Дәріс 10. Псевдокездейсоқ тізбекті генераторлар

Жоспар:

1. ПТГ генераторлары
2. Блум–Блум–Шуб (BBS) ПКТ генераторы
3. Кері байланыс жылжу регистрлері

Криптожүйенің тұрақтылығы шифрланған ақпаратта қандай да бір заңдылықтардың болмауына байланысты. Шифрлау кезінде заңдылықтардың болмауы кейбір талаптардың орындалуына байланысты. Осындай талаптардың бірі–кілттің кездейсоқтығы. Әдетте кілттің кездейсоқтығын псевдокездейсоқ тізбекті генераторлар (ПТГ) қамтамасыз етеді.

Кездейсоқ сандар генераторлары кез келген дербес компьютерге салынған. Дегенмен, оларды криптографиялық тапсырмалар үшін пайдалану мүмкін емес, өйткені мұндай генераторлар толығымен кездейсоқ емес. Көптеген криптографиялық емес қосымшаларда кездейсоқ сандар сирек қолданылады, сондықтан олардың жеткіліксіздігі байқалмайды. Алайда, кездейсоқ сандар тізбегі жиі қолданылатын криптографияда кіріктірілген генераторлар қолайсыз. Шын мәнінде, компьютердің көмегімен мүлдем кездейсоқ тізбекті құру мүмкін емес, өйткені компьютердің мүмкін күйлерінің саны көп болғанымен, шектеулі. Демек, компьютердегі кез-келген генератор мерзімді болып табылады және мерзімді кез-келген нәрсені болжауға болады.

Сондықтан, ПТГ генераторларын құрудағы негізгі міндет-қайталану кезеңі жеткілікті үлкен тізбекті қалыптастыру. Егер ол кездейсоқтықты бағалауға арналған барлық статистикалық сынақтардан сәтті өтсе, генераторды жалған кездейсоқ деп санауға болады. Барлық компьютерлік генераторлар мерзімді болса да, олардың периоды кемінде 2^{256} бит болса, мұндай генераторларды криптографиялық қосымшаларда қолдануға болады.Келесі есептерді шешу үшін жалған кездейсоқ тізбектер қолданылады:

1) гаммалық тізбектерді құру, яғни синхронды ағындық шифрларды құру кезінде;

2) ақпаратты хэштеу;

3) криптографиялық алгоритмдердің тұрақтылығын қамтамасыз ететін негізгі ақпаратты қалыптастыру;

4) криптографиялық хаттамалардың көп санын іске асыру кезінде кездейсоқ сұрауларды қалыптастыру, мысалы, ортақ құпия кілтті әзірлеу, құпияны бөлу, монетаны лақтыру, битке байланыстыру, аутентификация, электрондық қолтаңба және т. б.;

5) қорғалатын аппараттық–бағдарламалық құралдардың жұмысына белгісіздік енгізу.

Жалған кездейсоқ реттілік генераторы келесі талаптарды қанағаттандыруы керек:

1) криптографиялық төзімділік;

2) Жақсы статистикалық қасиеттер, статистикалық қасиеттері бойынша жалған кездейсоқ реттілік шынайы кездейсоқ реттіліктен ерекшеленбеуі керек;

3) қалыптасқан реттіліктің үлкен кезеңі;

4) тиімді аппараттық және бағдарламалық қамтамасыз ету.

Жалған кездейсоқ реттілік генераторларын олардың реляция әдісіне қарай жіктеуге болады. Генераторларды іске асыру үшін криптографиялық және криптогафиялық емес әдістерді қолдануға болады. Криптографиялық әдістердегі генераторлар қолданылады:

1) ағындық шифрлар;

2) блоктық шифрлар;

3) біржақты функциялар;

4) ашық кілттері бар шифрлар.

Криптографиялық емес әдістердегі генераторлар негізге салынған:

1) сәйкес генераторлар;

2) кері байланысы бар ауысым регистрлері.

Сәйкес ПТГ генераторлары

Сызықтық конгруентті генератор (СКГ) деп аталады жалған кездейсоқ тізбек генераторлары келесі түрдегі (6.1):

$$x_{n+1} = (ax_n + b)\ mod\ m, \qquad (6.1)$$

мұндағы x_{n+1} және x_n сәйкесінше $(n+1)$–тізбектің бірінші және екінші мүшелері, a–көбейткіш, b – өсім, m – модуль. Кез–келген тізбекті қалыптастыру үшін x_0 бастапқы нөмірін орнату керек. Келесі мәлімдеме әділ.

Теорема. m, a, b, x_0 сандарымен анықталған сызықтық конгруенттік тізбектің ұзындығы m периоды болады, егер:

1) m және b сандары өзара жай;

2) $(a-1)$ мәні m бөлгіш болып табылатын әрбір қарапайым p–ге еселік;

3) $(a-1)$ төртке еселік, егер m төртке еселік болса.

СКГ артықшылықтарына өнімділікті жатқызуға болады. Алайда оларды криптографияда қолдану мүмкін емес, өйткені олардың шығу мәнін болжауға болатын әдістер бар. Сызықтық генераторлардан басқа көпмүшелік генераторлар бар, мысалы квадрат түрінде

$$x_{n+1} = (ax_n^2 + bx_n + c)\ mod\ m$$

және куб түрінде

$$x_{n+1} = (ax_n^3 + bx_n^2 + cx_n + d) mod\ m.$$

Қазіргі уақытта кез келген көпмүшелік генераторды ашу әдістері әзірленді. Бұдан шығатыны, криптографияда сәйкес генераторларды пайдалану мүмкін емес.

Блум–Блум–Шуб (BBS) ПКТ генераторы

BBS генераторы сандар теориясынан қиын тапсырма негізінде жасалған, атап айтқанда теңдеуден x санын табу

$$x^2 \equiv a \; mod \; n.$$

BBS генераторын қалыптастыру үшін сізге қажет:

1) теңдіктер орындалатын екі p және q жай сандарын таңдаңыз, олар үшін $p \equiv 3 \; mod \; 4, \; q \equiv 3 \; mod \; 4,$ яғни p және q 4 модулімен 3–пен салыстыруға болады.

2) Блумның бүтін саны деп аталатын $n = pq$ санын анықтаңыз;

3) n–мен өзара қарапайым кездейсоқ x санын таңдаңыз;

4) $x_0 = x^2 \; mod \; n$ теңдеуінен x_0 есептеңіз.

Ұзындығы $(m + 1)$ ізделетін жалған кездейсоқ реттілік болады болып табылады реттілік

$$b_0 b_1 \ldots b_m,$$

мұндағы $b_i, \; i \leq m,$ – теңдеуден анықталатын x_i санының кіші биті:

$$x_i = x_{i-1}^2 \; mod \; n.$$

n санының көбейткіштерге ыдырауын білетіндер үшін x_i мәнін (6.2) формуласы бойынша есептеуге болады:

$$x_i = x_{i-1}^2 \; mod \; n, \qquad (6.2)$$

мұндағы

$$a = 2^i \; mod \; (p-1)(q-1).$$

Бұл алгоритм жоғары криптографиялық төзімділікті қамтамасыз етеді, өйткені p және q факторларын білместен, n құрама Модулінің квадрат түбірлерін есептеу қиындығына байланысты тізбекті қалпына келтіру қиын.

RSA реттілік генераторы

RSA реттілік генераторы RSA алгоритмінің криптографиялық беріктігіне және құпия кілтті білмей түрлендіру Модулінің кері есептеу тапсырмасының күрделілігіне негізделген. RSA криптожүйесі құрылды делік, яғни құпиямен бір жақты функцияның аналогы таңдалды. Естеріңізге сала кетейік, RSA жүйесі келесі параметрлермен анықталады:

1) $p, \; q$ жай сандар және $n = pq$ сан;

2) e саны $\varphi \; (n)$ – мен өзара жай, мұндағы $\varphi \; (n) \; = \; (p-1)(q-1)$;

3) теңдеуден анықталатын d саны $ed = 1 \; mod \; n.$

Ізделетін ұзындығы $m+1$ болатын жалған кездейсоқ тізбек,келіс түрдегі тізбек болады

$$b_0 b_1 \dots b_m,$$

мұндағы $b_i, i \leq m$, теңдеуден анықталатын x_i санының кіші биті:

$$x_i = x_{i-1}^e \, mod \, n.$$

Бұл генератор құпия кілтті білмей кері түрлендіруді есептеудің күрделілігіне негізделген d. реттілік кезеңі n модулінің қасиеттерімен және ашық экспоненттің мәнімен анықталады e. криптографиялық төзімділікті арттыру үшін бірнеше кіші биттерді қолдануға немесе x_i шығыс мәндерін хэштеуді қолдануға болады. бұл тәсіл генератордың ішкі күйі туралы ақпараттың ағып кетуіне жол бермейді және оның криптоаналитикалық шабуылдарға төзімділігін арттырады.

Кері байланыс жылжу регистрлері

Жалған кездейсоқ тізбекті құрудың бір жолы кері байланыс ауысым регистріне негізделген. Кері байланыс ауысу регистрі – бұл әрқайсысында бір бит мәні бар жад ұяшықтарының жиынтығы–0 немесе 1. Псевдо кездейсоқ реттік битті құрудың әр қадамында жад деп аталатын белгілі бір жад ұяшықтарының мазмұны кері байланыс функциясымен түрлендіріледі. N жад ұяшықтары бар регистрде сымдардың саны k-ге тең болсын. егер

$$a_1, a_2, \dots, a_k,$$

жады ұяшықтарының биттерінің мәні, олар сымдар, кері байланыс кейбір функция болып табылады

$$F(a_1, a_2, \dots, a_k),$$

бит мәнін есептейтін k айнымалыларынан

$$\beta = F(a_1, a_2, \dots, a_k).$$

Бұл жерде a_i, $i = 1, 2, \dots, k$ мәндеріндегі i төменгі индекстер Регистр ұяшықтарының нөмірлеріне сәйкес келмейтінін, бірақ жолдардың реттік нөмірлері екенін ескеріңіз. Есептейтін осы биттің мәні функция, қалған биттерді бір позицияға оңға жылжытқаннан кейін сол жақ Регистр ұяшығына жазылады. Сдысу регистрінен шығатын ең оң жақ бит жалған кездейсоқ реттілік элементінің кезекті мәні болып табылады. Регистрдің ең оң жақ ұяшығы шығару ұяшығы болуы мүмкін екенін ескеріңіз. Басқаша айтқанда, жадтың оң жақ ұяшығының бит мәні жалған кездейсоқ тізбектің келесі мәні

ғана емес, сонымен қатар $F(a_1, a_2, \ldots, a_{k)}$ функциясының дәлелі болып табылады. «Ең сол жақ ұяшық» және «ең оң жақ ұяшық» бағдарлары сенімділік үшін алынады, бұл пайымдау қауымдастығын бұзбайды.

Кері байланыс функциялары ретінде сызықтық емес функцияларды қолдану сенімдірек, бірақ іс жүзінде оны жүзеге асыру қиын. Сондықтан қазіргі уақытта *LSFR* (*Linear Feedback Shift Register*) сызықтық кері байланыс сдысу регистрлері кеңінен қолданылады және зерттелуде. LSFR сызықтық кері байланыс сдысу регистрлері криптоға төзімді емес. Сондықтан олар жалған кездейсоқ реттілік генераторларын жобалау үшін блоктар ретінде қолданылады.

LSFR қасиеттері екілік көпмүшенің қасиеттерімен байланысты

$$\Phi(x) = a_N x^N + a_{N-1} x^{N-1} + \ldots + a_1 x + 1,$$

мұндағы N регистрдегі ұяшықтар саны, ал a_i , $1 \leq i \leq N$ және x мәндері 1 немесе 0. Нөлге тең емес a_i сандары сызықтар болып табылатын Регистр ұяшықтарының сандарына сәйкес келеді. Егер белгілі бір көпмүшені қарастыратын болсақ, мысалы

$$\Phi(x) = x^8 + x^7 + x^5 + x^3 + 1$$

онда бұл көпмүше сегіз ұяшық регистріне сәйкес келеді. Бұл регистрдегі жолдар 3, 5, 7, 8 сандары бар ұяшықтар болып табылады. Функция ретінде

$$F(a_8, a_7, a_5, a_3)$$

сіз келесіні таңдай аласыз

$$F(a_8, a_7, a_5, a_3) = a_8 + a_7 + a_5 + a_3,$$

мұндағы a_8, a_7, a_5 және a_3сәйкес сандары бар Регистр ұяшықтарында мәндер бар.

LSFR тудыратын жалған кездейсоқ тізбектегі ең үлкен кезең генераторға қарабайыр көпмүше сәйкес келген жағдайда болады. Бұл жағдайда жалған кездейсоқ реттілік кезеңі $(2^N - 1)$ болады.

Қолданылған әдебиеттер тізімі

1. Ахметов Б.С., Корченко А.Г., Сиденко В.П., Сеилова Н.А. Прикладная криптология:методы шифрования / Ахметов. – М.: Лантар, 2021. – 516 с.

2. Ященко В.В. Введение в криптографию. / Под общ. ред. В.В. Ященко. – М.: МЦНМО, «ЧеРо.», 2018. – 212 с.

3. Применко Э.А. Алгебраические основы криптографии / Применко Э.А. – М.: «Кудиц-образ», 2017. – 468 с