УДК 004.056.55

В.М. Рудницький, д.т.н.
Е.В. Фауре, к.т.н
С.В. Сисоєнко

ОЦІНКА ЯКОСТІ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ ДОДАВАННЯ ЗА МОДУЛЕМ

Черкаський державний технологічний університет, м. Черкаси,
e-mail: rvn_2008@ukr.net, faureemil@gmail.com, sysoenko@mail.ru

У роботі розглянуто питання якості псевдовипадкових послідовностей чисел. Запропоновано кількісний показник оцінки якості побудови псевдовипадкових послідовностей на основі додавання за модулем M результатів Q операцій криптографічного перетворення інформації, який, крім імовірності виродженої результуючої операції, враховує час формування послідовності. За цим показником виконано дослідження побудованих послідовностей, визначено конфігурації перетворення, які дозволяють отримати найбільший коефіцієнт якості.

Ключові слова: *псевдовипадкова послідовність, операції додавання за модулем, виродженість результатів операцій, криптографічне перетворення.*

Вступ

Безпека інформації під час її зберігання, обробки та передавання є однією з основних задач, що постають перед розробниками телекомунікаційних систем і мереж. Постійна протидія систем захисту інформації та методів їх злому разом із розвитком апаратної та алгоритмічної бази для проведення криптоаналізу визначають необхідність і стимулюють розвиток методів і засобів підвищення ефективності криптографічного перетворення інформації.

Аналіз останніх досліджень та публікацій

У роботах [1-3] доведено ефективність комбінаційного генератора псевдовипадкових чисел, що використовує операцію додавання за модулем M декількох первинних псевдовипадкових послідовностей. У роботах [4, 5] цей підхід розширено і доведено можливість підвищення стійкості криптографічних систем за рахунок використання випадкових дворозрядних операцій криптографічного перетворення інформаційної послідовності замість первинних генераторів. Так, у роботі [4] використано процедуру додавання за модулем два результатів двох випадкових невироджених операцій криптографічного перетворення інформації. У роботі [5] виконано дослідження сумісного виконання трьох, чотирьох і п’яти випадкових операцій криптографічного перетворення інформації з подальшим додаванням отриманих результатів за модулем два та чотири. Разом із тим, у роботах [4, 5] встановлено тільки ймовірність виродженої результуючої операції, за якою визначено найкращі конфігурації перетворення. Як і в [5], під виродженою операцією будемо розуміти результуючу операцію, для якої не існує оберненої операції криптографічного перетворення.

Постановка задачі

Метою цієї роботи є розробка кількісного показника оцінки якості побудови псевдовипадкових послідовностей на основі додавання за модулем M результатів Q операцій криптографічного перетворення інформації, який, крім імовірності виродженої результуючої операції, враховує час формування послідовності; а також обчислення розробленого показника для побудови псевдовипадкових послідовностей при $M \in \{2;4\}$ і $Q \in \{2;3;4;5\}$.

Вирішення поставленої задачі

Проведемо аналіз імовірностей вироджених і невироджених результуючих операцій перетворення інформації в залежності від кількості первинних операцій криптографічного перетворення інформації, а також часу отримання результуючої псевдовипадкової послідовності.

Для цього введемо наступні позначення:

$P_{bo}(M,Q)$ – імовірність виродженої операції під час побудови псевдовипадкової послідовності на основі додавання за модулем M результатів Q операцій криптографічного перетворення;

$P_{bo}(M,Q)=1-P_{nbo}(M,Q)$ – імовірність невиродженої операції;

$t_{pp}(Q)$ – час побудови псевдовипадкової послідовності, який визначається таким чином:

$$t_{pp}(Q)=t_{po}(Q)+t_{+o}(Q), \tag{1}$$

де $t_{po}(Q)$ – час виконання Q операцій криптографічного перетворення;

$t_{+o}(Q)$ – час виконання операцій додавання за модулем M під час побудови результуючої псевдовипадкової послідовності.

Якщо допустити, що час, необхідний для кожного з Q перетворень, однаковий і дорівнює t_{po1}, то час побудови псевдовипадкової послідовності

$$t_{pp}(Q)=t_{po}(Q)+t_{+o}(Q)=Q\cdot t_{p1}+(Q-1)\cdot t_{+}, \tag{2}$$

де t_{+} – час виконання операції додавання за модулем M.

Відносний коефіцієнт якості псевдовипадкової послідовності на основі додавання за модулем M результатів Q операцій криптографічного перетворення інформації будемо визначати наступним чином:

$$k_{kv}(M,Q)=\frac{P_{bo}(M,Q)}{P_{bo}(M,2)}. \tag{3}$$

Відносний коефіцієнт часу формування псевдовипадкової послідовності на основі додавання за модулем M результатів Q операцій криптографічного перетворення інформації будемо визначати наступним чином:

$$k_{tv}(M,Q)=\frac{t_{pp}(Q)}{t_{pp}(2)}=\frac{Q\cdot t_{po1}+(Q-1)\cdot t_{+}}{2t_{po1}+t_{+}}. \tag{4}$$

Оскільки збільшення коефіцієнта $k_{kv}(M,Q)$ призводить до покращення статистичних характеристик псевдовипадкової послідовності, а збільшення коефіцієнта $k_{tv}(M,Q)$ призводить до збільшення латентності та часу очікування формування послідовності, відносний коефіцієнт якості побудови псевдовипадкової послідовності $k_{pkp}(M,Q)$ будемо визначати наступним чином:

$$k_{pkpv}(M,Q)=\frac{k_{kv}(M,Q)}{k_{tv}(M,Q)}. \tag{5}$$

З урахуванням виразів (2) і (4) вираз (5) можна представити у вигляді

$$k_{pkpv}(M,Q)=\frac{P_{bo}(M,Q)\cdot(2t_{po1}+t_{+})}{P_{bo}(M,2)\cdot(Qt_{po1}+(Q-1)\cdot t_{+})}. \tag{6}$$

Ураховуючи те, що пристрої цифрової обробки інформації, як правило, працюють синхронно і час їх роботи визначається максимальним часом виконання операції, то максимальний час виконання операції криптографічного перетворення можна представити як час виконання двох операцій додавання за модулем M. Виходячи з цього, вираз (6) можна спростити:

$$k_{pkpv}(M,Q)=\frac{P_{bo}(M,Q)\cdot(4t_{+}+t_{+})}{P_{bo}(M,2)\cdot(2Qt_{+}+(Q-1)\cdot t_{+})}=\frac{5P_{bo}(M,Q)}{(3Q-1)\cdot P_{bo}(M,2)}. \quad (7)$$

На основі отриманої залежності (7) проведемо розрахунки відносного коефіцієнта якості побудови псевдовипадкової послідовності у випадку використання двох, трьох, чотирьох та п'яти операцій криптографічного перетворення інформації з подальшим їх додаванням за модулем два та чотири.

Гістограма залежності відносного коефіцієнта якості побудови псевдовипадкової послідовності $k_{pkpv}(M,Q)$ від кількості операцій криптографічного перетворення інформації, які використані під час побудови результуючої псевдовипадкової послідовності на основі додавання за модулем два, представлено на рис. 1.

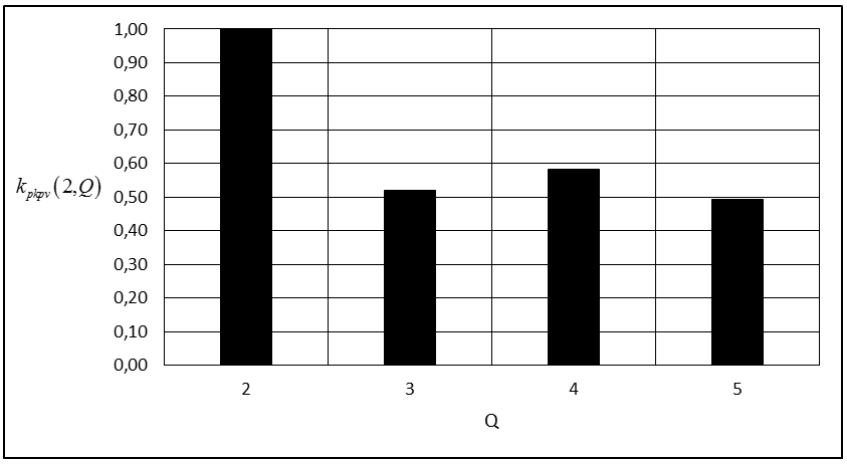

Рис. 1. Гістограма залежності відносного коефіцієнта якості побудови псевдовипадкової послідовності від кількості операцій криптографічного перетворення інформації під час використання додавання за модулем 2

Гістограма залежності відносного коефіцієнта якості побудови псевдовипадкової послідовності $k_{pkpv}(M,Q)$ від кількості операцій криптографічного перетворення інформації, які використані під час побудови результуючої псевдовипадкової послідовності на основі додавання за модулем чотири, представлено на рис. 2.

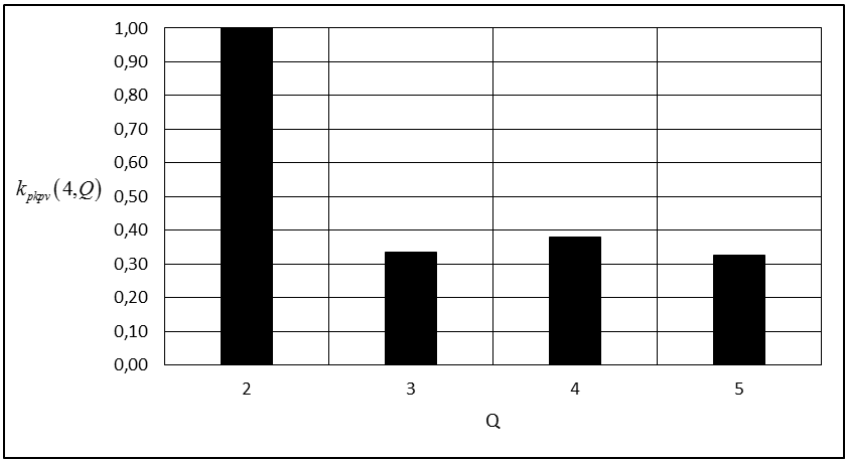

Рис. 2. Гістограма залежності відносного коефіцієнта якості побудови псевдовипадкової послідовності від кількості операцій криптографічного перетворення інформації під час використання додавання за модулем 4

Аналіз представлених гістограм свідчить про те, що за визначених умов відносний коефіцієнт якості побудови псевдовипадкової послідовності досягає максимального значення для Q=2 операцій криптографічного перетворення інформації. Разом із тим, варто зауважити, що для $M\epsilon\{2;4\}$ і $Q\epsilon\{3;4;5\}$ відносний коефіцієнт якості побудови псевдовипадкової послідовності досягає максимального значення для Q=2.

Висновки

У результаті проведеного дослідження встановлено, що показник якості побудови псевдовипадкової послідовності чисел на основі криптографічного перетворення вхідної інформації послідовно $Q \geq 2$ операціями криптоперетворення з наступним додаванням результатів за модулем M відрізняється для різних параметрів побудови. Отримані значення відносного коефіцієнта якості побудови псевдовипадкової послідовності в залежності від M і Q свідчать про те, що для $M\epsilon\{2;4\}$ і $Q\epsilon\{2;3;4;5\}$ за цим показником є найкращими наступні конфігурації перетворення: для M=2 – Q=2 (найгірша – Q=5); для M=4 – Q=2 (найгірша – Q=5).

Список літературних джерел

1. Лавданский А.А. Комбинационный метод формирования последовательности псевдослучайных чисел / А.А. Лавданский, Э.В. Фауре // Системний аналіз та інформаційні технології: матеріали 16-ї Міжнародної науково-технічної конференції SAIT-2014, Київ, 26-30 травня 2014р. / ННК «ІПСА» НТУУ «КПІ». – К.: ННК «ІПСА» НТУУ «КПІ», 2014. – С. 403-404. – Режим доступу: http://sait.kpi.ua/books/sait2014.ebook.pdf/view.
2. Фауре Э.В. Оценка статистических характеристик последовательности псевдослучайных чисел, порожденной комбинационным генератором / Э. В. Фауре, А. И. Щерба, А. А. Лавданский // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – 2015. – № 18. – С. 165-171.
3. Фауре Э.В. Анализ корреляционных свойств последовательностей (псевдо) случайных чисел / Э.В. Фауре, А.И. Щерба, А.А. Лавданский // Наука і техніка Повітряних Сил Збройних Сил України. – 2015. – №1(18) – С. 142-150. – Режим доступу: http://nbuv.gov.ua/j-pdf/Nitps_2015_1_32.pdf.
4. Ланських Є.В. Оцінка якості псевдовипадкових послідовностей на основі використання операцій додавання за модулем два / Є.В. Ланських, С.В. Сисоєнко, М.О. Пустовіт // Наука і техніка Повітряних Сил Збройних Сил України. – 2015. – №4(21) – С. 147-150. – Режим доступу: http://nbuv.gov.ua/UJRN/Nitps_2015_4_36.
5. Фауре Е.В. Синтез і аналіз псевдовипадкових послідовностей на основі операцій криптографічного перетворення / Е.В. Фауре, С.В. Сисоєнко, Т.В. Миронюк // Системи управління, навігації та зв'язку. – 2015. – №4(36) – С. 130-133.