Kirish

Inson hayotda duch keladigan hodisalar, jarayonlar, narsalarning aksariyati tasodifiy xususiyatga ega. Ularni yetarlicha tavsiflash, o'rganish va modellashtirish uchun deterministik usullardan foydalanishning o'zi etarli emas (ba'zi bir algoritm bilan to'liq aniqlanadi), shuning uchun tasodifiy sonlar ketma-ketligi va ularni hosil qiluvchi qurilmalar va algoritmlar (tasodifiy ketma-ketliklarning generatorlari) fanda keng qo'llaniladi. muhandislik, aloqa va axborot texnologiyalari. Axborot xavfsizligi kabi sohada tasodifiy ketma-ketliklar alohida rol o'ynaydi. Axborot xavfsizligi muammosini hal qilishning eng samarali va istiqbolli yondashuvlaridan biri bu kriptografik usullardan foydalanish bo'lib, unda tasodifiy ketma-ketlik generatorlari ko'pincha asosiy komponentlar bo'lib, asosan ularning ishonchliligini belgilaydi. Taklif etilayotgan qo'llanmada tasodifiy ketma-ketliklar, ulardan foydalanish, olish va sinovdan o'tkazish haqida asosiy ma'lumotlar keltirilgan.

Qo‘llanma 5 bo‘lim, ilova va tavsiya etilgan adabiyotlar ro‘yxatidan iborat. Har bir bo'lim o'rganilayotgan materialning o'zlashtirilishini nazorat qilish uchun savollar bilan birga keladi. Birinchi bo'limda tasodifiy sonlarni qo'llash sohalari va ularni olish usullari haqida ma'lumotlar mavjud. Ikkinchi va uchinchi bo'limlar mos ravishda haqiqiy tasodifiy va psevdo tasodifiy ketma-ketliklarning generatorlariga bag'ishlangan. Generatorning ishlashining umumiy tamoyillari ko'rib chiqiladi, ularning tasnifi, asosiy ishlab chiqarish usullari, xarakteristikalari, shuningdek, amalga oshirish misollari keltirilgan. Haqiqiy tasodifiy ketma-ketlik generatorlari uchun qayta ishlashdan keyingi jarayon muhokama qilinadi. To'rtinchi bo'lim psevdo-tasodifiy ketma-ketliklarning kriptoga chidamli generatorlarining ta'riflarini, bunday generatorlarga qo'yiladigan talablarni, ularning asosiy turlarini o'z ichiga oladi. Beshinchi bo'limda tasodifiy ketma-ketlik generatorlari sifatini tekshirishning asosiy yondashuvlari ko'rsatilgan. Eng keng tarqalgan test to'plamlari qisqacha tavsiflanadi. NIST STS statistik testlarining taniqli to'plami batafsil ko'rib chiqiladi. Ba'zi yangi sinov vositalari haqida ma'lumot beradi. Ilovada ehtimollar nazariyasi, matematik statistika va chekli maydonlar nazariyasidan kerakli materiallar mavjud.

Qo‘llanma “Axborot xavfsizligi” (10.03.01 va 10.04.01) yo‘nalishi bo‘yicha axborot xavfsizligi va xususan, axborotni himoya qilishning kriptografik usullaridan foydalanish bilan bog‘liq fanlarni o‘rganuvchi talabalar uchun mo‘ljallangan.

Qo'llanmada keltirilgan materialni ishlab chiqish ehtimollik nazariyasi asoslarini, chekli maydonlar nazariyasini bilishni, shuningdek, 5 ta shifrlash algoritmi haqida asosiy tushunchani talab qiladi. 1-3 bo'limlar tasodifiy ketma-ketliklar va ularni yaratish usullari bilan tanishtirish uchun mo'ljallangan. Ular birinchi navbatda bakalavriat talabalariga qaratilgan. 4 va 5 bo'limlardan kriptografiyaga ixtisoslashgan bakalavrlarga dars berishda foydalanish maqsadga muvofiqdir.

**1-bo'lim. Tasodifiy ketma-ketliklar. Ilovalar va ishlab chiqarish usullari**

**1.1 Tasodifiy ketma-ketliklar va ularning qo'llanilishi**

Atrofimizdagi narsalar, hodisalar va davom etayotgan jarayonlarning aksariyati tasodifiy xarakterga ega. Adekvat tavsif, o'rganish va modellashtirish uchun deterministik yondashuvlar ko'pincha etarli emas, shuning uchun turli muammolarni hal qilish uchun stokastik (ya'ni tasodifiy xarakterga ega) usullardan foydalanish tabiiydir. Shu munosabat bilan tasodifiy sonlar, bunday sonlar ketma-ketligi va ularni hosil qiluvchi generatorlar fan, texnika, aloqa, turli axborot texnologiyalari, shuningdek, kundalik hayotning ko‘p jabhalarida tobora ko‘proq foydalanilmoqda [1-13].

Tarixan kuzatishlarni tanlab olish uchun uzluksizlar o'rniga tasodifiy sonlar qo'llanila boshlandi. Tasodifiy raqamlar murakkab hisoblash masalalarini hal qilishda va hisoblash usullarini amalga oshirishda qo'llaniladi (masalan, Monte-Karlo usuli). EHMlarning rivojlanishi, bir tomondan, tasodifiy sonlardan foydalangan holda masalalar doirasini kengaytirsa, ikkinchi tomondan, ularni yaratish sifatiga yuqori talablar qo‘ydi. Vaqt o'tishi bilan tasodifiy sonlar informatika, taqsimlangan hisoblash, kriptografiya va boshqa sohalarda hal qiluvchi rol o'ynay boshladi.

Raqamlar ketma-ketligi, agar algoritmni va barcha dastlabki ma'lumotlarni bilgan holda uni takrorlashning iloji bo'lmasa, tasodifiy deb ataladi (generatorni bir xil sharoitda ikki marta ishga tushirib, biz turli xil ketma-ketliklarni olamiz). Ammo kompyuter tizimlari deterministikdir; ular qat'iy belgilangan holatlar to'plami bilan tavsiflanadi (bunday holatlar soni juda ko'p bo'lishi mumkin, lekin cheklangan). Bu ular yaratadigan ketma-ketliklar davriy va takrorlanadigan bo'lishiga olib keladi - bunday ketma-ketliklar psevdo-tasodifiy deb ataladi. Ma'lumki, davriy hamma narsa ma'lum darajada bashorat qilinadi; tasodifiy bo'lmagan. Haqiqiy tasodifiy ketma-ketliklarni olish juda mashaqqatli. Bundan tashqari, har bir jismoniy yoki axborot jarayoni ularni yaratish uchun mos emas.

Tasodifiy ketma-ketliklar inson faoliyatining turli sohalarida qo'llaniladi. Quyida tasodifiy ketma-ketliklar eng intensiv ishlatiladigan eng mashhur sohalar ro'yxati keltirilgan.

1. **Kriptografiya.** Kriptografik usullar axborot xavfsizligini ta'minlashda asosiy hisoblanadi. Kriptografiyada tasodifiy ketma-ketliklar hal qiluvchi rol o'ynaydi. Ular, xususan, ishlatiladigan shifrlash algoritmining kalitlar ketma-ketligini olish, oqim shifrlari diapazonini yaratish, shuningdek, ishga tushirish vektorlarini (blok shifrlarini) yaratish uchun ishlatiladi.
2. **Axborotni himoya qilishning boshqa sohalari.** Tasodifiy ketma-ketliklar parollar va foydalanuvchi kalitlarini shakllantirishda ajralmas hisoblanadi (yaxshi parol tasodifiy belgilarning qisqa ketma-ketligidir). Bundan tashqari, ular turli xil ma'lumotlarni himoya qilish algoritmlari natijalariga noaniqlik kiritish uchun, shuningdek, yon kanallarning oqishidan himoya qilish algoritmlari bosqichlarining davomiyligi uchun ishlatilishi mumkin. Ular autentifikatsiya qilish uchun tasodifiy so'rovlarni yaratishda va boshqa ko'plab muammolarni hal qilishda ham kerak.
3. **Algoritm sinovi.** Muhim vazifa - dasturlarning to'g'ri ishlashini tekshirish. Sinov ancha uzoq va mashaqqatli jarayon. Uni amalga oshirish katta hajmdagi kirish ma'lumotlarini talab qiladi. Tasodifiy sonlar generatorlaridan foydalanish test samaradorligini oshiradi va vaqtni tejaydi.
4. **Tarmoq protokollari.** Tasodifiy ketma-ketliklar, masalan, seans kalitlari sifatida, shuningdek, uning turli xil amalga oshirilishining o'ziga xosligini ta'minlaydigan tasodifiy protokol parametrlarini yaratish uchun ishlatilishi mumkin.
5. **Matematik va simulyatsiya modellashtirish.** Murakkab jismoniy, texnologik va ijtimoiy-iqtisodiy tizimlar va jarayonlarni modellashtirishda tasodifiylik manbalaridan foydalanmasdan amalga oshirish mumkin emas.

Shuningdek, tasodifiy ketma-ketliklar ko'pincha sonlar nazariyasida qo'llaniladi; statistik fizika; bashorat qilish; hisoblash usullari (shu jumladan Monte-Karlo usuli); boshqaruv nazariyasi; bank, to'lov, savdo tizimlari uchun axborot texnologiyalari; xatolarni tuzatuvchi kodlash; kompyuter tizimining komponentlarini avtonom va o'rnatilgan diagnostika; radiosignallarni modulyatsiya qilish; qo’riqchi protsessorlari yordamida dasturning bajarilishini monitoring qilishda; o'yin va lotereya sanoati.

Tasodifiy ketma-ketliklar muhim rol o'ynaydigan sohalardan biri bu axborot xavfsizligi.

Axborot xavfsizligining turli jihatlarida qo'llaniladigan tasodifiy ketma-ketliklar quyidagi muammolarni hal qilish uchun ishlatiladi:

* mutlaq himoyalangan shifr sxemasiga eng yaqin sxema bo'yicha axborotni oqimli shifrlashda o'yin ketma-ketligini yaratish;
* teskari aloqa rejimida ishlaydigan blokli shifrlar uchun initsializatsiya vektorlarini shakllantirish;
* assimetrik kriptotizimlarda ba'zi parametrlarni yaratish dasturlari uchun boshlang'ich qiymatlarni olish;
* foydalanuvchi kalitlari va parollarini shakllantirish;
* ko'pchilik kriptoalgoritmlarning barqarorligi maxfiyligi va sifatiga asoslangan asosiy ma'lumotlarni shakllantirish;
* ko'p sonli kriptografik protokollarni amalga oshirishda tasodifiy so'rovlarni shakllantirish, masalan, umumiy maxfiy kalitni yaratish, sirni almashish, bit bilan bog'lash, autentifikatsiya, elektron imzo va boshqalar protokollari;
* Himoya vositalarining ishiga noaniqlikni kiritish, masalan, ehtimolli shifrlash kontseptsiyasini amalga oshirishda, bunda juda ko'p miqdordagi shifrlangan matnlar bir xil kalit bilan bir xil manba matniga mos keladi;
* Statistik testlarni amalga oshirish;
* ko'r-ko'rona shifrlashda noaniq multiplikatorlarni shakllantirish (ko'r imzo protokoli).

Axborotni himoya qilishning eng kuchli va samarali usullaridan biri bo'lgan kriptografiyada tasodifiy raqamlardan foydalanish alohida o'rin tutadi. Kriptografiyada bit ketma-ketliklari asosiy rol o'ynaydi - "0" va "1" ning tasodifiy ajratilgan qiymatlaridan iborat ikkilik ketma-ketliklar. Aynan shu ketma-ketliklar ushbu qo'llanmada "tasodifiy" deb nomlanadi.

Bir qator kriptografik transformatsiyalar uchun tasodifiy birlamchi holatlar yoki butun ketma-ketliklar qo'llaniladi. Shuning uchun bunday holatlar yoki ketma-ketliklardan foydalangan holda kriptoalgoritmning kuchi bevosita tasodifiy sonlar va ketma-ketliklarni yaratish algoritmiga, aniqrog'i, chiqish ketma-ketliklarining tasodifiylik darajasiga bog'liq.

Tasodifiy ketma-ketliklarni qo'llash sohalarining kengligi va ahamiyati, axborot xavfsizligining yuqori darajasini ta'minlashdagi hal qiluvchi roli ularni o'rganishning dolzarbligini belgilaydi.

Tasodifiy raqamlarni yaratish jarayoni ko'plab kriptografik operatsiyalarning asosiy qismidir. Masalan, kriptografik kalitlarni imkon qadar tasodifiy tanlash kerak, shunda ularning qiymatlari amalda takrorlanmaydi. Kriptografik jihatdan kuchli tasodifiy sonlar generatorlari 0,5 dan yuqori ehtimollik bilan bashorat qilib bo'lmaydigan ma'lumotlarni ishlab chiqishi kerak; bu keyingi chiqish bitini bashorat qilishning har qanday usuli tasodifiy taxmin qilishdan ko'ra samaraliroq bo'lmasligi kerakligini anglatadi.

**1.2 Pseudo-tasodifiy ketma-ketliklarni yaratish usullari**

Hozirgi vaqtda turli darajadagi tasodifiy ketma-ketliklarni yaratishning ko'plab usullari mavjud [1-4, 7-9, 14-15]. Biroq, amalda, bu generatorlarning ko'pchiligi xossalari tasodifiylik talablariga javob bermaydigan ketma-ketliklarni ishlab chiqaradi. Buning eng keng tarqalgan misollaridan biri bu ko'plab dasturlash tillarining standart kutubxonalariga o'rnatilgan psevdo-tasodifiy raqamlar generatorlari (masalan, C standart kutubxona funktsiyasi rand()). Ko'pincha bunday funktsiyalar yordamida yaratilgan raqamlarda aniq naqshlar mavjud. Misol uchun, bir seansda olingan raqamlar vaqt o'tishi bilan monoton ravishda ortadi, bu tasodifiy (va psevdo-tasodifiy) ketma-ketliklarning xususiyatlariga qo'yiladigan talablarga bevosita zid keladi. Taniqli va keng tarqalgan chiziqli kongruensial generatorlar uchun to'rtta ma'lum hosil bo'lgan raqam keyingi qiymatlarni ham taxmin qilishi mumkin.

Ko'pgina kriptografik ilovalar kerakli ma'lumotlarni shifrlaydigan va parolini hal qiluvchi kalitlarni yaratish uchun tasodifiy sonlar generatorlaridan foydalanadi. Biroq, shifrlash tizimlarining eng zaif nuqtasi ko'pincha ularda ishlatiladigan generatorlardir. Gap shundaki, dasturiy ta'minot generatorlari butunlay deterministikdir. Odatda psevdo-tasodifiy raqamlarni hisoblash uchun turli xil murakkab funktsiyalardan foydalanadilar. Shunga ko'ra, bunday generatorlarning ishlashi natijasida hosil bo'lgan ketma-ketliklar ko'proq yoki kamroq prognoz qilinadigan va takrorlanishi mumkin va, masalan, kriptografik ilovalarda foydalanish uchun mos emas. Shuni ta'kidlash kerakki, ba'zi hollarda tasodifiy ketma-ketlikni takrorlash qobiliyati foydalidir (masalan, ishlab chiquvchi tomonidan algoritmlarni sinab ko'rishda). Shu bilan birga, ketma-ketlik zararli kriptoanalitikga himoyalangan dastur yoki protokolning ishlashini tahlil qilish jarayonida uni qayta tiklashga imkon beradigan xususiyatlarga ega bo'lmasligi kerak.

Tasodifiy ketma-ketliklarni yaratishning jadval usuli mavjud. Bu tasodifiy raqamlar RAMda yoki tashqi muhitda saqlanadigan jadval, qog'oz yoki elektron ko'rinishda taqdim etilishidadir. Tasodifiy sonlar jadvalining variantlaridan biri va ularni tanlash usuli GOST R ISO 24153-2012 (Statistik usullar. Tasodifiy namunani tanlash va tanlash tartibi). Ushbu usulning afzalligi shundaki, u bir xil psevdo-tasodifiy raqamlar ketma-ketligini takrorlash uchun ishlatilishi mumkin. Biroq, amaliy muammolarni hal qilishda bunday generatorlardan foydalanishga imkon bermaydigan jiddiy kamchilik - mavjud raqamlarning cheklanganligi. Shuningdek, ushbu yondashuv bilan kompyuter hisoblash resurslaridan samarasiz foydalanish mumkin (masalan, jadval yoki uning qismlarini operativ xotirada saqlash yoki tashqi xotiraga kirish zarurati tufayli). Hozirgi vaqtda bu nasl berish usuli kamdan-kam qo'llaniladi.

Yaratilgan ketma-ketlikning sifatiga jiddiy talablar qo'yiladigan muammolarni hal qilishda keng qo'llaniladigan va qo'llaniladigan psevdo-tasodifiy ketma-ketlik generatorlari(PTKKG) orasida apparat, dasturiy ta'minot va apparat-dasturiy ta'minot (aralash) mavjud.

Uskuna tasodifiy sonlar generatori - bu davom etayotgan jismoniy jarayonning o'lchangan, xaotik ravishda o'zgaruvchan parametrlari asosida tasodifiy sonlar ketma-ketligini hosil qiluvchi qurilma. Ishlab chiqarishning apparat usuli bilan tasodifiy sonlar entropiyaning ishonchli manbai bo'lib xizmat qiladigan ba'zi jismoniy miqdorlarning o'lchovlarining bevosita yoki qo'shimcha mahsulotidir. Odatda bu jonsiz tabiatda sodir bo'ladigan jarayonlar. Nazariy jihatdan, bunday jarayonlarni mutlaqo oldindan aytib bo'lmaydi, lekin amalda bu tarzda olingan tasodifiy sonlar maxsus statistik testlar yordamida tekshirilishi kerak. Eng yaxshi statistik xususiyatlarga va shunga mos ravishda yuqori darajadagi tasodifiylikka qaramay, apparat generatorlari quyidagi kamchiliklarga ega:

-PTKKG dasturiy ta'minoti bilan solishtirganda loyihalash, o'rnatish va sozlash uchun potentsial yuqori vaqt va moddiy xarajatlar;

-PTKKG dasturiy ta'minotini amalga oshirishga qaraganda tasodifiy sonlarni yaratish tezligining pastligi [14, 15];

-oldindan yaratilgan raqamlar ketma-ketligini takrorlashning mumkin emasligi (ba'zi hollarda bu istalmagan).

Dasturiy ta'minot (algoritmik) generatorlari (psevdotasodifiy ketma-ketlik generatorlari) deterministik algoritmlarga asoslanadi. Shu tarzda olingan ketma-ketliklar har doim davrga ega (ba'zan juda katta bo'lsa ham) va tasodifiylikdan boshqa og'ishlar ham kuzatiladi. Cheklangan resurslarga ega har qanday PTKKG ertami-kechmi tsiklga kiradi - u bir xil raqamlar ketma-ketligini takrorlashni boshlaydi. PTKKG davri generator turiga va uning parametrlariga bog'liq [1, 4, 7, 9]. Agar yaratilgan PTKKG ketma-ketligi juda qisqa muddatga ega bo'lsa, bunday PTKKG ko'plab amaliy ilovalar uchun yaroqsiz bo'ladi.

Ko'pgina oddiy arifmetik generatorlar tez bo'lishiga qaramay, ko'plab jiddiy kamchiliklarga ega:

- juda qisqa muddat

-ketma-ket qiymatlar mustaqil emas;

- ba'zi bitlar boshqalarga qaraganda "kam tasodifiy";

- notekis taqsimlash;

- qaytaruvchanlik.

Aslida, bunday generatorlarning natijasi tasodifiy ketma-ketlik emas. Biroq, dasturiy ta'minot generatorlari tomonidan ishlab chiqarilgan ketma-ketliklar ma'lum talablarga ega, chunki ular ma'lum darajada tasodifiy ketma-ketliklarni simulyatsiya qilishlari kerak. Xususan, bunday ketma-ketliklarning davri etarlicha katta bo'lishi kerak, shuning uchun kerakli uzunlikdagi ketma-ketlikni yaratishda hech qanday takrorlash sodir bo'lmaydi. Uskuna generatorlaridan farqli o'laroq, dasturiy ta'minot generatorlari ilgari yaratilgan ketma-ketlikni takrorlay oladi, bu ba'zi hollarda shubhasiz afzallikdir.

**Dasturiy ta'minot va apparat generatorlari.** Bunday generator tasodifiy shovqin oqimini yaratishi mumkin, keyinchalik u raqamlarga aylanadi. Shuningdek, "don" (ya'ni, shifrlash algoritmining ba'zi kirish ma'lumotlari) apparat generatori yordamida yaratilishi mumkin (chunki uning hajmi juda kichik va shunga mos ravishda uni ishlab chiqarish katta vaqt va resurslarni talab qilmaydi). va oxirgi ketma-ketlik dasturiy ta'minotdan foydalanishdir.

Dasturiy ta'minot va apparat tasodifiy sonlar generatorlari, masalan, kompyuter qurilmalarini o'z ichiga olishi mumkin. Xususan, kompyuter qurilmalarining shovqini (masalan, protsessor), tizim vaqti, tugmalar bosish orasidagi vaqt oraliqlari, sichqonchaning harakatlari va boshqalar tasodifiy ketma-ketlikning manbai bo'lishi mumkin. Qoida tariqasida, bunday jarayonlardan kelib chiqadigan ketma-ketliklar keyingi ishlov berishni talab qiladi. Bundan tashqari, ularni ishlab chiqarish tezligi ancha past (ayniqsa, etarlicha katta hajmdagi ketma-ketliklarni yaratishda). Bunday generatorlar qatoriga, xususan, Linux OS ning psevdo-qurilmalari /dev/random va /dev/urandom kiradi.

Keyingi bo'limlarda yuqorida tavsiflangan tasodifiy ketma-ketliklarni yaratishga yondashuvlar, shuningdek, tasodifiy ketma-ketlik generatorlarini statistik sinovdan o'tkazish jarayoni batafsilroq ko'rib chiqiladi.

Agar ketma-ketlikni takrorlash imkoni bo'lmasa, u haqiqiy tasodifiy (ИСП->HTKK) deyiladi. Bu shuni anglatadiki, agar siz haqiqiy tasodifiy ketma-ketlik generatorini bir xil kirish bilan ikki marta ishlatsangiz, u o'z chiqishida turli xil tasodifiy ketma-ketliklarni ishlab chiqaradi. Asosiy qiyinchilik tasodifiy ketma-ketlikni tasodifiy bo'lmagandan ajrata olishdir.

Biroq, amalda haqiqiy tasodifiy sonlar manbalarining chiqish ma'lumotlaridan to'g'ridan-to'g'ri foydalanish har doim ham mumkin emas. Shuning uchun, odatda, psevdo-tasodifiy ketma-ketliklardan foydalanish kerak. Pseudo-tasodifiy ketma-ketlik (PTKK) - berilgan deterministik algoritm tomonidan yaratilgan, lekin tasodifiy sonlar sifatida ishlatiladigan psevdo-tasodifiy ikkilik raqamlar ketma-ketligi. Bunday holda, PTKKni olish algoritmlarida odatda maxsus tasodifiy boshlang'ich qiymat yoki "don" (urug') ishlatiladi. PTKKlarni tasodifiy ketma-ketliklar sifatida ishlatish uchun ular statistik xususiyatlari bo'yicha HK ga yaqin bo'lishi kerak.

* 1. jadval - HTKK va PTKK ning xarakteristikalari

|  |  |  |
| --- | --- | --- |
| Xarakteristika | tasodifiy ketma-ketliklar | Psevdo-tasodifiy ketma-ketliklar |
| Davriylikning yo'qligi | ha | yo’q |
| Oldindan aytib bo’lmaydigan | ha | shartli |
| Qiymatlar erkinligi | ha | shartli |
| Xavfsizlik darajasi | yuqori | shartli |
| Generatsiya tezligi | past | yuqori |
| Takrorlanuvchanlik | yo’q | ha |
| Oddiy generatsiya | yo’q | ha |
| Generatsiya turg’unligi | yuqori | past |

Tasodifiylik mikro darajada (kvant mexanikasi) mavjudligini bilamiz, ammo makro darajaga o'tishda bu tasodifiylik saqlanib qoladimi yoki yo'qmi noma'lum. Tasodifiy ketma-ketlikning qo'shimcha xususiyati shundaki, tasodifiy ketma-ketlikni siqib bo'lmaydi.

Sifatli tasodifiy sonlar generatoriga qo'yiladigan talablar:

1. Ish natijalarining oldindan aytib bo'lmaydiganligi: noma'lum kalit / generatorning boshlang'ich holati bilan, RRPning ma'lum yakuniy qismiga asoslanib, uning keyingi elementini ham (to'g'ridan-to'g'ri oldindan aytib bo'lmaydigan yoki o'ng tomonda oldindan aytib bo'lmaydigan) aniqlash mumkin emas, va oldingi (teskari oldindan aytib bo'lmaydigan, chapga oldindan aytib bo'lmaydigan);
2. Haqiqiy tasodifiy ketma-ketlikning o'xshash xususiyatlaridan hosil bo'lgan PSPlarning statistik xususiyatlarining farqlanmasligi;
3. Katta ketma-ketlik davri;
4. Apparat va dasturiy ta'minotni samarali amalga oshirish imkoniyati.

Amalda, odatda, bu barcha shartlarning bajarilishiga erishish mumkin emas. Bundan tashqari, bu shartlar ko'pincha bir-birini istisno qiladi. Shuning uchun ular o'rtasida muvozanatni izlash va birinchi navbatda, hal qilinayotgan vazifa kontekstida eng muhim bo'lgan narsani bajarishga intilish kerak.

Ko'pincha eng yaxshi natijalar tasodifiy ketma-ketliklarni yaratish uchun turli usullarni birlashtirish orqali olinadi. Masalan, dastlabki ma'lumotni apparat generatori yordamida olish mumkin, yakuniy ketma-ketlikning o'zi esa apparat generatoridan dastlabki ma'lumotlarni kirish sifatida qabul qilgan dasturiy ta'minot yordamida olinishi mumkin.

1. **bo'lim. Haqiqiy tasodifiy ketma-ketliklarning generatorlari**

Haqiqiy tasodifiy ketma-ketliklar (HTKK) ketma-ketlik sifatida taqdim etilgan tasodifiy sonlardir. Tasodifiy raqamlar - bu ba'zi tasodifiy o'zgaruvchilarning realizatsiyasi. Tasodifiy o'zgaruvchi - bu ma'lum ehtimollik bilan haqiqiy qiymatlarni qabul qiladigan elementar hodisalar fazosidagi funktsiya. Shunday qilib, haqiqiy tasodifiy ketma-ketliklar statistik jihatdan bir-biridan mustaqil bo'lgan va tajriba natijasida oldindan aytib bo'lmaydigan ko'plab qiymatlardan birini qabul qiladigan qiymatlar ketma-ketligidir. Tasodifiy o'zgaruvchining qiymatlari va mos keladigan ehtimolliklar o'rtasidagi bog'liqlik taqsimot funktsiyasi yoki u bilan bog'liq bo'lgan ehtimollik zichligi funktsiyasi yordamida aniqlangan taqsimot qonuni bilan tavsiflanadi. Haqiqatan ham tasodifiy ketma-ketliklar bir xil taqsimotga ega bo'lishi kerak.

Haqiqiy tasodifiy ketma-ketliklarning generatorlari tasodifiy ketma-ketliklarni olish uchun ham makro darajada, ham mikro darajada sodir bo'ladigan jismoniy jarayonlarning ob'ektiv ravishda mavjud tasodifiyligidan foydalanadigan qurilmalardir. Qoida tariqasida, bunday generatorlar apparat yoki dasturiy-apparat hisoblanadi.

**2.1 Ishlash tamoyillari**

Uskuna tasodifiy ketma-ketlik generatorlarida tasodifiy sonlarni yaratish uchun entropiya manbalari ishlatiladi, masalan:

-termik va elektr shovqinlari;

-kvant jarayonlari;

-radioaktiv parchalanish;

-kosmik nurlanish;

-turli mexanik, optik va fotoelektrik hodisalar.

Haqiqiy tasodifiy ketma-ketliklarni yaratish uchun mos keladigan entropiya manbalarining o'ziga xos misollari:

- radioaktiv parchalanish vaqtida zarrachalar emissiyasi orasidagi vaqt oraliqlari;

-yarim o'tkazgichli diod yoki rezistorning termal shovqini;

- fotonlarning chigallanish holatlari;

-lazerlarning kvant shovqini;

- otishni o'rganish shovqini;

- osilatorlar chastotasining beqarorligi.

Uskuna-dasturiy ta'minotning haqiqiy tasodifiy generatorlari kompyuter uskunasining ishlashiga xos bo'lgan tasodifiylikka asoslanadi, masalan, tizim soati ko'rsatkichlari, protsessor yuklanish darajasi, tarmoq paketining kelishi o'rtasidagi kechikishlar, sichqonchani yoki klaviaturani bosish orasidagi vaqt oralig'i, kiritish/chiqish buferlarining tarkibi, protsessor shovqini yoki boshqa qurilmalar.

Tasodifiy ketma-ketliklar generatori (TKKG) ning amalda qo'llanilishiga ularning xususiyatlari to'sqinlik qilishi mumkin, masalan:

- ishning past tezligi;

- qayta o'ynash, takrorlash va protsessor bilan o'zaro ta'sir qilishning murakkabligi;

- o'lchovlar jarayonida tizimli xatolar yoki statistik sinovlar paytida aniqlangan to'lqin yoki boshqa davriy (tasodifiy bo'lmagan) komponentlarning mavjudligi bilan bog'liq bo'lgan ketma-ketlikdagi og'ishlar va korrelyatsiyalar.

TKKG operatsiyasining natijasi qo'shimcha ishlov berishni talab qilishi mumkin (post-processing deb ataladigan).

Olingan tasodifiy ketma-ketlik to'g'ridan-to'g'ri ishlatilishi yoki psevdo-tasodifiy ketma-ketlik generatoriga kiritilishi mumkin.

Tasodifiy ma'lumotlar manbalari orasida kvant fizikasi doirasida tasvirlangan jarayonlar alohida o'rin tutadi. Ularning ehtimollik tabiati nazariy jihatdan haqiqiy tasodifiy ketma-ketliklarni olish imkonini beradi. Radioaktiv parchalanish hodisalari, chigal kvant holatlari, lazer kvant shovqini, vakuumdagi kvant tebranishlari, fotonlarni chiqarish va aniqlash jarayonlari asosida haqiqiy tasodifiy sonlarning kvant generatorlari mavjud va yaratilmoqda.

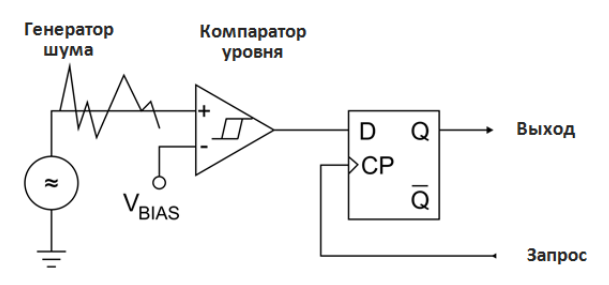
Turli tabiatdagi fizik hodisalar, agar ular tasodifiy tebranishlar bo'lsa, "tasodifiy shovqin" (oq shovqin) deb ataladi.

Tasodifiy shovqinning taniqli misoli termal shovqin yoki Jonson shovqinidir. Bu elektr qarshiligiga ega bo'lgan va mutlaq noldan yuqori haroratda bo'lgan har qanday material uchun o'lchanadigan kuchlanish tebranishlari. Bunday tebranishlarning sababi tasodifiy xarakterga ega bo'lgan elektr zaryad tashuvchilarning issiqlik harakatidir. Ammo shuni ta'kidlash kerakki, ko'rsatilgan kuchlanish haqiqatda mutlaqo tasodifiy emas, chunki elektr zaryadlarining harakatlarida korrelyatsiyalarni keltirib chiqaradigan o'tkazgichlarda tashuvchilarning ma'lum korrelyatsiyalari mavjud.

Yarimo'tkazgichli zener diodlarida kuzatilgan Zener tunnel effekti (buzilish zonasida teskari yo'nalish sharoitida ishlashi mumkin bo'lgan maxsus Zener diodlari) tashuvchilar kvant to'sig'idan o'tganda ("pushti shovqin" deb ataladi) tasodifiy kuchlanish sakrashiga olib keladi. Shu bilan birga, Zener effekti jismoniy qurilmalarda boshqa effektlardan to'liq ajratilmagan. Bundan tashqari, qarshiliklar va zener diodlardagi yuqoridagi jarayonlar xotira effekti bilan tavsiflanadi: qurilmadagi oniy kuchlanish yaqin o'tmishdagi kuchlanishga bog'liq. Bu shu tarzda olingan raqamlarning korrelyatsiyasiga olib keladi va bunday ketma-ketlikni haqiqatdan ham tasodifiy deb atash huquqini bermaydi.

Shovqinning boshqa mashhur manbalarini, masalan, bipolyar tranzistorlarda baza-emitterning buzilishi, lazer fazasi shovqini, tartibsiz shovqin va boshqalarni eslatib o'tish mumkin. Biroq, barcha bu shovqin manbalari uchun umumiy muammo shundaki, ular yaratadigan tasodifiylikni mutlaqo aniq nazorat qilib bo'lmaydi. mos keladigan qurilma yoki o'lchovni ishlab chiqarishda. Voltaj qiymatlari (masalan, Jonson shovqini uchun) juda kichik bo'lishi mumkin, bu raqamlashtirishdan oldin sezilarli kuchaytirishni talab qiladi. Bu kuchaytirgichning cheklangan tarmoqli kengligi va chiziqli bo'lmagan daromad tufayli qo'shimcha o'zgarishlarni qo'shadi. Tasodifiy ketma-ketlik generatori pallasida qo'llaniladigan ikkilik mantiqning tez almashinuvi kuchli elektromagnit shovqinlarni keltirib chiqaradi, buning natijasida yaqin atrofdagi generatorlar (ayniqsa, bitta chipda joylashganlar) odatda o'zaro sinxronlashadi, bu esa umumiy entropiyaning keskin pasayishiga olib keladi. Haqiqiy tasodifiy ketma-ketlikdagi shovqin generatorlariga juda sezgir kuchaytirgichlar ta'sirida kriptografik hujumlar xavfi ham mavjud.

Shovqin manbalariga asoslangan haqiqiy tasodifiy ketma-ketliklar generatorini qurishning asosiy g'oyasi quyidagicha. Shovqin manbasidan keladigan tasodifiy analog kuchlanish vaqti-vaqti bilan namuna olinadi, kuchaytiriladi va oldindan tanlangan chegara bilan taqqoslash uchun komparatorga beriladi. Agar bu chegara oshib ketgan bo'lsa, "1" qiymati hosil bo'ladi, aks holda "0" hosil bo'ladi. Chegara shunday o'rnatilishi mumkinki, "1" va "0" ning paydo bo'lish ehtimoli taxminan teng bo'ladi. Eshik chegarasini sozlash jarayoni murakkab, ko'p vaqt talab etadi va shovqin generatori ko'rsatkichlarining sezilarli buzilishiga olib kelishi mumkin.



* 1. rasm - Shovqin manbalariga asoslangan haqiqiy tasodifiy ketma-ketliklar generatorining sxemasi.

Generator chiqishining tasodifiyligini yaxshilash, xususan, xom shovqin oqimida mavjud bo'lgan moyillikni kamaytirish uchun yuqoridagi asosiy sxemaga turli xil o'zgartirishlar taklif etiladi. Bunday yechimlardan biriga Bagini-Bucci generatorini misol qilib keltirish mumkin.

Umuman olganda, shovqinga asoslangan har qanday tasodifiy ketma-ketlik generatorining ishonchliligi quyidagi omillarga bog'liq:

-ishlatiladigan shovqin manbasining tasodifiylik darajasi;

-signallarni tanlash va raqamlashtirish protseduralarining ta'siri;

-deterministik postprocessingdan foydalanish zarurati.

Natijada, ko'rsatilgan sabablarga ko'ra, shovqinga asoslangan TKKG ishonchliligini isbotlash deyarli imkonsiz bo'lib qoladi.