Якщо число зайнятих місць в матриці менше $m+n-1$, має місце випадок вродженості. При числі зайнятих місць в матриці менше ніж $m + n-1$, неможливо знайти всі значення потенціалів, і отже, неможливо дослідити незайняті місця матриці, тобто задачу розв'язати неможливо. Для усунення вродженості опорного плану в деякі незай-няті клітинки ставимо нульові поставки і ці їх вважають зайнятими місцями.

Література

1. Гриньова В. М. Організація виробництва : підручник / В. М. Гриньова, М. М. Салун. – Київ : Знання, 2009. – 580 с.

2. Івченко І. Ю. Математичне програмування / І. Ю. Івченко. – Київ : ЦУЛ, 2007. – 230 с.

3. Лугінін О. Є. Економіко-математичне моделювання / О. Є. Лугінін, В. М. Фомішина. – Київ : Знання, 2011. – 342 с.

4. Тригер Г. М. Оптимізація використання будівельних машин і транспорту у будівництві: методичні рекомендації для студентів спеціальності 7.092101 «Промислове і цивільне будівництво» / Г. М. Тригер, С. А. Ушацький. – Київ : КНУБА 2010. – 23 с.

5. Тригер Г. М. Розробка й оптимізація календарних планів зведення комплексу будівель і споруд : навч. посіб. / Г. М. Тригер. – Київ : ІСДО, 2013. – 72 с.

6. Цегелик Г. Г. Лінійне програмування / Г. Г. Цегелик. – Лівів : Світ, 2015. – 216 с.

7. Організація будівництва: підручник / Ю. П. Шейко, Г. М. Тригер и др. ; за ред. С. А. Ушацького. – Київ : Кондор, 2005. – 519 с.

ВИКОРИСТАННЯ ЦИФРОВИХ АВТОМАТІВ У ПРОЦЕСАХ ГЕНЕРАЦІЇ ПСЕВДОВИПАДКОВИХ БІНАРНИХ ПОСЛІДОВНОСТЕЙ

Баліна О. І.[1]*, Безклубенко І. С.*[2]*, Буценко Ю. П.*[3]
Гетун Г. В.[4] *, Лесько В. І.*[5]
[1,2,4,5]*Київський національний університет будівництва і архітектури*
03680, Київ, Повітрофлотський пр.-т, 31
[3]*м. Київ, НТУ України «Київський політехніхчний інститут» ім. І.Сікорського*
E-mail: [1]*elena.i.balina@gmail.com,* [2]*i.bezklubenko@gmail.com*
[3]*armchairdoc@ukr.net,* [4]*galinagetun@ukr.net,* [5]*Vitaless1@i.ua*

Сучасні телекомунікаційні системи не можуть функціонувати без використання процедур захисту інформації. Такі процедури можуть полягати в обмеженні доступу до каналів передачі інформації,

передаючих 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 ряду вимог, серед яких найпершою є високий рівень захищеності інформації. Зауважимо також, що використання одного і того ж шифру протягом тривалого часу різко знижує його стійкість. Таким чином, виникає задача генерації стійких шифрів, які мусять бути достатньо швидко створюваними.

Числові послідовності, які за своїми статистичними характеристиками схожі на випадкові, називають псевдовипадковими. Їх застосування у вигляді псевдовипадкових бінарних послідовностей (ПВБП) досить поширене та різноманітне, воно включає у себе формування найпоширенішого класу шифр-ключів. 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 послідовність багаторазово, принаймні двічі.

Один з 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 якого якість послідовності, суттєво спрощуючи питання, може визначатися 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 з прийнятними статистичними характеристиками

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).

Для узагальнення процедури формування ПВБП з урахуванням того, що мова йде саме про бінарні числа, представимо таблицю переходів у розгорнутому (побітовому) вигляді таблиці (табл. 1).

Таблиця 1

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

У цій таблиці символи 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 стовпчика таблиці) це число сягає 2^{2^n}, що при зовсім помірному значенні, наприклад, n = 8 дає фантастичне різноманіття варіантів різних таблиць $2^{256} \approx 10^{85}$. Але ж, 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. За 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 .

На рис. 1 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).

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

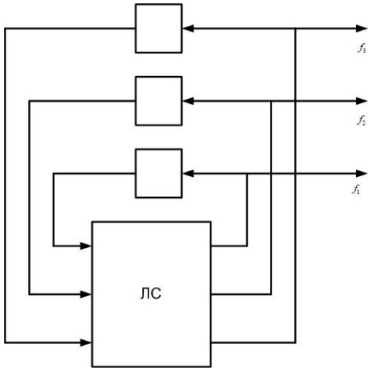

Рис. 1. Проста схема, що реалізує формування числових послідовностей

Як узагальнену модель генератора ПВБП можна застосувати модель скінченних цифрових автоматів Мілі (рис. 2).

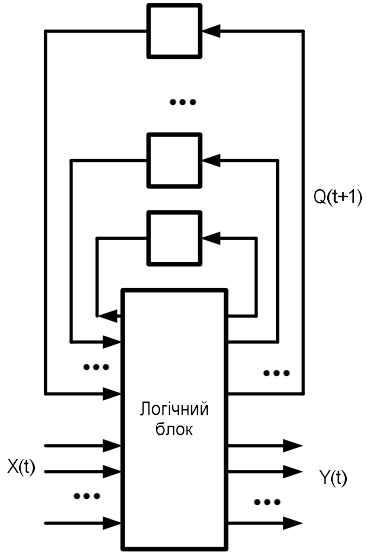

Рис. 2. Узагальнена схема генератора на основі моделі автомата Мілі

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_1 – 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. Таким чином, 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 більшою.

2. 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.

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

4. 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.

5. Сьогодні 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.

Література

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» / А. Н. Колмогоров // Проблемы передачи информации. – 1964, № 1 (1). – С. 3–11.

3. Вьюгин В. В. Колгоморовская сложность и алгоритмическая случайность. – М, 2012. –131 с.

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