Дәріс 10. Псевдокездейсоқ тізбекті генераторлар

Дәріскер: PhD Темирбекова Ж.Е.

Жоспар

- ПТГ генераторлары
- • Кілттің кездейсоқтығын қамтамасыз етеді
- • Криптожүйелердің тұрақтылығына әсер етеді
- • Компьютердегі барлық генераторлар мерзімді

ПТГ қолданылуы

- 1) Гаммалық тізбектер
- 2) Хэштеу
- 3) Негізгі ақпарат қалыптастыру
- 4) Криптографиялық хаттамалар
- 5) Белгісіздік енгізу

ПТГ талаптары

- • Криптографиялық төзімділік
- • Жақсы статистикалық қасиеттер
- • Үлкен кезең
- • Тиімді жүзеге асыру

ПТГ жіктелуі

- Криптографиялық әдістер:
- • Ағындық шифрлар
- • Блоктық шифрлар
- • Біржақты функциялар
- • Ашық кілтті шифрлар

Криптографиялық емес әдістер:

- • Сәйкес генераторлар
- • Кері байланыс регистрлері

Блум-Блум-Шуб (BBS) ПКТ генераторы

- Сызықтық конгруентті генератор (СКГ)
- $X_{n+1} = (aX_n + c) \bmod m$
- • Өнімді
- • Бірақ криптографияда қолдануға болмайды
- *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.

Дәріс 10

- СКГ қасиеттері
- • Период шарттары
- • Өнімділігі жоғары
- • Болжауға болатындықтан әлсіз

Блум-Блум-Шуб (BBS) генераторы

- • Қиын есепке негізделген
- • Жоғары криптографиялық қауіпсіздік
- • Кіші биттерден кездейсоқ реттік құрайды

BBS жұмыс принципі

- 1) p, q жай сандар таңдау
- 2) n = pq
- 3) x_0 таңдау
- 4) $x_{n+1} = x_n^2 \bmod n$

RSA реттілік генераторы

- • RSA алгоритміне негізделген
- • Кері есептеу қиын
- • Шығыс биттері – кіші биттер

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 $ed = 1\ mod\ n$.

RSA генераторы артықшылықтары

- • Қауіпсіздік жоғары
- • Хэштеумен жақсартуға болады

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:

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

Кері байланыс жылжу регистрлері (LFSR)

- • Жад ұяшықтары
- • Сдысу және кері байланыс
- • Жалған кездейсоқ тізбекқұрады

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

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

$$\beta = F(\, a_1, a_2, \dots, a_{k)}.$$

LFSR қасиеттері

- • Сызықтық көпмүшелерге негізделген
- • Қарабайыр көпмүше → максималды период

LSFR қолданылуы

- • Тікелей крипто ретінде әлсіз
- • Бірақ ПТГ блоктары ретінде қолданылады

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.

Қорытынды

- • ПТГ – криптография негізі
- • Дұрыс генератор таңдау өте маңызды
- • BBS және RSA – жоғары деңгейлі қауіпсіз генераторлар

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