WOJSKOWA AKADEMIA TECHNICZNA

**im. Jarosława Dąbrowskiego**

WYDZIAŁ CYBERNETYKI



##### PRACA DYPLOMOWA

###### STACJONARNE STUDIA I STOPNIA

Temat: **SPRZĘTOWA IMPLEMENTACJA WYBRANYCH ALGORYTMÓW MNOŻENIA W PIERŚCIENIACH Zn ORAZ ANALIZA ICH PRZYDATNOŚCI W PEWNYCH ZASTOSOWANIACH KRYPTOGRAFICZNYCH**

|  |  |
| --- | --- |
| Autor: | Kierownik pracy: |
| **Michał DASZCZUK** | **dr inż. Piotr BORA** |

W a r s z a w a 2015

Spis treści

[Wstęp 5](#_Toc435659526)

[Rozdział I. Podstawowe własności pierścieni Zn. 6](#_Toc435659527)

[1.1 Grupy 6](#_Toc435659528)

[1.2 Pierścienie 6](#_Toc435659529)

[1.3 Relacja przystawania modulo n 7](#_Toc435659530)

[1.5 Pierścienie Zn 8](#_Toc435659531)

[Rozdział II. Zastosowania pierścieni Zn w wybranych algorytmach kryptograficznych. 11](#_Toc435659532)

[2.1 RSA 11](#_Toc435659533)

[2.2 Digital Signature Algorithm (DSA) 11](#_Toc435659534)

[Rozdział III. Sprzętowe algorytmy mnożenia w pierścieniach Zn. 13](#_Toc435659535)

[Rozdział IV. Opis implementacji w strukturach programowalnych wybranego algorytmu kryptograficznego wykorzystującego mnożenie w pierścieniach Zn. 14](#_Toc435659536)

[Rozdział V. Analiza uzyskanych wyników. 15](#_Toc435659537)

[Zakończenie 16](#_Toc435659538)

[Bibliografia 17](#_Toc435659539)

# Wstęp

Ciągły rozwój techniki i komputeryzacja każdego z aspektów naszego życia ciągną za sobą potrzebę zabezpieczenia przekazywanych informacji. Z powodu szybkiego rozrastania się sieci Internet oraz dużej ilości wymienianych informacji przez otwarte sieci, systemy kryptograficzne zaczęły odgrywać szczególną rolę w życiu każdego użytkownika. Zaistniała potrzeba zabezpieczenia wielu podstawowych działań jak na przykład komunikacja, płatności czy transfery danych. Najlepsze wsparcie w projektowaniu i implementacji aplikacji kryptograficznych oferowane jest przez systemy wbudowane takie jak FPGA (ang. Field-Programmable Gate Array), a wraz z ich wzrastającą wydajnością stały się one kluczowymi elementami implementacji tych systemów.

Wiele współczesnych systemów kryptograficznych wykorzystuje operacje modularne na dużych liczbach całkowitych. Ich implementacja w układach programowalnych stawia przed projektantem wiele wyzwań optymalizacyjnych związanych z ograniczeniami sprzętowymi, ale także rodzi możliwości związane ze zwiększeniem ich wydajności.

Celem niniejszej pracy jest charakterystyka, opis implementacji oraz analiza przydatności wybranych sprzętowych algorytmów mnożenia w pierścieniach w zastosowaniach kryptograficznych.

# Rozdział I. Podstawowe własności pierścieni Zn.

Zacznijmy od zdefiniowania podstawowych pojęć niezbędnych do określenia pojęcia pierścienia .

## 1.1 Grupy

**Definicja 1.1.** Struktura algebraiczna jest nazywana grupą jeśli działanie w zbiorze spełnia następujące warunki:

1. łączność
2. istnieje element neutralny taki, że
3. istnieje element odwrotny (przeciwny) dla każdego elementu w

Jeżeli dodatkowo działanie jest:

1. przemienne  
   to jest grupą przemienną (abelową).

## 1.2 Pierścienie

**Definicja 1.2.** Struktura algebraiczna jest nazywana pierścieniem, jeśli działanie addytywne oraz działanie multiplikatywne w zbiorze spełniają następujące warunki:

1. jest grupą abelową (grupa addytywna pierścienia ),
2. działanie jest łączne,
3. działanie jest rozdzielne względem działania +

Jeśli dodatkowo:

1. działanie jest przemienne, to określa się jako pierścień przemienny,
2. istnieje element neutralny działania (jedynka pierścienia )

to nazywamy pierścieniem z jedynką.

**Twierdzenie 1.1.** Niech będzie pierścieniem. Wtedy:

1. element neutralny jest unikalny,
2. element neutralny działania (zero pierścienia ) spełnia zależność:
3. elementy pierścienia oraz elementy do nich przeciwne spełniają zależność:

oraz

1. dla dowolnej wartości skalarnej zachodzi zależność:

## 1.3 Relacja przystawania modulo n

W zbiorze liczb całkowitych wprowadzamy relację przystawania modulo zdefiniowaną jako:

**Twierdzenie 1.2.** Relacja przystawania modulo jest relacją równoważności.  
Dowód.  
Niech . Wtedy:

1. zwrotność  
   ponieważ
2. symetria  
   wtedy
3. przechodniość  
   wtedy stąd odejmując od siebie równania otrzymujemy

Relacja przystawania modulo jest relacją równoważności, zatem dzieli zbiór liczb całkowitych na klasy abstrakcji (równoważności). Klasy równoważności są postaci

a zbiór klas abstrakcji to

## 1.5 Pierścienie Zn

Po ogólnym scharakteryzowaniu pierścieni możliwe jest wprowadzenie pojęcia pierścienia .

**Twierdzenie 1.3.** Struktura algebraiczna , gdzie

jest pierścieniem przemiennym z jedynką.

Dowód.  
Niech wtedy dla działania zachodzą następujące własności:

1. przemienność  
   gdzie - reszta z dzielenia modulo
2. łączność  
   Analogicznie  
   stąd
3. istnieje element neutralny
4. istnieje element przeciwny

oraz  
zatem

Stąd struktura jest grupą abelową.

Następnie dla działania zachodzą następujące własności:

1. przemienność
2. łączność
3. rozdzielność działania względem działania
4. istnieje element neutralny (jedynka pierścienia)

Z powyższych własności wynika, że struktura algebraiczna jest pierścieniem przemiennym z jedynką.

# Rozdział II. Zastosowania pierścieni Zn w wybranych algorytmach kryptograficznych.

Pierścienie ze względu na swoje własności zaprezentowane w poprzednim rozdziale znalazły zastosowanie głównie w algorytmach kryptograficznych opartych na problemie faktoryzacji i pokrewnych.

## 2.1 RSA

Asymetryczny algorytm z kluczem publicznym używany zarówno do szyfrowania, jak i do tworzenia podpisów cyfrowych. Do dzisiaj jest najbardziej popularnym algorytmem, nie tylko z powodu jego prostoty, ale także łatwości implementacji.

Bezpieczeństwo algorytmu opiera się na trudności faktoryzacji dużych liczb. Aby wygenerować klucze publiczny i prywatny, należy wybrać dwie duże liczby pierwsze,  i , a następnie obliczyć ich iloczyn . Klucz szyfrujący należy wybrać, tak aby był względnie pierwszy z . Wtedy, w celu obliczenia klucza deszyfrującego , rozwiązujemy równanie modularne postaci:

a zatem

Otrzymane w ten sposób pary oraz są odpowiednio kluczem publicznym i prywatnym.

Szyfrowanie z użyciem algorytmu RSA polega na podzieleniu tekstu jawnego w postaci binarnej na bloki takiej samej długości, których wartość liczbowa jest mniejsza niż . Szyfrogram jest tej samej postaci i otrzymuje się go przez obliczenie:

Aby odszyfrować wiadomość należy wykonać podobne działanie z kluczem prywatnym:

Powyższe równości są spełnione ponieważ:

stąd również wynika, że tekst mógłby zostać zaszyfrowany kluczem i odszyfrowany kluczem

## 2.2 Digital Signature Algorithm (DSA)

Algorytm służący do generacji podpisu cyfrowego z kluczem publicznym zaproponowany przez NIST (The National Institute of Standards and Technology) jako algorytm spełniający standard DSS (Digital Signature Standard). Bezpieczeństwo podpisu opiera się na trudności obliczenia logarytmu dyskretnego [2].

Przed generacją podpisu należy zdefiniować następujące parametry:

1. - liczba pierwsza z przedziału , gdzie jest wartością z przedziału od 1024 do 3072,
2. - dzielnik pierwszy liczby , gdzie i jest wartością z przedziału od 160 do 256,
3. - generator podgrupy rzędu q grupy multiplikatywnej , gdzie .

Standard także określa wybór wartości L w zależności od N jak poniżej:

Kluczem prywatnym jest dowolna wartość mniejsza od , z której obliczamy klucz publiczny . Należy zaznaczyć, że wszystkie parametry poza są jawne.

Podpisywanie wiadomości przebiega według poniższej listy kroków [1]:

1. Wygenerowanie losowej i unikalnej dla każdej wiadomości liczby takiej, że
2. Obliczenie pary , która jest podpisem cyfrowym

gdzie jest funkcją skrótu o rozmiarze wyjściowym równym .

W celu weryfikacji należy sprawdzić, czy i oraz wykonać szereg obliczeń:

1. .

Jeżeli to podpis jest poprawny.

## 2.3 Rabin

Algorytm Rabin [1] opiera swoje bezpieczeństwo na trudności obliczenia pierwiastka kwadratowego modulo liczba złożona, ponieważ nie istnieje efektywna metoda jego obliczania jeżeli nie znamy czynników pierwszych. Problem jest równoważny z problemem faktoryzacji, gdyż atakujący musi rozłożyć moduł.

W celu zaszyfrowania wiadomości trzeba najpierw wygenerować dwie duże liczby pierwsze  i  kongruentne do 3 modulo 4. Liczby te są kluczem prywatnym, a ich iloczyn jest kluczem publicznym.

Sam proces szyfrowania polega tylko na podniesieniu wiadomości do kwadratu:

Deszyfrowanie wiadomości jest trochę bardziej skomplikowane. Znając tajne czynniki  i  odbiorca jest w stanie obliczyć wartość M korzystając z Chińskiego Twierdzenia o Resztach.

Wtedy obliczamy dwie dodatkowe wartości:

Następnie otrzymujemy cztery możliwe rozwiązania:

Jedno z rozwiązań jest wynikiem i jest równe .

Podstawową i bardzo mocną zaletą algorytmu Rabin jest efektywność szyfrowania i łatwość implementacji. Deszyfracja ma złożoność zbliżoną do RSA, wadą która uniemożliwia wprowadzenie szyfru do użycia jest konieczność rozpoznania, który z wyników jest pożądaną wiadomością. Jeżeli przesyłamy zaszyfrowany tekst w konkretnym języku rozpoznanie nie jest problematycznie, ale jeżeli przesyłany jest losowy ciąg bitów (np. klucz) nie da się przeprowadzić takiej weryfikacji.

# Rozdział III. Sprzętowe algorytmy mnożenia w pierścieniach Zn.

# Rozdział IV. Opis implementacji w strukturach programowalnych wybranego algorytmu kryptograficznego wykorzystującego mnożenie w pierścieniach Zn.

# Rozdział V. Analiza uzyskanych wyników.

# Zakończenie

# Bibliografia

|  |  |
| --- | --- |
| [1] | National Institute of Standards and Technology, NIST FIPS PUB 186-4, "Digital Signature Standard", U.S.: Department of Commerce, 2013. |
| [2] | B. Schneier, "Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C", New York: John Wiley & Sons, Inc., 1996. |
| [3] | H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen i F. Vercauteren, "Handbook of Elliptic and Hyperelliptic Curve Cryptography", Boca Raton: Taylor & Francis Group, 2006. |