УДК 004.056.55

Р.О. ГАВРИЛКО, Ю.І. ГОРБЕНКО, канд. техн. наук

КВАНТОВИЙ ФІЗИЧНИЙ ГЕНЕРАТОР ВИПАДКОВИХ ЧИСЕЛ НА ОСНОВІ РОЗЩЕПЛЕННЯ ПУЧКА ФОТОНІВ

Вступ

У статті представлено реалізацію фізичного квантового генератора випадкових чисел, дія якого основана на процесі поділу пучка фотонів, завдяки розщеплювачу променя – квантово-механічному джерелі істинної випадковості. Представлені пристрої здатні генерувати двійковий випадковий сигнал з часом автокореляції 11,8 нс і безперервний потік випадкових чисел зі швидкістю 1 Мбит/с. Це можливо завдяки використанню розщеплювача променя або поляризаційного розщеплювача променя, одиночних детекторів фотонів і високої швидкості електроніки. Наведено результати серії випробувань на зразках даних, які показують випадковість генеруємих сигналів і чисел. Пристрої, описані в цій статті, вбудовані в компактні корпуси і прості в експлуатації.

Випадкові числа є життєво-важливим компонентом у багатьох областях. Починаючи, наприклад, від обчислювальних методів, таких як Монте-Карло, і програмування, закінчуючи великою областю криптографії. Вони використовуються для генерації крипто кода або для маскування повідомлень. Потрібні в комерційних областей, таких як лотереї та ігрові автомати. Нещодавно ряд областей, що вимагають випадкових чисел був розширений завдяки розвитку квантової криптографії та квантової обробки інформації. Також новою є область, для якої представлений генератор випадкових чисел був розроблений – експеримент з приводу заплутаності двох частинок, фундаментального поняття в квантовій теорії. По-перше, цей експеримент потребував генерації випадкових сигналів з часом автокореляції <100 нс. По-друге, для ясності експериментальних результатів було необхідно, щоб не була реалізована істинна, тобто об’єктивна, випадковість.

1. Теоретична частина

Принципова відміна квантової фізики від класичної полягає в тому, що:

1) закономірності квантової фізики носять статистичний (ймовірнісний), а класичної фізики – динамічний (детерміністичний) характер;

2) процес вимірювання стану мікрооб'єкта істотно впливає на його стан, і тому в квантовій фізиці, на відміну від класичної, неможливо абстрагуватись від фізичної природи процесу вимірювання. Внаслідок цього, стан квантового об'єкта описується через так звані базисні стани, що задаються можливостями вимірювального приладу.

Квантові об’єкти мають декілька важливих властивостей:

- суперпозиція станів (здатність однієї частки перебувати в кількох станах одночасно)
- здатність системи із кількох часток перебувати в корельованиих (переплутаних) станах і пов'язана з цим нелокальність
- суттєвий вплив процесу вимірювання на стан об'єкта
- неможливість клонування квантових станів.

Усі ці властивості повною мірою використовує квантова інформатика. Стан фотона заданої частоти характеризується його поляризацією. Поляризаційний стан фотона визначається за допомогою поляризатора, вісь якого ми можемо розташувати довільним чином. Таким чином, можливі стани поляризатора утворюють *базис,* вертикальній поляризації відповідає вектор стану $|1\rangle$, горизонтальній поляризації – вектор стану $|0\rangle$. Стан фотона описують за допомогою амплітуди ймовірності, або хвильової функції, яка в зазначеному вище базисі має вигляд:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle. \quad (1)$$

Коефіцієнти α та β можуть бути комплексними. Відповідно, безпосередньо хвильова функція та коефіцієнти не є *спостережуваними* (їх неможливо виміряти). Із результатів вимірювання можна лише визначити квадрати модулів $|\alpha|^2$ та $|\beta|^2$, що характеризують ймовірність знайти систему в стані $|0\rangle$ або $|1\rangle$, відповідно.

Так, для вертикально поляризованого фотона $\alpha = 0, \beta = 1$, для горизонтально поляризованого навпаки, $\alpha = 1, \beta = 0$. Якщо фотон був поляризований під кутом 45° до вертикальної осі, то $\alpha = \beta = 1/\sqrt{2}$, тобто фотон з однаковою ймовірністю ½ пройде чи не пройде через поляризатор.

Квантова криптографія вирішує проблему розподілу ключів за допомогою використання властивості квантових систем змінювати свій стан в процесі вимірювання та неможливість клонування квантових станів.

До основних фундаментальних властивостей квантових систем, які використовуються в квантовій криптографії, можна віднести:

1. Вимірювання фізичних характеристик квантових систем (спостережуваних).

У результаті процесу вимірювання деякої фізичної величини стан квантової системи змінюється. Це обумовлено впливом на квантовий об'єкт вимірювального приладу, який принципово неможливо зробити як завгодно слабким. Чим точніше вимірювання, тим сильніший вплив, що воно здійснює, і лише при вимірюваннях дуже малої точності вплив на об'єкт вимірювання може бути досить слабким.

Крім того, збурювання, яке вноситься взаємодією квантового об'єкта з вимірювальним приладом, може бути передбачено тільки статистично й тому не може бути виключено. Цей факт перебуває в різкому протиріччі із класичною теорією вимірювань, яка базується на припущенні, що взаємодія між об'єктом і приладомякщо й не може бути зроблена як завгодно малою, то, принаймні, може бути точно врахованою й, отже, її можна виключити.

2. Неможливість точного клонування невідомих квантових станів (теорема про заборону клонування).

Внаслідок лінійності й унітарності квантової механіки неможливо створити точну копію невідомого квантового стану. Таким чином, зловмисник не може виготовити точну копію кубітів або кудитів, що передаються комунікаційним каналом, щоб провести вимірювання над копією, а оригінал переслати законному користувачеві каналу, не проводячи над ним вимірювання. Цей факт лежить в основі більшості протоколів квантової криптографії, тому що змушує зловмисника вимірювати передаванні кудити, або переплутувати їх зі своїми допоміжними квантовими системами, що призводить до зміни станів цих кудитів. Ці зміни передаваних станів можуть виявити законні користувачі, виконуючи квантові вимірювання й обмінюючись результатами цих вимірювань по звичайному відкритому каналу зв'язку.

3. Неортогональні квантові стани неможливо розрізнити.

4. Переплутування (квантові кореляції).

Дві або більше квантових системи можуть бути переплутані. Так, пара фотонів у синглетному поляризаційному стані

$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|1\rangle_2 - |0\rangle_2|1\rangle_1\right), \qquad (2)$$

де індекси позначають номери фотонів. Це приклад максимально переплутаного стану двох кубітів. Такий стан називають парою Ейнштейна– Подольського–Розена (ЕПР-парою).

Якщо вимірювання виконується над одним із двох переплутаних кубітів в стані $\left|\Psi^-\right\rangle$ (3), наприклад, в базисі $\{|0\rangle, |1\rangle\}$, який називається обчислювальним базисом, то результат буде "0" або "1" з однаковою ймовірністю 1/2. Стан другого кубіту антикорельований з першим, тобто якщо перший кубіт в результаті вимірювання перейшову стан $|0\rangle$, то другий

перейде в стан $|1\rangle$ і навпаки. Без проведення вимірювання, однак, жодний із цих двох кубітів не перебуває в певному стані. Відзначимо, що переплутування, як і суперпозиція станів, – винятково квантові ефекти, що не мають аналога для об'єктів класичної фізики.

Квантові протоколи розподілення секретних ключів пропонують інший підхід до вирішення цієї проблеми. Теоретично, квантова криптографія може забезпечити захищене від перехоплення розподілення ключа, оскільки на відміну від класичної криптографії, вона заснована на законах фізики, а не на тому факті, що для успішного перехоплення потрібні були б величезні обчислювальні потужності. Внаслідок зазначених властивостей квантових систем зловмисник вносить у передану окремими фотонами інформацію деяку кількість помилок, які можуть бути виявлені легітимними користувачами. Відзначимо, що закони квантової механіки дозволяють не тільки виявити збурювання станів, але й зв'язати рівень помилок при вимірюваннях у легітимних користувачів з кількістю інформації, що міг отримати зловмисник. Це дозволяє провести процедуру підсилення секретності, при якій довжина переданого ключа зменшується на деяке число біт, що залежить від рівня помилок при передачі. У результаті кількість інформації про ключ, що може мати зловмисник після цієї процедури, обмежена зверху як завгодно малою величиною, з імовірністю, як завгодно близької до одиниці. Таким чином, протоколи квантового розподілення ключів, на відміну від більшості класичних схем, мають теоретико-інформаційну стійкість, що не залежить від обчислювальних та інших технічних можливостей зловмисника.

Великий діапазон областей, які використовують випадкові числа, привів до розвитку різніх генераторів випадкових чисел, а також засобів для перевірки їх вихідних даних на випадковість. Взагалі є два підходи до генерації випадкових чисел. Перший це псевдогенератори випадкових чисел, які покладаються на алгоритми, які реалізуються на обчислювальному пристрої. Другі – це фізичні генератори випадкових чисел, що вимірюють деякі фізичні спостереження, які мають вести себе випадковим чином.

Псевдогенератори випадкових чисел засновані на алгоритмах або навіть на комбінації алгоритмів. Вони були високо уточнені в плані періодів повторення (2^{800}) і стійкості до тестів на випадковість. Але притаманна алгоритмічна еволюція псевдовипадкових генераторів є суттєвою проблемою в областях, що вимагають випадкових чисел. Вимоги нашої конкретної реалізації були такі, що використання генератора псевдовипадкових чисел само по собі вже виключило його детерміновану природу.

Фізичні генератори випадкових чисел використовують випадковість чи шум, які спостережуються фізично. Наприклад, шум електронних приладів, сигналів мікрофонів та ін. Основою багатьох фізичних генераторів є дуже великі і складні фізичні системи, які мають хаотичну, але в принципі детерміновану, поведінку у часі. Завдяки багатьом невідомим параметрам великих систем їх поведінка сприймається як істинна випадковість. Суто класичні системи мають детермінований характер протягом відповідних періодів часу і зовнішній вплив у генератор випадкових чисел може залишатися прихованим.

Сучасна теорія припускає, що єдиний спосіб реалізувати чітке і зрозуміле фізичне джерело випадковості є використання елементарних квантових рішень, так як в загальному розумінні виникнення кожного окремого результата такого квантово-механічного рішення об'єктивно випадкове. Існує ряд таких елементарних рішень, які є підходящими кандидатами для джерела випадковості. Найбільш очевидний – процес розпаду радіоактивного ядра (^{85}Kr, ^{60}Co), який вже використовується. Однак поводження з радіоактивними речовинами вимагає додаткових заходів обережності. Особливо на радіоактивність перемикача частоти випадкових сигналів.

Альтернативою є оптичні процеси, які придатні у якості джерел випадковості.

До них відносятся:

- 1. Розщеплення окремих пучків фотонів
- 2. Вимірювання поляризації одиночних фотонів
- 3. Просторовий розподіл лазерних спеклів

- 4. Світло-темні періоди резонансного сигналу
- 5. Флуоресценції окремо захопленного іона.

Але тільки перші два з зазначених оптичних процесів досить швидкі і, крім того, не вимагають переважних технічних зусиль у їх реалізації. Таким чином, ми розробили фізичний квантово-механічний генератор випадкових чисел на основі розщеплення пучка фотонів з оптичним розщеплювачем променя 50:50 або шляхом вимірювання поляризації окремих фотонів з поляризаційним розщеплювачем променя

2. Принцип роботи

У першому випадку (рис.1) використовується розщеплювач променя 50:50 (РП), де кожний окремий фотон з однаковою ймовірністю можна знайти в будь-якому виході розщеплювача променя.

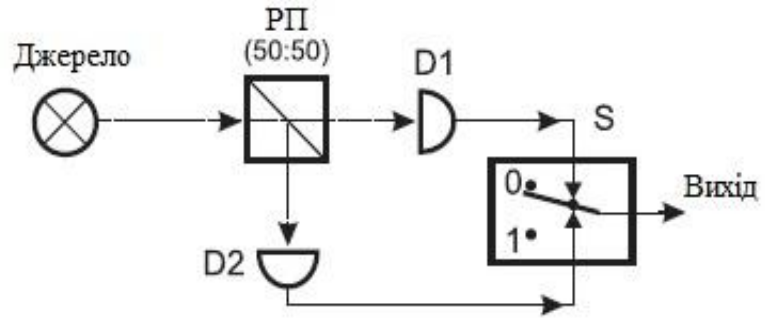

Рис. 1

В другому випадку (рис.2) використовується поляризаційний розщеплювач променя (ПРП), у якому кожний окремий фотон поляризується на 45° і має однакову ймовірність бути знайденим в горизонтальному або вертикальному поляризаційному виході.

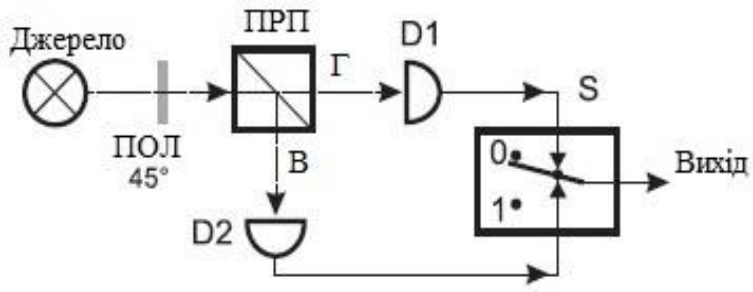

Рис. 2

Квантова теорія передбачає, що окремі результати є дійсно випадковими і незалежними один від одного. У цьому генераторі це реалізується завдяки виявленню фотонів у двох вихідних пучках світла (рис. 3).

Виявлені імпульси поєднуються в тумблері S. Він має два стани 1 або 0. Якщо імпульс було виявлено на детекторі D1, то перемикач S перейде у стан 0 і залишиться в цьому стані до тих пір поки не буде виявлено імпульс в детекторі D2. Якщо імпульс виявлено на детекторі D2 перемикач S перейде у стан 1 і залишиться в ньому до тих пір, поки подія детектора D1 не відбувається знову, і не встановить перемикач S у стан 0. У випадку, якщо виявляється декілька подій поспіль в одному і тому ж датчику, то тільки перше виявлення перемикає перемикач S у відповідний стан, і після цього залишає перемикач в незміненому стані.

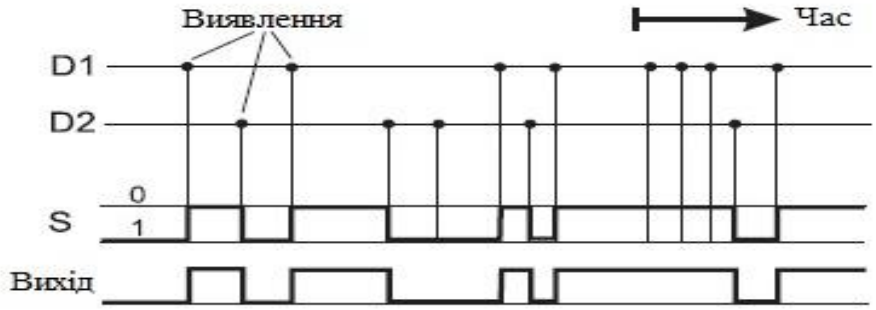

Рис. 3

Отже, перемикання тумблера S між двома станами являє собою двійковий випадковий сигнал з випадковістю, яка лежить у часі переходу між двома станами. Для того щоб уникнути будь-яких помилок, джерело світла повинне отримувати значно менше одного фотона за час когерентності.

3. Реалізація пристрою

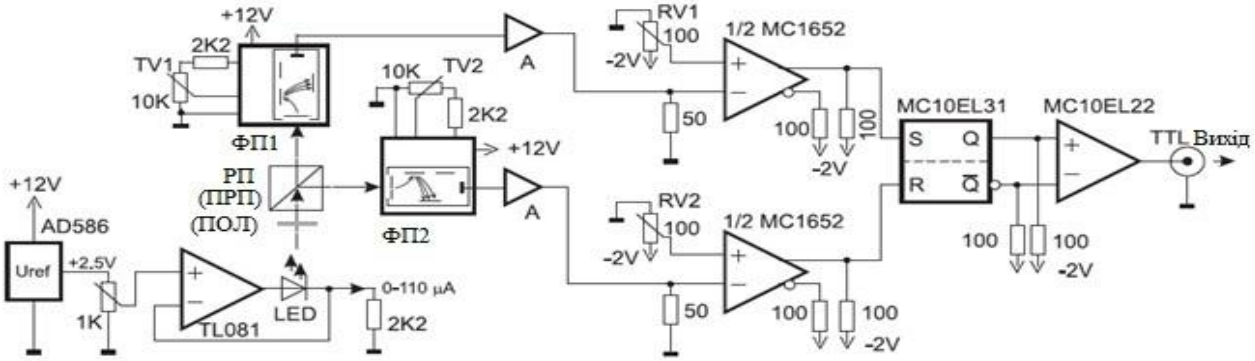

Рис. 4

На рис. 4 показана принципова схема фізичного квантового генератора випадкових чисел. Джерелом світла виступає червоний світлодіод (LED), який керуєтеся регульованим джерелом струму з максимумом 110 мкА (μA.). Через дуже малу довжину когерентності даного виду джерела (< 1 ПС) можна стверджувати, що більшу частину часу немає жодних фотонів, присутніх в межах часу когерентності, тим самим усуваються помилки. Світло, яке виникає від світло діода, прямує через шматок труби на розщеплювач променя, який може бути розщеплювачем променя 50:50 або поляризаційним розщеплювачем променя. В останньому випадку фотони поляризуються заздалегідь. Фотони в двох вихідних пучках виявляються за допомогою швидкісного фотоелектронного помножувача (PM1, PM2). Фотоелектронні помножувачі – це закриті модулі, які містять всю необхідну електроннику, а також

генератор лампової напруги і, таким чином, вимагають тільки +12V живлення. Лампову напругу можна регулювати за допомогою потенціометра (TV1, TV2) для оптимального виявлення частоти і амплітуди імпульсу. Вихідні сигнали посилюються в двох підсилюючих модулях і передаються до сигналізуючої електроніки, яка реалізується у емітерно-зв'язаній логіці (ЕЗЛ) Імпульси детектора перетворюються в сигнали ECL за допомогою двох компараторів (MC1652) в залежності від порогових напруг, встановлених для потенціометрів (RV1, RV2). Фактичний синтез випадкового сигналу здійснюється в межах RS-тригера (MC10EL31) як PM1 запускає S-вхід і PM2 запускає R-вхід тригера. Вихід цього тригера перемикається між високим і низьким станом, залежно від того, де відбулася остання подія –

в PM1 або PM2. Нарешті випадковий сигнал перетвориться з ECL в логічні рівні TTL (MC10EL22) для подальшого використання.

Для того щоб генерувати випадкові числа на персональному комп'ютері, сигнал від генератора випадкових чисел періодично відбирають і накопичують в 32-розрядному регістрі широкого зсуву. Кожні 32 такти вміст регістру передається паралельно до персонального комп'ютера за допомогою плати швидко цифрового вводу/виводу.

Таким чином, безперервний потік випадкових чисел передається на персональний комп'ютер.

4. Переваги та недоліки

При реалізації квантових генераторів на практиці зазвичай є недоліки. Основний недолік таких систем те, що вірогідність неточно дорівнює ймовірності нулів, тому що фотони виявляються двома і більше детекторами. Ефективність виявлення фотона детектором може значно змінюватися від одного фізичного пристрою до іншого. Зазвичай електроніка дуже чутлива до зміни параметрів під впливом температури, коливань напруги живлення, зносу. Для того щоб як найбільш мінімізувати зсув, квантові генератори випадкових чисел повинні бути точно налаштовані перед використанням. Це не дуже зручно тому, що точне налаштування – дуже трудомістка процедура через статистичну природу вимірювання зсуву. Крім того, через проблеми стійкості, не можна очікувати, що зміщення, скореговане раніше, залишалося б постійним протягом тривалого часу.

Але у таких генераторів є безліч переваг. Однією з основних є дуже велика швидкість генераціх випадкових чисел. Це досягається шляхом використання швидких одиночних детекторів фотонів, а також високошвидкісної електроніки. До переваг можно віднести те, що квантовий генератор здатен виробляти послідновність с часом автокореляції 12 нс та внутришнім часом затримки 75 нс. Час затримки складається з: 20 нс – час затримки в джерелі світла, 20 нс – час затримки підсилювачів і кабелів, а також 35 нс – затримка за часом в основній електроніці. Також цей пристрій може виробляти випадкові числа шляхом періодичного відбору проб сигналу і циклічної передачі даних на персональний комп'ютер.

5. Перспективи пристрою

Експериментальні результати, представлені в попередній главі, дозволють очікувати, що фізичний квантовий генератор випадкових чисел здатен виробляти випадкову двійкову послідовність з часом автокореляції 12 нс і внутрішнім часом затримки 75 нс. Це підкреслює придатність цих пристроїв для їх використання в нашому конкретному експерименті, який вимагає генератори випадкових сигналів з часом встановлення випадкового стану на виході менше, ніж <100 нс, що легко досягається за допомогою фізичних квантових генераторів випадкових чисел, представлених у цій статті.

Висока швидкість наших генераторів стала можлива завдяки використанню швидких одиночних детекторів фотонів, а також високошвидкісної електроніки. Крім того, набір тестів продемонстрував якість випадковостей, які отримуються за допомогою фундаментального квантово-механічного рішення в якості джерела випадковості.

Деякі методи для підвищення продуктивності можна передбачити. Наприклад, інший спосіб генерації випадкового сигналу полягає у тому, що кожен фотоелектронний помножувач (PM) перемикає 1/2 дільника, який призводить рівномірно розподілені сигнали. Ці сигнали можуть бути об'єднані в XOR-gate (XOR- схема), щоб використовувати квантову випадковість аналізатора поляризації, але повністю зберігаючи рівнорозподіл сигналу. Скорочення часу автокореляції сигналу можливе за рахунок оптимізації сигналів електроніки (наприклад, з використанням сигналів ECL всієї конструкції). Крім того, нескладно об’єднати кілька таких випадкових генераторів в рамках одного пристрою, тому що немає перехресних перешкод між субодиницями, так як елементарні квантові процеси повністю незалежні і не визначені. Тому проектування фізичного квантового генератора випадкових чисел, який

здатен виробляти істинно випадкові чисела зі швидкістю > 100 Мбіт/с або навіть вище 1 Гбіт/с, – посильне завдання. Ми вважаємо, що для генераторів випадкових чисел, розташованих навколо елементарних квантово-механічних процесів, буде знайдено безліч застосувань для виробництва випадкових сигналів і цифр, оскільки джерело випадковості зрозуміле.

Висновок

Квантові генератори випадкових сигналів на основі квантово-механічних рішень є перспективними. Такі генератори мають швидкодію до 10^9 біт/с, а також малий час затримки. Крім того, квантові генератори забезпечують необхідну для криптографічних додатків нерозрізнюваність. Такий ефект досягається за допомогою фундаментального квантово-меха-нічного рішення. Також існує можливість прискорення швидкодії, в тому числі навіть більше 1 Гбіт/с. Вказане дозволяє вважати такий генератор перспективним для застосування в криптографічних додатках.

Список літератури: 1. *Горбенко, І. Д.* Прикладна криптологія / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Форт, 2012. – 868 с. 2. *A Fast* and Compact Quantum Random Number Generator/ Thomas Jennewien, Ulrich Achleitner, Gregor Weihs, Harald Weinfurter and Anton Zeilinger – 4/III D-80799 Munchen, Germany February 1, 2008.

Харківський національний університет
імені В.Н.Каразаіна

Надійшла до редколегії 19.05.2015