алгоритмінің жоғарыда көрсетілген криптоталдау әдістеріне қарсы тұра алуын тексеру керек.

2. Блоктық криптоалгоритм кірісіне бір блокты құрайтын бірнеше бекітілген бит түріндегі ақпарат беріледі.

Ұзындығы 64 битке тең блоктар жиі қолданылады. Мұндай алгоритмді кезкелген санды биттерден тұратын мәтінді шифрлау үшін қалай қолдануға болады? Біріншіден, ағындық шифрларды қолданған қолайлы сияқты. Бірақ блоктық шифрларды талдау олардың кез келген ұзындықты хабарларды шифрлау үшін жарамды екенін көрсетті. Блоктық шифрлауды қолданудың төрт негізгі стандарты анықталған.

Электронды кодтық кітап (electronic code book – ECB) –әрбір блоктардан тәуелсіз шифрлау әдісі. ГОСТ-та мұндай әдіс жай ауыстыру режимі деп аталады.

(CipherBlockChaining-CBC) – шифрланған блоктарды тіркеу. Шифр мәтіні бойынша кері байланыс (CipherFeedback- CFB).

m биттен тұратын әрбір символды криптожүйеге түскен бойда блокты құрайтын басқа биттердің түсуін күтпей шифрлау әдісі. Бұл әдіс ГОСТ-та анықталған кері байланысты гаммалау әдісіне ұқсас.

Шығыс бойынша кері байланыс (OutputFeed-back – OFB). *m* битті әрбір символды шифрлау үшін блоктық шифрлау көмегімен алынатын кездейсоқ тізбек қолданылады. Бұл әдіс ГОСТ 28147-89 -да анықталған *m=4* болғандағы гаммалық режимге ұқсас.

2.3. SKIPJACK шифрлау алгоритмі

SKIPJACK Американдық стандарт (escrowed encryption standard (EES)). SKIPJACK мәліметтерді шифрлау және шифрын шешу алгоритмін және деректерді қалпына келтіру өрісінің құрылу және пайдаланылу процедураларын (LEAF-low enforcement access field), форматын анықтайды, олар электронды құрылғыларда қолданылуы және мемлекеттік телекоммуникациялық жүйелерді қорғау үшін қолданылады. SKIPJACK және LEAF пайдаланатын жүйе аппараттық тәсілмен жүзеге асырылуы тиіс, ал электрондық құрылғылар FIPS 140-1 стандартының талаптарын қанағаттандыруы қажет. LEAF ішіндегі мәліметке қатысты K_u ену кілті екі пайдаланушы арасында келесідей түрде бөлінеді:

$$K_u = K_{u1} \oplus K_{u2},$$

мұнда K_{u_1}, K_{u_2} - бірінші және екінші пайдаланушыда сәйкесінше сақтаулы кілттер.

SKIPJACK алгоритмі туралы белгілі [2]: ұзындығы 80 биттік кілті бар, блок типіндегі шифрлаудың симметриялы алгоритмі, ену блогының ұзындығы 64 бит, шифрлаудың 4 режимі (DES және ГОСТ 28147-89 режимдері сияқты), 32 цикілі бар, оны дайындау АНБ-да 1985 жылы басталған, алгоритмде тестен өткізу 1990 жылы аяқталды. Алгоритмді Mykotronx фирмасының Clipper микросхемасында жүзеге асыруда қарапайым ауыстыру режиміндегі бір блокты шифрлау 64 уақыттық циклді алады, осылайша алгоритмнің әрбір цикілі 2 уақыттық циклді алады. Алгоритм 16 биттік ішкі блоктармен жұмыс жасайды, сонымен бірге үш ішкі блок (48 бит) кілтке тәуелді біржақты функциясын пайдалана отырып түрленіп, 16 бит алынады, ол екінші модуль бойынша қалған 16 биттік блокпен қосылады, яғни DES алгоритмінен айырмашылығы SKIPJACK блоктың өлшемінің жартысымен жұмыс жасамайды. Біржақты функция құру үшін жадының 128 байтын алатын 16 S блок және жылжу амалдары пайдаланылады.

EES стандартында берілгендерді қайта қалпына келтіру өрісі ретінде келесі форматтағы LEAF өрісі пайдаланылады: Ek_F *(U,* Ek_u *(*K_S*), C),* мұнда $E_k(D)$ – *K* кілтіне *D*-ны шифрлау, K_F – құрылғылар топтары (микросызбалар) үшін ортақ кілт, K_u - микросызбаның ерекшекілті, K_s – сеанстық кілт, *U* - микросызбаның 32 биттік идентификаторы, *C* - 16 биттік бақылау сомасы, LEAF-тың жалпы ұзындығы 128 бит. K_u кілті жоғарыда айтылған тәсіл бойынша екі пайдаланушы арасында бөлінген.

EES стандартының аппараттық құрылғылары ретінде Clipper және Capstone атақты микросызбалары қолданылады. Clipper (МУК-78Т) микросызбасы дыбыстық ақпаратты қорғау жүйелерінде қолдану үшін жасалған және қазіргі уақытта AT& T (Model 3600) фирмасының телефондағы ақпаратты қорғау құрылғыларына орнатылған. Микросызбаның негізгі жұмыстарын ғылым Академиясы анықтады, оның логикалық сызбасын Mykotronx фирмасы жасады, ал микросызбаларды дайындап шығаруды VLSI фирмасы жүзеге асырған. Микросызбада SKIPJACK шифрлау алгоритмі тек OFB DES режиміне ұқсас режимде жүзеге асырылған. Шифрлау жылдамдығы

15-20 МБ/с. микросызба келесі ақпаратпен бір рет бағдарламаланады: өзіндік ерекше сериялық нөмір, микросызбаның өзіндік ерекше кілті, микросызбалар тобының кілті, арнайы басқарушы бағдарламалық қамтамасыз ету. LEAF өрісін жасағанда келесі әрекеттер орындалады: 80 биттік сеанстық кілтті құрылғы кілтіне шифрлайды, алынған 80 биттік нәтиже 32 биттік идентификатормен және 16 биттік аутентификациялық кодпен сәйкестірленеді, пайда болған 128 биттік кілт құрылғылар тобының кілтімен шифрланады. Сеанстық кілт ақпаратты шифрлау және шифрді шешу үшін екі бағытта да (алу және беру) пайдаланылады. Capstone (МҮК-80) цифрлық (сандық) берілгендерді қорғау үшін жасалған. Clipper және Capstone-да жүзеге асырылған шифрлау алгоритмдеріне қоса SKIPJACK алгоритмі бойынша шифрлаудың барлық 4 режимі жүзеге асырылған: цифрлық қол қоюдың стандартты алгоритмі Digital Signature Algorithm (DSA); хэшрлеудің стандартты алгоритмі Secure Hashing Algorithm (SHA); ассиметриялық криптограмма пайдаланатын кілтті басқару алгоритмі; көп разрядты сандардың модулі бойынша дәрежеге шығару алгоритмі; кездейсоқ сандардың Фибоначи датчигін қолданатын кездейсоқ сандардың генераторы. Осылайша, кілттерді қайта қалпына келтіретін стандартты криптожүйелер ретінде АҚШ үкіметі EES стандартын ұсынған, оның негізгі құрамдас бөліктері жоғарыда қарастырылды. Шифрлау алгоритмінің аппараттық жүзеге асырылуы және оның құпиялылығы заңсыз көшіруден қорғау, ал EES-ті пайдалану криптожүйелерді заңды түрде бақылау және оларды экспортқа шығыру мәселелерін шешуге мүмкіндік береді. Заңды мәселелерден басқа, EES стандарты жүзеге асырушы жүйелерге жасалатын бірнеше криптоаналитикалық шабуылдар белгілі. Олар LEAF-ң мықтылығын бұзу мүмкіндігімен және K_u, K_F кілттерін алу мақсатында микросызбалардың өзіне де жасалған «технологиялық шабуылдармен» байланысты.

AES-ке (Advanced Encryption Standard) кандидат деп аталатын 15 алгоритмнің бар екенін атап өту керек, олар 1997 жылдың 20-шы қаңтардағы Fourth Fast Software Encryption конференциясында талқыланды:

http://www.nist/gov/aes

CAST-256 (Entrust Teclщol. Inc., C. Adaшs), Crypton (Future System Inc., Chae Hoon Lim), DEAL (R. Outerbride,-L. Knudsen), DFC (Ұлттық ғылыми зерттеу орталығы (Франция), S.Vaudenay), E2 (NTT

(Nippon) Masayuki Kanda), FROG (TecApro Int.S.A, D.Georgoudis), ИРС (RichSbroeppel), LOK197 (L. Brown, J.Pieprzyk,J. Seberry), MAGENTA (Germ. Telecom AG, Klaus Huber), MARS (IBM. N. Zunic), RC6 (RSA Labs,M. Robshaw), RIJNDAEL (J. Daemen V. Rijmen), SAFER+ (Cylink Corp., Lily Vhen), SERPENT (R. Andersson, E. Biham, Lars Knudsen), TWOFISH (B. Schneier, 1. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson)

Бақылау сұрақтары

1. DES алгоритмі қай елдің алгоритмі?
2. DES алгоритмінің 4 режимін атап беріңіз.
3. ГОСТ 28147-89 шифрлау алгоритмінің кемшіліктері қандай?
4. ГОСТ 28147-89 және DES алгоритмдердің айырмашылықтарын атап беріңіз.
5. DES және ГОСТ 28147-89 алгоритмдерінің кілт ұзындықтары қандай?
6. Қазіргі таңда DES криптожүйесін не себепті кеңінен қолданылмайды?
7. SKIPJACK криптожүйесін қандай криптожүйемен алмастырылды?

Есептер

1. DES алгоритмін қолдану арқылы ақпаратты шифрлаңыз.
2. DES криптожүйесіндегі кілтті генерациялауға программа құрыңыз.
3. ГОСТ 28147-89 алгоритмін қолдану арқылы ақпаратты шифрлаңыз.
4. ГОСТ 28147-89 криптожүйесіндегі кілтті генерациялауға программа құрыңыз.
5. Skipjack алгоритмін қолдану арқылы ақпаратты шифрлаңыз.
6. DES алгоритмін қолдану арқылы файлдағы ақпаратты шифрлаңыз.

3. АСИММЕТРИЯЛЫҚ КРИПТОГРАФИЯ ЖӘНЕ ЖЫЛДАМ ӘДІСТЕР

3.1. Ашық кілтті криптожүйелердің концепциясы

Мәліметтерді криптографиялық қорғаудың тиімді жүйесі асимметриялық криптожүйелер болып табылады [29]. Сонымен қатар, оларды ашық кілтті криптожүйелер деп те атайды. Мұндай жүйелерде мәліметтерді шифрлауды бір кілт, ал мәліметтерді ашуда басқа кілт қолданылады (асимметриялық атауы осыдан шыққан). Бірінші кілт ашық кілт болып табылады және мәліметтерді шифрлайтын жүйелердегі барлық қолданушыларға пайдаланылуы үшін ол жария болуы мүмкін. Мәліметтерді ашық кілт көмегімен ашу мүмкін емес.

Шифрланған хабардың қабылдаушысы мәліметтерді ашу үшін құпия кілт болып табылатын екінші кілтті қолданады. Әрине, ашу кілті шифрлау кілтінен анықталуы мүмкін емес, яғни олар бір-бірімен байланысы жоқ.

Ашық кілтті асимметриялық криптожүйенің жалпы сызбасы 4-суретте көрсетілген. Бұл криптожүйеде екі әртүрлі кілт қолданылады. $K_B - A$ жіберушінің ашық кілті, $k_B - B$ қабылдаушының құпия кілті. Кілттер генераторы B қабылдаушының жағында орналастырған жөн (k_B құпия кілтін қорғалмаған канал арқылы жіберілмеуі үшін). K_B және k_B кілттерінің мәні кілттер генераторының бастапқы күйіне тәуелді. k_B құпия кілтін белгілі K_B ашық кілті арқылы ашу шешілмейтін есеп болуы мүмкін.

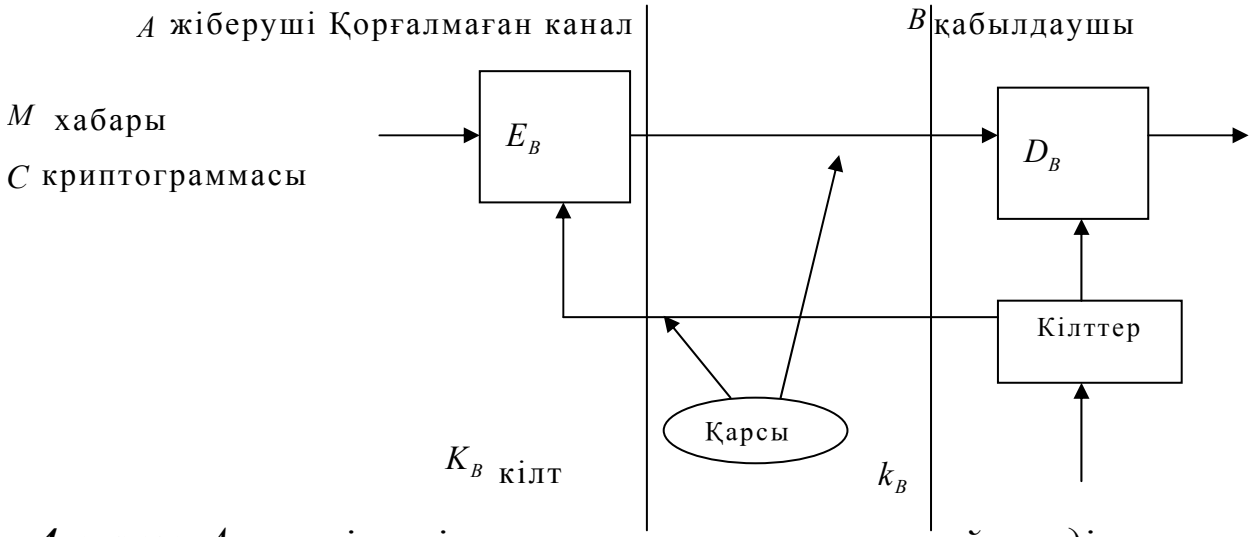
Асимметриялық криптожүйелердің өзіне тән ерекшеліктері:

1. K_B ашық кілті және C криптограммасы қорғалмаған канал арқылы жіберілуі мүмкін, яғни қарсыласқа K_B және C белгілі.
2. Шифрлау және ашу алгоритмдері

$$E_B : M \to C$$

$$D_B : C \to M$$

ашық болып табылады



4-сурет. *Ашық кілтті асимметриялық криптожүйелердің жалпы сызбасы.*

Асимметриялық криптожүйедегі хабардың қауіпсіздігі k_B кілттің құпиялығына негізделген.

У. Диффи мен М. Хеллман асимметриялы криптожүйенің қауіпсіздігін қамтамасыз ететін талаптарды анықтады.

1. B қабылдаушының (K_B, k_B) кілттер жұбын бастапқы шарттар негізінде есептеуі қарапайым болуы керек.

2. A жіберуші K_B ашық кілті мен M хабарын біле отырып, криптограмманы оңай есептей алады: $C = E_{K_B}(M) = E_B(M)$.

3. B қабылдаушы k_B құпия кілтін және C криптограммасын қолдана отырып, алғашқы хабарды оңай аша алады:

$$M = D_{K_B}(C) = D_B(C) = D_B[E_B(M)].$$

4. Қарсылас K_B ашық кілтін біле отырып, k_B құпия кілтін алу әрекетінде үлкен есептеу қиындығына тіреледі.

5. Қарсылас (K_B, C) жұбын біле отырып, M алғашқы хабарын есептегенде қиындыққа тіреледі.

Ашық кілтті асиммертриялық криптографиялық жүйелердің концепциясы біржақты функцияның қолданылуына негізделген. Біржақты функцияны формалды емес түрде келесідей анықтауға болады. X және Y кейбір кез келген жиындар болсын.

Функция $f : X \to Y$ біржақты болып табылады. Егер барлық $x \in X$ үшін

$y = f(x)$, мұнда, $y \in Y$

функциясын оңай есептеуге болатын болса.

Сонымен қатар, $y \in Y$ көп мәндері үшін $f(x) = y$ болатындай $x \in X$ мәнін табу қиынға соғады, мұнда кем дегенде бір x мәні бар деп есептелінеді. Тиімді кері бейнелеу $Y \to X$ жоқ екендігі f функциясының біржақты функциялар тобына жатуының негізі болып табылады.

Біржақты функцияның мысалы ретінде бүтін санды көбейтуді қарастырайық. Тікелей есеп – өте үлкен көп разрядты P және Q сандарының көбейтіндісін есептеу, яғни

$$N = P * Q$$

мәнін табу ЭЕМ үшін қиын есептердің қатарына жатпайды.

Кері есеп – үлкен көбейткіштерге жіктеу, яғни $N = P * Q$ көп разрядты үлкен санның P және Q көбейткіштерін табу, бұл N-нің үлкен мәнінде шешілмейтін есеп болып табылады. Қазіргі сандар теориясының бағасы бойынша $N = 2^{664}$ бүтін саны және $P \approx Q$ үшін N санының жіктеуі 10^{23} жуық амалдарды қажет етеді, яғни қазіргі таңдағы ЭЕМ үшін шешілмейтін есеп.

Біржақты функцияның келесі мысалы ретінде негізі мен модулі бекітілген модульдік экспонентті қарауға болады. $1 \le A \le N$ болатындай A және N бүтін сандар болсын. Z жиынын анықтайық: $Z_N = \{0,...,N-1\}$.

Онда N модулі бойынша A негіздегі модульдік экспонентінің өзі функция болады

$$f_{A,N} : Z_N \to Z_N,$$
$$f_{A,N}(x) = A^x \pmod N$$

мұнда, x - бүтін сан, $1 \le x \le N-1$.

$f_{A,N}(x)$ функциясының мәнін есептейтін тиімді алгоритмдер бар.

Егер $y = A^x$ болса, онда $x = \log_A(y)$ жазу айқын.

Сондықтан $f_{A,N}(x)$ функцияға бағыттау есебі дискретті логарифмді табу есебі немесе дискретті логарифмдеу есебі деп аталады.

Дискретті логарифмдеу есебі келесі түрде өрнектеледі. Белгілі A, N, y бүтін сандар үшін

$$A^x \bmod N = y$$

орындалатындай, x бүтін санды табу. Дискретті логарифмді жылдам белгілі уақыт ішінде есептеу алгоритмі әлі табылған жоқ. Сондықтан модульдік экспоненті біржақты функция деп есептелінеді.

Қазіргі таңдағы сандар теориясының бағасы бойынша $A = 2^{664}$ және $N = 2^{664}$ бүтін сандары үшін дискретті логарифмдеу белгілі y үшін x дәрежесінің көрсеткішін табу есебінің шешімі 10^{26} амалды қажет етеді, яғни көбейткіштерге жіктеу есебінен 10^3 есе қиын. Санның ұзындығын үлкейткенде, есептердің қиындық бағасының айырымы да өседі.

Белгілі бір тез уақыт ішінде дискретті логарифмді табудың тиімді алгоритмі жоқ екендігі дәлелденбегенін айта кеткен жөн. Осыған байланысты модульдік экспоненті біржақты функциялар қатарына шартты түрде кіргізілген, бірақ бұл оның тәжірибиедеқолданылуына кедергі келтірмейді.

Ашық кілтті криптожүйелерді құруда қолданылатын функциялардың екінші класы «құпия жол» біржақты функциялар деп аталады. Мұндай функцияның формалды емес түрдегі анықтамасын берейік:

$$f = X \to Y$$

функциясы «құпия жол» біржақты функциялар класына жатады, егер ол біржақты және сонымен қатар, «құпия жол» (бұл функциямен сипаттайтын құпия сан, жол немесе басқа ақпарат) белгілі болғанда кері функция оңай есептелінетін болса.

«Құпия жол» біржақты функцияның мысалы ретінде RSA криптожүйесінде қолданылатын модулі және дәреже көрсеткіші және модульдік экспонентті айтуға болады. Модульдік экспонентінің айнымалы негізі M хабарының сандық мәнін немесе C криптограммасын көрсетеу үшін қолданылады.

3.2. Ақпараттарды RSA криптожүйесін қолданып шифрлау және шифрларды ашу

«Құпия жол» біржақты функциялар анықтамасына негізделіп, Диффи мен Хеллман желі үшін көптеген пайдаланушыларымен ашық кілтті криптожүйенің құрылымын ұсынды.

Әрбір пайдаланушы, яғни i пайдаланушы десек, кездейсоқ жолмен көрсеткіштің z_i мәнін таңдап, оны құпияда ұстайды. Содан кейін, ол E_z алгоритмін қалыптастырады және оны ашық анықтама бөлімінде жариялайды (мысалы, интернетте). Ол тағы да D_{z_i} алгоритмін қалыптастырып, оны да құпияда ұстайды. Егер j пайдаланушы i пайдаланушыға x құпия хабарлама жібергісі келсе, онда ол E_{z_i} алгоритмін анықтама бөлімінен алады және оны i пайдаланушыға жіберетін, $y = f_{z_i}(x)$ криптограммасының құрылуы үшін қолданады. i пайдаланушы өзінің D_{z_i} құпия алгоритмін $f_{z_i}^{-1}(Y) = X$ есептеу үшін қолданады.

Егер f_z шын мәнінде, «құпия жолды» біржақты функциялар болса, онда бұл криптожүйе сөзсіз тәжірибелі тұрақтылықты қамтамасыз етеді.

Егер барлық көрсеткіште z анықталу облысындағы f_z функциясы оның мәндер облысымен сәйкес келсе, онда осындай біржақты функция көмегімен цифрлық жазулар алуға болады. Егер i пайдаланушы x құпиясыз хабарлама жібергісі келсе, онда ол $Y = f_{z_i}^{-1}(x)$ алу үшін өзінің құпия алгоритмін қолданады. Әрбір пайдаланушы E_{z_i} ашық алгоритмін біліп, $F_{z_i} = x$-ті алады, бірақ, тек қана i пайдаланушы $f_{z_i}^{-1}$-ді есептей алатындықтан, x хабарламасын i пайдаланушыдан өзгелері түсіне алмайды.

Әрине, i пайдаланушы j пайдаланушыға құпия хабарламаны сөзбен жібере алады, ол үшін j пайдаланушыға E_{z_i} ашық кілтін қолдана отырып, ол Y-ті жабықтүрде шифрлап жіберуі қажет.

RSA криптожүйесі 1976 жылы Диффи мен Хеллман жасырын жолды біржақты функция бар екенін білмей тұрып, олар өз мақалаларында осындай функциялардың мүмкін түрлерін көрсеткен жоқ.

Алғаш рет 1978 ж. «құпия жолды» біржақты функция ұғымын Массачусеттік технологиялық институтта жұмыс істейтін Американ математиктері Р. Л. Ривест, А. Шамир, және Л. Адельман ұсынған болатын [5]. RSA біржақты функциясы жәй қарапайым емес, оны түсіну үшін сандардың элементарлық теориясынан кейбір мағлұматтарды қажет етеді.

Е.Ү.О.Б. (*i, n*) *i* және *n* бүтін сандарының ең үлкен ортақ бөлгішін білдіреді, олар бір уақытта нөлге тең емес.

p жай саны үшін, $\varphi(p) = p - 1$ болады *p* және *q* екі тең емес жай сандар үшін мынаны байқау қиын емес:

$$\varphi(pq) = (p-1)(q-1) \tag{2.1}$$

Мысалы, $\varphi(6) = \varphi(2 \times 3) = 1 \times 2 = 2$. Белгілі Эйлер теориясында $EYOБ(X, n) = 1$ тең болған жағдайда *x* және $n(X, n)$ кез келген бүтін саны үшін

$$x^{\varphi(n)} = 1(\mathrm{mod}\, n) \tag{2.2}$$

болатындығын хабарлайды.

Сандар теориясынан бізге белгілі Евклид алгоритмі. Егер $EYOБ(n, e) = 1$, $0 < l < n$ жағдайда *e* және *n* қанағаттандырса, онда жалғыз d, $0 < d < n$,

$$de = 1(\mathrm{mod} n), \tag{2.3}$$

және $EYOБ(n, e)$ табу үшін, Евклидтің *"кеңейтілген"* алгоритмінің көмегімен d есептеуге болады.

«Құпия жолда» RSA біржақты функциясы

$$f_z(x) = x^e (\mathrm{mod} n), \tag{2.4}$$

мұндағы, *x* - оң бүтін $n = pq$, $z = \{p, q, e\}$, p және q - үлкен тең емес сан, ал, *e* - ЕҮОБ $(e, \varphi(n)) = 1$ үшін $\varphi(n)$ оң бүтін сан.

Кері функцияның мынандай түрі бар:

$$F_z^{-1}(Y) = Y^d (\mathrm{mod} n), \tag{2.5}$$