Prof. dr hab. inż. Zbigniew Kotulski,

Instytut Telekomunikacji Politechniki Warszawskiej

Warszawa, 6 czerwca 2012 r

RECENZJA ROZPRAWY DOKTORSKIE J DLA RADY NAUKOWEJ INSTYTUTU PODSTAWOWYCH PROBLEMÓW TECHNIKI POLSKIEJ AKADEMII NAUK

Tytuł rozprawy: Wydajne metody generowania bezpiecznych parametrów algorytmów klucza publicznego

Autor rozprawy: mgr Andrzej Chmielowiec

Wstęp

Problem wydajności obliczeń jest jednym z najważniejszych wyzwań współczesnej kryptografii związanym z jej praktycznym wykorzystaniem. Nie chodzi przy tym o wykonanie wielkich obliczeń gdziekolwiek, to znaczy na silnym komputerze. Takie obliczenia są dziś łatwe: dysponujemy superkomputerami, gridami obliczeniowymi lub też siecią komputerową łączącą wiele maszyn i umożliwiająca obliczenia rozproszone. Ważne jest, żeby wydajne obliczenia można było wykonywać w małych urządzeniach (komputerach przenośnych, smartfonach czy wręcz na kartach procesorowych). Takie urządzenia służą obecnie jako punkty dostępowe do dużych systemów i powinny one zapewniać zbliżony poziom bezpieczeństwa jak duże systemy komputerowe. W takim przypadku ważne jest stosowanie wydajnych algorytmów obliczeniowych, które są w stanie realizować obliczenia kryptograficzne w czasie rzeczywistym. Fakt, że obliczeniom poddawane są duże liczby (znacznie większe niż standardowa długość liczb w komputerach), a obliczenia muszą być wykonywane w sposób dokładny, umożliwiający odwracanie operacji, jest dodatkowym wyzwaniem dla projektantów takich algorytmów.

Niniejsza praca jest poświęcona problematyce wydajnych obliczeń arytmetycznych, w szczególności wymagających doboru parametrów algorytmów umożliwiających takie obliczenia. Tym niemniej, tytuł pracy „***Wydajne metody generowania bezpiecznych parametrów algorytmów klucza publicznego***" nie oddaje zbyt precyzyjnie jej treści, a zwłaszcza tematyki oryginalnych wyników uzyskanych w rozprawie. Tytuły przyszłych publikacji naukowych opisujących te wyniki z pewnością będą lepiej dobrane do ich treści.

Struktura rozprawy

Rozprawa doktorska pana mgr. Andrzeja Chmielowca zawiera 8 rozdziałów i 2 dodatki oraz bibliografię liczącą 64 pozycje literatury. Po wstępie (rozdział 1) znajduje się pierwsza część pracy, obejmująca rozdziały 2-4, poświęcona krzywym eliptycznym i kryptografii na krzywych eliptycznych. Druga część rozprawy, czyli rozdziały 5 i 6, dotyczy głównego wyniku, czyli konstrukcji efektywnego algorytmu mnożenia wielomianów nad ciałami skończonymi. Ostatnie dwa rozdziały to podsumowanie, zawierające również wyszczególnienie elementów oryginalnych pracy. Dodatki z kolei to prezentacja biblioteki implementującej algorytmy opracowane w niniejszej rozprawie i kody źródłowe tych algorytmów.

Struktura recenzowanej rozprawy doktorskiej jest nietypowa. Część pracy dotycząca krzywych eliptycznych (bardzo precyzyjnie i wyczerpująco napisana) dominuje w pracy swoją objętością (liczy 44 strony), jednak przy pierwszym czytaniu trudno się zorientować, jaką pełni w niej rolę, praca dotyczy wszak szybkich algorytmów mnożenia wielomianów. Dopiero ostatnie zdanie w części podsumowującej wyjaśnia, że opracowane przez doktoranta algorytmy zostały zaimplementowane w aplikacji komercyjnej realizującej kryptografię na krzywych eliptycznych, dając przyspieszenie obliczeń gwarantujące realną możliwość jej wykorzystanie (jak podaje autor, dla obliczeń wstępnych służących konstrukcji kryptosystemu, jest to skrócenie obliczeń z 648 do 41 godzin, czyli więcej niż o rząd wielkości). Tak więc ta część wstępna ma uzmysłowić czytelnikowi, jakie obliczenia powinny być wykonane, aby można było użyć kryptosystemu (w szczególności, kryptosystemu klucza publicznego) działającego na krzywej eliptycznej.

Druga, oryginalna część pracy, ma w dużej mierze charakter matematyczny. Z precyzją charakteryzującą tę dziedzinę wiedzy, autor przedstawił sformułowanie problemu, a następnie szereg lematów i twierdzeń stanowiących jego rozwiązanie. Wartościowym elementem tej części są też algorytmy opracowane przez magistra Andrzeja Chmielowca, zapisane w postaci pseudokodu. Ważnym elementem pracy są również zaprezentowane w rozdziale 6 wyniki testów obliczeniowych przeprowadzonych na procesorze 32-bitowym, pozwalające ocenić wydajność zaproponowanego rozwiązania.

W dodatkach do pracy załączone zostały pełne biblioteki procedur napisanych w języku C i realizujących mnożenie wielomianów metodą zaproponowaną w rozprawie doktorskiej.

Omówienie i ocena rozprawy

Jak już wspomniałem, pierwsza część pracy jest systematycznym omówieniem problematyki obliczeń na krzywych eliptycznych. Jest napisany bardzo kompetentnie i świadczy o szerokiej wiedzy Doktoranta i jego dużej biegłości w tematyce implementacji algorytmów kryptograficznych na krzywych eliptycznych, jednak jest zbyt obszerny jako jedynie motywacja do podjęcia problematyki szybkiego mnożenia wielomianów. Byłby dobrym wprowadzeniem do szerszej biblioteki algorytmów obliczeniowych dla krzywych eliptycznych (jak już pisałem, pan mgr Andrzej Chmielowiec w oprogramowaniu takiej profesjonalnej biblioteki procedur uczestniczył).

Z kolei w drugiej, oryginalnej części rozprawy brakuje wstępu stanowiącego przegląd metod szybkiego mnożenia dużych liczb (czy też wielomianów wysokiego stopnia). Nie przedstawiono tu zarówno historii rozwoju dziedziny, od pomysłu Gaussa, by w mnożeniu sum dwóch wyrażeń cztery mnożenia zastąpić trzema, do fundamentalnej pracy Karatsuby i Ofmana z 1962 roku z asymptotycznym uogólnieniem idei Gaussa, umożliwiającym zrównoleglenie obliczeń (por. *Dokl. Akad. Nauk SSSR, vol.145, pp. 293-294 (1962)*, przekład angielski: *A. A. Karatsuba and Yu. Ofman.* ***Multiplication of multidigit numbers on automata.*** *Doklady Akademii Nauk SSSR, 7:595–596, 1963*). Brakuje również omówienia współczesnych wyników uzyskanych przez innych autorów. Wsród nowych prac znalazłem doktorat: *Daniel Steven Roche,* ***Efficient Computation with Sparse and Dense Polynomials****, A thesis presented to the University of Waterloo in fulfillment of the thesis requirement for the degree of Doctor of Philosophy in Computer Science, Waterloo, Ontario, Canada, 2011*, zawierający rozdział o mnożeniu wielomianów o współczynnikach całkowitoliczbowych. (W tej pracy celem jest minimalizacja obszaru pamięci wykorzystywanej do obliczeń, jak to wynika z poniższego omówienia treści odpowiedniego rozdziału rozprawy:

"In the area of arithmetic operations, new algorithms are presented for the multiplication of dense polynomials. These have the same asymptotic time cost of the fastest existing approaches, but reduce the intermediate storage required from linear in the size of the input to a constant amount. Two different algorithms for so-called "adaptive" multiplication are also presented which effectively provide a gradient between existing sparse and dense algorithms, giving a large improvement in many cases while never performing significantly worse than the best existing approaches.")

Informacje odzwierciedlające stan sztuki są zwyczajowo przyjętą częścią rozprawy

doktorskiej, zatem odpowiednie opracowanie powinno być do recenzowanej pracy doktorskiej dołączone w formie aneksu. Piszę tu ogólnym przeglądzie stanu badań; w części drugiej rozprawy jest nawiązanie do bezpośrednio rozwijanych wyników i uzyskane rezultaty są dobrze umotywowane. Główny cal rozprawy, jakim było opracowanie nowego wydajnego algorytmu mnożenia wielomianów, został zrealizowany. Mimo iż sama idea wykorzystania Chińskiego Twierdzenia o Resztach i FFT do takiego mnożenia nie jest nowa, to zarówno propozycja ich konkretnego użycia dla zrównoleglenia obliczeń, jak i twierdzenia dotyczące poprawności i wydajności opracowanego algorytmu są oryginalne i wartościowe, co zresztą zostało potwierdzone przez praktyczną implementację algorytmu.

Ważną i oryginalną częścią rozprawy jest kod numeryczny stanowiący profesjonalną bibliotekę do obliczeń na wielomianach. O przydatności tego kodu w praktyce już pisałem. Z punktu widzenia struktury rozprawy doktorskiej (będącej pracą z dziedziny nauk technicznych w dyscyplinie naukowej informatyka), w opisie eksperymentów numerycznych brak jest porównania wydajności przedstawionych procedur z opracowanymi przez innych autorów i dostępnymi publicznie bibliotekami (wykorzystującymi różne, inne niż w recenzowanej rozprawie, procedury przyspieszania obliczeń). Znalazłem na przykład bibliotekę:

David Harvey. zn_poly: a C library for polynomial arithmetic in Z/nZ[x].

Online, ***http://web.maths.unsw.edu.au/~davidharvey/code/zn_poly/****. Version 0.9.*

do szybkich obliczeń na wielomianach o współczynnikach w ciele skończonym. Zaprogramowana tam procedura mnożenia używa kombinacji metody Karatsuby-Ofmana, podstawienia Kroneckera i FFT w wersji Schoenhage-Nussbaumera. Uważam, że rozprawa powinna być uzupełniona o porównanie wydajności zaproponowanego algorytmu z propozycjami innych autorów. Dotyczy to zwłaszcza porównań dla wielomianów stopni różnego rzędu: w literaturze przyjęte jest, że FFT jest bardziej wydajna jedynie dla liczb/wielomianów rzędu tysięcy cyfr, a CRT – rzędu setek tysięcy cyfr. Dlatego też warto porównać wydajność mnożenia dla różnych schematów zrównoleglenia obliczeń i różnych rzędów mnożonych liczb (czy też stopni mnożonych wielomianów).

Podsumowując tę część recenzji chciałbym podkreślić, że mimo przedstawionych wyżej braków, które traktuję jako usterki formalne, praca stanowi kompletne, matematycznie poprawne i spójne rozumowanie zawierające zarówno precyzyjne sformułowanie problemu, jak i jego pełne rozwiązanie.

Podsumowanie

W swojej rozprawie doktorskiej pan mgr Andrzej Chmielowiec zaproponował nową konstrukcję algorytmu mnożenia wielomianów wysokiego stopnia nad ciałem skończonym pozwalającą na równoczesne zrównoleglenie obliczeń (dzięki wykorzystaniu CRT) i ich przyspieszenie w każdym procesorze w stosunku do obliczeń tradycyjnych (dzięki FFT). Uzyskane wyniki są wartościowe z teoretycznego punktu widzenia (przedstawione zostały twierdzenia potwierdzające poprawność obliczeń równoległych, poprawność wykorzystania zaproponowanej wersji algorytmu szybkiej transformaty Fouriera oraz oszacowanie złożoności obliczeniowej zaproponowanego schematu). Ważnym wynikiem pracy jest też kod procedur napisany w języku C, zarówno jako narzędzie do testów algorytmów, jak i produkt finalny przydatny w aplikacjach kryptograficznych.

Uważam, że dla pełniejszej oceny w czasie publicznej obrony uzyskanych wyników na tle prac innych autorów, niezbędne jest uzupełnienie tekstu rozprawy o opis stanu sztuki w zakresie mnożenia wielomianów (lub szerzej, także dużych liczb naturalnych) oraz porównanie opracowanych procedur z procedurami dostępnymi publicznie a korzystającymi z alternatywnych rozwiązań.

Rozprawę doktorską pana magistra Andrzeja Chmielowca oceniam bardzo wysoko. Uważam, że wyniki naukowe w niej uzyskane spełniają wymagania stawiane przez Ustawę rozprawom doktorskim w dyscyplinie naukowej informatyka w dziedzinie nauk technicznych i wnioskuję o jej dopuszczenie do publicznej obrony.

Prof. dr hab. inż. Zbigniew Kotulski

Kotulski