Szyfrowanie, klucz symetryczny,
Szyfry blokowe, FPGA

Roman PNIEWSKI[1]

SPRZĘTOWA REALIZACJA SZYFROWANIA

W artykule przedstawiono wybrane algorytmy szyfrowania, wykorzy-stujące klucz symetryczny. Omówiono nowe algorytmy AES (Advanced Encryption Standards), wyłonione w wyniku konkursu ogłoszonego przez NIST. Porównano wydajność zaprezentowanych algorytmów. Pokazano możliwości implementacji układów do szyfrowania i deszyfrowania w strukturach FPGA.

HARDWARE IMPLEMENTATION OF ENCODING)

In the article chosen algorithms of encoding, using the symmetrical key has been presented. Advanced Encryption Standards algoritms choosing by National Institute of Standards and Technoogy has ben discused. E performance comparision of algoritms has been described.

1. WSTĘP

Metody szyfrowania, stosowane w kryptografii można podzielić, ze względu na stosowane klucze na algorytmy symetryczne i asymetryczne.

W algorytmach asymetrycznych wykorzystywane są dwa różne klucze: pierwszy z nich jest używany do szyfrowania informacji i może być udostępniony publicznie bez ryzyka ujawnienia zawartości szyfrowanych informacji (stąd nazywany jest kluczem publicznym). Klucz deszyfrujący nazywany jest kluczem prywatnym (lub kluczem tajnym).

Algorytmy symetryczne wykorzystują ten sam klucz do szyfrowania i deszyfrowania wiadomości. Zapewniają one znacznie większą szybkość przetwarzania informacji (do stu razy) dlatego są znacznie częściej stosowane w systemach online (np. do szyfrowania przesyłanych sygnałów wizyjnych w systemach monitoringu).

Algorytmy wykorzystujące klucz symetryczny można podzielić na dwie główne kategorie:

- algorytmy blokowe: szyfrują dane blokami przy czym każdy blok jest szyfrowany niezależnie
- algorytmy strumieniowe: szyfrowane są ciągłe strumienie danych.

[1]Politechnika Radomska, Wydział Transportu i Elektrotechniki; 26-600 Radom; ul. Malczewskiego 29.
Tel: + 48 48 361-77-84, E-mail: r.pniewski@pr.radom.pl

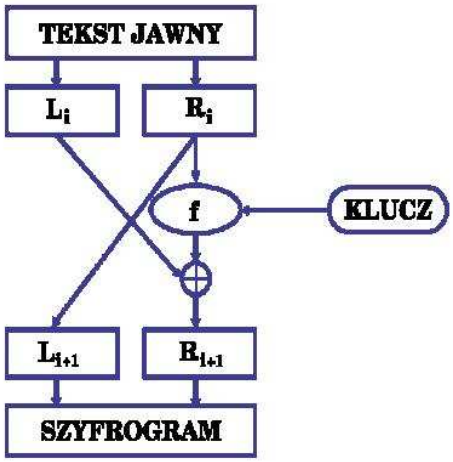
2. ALGORYTMY AES (ADVANCED ENCRYPTION STANDARD)

Ze względu ograniczenia algorytmu DES (Data Encryption Standard) w 1997 roku NIST (National Institute of Standards and Technology) ogłosił konkurs na opracowanie ulepszonych algorytmów blokowych z kluczem symetrycznym. Do finału konkursu zakwalifikowano 5 algorytmów:

- MARS: nowy szyfr z firmy IBM,
- RC6: szyfr Ronalda Rivest'a,
- Rijandel: autorstwa dwu Belgów (Joan Daemen i Vincent Rijmen),
- SERPENT: szyfr międzynarodowego zespołu z Anglii, Izraela i Norwegii,
- TwoFish: Bruce'a Schneiera (twórca BlowFish).

W wyniku przeprowadzonego konkursu, za najlepszy algorytm uznano Rijandel (ze względu na szybkość). Pod względem oferowanego bezpieczeństwa nie ma znaczącej różnicy między przedstawionymi metodami szyfrowania (dotychczas nie udało się złamać żadnego z szyfrów). Poniżej skrótowo opisano, algorytm TwoFish najlepszy (zdaniem autora) ze względu na możliwość sprzętowej implementacji.

Twofish – jest pewną kontynuacją opracowanego w 1993 r. algorytmu BlowFish. Operuje na blokach danych o wielkości 128 bitów. Wykorzystywane są klucze o długościach 128, 192 i 256 bitów. Algorytm bazuje na sieci Feistela (rys.1.).

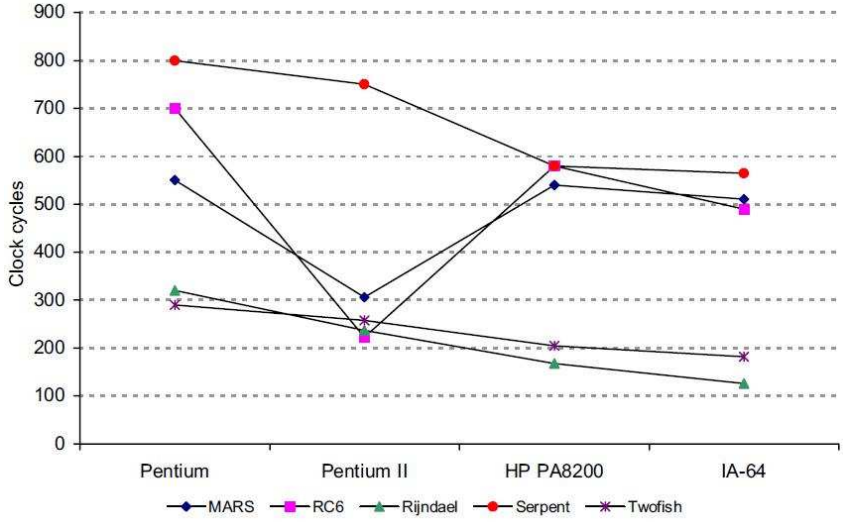


Rys.1. Szyfrowanie TwoFish – sieć Feistela [6]

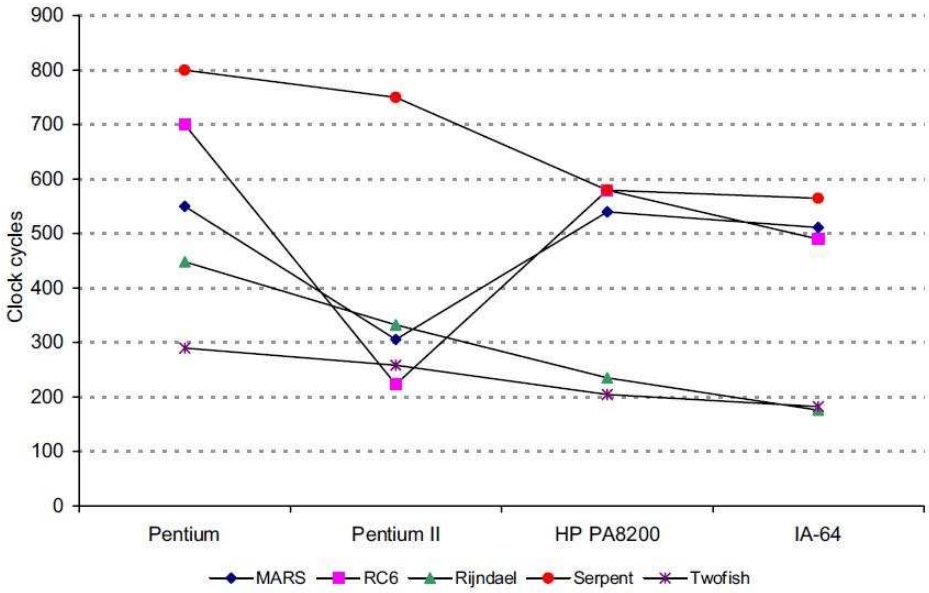
Cechą charakterystyczną algorytmu jest wykorzystanie S-boxów (rys.5) do kluczowania sygnałów.

2.1 Wydajność algorytmów

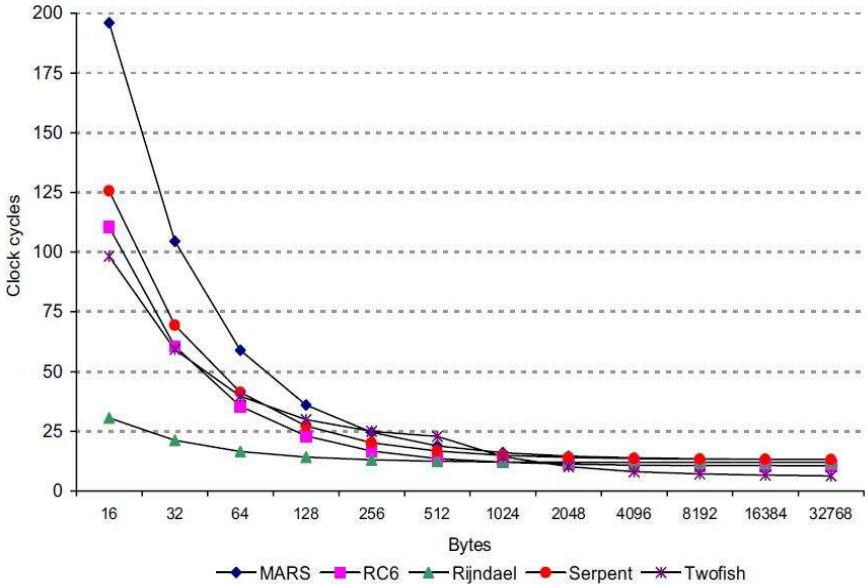
Na rysunkach 2,3,4 pokazano (zaczerpnięte z literatury) wydajności poszczególnych algorytmów AES przy realizacji programowej z wykorzystaniem komputera.



Rys.2. Porównanie szybkości algorytmów (assembler) dla klucza 128-bitowego[5]



Rys.3. Porównanie szybkości algorytmów (assembler) dla klucza 256-bitowego[5]

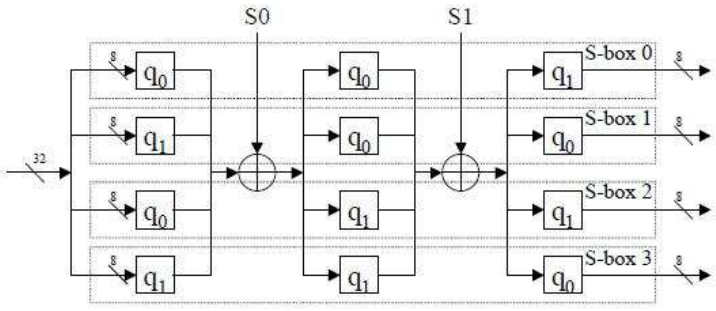


Rys.4. Porównanie szybkości algorytmów: liczba cykli/bajt w funkcji długości bloku danych

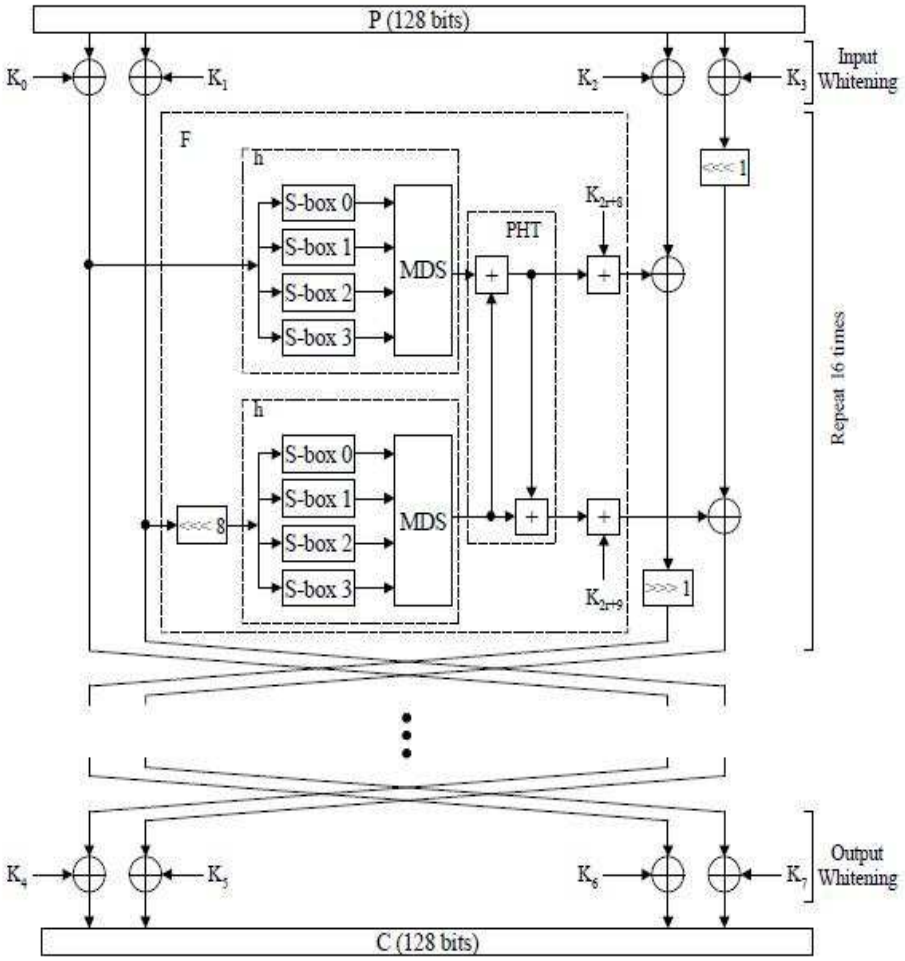
Zaprezentowane na powyższych rysunkach wydajności prezentowanych algorytmów w przypadku realizacji sprzętowej będą się nieznacznie różnić.

3. SPRZĘTOWA REALIZACJA ALGORYTMÓW

Do większości wymienionych w artykule algorytmów AES zostały opracowane modele w języku VHDL. Większość opracowanych układów szyfrujących [4] rozpowszechniana jest w oparciu o licencję GPL, co umożliwia dowolne wykorzystanie w realizowanych projektach. W ramach prowadzonych badań autor przetestował układ szyfrowania i deszyfrowania oparty na algorytmie TwoFish. Na rys 5 pokazano schematycznie S-box, rys.6. przedstawia schemat blokowy algorytmu.



Rys.5 Schemat S-boxów [5]



Rys.6 Schemat blokowy algorytmu TwoFish [5]

4. WNIOSKI

Zastosowanie układów FPGA do kodowania i dekodowania informacji w systemach kryptograficznych pozwala na realizację procesu szyfrowania i deszyfrowania w czasie rzeczywistym także dla sygnałów wizyjnych. Rozwiązanie to pozwoli zwiększyć bezpieczeństwo w systemach alarmowych i monitoringu, szczególnie przy znacznych odległościach chronionych obiektów lub przy transmisji radiowej. Przesyłanie informacji bez szyfrowania jest narażone na złośliwą ingerencję, zmniejszającą bezpieczeństwo systemu.

5. BIBLIOGRAFIA

[1] Mochnacki W.: *Kody korekcyjne i kryptografia* , Oficyna Wydawnicza Politechniki Wrocławskiej. Wrocław 2000
[2] Kutyłowski M., Strothmann W.B.: *Kryptografia teoria i praktyka zabezpieczenia systemów komputerowych* , Oficyna Wydawnicza Read Me Warszawa 1998
[3] http://csrc.nist.gov/archive/aes/index.html
[4] www.opencores.org
[5] www.schneier.com/twofish.html