



# **Analiza implementacji algorytmu HIEROCRYPT w strukturach programowalnych.**

**Wojskowa Akademia Techniczna**  
**Instytut Matematyki i Kryptologii.**

**Marcin ROGAWSKI**

**Opiekun naukowy:**

**Dr inż. Piotr BORA**



# Wprowadzenie 1/2

- ♦ autorzy: **TOSHIBA Corp.**;
- ♦ szyfr blokowy;
- ♦ długość bloku danych: 128, 64 bity;
- ♦ długość klucza: 128, 192, 256 bitów;
- ♦ ilość rund: 6, 7, 8;
- ♦ **NESSIE** (ang. *New European Schemes for Signature, Integrity, and Encryption*, <http://cryptonessie.org/> ).



# Wprowadzenie 2/2

- ◆ „Strategia szerokiej ścieżki” + SHARK;
- ◆ Struktura szyfru: **NSPN** + **Sieć Feistela**;
- ◆ **NSPN** (ang. *Nested Substitution-permutation network* );
- ◆ **Sieć Feistela** (ang. *Feistel Network*);
- ◆ Algorytm nieinwolucyjny;



# Kryteria Projektowe.

- ◆ Bezpieczeństwo;
- ◆ Szybkość działania;
- ◆ Efektywność implementacji;

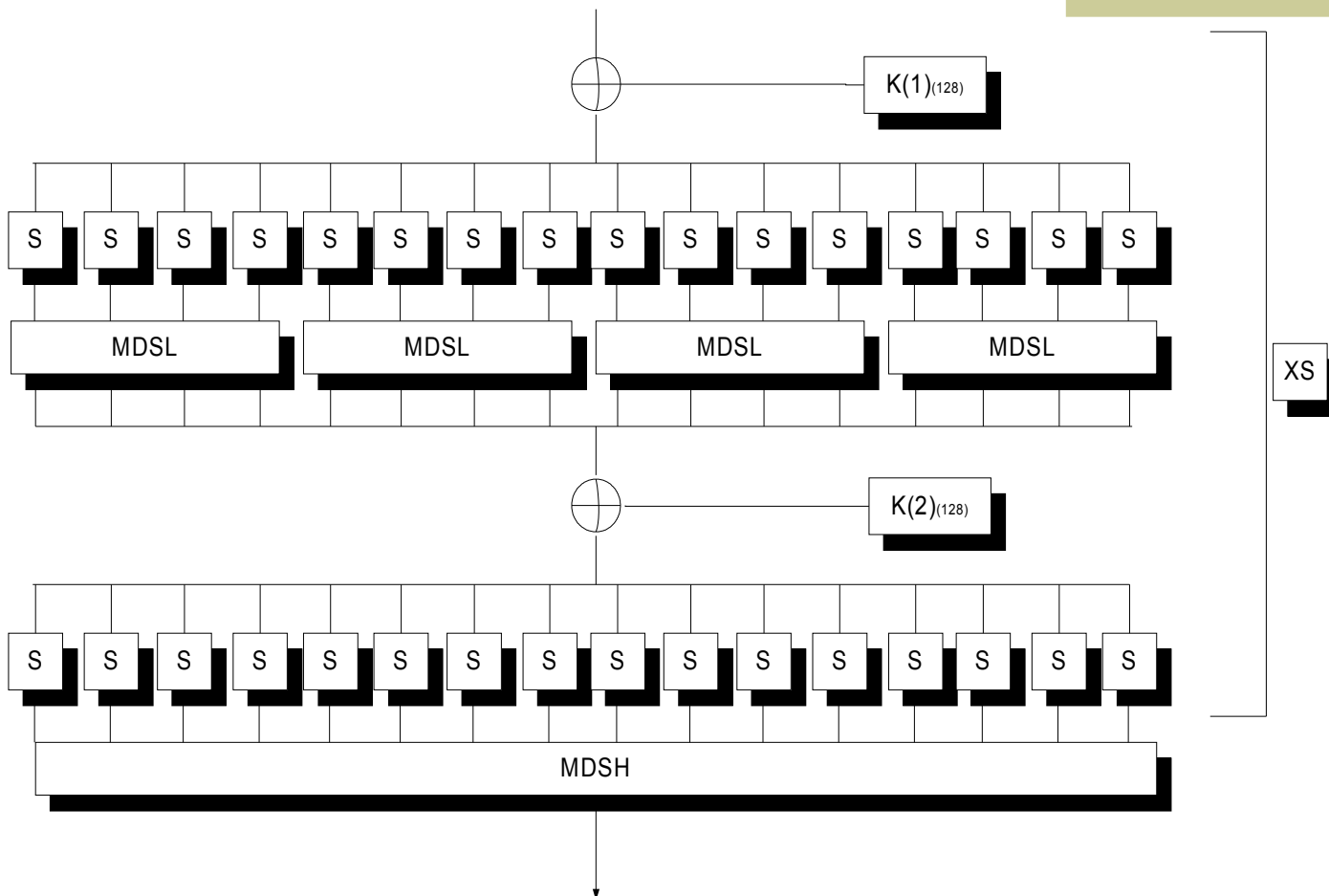


# Hierocrypt w NESSIE – odrzucony po pierwszej fazie.

- ◆ Atak typu SQUARE – Barretto;
- ◆ Różniczki niemożliwe – Cheon;
- ◆ Zależności pomiędzy bitami podklucza – Furuya;
- ◆ **Bardzo słabe wyniki implementacji sprzętowej i programowej.**



# Runda szyfru.





# Algorytm generacji podkluczy.

- ◆ uaktualnienie podklucza przejściowego;
- ◆ odwrotność uaktualnienia podklucza przejściowego;
- ◆ generacja podklucza rundy;



# Założenia projektowe.

- ◆ długość bloku, długość klucza – 128 bitów;
- ◆ implementacja w układach firmy ALTERA (Flex 10KE);
- ◆ uzyskanie jak największej szybkość działania układu;
- ◆ realizacja architektury ITERACYJNEJ.

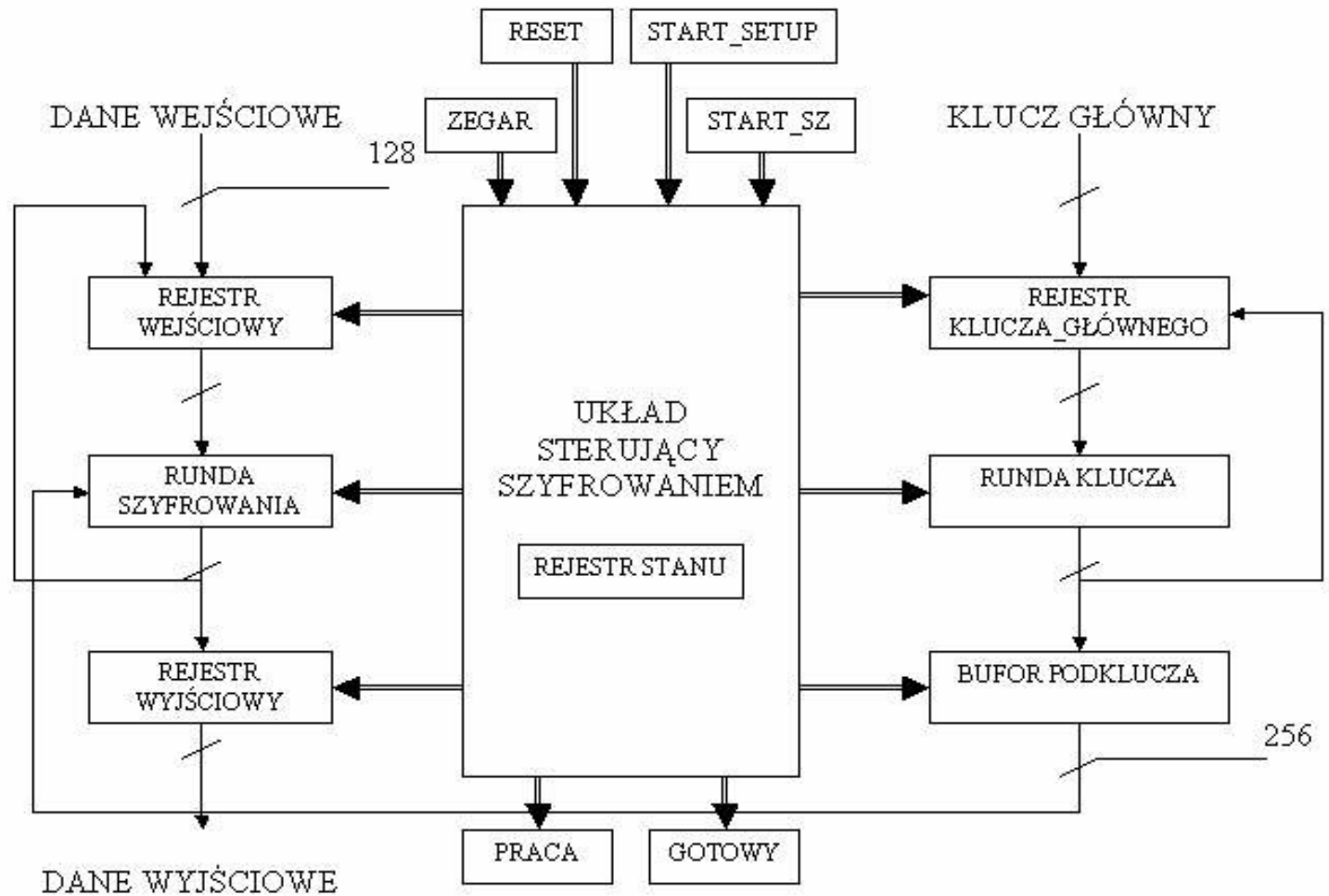


# Cechy charakterystyczne projektów ITERACYJNYCH.

- ◆ Operacja ustawienia podklucza;
- ◆ Wykorzystanie 24 bloków pamięci wbudowanej (EAB) (16 sbox z funkcji rundy + 8 algorytm generacji podkluczy);
- ◆ Funkcja szyfrowania i deszyfrowania w oddzielnych układach;
- ◆ Idea działania.



# Architektura ITERACYJNA.





# Architektura ITERACYJNA.

- ◆ Projekt z „krótkim” okresem przygotowania układu;
- ◆ Projekt z „długim” okresem przygotowania układu (1 runda podłącza - 1 cykl);
- ◆ Projekt z „długim” okresem przygotowania układu (1 runda podłącza – 3 cykle);



## Podsumowanie 1/3.

- ◆ Działania układu SZYFROWANIE – 8 cykli;
- ◆ Działanie układu DESZYFROWANIE – 9 cykli;
- ◆ Ustawienie układu – 2 („krótki” okres ustawienia), 7 („długi” okres ustawienia – 1 cykl) i 17 cykli („długi” okres ustawienia – 3 cykle);



## Podsumowanie 2/3.

- ◆ Projekt z „krótkim” czasem ustawienia układu:  
Okres zegara: **124ns**. Częstotliwość: **8,05 MHz**. Szybkość działania: **115 Mb/s**.
- ◆ Projekt z „długim” czasem ustawienia układu (1 runda–1 cykl):  
Okres zegara: **84ns**. Częstotliwość: **11,91MHz**. Szybkość działania: **190 Mb/s**.
- Projekt z „długim” czasem ustawienia układu (1 runda–3 cykle):  
Okres zegara: **64ns**. Częstotliwość: **15,62 MHz**. Szybkość działania: **250 Mb/s**.



# Podsumowanie 3/3.

- ◆ TOSHIBA Corp.:

Efektywność implementacji: **22700 LC.**

Szybkość przetwarzania: **52,6 Mb/s.**

- ◆ Rozwiązanie z „długim” okresem przygotowania układu (1runda–3 cykle):

Efektywność implementacji: **9761 LC.**

Szybkość przetwarzania: **250 Mb/s.**



# Koncepcja rozwoju projektu.

- ◆ Połączenie warstwy sbox z MDS lower level (zmniejszenie);
- ◆ Umieszczenie wszystkich elementów o wymiarze 8x8 w EAB (88);
- ◆ Użycie układów typu STRATIX.
- ◆ Projekt z „długim” okresem przygotowania układu (1 runda – 3 cykle)



# Wyniki.

- ◆ Długość trwania rundy szyfrowania – **48 ns.**
- ◆ Okres zegara taktującego układ – **52ns.**
- ◆ Szybkość przetwarzania – **307Mb/s**
- ◆ Efektywność implementacji – **25000 LE.**



Dziękuję za uwagę ...

Pytania ???

Marcin ROGAWSKI

[mrogawski@dino.wcy.wat.waw.pl](mailto:mrogawski@dino.wcy.wat.waw.pl)

+48-607-868-464