УДК 681.324.067

Т.О. Гріненко[1], О.П. Нарєжній[2]

[1] *Харківський національний університет радіоелектроніки, Харків*
[2] *Харківський національний університет імені В.Н. Каразіна, Харків*

КВАНТОВІ ГЕНЕРАТОРИ ВИПАДКОВИХ ЧИСЕЛ В КРИПТОГРАФІЇ

Наводиться аналіз існуючих методів генерації випадкових чисел. Відзначаються переваги і недоліки існуючих методів. Пропонується використовувати для генерації випадкових чисел генератори, які базуються на квантових процесах, що дозволить збільшити стійкість криптографічних систем. Розглядається питання тестування генераторів випадкових чисел.

Ключові слова: *генератор випадкових чисел, детермінований генератор випадкових чисел, квантовий генератор випадкових чисел, тестування, криптографічний протокол.*

Вступ

У зв'язку з розвитком інформаційно-телекомунікаційних систем все більш актуальною стає задача побудови надійних систем обробки інформації з функціями криптографічного захисту інформації.

Одним з основних елементів таких систем, від характеристик якого залежать характеристики системи в цілому, є засіб генерації ключів. Генерація дійсно випадкових чисел відіграє дуже важливу роль в самих різних додатках – в криптографії (класичній, квантовій), в області чисельного моделювання, в ігровій індустрії та інших областях. У зв'язку з розширенням області застосування комп'ютерних технологій і швидким розвитком електронних мереж зв'язку, число таких додатків постійно зростає [1, 2].

Аналіз сучасних методів генерування випадкових чисел

Задача генерації випадкових і псевдовипадкових послідовностей, які використовуються в криптографії в якості ключів, загальносистемних параметрів та ін. вирішується за допомогою застосування високошвидкісних генераторів випадкових чисел (ГВЧ) і генераторів псевдовипадкових чисел (ГПСЧ).

При цьому сучасна класифікація даних генераторів відображає як методи їх побудови, так і обрану термінологію.

Генератор випадкових чисел являє собою пристрій, який створює послідовності чисел, які породжені процесом, результат якого непередбачуваний і який не може бути згодом відтворений надійно [1]. Існують два основних види генераторів:

програмні (програмне забезпечення);

апаратні (фізичні генератори).

Із загальної точки зору програмного забезпечення генератори виробляють так звані псевдовипадкові числа, неможливо за допомогою програми отримати послідовність істинно випадкових чисел.

Отримана послідовність може мати деякі властивості випадкових послідовностей і, таким чином, пройти кілька статистичних тестів випадковості, але її завжди можна відтворити. Ніякий детермінований алгоритм, не може генерувати повністю випадкові числа, він може тільки апроксимувати деякі їх властивості. Такі генератори називають генератором псевдовипадкових послідовностей (ГПВП) або детермінованим генератором випадкових послідовностей (ДГВП).

Будь-який ГПВП з обмеженими ресурсами рано чи пізно зациклюється – починає повторювати одну і ту ж послідовність чисел.

Більшість простих арифметичних генераторів хоча і володіють великою швидкістю, але страждають від багатьох серйозних недоліків:

занадто короткий період;

послідовні значення не є незалежними;

деякі біти «менш випадкові», ніж інші;

нерівномірний одномірний розподіл;

оборотність [1].

ГПВП складається з алгоритму, в якому вводиться деяке початкове значення – рядок бітів, який використовується в якості вхідних даних для детермінованого генератору випадкових бітів. Початкове значення визначає частину стану ГПВП і потім методом ітерацій генерується послідовність псевдовипадкових чисел. Хоча період послідовності може бути дуже довгим, але вона завжди буде періодичною. Однією з властивостей таких послідовностей є той факт, що, як тільки один з елементів послідовності відомий, всі інші елементи – і попередні, і наступні – можуть бути визначені. Очевидно, що цю властивість особливо важливо враховувати при використанні таких послідовностей в криптографії для генерації ключа.

До ДГВП та методів, за якими формуються псевдовипадкові послідовності (ПВП) висунуто

ряд вимог. Основними з них є: пряма та зворотна непередбачуваність чисел або структурна скритність, складність або швидкодія генерування, необоротність функції генерування ключа, під якою розуміється обчислювальна складність визначення ключа ДГВП, що застосовується, захищеність генератора від впливу на процес генерування ключа, а також забезпечення заданого періоду повторення ПВП. При цьому рівень гарантій в суттєвій мірі залежить від ентропії джерела ключів і на сьогодні вона повинна складати від 80 до 512 бітів [1].

Незважаючи на те, що ГПВП не виробляють істинно випадкові числа, ці генератори мають ряд переваг. По-перше, їх вартість практично дорівнює нулю, так як вони можуть бути реалізовані в програмному забезпеченні і численні бібліотеки знаходяться у вільному доступі. По-друге, їх головний недолік – а саме, що послідовності, які вони виробляють, відтворювані – може в деяких випадках представляти собою перевагу. Наприклад, при використанні випадкових чисел для наукових розрахунків іноді буває корисно мати можливість відтворити послідовність чисел при налагодженні програми моделювання.

У випадках, коли використання псевдовипадкових чисел не підходить, необхідно вдаватися до використання апаратного (фізичного) генератора випадкових послідовностей або недетермінованого генератора випадкових послідовностей (НГВП). Апаратний генератор випадкових послідовностей – пристрій, який генерує послідовності випадкових чисел, що формуються з використанням фізичних випадкових процесів, та які не можуть бути відновлені в просторі та часі. Процес може описуватися або класичною, або квантовою фізикою.

Класична фізика, розроблена фізиками до початку XX століття, описує макроскопічні системи. Квантова фізика описує мікроскопічні системи, такі як атоми, молекули, елементарні частинки і т.п.

На відміну від ГПВП, апаратні генератори мають недолік, який полягає в зміщенні b, що визначається як різниця ймовірностей появи 1 та 0:

$$b = p(1) - p(0) \qquad (1)$$

і можливими кореляційними залежностями на довгих інтервалах вихідних послідовностей.

Зсув виникає через труднощі у розробці точно збалансованих фізичних процесів. Однак існують алгоритми пост-обробки, які можуть бути використані для видалення зміщення в послідовності випадкових чисел.

Макроскопічні процеси, описувані класичною фізикою, можна використовувати для генерації випадкових чисел. Наприклад, фізичні генератори випадкових чисел на основі хаотичних процесів включають моніторинг електричних шумів струму в резисторі. Як генератор шуму використовують шумлячий тепловий пристрій, наприклад, транзистор. Існують фізичні генератори випадкових чисел, що використовують різні фізичні процеси, такі як радіоактивний розпад, шуми аналогових мереж, космічне випромінювання, фотоелектричний ефект.

На відміну від класичної фізики квантова фізика принципово ймовірна. Тому при виборі процесу, що лежить в основі генератора істинно випадкових чисел, вибір природним чином падає на квантові процеси як джерела випадковості. Формально квантові генератори випадкових чисел є єдино вірними генераторами випадкових чисел, однак володіють і іншими перевагами. Імовірнісна природа (внутрішня випадковість) квантової фізики дозволяє вибрати дуже простий процес як джерело випадковості. Це означає , що такий генератор легко моделювати і його функціонування можна контролювати для того, щоб підтвердити, що він працює правильно і насправді виробляє випадкові числа.

Донедавна єдиний існуючий квантовий генератор випадкових чисел був заснований на спостереженні радіоактивного розпаду деяких елементів. Хоча подібні генератори створюють послідовності високого ступеня випадковості, ці генератори є вельми громіздкими, а використання радіоактивних матеріалів може бути шкідливо для здоров'я. Сучасний розвиток науки і техніки дозволили вченим створити прості й недорогі квантові генератори випадкових чисел, що використовують квантовий оптичний процес як джерело випадковості.

Світло складається з елементарних "частинок", званих фотонами. У певній ситуації фотони демонструють випадкову поведінку. Одна з таких ситуацій, яка дуже добре підходить для генерації бінарних випадкових чисел, полягає в наступному. На напівпрозоре дзеркало направляються фотони, що генеруються джерелом одиночних фотонів. Фотон може відбитися, а може пройти через напівпрозоре дзеркало з імовірністю 50%. Вибір, який «робить» фотон, абсолютно випадковий. На виході системи стоять два лічильника фотонів, що реєструють минулі і відбиті фотони і формують вихідні електричні сигнали.

Крім оптичної частини - генератора випадкових чисел - система включає в себе підсистему, яка управляє синхронізацією, а також збором і обробкою даних, що надходять з детекторів, виконує статистичні та апаратні перевірки послідовності. Як зазначалося вище, фізичні процеси важко точно збалансувати. Таким чином, важко гарантувати, що ймовірність запису 0 і 1 в точності дорівнює 50%. Наприклад, в генераторі Quantis різниця між цими

двома ймовірностями менше 10%, що еквівалентно ймовірностям від 45% до 55%. Оскільки це зміщення не може бути прийнятним для деяких додатків, то обов'язково виконується алгоритм постобробки для видалення зміщення в послідовності випадкових чисел. Як вже говорилося вище, одним з головних переваг квантових генераторів випадкових чисел на оптичних фотонах є те, що вони засновані на простому і принципово випадковому процесі, який легко моделювати і контролювати. Подібні квантові генератори мають високу швидкість вихідного потоку – до 10-16 Мбіт / с, - при якій не спостерігається ніяких кореляцій і виконуються всі статистичні тести.

Ще одним прикладом є генератор випадкових чисел з використанням напівпровідникового лазера з короткими і різкими піками інтенсивності. Лазер пропускається через середовище зі зворотним зв'язком із затримкою, тобто інтенсивність випромінювання на виході визначається інтенсивністю сигналу на вході і станом середовища, яке залежить від інтенсивності на вході.

Відомо, що зміна інтенсивності – процес квазіперіодичний, тобто з плином часу майже повторюється, тому безпосередньо використовувати його в якості генератора випадкових чисел не можна. Для того щоб позбутися від квазіперіодичності, інтенсивність випромінювання вимірюється приблизно 2.5 мільярда раз в секунду. Результат кожного вимірювання записується в рядок довжиною в 8 біт. Він віднімається із значення попереднього вимірювання, а результат буде скорочуватися.

Таким чином, вдається позбутися від квазіперіодичності і добитися генерації випадкового потоку нулів і одиниць зі швидкістю приблизно 12,5 Гігабіт в секунду.

Можна зробити висновок, що при генерації випадкових чисел доцільно використовувати саме квантові генератори випадкових послідовностей, які генерують послідовності випадкових чисел, що формуються з використанням квантових (мікроскопічних) фізичних випадкових процесів, та які не можуть бути відновлені в просторі та часі. Головною перевагою квантового генератора випадкових послідовностей є швидкість генерації вихідного потоку даних, яка значно перевищує швидкість ГПВП та ГВП.

Квантовий генератор випадкових чисел

Деякі частинки в природі знаходяться в найдрібніших кількостях, відомих як кванти. Крім того, існує найменша кількість інформації, яка називається кубіт. Кубіт - квантовий розряд або найменший елемент для зберігання інформації в квантовому комп'ютері. Один квант світла (фотон) може бути використаний в якості носія одного кубіта, але є багато інших прикладів, і вони не обмежуються тільки елементарними частинками. Кубіт може розглядатися як лінійна комбінація двох бітових значень: 0 і 1. Як і біт, кубіт допускає два власних стани, що позначаються $|0\rangle$ і $|1\rangle$, але при цьому може знаходитися і в їх суперпозиції, тобто в стані $A * |0\rangle + B * |1\rangle$, де A і B – комплексні числа, що задовольняють умові $|A|^2 + |B|^2 = 1$. Кубіт в одну одиницю часу дорівнює і 0, і 1, а класичний біт в ту ж одиницю часу дорівнює або 0, або 1.

Для ілюстрації цього розглянемо кругову поляризацію світла, що потрапляє на поляризаційний роздільник променя (рис. 1).

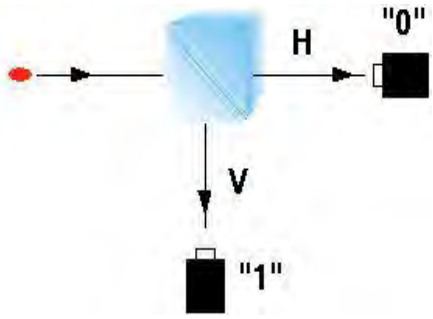

Рис. 1. Поляризований фотон

Поляризований фотон розпадається на вертикальну/горизонтальну складові з імовірністю 50% потрапити в будь-який з двох вихідних портів.

Використовуючи ці або інші принципи можна отримати теоретично ідеальний ГВЧ, випадковість якого гарантується законами квантової фізики.

Тестування генераторів випадкових послідовностей

Більшість тестів на випадковість служать для перевірки однієї або декількох статистичних властивостей довгих послідовностей випадкових чисел, наприклад, випадковість появи символів послідовності, незалежність, зсув, повторюваність, автокоррельованість і т.д. Деякі набори тестів більше орієнтовані на тестування ГПВП (наприклад, DIEHARD [3]), велика частина на тестування апаратних ГВП (наприклад, ENT [4]), а деякі носять загальний характер (наприклад, NIST STS [5]). Існує нескінченна кількість статистичних властивостей, яким повинні задовольняти дійсно випадкові послідовності чисел. Тести самі по собі не є досконалими: деякі містять помилки, виявлені пізніше [5], [6], або константи, які отримані шляхом моделювання за допомогою "довіреного" генератора випадкових чисел.

Важливо правильно інтерпретувати результати статистичних тестів. Якщо генератор проходить

всі відомі статистичні тести, це ще не доводить, що він видає дійсно випадкову послідовність. Це лише означає, що послідовність проходить всі відомі на даний час тести на випадковість. Завтра може з'явиться який-небудь новий тест або існуючих тестів стане недостатньо для розробників.

Тим не менш, тестування на випадковість є дуже важливим питанням для розробників генераторів випадкових чисел. У деяких випадках (особливо для квантових ГВЧ) можна обґрунтовано очікувати тільки певні типи відхилень від необхідних властивостей і застосовувати тести, орієнтовані виключно на виявлення цих проблем.

Висновок

В основі побудови ГПВЧ лежить вимога наближення властивостей згенерованих ними послідовностей до властивостей послідовностей рівномірно розподілених незалежних випадкових величин, тобто по суті, побудова генераторів, виходи яких важко відрізнити від дійсно випадкових послідовностей [3 – 6]. Внаслідок цього сучасна тенденція побудови генераторів дійсно випадкових чисел, заснована на використанні різних квантових процесів для генерації випадкових чисел, опису їх імовірнісних схем з позицій квантової фізики.

Дослідження методів побудови ГВЧ на основі квантових ефектів і процесів, аналіз вимог, пред'явлених до них, розробка структури джерел випадкових подій і обґрунтування вибору фізичного процесу, покладеного в його основу, є актуальним напрямом дослідження перспективних криптографічних систем.

Найбільш відмітною характеристикою квантового ГВЧ є науковий доказ випадковості його вихідних послідовностей.

Ретельна практична реалізація досить близька до ідеалізованої теоретичної моделі і дозволяє провести незалежну оцінку відхилень від необхідних властивостей, яка, при необхідності, може бути виконана на основі інформаційно-теоретичної постобробки.

Квантові ГВЧ є кращим рішенням для криптографії та інших додатків, які критично залежать від якості випадкових послідовностей. Найбільш істотним недоліком існуючих рішень є необхідність застосування досить габаритних фізичних рішень без можливості їх мініатюризації до рівня застосування сучасних технологій виробництва мікросхем.

Науково-технічні рішення, що з'являються в області оптичних мікросхем, пропонують перспективні засоби для квантових ГВЧ.

Список літератури

1. Горбенко Ю. Методи та засоби генерування псевдовипадкових послідовностей / Ю. Горбенко, Т. Гріненко, Н. Шапочка // Прикладна радіоелектроніка, 2011, том 10, №2. – С. 141-152.

2. Jennewein T. A Fast and Compact Quantum Random Number Generator / T. Jennewein, U. Achleitner // Rev. Sci. Instrum. 71, 200. – P. 1675–1680.

3. Marsaglia G. DIEHARD battery of stringent randomness tests (various articles and software) / G. Marsaglia // Internet: http://stat.fsu.edu/~geo/diehard.html.

4. Walker J. Ent: A Pseudorandom Number Sequence Test Program. http://www.fourmilab.ch/random/.

5. Ruhkin A. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A. Ruhkin // NIST Special Publication 800-22rev1a, NIST April 2010.

6. Ruhkin A. Statistical Testing of Randomness: Old and New Procedures / A. Ruhkin // Chapter in Randomness through Computation, H Zenil ed. World Scientific, 2011

Надійшла до редколегії 28.08.2015

Рецензент: д-р техн. наук, проф. І.Д. Горбенко, Харківський національний університет ім. В.Н. Каразіна, Харків.

КВАНТОВЫЕ ГЕНЕРАТОРЫ СЛУЧАЙНЫХ ЧИСЕЛ В КРИПТОГРАФИИ

Т.А. Гриненко, А.П. Нарежний

Приводится анализ существующих методов генерации случайных чисел. Отмечаются преимущества и недостатки существующих методов. Предлагается использовать для генерации случайных чисел генераторы, которые базируются на квантовых процессах, что позволит увеличить стойкость криптографических систем. Рассматривается вопрос тестирования генераторов случайных чисел.

Ключевые слова: *генератор случайных чисел, детерминированный генератор случайных чисел, квантовый генератор случайных чисел, тестирование, криптографический протокол.*

QUANTUM RANDOM NUMBER GENERATORS IN CRYPTOGRAPHY

T.A. Grinenko, A.P. Narezshhy

An analysis of known random number generation methods, their advantages and disadvantages are noticed. An application of generators is proposed that is based on quantum processes for random number generation that allows strength improvement of cryptographic systems. The problem of random number generation testing is considered.

Keywords: *random number generator, deterministic random number generator, quantum random number generator, testing, cryptographic protocol.*