Раздел 3. «Информационно-коммуникационные технологии»

ҒТАМР 28.23.15
ӘОЖ 004.056.55

DOI: 10.53002/075

Д.М. Амангельды, В.Д. Николенко

Карагандинский индустриальный университет, г. Темиртау
(E-mail: v.nikolenko@tttu.edu.kz)

FPGA негізіндегі эллиптикалық қисықтарды есептеу

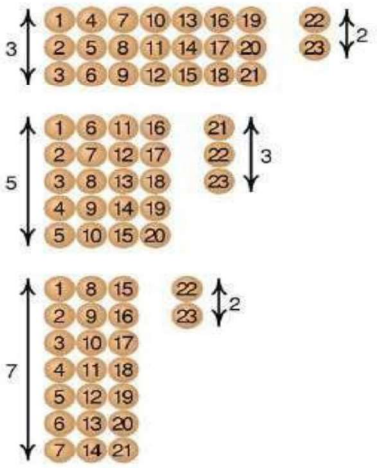
Мақала мәндердің шекті өрісі жағдайында өнімділікте артықшылығы бар қалдық кластар жүйесінде есептеу принциптерін қолданатын есептеу әдістеріне арналған. Қолданудың мүмкін аймақтары сипатталып, есептеулерді оңтайландыру қажеттілігі негізделеді. Есептеу құрылғысы ретінде FPGA көмегімен әдісті тестілеу туралы ақпарат берілген.

Түйін сөздер: Галуа алгебрасы, қалдық класс жүйесі, эллиптикалық қисықтар, FPGA.

Кіріспе

Мәліметтердің үлкен көлемін параллельді есептеудегі қиындықтардың бірі деректердің алатын жады көлемі болып табылады. Екілік логикадағы есептеу процесі, әдетте, қосқыштарды қолдануға және/немесе деректерді разрядқа ауыстыруға байланысты: осылайша, өңделетін санның кейбір биттері мүлдем пайдаланылмауы мүмкін. Бірдей нәтижені сақтай отырып өңделетін деректер көлемін азайтудың бір жолы модульдік алгебраға негізделген санау жүйесін пайдалану болып табылады.

Сандарды ұсынудың бұл түрі шамамен 3-5 ғасырларда математик Сун Цзы түсіндірген қытайлық қалдық теоремасына негізделген. н.е. және З.Цзюшао 1247 жылы өзінің «9 тараудағы математикалық пайымдау» еңбегінде жазып алған.Бұл теорема бойынша кез келген санды берілген өзара жай бөлгіштер санына бөлуден алынған қалдықтар жиыны ретінде көрсетуге болады және бұл жиын бір сан үшін бірегей болады (1-сурет).



Сурет 1. 23 санын RNC {2, 3, 2} мод {3, 5, 7} ретінде көрсететін Сунь Цзы қытайлық қалдық теоремасының бастапқы тұжырымы.

Әлбетте, қалдық жиынының элементтері олардың сәйкес бөлгіштерінен кішірек болады: осылайша, үлкен санды кішірек сандар жиыны ретінде көрсетуге болады, олар биттердің аз мөлшерін алады және табиғи түрде арифметикалық амалдарды орындау процесін тездетеді. Санды КОК түрінде көрсетудің ерекшелігі қосу, алу және көбейтудің арифметикалық амалдары құрамдас бөлікте орындалады, бұл есептеулерді параллельдеу мүмкіндіктерін кеңейтеді.

Раздел 3. «Информационно-коммуникационные технологии»

Санды СОК көрсетуінен классикалық түрге түрлендіру алгоритмдері бар, мысалы, есептеу күрделілігі бар Гарнер алгоритмі. Сандарды салыстыру мүмкіндігін қамтамасыз ету үшін позициялық санау жүйесіне және кері түрлендіру алгоритмдері жылдам орындалатын жұптық өзара жай сандар жиынын қолдануға болады. Мұндай сандардың ең танымал жиындарының бірі {2n-1, 2n, 2n+1} [1, б. 12].

Қолдану аймақтары. Параллельді есептеу тапсырмалардың кең ауқымында, мысалы, деректерді қорғау және түрлендіру алгоритмдерін әзірлеуде, нейрондық және жасанды интеллект жүйелері үшін үлгіні тану, кескінді цифрлық сүзу және мүмкіндіктерді шығару, автономды көліктердің траекториялары мен бағыттарын есептеуде қолданылады.

Мұндай есептеулердің энергия тиімділігінің негізгі шектеулерінің бірі дискретті ортогоналды түрлендірулердің жоғары есептеу күрделілігі болып табылады [2, б. 6], оның практикалық жүзеге асырылуы негізгі математикалық операциялардың үлкен санын жүзеге асыруды көздейді. Қалдық класс жүйелерін қолдану арқылы есептеулерді пайдалану параллелизмнің жоғары деңгейіне қол жеткізуге мүмкіндік береді және оларды жүзеге асыру үшін мамандандырылған есептеу құрылғысын құруды жеңілдетеді. RNS үшін Галуа алгебрасындағы амалдардың шағын разрядтылығы кестені іздеу схемалары негізінде арифметикалық амалдарды орындауға мүмкіндік береді.

Алгебра және Галуа өрістерін қолданудың ерекше жағдайы эллиптикалық қисықтардағы амалдарды қолданатын есептеулер болып табылады. FPGA негізіндегі бұл алгоритмдердің аппараттық түсіндірмесі энергияны үнемдейтін автономды есептеу жүйелерімен шешілетін мәселелердің кең ауқымы үшін қызығушылық тудырады, атап айтқанда ауыстыру кестесі әдістеріне негізделген.

RNS негізіндегі түрлендіру алгоритмі. Эллиптикалық қисықтар – жазықтықтағы геометриялық қисықтардың ерекше түрі. Олар мына түрдегі теңдеумен анықталады:

$$Y^2 = x^3 + ax + b,$$

мұндағы a және b нақты қисық сызықты сипаттайтын параметрлер.

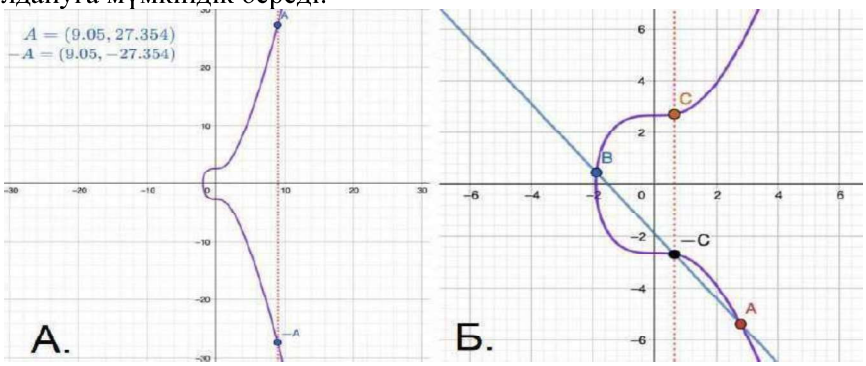
Бұл қисықтардың есептеу тиімділігін арттыратын бірқатар қасиеттері бар (2-сурет):

1. X осіне қатысты симметрия: R(x, y) нүктесі болса,

кері –R(x, –y) нүктесінің координаталарын есептеуге болады.

2. Эллиптикалық қисықтағы нүктелерді қосу заңы: A және B нүктелері арқылы өтетін түзу қисық сызықты тура бір C нүктесінде қиып өтеді. Кері C нүктесі C = A + B тең деп алынады.

Осылайша скалярға инверсия, қосу және көбейту амалдары анықталады. Эллиптикалық кеңістіктегі нүктені скалярға көбейтуге кері операция жоқ, бұл бұл процесті деректерді шифрлау үшін криптографияда қолдануға мүмкіндік береді.



Сурет 2. Графикалық бейнелер: а) симметрия мен кері нүктенің анықтамасы б) қосу амалының анықтамасы.

SOC пайдаланған жағдайда эллиптикалық қисықтардың қасиеттері келесідей толықтырылады:

1. Кері -A нүктесінің координатасы (-1 mod p) көбейтіндісіне тең, мұндағы p - ROC негізі. Осылайша, -A координаталары (x, y mod p) тең болады,

2. A(x, y) = A(x, k + y), мұндағы k - p санының бүтін еселігі.

Кейбір криптографиялық кілттің қатысуымен кері процесті орындауға мүмкіндік беру үшін эллиптикалық қисық сызықтардағы алгебралық есептеулерді Галуа кеңістігі деп те аталатын шекті

өрістер құрылымына ауыстыруға болады. Бұл алгебралық құрылымда қосу және көбейту амалдары элементтердің ақырлы жиыны арқылы анықталады. Өрістің әрбір элементі берілген арифметикалық операция үшін эквиваленттік кластың өкілі болып табылады, мысалы, қалдық кластар жүйелерінде есептеулерді қолдануға мүмкіндік беретін санға бөлудің қалған бөлігі үшін. Осылайша, ақырлы өрістегі эллиптикалық қисық формуласы келесі пішінді алады:

$$y2 \bmod p = (x3 + ax + b) \bmod p,$$

мұндағы p – шекті өрістің ретін анықтайтын негіз, демек, қисық шекті нүктелер жиынының түрін қабылдай алады.

ROC және классикалық санау жүйелері арасындағы түрлендіру. Ақырлы өрісте Галуа алгебрасының есептеулерін қолдануда, негізінен, позициялық және классикалық санау жүйелері арасындағы аудармаға байланысты бірқатар қиындықтар туындайды. ROC негізі кез келген натурал сан болуы мүмкін болғандықтан, санау жүйелері арасында аударудың жалпыланған алгоритмі қажет. Бір санды өзара жай бөлгіштер жиынына бөлудің қалдықтары жиынын табу операциясының бірқатар шешімдері бар, олардың әрқайсысының өзіндік артықшылықтары мен кемшіліктері бар:

1. Қалдықтардың мәндерін бірқатар негіздер бойынша синхронды санау: алгоритмнің логикалық қарапайымдылығымен базаның мәнін өзгерту кезінде қосындылардың басқа санын қосу қажет: операцияның ұзақтығы енгізу операторларының мәндеріне тікелей байланысты,

2. Бөлуден қалдықты алудың аналитикалық процесі: операцияның ұзақтығы база мен бастапқы санның мәндеріне байланысты. Сонымен қатар, бұл әдісті пайдаланып әртүрлі бөлгіштер үшін параллель қалдық есептеулерді жүргізу қиын.

3. Ауыстыру кестесін пайдалану: кіріс аргумент опцияларының аз санымен бұл әдіс ең жылдам болып табылады, өйткені барлық есептеулер кестені құру кезеңінде орындалған, алайда, кестені алып жатқан жады көлемі артады және онымен бірге қажетті кесте мәнін іздеу қажеттілігіне байланысты өнімділік төмендейді; Соңғы факторға FPGA матрицасын ақпаратты тасымалдаушы және деректерді өңдеу модулі ретінде пайдалану арқылы қарсы тұруға болады.

Шығару алдында есептеу нәтижесін RNS-тен классикалық санау жүйесіне қайта түрлендіру керек, оны ортогональды матрицалық түрлендірулер арқылы жасауға болады.

Балама ретінде, санның биттерінің санымен анықталатын уақыт ішінде оның қалдықтарының жиынынан бастапқы санды табуға мүмкіндік беретін Гарнер алгоритмін қолдануға болады: RNS-де A саны келесі түрде берілген деп есептейік:

$$A = x_1p_1 + \ldots + x_np_n,,$$

мұндағы xn - pn арқылы бөлгеннен кейінгі қалдық.

Онда RNS абсолюттік мәніне кері сандар жиыны пусть $r_{ij} = (p_i)^{-1}$ болсын.

Содан кейін алгоритмді орындау арқылы A-ны қалпына келтіруге болады (3-сурет):

```
for (int i=0; i<k; ++i) {
        x[i] = a[i];
        for (int j=0; j<i; ++j) {
                x[i] = r[j][i] * (x[i] - x[j]);

                x[i] = x[i] % p[i];
                if (x[i] < 0)  x[i] += p[i];
        }
}
```

Сурет 3. Гарнер алгоритмінің алгоритмдік сипаттамасы.

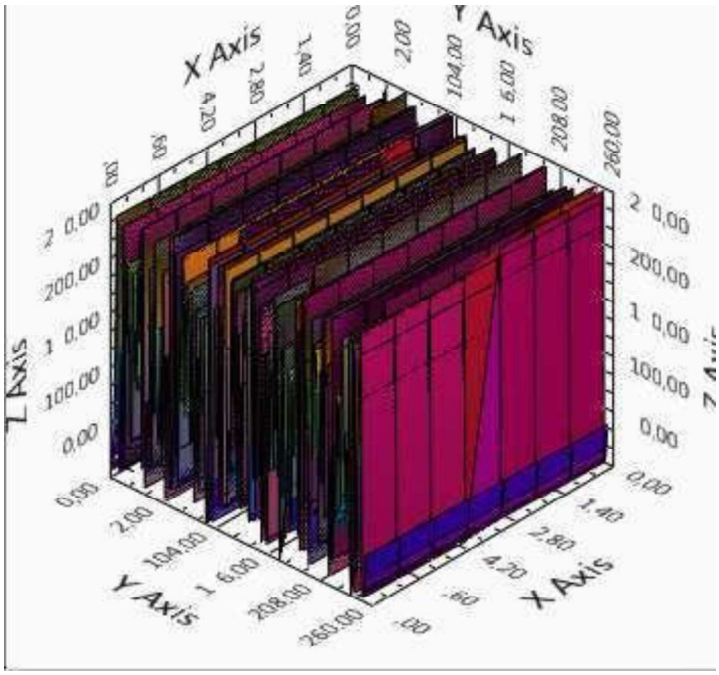
Алгоритмнің күрделілігі O(n2) болып табылады, бұл RNS негіздерінің шағын мәндері бар есептеулерде артықшылық алуға мүмкіндік береді.

Раздел 3. «Информационно-коммуникационные технологии»

Нәтижелерді сынау.

Xilinx Virtex-5 FPGA-мен жабдықталған NI PXIe-7962R модулі алмастыру кестелерін пайдалана отырып, есептеулер көлемін азайту үшін қалдық класс жүйесінің принциптерін пайдалана отырып, эллиптикалық қисық есептеу алгоритмін практикалық жүзеге асыру үшін есептеу құрылғысы ретінде пайдаланылды. Алгоритмнің тиімділігін бағалау үшін 8-биттік айнымалылармен жұмыс істеуге арналған модификация әзірленді (ROC негіздеріне негізделген).

Құрастырылған екі өлшемді ауыстыру кестесі берілген негіздер үшін эллиптикалық қисық мәндерінің барлық ықтимал нұсқаларын қамтиды; Эллиптикалық қисықтар {239 шекті өрісте a, b = {0, 1..7} шегінде қарастырылды. 241. 251}. Бағдарлама берілген санды RNS жиынына аударды, синхронды санау әдісін қолданып эллиптикалық қисық сызықтардағы жүйе элементтерінің мәндерін есептеді және Гарнер әдісі арқылы кері түрлендіруді орындады. 8 разрядты сандар үшін FPGA шинасын синхрондау сигналының генераторының бір циклінде шекті өрісте көбейту-бөлу амалдарын орындау мүмкіндігімен ұсынылған есептеу алгоритмінің тиімділігі көрсетілген. Бұл алгоритмді практикалық қолдану қазіргі уақытта төмен тиімділікпен және сандарды RNS және кері түрлендіру процестерінің жоғары математикалық күрделілігімен қиындады.



Сурет 4. a = 3 үшін эллиптикалық қисығының квадраттық модулінің соңғы өрісіндегі мәндердің матрицасы.

Қорытынды

Ортогональды түрлендірулер үшін жоғары жылдамдықты көбейту-бөлу амалдарының алгоритмдеріне талдау жүргізілді, оны Галуа кеңістігіндегі есептеулерді және қалдық кластар жүйесін қолдану арқылы іс жүзінде оңтайландыруға болады. Зерттеу және оңтайландыру объектісі ретінде эллиптикалық қисық сызықтарға негізделген шифрлау алгоритмі таңдалды, өйткені ROC пайдалану мақсатында ол үшін LUT құрастыру тиімді алгоритмденеді және ROC негізін өзгерту кезінде де, қисық параметрлерін өзгерту кезінде де ұзақ қайталауды қажет етпейді.

Тестілеу барысында GF(2m) Галуа кеңістігіндегі GF(2m) санның RNS-те көрсетілген элементтерінің көбейту-бөлу амалдары шын мәнінде бір уақытта орындалғаны анықталды. Сонымен қатар, бір сан үшін осы операциялардың жалпы орындалу уақыты құрылғының бір тактілік цикліне тең болды. Энергия үнемдейтін графикалық процессорлар мен модульдер үшін FFT модульдерін ағынды есептеу технологиясы бойынша зерттеу нәтижелерін енгізу қызығушылық тудырады.

Раздел 3. «Информационно-коммуникационные технологии»

Әдебиеттер тізімі

1. Финко О.А. Параллель логикалық есептеулердің модульдік арифметикасы: Монография – М.: РҒА ИПУ, 2003. – 214 б;
2. Блейхут Р. Сандық сигналдарды өңдеудің жылдам алгоритмдері. Транс. ағылшын тілінен М.: Мир, 1989. - 448 б;
3. Коблиц Н. Сандар теориясы және криптография курсы: ағылшын тілінен аударма. М.А.Михайлова және В.Е.Тараканов / Ред. Зубкова А.М. — Мәскеу: ТВП Ғылыми баспасы, 2001. — 260 б.

Д.М. Амангельды, В.Д. Николенко

Расчет эллиптических кривых на основе FPGA

Статья посвящена вычислительным методам, использующим принципы расчета в системе классов остатков, которые имеют преимущество в производительности в случае предельного поля значений. Описаны возможные области применения и обоснована необходимость оптимизации расчетов. Информация о тестировании метода с использованием FPGA в качестве вычислительного устройства.

Ключевые слова: алгебра Галуа, система остаточных классов, эллиптические кривые, FPGA.

D.M. Amangeldy, V.D. Nikolenko

Calculation of elliptic curves based on FPGA

The article is devoted to calculation methods that use the principles of calculation in a system of residual classes with an advantage in performance in the conditions of a marginal field of values. Possible areas of application are described and the need to optimize calculations is justified. Information on testing the method using FPGA as a computing device is provided.

Keywords: Galois algebra, residual class system, elliptic curves, FPGA.

References

1. Finko O. A. modular arithmetic of parallel logical calculations: monograph-M.: IPU Ras, 2003. - 214 P.;
2. Bleyhut R. fast algorithms for processing digital signals. Trans. from English M.: Mir, 1989. - 448 P;
3. Koblitz N. Course Number Theory and cryptography: translation from English. M. A. Mikhailova and V. E. Tarakanov / Ed. Zubkova a.m.-Moscow: TVP scientific publishing house, 2001 - 260 P.