2002 г. На выставке «Безпека 2002» в Киеве ЕПОС демонстрирует возможность передачи информации путем программного управления излучением компьютера (вариант Soft TEMPEST).

Список литературы

1. Wim van Eck. Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk. Computers & Security, #4, 1985, pp. 269-286.

2. Peter Wright. Spycatcher - The Candid Autobiography of a Senior Intelligence Officer. William Heinemann Australia, 1987.

3. Markus G. Kuhn, Ross J. Anderson. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations

4. Peter Smulders. The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables. Computers & Security, #9, 1990, pp. 53-58.

5. Markus G. Kuhn. Optical Time-Domain Eavesdropping Risks of CRT Displays. IEEE Symposium on Security and Privacy, Oakland, California, May 12-15, 2002.

6. С. Чеховский. Концепция построения компьютеров, защищенных от утечки информации по каналам электромагнитного излучения. Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». Тезисы докладов. Издательство "Інтерлінк", Киев, 2002, стр. 80.

7. С.Р. Коженевский, Г.Т. Солдатенко. Предотвращение утечки информации по техническим каналам в персональных компьютерах. Научно-технический журнал "Захист інформації", 2002, №2, стр.32-37.

8. В. В. Овсянников, Г. Т. Солдатенко. Нужны ли нам защищенные компьютеры? Научно–методическое издание «Техника специального назначения», 2001, №1, стр. 9-11.

Поступила 23.01.2003г.

УДК 681.3

О.І.Гарасимчук, В.М.Максимович

ГЕНЕРАТОРИ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ, ЇХ ЗАСТОСУВАННЯ, КЛАСИФІКАЦІЯ, ОСНОВНІ МЕТОДИ ПОБУДОВИ І ОЦІНКА ЯКОСТІ

Послідовність називається псевдовипадковою, якщо вона виглядає, як безсистемна і випадкова, хоча насправді вона створювалась з допомогою суто детермінованого процесу, відомого під назвою псевдовипадкового генератора. Подібні генератори переважно задаються деяким початковим значенням і за допомогою певних алгоритмів отримують з нього випадкові послідовності. В цьому сенсі псевдовипадкові генератори можна розглядати як розповсюджувачі випадковості.

Комп'ютери є детермінованими машинами, що завжди роблять саме те на що вони запрограмовані і це усуває можливість звертатися до комп'ютерів як до джерела істинної випадковості. Саме краще, на що здатний комп'ютер, – це згенерувати псевдовипадкову послідовність, яка хоча і виглядає випадковою, але, насправді, такою не є [1].

Згенерувати дійсно випадкову послідовність можна лише при апаратній реалізації генератора, який би для отримання випадкових чисел використовував деяке фізичне явище, наприклад, шум, який генерують напівпровідникові прилади, молодші біти оцифрованого звуку, інтервали між перериванням пристроїв або натисканням клавіш, температуру повітря і т.д. В сучасних потужних криптосистемах військового призначення використовують генератори випадкових чисел (ГВЧ), які є платами або зовнішніми пристроями, які підключаються до ЕОМ через порт вводу-виводу, а основними джерелами білого Гаусівського шуму є високоточне вимірювання теплових флуктуацій і запис радіоефіру на частоті вільній від радіомовлення.

Незважаючи на труднощі, які виникають при проектуванні генераторів псевдовипадкових чисел (ГПВЧ), вони широко використовуються в прикладних комп'ютерних програмах і легко компонуються з усіма типами комп'ютерних систем. Тому, на сьогоднішній день, більшість прикладних комп'ютерних програм використовують ГПВЧ для генерації потрібних випадкових даних [2].

ГПВЧ широко застосовуються в багатьох галузях, а особливо в тих, які пов'язані з використанням електронної та електронно-обчислювальної техніки. На рис.1 відображені основні сфери використання ГПВЧ.

Оскільки збільшується передача даних через загальні і приватні мережі передачі, стає все більш важливим захист приватності інформації яка зберігається і обмінюється між комп'ютерами. Один із стандартних блоків безпеки є ГВЧ [2].

Проблема захисту інформації є багатогранна і вирішується комплексно, з використанням великої кількості способів.

Випадкові числа – фундаментальний стандартний блок для зміцнення і забезпечення конфіденційності зв'язків радіоелектронними засобами. Вони основний елемент криптографії, цифрового підпису, протоколів безпеки і іншого забезпечення надійності при зв`язку через комп'ютер.

ГВЧ також часто застосовують в імітаційному моделюванні. В багатьох випадках потрібне використання різних послідовностей випадкових чисел. Наприклад для запуску однієї і тієї ж самої програми (але використовуючи різні потоки випадкових чисел) на багатьох процесорах, з метою отримання статистично незалежних результатів на кожному процесорі, а потім ці результати можуть бути усереднені. Але використання детермінованого алгоритму при генерації чисел є також корисним в багатьох випадках. Наприклад, при моделюванні всіх видів процесів, починаючи від автоматизації телефонних ліній і закінчуючи дорожнім рухом, вимагається, щоб послідовність псевдовипадкових чисел можна було повторити для досліджень поставленої задачі при інших параметрах. А за допомогою ГВЧ це зробити неможливо [3]. ГПВЧ використовуються для імітаційного моделювання не лише у фізичних галузях, але і в інших. Як приклад використання ГПВЧ в імітаційному моделюванні можна навести його застосування для імітації мутацій в біологічних дослідження [4].

Ще одна важлива галузь застосування ГВЧ – це їх застосування для контролю якості друкованих плат, окремих модулів або й цілих пристроїв [5], [6], [7], [8], [9]. Цьому питанню на сьогоднішній день приділяється не менша увага ніж застосування таких генераторів при вирішенні питань пов'язаних із захистом інформації. Наприклад в [7] автор запропонував декілька нових цікавих методик дослідження аналогових схем і електронних модулів. В [5] використана методика псевдовипадкового тестування за допомогою цифрового білого шуму з обмеженою смугою пропускання (псевдовипадкові зразки), як вхідного збуджувача. Характеристика будується, на основі обчислення взаємної кореляції між вихідною реакцією і псевдовипадковою вхідною послідовністю.

Рис.1 Основні сфери застосування ГПВЧ

В [9] розроблені схеми сканування з вбудованою самоперевіркою, які використовують лінійні зсувні регістри, як генератори псевдовипадкових зразків. Ці схеми сканування досягають досить високого покриття дефектів, які є в досліджуваних об'єктах.

При використанні ГПВЧ необхідно враховувати те, що вони мають бути достатньо надійними. Наприклад, електронний автомат потребує таку послідовність, яку не можна було б передбачити, знаючи попереднє значення; інакше система зазнала б невдачі, якщо б гравець визначав наступні оберти на основі аналізу моделі попередніх обертів; аналогічна ситуація при кодуванні повідомлень – потрібно забезпечити таку випадкову послідовність, щоб знаючи частину розсекреченого документа неможливо було б розсекретити весь документ.

Найчастіше ГПВЧ застосовують в криптографії [1], [10], [11], [12], [13], [14], [15]. Випадковість і криптографія дуже сильно взаємопов'язані. Важко знайти добре розроблене криптографічне прикладне забезпечення, яке не використовує випадкові числа. Криптографічні ключі, їх ініціалізація, тонкощі хешування з паролями, унікальні параметри в операціях цифрового підпису системними розробниками повинні прийматися випадковими [13]. ГПВЧ є криптографічно сильним, якщо послідовність, яку він генерує з короткого таємного вихідного ключа, є майже такою самою, як і справжня випадкова послідовність і ніяке практично легко здійснюване обчислення не може дозволити криптоаналітику отримати яку-небудь інформацію про відкритий текст при перехопленні ним шифротексту (за виключенням хіба що дуже малої ймовірності). Для застосування в криптографічних системах ГПВЧ повинні відповідати наступним вимогам:

- послідовність, що генерується повинна мати максимально великий період;
- послідовність, що генерується не повинна мати схованих періодичностей;
- послідовність, що генерується повинна мати різномірний спектр.

Питанню проектування надійних і якісних ГПВЧ часто не надають належної уваги. Сама система шифрування може бути виконана на дуже високому рівні, але якщо криптографічний ГПВЧ видає ключі, які легко вгадати, то всі інші бар'єри захисту долаються без особливих зусиль. В ряді продуктів використовуються ГПВЧ, що продукують ключі, в яких відслідковується певна закономірність. В таких випадках про

безпеку говорити не варто. Цікавим є те, що використання одного і того ж генератора в деяких областях забезпечує необхідну степінь захисту, а в інших – ні. Таким чином, необхідно підкреслити важливість криптографічного ГПВЧ – якщо він розроблений погано, то він легко може стати самим вразливим елементом системи.

Найважливішою характеристикою ГПВЧ є довжина періоду повторення, після якого випадкові числа, на виході ГПВЧ почнуть повторюватися. Другою за важливістю характеристикою ГПВЧ є його продуктивність, тобто кількість чисел, які генеруються за одиницю часу. Для окремих прикладних програм (статистичне зондування, моделювання в реальному часі і т.д.) може бути потрібною продуктивністю порядку $10^{10} - 10^{12}$ випадкових чисел за секунду.

В загальнбму випадку, як було сказано вище, ГПВЧ можна поділити на дві основні групи за способом їх реалізації:

1. ГПВЧ реалізовані програмно;
2. ГПВЧ реалізовані апаратно.

Хоча такий поділ ГПВЧ є досить умовним, оскільки більшість генераторів можуть бути реалізовані як програмно, так і апаратно. Це також залежить від того, де саме буде використовуватися той чи інший ГПВЧ. Наприклад, при розробці комп'ютерних ігор доцільним є використання програмних ГПВЧ, а, наприклад, у вимірювальній техніці застосовують апаратно реалізовані ГПВЧ.

Винайти якісний ГПВЧ не так вже й легко. Вчені показали, що добру послідовність псевдовипадкових чисел неможливо виробляти за допомогою випадково вибраного алгоритму. Потрібна певна теорія.

Розробкою ефективних методів для створення надійних і якісних ГПВЧ займається багато вчених. На сьогоднішній день, на основі математичних та експериментальних досліджень, було розроблено ряд методів побудови ГПВЧ [3], [10], [11], [16], які відрізняються один від одного оперативністю, доступністю, періодом випадкової послідовності, іншими характеристиками. Найбільш поширеними є наступні методи:

1. Лінійний конгруентний метод;
2. Метод середини квадратів;
3. Дробові ГПВЧ;
4. Генератор М – послідовностей;
5. ГПВЧ побудовані на основі різних математичних алгоритмів.

В залежності від сфери застосування кожен із вище вказаних методів має свої переваги і недоліки.

Головна перевага лінійних конгруентних генераторів в тому, що вони швидко працюють і потребують мало операцій на біт послідовності. Самий великий недолік – передбачуваність таких послідовностей. Варто відмітити, що лінійні конгруентні генератори продовжують широко використовуватися для не криптографічних прикладних задач, таких, як симулювання випадкової поведінки. Такі послідовності ефективно генеруються і демонструють добрі статистичні властивості при дослідженні більшістю емпіричних тестів.

Недолік методу середини квадратів полягає в тому, що послідовності, які видають генератори побудовані на основі цього методу мають тенденцію перетворюватися в короткі цикли елементів, які повторюються. Наприклад, якщо який-небудь член послідовності виявиться рівним нулю, то всі наступні члени також будуть нулями.

Дробові ГПВЧ також не знайшли широкого застосування. Результати їх роботи, на сьогоднішній день, є далекі від практичного використання. Оскільки для представлення ірраціональних чисел в пам'яті комп'ютера необхідна нескінченна кількість розрядів, що є нездійсненним, а у випадку використання раціональних чисел дуже великою є ймовірність отримання циклів з малими періодами. Крім того, для даного класу ГПВЧ неможливо дати

математичне обґрунтування нижньої границі періоду повторення послідовності, тому що вона сильно залежить від вихідних чисел.

До переваг генераторів М-послідовностей можна віднести просту їх, як програмну, так і апаратну реалізацію, а також рівноймовірність випадкових величин, які генеруються. Але даний тип генераторів не задовольняють вимогу щодо непередбачуваності чисел, які послідовно генеруються. На практиці для усунення цього недоліку вихід лінійних послідовних машин додатково обробляється хеш-функцією або кодується DES алгоритмом.

Часто потребують випадкові величини, які згенеровані не лише за рівномірним розподілом, але й за деякими іншими, тому ГПВЧ можна також класифікувати за законом розподілу:

- F-розподіл;
- бета-розподіл;
- біноміальний розподіл;
- розподіл Вейбула;
- гамма-розподіл;
- геометричний розподіл;
- дискретний рівномірний розподіл;
- експоненційний розподіл;
- розподіл Ерланга;
- розподіл Коші;
- логістичний розподіл;
- логнормальний розподіл;
- нормальний розподіл;
- від'ємний біноміальний розподіл;
- розподіл Паскаля;
- розподіл Пуассона;
- степеневий розподіл;
- розподіл Стюдента;
- розподіл хі-квадрат.

Апаратні ГВЧ є недетерміновані – ніякий алгоритм не може використовуватися, щоб визначити послідовність бітів. Таким чином, апаратні ГВЧ є нечуттєвими до вторгнення або впливу алгоритму демонтування або виявлення. Властивість недетермінізму має особливо важливе значення у специфічних прикладних програмах генерування випадкових чисел, таких як деякі методи наукового і фінансового моделювання, лотерей, які підтримуються урядом, а також для різноманітних технологій безпеки комп'ютера, таких як криптографія і цифровий підпис [2].

Апаратні ГВЧ звільняють користувача від необхідності вибору початкового значення. Це робить процес генерації випадкового значення високо ефективним, а якість початкового значення не залежить від навичок програміста [17].

Апаратні ГВЧ є особливо важливими коли сервер, такий як Web-сервер або файловий сервер, повинні виконувати шифрування.

В свою чергу апаратні генератори можуть бути комбінованими, тобто вони можуть крім певних фізичних явищ використовувати і певні математичні алгоритми для обробки цих фізичних явищ. Наприклад, деякі прикладні програми або Web сервер, які використовують апаратний ГВЧ, потребують безперервний доступ до ГВЧ, який може їх сповільняти. Тому спочатку вони за допомогою апаратного ГВЧ отримують певне початкове значення, а потім використовують ГПВЧ для створення багатьох ключів високої ефективності. Навіть якщо апаратний ГВЧ стає недоступним з деяких причин, ГПВЧ може продовжувати створювати ключі маючи лише це початкове значення.

Апаратні ГВЧ від Intel, поєднані з програмним забезпеченням RSA Data Security, забезпечують недорогий розповсюджений, автоматизований і добре налагоджений процес для генерації початкового матеріалу. Крім цього створений початковий матеріал є дійсно випадковим [17].

Розглянемо переваги апаратного ГВЧ:

• Недорогий: великомасштабне виробництво знижує затрати.

• Автоматизований: людина, яка створює ключі, надає перевагу апаратній генерації випадкового числа оскільки це більш зручно і автоматизована процедура є більш безпечна.

• Випадковість: створення початкових значень, використовуючи такі часткові методи отримання випадковості, як переміщення мишки або натискання користувачем клавіш, є не таким випадковим, як випадкові числа створені апаратними ГВЧ. Вихідна послідовність апаратного ГВЧ є дійсно випадковою.

• Добра налагодженість: ГПВЧ, які комбідовані з апаратними ГВЧ є більш простіші і мають більшу швидкодію. З точки зору розробників перевагою таких ГПВЧ є їх полегшене програмування, а з точки зору користувачів, перевага полягає в тому що ГПВЧ працюють більш ефективно.

Як було сказано вище основна задача при генеруванні псевдовипадкових чисел полягає в отриманні послідовностей, які подібні на випадкові. Великий період послідовності ще зовсім не означає, що вона добра для роботи.

Як можна охарактеризувати якість ГПВЧ? Зрозуміло, що алгоритм повинен бути швидким, мати великий період повторення і графік автокореляційної функції в ідеалі повинен наближатися до прямої лінії. Головна думка всього сказаного полягає в тому, що ми не можемо довірити собі в суб'єктивній оцінці, випадкова чи ні дана послідовність чисел. Необхідно використовувати які-небудь неупереджені тести. Існує багато методів для тестування псевдовипадкових послідовностей.

Якщо послідовність веде себе добре відносно тестів T_1, T_2,..., T_n, то ми не можемо бути впевнені у тому, що вона витримає і наступний T_{n+1} тест.

Розрізняють наступні види тестів:

- Емпіричні тести;
- Теоретичні тести;
- Прикладні тести.

Емпіричні тести – це коли машина маніпулює з групами чисел послідовності і виконує оцінку за допомогою визначених статистичних критеріїв.

Теоретичні тести є подібними до емпіричних тестів, але оцінка якості ГПВЧ відбувається на основі абстрактних статистичних властивостей.

Прикладні тести прямо перевіряють придатність алгоритму для особливих прикладних програм. Вони завжди покладаються на існування відомих результатів, які можуть бути обчислені аналітично.

Є багато статистичних властивостей істинних випадкових чисел. В принципі кожна з цих властивостей може бути використана як базис емпіричного або теоретичного тесту.

До найважливіших статистичних властивостей можна віднести однорідність і кореляцію.

Однорідність – це статистична властивість, яка полягає в тому, що кожне число випадкової послідовності повинно траплятися рівне число раз за цикл. Досить ефективним методом для перевірки псевдовипадкових послідовностей є використання автокореляційної функції, яка використовується для перевірки відсутності залежності наступних чисел від попередніх. Для цього використовують спеціальні кореляційні аналізатори.

Але, при тестуванні ГПВЧ, не можна довіряти результатам лише якогось одного тесту. Питання про необхідність достатньо великого набору тестів не раз піднімалося у літературі. Бажано використовувати декілька тестів для оцінки якості ГПВЧ і потім на основі результатів, отриманих в результаті тестування робити певний висновок про придатність чи непридатність того, чи іншого ГПВЧ.

Підсумовуючи вище сказане, можна зробити висновок, що, на сьогоднішній день, ГПВЧ є поширеними і мають надзвичайно важливе значення. Тому їх дослідження і удосконалення з використанням сучасних технологічних можливостей, наприклад, з використанням сучасних програмованих логічних інтегральних схем, є безумовно актуальною задачею. Також не менш важливою задачею є проведення порівняльного аналізу характеристик ГПВЧ і розроблення рекомендацій стосовно використання того чи іншого типу генераторів для конкретного використання.

Список литературы

1. *Анин Б.Ю.* Защита компьютерной информации. – СПб.: БХВ-Петербург, 2000. – 384 с.: ил.

2. Random Numbers in Data Security Systems. Intel Random Number Generator. *Scott Durrant*. Intel Corporation 1999.

3. *Оберман Р.М.М.* Счет и счетчики: Пер. с англ. – М.: Радио и связь, 1984. – 176 с., ил.

4. *Левченко В.Ф.* Модели в теории биологической эволюции Автореферат диссертации на соискание ученой степени доктора биологических наук в форме научного доклада Санкт-Петербург 1998.

5. Characterization of a Pseudo-Random Testing Technique for Analog and Mixed-Signal Bult-In-Self-Test. *Jan Arlid Tofte, Chee-Kian Ong, Juin-Lang Huang, Kwang-Ting (Tim) Cheng*. Department of Electrical and Computer Engineering, Univ. Of California, Santa Barbara, CA, US.

6. Experimental Modal Analysis. *Brian J.Schwarz & Mark H. Richardson,* Vibrant Technology, Inc. Jamestown, California 95327, October, 1999.

7. Mixed-Signal Testing of Integreted Analog Circuits and Electronic Modules. A Dissertation Presented to the Faculty of the Fritz J. and Dolores H.Russ College of Engineering and technology Ohio University In partial Fulfillment of the Requirement for the Degree Doctor of Philosophy by *Zhi-Hong Liu*, March 20, 1999.

8. Products of Random Matrices in Control and Signal Processing. *Jelel EZZINE*. ACS, ENIT, Campus Universitaire, BP 37 Le Belvedere, Tunis, TUNISIA.

9. Spherical Pseudo-Random Pattern Testing. *Malgorzata Marek-Sadowska*. Electrical and Computer Engineering Department University of California, Santa Barbara, CA 93106. Final Report 1997-98 for MICRO Project 97-109.

10. *Гундарь К.Ю., Гундарь А.Ю., Яншевский Д.А.,* Защита информации в компьютерных системах – К.: "Корнейчук", 2000. – 152с., ил.

11. *Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – 2-е изд., перераб. И доп. – М.: Радио и связь, 2001. – 376 с.: ил.

12. Bluetooth Security. *Juha T. Vainio*, Department of Computer Science and Engineering Helsinki University of Technology, 2000.

13. Cryptanalytic Attacks on Pseudorandom Number Generators. *John Kelsey, Bruce Schneier, David Wagner, Chris Hall*. Fast Software Encryption, Fifth International Workshop Proceedings (March 1998), Springer-Verlag, 1998, pp. 168-188.

14. *M.Blum, S.Micali*. How to generate cryptographically strong sequences of pseudo-random bits// SIAM J. Comput., vol.13, no.4, 1984, pp.850-864.

15. Randomness Recommendations for Security. *D.Eastlake*, 3rd DEC *S.Crocker* Cybercash, *J.Schiller* MIT, December 1994.

16. *Кнут Д.* Искусство программирования для ЭВМ: В 3-х т. Получисленные алгоритмы. Пер. с англ. – М.: Мир, 1977. – Т.2. – 724 с.

17. Hardware-based Random Number Generation, An RSA Data Security While Paper, RSA Data Security, Inc, 1999.

Надійшла 4.02.2003р.

УДК 681.324

Коженевский Р.С.

МЕТОДЫ ГАРАНТИРОВАННОГО УНИЧТОЖЕНИЯ ДАННЫХ НА НАКОПИТЕЛЯХ НА ЖЕСТКИХ МАГНИТНЫХ ДИСКАХ

За последние несколько десятилетий компьютерные информационные технологии прочно вошли в нашу жизнь и стали составной частью документооборота. Первоначально отработанные механизмы обеспечения информационной безопасности для новых компьютерных систем уже не подходят, и требуют существенной модернизации. В первую очередь это касается отношения к информации, хранящейся на накопителях на жестких магнитных дисках (НЖМД).

Ранее для снятия информации с НЖМД был необходим физический доступ к носителю. Появление же компьютерных сетей создало новые угрозы безопасности информации, так как позволяет дистанционно, а иногда и скрыто от пользователя, получить доступ к хранимой на компьютере информации.

В настоящее время на развитие индустрии защиты информации (ЗИ), тратятся миллионы долларов. А по сути дела, решается одна задача – сделать открытую информацию доступной всем пользователям, а конфиденциальную – доступной только тому, кому она предназначается. Как в сфере бизнеса, так и в сфере государственного управления, уже скопились значительные объемы конфиденциальной информации, хранящиеся в базах данных персональных компьютеров (ПК). Эта информация представляет собой реальную ценность, а утечка ее в ряде случаев способна влиять даже на государственную безопасность.

Данное обстоятельство дало мощный толчок к развитию всевозможных программных и аппаратных средств добывания информации из ПК и компьютерных сетей. Особенно уязвимыми оказались сети, имеющие прямой выход в интернет.

Пути или каналы утечки информации, позволяющие несанкционированно и безнаказанно снимать копии с информации, непосредственно связаны с технологиями обработки, передачи и утилизации информации, хранящейся на НЖМД [1].

Утечка информации при замене НЖМД

Быстрое устаревание компьютерных технологий это уже установившееся явление. Каждые два года (по закону Мура) ПК удваивают свою мощность. После смены двух поколений ПК не представляет собой никакой ценности и его нецелесообразно поддерживать технически и программно. Как правило, персональные компьютеры окупаются за 4 года, а это означает, что ИТ-компании должны заменять 25%