PROKOM SOFTWARE SA

Architektury akceleratorów kryptograficznych opartych o układy programowalne.

Marcin Rogawski
rogawskim@prokom.pl

PROKOM SOFTWARE SA

Plan referatu:

- Budowa akceleratora kryptograficznego;
- Struktura programowalna – element fizyczny;
- Projekt akceleratora – element logiczny;
- Architektury akceleratorów kryptograficznych;
- Projekt Hierocrypt-3;
- Szyfry blokowe, strumieniowe, funkcje skrótu – możliwosci i ograniczenia implementacyjne;
- Podsumowanie.

Budowa Akceleratora Kryptograficznego

PROKOM SOFTWARE SA

- Blok wspomagający operacje I/O;
- Wewnętrzna pamięć RAM;
- Moduły kryptograficzne;
- Kontroler;

Tryby pracy modułu sprzętowego

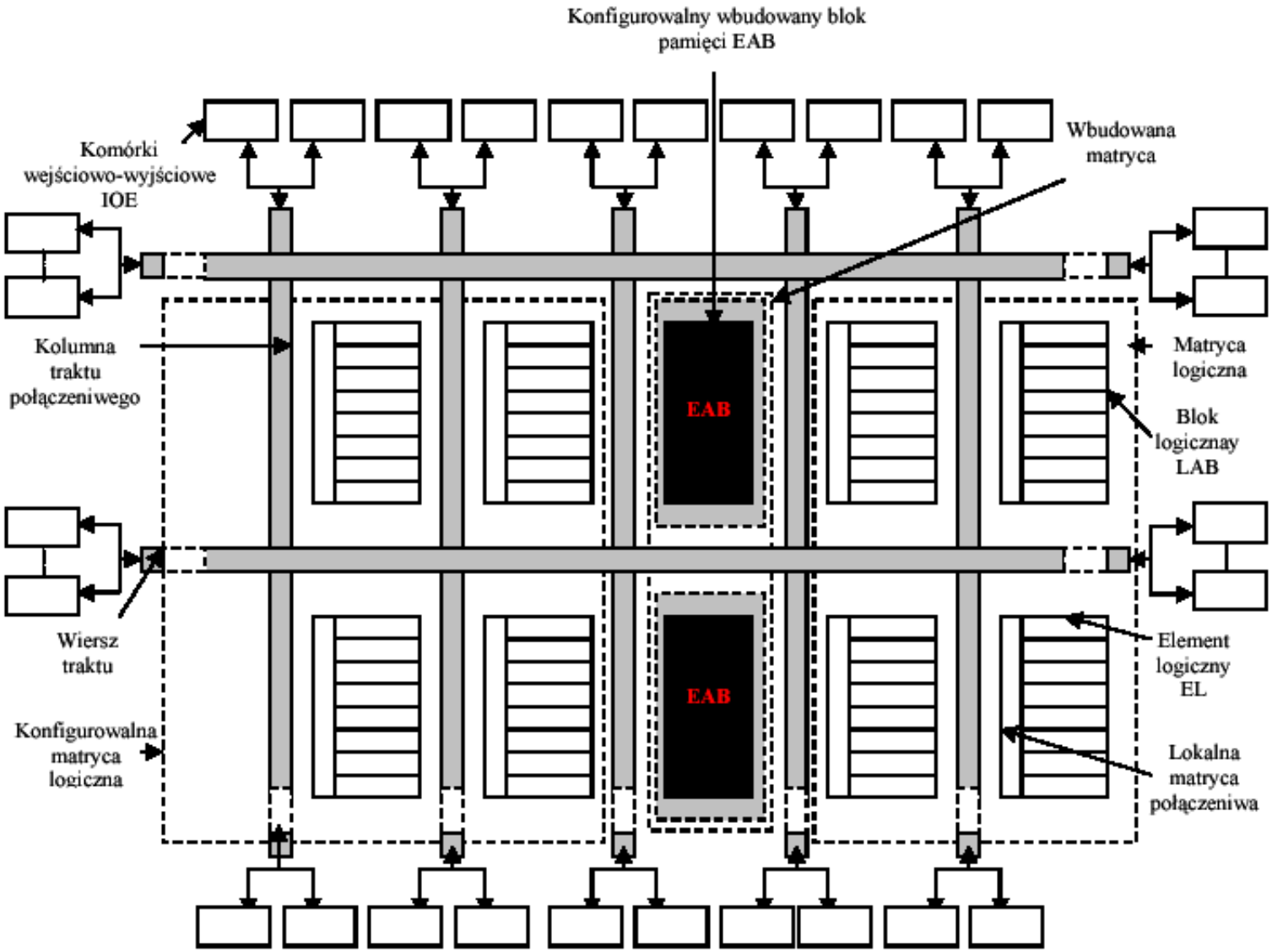
- Tryb Slave:
  - “inteligentna pamięć”;
- Tryb Master:
  - “fetch-load-do-store”;
  - 99% czasu pracy;

Układy programowalne – warstwa fizyczna

- Producenci:
  - ALTERA;
  - XILINX;
- Zasoby:
  - liczba wyprowadzeń;
  - bloki logiczne;
  - bloki pamięci wbudowanej;
  - bloki DSP;

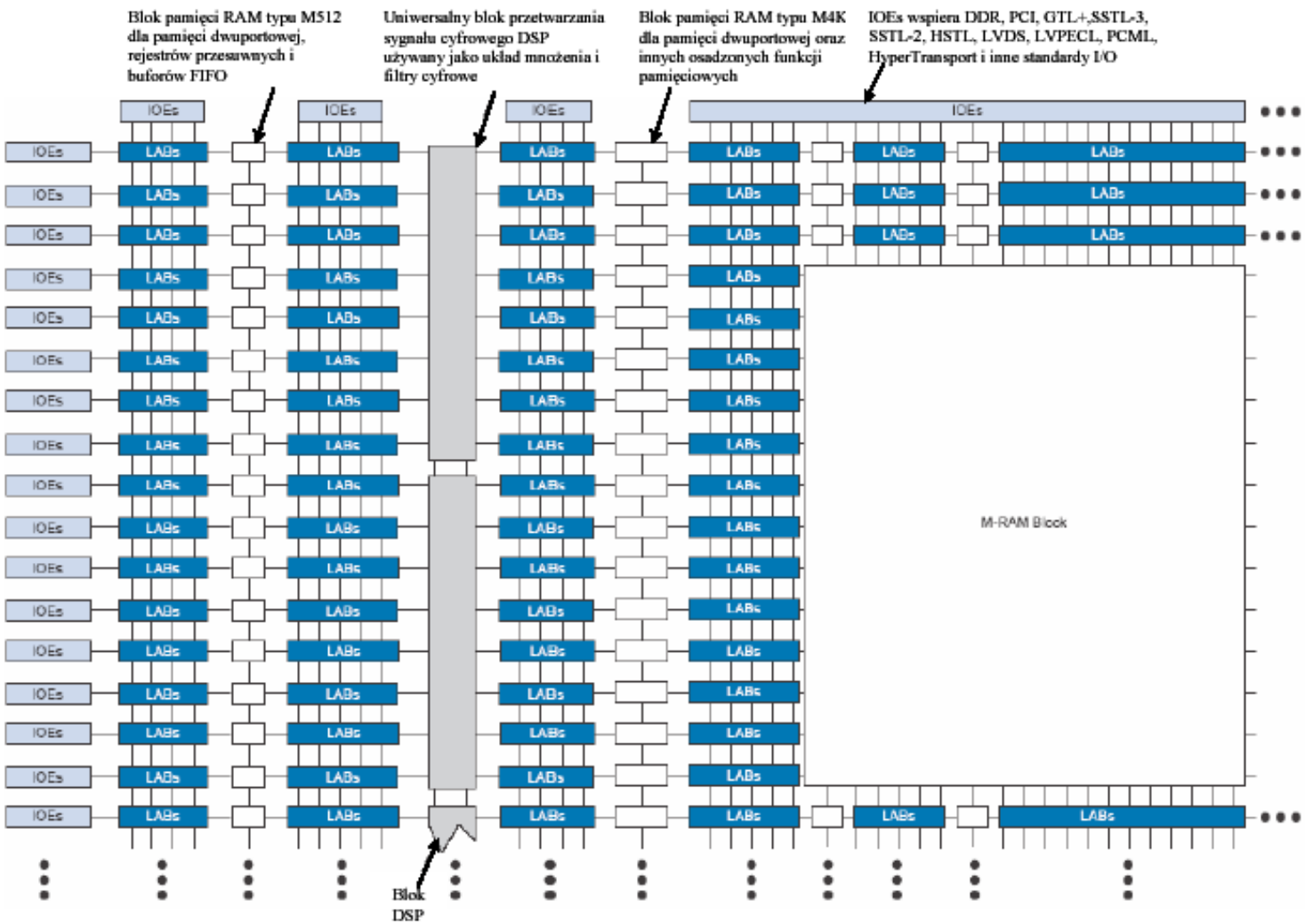
ALTERA
Uklady programowalne

FLEX 10KE


Konfigurowalny wbudowany blok pamięci EAB
Komórki wejściowo-wyjściowe IOE
Wbudowana matryca
Kolumna traktu połączeniwego
EAB
Matryca logiczna
Blok logicznay LAB
Wiersz traktu
EAB
Element logiczny EL
Konfigurowalna matryca logiczna
Lokalna matryca połączeniwa

PROKOM SOFTWARE SA

Stratix



PROKOM SOFTWARE SA

Warstwa logiczna akceleratora

- Systemy projektowe:
  - Max Plus II (Altera);
  - Quartus II 4.0 (Altera);
  - Leonardo Spectrum (Altera);
  - Foundation (Xilinx);
- Języki opisu sprzętu:
  - VHDL;
  - AHDL;
  - Aldec;
  - Verilog;

Warstwa logiczna akceleratora

- Analiza założeń funkcjonalnych dla akceleratora: szyfry blokowe, strumieniowe, funkcje skrótu;
- Kryterium optymalizacji projektu: szybkość, efektywność, cena ☹;

PROKOM SOFTWARE SA

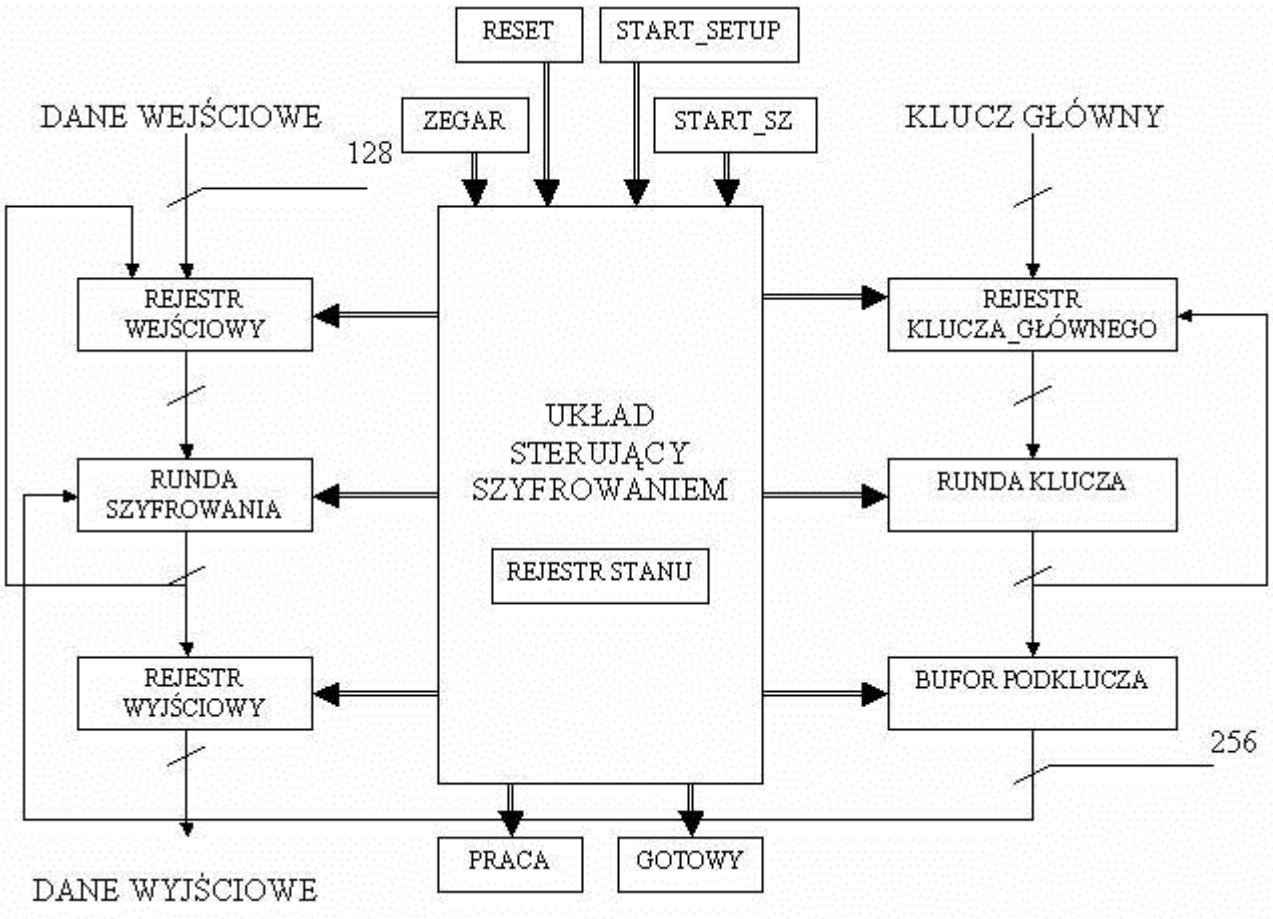
Analiza budowy algorytmu

- Runda szyfru;
- Generacja podkluczy:
  - wcześniejsze wyznaczenie podkluczy;
  - równoczesne wyznaczanie podkluczy;
  - częściowe wyznaczenie podkluczy;
- Funkcje nieliniowe:
  - funkcja kombinacyjna;
  - ROM sync., async.;

Architektury modułów kryptograficznych

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

Architektura ITERACYJNA

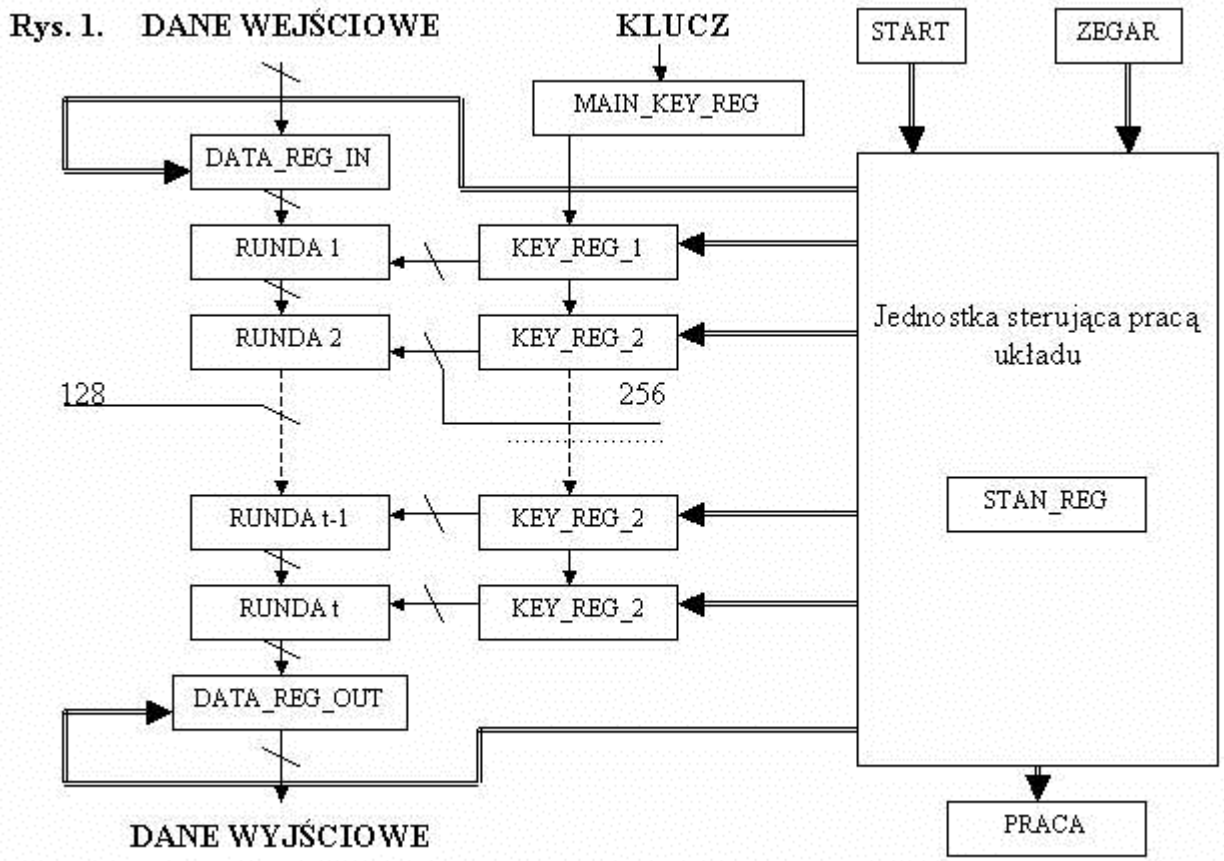


PROKOM SOFTWARE SA

Architektura ITERACYJNA

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

Architektura KOMBINACYJNA

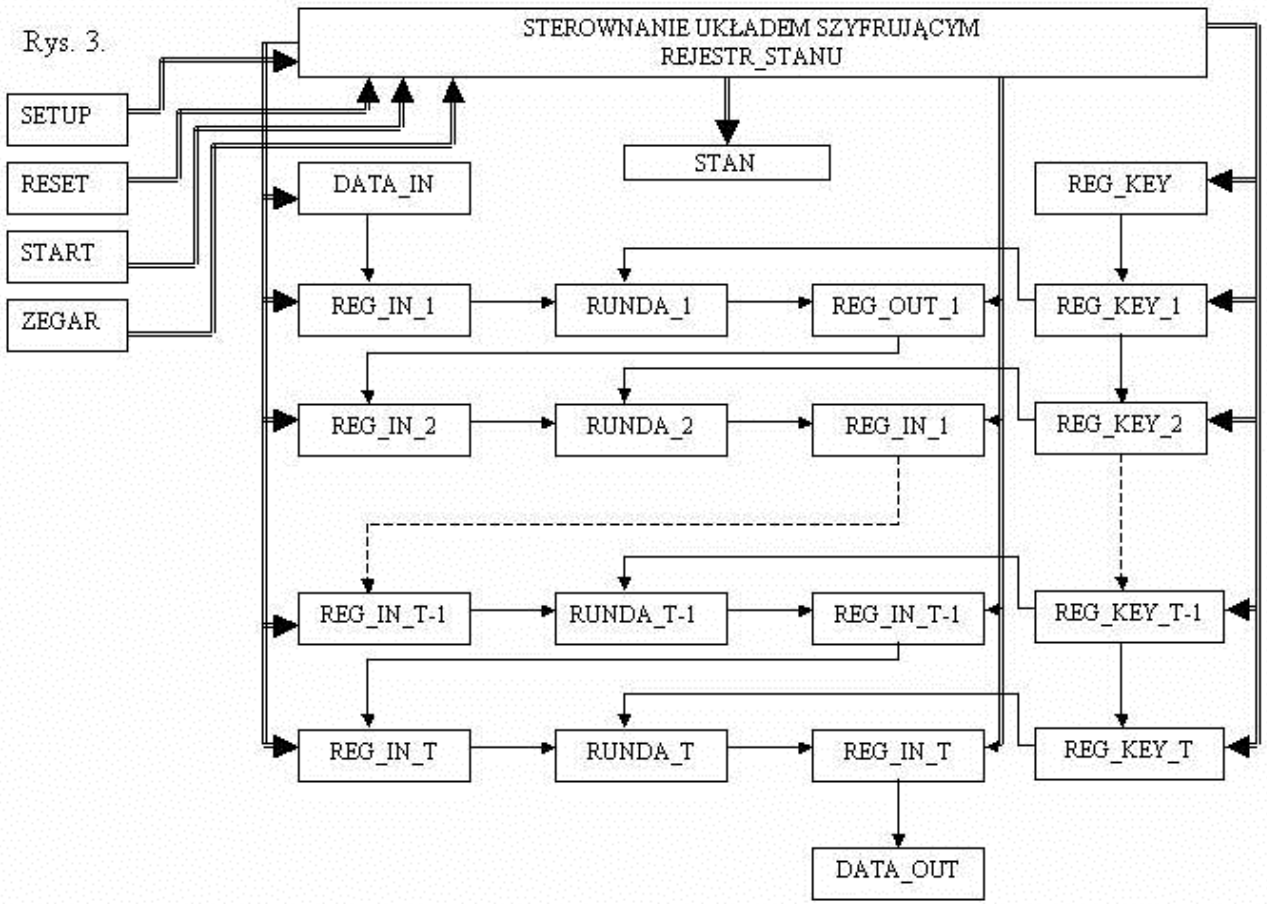


PROKOM SOFTWARE SA

Architektura KOMBINACYJNA

- niska efektywność;
- układ sterujący – nieskomplikowany;
- ograniczona możliwość realizacji większości algorytmów blokowych,

Architektura POTOKOWA



PROKOM SOFTWARE SA

Architektura POTOKOWA

- Natura procesorów typu RISC;
- Mała efektywność;
- Największa szybkość przetwarzania;
- Możliwość realizacji każdego algorytmu blokowego;
- WADA: architektura tylko dla ECB ☹;
- WADA: brak wsparcia dla funkcji skrótu;

PROKOM SOFTWARE SA

Projekt Hierocrypt-3

- NESSIE;
- autorzy: TOSHIBA Corp. (Kenji Ohkuma);
- szyfr blokowy;
- długość bloku danych – 128 bitów;
- długość klucza – 128, 192, 256 bitów;
- ilość rund – 6, 7, 8;
- „Strategia szerokiej ścieżki” + SHARK;
- struktura szyfru: NSPN (ang. Nested Substitution Permutation Network) + Sieć Feistela;
- algorytm nieinwolucyjny;

TOSHIBA

PROKOM SOFTWARE SA

Kryteria projektowe

- bezpieczeństwo;
- szybkość działania;
- efektywność implementacji;

Szyfrowanie/Deszyfrowanie

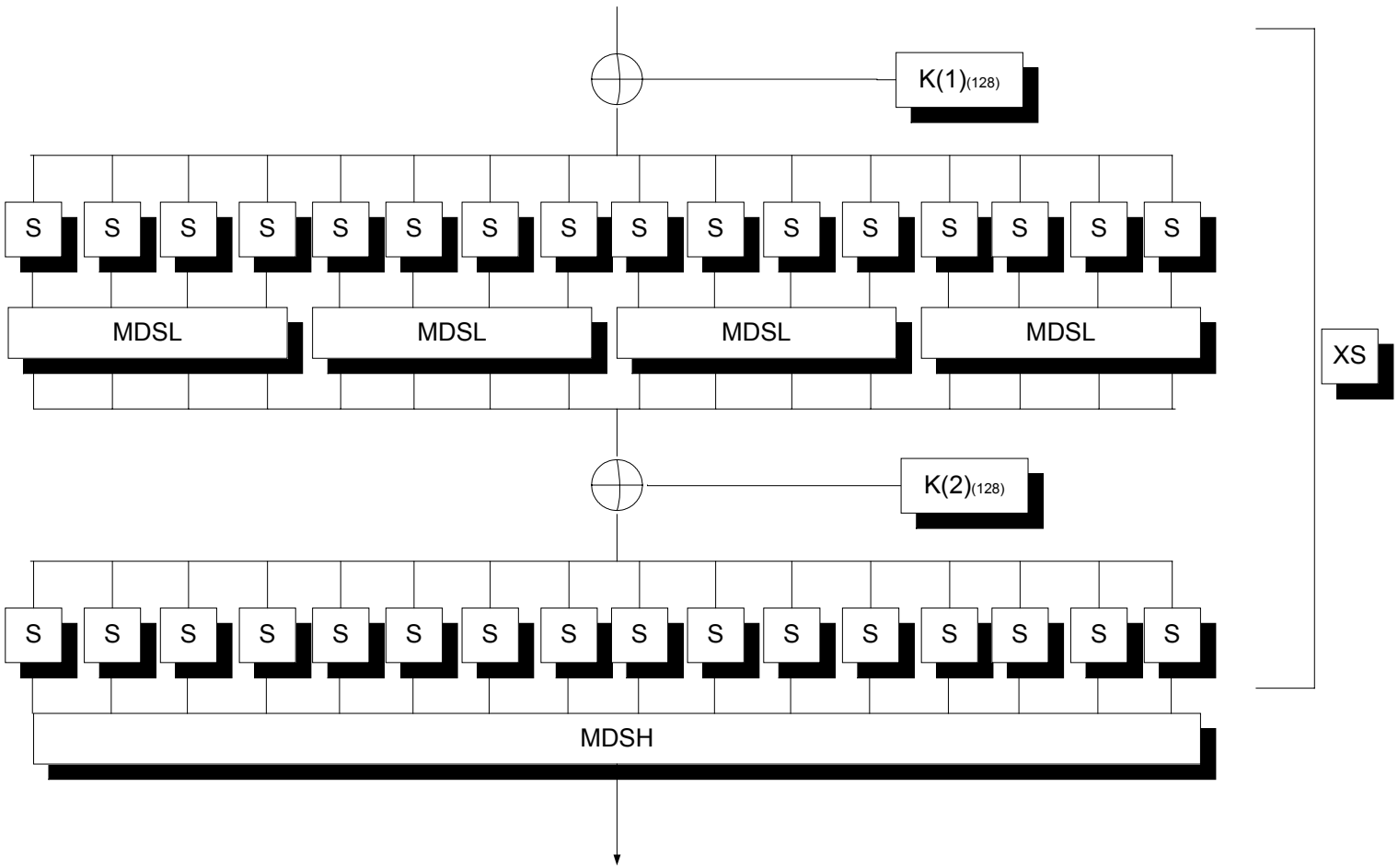
- Szyfrowanie:

$$P_{(128)} \equiv X^{(0)}_{(128)} \stackrel{\rho}{\longmapsto} X^{(1)}_{(128)} \stackrel{\rho}{\longmapsto} \cdots \stackrel{\rho}{\longmapsto} X^{(T-1)}_{(128)} \stackrel{XS}{\longmapsto} X^{(T)}_{(128)} \stackrel{AK}{\longmapsto} C_{(128)}$$

- Deszyfrowanie:

$$\begin{aligned}
X^{(T)}_{(128)} &= C_{(128)} \oplus (K^{(T+1)}_{1(64)} \| K^{(T+1)}_{2(64)}) \ , \\
X^{(T-1)}_{(128)} &= XS^{-1}(X^{(T)}_{(128)}, K^{(T)}_{(256)}) \ , \\
X^{(t-1)}_{(128)} &= \rho^{-1}(X^{(t)}_{(128)}, K^{(t)}_{(256)}) \ , \ t = T-1, \ldots, 2, 1.
\end{aligned}$$

Runda szyfru



Macierz MDS nizszego rzędu

$Y_{1(8)}$	=	C4	65	C8	8B	*	$x_{1(8)}$
$Y_{2(8)}$		8B	C4	65	C8		$x_{2(8)}$
$Y_{3(8)}$		C8	8B	C4	65		$x_{3(8)}$
$Y_{4(8)}$		65	C8	8B	C4		$x_{4(8)}$

$$y_{1(8)} = C4 * x_{1(8)} \oplus 65 * x_{2(8)} \oplus C8 * x_{3(8)} \oplus 8B * x_{4(8)}$$

$$y_{2(8)} = 8B * x_{1(8)} \oplus C4 * x_{2(8)} \oplus 65 * x_{3(8)} \oplus C8 * x_{4(8)}$$

$$y_{3(8)} = C8 * x_{1(8)} \oplus 8B * x_{2(8)} \oplus C4 * x_{3(8)} \oplus 65 * x_{4(8)}$$

$$y_{4(8)} = 65 * x_{1(8)} \oplus C8 * x_{2(8)} \oplus 8B * x_{3(8)} \oplus C4 * x_{4(8)}$$

wielomian charakterystyczny: $x^8 + x^6 + x^5 + x + 1$.

PROKOM SOFTWARE SA

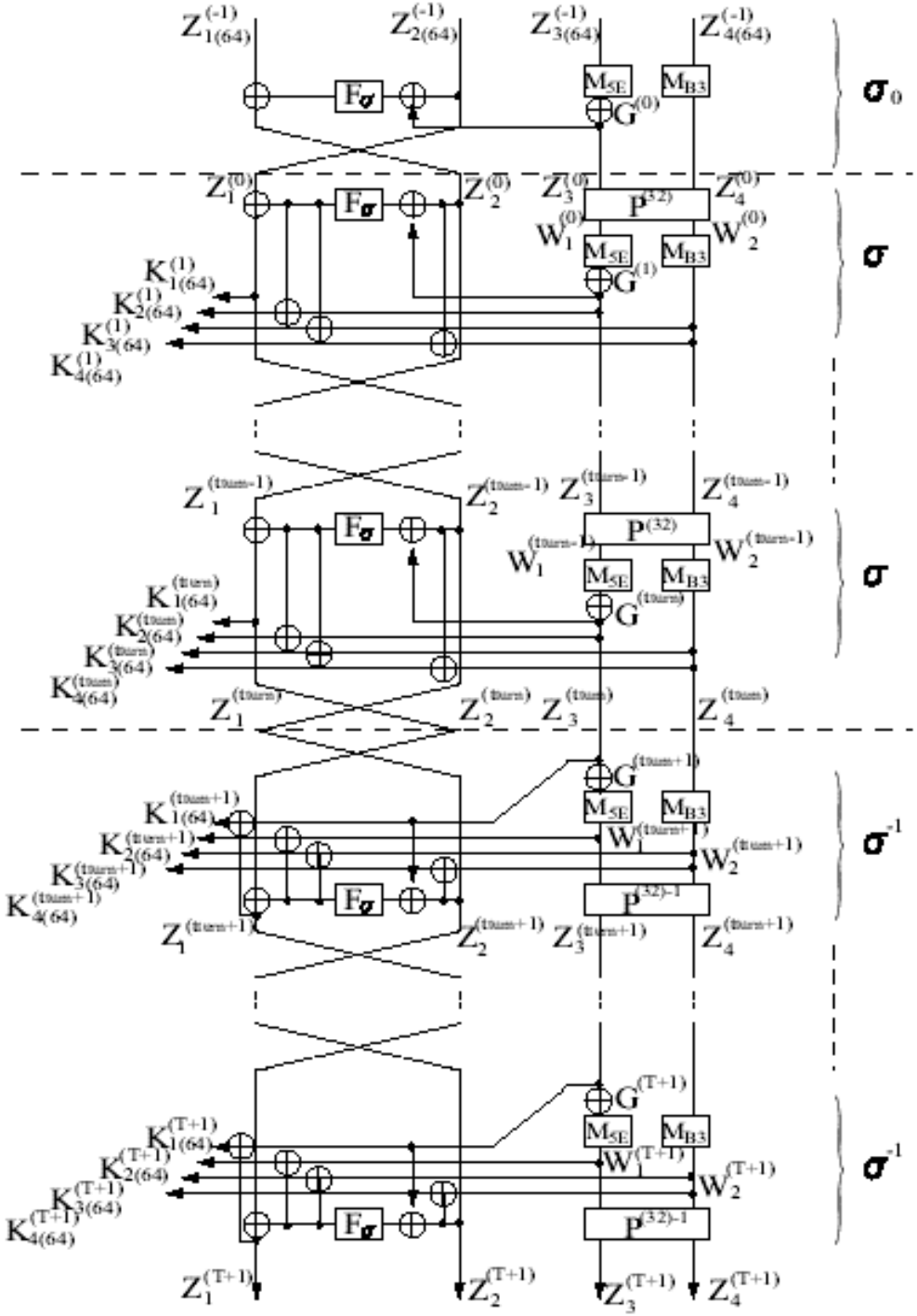
Macierz MDS wyższego rzędu

$Y_{1(8)}$	=	1	0	1	0	1	0	1	0	1	1	0	1	1	1	1	1	$x_{1(8)}$
$Y_{2(8)}$		1	1	0	1	1	1	0	1	1	1	1	0	0	1	1	1	$x_{2(8)}$
$Y_{3(8)}$		1	1	1	0	1	1	1	0	1	1	1	1	0	0	1	1	$x_{3(8)}$
$Y_{4(8)}$		0	1	0	1	0	1	0	1	1	0	1	0	1	1	1	0	$x_{4(8)}$
$Y_{5(8)}$		1	1	1	1	1	0	1	0	1	0	1	0	1	1	0	1	$x_{5(8)}$
$Y_{6(8)}$		0	1	1	1	1	1	0	1	1	1	0	1	1	1	1	0	$x_{6(8)}$
$Y_{7(8)}$		0	0	1	1	1	1	1	0	1	1	1	0	1	1	1	1	$x_{7(8)}$
$Y_{8(8)}$		1	1	1	0	0	1	0	1	0	1	0	1	1	0	1	0	$x_{8(8)}$
$Y_{9(8)}$		1	1	0	1	1	1	1	1	1	0	1	0	1	0	1	0	$x_{9(8)}$
$Y_{10(8)}$		1	1	1	0	0	1	1	1	1	1	0	1	1	1	0	1	$x_{10(8)}$
$Y_{11(8)}$		1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	0	$x_{11(8)}$
$Y_{12(8)}$		1	0	1	0	1	1	1	0	0	1	0	1	0	1	0	1	$x_{12(8)}$
$Y_{13(8)}$		1	0	1	0	1	1	0	1	1	1	1	1	1	0	1	0	$x_{13(8)}$
$Y_{14(8)}$		1	1	0	1	1	1	1	0	0	1	1	1	1	1	0	1	$x_{14(8)}$
$Y_{15(8)}$		1	1	1	0	1	1	1	1	0	0	1	1	1	1	1	0	$x_{15(8)}$
$Y_{16(8)}$		0	1	0	1	1	0	1	0	1	1	1	0	0	1	0	1	$x_{16(8)}$

PROKOM SOFTWARE SA

Runda klucza

- dwa rodzaje podkluczy: przejściowe, rundy;
- trzy rodzaje operacji:
  - uaktualnienia podklucza przejściowego;
  - odwrotność uaktualnienia podklucza przejściowego;
  - generacji podkluczy rundy;
- Komponenty rundy klucza:
  - $P^{(32)}$;
  - M_{5E};
  - M_{B3};
  - F_{σ};



PROKOM SOFTWARE SA

Aktualizacja podklucza przejsciowego

PROKOM SOFTWARE SA

$$W^{(t-1)}_{1(64)} \| W^{(t-1)}_{2(64)} = P^{(32)}(Z^{(t-1)}_{1(64)} \| Z^{(t-1)}_{2(64)})$$

$$Z^{(t)}_{1(64)} = Z^{(t-1)}_{2(64)},$$

$$Z^{(t)}_{2(64)} = Z^{(t-1)}_{1(64)} \oplus F_{\sigma}(Z^{(t-1)}_{2(64)} \oplus Z^{(t)}_{3(64)}),$$

$$Z^{(t)}_{3(64)} = M_{5E}(W^{(t-1)}_{1(64)}) \oplus G^{(t)}_{(64)},$$

$$Z^{(t)}_{4(64)} = M_{5E}(W^{(t-1)}_{2(64)}).$$

Odwrotność aktualizacji podklucza przejściowego

PROKOM SOFTWARE SA

$$Z^{(t)}_{1(64)} = Z^{(t-1)}_{2(64)} \oplus F_{\sigma}(Z^{(t-1)}_{1(64)} \oplus Z^{(t-1)}_{3(64)}),$$

$$Z^{(t)}_{2(64)} = Z^{(t-1)}_{1(64)},$$

$$W^{(t)}_{1(64)} = M_{B3}(Z^{(t-1)}_{3(64)} \oplus G^{(t)}_{(64)}),$$

$$W^{(t)}_{2(64)} = M_{B3}(Z^{(t-1)}_{4(64)}),$$

$$Z^{(t)}_{3(64)} \| Z^{(t)}_{4(64)} = P^{(32)\,-1}(W^{(t-1)}_{1(64)} \| W^{(t-1)}_{2(64)}).$$

PROKOM SOFTWARE SA

Generacja podkluczy rund

$$V^{(t)}_{(64)} = F_{\sigma}(Z^{(t-1)}{}_{2(64)} \oplus Z^{(t-1)}{}_{3(64)}),$$

$$K^{(t)}{}_{1(64)} = Z^{(t-1)}{}_{1(64)} \oplus V^{(t)}_{(64)},$$

$$K^{(t)}{}_{2(64)} = Z^{(t)}{}_{3(64)} \oplus V^{(t)}_{(64)},$$

$$K^{(t)}{}_{3(64)} = Z^{(t)}{}_{4(64)} \oplus V^{(t)}_{(64)},$$

$$K^{(t)}{}_{4(64)} = Z^{(t-1)}{}_{2(64)} \oplus Z^{(t)}{}_{4(64)},$$

$$V^{(t)}_{(64)} = F_{\sigma}(Z^{(t-1)}{}_{1(64)} \oplus Z^{(t)}{}_{3(64)}),$$

$$K^{(t)}{}_{1(64)} = Z^{(t)}{}_{1(64)} \oplus Z^{(t-1)}{}_{3(64)},$$

$$K^{(t)}{}_{2(64)} = W^{(t)}{}_{1(64)} \oplus V^{(t)}_{(64)},$$

$$K^{(t)}{}_{3(64)} = W^{(t)}{}_{2(64)} \oplus V^{(t)}_{(64)},$$

$$K^{(t)}{}_{4(64)} = Z^{(t-1)}{}_{1(64)} \oplus W^{(t)}{}_{2(64)},$$

PROKOM SOFTWARE SA

Projekt TOSHIBA Corp.

TOSHIBA

	ilość LC	przepustowość	szczegóły
high speed	22700	**52,6 Mb/s**	5 x FPGA
small area	6300	4,3 Mb/s	

- układy rodziny Flex 10K,
- ustawienie układu.

PROKOM SOFTWARE SA

Zalozenia projektowe

- wersja algorytmu: 128 bitowy klucz główny, 128 bitowy blok danych;
- układy programowalne – Flex 10KE (9986 LC / 49152 bity);
- uzyskanie jak NAJWIĘKSZEJ szybkości działania;
- architektura ITERACYJNA;

Realizacja skrzynek podstawieniowych

PROKOM SOFTWARE SA

- struktura komórki logicznej (ALTERA),
- dekompozycja funkcjonalna.

	efektywność	opóźnienie	efekt. całk.
ALTERA	329 LC	25,7 ns	13160 LC
DEMAIN	253 LC	20,8 ns	10120 LC
Pamięć ROM	2048 bit	17,7 ns	81920 bit

Cechy charakterystyczne projektów ITERACYJNYCH

- operacja ustawienia podklucza;
- równoległość operacji rundy klucza i szyfru;
- funkcja szyfrowania i deszyfrowania w oddzielnych modułach;
- Skrzynki podstawieniowe:
  - 16+8 x ROM;
  - 16 x DEMAIN;

PROKOM SOFTWARE SA

Projekt „krótki czas ustawienia układu˝

- jednoczesne wykonanie:
  - runda szyfru,
  - operacja uaktualnienia podklucza (jej odwrotność),
  - operacja wyznaczenia podklucza rundy.
- 2 fazy działania:
  - ustawienie układu,
  - szyfrowanie (deszyfrowanie),
- wyniki implementacji:
  - 8599 LC, 48kb EAB,
  - max. częstoliwość zegara taktującego – 8,05 MHz (124ns),
  - ilość cykli – 9,
  - przepustowość – **115Mb/s,**
- najdłużej trwająca operacja – runda klucza.

PROKOM SOFTWARE SA

Projekt „długi czas ustawienia układu´´

- **symetria algorytmu generacji podkluczy przejściowych**,
- **2 fazy działania**:
  - ustawienie układu,
  - szyfrowanie (deszyfrowanie).
- **1600 bitów** niezbędnych do wyznaczenia wszystkich podkluczy rund,
- **nie potrzebna odwrotność aktualizacji podkluczy przejściowych**,
- **wyniki implementacji**:
  - 9497 LC, 48kb EAB,
  - max. częstoliwość zegara taktującego – 11,95 MHz (84ns),
  - ilość cykli – 9,
  - przepustowość – **190 Mb/s,**
- **najdłużej trwająca operacja** – obliczenie funkcji $F\sigma$ w operacji

Projekt „bardzo długi czas ustawienia układu”

- **ustawienie układu** – 3 cykle – 1 operacja aktualizacji podkluczy:
  - **1 cykl:**
    $W^{(t-1)}_{1(64)} \,||\, W^{(t-1)}_{2(64)} = P^{(32)} (Z^{(t-1)}_{1(64)} \,||\, Z^{(t-1)}_{2(64)})$
    $Z^{(t)}_{1(64)} = Z^{(t-1)}_{2(64)}$,
  - **2 cykl:**
    $Z^{(t)}_{3(64)} = M_{5E}(W^{(t-1)}_{1(64)}) \oplus G^{(t)}_{(64)}$,
    $Z^{(t)}_{4(64)} = M_{5E}(W^{(t-1)}_{2(64)})$.
  - **3 cykl:**
    $Z^{(t)}_{2(64)} = Z^{(t-1)}_{1(64)} \oplus F_{\sigma} (Z^{(t-1)}_{2(64)} \oplus Z^{(t)}_{3(64)})$,
- **poprawienie sterowania** – oszczędność jednego cyklu,
- **połączenie operacji XS (ostatnia runda) z AK (ostatnie dodanie podklucza) w jedną – realizacja podczas 1 cyklu**,
- **wyniki implementacji**:
  - 9758 LC, 48kb EAB,
  - max. częstoliwość zegara taktującego – 15,64 MHz (60ns),
  - ilość cykli – 7,
  - przepustowość – **304 Mb/s,**
- **najdłużej trwająca operacja** – runda szyfru.

Ekstensywny projekt „bardzo długi czas ustawienia układu”

- **projekt „bardzo długi czas ustawienia układu” + przekształcenie matematyczne rundy**,
- **połączenie warstw: skrzynki podstawieniowe + macierz MDSL**

$$y_{1(8)} = C4*x_{1(8)} \oplus 65*x_{2(8)} \oplus C8*x_{3(8)} \oplus 8B*x_{4(8)}$$
$$y_{2(8)} = 8B*x_{1(8)} \oplus C4*x_{2(8)} \oplus 65*x_{3(8)} \oplus C8*x_{4(8)}$$
$$y_{3(8)} = C8*x_{1(8)} \oplus 8B*x_{2(8)} \oplus C4*x_{3(8)} \oplus 65*x_{4(8)}$$
$$y_{4(8)} = 65*x_{1(8)} \oplus C8*x_{2(8)} \oplus 8B*x_{3(8)} \oplus C4*x_{4(8)}$$

  - mnożenie elementów ciała GF(28) przez stały element z tego ciała powoduje permutację tego ciała,
  - bijektywna skrzynka podstawieniowa jest permutacją elementów pewnego ciała,
  - każda 8 bitowa wiązka jest mnożona przez 4 różne, stałe elementy z macierzy MDSL,
  - każda permutacja (skrzynka podstawieniowa) składana jest z czterema różnymi permutacjami (4 różne wartości z macierzy MDSL),
- **wyniki implementacji**:
  - 26000LC,
  - max. częstoliwość zegara taktującego – 21,73 MHz (46ns),
  - ilość cykli – 7,
  - przepustowość – **397 Mb/s,**
- **najdłużej trwająca operacja** – runda szyfru,

Implementacja algorytmów blokowychRijndael i Camellia

- Zwycięzcy konkursu AES i NESSIE,
- Dwie fazy działania układu:
  - ustawienie układu,
  - szyfrowanie (deszyfrowanie),
- Camellia – architektura HYBRYDOWA LU-3
- Wyniki implementacji:
  - 2973LC /48kb EAB,
  - max. częstoliwość zegara taktującego – 13,15 MHz (76ns),
  - ilość cykli – 7,
  - przepustowość – **240 Mb/s.**
- Rijndael – architektura ITERACYJNA
- Wyniki implementacji:
  - 1030LC /40kb EAB,
  - max. częstoliwość zegara taktującego – 76,92 MHz (13ns),
  - ilość cykli – 24,
  - przepustowość – **410 Mb/s.**

Szyfr Strumieniowy - VMPC

- Układy FLEX10KE:
  - efektywność: 134 LC/12888mbit,
  - częstotliwość: 71,94 MHz,
  - przepustowość: 44,4 Mb/s,
- Układy STRATIX:
  - efektywność: 107 LC/ 12888mbit,
  - częstotliwość: 100,0 MHz,
  - przepustowość: 80,0 Mb/s.

PROKOM SOFTWARE SA

Funkcje skrótu:

- SHA-1:
  - efektywność: 3592 LC,
  - częstotliwość: 64 MHz,
  - przepustowość: 103 Mb/s,

- RIPEMD:
  - efektywność: 4097 LC,
  - częstotliwość: 64 MHz,
  - przepustowość: 101 Mb/s,

- MD5:
  - efektywność: 3222 LC,
  - częstotliwość: 64 MHz,
  - przepustowość: 110 Mb/s.

PROKOM SOFTWARE SA

Podsumowanie

- Przyszłość akceleratorów kryptograficznych:
  - rozwój układów programowalnych,
  - rozwój sieci VPN,
  - wzrost ilości informacji w internecie,
  - Quo Vadis Cryptology ? “AES under attack”. (Camellia, Misty1, … ?)
  - Xilinx – przyszlosc ? (wsparcie kryptografii)

PROKOM SOFTWARE SA

Dziekuję za uwagę.

Pytania ???

rogawskim@prokom.pl