

6) $R_{i-1}(32 \cdot n \text{ бит}) - i$ -раунд ўнг қисми.

7) $L_{i-1}^1(32 \text{ бит}), L_{i-1}^2(32 \text{ бит}), \dots, L_{i-1}^n(32 \text{ бит}) - i$ -раунд чап қисмининг 32 битлик бўлаклари.

8) $R_{i-1}^1(32 \text{ бит}), R_{i-1}^2(32 \text{ бит}), \dots, R_{i-1}^n(32 \text{ бит}) - i$ -раунд ўнг қисмининг 32 битлик бўлаклари.

9) $DES(R_{i-1}^1, K_i^1), DES(R_{i-1}^2, K_i^2), \dots, DES(R_{i-1}^n, K_i^n) - i$ -раунд DES алгоритми базавий акслантиришлари.

Такомиллашган DES i -раунди математик модели қуйидагича ифодаланади:

$$\begin{cases} L_i(32 \cdot n \text{ бит}) = R_{i-1}(32 \cdot n \text{ бит}) \\ R_i(32 \cdot n \text{ бит}) = L_{i-1}(32 \cdot n \text{ бит}) \oplus DES(R_{i-1}, K_i)(32 \cdot n \text{ бит}) \end{cases}$$

Такомиллаштириш параметри n га боғлиқ бўлган ҳолда бир неча $DES(R_{i-1}^1, K_i^1), DES(R_{i-1}^2, K_i^2), \dots, DES(R_{i-1}^n, K_i^n)$ акслантиришларидан фойдаланилади. Бу эса n га боғлиқ ҳолда бир неча Фейстел тармоғига асосланган алгоритмлар функцияларидан ёки бир неча S -блоклардан фойдаланиш имконини беради. Шунингдек, n га боғлиқ равишда калит узунликлари ҳам ортиб боради, яъни $n=1$ да калит узунлиги 256 бит бўлса, $n=2$ да калит узунлиги 512 ва ҳаказо бўлади. Калит узунлиги ва такомиллаштириш параметри n орасида қуйидагича боғлиқлик ўрнатиш мумкин:

$$l_1 = l \cdot n$$

бу ерда l – асосий алгоритм калити узунлиги, l_1 – такомиллашган алгоритм калити узунлиги.

Такомиллашган **MDES–TDES** ва **DES** асосий алгоритмларнинг шифрлаш ва дешифрлаш тезлиги тенг, чунки $n=1$ да алгоритм блок узунлиги 64 га тенг бўлиб, алгоритм тезлиги 20 тактдан иборат бўлса, $n=2$ да такомиллашган алгоритм блок узунлиги 128 бит бўлиб, тезлиги 40 тактдан иборат бўлади.

ОЛИЙ АЛГЕБРА КУРСИНИНГ МЕТОДИК ТАЪМИНОТИ УЧУН MAPLE СЕРВИС ПРОЦЕДУРАЛИ КУТУБХОНАСИ

Д.Султонова – ТАТУ ФФ магистранти

Олий алгебра ўқув модули номатематик йўналишлар учун олий математиканинг таркибий ва асосий қисмларидан бири ҳисобланади. Модулнинг асосий мақсади – чизиқли алгебраик тенгламалар назариясини ўрганиш, бевосита олий математиканинг бошқа модулларидаги ва табиий фанлар циклидаги ҳамда кўпсонли тадбикий масалаларнинг ечимини топиши билан алоҳида ўрин тутади.

Бундан ташқари бу модулда матрицаларни ҳисоблаш асослари, детерминатлар назарияси, чизиқли тенгламалар системасининг ечилиш йўллари ва олий математика курсининг бир қатор модулларин элементлари ўрганилади. Ишда компьютер математикаси тизими ҳисобланадиган Maple

тизимида чизиқли алгебра ва аналитик геометрия асосий объектларининг математик ва компьютерли моделлаштириш принциплари кўриб чиқилган.

Хусусан, бу кўрсатилган ишда чизиқли алгебраик тенгламалар системасининг ечимини топишнинг Maple тизимида автоматлаштирилган дастурий таъминоти келтирилган. Лекин ишда дастур процедурасида жиддий камчиликка йўл қўйилган. Жумладан, ўзгарувчилар олдидаги коэффициентларнинг нол қийматлари бўлса, бу ўзгарувчилар эътиборга олинмасдан кетилган, ваҳоланки, мос ҳолдаги ноллар система кенгайтирилган матричасига тушмаган.

Бундан ташқари, бошқа дастурий воситаларда тузилган дастур процедураси чизиқли алгебраик тенгламалар системасининг фундаментал ечимини топишнинг имкониятини бермайди. Maple тизимида тузилган дастур бу ишларни анча енгиллаштиради. Бу ерда қайд этиб ўтиш лозимки, дастурий маҳсулотларни яратишнинг умумий қоидаси ишлаб чиқилган.

Algebra кутубхонасининг SolLinBasics процедураси ёрдамида тенгламалар системасининг фундаментал ечими осон ва элементар тарзда стандарт ва рўйхатли кўринишда топилади.

Қуйида SolLinBasics процедурасини қўллаган ҳолда мисол келтирилган.

Eq3 тенгламалар системасини кўриб чиқамиз:

>Eq3:=[x+2*y-3*z+u-6*t+8*n=1,x-y+2*z-tn=

0,2*x+y-z+3*u-t=1]:

> Algebra[SolLinBasics](Eq3);

$$\left[[0, 2, 1, 0, 0, 0], \left[\frac{-17}{6}, \frac{-23}{6}, 0, 1, \frac{7}{2}, 0 \right], [4, 3, 0, 0, -3, 1] \right].$$

Қурилган процедура кутубхонаси математика махсус фан ҳисобланмайдиган йўналишдаги талабалар учун қулай ва осон ҳисобланади. Бундан ташқари бу ишдан профессор-ўқитувчилар талабаларнинг ёзма иш натижаларини текшириш ва масалаларнинг генерацияси учун ишлатишлари мумкин.

АРХИТЕКТУРА ПРОЦЕССОРА, ОСНОВАННАЯ НА МУЛЬТИКЛЕТОЧНОЙ СТРУКТУРЕ

А.Горовик – ассистент ТУИТФФ, Д.И.Исмоилов – студент ТУИТФФ

«Фон-неймановская» эпоха в компьютерной индустрии завершается. Современная производственная потребность требует новых более совершенных производительных архитектур. Совершенно иная архитектура лежит в основе принципиально нового направления построения процессоров – мультиклеточных процессоров, качественные и количественные характеристики которых позволяют говорить о появлении нового пост-неймановского поколения и которые были подтверждены разработкой первого мультиклеточного процессора МСр0402100100.

Описание алгоритма работы мультиклеточного процессора в виде «триад»