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*

МЕТОДИ ГЕНЕРУВАННЯ ШУМОВИХ СИГНАЛІВ, ЩО ЗАСТОСОВУЮТЬСЯ В КРИПТОГРАФІЧНИХ МОДУЛЯХ

Наводиться аналіз існуючих фізичних датчиків шуму, які є стійкими до жорстких впливів зовнішнього середовища і мають досить високу експлуатаційну надійність. Відзначаються переваги і недоліки існуючих методів формування випадкових послідовностей в криптографічних модулях. Пропонується використовувати в якості фізичного джерела випадковості методи, які базуються на квантових процесах, що дозволить збільшити стійкість криптографічних систем. Відмічається, що недоліком даних джерел випадковості є вимога індивідуальної калібровки квантових датчиків.

Ключові слова: *генератор випадкових послідовностей, квантовий генератор випадкових чисел, датчик шуму, ентропія, засіб генерації ключів.*

Вступ

Одним з основних елементів криптографічних систем захисту інформації, від характеристик якого залежать характеристики системи в цілому, є засіб генерації ключів. 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 (ГПВЧ). Тому гарантії криптографічної стійкості суттєво визначаються якістю випадковості джерел ентропії ГВЧ і ГПВЧ.

Проведений аналіз показав, що складовим чи основним елементом генераторів ключів є фізичний генератор випадкових чисел. Фізичний генератор випадкових чисел (ФГВЧ) – пристрій, який генерує випадкові числа на основі фізичного процесу (тепловий шум, фотоелектричний ефект або квантові явища), який є абсолютно непередбачуваним.

У деяких джерелах ФГВЧ називають недетермінованим генератором випадкових чисел (НГВЧ) або ГВЧ.

Основною відмінністю генератора випадкових чисел від генератора псевдовипадкових чисел є те, що джерело ентропії обов'язково містить фізичний датчик шуму. В статті наводиться аналіз існуючих фізичних датчиків шуму, відзначаються їх переваги і недоліки.

Аналіз фізичних датчиків шуму

Аналіз показав, що в сучасних криптографічних системах швидкість генерації випадкових послідовностей повинна перевищувати 1 Мбіт/сек. Такі параметри можуть бути реалізовані на основі електронних датчиків шуму з широким спектром частот [1, 2].

В табл. 1 наведено загальну класифікацію датчиків згідно з фізичними властивостями, для виміру яких вони розроблені.

Таблиця 1

Класифікація датчиків
згідно з фізичними властивостями

Властивість	Датчик	Активний/ пасивний	Вихід
Температура	Термоелемент	Пасивний	Напруга
	Тиристор	Активний	Напруга струм
	Резистивний термометр	Активний	Опір
	Термистор	Активний	Опір
Сила/тиск	Тензометр	Активний	Опір
	П'єзокварцевий датчик	Пасивний	Напруга
Прискорення	Акселерометр	Активний	Ємність
Позиція	Перетворювач переміщення	Активний	Змінна напруга
Інтенсивність світла	Фотодіод	Пасивний	Струм

Випадкові зміни параметрів (тепловий шум) спостерігаються в усіх електронних компонентах при температурах вище абсолютного нуля за Кельвіном.

Тому як фізичні датчики шуму можуть бути використані будь-які електронні компоненти.

В якості фізичного датчика шуму, можна використовувати датчики шуму на основі резисторів, які генерують випадковий сигнал у смузі частот від одиниць Гц до сотень МГц з амплітудами вихідної напруги не більше 0,1 мВ [1, 2]. Тому для сполучення з цифровими пристроями необхідно застосовувати підсилювачі з коефіцієнтом посилення за напругою в декілька тисяч разів. Споживна потужність такого датчика визначається в основному потужністю підсилювача і становить від десятків до сотень мВт при напрузі живлення від 5 до 15 В. Перевагами датчиків шуму на основі резисторів є малі габаритні параметри, невеликі економічні витрати на виготовлення фізичного датчика шуму.

В якості генератора шумових напруг можна використовувати діод в діапазоні зворотних струмів [1,2]. Напівпровідниковий шумовий діод – це напівпровідниковий прилад, що є джерелом шуму із заданою спектральною щільністю в певному діапазоні частот. Наприклад, датчики шуму на основі кремнієвих діодів Зенеровського пробою (стабілітрони) генерують випадковий сигнал з рівномірним спектром від одиниць Гц до десятків МГц і амплітудами в десятки мВ. Такі прилади розроблені і випускаються як спеціалізовані шумові діоди із Зенеровським пробоєм (наприклад, КГ401). Вони при напрузі 8-9 В і струмі від 50 до 100 мкА генерують широкий спектр (до десятків МГц) випадкових імпульсів з амплітудами від 0,1 до 1В. Споживна потужність таких датчиків шуму менше 1 мВт при напрузі живлення від 10 до 20 В, що дозволяє легко вбудовувати їх в обчислювальні системи. Малогабаритні та економічні показники датчиків шуму на основі шумових діодів із Зенеровським пробоєм є одними з найкращих при реалізації в інтегральному виконанні на одному кристалі з обчислювальною системою.

Датчики шуму на основі електронних ламп (діоди, тріоди і т.д.) генерують випадковий сигнал (дробовий шум) з рівномірним спектром від одиниць Гц до десятків МГц і амплітудою менше 1 мВ [1,2]. Тому для них обов'язковим є застосування підсилювачів на лампах або транзисторах. Споживна потужність складає одиниці Вт, живильні напруги – від 50 до 200 В. Малогабаритні показники значно перевищують аналогічні показники сучасних інтегральних схем. Необхідно також враховувати зміну параметрів у процесі експлуатації електронних ламп за рахунок погіршення емісійних властивостей катодів. Недолік таких датчиків – великі масогабаритні показники, тому застосування таких датчиків шуму в сучасних системах практично неможливе.

Датчики шуму на основі застосування газорозрядних ламп (стабілітрони), що генерують випадковий сигнал у смузі частот від одиниць Гц до сотень кГц і амплітудою до 1 В [1,2]. Недоліками таких датчиків є великі масогабаритні показники і необхідність високої напруги живлення (від 70 до 200В), тому застосування таких датчиків шуму в сучасних системах є недоцільним.

Датчики шуму на основі фотоелектронних помножувачів [1, 2], які формують випадкові імпульси амплітудою менше 1 мА з частотою, обумовленою як тепловими процесами на поверхні фотокатода, так і рівнем зовнішнього засвічення. Це дозволяє легко регулювати середню частоту випадкових імпульсів в інтервалі від одиниць кГц до десятків МГц зі зміною оптичного сигналу підсвічування фотокатода. У цьому випадку необхідно враховувати залежність генерованого сигналу від напруги живлення та температури навколишнього середовища. Недоліками таких датчиків є великі масогабаритні показники і необхідність високої напруги живлення (від 500 В до 3 кВ), тому застосування таких датчиків шуму в сучасних системах є недоцільним.

Зробивши аналіз існуючого матеріалу можна зробити висновок, що в криптографічних додатках в якості фізичних датчиків шуму доцільно використовувати датчики на основі резисторів або датчиків на основі кремнієвих діодів Зенеровського пробою.

Ряд переваг перед ГПВЧ мають генератори, що ґрунтуються на випадковості квантових процесів. 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.

На основі аналізу основних джерел [3-9] визначено, що в якості фізичних явищ при створенні квантових генераторів можна використовувати такі.

1. Дробовий шум – це шум в електричних ланцюгах, що викликаний дискретністю носіїв електричного заряду, шум у оптичних пристроях. Як джерело шуму використовують фотоелектронний помножувач або електровакуумні фотоелементи.

2. Радіоактивний розпад, для якого характерна випадковість забезпечується за допомогою кожного окремого акту розпаду. В результаті на приймач

в різні проміжки часу потрапляє різна кількість частинок.

3. Квантовий оптичний процес як джерело випадковості.

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. До таких процесів можна віднести: розщеплення окремих пучків фотонів; вимірювання поляризації одиночних фотонів; світло-темні періоди резонансного сигналу флуоресценції окремо захопленого іона.

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.

Метрологічні характеристики квантових датчиків шуму

На основі аналізу виду графіків квантових генераторів шуму (ГШ), що відображають їхню спектральну щільність, джерела шуму можна поділити на дві категорії [1]. На високих частотах домінує білий шум, а на низьких – флікер-шум ($1/F$-шум). Для білого шуму характерна рівномірна спектральна щільність. У цьому випадку енергія сигналу буде однакова в будь-якій заданій смузі частот. У разі флікер-шуму енергія сигналу буде однакова в кожній декаді. Частота, нижче якої інтенсивність флікер-шуму починає перевищувати інтенсивність білого шуму, називається частотою зламу F_C.

Напругу шуму квантових ГШ в смузі частот можна оцінити, взявши спектральну щільність білого шуму (ND) з таблиці калібрувальних параметрів, верхню (F_h) і нижню (F_l) робочі частоти:

$$U_n = ND\sqrt{F_h - F_l} \ \text{[В]}. \qquad (1)$$

У рівняння (1) не входить флікер-шум і, отже, воно вірно тільки для діапазонів, частота нижньої межі яких істотно більше частоти зламу ($F_l >> F_C$). Теоретично можна передбачити напругу шуму в будь-якій бажаній смузі частот, якщо спектральна щільність шуму (ND) і частота зламу (F_C) задані.

Середньоквадратичне (RMS) значення шуму в смузі частот визначається площею під кривою спектральної щільності шуму між верхньою (F_h) і нижньою (F_l) частотами смуги і записується у вигляді:

$$\overline{U}(F_h, F_l, F_C) = \sqrt{\int_{F_l}^{F_h} \left(ND\sqrt{\frac{F_C}{F} + 1} \right)^2 dF} \ \text{[В]}, \qquad (2)$$

де ND – спектральна щільність білого шуму $\left[\text{мкВ}/\sqrt{\text{Гц}} \right]$; F_C – частота зламу [Гц]; F_l – нижня межа смуги частот [Гц]; F_h – верхня межа смуги частот [Гц].

Для оцінки калібрувальної характеристики спектральної щільності потужності шуму (СЩПШ) квантового ГШ пропонується використовувати спрощений вираз (2), що приведений до смуги аналізу 1 Гц, в наступному вигляді:

$$S_U(F_h, F_l, F_C) = ND^2 \left[F_C \ln\left(\frac{F_h}{F_l} \right) + F_h - F_l \right] \ \text{[Вт/Гц]}. \qquad (3)$$

Індивідуальні калібрувальні характеристики СЩПШ квантових ГШ пропонується отримувати методом звірення за допомогою компаратора шляхом застосування низькотемпературних мір (ГШ) державного первинного еталона спектральної щільності потужності шумового радіовипромінювання. Отримані оцінки СЩПШ $\hat{S}_u(F)$ записують у таблицю калібрувальних параметрів ГШ.

Використовуючи вираз (3) апроксимують калібрувальні характеристики методом найменших квадратів в заданій смузі частот для оцінки невідомих характеристик спектральної щільності шуму (ND) і частоти зламу (F_C).

Пропонується значення ND і F_C записувати або в таблицю електричних параметрів технічного опису криптографічного модуля, або представляти у вигляді графіка СЩПШ, що наводиться в розділі типових умов експлуатації.

Так, використовуючи виконаний у логарифмічному масштабі графік СЩПШ (3), можна знайти F_C на перетині ліній ND і 1/F. При цьому квантові ГШ можна калібрувати спільно з вимірювачами коефіцієнта шуму серії NFA компанії Agilent або Keysight. Крім того, для отримання СЩПШ квантові ГШ повинні мати коаксіальний вихід для підключення до аналізаторів спектра серії ESA або

аналізаторів сигналів MXA і EXA компанії Agilent або Keysight.

Квантові джерела шуму повинні мати також можливість автоматичного вимірювання своєї власної шумової температури.

Висновок

В якості фізичних джерел випадковості доцільно використовувати генератори, що ґрунтуються на випадковості квантових процесів, так як в загальному розумінні такі процеси є об'єктивно випадковими. Ці процеси обумовлені законами квантової фізики, тому заслуговують уваги та подальшого дослідження. Існує ряд методів, які є підходящими кандидатами для джерела випадковості.

Серед них можна виділи оптичні процеси, так як вони досить швидкі і, крім того, не вимагають переважних технічних зусиль у їх реалізації. Аналіз показує, що доступні через онлайн сервіси квантові генератори, за результатами тестування згідно NIST 800-90 [10] мають не гіршу нерозрізнюваність (випадковість), ніж класичні генератори випадкових послідовностей.

Оцінки теоретичної стійкості квантових генераторів випадкових чисел дозволяють зробити висновок, що по цьому показнику вони мають переваги, це пояснюється тим, що механізми випадковості квантових ГШ засновані на фундаментальних законах квантової фізики.

Список літератури

1. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування. Монографія. / І.Д. Горбенко, Ю.І. Горбенко. – Харків, Вид. «Форт», 2012. – 878 с.

2. Торба А.А. Математические модели датчиков шума. / А.А. Торба, В.А. Бобух, А.А. Торба // Прикладна радіоелектроніка. – 2007. – Том 6. №2. – С. 277-282.

3. Гаврилко Р. Квантовий фізичний генератор випадкових чисел на основі розщеплення пучка фотонів / Р. Гаврилко, І. Горбенко // Матеріали IV-ої Міжнародної НТК [Захист інформації і безпека інформаційних систем], (м. Львів, 04-05 червня 2015 р.) – С. 149–150.

4. 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.

5. Osung Kwon, Young-Wook Cho, and Yoon-Ho Kim. Quantum Random Number Generator using Photon-Number Path Entanglement. Department of Physics, Pohang University of Science and Technology (POSTECH), Pohang, 790-784, Korea-2013.

6. Kwon O., Cho Y.-W.,Kim Y.-H. Quantum Random Number Generator using Photon-Number Path Entanglement // arXiv:0807.3440v2 [quant-ph] 4Aug 2008. – pp. 1–4.

7. Stipčevića M., Medved Rogina B Quantum random number generator based on photonic emission in semiconductors // REVIEW OF SCIENTIFIC INSTRUMENTS. – Vol. 78 – 2007. – pp. 1–7.

8. Feihu Xu, Bing Qi, Xiongfeng Ma, He Xu, Haoxuan Zheng. Ultrafast quantum random number generation / OPTICS EXPRESS. – Vol. 20. – No. 11. –2012.

9. Qi B., Chi Y-M., Lo H-K., Qian L. Experimental demonstration of a high speed quantum random number generations cheme based on measuring phase noise of a single mode laser // Optics Letters, 2010. – Vol. 35– pp. 312-314.

10. 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.

Надійшла до редколегії 6.12.2014

Рецензент: д-р техн. наук, проф. В.І. Долгов, Харківський національний університет імені В.Н. Каразіна, Харків.

МЕТОДЫ ГЕНЕРАЦИИ ШУМОВЫХ СИГНАЛОВ, ПРИМЕНЯЕМЫЕ В КРИПТОГРАФИЧЕСКИХ МОДУЛЯХ

Т.А. Гриненко, А.П. Нарежний

Приводится анализ существующих физических датчиков шума, устойчивых к жестким воздействиям внешней среды и имеющих достаточно высокую эксплуатационную надежность. Отмечаются достоинства и недостатки существующих методов формирования случайных последовательностей в криптографических модулях. Предлагается использовать в качестве физического источника случайности методы, основанные на квантовых процессах, что позволит увеличить стойкость криптографических систем. Отмечается, что основным недостатком данных источников случайности является требование индивидуальной калибровки квантовых датчиков.

Ключевые слова: *генератор случайных последовательностей, квантовый генератор случайных чисел, датчик шума, энтропия, средство генерации ключей.*

NOISE SIGNAL GENERATION METHODS FOR APPLICATION IN CRYPTOGRAPHIC MODULES

T.A. Grinenko, A.P. Narezshny

It is given an analysis of existing physical noise units robust to hard environment influence and having sufficient operation reliability. It is noted advantages and disadvantages of known methods of random sequences generation in cryptographic modules. It is proposed to use methods based on quantum processes as entropy source that allows cryptographic systems strength improvement. It is noted that the main disadvantage of such entropy sources is a requirement of quantum units individual adjustment.

Keywords*: random sequences generator, quantum random number generator, noise unit, entropy, key generation means.*