АДАПТИВТІ ЖӘНЕ ҚАЙТА КОДТАУ ӘДІСТЕРІ НЕГІЗІНДЕ M^E ЕСЕПТЕУДІҢ ТИІМДІ АЛГОРИТМДЕРІ

9 - Л Е К Ц И Я

ЛЕКЦИЯ МАҚСАТЫ ЖӘНЕ МАЗМҰНЫ

Мақсаты:Модульдік дәрежеге шығару операциясын оңтайландырудың кеңейтілген әдістерін зерттеу. Көбейту амалдарының санын азайту үшін әртүрлі стратегияларды қарастыру.

Негізгі сұрақтар:

Адаптивті m-арлы әдіс
"Жылжымалы терезелер" тәсілі (CLNW және VLNW)
Кнут ұсынған Фактор-әдіс
Қайта кодтау әдістері және Booth алгоритмі

МӘСЕЛЕ: СТАНДАРТТЫ М-АРЛЫ ӘДІС

Проблема:

Стандартты m-арлы әдіс алдын ала есептеу кезеңінде өте көп көбейту амалын қажет етеді[8]. Ол көрсеткіште кездесуі мүмкін барлық бит-секциялар үшін дәрежелерді есептейді.

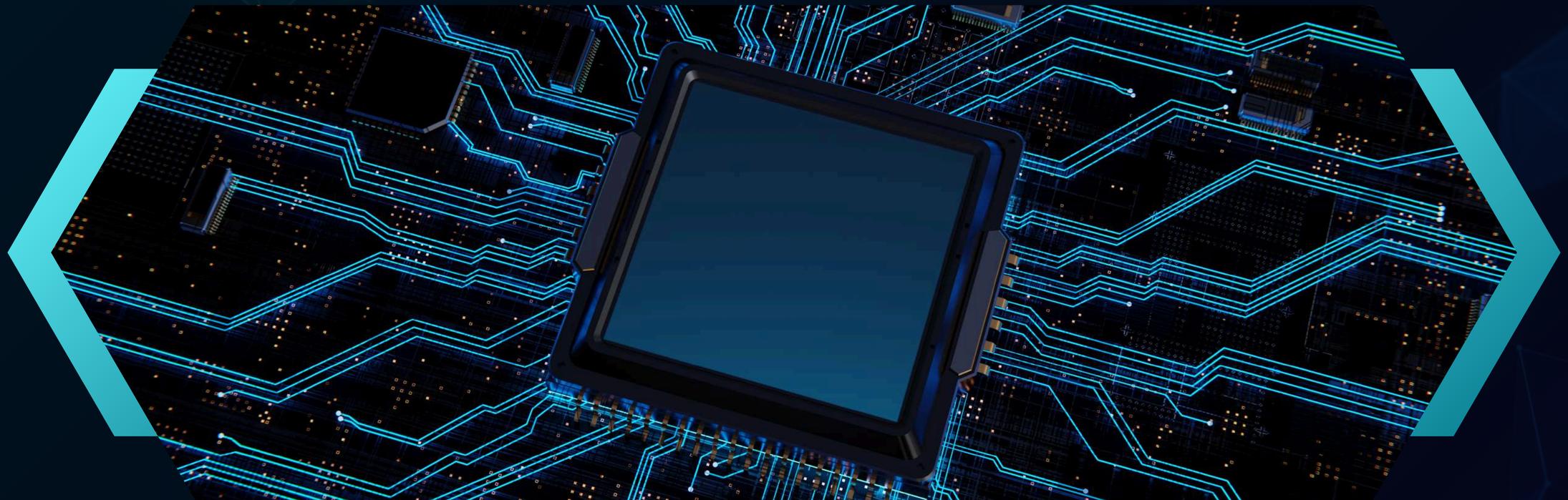
Мысал (d=4 бит секциясы үшін):

Стандартты m-арлы әдіс M^2 , M^3 , ..., M^{15} мәндерін есептеу үшін 14 көбейту амалын қажет етеді.

АДАПТИВТІ М-АРЛЫ ӘДІС

Идея: Алгоритм е көрсеткішінің мәніне тәуелді түрде құрылымын өзгертеді[10]

Шешім:Барлық мүмкін мәндердің орнына, тек көрсеткіште (e) нақты бар бит-секциялар үшін ғана дәрежелерді алдын ала есептеу.



"ЖЫЛЖЫМАЛЫ ТЕРЕЗЕЛЕР" ТӘСІЛІ

01

Негізгі идея:Көрсеткішті (e) нөлдік (ZW) және нөлдік емес (NW) блоктарға (терезелерге) бөлу.

02

Артықшылықтары:
Нөлдік блоктарды тиімді өткізіп жіберу: Нөлдік терезелер кезінде көбейту орындалмайды.
Алдын ала есептеуді азайту: Нөлдік емес терезелер әрқашан '1' битімен аяқталатындай етіп құрылады (яғни, олар тақ сандар).
Нәтиже: Алдын ала есептеулер саны шамамен жартысына қысқарады, себебі тек тақ көрсеткіштері үшін (M^3 , M^5 , M^7 , ...) дәрежелер есептеледі.

CLNW ЖӘНЕ VLNW ӘДІСТЕРІ

01

CLNW (Constant Length Non-Zero Windows):Тұрақты ұзындықты нөлдік емес терезелер.Көрсеткішті d ұзындықтағы нөлдік емес терезелерге және еркін ұзындықтағы нөлдік терезелерге бөледі[20].

02

VLNW (Variable Length Non-Zero Windows):Түрлі ұзындықты нөлдік емес терезелер.
Нөлдік емес терезелердің орташа санын азайтады.

03

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco

ФАКТОР-ӘДІС (КНУТ ӘДІСІ)

Негізгі идея:Көрсеткішті (e) көбейткіштерге жіктеуге негізделген: e = r *s

Процесс:

1. Алдымен $C_1 = M^r \pmod{n}$ есептеледі.
2. Содан кейін $C_2 = (C_1)^s \pmod{n}$ есептеледі.
3. Нәтиже: $(M^r)^s = M^{rs} = M^e$.

Мысал: $e = 55 = 5 \cdot 11$

- Бинарлық әдіс 9 көбейтуді қажет етеді.
- Фактор-әдіс 8 көбейтуді қажет етеді.

ҚАЙТА КОДТАУ ӘДІСТЕРІ

Негізгі идея:Көрсеткішті е "сиретілген" түрде жазу, яғни '1'-лер санын азайту. Бұл үшін {0, 1, -1\}цифрлары қолданылады

BOOTH АЛГОРИТМІ

Қайта кодтаудың кең тараған әдісі. Көрсеткішті оңнан солға қарай сканерлейді.

ҚОРЫТЫНДЫ

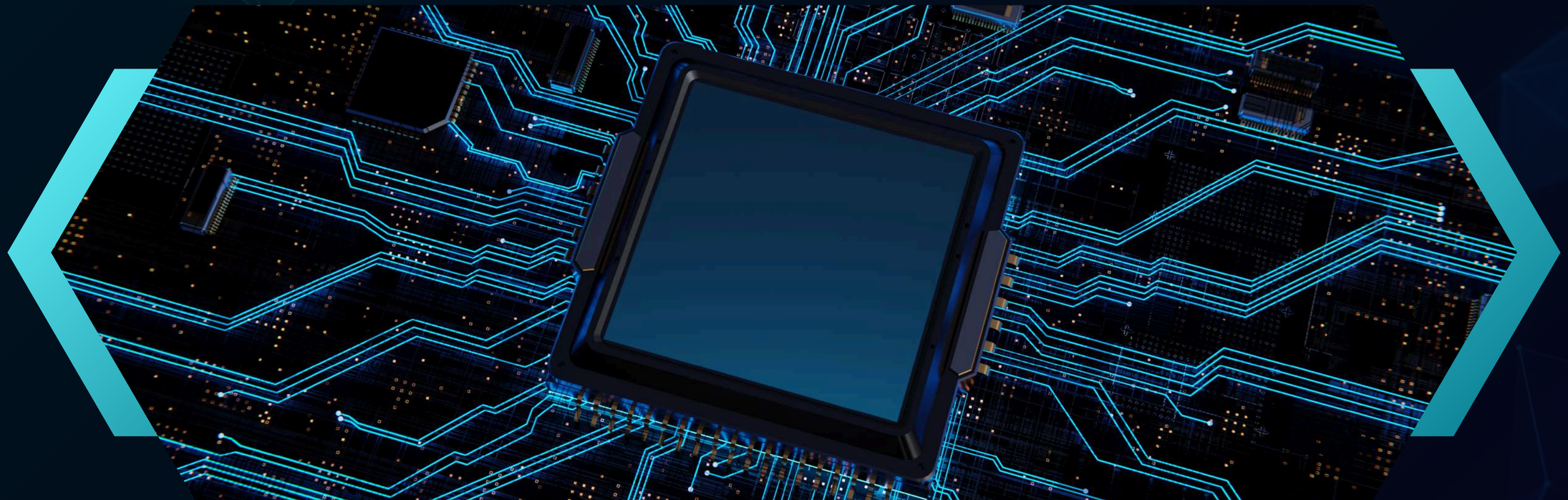
Адаптивті m-арлы әдіс алдын ала есептеулерді тек e көрсеткішінде бар бит-секциялар үшін орындау арқылы үнемдейді[47474747].

"Жылжымалы терезелер" (CLNW, VLNW) нөлдік блоктарды өткізіп жіберуге және тек тақ дәрежелерді алдын ала есептеуге мүмкіндік береді.

VLNW әдісі m-арлы әдіске қарағанда 5.8% тиімдірек[49494949].

Фактор-әдіс тиімді, бірақ сандарды факторизациялау қиындығымен шектеледі.

Қайта кодтау (Booth) $M^{\{-1\}}$ кері мәнін қолданып, '1'-лер санын азайту арқылы көбейтулерді үнемдейді[51515151].



БАҚЫЛАУ СҰРАҚТАРЫ

Адаптивті m-арлы әдіс алдын ала есептеу қадамында көбейту санын қалай азайтады?

"Жылжымалы терезелер" әдісі неліктен алдын ала есептеу үшін тек тақ дәрежелерді (3, 5, 7...) есептеуді талап етеді?

CLNW және VLNW әдістерінің негізгі айырмашылығы неде? Неліктен VLNW тиімдірек?

Фактор-әдістің (Кнут) негізгі кемшілігі неде?

ӘДЕБИЕТТЕР ТІЗІМІ:

1. Knuth, D. E. (1997). The Art of Computer Programming, Volume 2: Seminumerical Algorithms (3rd ed.). Addison-Wesley Professional. (Мәтінде [6] және [15] ретінде сілтеме жасалған негізгі дереккөз).
2. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press. (14-тарау, "Efficient Exponentiation").
3. Bos, J., & Coster, M. (1990). Addition chain heuristics. In Advances in Cryptology — CRYPTO ’89 Proceedings (pp. 400-407). Springer-Verlag. (VLNW әдісін ұсынған авторлар).

THANK YOU