

Лек1. Қауіпсіз сандық жүйелерді
жобалауға кіріспе, Абстракция
деңгейлері, жобалау ағындары,
қауіпсіздікке қойылатын талаптар.

Пәнге кіріспе

Мақсаты: Студенттерді заманауи цифрлық құрылғыларды жобалау әдістерімен, **бағдарламаланатын логикалық интегралдық схемалармен (ПЛИС)**, аппараттық сипаттау тілдерімен (**HDL**), автоматтандырылған жобалау жүйелерімен (**Vivado**) және қауіпсіздікке бағытталған архитектуралармен таныстыра отырып, **CAD** сенімді әрі қауіпсіз сандық жүйелерді құруға қажетті білім мен тәжірибелік дағдыларды қалыптастыру.

Міндеті:

Студенттерден сандық құрылғыларды құру принциптері және аппараттық деңгейде ақпаратты өңдеу принциптері туралы теориялық білім алу және бекіту, есептеудің арифметикалық және логикалық негіздерін үйрету, сандық құрылғылардың құрылыс принциптерін және микропроцессорлық технология негіздерін үйрету. инженерлік ойлау қабілетін, командада жұмыс істей білу және кәсіби этика мәдениетін дамыту.

Білуі керек:

Сандық құрылғыларды жобалау принциптері мен абстракция деңгейлерін; автоматтандырылған жобалау жүйелерінің мүмкіндіктері мен қолдану әдістерін; **аппараттық сипаттау тілдерінің (Verilog)** синтаксисін, жобалау стильдерін және олардың айырмашылықтарын; комбинациялық және тізбекті құрылғылардың жұмыс істеу логикасын; логикалық синтез және оңтайландырудың негізгі тәсілдерін және олардың өнімділікке, қуат тұтынуға және ресурстарға әсерін; **жады құрылғыларының (ROM, RAM, FIFO)** және **интерфейстердің (UART, SPI, I2C)** жұмыс істеу қағидаларын; аппараттық деңгейдегі ақпараттық қауіпсіздік әдістерін, соның ішінде криптографиялық модульдерді, рандом генераторларды және **side-channel attack** шабуылдардан қорғау тәсілдерін; сондай-ақ заманауи архитектуралық трендтерді – RISC-V, жасанды интеллект жеделдеткіштері мен кванттық қауіпсіздікке төзімді жүйелердің ерекшеліктерін.

Қауіпсіз сандық жүйелер маңзы

Қазіргі әлемде цифрлық құрылғыларсыз өмір сүру мүмкін емес. Қажетті деңгейде қорғалмаған жүйе – пайдаланушыға, ұйымға және мемлекетке қауіп төндіреді. Қауіпсіздік тек бағдарламалық деңгейде ғана емес, **аппараттық деңгейде де** қамтамасыз етілуі тиіс. Аппараттық құрал – кез келген жүйенің «іргетасы». Егер аппараттық деңгей бұзылса, ең мықты бағдарламалық **қорғаныс та пайдасыз**. Сенімді процессорлар, криптографиялық модульдер, қауіпсіз жад – негізгі элементтер болып табылады.

Мысал: Смарт-карталар – банк және сәйкестендіру жүйелерінде қолданылады. **IoT құрылғылар** – үй автоматтандырудан бастап, медицинада қолданылады. Өнеркәсіптік контроллерлер (SCADA) – өндіріс пен энергетиканы басқарады.

Сандық жүйелердегі осалдықтар

1. Архитектуралық қателер – дұрыс жобаланбаған архитектура, әлсіз протоколдар

2. Аппараттық **тройндар** – жасырын енгізілген зиянды логика.

“2018 жылы Bloomberg басылымы Қытайдың барлау агенттері Supermicro серверлік платаларына жасырын микрочиптер орнатты деп мәлімдеді. Бұл платалар ірі америкалық компанияларда қолданылған. Кейін бұл ақпарат қызу талқыланып, бір бөлігі дауға айналды”.

3. **Side-channel attack** шабуылдары – қуат, уақыт, электромагниттік сәуле арқылы құпия ақпаратты алу.

“1998 жылы Пол Кочер (Paul Kocher) және әріптестері Differential Power Analysis (DPA) әдісін көрсетті. Олар смарт-картадағы DES шифрлау алгоритмінің құпия кілтін чиптің тұтынатын қуатындағы ұсақ ауытқуларды өлшеп алып шықты. Яғни, құрылғыны бұзбай-ақ, тек ток тұтынуын бақылап отырып кілтті анықтауға болатынын көрсетті”

4. Бағдарламалық қателер – қауіпсіздікке әсер ететін логикалық олқылықтар

Абстракция деңгейлері

Сандық жүйелерді жобалау көпдеңгейлі иерархия арқылы жүзеге асады:

1. Жүйелік деңгей
2. Алгоритмдік деңгей
3. RTL деңгейі
4. Қақпа деңгейі
5. Транзистор деңгейі
- 6. Физикалық деңгей**

Бұл тәсіл күрделі жүйені басқаруға, әр деңгейде верификация жүргізуге мүмкіндік береді.

Әр деңгейдегі қауіптер

- Жүйелік деңгей – **архитектурада осалдық қалуы** мүмкін
- Алгоритмдік деңгей – әлсіз алгоритмді, шешімдерді таңдау
- RTL деңгейі – зиянды троян енгізілу қаупі
- Қақпа деңгейі – логикалық элементтердің комбинациясындағы осалдық
- **Физикалық деңгей** – энергия тұтыну, сәуле шығару арқылы құпия ақпараттың ағып кетуі

Жобалау ағындары

Сандық жүйені жобалау келесі негізгі қадамдардан тұрады:

1. Техникалық талаптар анықтау
2. Модельдеу (SystemC, MATLAB)
3. RTL жобалау (**VHDL, Verilog, SystemVerilog**)
4. Синтез (RTL / қақпа деңгейі)
5. Іске асыру(Implementation) – орналасу, уақыттық талдау
6. Верификация – функционалдық, формальды және қауіпсіздік тексерулері
7. Өндіру немесе **FPGA**-ға жүктеу
8. Тестілеу және қорғау

Қауіпсіздікке қойылатын жалпы талаптар

- Құпиялылық (Confidentiality) – мәлімет сыртқа шықпау керек
- Бүтіндік (Integrity) – мәлімет өзгертілмеуі керек
- Қолжетімділік (Availability) – жүйе әрқашан жұмысқа дайын болуы тиіс
- Аутентификация – құрылғы немесе қолданушының түпнұсқалығын тексеру
- Бақылау және аудит – оқиғаларды тіркеу, талдау мүмкіндігі

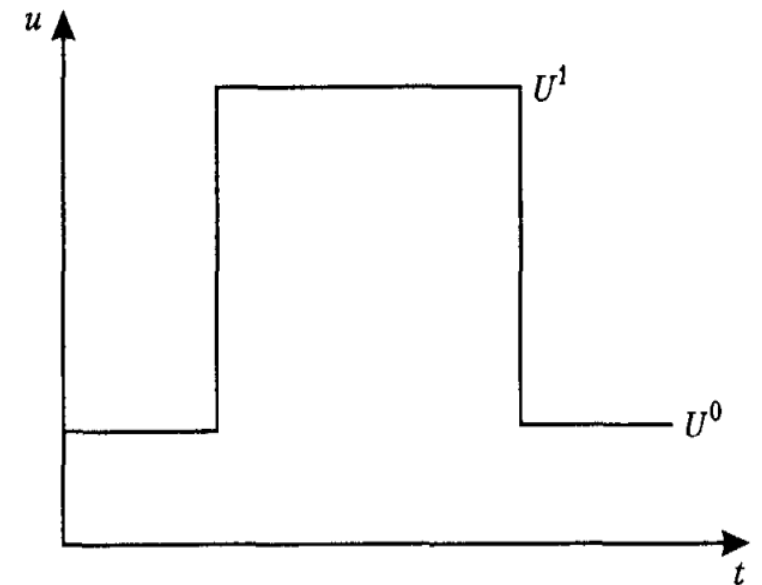
Аппараттық қауіпсіздік талаптары

- Аппараттық қауіпсіздік талаптары
- Қорғалған жад аймақтары
- Сенімді кездейсоқ сандар генераторы (RNG)
- Қуат талдауына төзімді схемалар (мысалы, теңгерімді логика)
- Аппараттық трояндарды анықтау және болдырмау әдістері

Сандық интегралдық схемалар

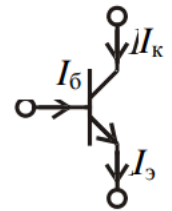
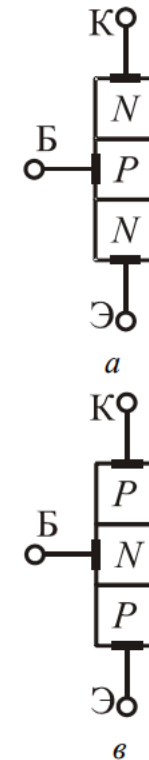
- Сандық интегралдық схемалар (ЦС) дискретті функция заңына сәйкес өзгертін сигналдарды түрлендіруге арналған. Мұндай сигналдарда сәйкесінше логикалық нөл және логикалық бірдеп аталатын U^0 және U^1 деген екі ғана мән бар. Логикалық нөлге және логикалық бірге сәйкес келетін кернеулер айырмашылығы логикалық дифференциал деп аталады:

$$U_{\text{л}} = U^0 - U^1.$$

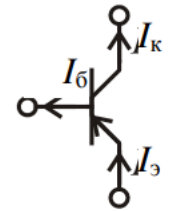


Биполярлы **транзистор**

- Биполярлы транзистор – екі р–n өткелінен тұратын үш терминалды жартылай өткізгішті құрылғы болып табылады. Ол электр өткізгіштігінің әртүрлі типтері бар жартылай өткізгіштің ауыспалы аймақтарынан тұрады.
- n- және р-аймақтардың кезектесу ретіне қарай n–р–n- және р–n–р-типті транзисторлар бөлінеді. Іс жүзінде транзисторлардың екі түрі де бір қызмет атқарады; олардың жұмыс істеу принципі бірдей. n-р-n-типті транзистордағы негізгі заряд тасымалдаушылар электрондар, ал р-n-р транзисторында олар кемтіктер. Кремнийдегі электрондардың қозғалғыштығы жоғары болғандықтан практикада n–р–n-типті транзисторлар жиі қолданылады.



б

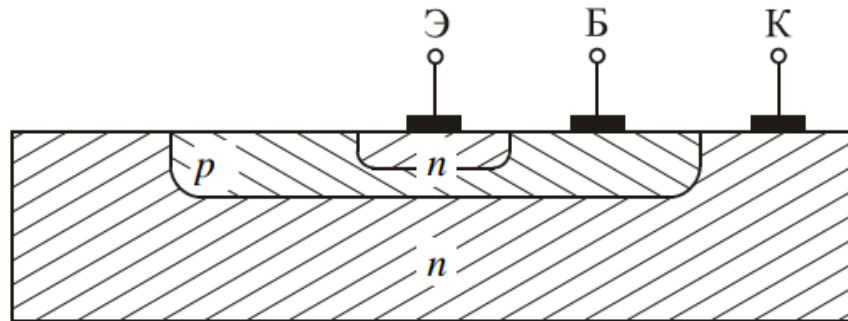


г

Транзистордың ортанғы бөлігі, екі шеті коллектор және эмиттер база деп аталады. Базаның қалыңдығы шағын және ол бірнеше микроннан аспайды.

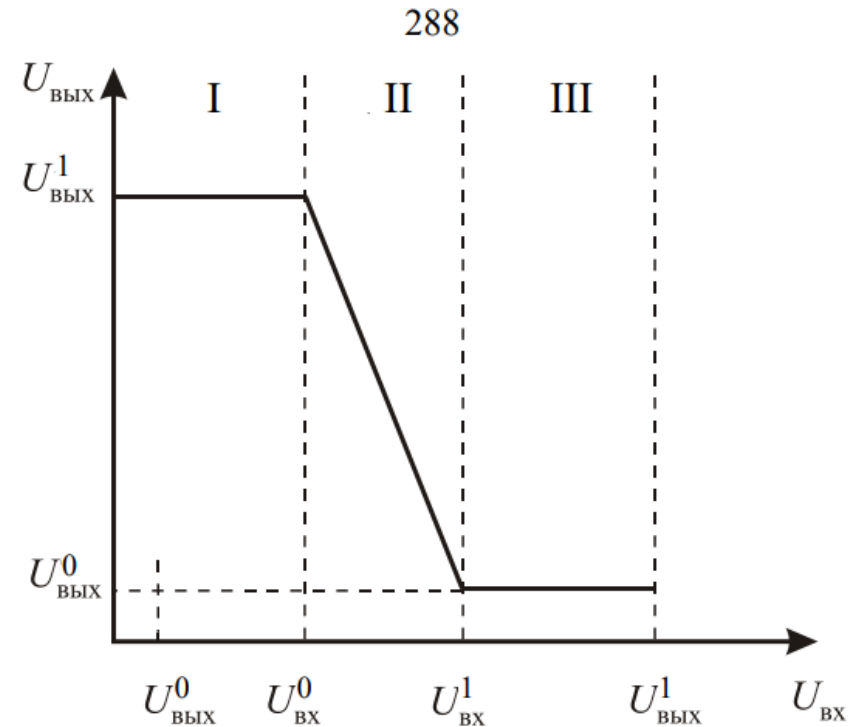
База мен эмиттер арасындағы ауысуды эмиттерлік деп атайды, ал база мен коллекторды коллекторлық деп атайды.

Нақты транзистордың құрылымы асимметриялық. Коллекторлық түйіннің ауданы әлдеқайда үлкен, эмитентке қарағанда.



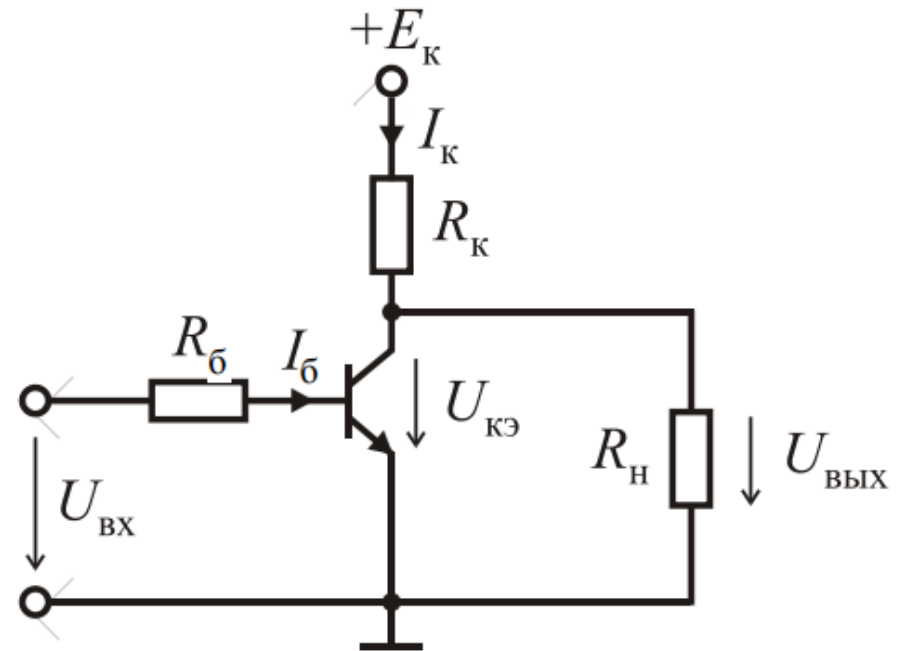
Логикалық инвертор

- Инвертор ЕМЕС функциясын жүзеге асырады және ең қарапайым негізгі логикалық элемент болып табылады. Инвертордың беріліс сипаттамасы суретте көрсетілген. Жоғары кернеу деңгейі логикалық деңгейге, ал төмен кернеу деңгейі логикалық нөлге сәйкес келеді. Суреттегі түрлендіргіштің тасымалдау сипаттамасы үш аймақтан тұрады. I аймақ шығыстағы логикаға, III аймақ логикалық нөлге сәйкес келеді. II аймақ өтпелі. Бұл аймақта инвертор күшейткіш ретінде әрекет етеді.



Биполярлы транзисторлы негізіндегі Инвертор

- Биполярлы транзисторға негізделген қарапайым инвертор суретте көрсетілген. Негізгі тізбектегі резистор R_b қажетті базалық токты орнату үшін қызмет етеді. Резистор R_k — инвертордың ішкі жүктемесі, ал R_n резисторы — оның сыртқы жүктемесі. Сыртқы жүктеменің шамасы кең шектерде өзгеруі мүмкін. R_k шексіздікке ұмтылғанда түрлендіргіш бос режимде жұмыс істейді. Инвертор әлі де өз параметрлерін сақтауы тиіс максималды жүктеме $R_k = R_n$ мәні болып саналады.



Статикалық режим

- Статикалық режим. Статикалық режимде логикалық инвентор жабық болуы мүмкін (транзистор кесу режимінде) немесе ашық (транзистор қанықтыру режимінде). Кіріс кернеуі логикалық нөлдік кернеуден U төмен болғанда түрлендіргіш жабылады. Кремний биполярлы транзисторлар негізіндегі инверторлар үшін ол $0,4 - 0,5$ В. Бұл режимде
$$I_K = I_{\bar{O}} \approx 0, \quad U_{K\bar{O}} = E_K - R_K I_K \approx E_K$$
- Жабық инвертордың кедергісі жүздеген кОмды құрайды.

- Егер транзистор қанықтыру режимінде болатын кіріске осындай шамадағы кернеу импульсі берілсе, онда базалық ток

$$I_{\text{б}} = \frac{U_{\text{вх}} - U_{\text{бэ}}}{R_{\text{б}}} \approx \frac{U_{\text{вх}}}{R_{\text{б}}}.$$

- Қанықтыру режимінде екі түйіспе де алға бағытталған және коллектор тогы ең үлкен мәнге дейін артады:

$$I_{\text{к}} = I_{\text{кнас}} = \frac{E_{\text{к}} - U_{\text{кэ}}}{R_{\text{к}}} \approx \frac{E_{\text{к}}}{R_{\text{к}}}.$$

- Қанықтыру режиміндегі $U_{\text{ке}}$ кернеуі 0,2–0,3 В, шығыс кедергісі бірнеше ондаған Ом. Транзисторды қанықтыру үшін базалық ток транзистордың қанығуы басталатын минималды мәнден жоғары болуы керек:

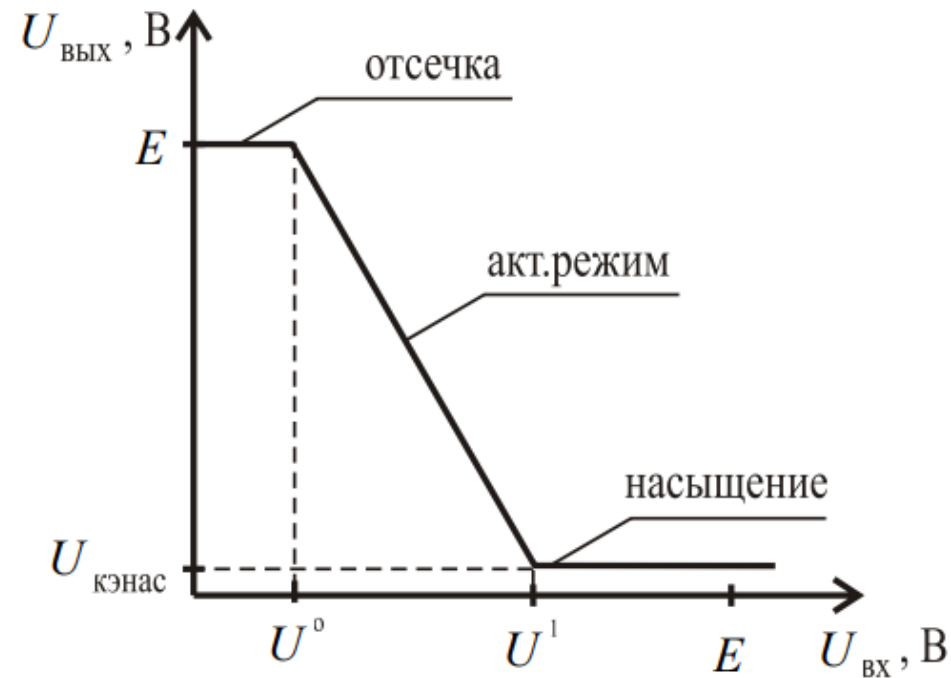
$$I_{\text{б}} > \frac{I_{\text{кнас}}}{\beta} \approx \frac{E_{\text{к}}}{\beta R_{\text{к}}}.$$

- Транзистордың қанығу тереңдігі қанығу коэффициентімен (дәрежесі) сипатталады, ол нақты базалық ток қанығу режимі пайда болатын минималды мәннен қанша есе асатынын анықтайды:

$$S = \frac{I_{\text{б}}}{I_{\text{бнас}}}.$$

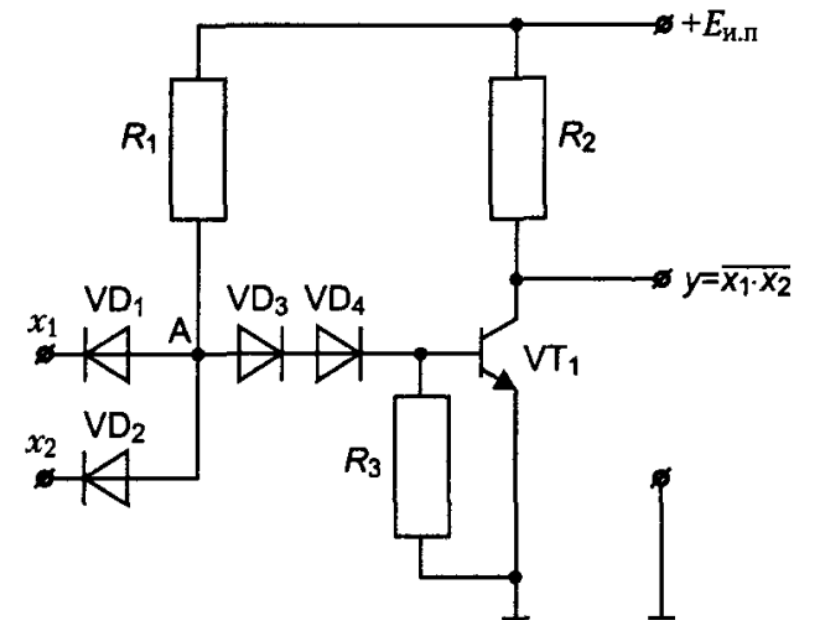
- Қанықтыру коэффициентінің мәні 1,5-тен 3-ке дейін таңдалады. Кіріс кернеуі логикалық бірлік кернеуінен U_1 асатын кезде транзистор қанықтыру режиміне өтуі керек. Биполярлы транзисторларға негізделген инверторлар үшін $U_{\text{вх}}^1 \approx 1.5 \text{ В.}$

- БТ-дағы инвертордың беріліс сипаттамасы суретте көрсетілген. Жұмыс аймақтары кесу мен қанықтылыққа сәйкес келетін өтпелі реакцияның бөлімдері болып табылады.



ДИОД-ТРАНЗИСТОРЛЫҚ ЛОГИКА

- Бұл схемада тізбектей жалғанған екі функционалды бөліктен тұрады: біріншісінде, кіріс сигналдары x_1 және x_2 диодтық элементке (VD_1 және VD_2 диодтары және R_1 резисторы) беріледі, ол ЖӘНЕ операциясын орындайды; VT_1 транзисторында жасалған екінші бөлік; инвертор болып табылады. Осылайша, ЖӘНЕ және ЕМЕС логикалық операциялар схемада бөлек орындалады, сондықтан схема 2ЖӘНЕ-ЕМЕС логикалық операциясын жүзеге асырады (2 саны кірістерінің санын білдіреді). VD_3 және VD_4 диодтары тізбектің екі бөлігі арасындағы байланыстырушы элемент рөлін атқарады және оның шуға төзімділігін арттырады.



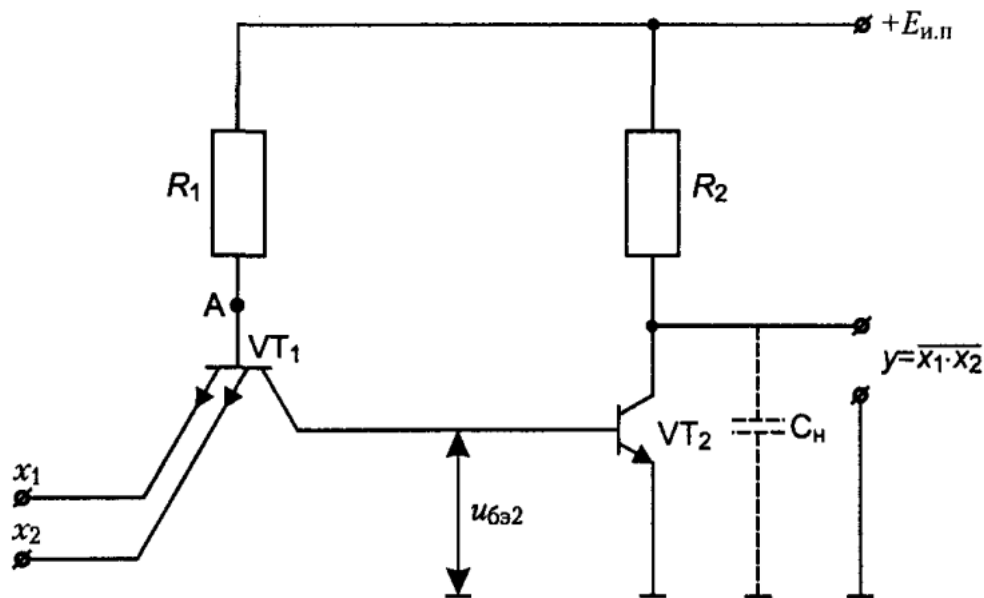
- Егер $U = 0$ сигналы x_1 немесе x_2 кірістерінің біріне берілсе, онда диодтардың біреуі ашық және ток тізбекте E көзінен R_1 резисторы және ашық диод арқылы өтеді. Бұл жағдайда A нүктесінде $U = 0,7$ В потенциалы орнатылады, ол VD_3 және VD_4 сериялы қосылған екі диодты ашу үшін жеткіліксіз. Нәтижесінде VT_1 транзисторы жабылады және тізбектің шығысында U кіріс $= E$ сәйкес келетін логикалық күй орнатылады. X_1 және x_2 кірістерінің екеуі де жоғары сигнал деңгейі U кірісімен қамтамасыз етілгенше схема осы күйде қалады. Бұл жағдайда VD_1 және VD_2 диодтары жабылады, A нүктесінің потенциалы артады, VD_3 және VD_4 диодтарын ашу үшін жеткілікті болады және ток E_{ip} көзінен R_1 резисторы арқылы, VD_3 және VD_4 диодтары VT_1 транзисторының негізіне өтеді.

- Нәтижесінде VT1 транзисторы ашылады, ал тізбек шығысында төмен кернеу деңгейі орнатылады $U_{\text{шығыс}} = U_{\text{тыныштық}} = 0,1 \text{ В}$ (логикалық нөл), сондықтан және емес операциясы DTL тізбегінде орындалады. R3 резисторы осы тізбекте VT1 транзисторының базасында жинақталған зарядтың резорбциялық тізбегін құру үшін қызмет етеді (VT1 ашық күйден жабық күйге ауысқанда).
- Кейбір жағдайларда R3 резисторы жерге емес, негізгі зарядтың жылдам резорбциясын қамтамасыз ету және сигналдың кешігу уақытын азайту үшін теріс кернеу $E = -2 \text{ В}$ көзіне қосылады.

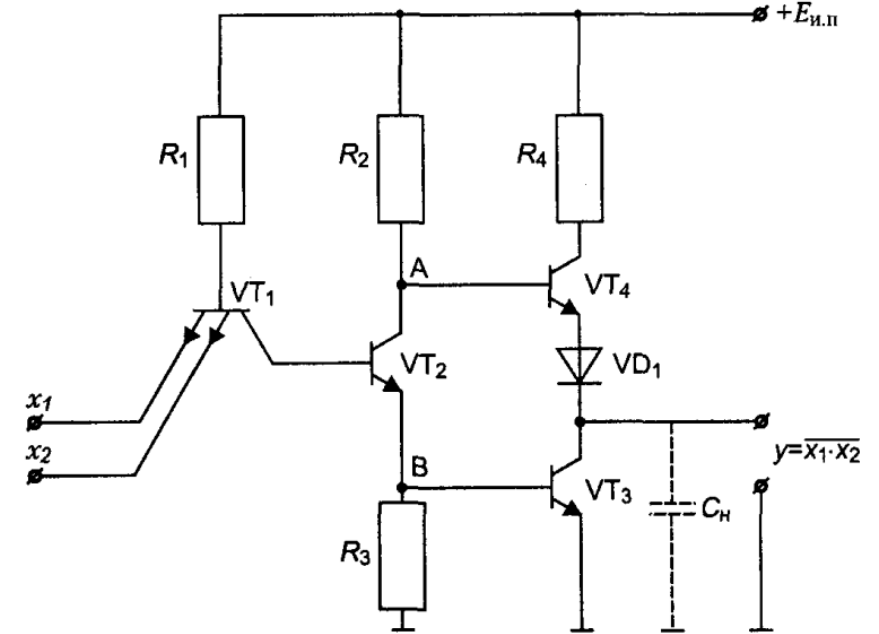
Транзисторлық-транзисторлық логикалық (TTL)

- Негізгі TTL элементінде VD1 және VD2 диодтарының функцияларын көп эмиттерлі транзистордың эмитенттері орындайды, ал VD3 және VD4 диодтарының рөлі оның коллекторлық түйіні болып табылады. Сондықтан TTL тізбегі DTL тізбегі сияқты логикалық операцияны орындайды, яғни және емес. Шынында да, егер x_1 немесе x_2 кірісінде төмен деңгейлі сигнал $u = 0$ (логикалық нөл) болса, онда ток тізбекте E қоректендіру көзінен R1 резисторы және сәйкес ашық эмитент торабы арқылы өтеді. VT1 транзисторының базалық потенциалы шамамен 0,7 В болады. Бұл потенциал VT1 транзисторының коллекторлық түйіні мен VT2 транзисторының эмитенттік түйіні арасында шамамен бірдей бөлінеді. Сондықтан, $U_{бэ2}$ кернеуі VT2 транзисторының құлпын ашу үшін жеткіліксіз және тізбектің шығысында $U_1 = E$ (логикалық бірлік) жоғары кернеу деңгейі орнатылады.

- Егер x_1 және x_2 кірістерінде жоғары сигнал деңгейі U 1 кіріс (логикалық блок) болса, онда VT_1 транзисторының эмитенттік өткелдері құлыпталады, ток E көзінен R_1 резисторы, VT_1 коллекторлық түйіні және эмиттерлік өткел арқылы өтеді. VT_2 . VT_2 транзисторының базалық әлеуеті $U_{бэ2} = 0,7$ В, ал потенциал $U_a = 1,4$ В тең болады. VT_2 транзисторының құлпы ашылды және тізбектің шығысында $0,1$ В төмен кернеу деңгейі U_0 орнатылады.



- TTL тізбегі DTL тізбегінің барлық артықшылықтарын сақтай отырып, ауданда айтарлықтай өсімге ие. Сондықтан бұл схема қазір DTL схемаларын іс жүзінде ауыстырды және өте кең тарады. Дегенмен, қарастырылған нұсқада TTL тізбегі, оның қарапайым технологиясына қарамастан, оның төмен жүктеме қабілетіне және төмен өнімділігіне байланысты қолданылмайды. Шынында да, тізбектің шығысына ұқсас тізбектер түріндегі бірнеше жүктемелер қосылғанда, жүктеме сыйымдылығы C_H артады және R_2 резисторы жеткілікті үлкен мәнге ие болғандықтан, сыйымдылықты зарядтау үшін уақыт тұрақтысы артады және өнімділігі артады. тізбек азаяды. TTL тізбектеріндегі бұл кемшілікті жою үшін қарапайым инвертордың орнына күрделі инвертор қолданылады

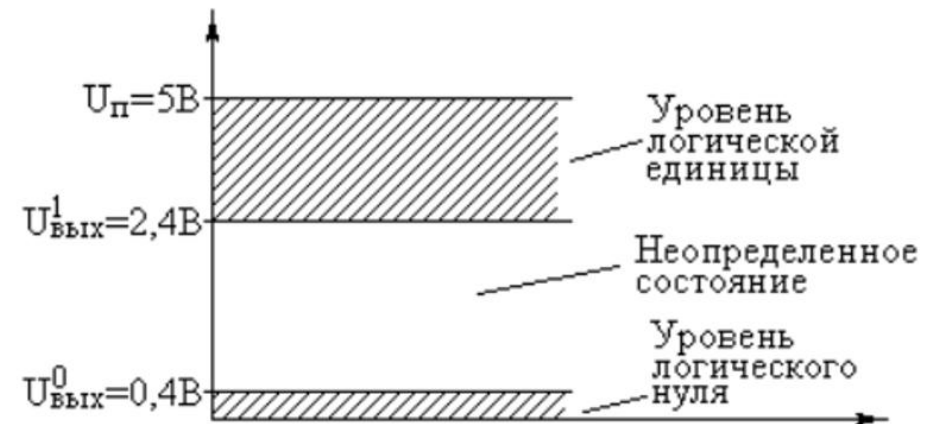


- Бұл тізбектегі транзистор VT2 «фазалық бөлгіш» функциясын орындайды. Инвертордың жұмысын қарастырайық. Инвертордың кірісінде (VT2 транзисторы негізінде) төмен кернеу деңгейі U_0 (логикалық нөл) болсын. VT2 транзисторы жабық, А нүктесінің потенциалы жоғары, ал В нүктесі төмен, сондықтан VT3 транзисторы жабық және VT4 ашық. Жүктеме сыйымдылығы C_h Е көзінен R2 резисторы, VT4 транзисторының ашық эмитенттік түйіні және VD1 диоды арқылы жылдам зарядталады. Тізбектің шығысында жоғары кернеу деңгейі орнатылады $U_{1out} = E_{ip} - U_{бэ} - U_d = 3,6 \text{ В}$ (логикалық бірлік). R4 резисторы VT4-VD1-VT3 дәйекті тізбегіндегі тоқты шектеуге арналған. Шын мәнінде, тізбек бір күйден екінші күйге ауысқан кезде транзисторлардың екеуі де VT3 және VT4 ашық (олардың бірі ашылады, бірақ екіншісі жабылуға уақыт жоқ) және E_{ip} көзінің тұйықталуын болдырмау үшін. жерге қосу үшін R4 шектеу резисторы орнатылған.

- Егер түрлендіргіш кірісінде жоғары кернеу деңгейі U_1 (логикалық блок) орнатылса, онда транзистор VT_2 ашық, VT_4 жабық және VT_3 ашық. Сыйымдылық C_H ашық транзистор VT_3 арқылы разрядталады, ал тізбектің шығысында төмен кернеу деңгейі $U_{0\text{ out}} = 0,1\text{ В}$ (логикалық нөл) орнатылады. VD_1 диоды VT_3 транзисторы ашық кезде VT_4 транзисторының сенімді блокталуын қамтамасыз етеді. Паразиттік сыйымдылық C_H заряды мен разряды қосу кедергісі төмен VT_3 және VT_4 транзисторлары арқылы өтетіндіктен, күрделі инверторы бар TTL тізбегі жоғары өнімділікке ие. Бұл схемадағы сигналдың таралуының орташа кешігу уақыты шамамен 10 нс құрайды. TTLSH сұлбасы жоғары өнімділікке ие, онда әдеттегі биполярлы транзисторлардың орнына Шоттки кедергісі бар транзисторлар қолданылады. Бұл жағдайда $t = 3\text{ нс}$.

TTL микросұлбаларының логикалық деңгейлері

- Қазіргі уақытта TTL микросұлбаларының екі түрі қолданылады - бес және үш вольтты қуат көзі бар, бірақ микросұлбалардың қоректену кернеуіне қарамастан, бұл микросұлбалардың шығысындағы нөлдік және бір логикалық деңгейлері бірдей. Сондықтан TTL чиптері арасында қосымша үйлестіру әдетте талап етілмейді. Цифрлық TTL микросұлбасының шығысындағы рұқсат етілген кернеу деңгейі суретте көрсетілген.



- Бұрын айтылғандай, шығыспен салыстырғанда сандық чиптің кірісіндегі кернеу әдетте үлкен шектерде рұқсат етіледі. TTL микросұлбалары үшін логикалық нөлдік және бір деңгейдің шекаралары суретте көрсетілген.

