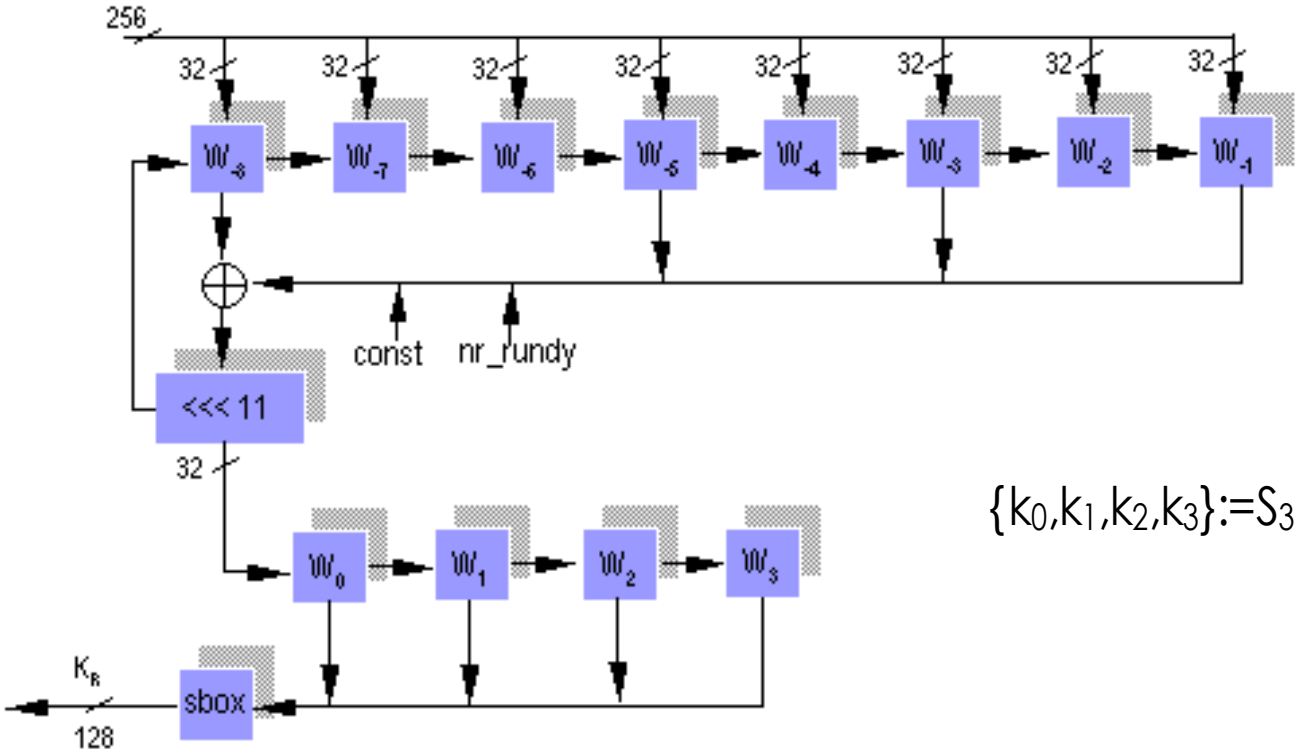
- *Serpent* (Ross Anderson, Eli Biham, Lars Knudsen)
  - sieć permutacyjno-podstawieniowa (SP-network)
  - skrzynki podstawieniowe (*s-box*) bazujące na skrzynkach podstawieniowych algorytmu DES
  - klucz - 128, 192, 256 bitów
  - wektor danych - 128 bitów
  - 32 rundy
  - brak słabych kluczy

Budowa

- permutacja początkowa IP
- 32 rundy
  - maskowanie klucza
  - przejście przez skrzynki podstawieniowe
  - przekształcenie liniowe
    (we wszystkich rundach poza ostatnią)
  - w ostatniej rundzie maskowanie klucza
- permutacja końcowa FP



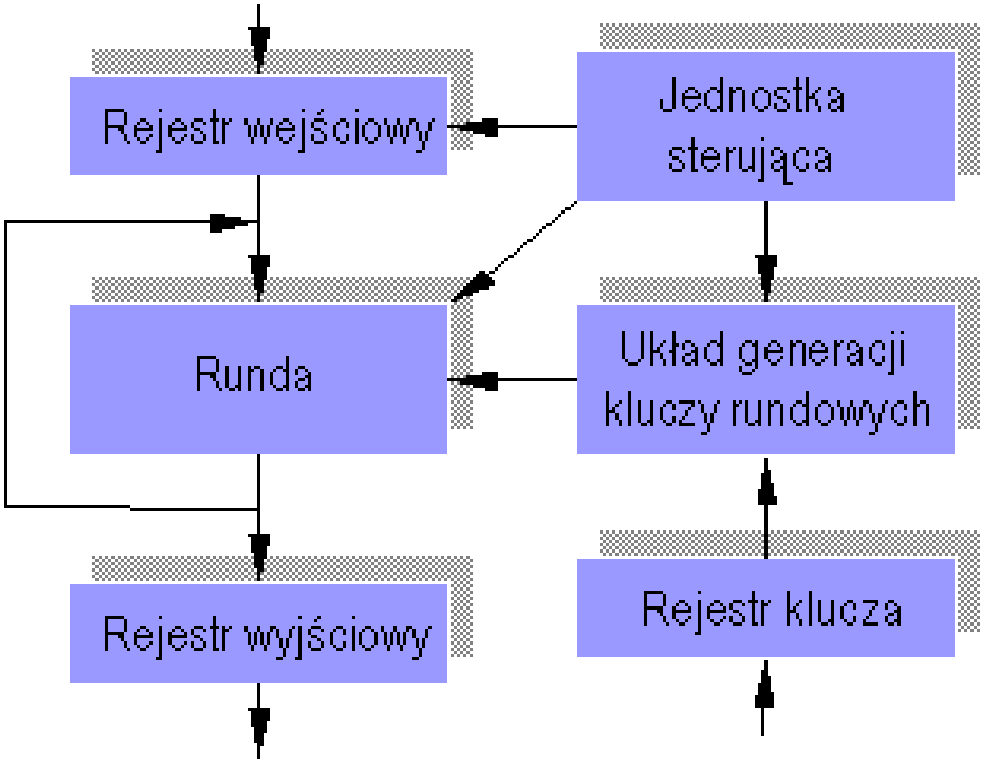
Generacja kluczy rundowych



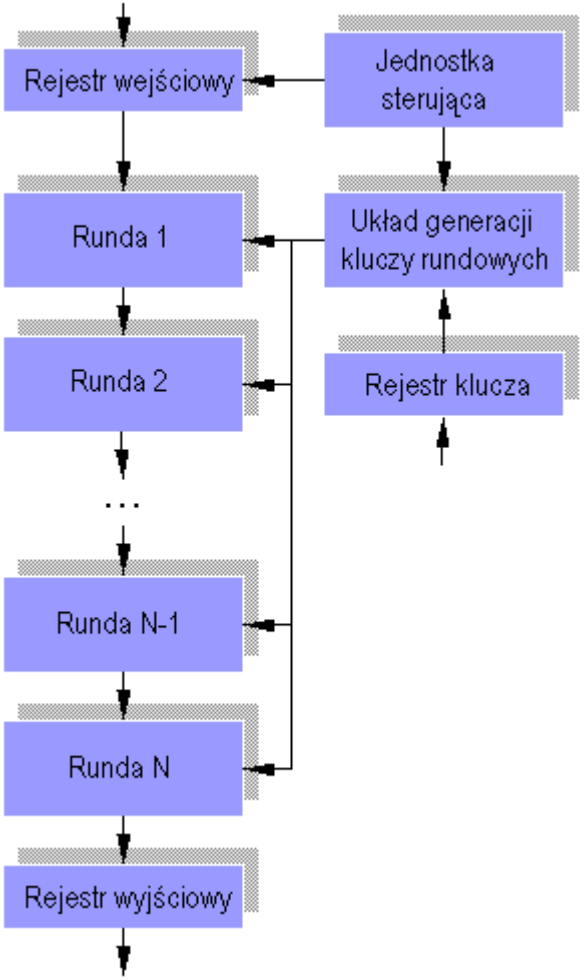
$\{k_0,k_1,k_2,k_3\} := S_3(w_0,w_1,w_2,w_3)$

$$W_i := (W_{i-8} \oplus W_{i-5} \oplus W_{i-3} \oplus W_{i-1} \oplus \phi \oplus i) <<< 11$$

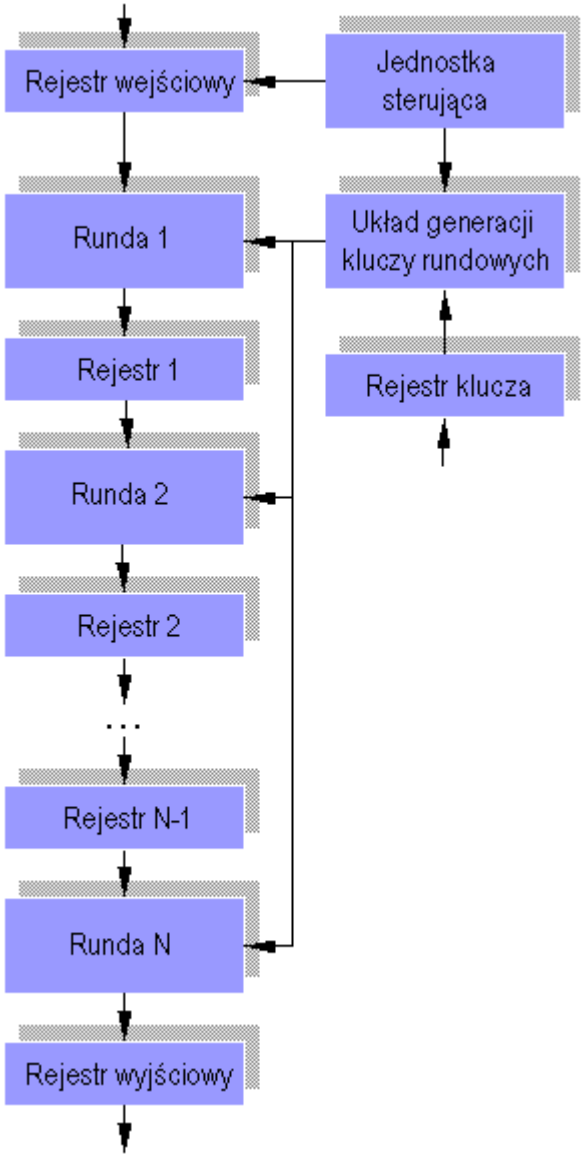
Architektura iteracyjna (L)



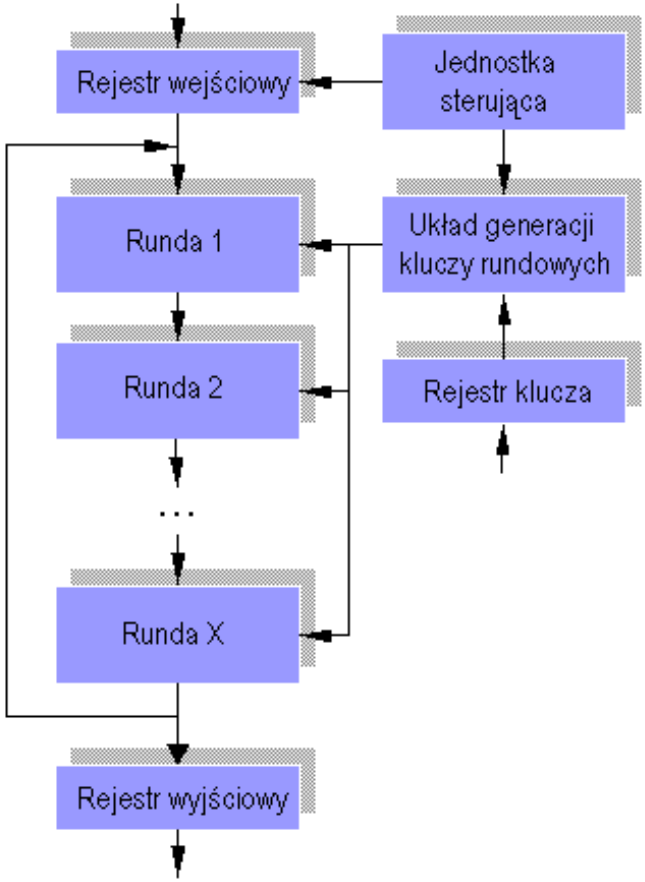
Architektura kombinacyjna (LU)



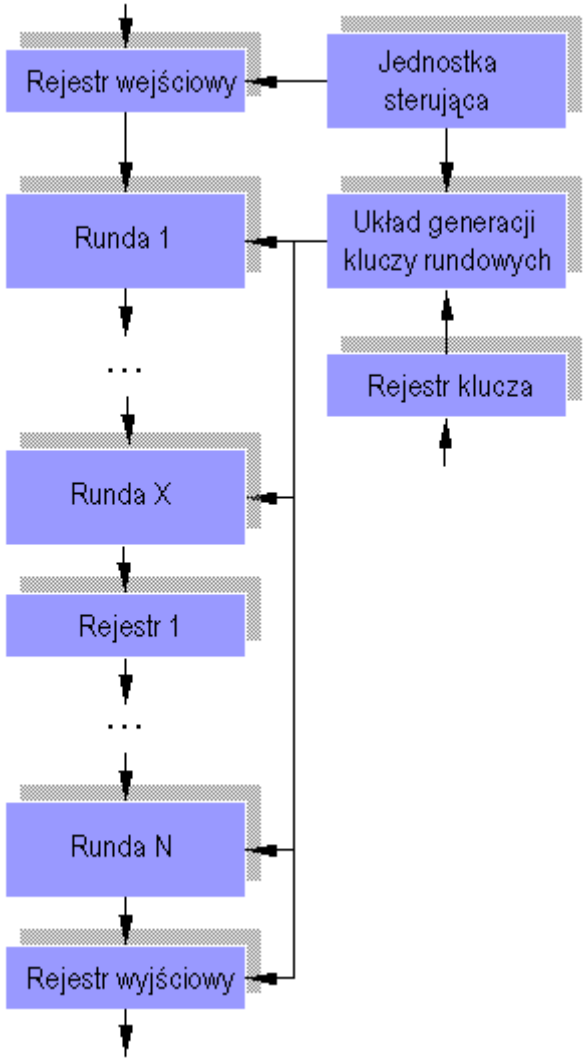
Architektura potokowa (P)



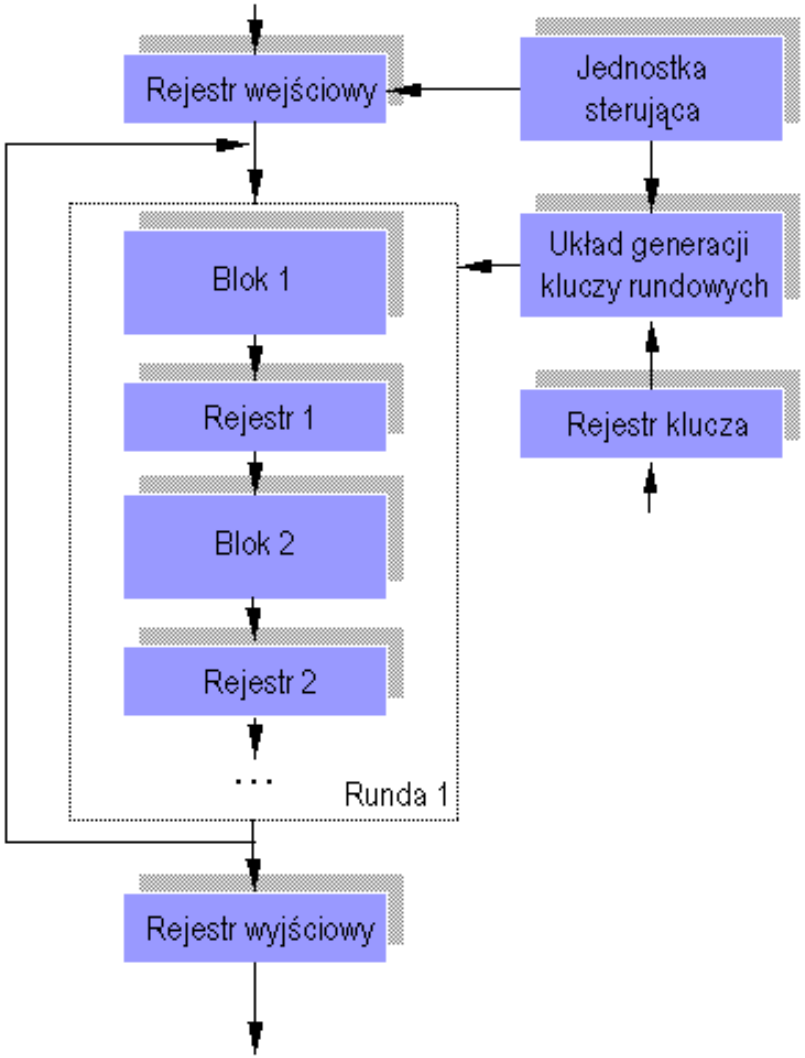
Architektura hybrydowa (LU-x)



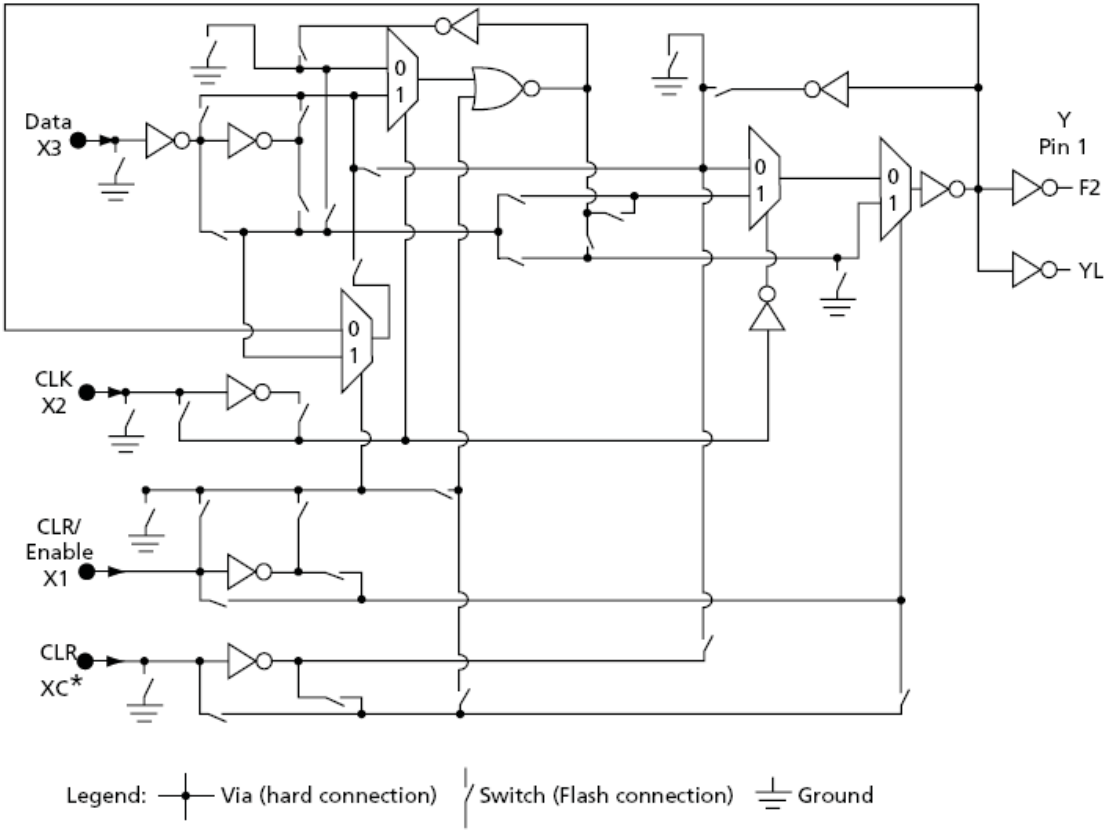
Architektura hybrydowa (PP-x)



Architektura hybrydowa (SP-x)

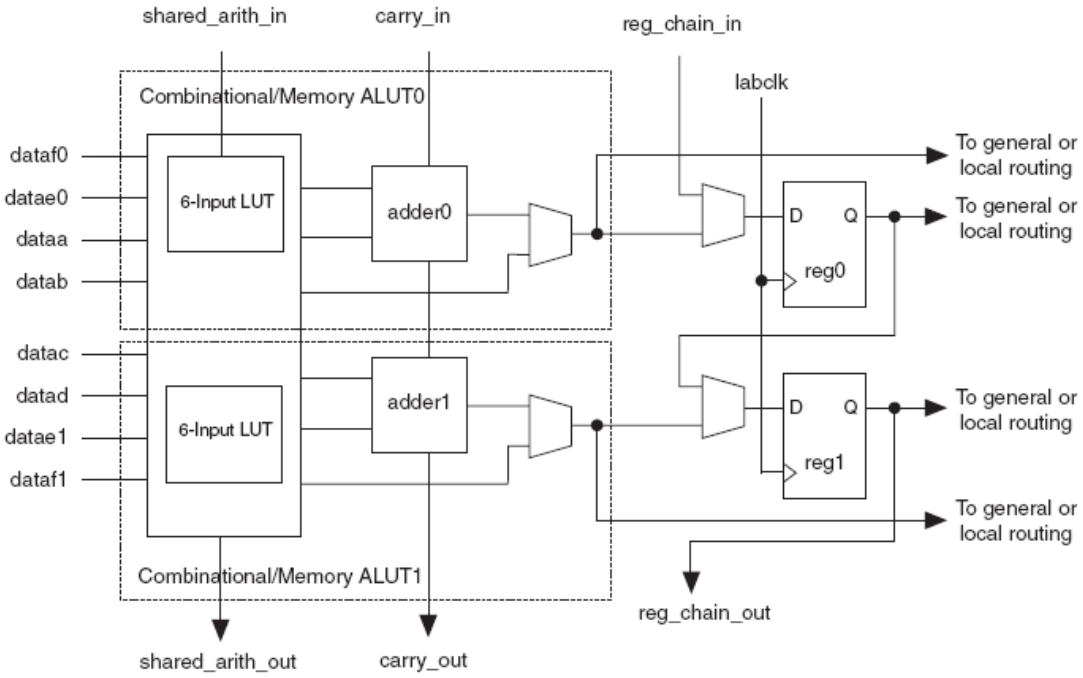


FPGA (Actel)



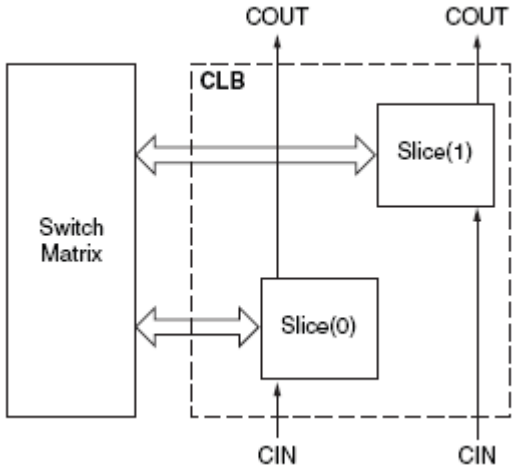
Podstawowa komórka logiczna (*tile*) w układzie ProASIC3E firmy Actel (źródło www.actel.com)

FPGA (Altera)



Podstawowa komórka logiczna (ALM) w układach z rodziny Stratix III firmy Altera (źródło www.altera.com)

FPGA (Xilinx)



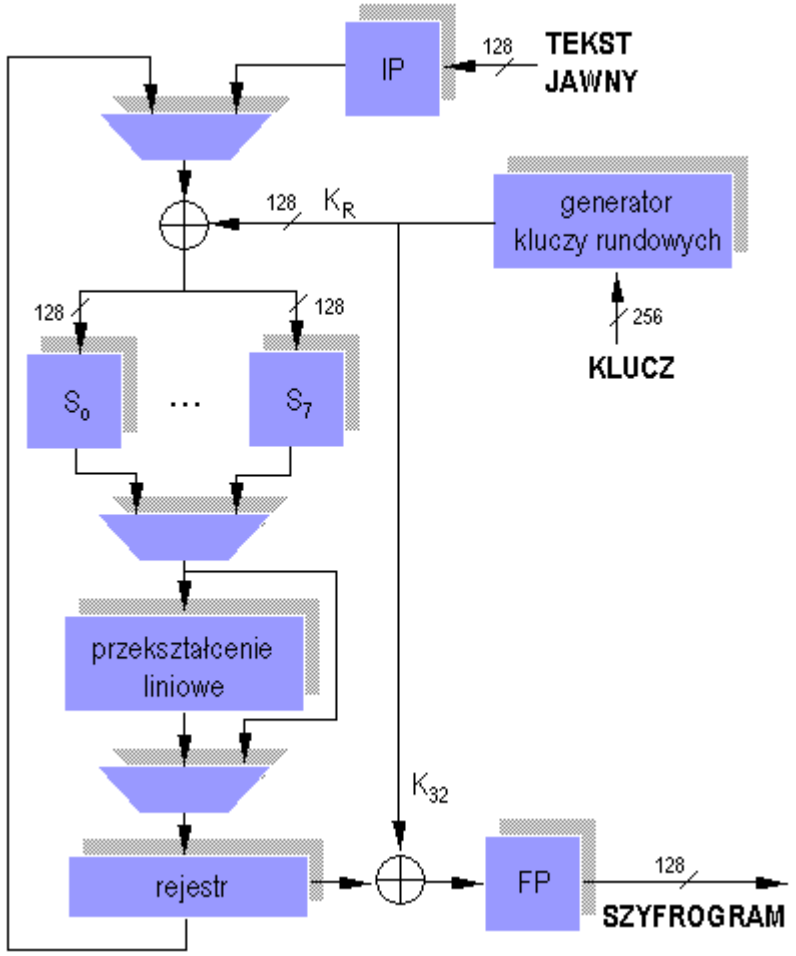
Podstawowa komórka logiczna (CLB) w układach z rodziny Virtex-5 firmy Xilinx (źródło www.xilinx.com)

Założenia projektowe

- 128-bitowa architektura
- 256-bitowy klucz szyfrowania
- możliwość realizacji bez zmian na wielu różnych platformach (przenaszalność)
- język VHDL
- realizacja z wykorzystaniem najnowszych układów *ProASIC3E* (Flash, 130 nm), *Stratix III* (SRAM, 65 nm), *Virtex-5* (SRAM, 65nm)
- realizacja i weryfikacja projektu w systemach *Quartus II* (*Altera*), *ISE* (*Xilinx*) oraz *Libero* (*Actel*)
- implementacja wybranego modułu (szyfrowania/deszyfrowania) na dostępnym zestawie startowym z układem ProASIC3 (Actel)

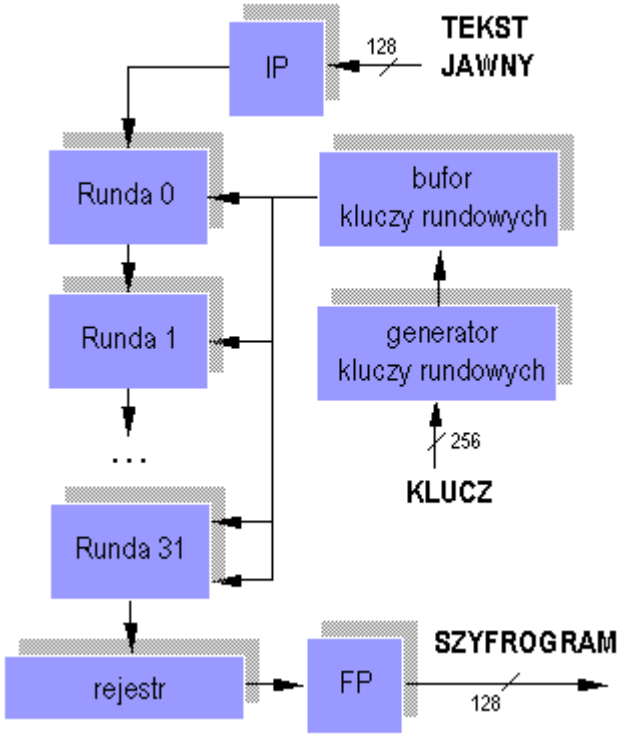
Architektura iteracyjna (LMax_KS LMaxO)

- Actel: 13 % 194 Mbit/s
- Altera: 8% 539 Mbit/s
- Xilinx: 25% 725 Mbit/s



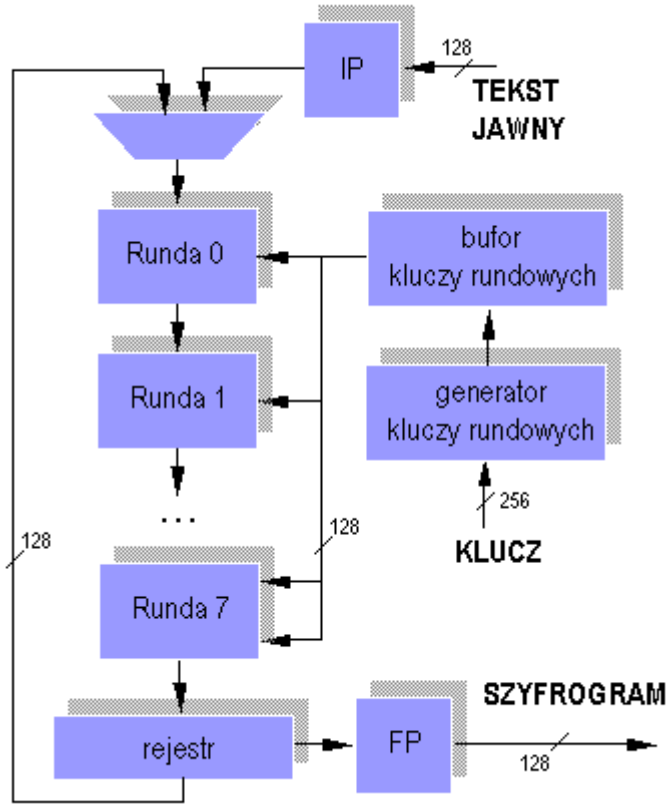
Architektura kombinacyjna (LU_KS LMaxP)

- Actel: 49 % 512 Mbit/s
- Altera: 32% 1280 Mbit/s
- Xilinx: 76% 2432 Mbit/s



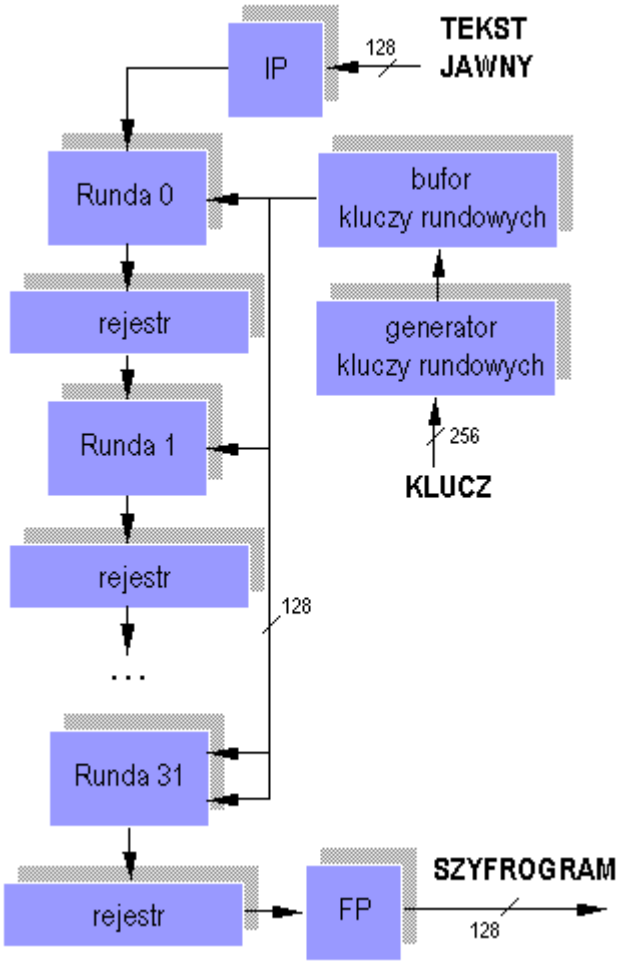
Architektura hybrydowa (LU8_KSLMaxP)

- Actel: 18 % 448 Mbit/s
- Altera: 22% 1216 Mbit/s
- Xilinx: 53% 2176 Mbit/s



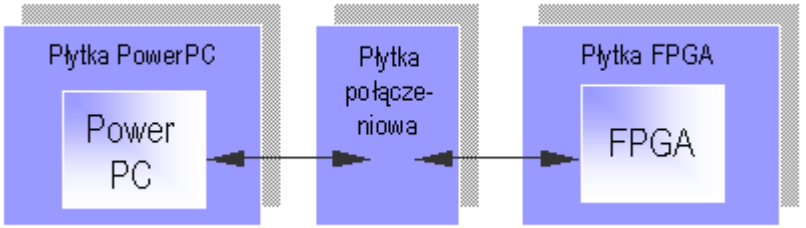
Architektura potokowa (Pipe_KSLMaxP)

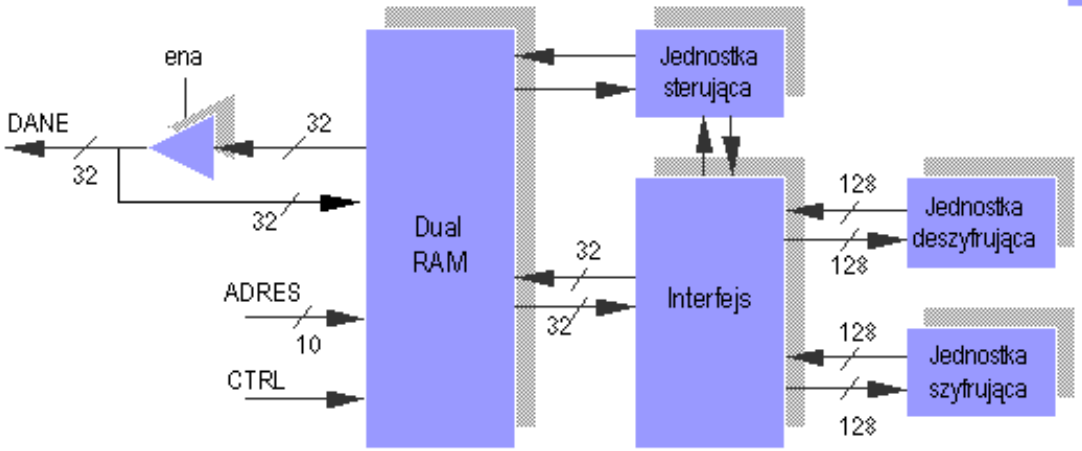
- Actel: 51 % 11392 Mbit/s
- Altera: 37% 20096 Mbit/s
- Xilinx: 83% 39296 Mbit/s



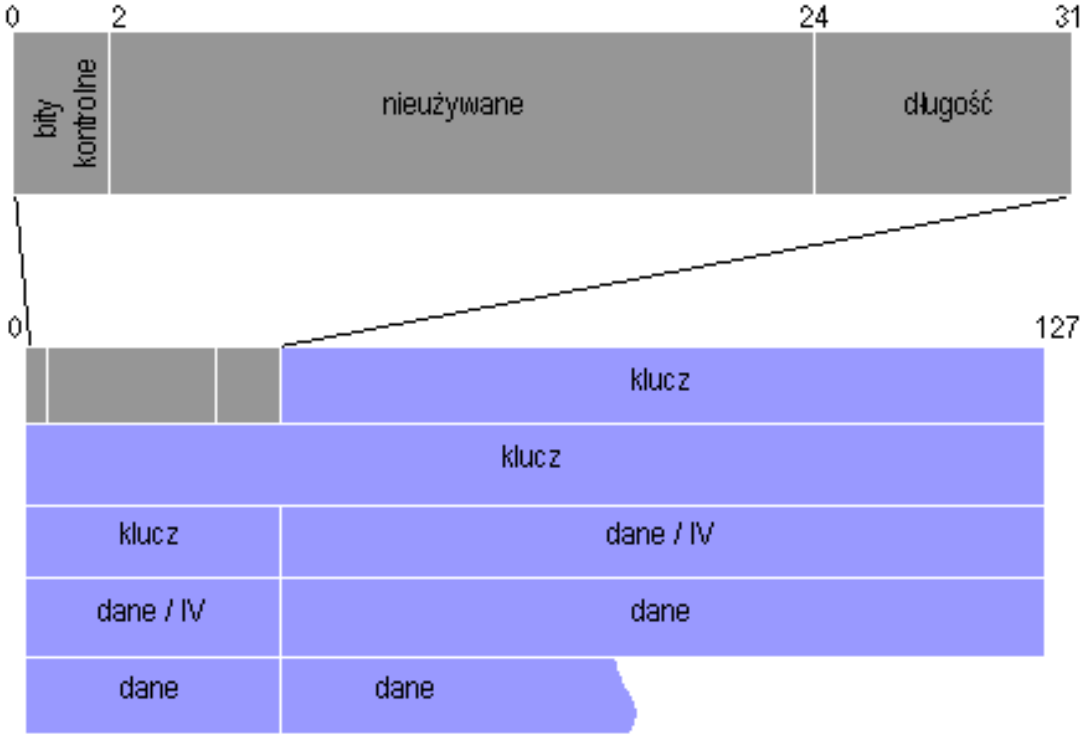
Koprocesor

- Actel (A3P1000):
  - 99% 70 Mbit/s
  - LMax_KSLMaxO
  - InvLMax_KSLMaxO





Koprocesor (cd)

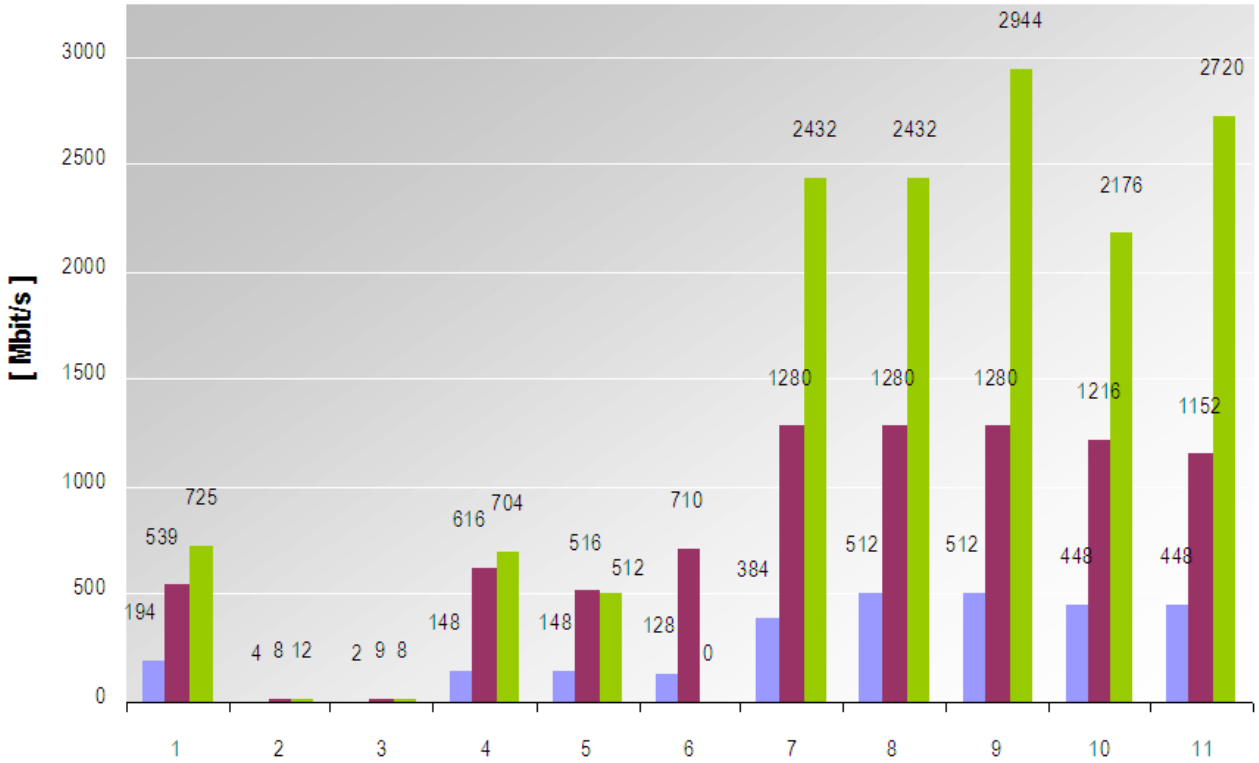


Ramka w pamięci dwuportowej.
Realizowane polecenia ENC_ECB, ENC_CBC, DEC_ECB, DEC_CBC.

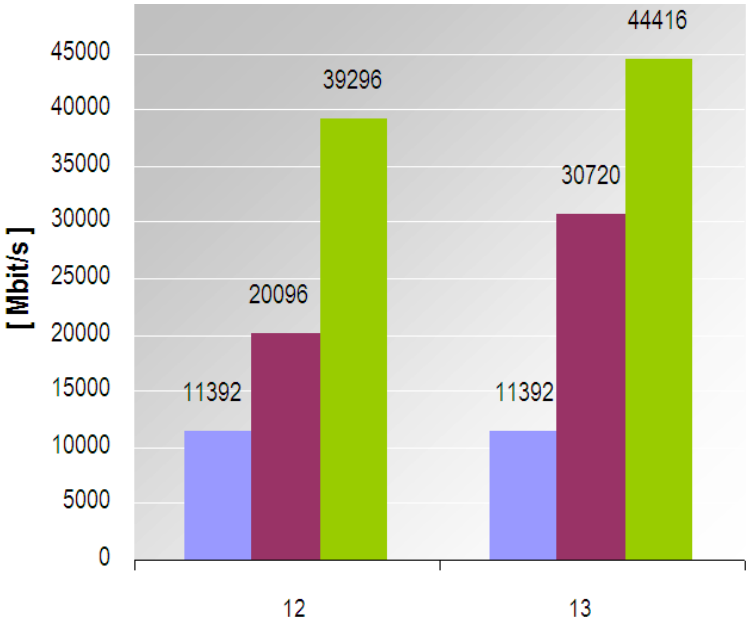
Wyniki optymalizacji

Lp.	Nazwa układu	Przepustowość (Actel) [Mbit/s]	Zajętość układu (Actel) [%]	Przepustowość (Altera) [Mbit/s]	Zajętość układu (Altera) [%]	Przepustowość Xilinx [Mbit/s]	Zajętość układu (Xilinx) [%]
1	LMax_KSLMaxO	194	13	539	8	725	25
2	LMed_KSLMedO	4	5	8	4	12	10
3	LMin_KSLMinO	2	4	9	3	8	7
4	InvLMax_KSLMaxP	148	17	616	9	704	33
5	InvLMax_KSLMedP	148	11	516	7	512	22
6	InvLMax_KSLMaxO	128	19	710	9	0	0
7	LU_KSLUO	384	71	1280	57	2432	98
8	LU_KSLMaxP	512	49	1280	32	2432	76
9	InvLU_KSLMaxP	512	50	1280	37	2944	67
10	LU8_KSLMaxP	448	18	1216	22	2176	53
11	InvLU8_KSLMaxP	448	18	1152	23	2720	52
12	Pipe_KSLMaxP	11392	51	20096	37	39296	83
13	InvPipe_KSLMaxP	11392	51	30720	36	44416	76

Wyniki (autor)



przepustowość dla architektur innych niż potokowe



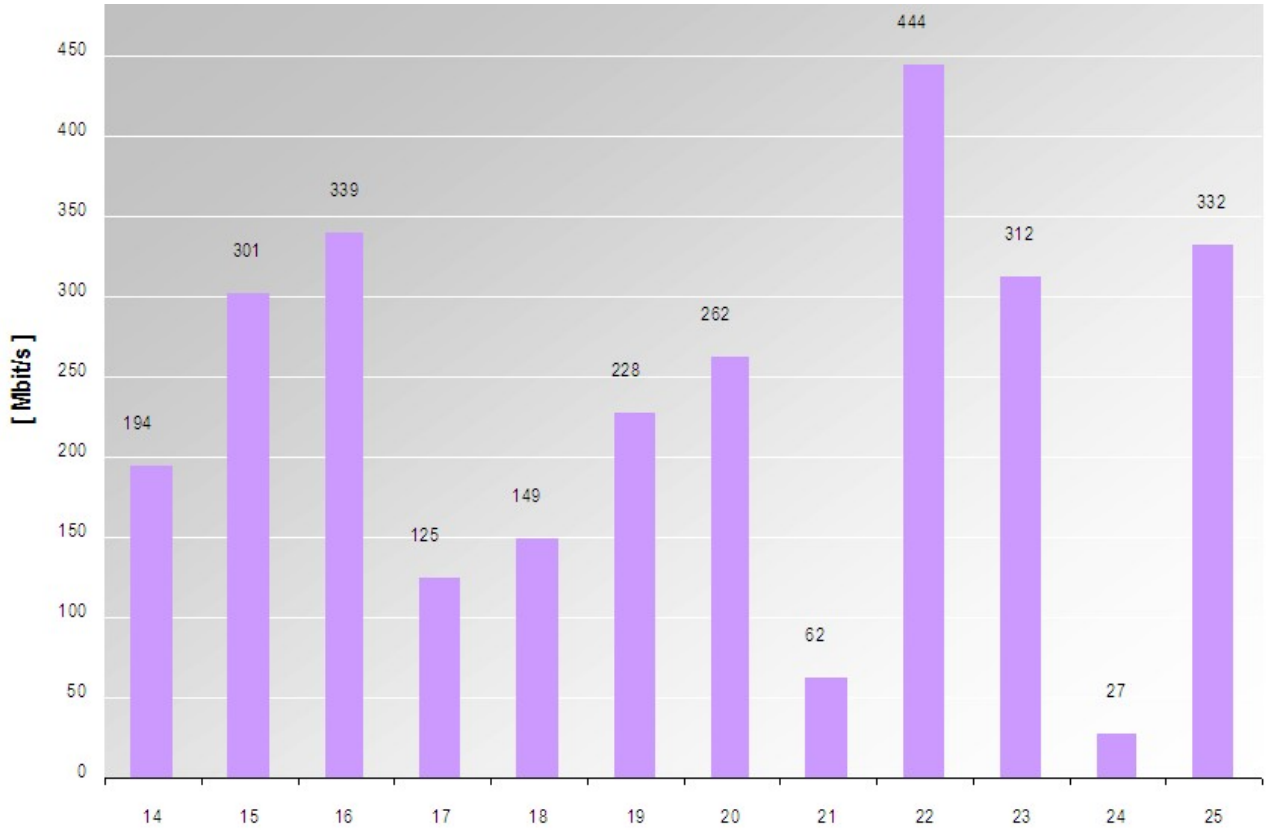
przepustowość dla architektur potokowych

Actel

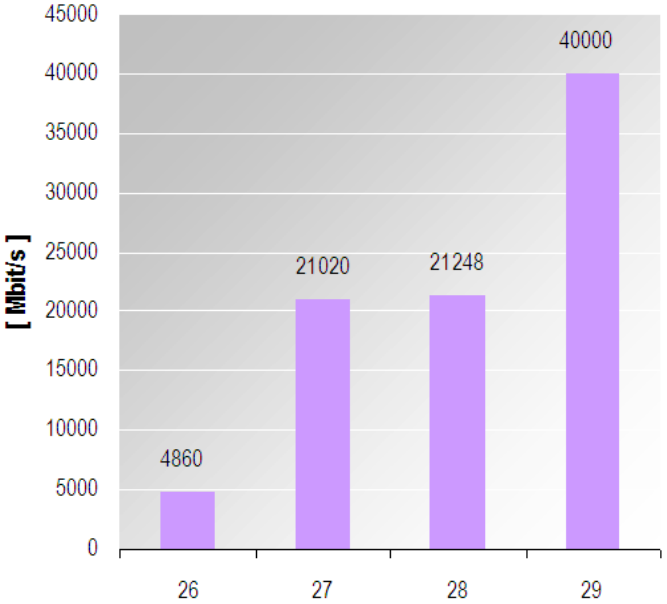
Altera

Xilinx

Wyniki (literatura)

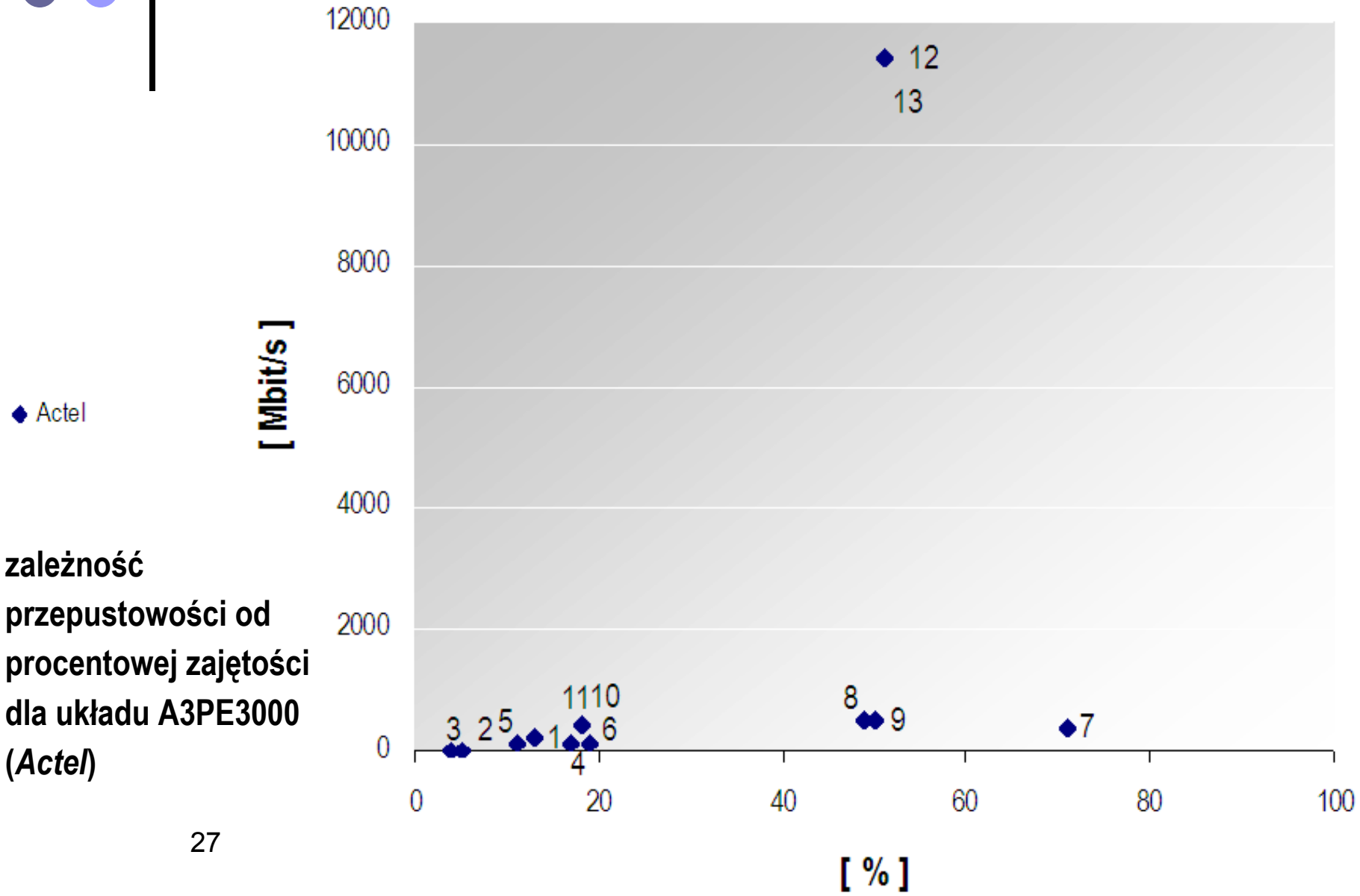


przepustowość dla architektur innych niż potokowe



przepustowość dla architektur potokowych

Wyniki (autor)



zależność przepustowości od procentowej zajętości dla układu A3PE3000 (*Actel*)

Podsumowanie

- dwie wersje kompaktowe (lightweight crypto)
- przepustowość 11 z 13 wersji >100 Mbit/s
- wykorzystanie w dedykowanych akceleratorach kryptograficznych
- perspektywy rozwoju:
  - zwiększenie stopni potoku, optymalizacja koprocesora (wydajniejsze sterowanie, bezpośrednie podłączanie do szyny procesora z pominięciem pamięci, lepsza ochrona dostarczanego klucza)

Dziękuję za uwagę