DOI: 10.6084/m9.figshare.9788447
УДК 519.725

Баліна Олена Іванівна
Кандидат технічних наук, доцент кафедри інформаційних технологій проектування і прикладної математики, *orcid.org/0000-0001-6925-0794*
Київський національний університет будівництва і архітектури, Київ
Буценко Юрій Павлович
Кандидат фізико-математичних наук, доцент кафедри математичного аналізу та теорії імовірностей, *orcid.org/0000-0003-4806-9587*
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ
Савченко Юлій Григорович
Доктор технічних наук, професор кафедри звукотехніки та реєстрації інформації, *orcid.org/0000-0002-7123-9165*
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ

АЛГОРИТМИ ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ БІНАРНИХ ПОСЛІДОВНОСТЕЙ

Анотація. *Задачі захисту інформації наразі належать до найактуальніших при дослідженні телекомунікаційних систем.Це вимагає використання якомога більш досконалих процедур шифрування.Розглянуто задачу побудови узагальненого опису процедури формування псевдовипадкових числових послідовностей, що використовуються як ключі при шифруванні інформаційного обміну в телекомунікаційних системах обмеженого доступу, а також моделюванні зовнішніх впливів при діагностуванні технічного стану цифрових пристроїв. Показано, що ця задача безпосередньо пов'язана із задачею кількісної оцінки якості псевдовипадкової послідовності з точки зору її наближення до істинно випадкової. На відміну від традиційного підходу, що базується на використанні для генерації послідовностей цього класу лінійних регістрових фільтрів, запропоновано застосувати універсальні моделі цифрових автоматів (моделі Мілі та Мура). Такий підхід суттєво збільшує комбінаторне різноманіття можливих алгоритмів генерації, що утруднює криптоаналіз та, по суті, збільшує захищеність інформаційних систем з обмеженим доступом. В той же час практична реалізація відповідних процедур формування псевдовипадкових числових послідовностей може бути здійснена як програмно, так і апаратно без ускладнень.*

Ключові слова: захист інформації; процедури шифрування; псевдовипадкові послідовності; цифрові автомати; моделі Мілі та Мура; алгоритми генерації

Вступ

Сучасні телекомунікаційні системи не можуть функціонувати без використання процедур захисту інформації.

Такі процедури можуть полягати в обмеженні доступу до каналів передачі інформації передавальних та приймальних пристроїв, але найактуальнішою, зі зрозумілих причин, є проблематика захисту інформації, яка передається відкритими каналами [1;2]. Методи, які при цьому використовуються, досить різноманітні. Інформація може, наприклад, «маскуватись» (методи стеганографії) або, що частіше, шифруватись. Ключі шифрів, які використовуються при цьому, повинні задовольняти вимоги, серед яких найперша – це високий рівень захищеності інформації. Наразі цей рівень вимірюється часом, за який «ворожі» комп'ютери зламують шифр. Водночас час використання шифрів передбачає прийнятну простоту їх використання-шифрації та дешифрації інформації. Зауважимо також, що використання одного і тогож шифру протягом тривалого часу різко знижує його стійкість. Таким чином, виникає задача генерації стійких шифрів, які мають бути достатньо швидко створюваними.

Мета статті

Запропоновано загальну схему процедури формування найпоширенішого класу шифр-ключів-псевдовипадкових бінарних послідовностей. Проаналізовано тестування послідовностей з точки зору їх близькості до дійсно випадкових. Розглянутро формування псевдовипадкових послідовностей за допомогою цифрових автоматів Мілі та Мура. Метою роботи є запровадження

більш різноманітних процедур формування псевдовипадкових послідовностей, спрямованих на підвищення криптостійкості.

Виклад основного матеріалу

Псевдовипадкові бінарні послідовності та їх тестування

Числові послідовності, які за своїми статистичними характеристиками схожі на випадкові, називають псевдовипадковими. Їх застосування у вигляді псевдовипадкових бінарних послідовностей (ПВБП) досить поширене та різноманітне. Передусім, це використання ПВБП як ключів при шифруванні повідомлень при їх передаванні по відкритих каналах зв'язку. Це також моделювання впливів зовнішнього середовища на об'єкти різної природи при їх проектуванні або тестуванні. У першому випадку (при шифруванні) до ПВБП висуваються досить жорсткі вимоги щодо якості таких послідовностей, оскільки сучасний криптографічний захист інформації базується на застосуванні стандартних і відомих потенційному зловмиснику алгоритмів шифрування. Тому небезпека несанкціонованого розкриття змісту (криптостійкість) повідомлення повністю залежить від можливості знайти (обчислити або «вгадати») ключ. Саме якість ПВБП з точки зору її наближення за своїми статистичними характеристиками до дійсно випадкової визначає безпеку інформаційного обміну. У більшості випадків застосування ПВБП виникає додаткова вимога до засобів формування ПВБП, а саме, необхідність мати можливість повторити генерацію, тобто створювати таку саму послідовності багаторазово, принаймні двічі. Оскільки при інформаційному обміні ПВБП – це ключ шифрування, то при дешифруванні необхідно сформувати такий самий ключ. Ця вимога визначена, власне, основним призначенням генераторів ПВБП.

При сигнатурному діагностуванні цифрових пристроїв також принципово важливо формувати вихідні еталонні сигнатури та проводити діагностування з використанням однакових тестових послідовностей. Тому використання генераторів дійсно випадкових чисел (наприклад, таких, що базуються на квантуванні шумових сигналів) є принципово неприйнятним.

Виходячи з цих попередніх зауважень, зрозуміла увага, яку приділяють питанню якості ПВБП, сформованих за допомогою різних алгоритмів та процедур. На змістовному рівні, який, на жаль, не пропонує кількісного критерію, якість конкретної псевдовипадкової числової послідовності можна було б оцінювати мірою наближення її до дійсно випадкової, в якій будь-який фрагмент деякої фіксованої довжини з'являється з однаковою частотою, яка залежить лише від довжини фрагмента.

Мабуть, один із найбільш відомих та цікавих тестів на перевірку «випадковості» бінарної послідовності є так званий «тест на наступний біт». Ідея полягає в тому, що не повинно існувати поліноміального алгоритму, який би міг на основі перших k біт послідовності спрогнозувати $k+1$ біт з ймовірністю, більшою ½. Ендрю Яо ще у 1982 році довів, що генератор, який пройшов тест на наступний біт, пройде також будь-які інші статистичні тести на випадковість, що можуть бути виконані за поліноміальний час [1]. На жаль, цей тест не надає конструктивної процедури реалізації, яку можна було б практично здійснити.

Один із тестів, що може наблизити до отримання кількісної оцінки якості, використовує критерій складності алгоритму генерації. На думку авторів, складність будь-якого алгоритму чисельно (об'єктивно) оцінити проблематично, навіть, якщо обмежитись апаратною його реалізацією, наприклад, на регістрах зсуву. Зупинимось на цьому питанні дещо детальніше. Критерій був запропонований А.М. Колгоморовим [3; 4], відповідно до нього якість послідовності, суттєво спрощуючи питання, може визначається довжиною опису алгоритму (процедури) формування послідовності. Такий підхід значною мірою є гіпотетичним, оскільки існують приклади алгоритмів, коли при короткому описі генерується послідовність відносно великої довжини із прийнятними статистичними характеристиками. Але переконливого спростування постулату А.М. Колмогорова не існує. В той же час на користь цього постулату можна гіпотетично припустити, що для справжньої (істинно випадкової) послідовності не існує більш короткого опису процедури її формування, ніж сама послідовність, тобто її безпосередній запис (!). Дійсно, істинно випадкова послідовністьце будь-яка послідовність чисел, тобто жодної закономірності при її побудові за визначенням немає та не може бути. Тому задати її можна лише самою послідовністю.

На наш погляд, при оцінюванні якості ПВБП слід обов'язково розрізняти дві задачі: 1) визначити якість однієї конкретної послідовності; 2) оцінити якість сукупності послідовностей, які формуються деяким умовним (чи навіть конкретним і реальним) генератором. У першому випадку принциповим є наявність (існування) закономірності у формуванні кожного наступного числа залежно від попередніх чисел послідовності. Якщо ця закономірність легко може бути знайдена криптоаналітиком, то, вочевидь, якість послідовності низька. Наприклад, якщо це ряд арифметичної або геометричної прогресії, то про випадковість не може бути й мови.

У другому випадку закономірність за визначенням обов'язково повинна існувати, оскільки будь-яка процедура формування ПВБП є детермінованою. Якщо це не так, то зникає можливість сформувати ще раз таку саму послідовність, а це є необхідним у більшості практичних застосувань. Тому потрібно оцінювати умовну якість не однієї послідовності, а їх сукупності, яка сформована конкретним генератором. Теоретично тут все зрозуміло: в ідеальному випадку всі послідовності сукупності повинні з'являтися у статистичному експерименті з однаковою ймовірністю (частотою), а відхилення від рівномірного розподілу і може бути мірою «неідеальності» генератора. Але практично такий статистичний експеримент здійснити нереально вже при довжині послідовності $N \geq 40 \ldots 50$.

На практиці є виправданим використання ентропійного підходу. Наприклад, розглядаючи частоти, з якими у послідовності зустрічаються агрегати (блоки) довжини *k,* порівнюються їх розподіли (із характерним для достатньо довгої випадкової послідовності) із рівномірним розподілом імовірностей $p = {}^{1}/_{k}, 1 \leq k \leq 2^k$. При цьому обчислюється інформаційна дивергенція або відстань Кульбака-Лейблера [5]:

$$D_{KL}^{(k)} = \sum_{k=1}^{2^k} p_k \, log_2 \frac{p_k}{q_k} = -\frac{1}{2^k} \sum_{k=1}^{2^k} (k + log_2 q_k).$$

Відомо, що $-D_{KL}^{(k)} \geq 0$ для будь-яких розподілів $\{q_k\}_{k=1}^{2^k}$, $-D_{KL}^{(k)} = 0$ тільки у випадку. Таким чином, перевищення значенням $D_{KL}^{(k)}$ встановленого порогу D_0вказує [5; 6] на низьку якість послідовності, що тестується. Більш загальним є метод, який використовує ентропію Реньї (Renyienthropy) [7].

Серед тестів для перевірки якості ПВБП, які найчастіше на сьогодні застосовуються [8–10], мабуть найпростішим для реалізації є тест «на компресію». Ідея полягає в тому, що істинно випадкова послідовність, якщо вона достатньо довга, теоретично не повинна стискатися на відміну від реальної ПВБП. Тому коефіцієнт стиснення при застосуванні стандартних алгоритмів архівації може слугувати показником якості ПВБП – чим більший коефіцієнт стиснення, тим нижча якість послідовності.

Цифрові автомати як генератори ПВБП

Повертаючись до оцінки якості ПВБП на основі складності опису процедури її формування, з точки зору практичної реалізації зазначимо, що у традиційному випадку – це історично одні з перших реалізацій генераторів псевдовипадкових бінарних чисел на основі регістрів зсуву із зворотними зв'язками по модулю 2 або LFSR (Linear feedback shift register) [5]. Популярність та поширеністьтаких генераторів пов'язана із обмеженнями функціональних можливостей елементної бази того часу. Зокрема, важливим фактором були (і залишаються) масо-габаритні обмеження при апаратній реалізації та необхідність вбудовування генераторів у портативну апаратуру зв'язку та пристрої спеціального призначення. На сьогодні ситуація докорінно змінилася насамперед з точки зору можливостей сучасної мікроелектроніки. Очевидно, що, застосовуючи для побудови генераторів ПВБЧ компоненти із практично необмеженими функціональними можливостями (в межах детермінованих перетворень), можна сподіватися на створення більш досконалих генераторів.

Повний опис генератора на основі LFSR вичерпується описом конкретного виду зворотних зв'язків в регістрі та *n*-розрядним стартовим словом, з якого починається генерація. Загалом, цей опис має об'єм $2n$ біт, де *n*довжина регістра. Зважаючи, що реальні значення n лежать в межах 32…64 біт, опис конкретного генератора є доволі коротким. Формально це може свідчити про невисоку умовну «якість» відповідного генератора (якщо вважати, що якість еквівалентна складності алгоритму генерації та його опису). Тому, мабуть, алгебраїчні атаки при крипто аналізі процедур формування ПВБП цього класу є досить ефективними [11].

А тепер спробуємо визначити, які у самому загальному випадку можливі процедури формування ПВБП (діапазон таких процедур) окрім LFSR. Зафіксуємо насамперед діапазон чисел, з яких буде складатися послідовність. Нехай це будуть числа натурального ряду 0, 1, 2,…, *N-1*. Процедуру формування ПВБП будемо шукати за допомогою таблиці, що задає перехід від поточного числа $N(t)$ в послідовності до наступного $N(t+1)$. Звичайно, було б добре цей перехід задати більш компактно, наприклад, деякою функцією, але це кінцева мета нашого пошуку, а поки приймемо табличне представлення, яке можна, мабуть, вважати, за універсальне. Окрім того, числа $N(t)$ запишемо у порядку їх зростання, а саму процедуру формування послідовності зобразимо у вигляді табл. 1

Таблиця 1

0	1	…	X_i	…	N -1
X_1	X_2	…	X_j	…	X_N

Тут X_j– число, яке «з'явиться» в послідовності після числа X_i.

Розглянемо тепер, які можуть бути різновиди (варіанти) таких таблиць.

Варіант А. Нижній рядок містить усі числа від 0 до *N-1*. Тоді кількість можливих різних варіантів таблиць (і послідовностей) буде *N!*. Але їх довжина до повторення числа в послідовності може виявитися різною. Очевидно, для отримання послідовності максимальної довжини без повторів необхідно, щоб граф переходів від числа до числа був однозв'язаним, тобто не містив циклів. (Відсутність повторів не є обов'язковою вимогою до ПВБП). Таку послідовність чисел формує, наприклад, звичайний лічильник

N(t): 1,2,3…,N;

N(t+1): 2,3,4,…1.

Але навряд чи хтось наважиться назвати таку послідовність навіть схожою на випадкову.

Інший приклад, про який ми вже згадували, це ПВБП, що формується регістрами зсуву із зворотними зв'язками по модулю 2. У цьому випадку наступне число послідовності утворюється з поточного шляхом зсуву всіх розрядів на один біт праворуч, а на місце молодшого розряду записується сума по модулю 2 деякої фіксованої сукупності значень розрядів поточного числа. Якщо таку сукупність вибрано відповідно до коефіцієнтів примітивного поліному степеня *n-1*, який є дільником бінома $X^{n-1}+1$, то формована послідовність має максимальну довжину, яка дорівнює 2^n*-1*, де *n* – довжина регістра. На рис.1 забрежено стандартну структуру LFSR, де коефіцієнти $b_0, b_1, b_2, \dots, b_{n-1}; b_i = \{0,1\}$задають конкретний поліном, який використовується для генерації ПВБП [11].

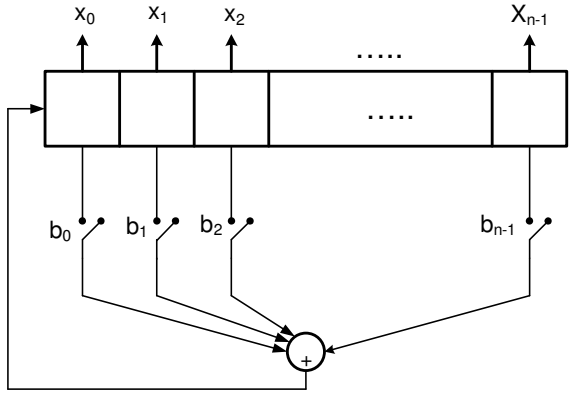

Рисунок 1 – Стандартна схема LFSR-генерації псевдовипадкових послідовностей

Варіант В. В загальному випадку ПВЧП зовсім не обов'язково не повинна містити повторів, тобто ситуацій, коли в процесі генерації виникає «зациклювання» до вичерпання всіх можливих чисел діапазону – деякі вершини графу переходів виявляються недосяжними, а сформована послідовність укороченою. Добре це, чи погано? Відповідь на це питання неоднозначна. Все залежить від зовнішніх вимог до довжини послідовності. Якщо сформована послідовність використовується як ключ шифрування, то у цьому випадку її довжина може бути порівняно невеликою. Наприклад, для більшості поширених на практиці блокових шифрів $N \leq 512$бітів. Але для потокових шифрів класу скремблерів довжина послідовності має бути не меншою, ніж довжина відкритого тексту, що подається на вхід шифратора.

Для узагальнення процедури формування ПВБП з урахуванням того, що йдеться саме про бінарні числа, представимо таблицю переходів у розгорнутому (побітовому) вигляді (табл. 2).

Таблиця 2

$N(t)$	$N(t+1)$
0 0 … 0	$\alpha_{11}\alpha_{12}\dots\alpha_{1n}$
0 0 … 1	$\alpha_{21}\alpha_{22}\dots\alpha_{2n}$
……..	……
1 1 … 1	$\alpha_{2^n1}\alpha_{2^n2}\dots\alpha_{2^nn}$

У цій таблиці символам α_{ij}відповідають значенням 0 або 1 двійкових чисел, які є наступними у ПВБП. Тому така таблиця не що інше, як об'єднання *n* таблиць істинності для *n*булевих функцій, які задають правила утворення для кожного біта наступного двійкового числа. Таких таблиць для кожної з функцій може бути теоретично доволі багато. Вже для однієї з функцій (одного стовбчика таблиці) це число сягає 2^{2^n}, що при зовсім помірному значенні, наприклад, *n=8* дає фантастичне різноманіття варіантів різних таблиць $2^{256} \approx 10^{85}$.

Проте мабуть не всі з цих функцій формують ПВБП із задовільними статистичними характеристиками за означеними вище критеріями. Так, зразу ж потрібно відкинути константи 0 та 1. Із інтуїтивних міркувань можна також сподіватися, що «кращими» функціями будуть такі, які приблизно на половині двійкових вхідних наборів приймають значення 1, а на інших 0.Все це звужує діапазон можливих (перспективних) варіантів. Однак, якщо обмежитись, наприклад, лише лінійними булевими функціями, то різноманіття можливих варіантів лишається достатнім, щоб забезпечити практичну неможливість простим перебором визначити правила (закономірності) утворення послідовності.

Однією з важливих характеристик послідовності, що формується, є її довжина. У більшості випадків бажано отримати послідовність максимальної довжини, яка, очевидно, не може перевищувати 2^n двійкових чисел за умови відсутності їх повторів у послідовності. Звичайно, цю умову не слід сприймати як обов'язкову, оскільки випадкова (і, навіть, псевдовипадкова) послідовність може бути будь-якою вже за визначенням.

Для отримання послідовності максимальної довжини без повторів чисел, очевидно, таблиці істинності булевих для функцій мають містити у правій частині таблиці (значень булевих функцій) усі можливі двійкові числа відповідної розрядності. Але ця необхідна умова не є достатньою для формування послідовності максимальної довжини. Для пояснення наведемо два приклади (табл. 3, 4).

Таблиця 3

$N(t)$ $q_1q_2q_3$	$N(t+1)$ $f_1f_2f_3$
0 0 0	0 1 0
0 0 1	1 1 1
0 1 0	1 0 0
0 1 1	0 0 1
1 0 0	1 1 0
1 0 1	0 1 1
1 1 0	1 0 1
1 1 1	0 0 0

При використанні табл. 2 буде сформована 24-бітова послідовність без повторення 3-бітових фрагментів у послідовності. Еквівалентною числовою послідовністю десяткових чисел буде: 2,7,4,1,6,3,5,0. Відповідні булеві функції при реалізації генератора автоматом Мура мають вигляд

$$f_1 = \overline{q_1}(q_2\overline{q_3} \vee \overline{q_2}q_3) \vee q_1\overline{q_3};$$
$$f_2 = \overline{q_2};\ f_3 = \overline{q_1}q_3 \vee q_1(q_2\overline{q_3} \vee \overline{q_2}q_3).$$

А це інший автомат (табл. 4) та інші функції переходів, які він реалізує.

Таблиця 4

$N(t)$ $q_1q_2q_3$	$N(t+1)$ $f_1f_2f_3$
0 0 0	1 0 1
0 0 1	0 1 0
0 1 0	0 0 0
0 1 1	0 1 1
1 0 0	1 1 0
1 0 1	1 0 0
1 1 0	0 0 1
1 1 1	1 0 1

Автомат, побудований відповідно до табл. 4, буде формувати послідовність лише з шести чисел: 5,4,6,1,2,0. Хоча в правій частині наявні всі числа діапазона, але числа 3 та 7 у цій послідовності відсутні, оскільки граф переходів автомата не містить цих вершин. Таким чином, можна стверджувати, що необхідною та вже достатньою умовою для генерації послідовності максимальної довжини є 1-зв'язаність графа переходів автомата, який реалізує процедуру генерації, та наявність у графі всіх верши діапазону *N(t)*. На рис. 2 наведено просту схему, що реалізує формування числових послідовностей відповідно до наведених вище прикладів. Ця схема – автомат Мура, тобто схема «без входів» (на ній не показані лише сигнали синхронізації та установки стартового стану генерації).

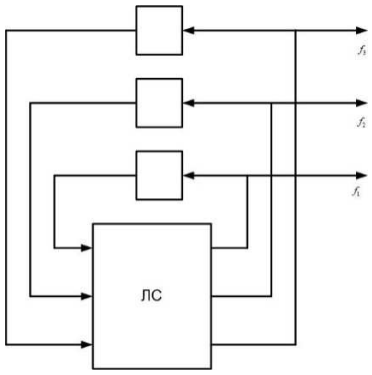

Рисунок 2 – Проста схема, що реалізує формування числових послідовностей

Зазначимо також, що у разі виконання обох умов (наявність усіх без винятку чисел у правій частині таблиці та 1-зв'язаність графу переходів) автоматично забезпечуються добрі статистичні параметри генерованої послідовності. Зокрема мова йде про частоти (ймовірності) появи в послідовності 0 та 1та фрагментів довжини 1,2,3,…*n*.

Як узагальнену модель генератора ПВБП можна застосувати модель скінченних цифрових автоматів Мілі (рис. 3).

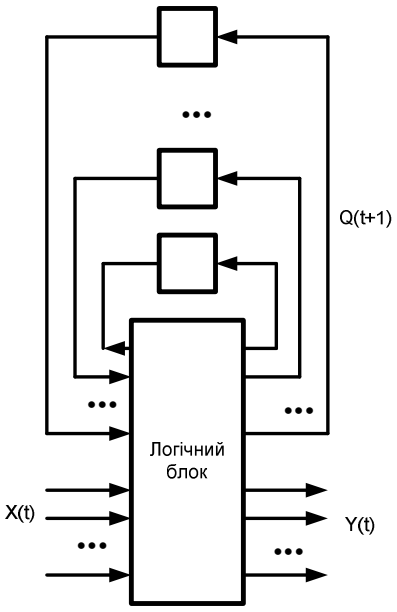

Рисунок 3 – Узагальнена схема генератора на основі модель автомата Мілі

Слід зазначити, що навіть модель автомата Мура є достатньо універсальною та охоплює як окремий випадок і генератори на регістрах зсуву із зворотними зв'язками по модулю 2. Відповідні автоматні рівняння переходів такої схеми мають вигляд:

$$q_1(t+1) = \oplus \sum_{\lambda \in M} q_\lambda(t),$$
$$q_2(t+1) = q_1(t),$$
$$q_3(t+1) = q_2(t),$$
$$\ldots\ldots\ldots\ldots$$
$$q_n(t+1) = q_{n-1}(t),$$

де $\oplus \sum_{\lambda \in M} q_\lambda(t)$ – сума по модулю 2 бітів відповідно до вибраного поліному, $q_1(t), q_2(t),\ldots; q_n(t)$ – значення символів, які відповідають внутрішньому стану регистру в поточний момент часу t, а $q_1(t+1), q_2(t+1), \ldots, q_n(t+1)$ – те ж саме в наступний момент.

У випадку використання моделі Мура порядок чисел у послідовності однозначно задається рівняннями переходів і є незмінним. Зовнішнім впливом можна змінити лише «стартове» число, тобто двійкову комбінацію, з якої починається послідовність. Очевидно, для утворення інших послідовностей необхідно створити умови для зовнішнього керування, тобто на генератор подавати ще й вхідні сигнали (впливи) та перейти до загальної моделі Мілі. У цьому випадку для визначення поведінки автомата необхідно додатково задати ще й його функції виходів

$$y_j(t) = f_j[x_1(t), x_2(t), \ldots x_l(t); q_1(t), q_2(t), \ldots q_m(t)]$$

$j=1,2,\ldots,l,$ де f_l– вихідні булеві функції автомата (генератора).

Залежно від різноманіття таких впливів можна створити більшу чи меншу кількість послідовностей. Очевидно, максимальна кількість цих траєкторій визначається кількістю входів автомата l і дорівнює 2^l, а для формування відповідних вхідних керуючих сигналів необхідно передбачити деякі додаткові апаратні або програмні засоби. Функцією цих засобів є змінення траєкторії переходів від одного внутрішнього стану генератора до наступного за певною програмою або часовим регламентом, що є додатковим інструментом керування розподілом, наприклад, ключів в захищеній телекомунікаційній мережі.

Висновки

Отже, розглядаючи автоматні моделі як узагальнюючі та універсальні, можна зробити такі висновки.

1. Різноманіття псевдовипадкових послідовностей, що можуть бути сформовані на базі автоматних моделей, суттєво більше, ніж на регістрах зсуву із зворотними зв'язками по модулю.

2. Якщо для регістрів комбінаторна кількість варіантів не перевищує 2^n (це максимальне число різних поліномів, які утворюють коло зворотного зв'язку, зокрема і таких, що не відповідають вимогам генерації послідовності максимальної довжини), то для генератора на основі моделі Мура ця кількість наближається до $n2^n$. Зрозуміло, що така оцінка є занадто завищеною, оскільки значна кількість з цих варіантів процедур формування бінарної послідовності не буде відповідати вимогам з боку статистики появи тих чи інших чисел у послідовності. Однак, можна сподіватись, що після попереднього відбору різноманіття варіантів у порівнянні з регістровими реалізаціями залишиться на порядки більшим.

3. Криптоаналіз ПВБП, отриманих на основі автоматних моделей, суттєво ускладнюється, оскільки клас булевих функцій, що використовуються при генерації, практично нічим не обмежений, а прямий перебір варіантів не може бути здійснений за часовими обмеженнями.

4. При використанні моделі Мілі з'являється зручний спосіб зміни, фактично, алгоритму формування послідовності, наприклад, для кожного сеансу інформаційного обміну, що сприяє підвищенню рівня захисту від несанкціонованого доступу.

5. Апаратна реалізація пропонованого підходу на сьогодні не є проблемою, наприклад, на основі замовних ВІС. Це створює передумови для компактної реалізації генераторів ПВБП та застосування їх в системах захищеного мобільного зв'язку.

6. Натепер потреба в застосуванні засобів захисту інформаційних ресурсів від несанкціонованого доступу стає стандартною вимогою не лише для систем оборонного або спеціального призначення, але й для комерційних, громадських [12] та банківських комп'ютерних систем відповідно до вимог законодавства. Тому проблема вдосконалення засобів захисту залишається актуальною.

Список літератури

1. *Danny Dolev Andrew.On the security of public key protocols / Danny Dolev Andrew, Chi-Chih Chao // IEEE Trans. Information Theory – 1983. – № 29(2). – P. 198 – 207.*
2. *Колмогоров А.Н. Три подхода к определению понятия «количество информации» [Текст] / А.Н. Колмогоров // Проблемы передачи информации. – 1964. – №1 (1). – С. 3 – 11.*
3. *Вьюгин В.В. Колгоморовская сложность и алгоритмическая случайность [Текст]. – М. 2012. – 131 с.*

4. Kullback S. Letter to editor: The Kullback-Leibler distance / Kullback S., Leibler R.A. // The American Statistician, – 1987. – v.41 (4). – P. 340 – 341.

5. Ali E.Abbas (2017). A Kullback-Leibler View of Maximum Entropy and Maximum-Log Probability Methods / Ali E. Abbas, Andrea H. Cadenbach, Elsan Salini. Retrieved from http//creativecommons/licenses/by/4.0/.

6. Renyi Alfred. On measures of information and enthropy // Proceedins of Fourth Berkeley Symposium on Mathematics, Statistics and Probability. – 1961. – P. 547 – 561.

7. Потий А. Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS / А.Потий, С.Орлова // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – 2001. – Вип. 2, – С. 206 – 214.

8. Andrew Rukhin, NIST Statistical Test Suite, Retrieved from http//csrc/nist.gov/groups/ ST/toolkit/rng/documentation_software. html.

9. Soto Juan. Statistical Testing of Random Number Generators// Proceedings of the XXII and National Information Systems Security Conference. – 1999. – P. 101 – 112.

10. Пометун С.О. Алгебраїчні атаки на потокові шифратори як узагальнення кореляційних атак // Системні дослідження та інформаційні технології. – 2008. – №2. – С. 29 – 40.

11. Малогулко Р.В. Вдосконалення генераторів ПВП та їх застосування в системах скремблер-дескремблер телекомунікаційних пристроїв / Р.В. Малогулко., Ю.Г. Савченко // Наукові записки УНДІЗ. – 2008. – № 6(8). – С. 43 – 49.

12. Хлапонін Ю.І. Побудовакомплексних системзахисту для громадських інформаційних систем управління / Ю.І. Хлапонін, Є.Є. Шабала, О.В. Бойко, Б.О. Бондаренко // Управління розвитком складних систем. – 2018. – №34. – С. 104 – 108.

Стаття надійшла до редколегії 11.03.2019

Балина Елена Ивановна
Кандидат технических наук, доцент кафедры информационных технологий проектирования и прикладной математики, *orcid.org/0000-0001-6925-0794*
Киевский национальный университет строительства и архитектуры, Киев
Буценко Юрий Павлович
Кандидат физико-математических наук, доцент кафедры математического анализа, *orcid.org/0000-0003-4806-9587*
Национальный технический университет Украины «Киевский политехнический институт имени Игоря Сикорского», Киев
Савченко Юлий Григорьевич
Доктор технических наук, профессор кафедры звукотехники, *orcid.org/0000-0002-7123-9165*
Национальный технический университет Украины «Киевский политехнический институт имени Игоря Сикорского», Киев

АЛГОРИТМЫ ФОРМИРОВАНИЯ ПСЕВЛОСЛУЧАЙНЫХ БИНАРНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Аннотация. *Рассмотрена задача построения обобщающего описания процедуры формирования псевдослучайных числовых последовательностей, которые используются в качестве ключей при шифровании информационного обмена в телекоммуникационных системах с ограниченным доступом, а также моделировании внешних влияний при диагностировании технического состояния цифровых устройств. Показано, что эта задача непосредственно связана с задачей количественной оценки качества псевдослучайной последовательности с точки зрения ее близости к истинной случайности. В отличие от традиционного подхода, базирующегося на использовании для генерации последовательностей этого класса линейных регистровых фильтров, предложено использование универсальных моделей цифровых автоматов (модели Мили и Мура). Такой подход существенно увеличивает комбинаторное разнообразие возможных алгоритмов генерации, что усложняет криптоанализ. Как результат, повышается защищенность соответствующих информационных систем с ограниченным доступом. В то же время практическая реализация соответствующих процедур формирования псевдослучайных бинарных последовательностей может быть реализована практически без осложнений как программного, так и аппаратного характера.*

Ключевые слова: защита информации; процедуры шифрования; псевдослучайные последовательности; цифровые автоматы; модели Мили и Мура; процедуры генерации

Balina Elena
Ph.D., Associate Professor, Department of Information Technology of Design and Applied Mathematics, *orcid.org/0000-0001-6925-0794*
Kyiv National University of Consruction and Architecture, Kyiv
Butsenko Yurij
Ph.D. (Physics-Mathematics), associate professor of mathematical analysis and probability theory, *orcid.org/0000-0003-4806-9587*
Igor Sikorsky Kyiv Polytechnic Institute, Kyiv
Savchenko Yulij
DSc (Eng.), Professor of audio engineering anddata recording, *orcid.org/0000-0002-7123-9165*
Igor Sikorsky Kyiv Polytechnic Institute

ALGORYTHMS OF GENERATION OF PSEUDORANDOM BINARY SEQUENCES

Abstract. *A pseudorandom binary sequence (PRBS) is a sequence of 1' and 0's, that, while generated with a deterministic algorithm, is difficult to predict and exhibits statistical behavior similar to truly random sequence. PRBS are used in telecommunication, especially to spread information content in Analog-to-Information Converters, but also in encryption, simulation technique and time-of-flight spectroscopy. Generation of PRBS can be realized by using of discrete shift register (DSR), flip-flops, FPGA-based implementation, virtual instrumentation etc. However, methods of pseudorandom binary sequences generation based on finite automaton concept are presented in this paper. A direct connection with the issues of numerical evaluation of the quality of pseudorandom binary sequence in terms of its proximity to a random sequence is shown. The using for the generation of PRBS universal models of numerical automaton (models of Mealy and Moore machines) are proposed. Such an approach significantly increases the combinatorial variety of generation algorithms. Thus, crypto-analyses is significantly complicated, and, as a result, security of information systems with limited access is increased. It is significant that in this case, the practical implementation of procedures for theformation of pseudorandom binary sequence can be implemented both in hardware and software without complications.*

Keywords: seudorandom binary sequence; encryption; PRBS quality; numerical automaton; Mealy and Moore machines; information systems with limited access.

References

1. Dolev, Danny, Yao, Chi-Chih. (1983). On the security of public key protocols. IEEE Trans.Information Theory, 29 (2), 198 – 207.

2. Hlaponin, Yu.I., Shabala, E.E., Boyko, O.V., Bondarenko, B.O. (2018). Construction of complex defensive systems for public information systems of management. Management of development of complex systems. Kyiv, Ukraine: 34, 104 – 108.

3. Kolmogorov, A.N. (1964). Three approaches to notion of "quantity of information". Problems of Information Transfer, 1(1), 3 – 11.

4. Vjugin, V.V. (2012). Kolmogorov's complexity and algorithmic randomness. MFTI, Moskow; 131.

5. Kullback, S., Leibler, R.A. (1987). Letter to editor: The Kullback-Leibler distance. The American Statistician, 41 (1), 340 – 341.

6. Abbas, Ali E., Cadenbach, Andrea H., Salini, Elsan. (2017). A Kullback-Leibler View of Maximum Enthropy and Maximum-Log Probability. Retrieved from http//creativecommons/licenses/by/4.0/.

7. Renyi, Alfred. (1961). On measures of information and enthropy. Proceedings of Fourth Berkeley Symposium on Mathematics, Statistics and Probability, 547 – 561.

8. Potij, A., Orlova, S. (2001). Statistical testing of generators of random and pseudorandom numbers using NIST STS statistical tests suite. Law, normative and technologic support of information defence systems at Ukraine: 2, 206 – 214.

9. Rukhin, Andrew L. NIST statistical test suite. Retrived from http// csrc. nist.gov/groups/ST/toolkit/png/documentation software html.

10. Soto, Juan. (1999). Statistical testing of random number generators.Proceedings of XXII and National Information Systems Security Conference, USA, NIST.

11. Pometun, S.O. (2008). Algebraic attacks on stream ciphers as generalization of correlation attacks. System research and information technologies, 2, 29 – 40.

12. Malogulko, R.V., Savchenko, Yu.G. (2008). Improvement of generators of pseudorandom sequences and their applications at systems scrambler-descrambler of telecommunication devices.Scientific papers of Ukrainian scientific-researching Institute of Telecommunicatios, 8, 104 – 108.

Посилання на публікацію

APA *Balina, Elena, Butsenko, Yurij & Savchenko, Yulij. (2019). Algorythms of generation of pseudorandom binary sequences. Management of Development of Complex Systems, 38, 56 – 63, dx.doi.org\10.6084/m9.figshare.9788447.*

ДСТУ *Баліна О.І. Алгоритми формування псевдовипадкових бінарних послідовностей [Текст] / О.І. Баліна, Ю.П. Буценко, Ю.Г. Савченко // Управління розвитком складних систем. – 2019. – № 38. – С. 56 – 63, dx.doi.org\10.6084/m9.figshare.9788447.*