Jerzy August Gawinecki, prof. dr hab. n. mat. inż., prof. zw. WAT
Telefon : (022) 683 95 56, E-mail: jgawinecki@wat.edu.pl
Instytut Matematyki i Kryptologii, Wydział Cybernetyki WAT, 00-908 Warszawa,
ul. Kaliskiego 2
IMiK WCY WAT: sekretariat telefon: (022) 683 95 56, faks: (022) 683 79 19

Warszawa, 4.06.2012

RECENZJA ROZPRAWY DOKTORSKIEJ DLA RADY INSTYTUTU PODSTAWOWYCH PROBLEMÓW TECHNIKI POLSKIEJ AKADEMII NAUK

Tytuł rozprawy: **Wydajne metody generowania bezpiecznych parametrów algorytmów klucza publicznego**
Autor rozprawy: mgr **Andrzej CHMIELOWIEC**
Druk: Instytut Podstawowych Problemów Techniki, Polska Akademia Nauk, Warszawa, 2012

1. Uwagi wstępne

Recenzowana rozprawa przedstawiona została w jednym tomie składającym się z 8 rozdziałów (w tym wstęp, podsumowanie oraz rozdziału opisującego wkład własny autora), spisu tablic, spisu rysunków, listy algorytmów, wykazu literatury (64 pozycje) oraz dwóch załączników zawierających opis biblioteki i kody źródłowe. Wolumin składa się ze 120 stron.

2. Dziedzina badań, cel rozprawy

Rozprawa dotyczy zarówno jednego z podstawowych działów kryptologii – kryptografii klucza publicznego, jak również obliczeń numerycznych – Szybkiej Transformaty Fouriera.

W kryptografii klucza publicznego doktorant skupił się na ważnym i coraz powszechniej wykorzystywanym problemie logarytmu dyskretnego w grupie punktów krzywej eliptycznej. Obecnie trudność wyznaczania logarytmu dyskretnego stanowi podstawę bezpieczeństwa powszechnie wykorzystywanych algorytmów podpisu cyfrowego (np. ECDSA) i protokołów uzgadniania klucza (np. ECMQV). Na potrzeby praktycznych zastosowań krzywe eliptyczne muszą charakteryzować się określonymi własnościami.

W procesie generowania bezpiecznych kryptograficznie krzywych zdefiniowanych, nad ciałami prostymi dużej charakterystyki, do wyznaczania rzędu grupy punktów wykorzystywany jest algorytm Schoofa-Elkiesa-Atkina, operujący na wielomianach o współczynnikach całkowitych. Wielomiany te mogą charakteryzować się dużymi współczynnikami i operowanie na nich może być czasowo kosztowne.

Cel rozprawy został przedstawiony w punkcie 1.2. doktorant określił go w następujący sposób:

1) Zaprojektowanie efektywnego, równoległego algorytmu mnożenia wielomianów i szeregów potęgowych z użyciem jednocześnie CRT (Chinese Remainder Theorem) i FFT (Fast Fourier Transform).

2) Zastosowanie opracowanego algorytmu w procesie generowania bezpiecznych kryptograficznych krzywych eliptycznych.

3. Uwagi o rozwiązaniu zadania naukowego

Głównym naukowym zadaniem w pracy było opracowanie nowego równoległego algorytmu mnożenia wielomianów z wykorzystaniem jednocześnie CRT i FFT. W celu realizacji tego zadania autor sformułował i udowodnił następujące twierdzenia:

1. Twierdzenie 7. – twierdzenie o izomorfizmie dwóch pierścieni.

2. Lemat 5. – autor wykazuje, że przy spełnieniu pewnych warunków mnożenie wielomianów o współczynnikach z pierścienia $M[X]$, gdzie M jest liczbą całkowitą, daje taki sam wynik jak w przypadku pomnożenia tych samych wielomianów w $Z[X]$ (brak konieczności wykonywania redukcji modularnych).

3. Twierdzenie 8. – w twierdzeniu tym określone zostały warunki konieczne do poprawnego mnożenia wielomianów z $Z[X]$ w pierścieniu $F_p[X]$.

4. Twierdzenie 9. – jest to twierdzenie o złożoności obliczeniowej algorytmu mnożenia wielomianów o współczynnikach całkowitych z wykorzystaniem FFT opartego o Twierdzenie 8.

5. Twierdzenie 10. – określa ono warunki jakie muszą być spełnione aby zaproponowany przez autora algorytm mógł być zastosowany. Twierdzenie to jest podobne do Twierdzenia 8., jednak uzasadnia poprawność wykorzystania CRT w trakcie obliczeń.

6. Twierdzenie 11. – jest to twierdzenie o złożoności obliczeniowej proponowanego przez autora algorytmu. Dzieki temu możliwe było porównanie złożoności obliczeniowej tego rozwiązania z rozwiązaniem, do którego odnosi się Twierdzenie 8. oraz powszechną metodą wykorzystującą FFT.

W Rozdziale 5., w oparciu o udowodnione twierdzenia doktorant zaproponował własny algorytm pozwalający na szybkie mnożenie wielomianów o współczynnikach całkowitych. W swoim rozwiązaniu doktorant wykorzystał:

- Chińskie Twierdzenie o Resztach pozwalające z jednej strony na zrównoleglenie obliczeń, jak i na operowanie na wielomianach o mniejszych współczynnikach;

- Szybką Transformatę Fouriera stosowaną do efektywnego mnożenia wielomianów w podpierścieniach wyjściowego pierścienia.

Złożoność obliczeniowa zaproponowanego algorytmu została określona w Twierdzeniu 11. Istotnym wynikiem doktoranta jest Wniosek 2. do powyższego twierdzenia. Wskazuje

on na mniejszą złożoność zaproponowanego rozwiązania ($O(n \log^2 n)$) niż złożoność „klasycznego" algorytmu wykorzystującego FFT ($O(n \log^2 n \log \log n)$) przy spełnieniu dodatkowego warunku (w przypadku algorytmu Schoofa i Elkiesa warunek ten jest najczęściej spełniony).

Kolejnym celem pracy było wykonanie praktycznej implementacji opracowanej przez Autora metody mnożenia. Autor uwzględnił w tym miejscu architekturę współczesnych komputerów (32-bitowe i 64-bitowe procesory). Z praktycznego punktu widzenia ważnym elementem pracy jest porównanie czasów realizacji implementacji opracowanego algorytmu z „klasycznym" rozwiązaniem wykorzystującym FFT. Wyniki porównania doktorant przedstawił w Tablicach 6.1 i 6.2. Na uwagę zasługują wartości parametrów T_1/T_2 i T_2/T_3 określające, odpowiednio, stosunki czasów wykonywania się kolejno trzech algorytmów: powczechnie wykorzystywanego algorytmu bazującego na FFT, metody doktoranta uruchamianej na jednym rdzeniu procesora i tej samej metody wykonywanej równolegle na czterech rdzeniach procesora. Zarówno w przypadku współczynników wielomianów ze zbioru $\{0, 1, \ldots, 2^{256} - 1\}$, jak i $\{0, 1, \ldots, 2^{512} - 1\}$ otrzymane przez doktoranta wyniki pokazują:

- znaczne przyspieszenie obliczeń (parametr T_1/T_2) przy zastosowaniu metody doktoranta.
- duże wykorzystanie mocy obliczeniowej procesora wielordzeniowego (parametr T_2/T_3). Dla danych testowych najmniejsza otrzymana wartość tego parametru wyniosła 3.1, co oznacza wykorzystanie mocy testowego procesora w minimum 77.5%.

4. Uwagi krytyczne, uwagi o redakcji pracy

Rozprawa napisana jest w sposób wskazujący na to, że doktorant dogłębnie przeanalizował zarówno dziedzinę badań, jak i postawione cele pracy. Rozważania przedstawione zostały w sposób uporządkowany. Sformułowane przez doktoranta twierdzenia i lematy zostały dowiedzione.

Opracowane algorytmy i metody zostały jasno i precyzyjnie opisane. Wnioski wynikające z porównania metody opracowanej przez doktoranta z istniejącymi są poprawne i wskazują na zalety nowego rozwiązania.

Do pracy mam następujące uwagi:

1. Str. 7. – w definicji logarytmu dyskretnego nie jest oczywiste czy liczba oznaczona przez x istnieje. Element $h \in G$ nie musi należeć do podgrupy cyklicznej generowanej przez element g.
2. Str. 8. – pojęcia „operacja prywatna" i „operacja publiczna" nie są zdefiniowane.
3. Str. 10. – doktorant opisuje podział procesu generowania krzywej eliptycznej do zastosowań kryptograficznych. Proces ten nie musi przebiegać w ten sposób, szczególnie gdy ciało bazowe ma charakterystykę równą 2.
4. Str. 31. – brak określenia, co oznacza $[x]G$.
5. Str. 34. – określenie funkcji $KDF_G : G \mapsto \{0,1\}^*$ sugeruje, że zbiorem wartości funkcji są ciągi binarne o dowolnej długości, gdzie według doktoranta długość jest zadana.

6. Str. 36., 37. – w opisie algorytmu ElGamala o rzędzie n grupy $< G >$ nie czynione są żadne założenia, podczas gdy wykonalność działań algebraicznych wymaga pierwszości liczby n.

7. Str. 37., 38. – brak założeń pozwalających na istnienie, a w konsekwencji wykonalność wyznaczenia odwrotności modularnej na potrzeby algorytmu DSA.

8. Str 43. – brak założenia o pierwszości rzędu generatora podgrupy cyklicznej (w pracy oznaczonego przrz n). W przypadku, gdy n jest liczbą złożoną, to zastosowanie, przy obliczaniu logarytmu dyskretnego, ma także algorytm Pohliga-Hellmana.

9. Str. 76. – w dowodzie Lematu 7. w równości

$$(D \cdot B + R) \ mod \ C = (D \ mod \ C)(B \ mod \ C) + (R \ mod \ C)$$

jest przeoczenie. Powinno być:

$$(D \cdot B + R) \ mod \ C = (((D \ mod \ C)(B \ mod \ C)) \ mod \ C) + (R \ mod \ C).$$

10. Brak formalnej definicji Dyskretnej i Szybkiej Transformaty Fouriera.

11. Przy porównaniu szybkości działania algorytmów mnożenia wielomianów doktorant przedstawił otrzymane czasy, ale nie zaprezentował metody ich wyznaczania. Z pracy nie wynika, czy dla danego stopnia wielomianów wykonywane było mnożenie dla jednej pary wielomianów, czy też dla większej liczby, a podany czas jest średnim czasem wykonania algorytmu. Doktorant nie podaje także, w jaki sposób generowane były dane wejściowe.

5. Wnioski końcowe

Na podstawie przedstawionej powyżej oceny rozprawy doktorskiej mgr. Andrzeja Chmielowca stwierdzam, że:

1. Recenzowana rozprawa stanowi oryginalne rozwiązanie zadania opracowania metody mnożenia wielomianów o współczynnikach całkowitych. Metoda doktoranta, wykorzystująca zarówno Szybką Transformatę Fouriera, jak i Chińskie Twierdzenie o Resztach, pozwala na zrównoleglenie obliczeń, co stanowi jej ogromną zaletę. Pozwala na wykorzystanie potencjału stosowanych powszechnie komputerów z procesorami wielordzeniowymi). Opracowana metoda znajduje zastosowanie w procesie generowania bezpiecznych kryptograficznie krzywych eliptycznych. Może być także stosowania wszędzie tam, gdzie zachodzi konieczność wykonywania działań na wielomianach spełniających założenia proponowanej metody.

2. Doktorant wykazał bardzo duży stopień wiedzy w zakresie kryptologii, algebry, teorii liczb i obliczeń numerycznych. Potwierdził umiejętność samodzielnego rozwiązywania zagadnień naukowych i prowadzenia pracy naukowej. Uwagi wyszczególnione przez mnie w poprzedniej części recenzji nie wpływają na pozytywną ocenę rozprawy.

3. Opiniowaną rozprawę oceniam bardzo wysoko: stwierdzam, że odpowiada ona warunkom określonym w art. 13 ust. 1 Ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki (Dz.U. z 2003 r. Nr 65, poz. 595) stawianym rozprawom doktorskim w dyscyplinie naukowej informatyka w dziedzinie nauk technicznych i wnioskuję o jej dopuszczenie do publicznej obrony.

DYREKTOR INSTYTUTU
MATEMATYKI I KRYPTOLOGII
WYDZIAŁU CYBERNETYKI WAT

prof. zw. dr hab. inż. Jerzy GAWINECKI