УДК 621.3.06

Ю.І. ГОРБЕНКО, канд. техн. наук, Д.Е. ХРЯПІН, В.І БОНДАРЕНКО

АНАЛІЗ ВИМОГ ДО ГЕНЕРАТОРІВ ВИПАДКОВИХ І ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ, ВСТАНОВЛЕНИХ В СТАНДАРТАХ AIS 20 ТА AIS 31

Вступ

У зв'язку з розвитком інформаційно-телекомунікаційних систем усе більше актуальними стають задачі побудови надійних систем обробки інформації з функціями криптографічного захисту інформації. Один з найважливіших елементів цих систем, з точки зору забезпечення високого рівня захищеності, є засоби генерації ключів та параметрів. На сучасному етапі засоби генерації ключів будуються на основі генераторів випадкових послідовностей(ГВП) (недетермінованих) та псевдовипадкових (детермінованих) послідовностей (ПВП). Вони майже завжди входять до складу криптографічних засобів, прикладом їх використання є генерація ключів, загальносистемних параметрів, випадкових чисел, які використовуються для забезпечення захисту від повторної передачі повідомлень, при виконанні різноманітних протоколів, тощо. Саме тому аналіз та розробка засобів оцінки властивостей генераторів випадкових послідовностей є дуже актуальним та важливим напрямком досліджень.

Задача оцінки ГВП виникла у зв'язку з необхідністю використання при розробці технічних рішень спеціальних методів оцінки, які базуються на ряді керівних принципів. Аналіз показав, що для вирішення цих задач у Німеччині прийняті нормативні документи відповідно для оцінки ПВП застосовується AIS 20 [1], а для ГВП AIS 31 [2]. При їх розробці були враховані основні положення й досвід застосування федеральних стандартів США FIPS 140-1 [3] і FIPS 140-2 [4]. Обидва ці документи містять критерії для оцінки детермінованих генераторів випадкових послідовностей (ДГВП). Основна ідея полягає в тому, що придатність ДГВП повинна бути оцінена з урахуванням криптографічних засобів, у яких вони використовуються.

Метою даної статті є аналіз основних положень AIS 20 і AIS 31 та визначення можливостей їх застосування в Україні при розробці ДГВП.

1. Аналіз загальних положень AIS 20

В AIS 20 визначені вимоги до ДГВП. Такий генератор генерує псевдо випадкові числа, які залежать виключно від ініціюючого внутрішнього стану. Логічна структура генератора й процес вибору початкового числа визначаються п'ятьма параметрами (S, R, φ, ψ, p_A). Ці параметри мають такі визначення (табл.1):

Таблиця 1

Параметри	Визначення параметрів
S	кінцева множина можливих внутрішніх станів ГВП
R	множина можливих вихідних значень (випадкові числа)
φ	функція стану
ψ	функція виходу
p_A	імовірнісна міра, що описує розподіл випадкової величини, яка використовується як початкове значення

На кроці $n > 1$ внутрішній стан спочатку модифікується за допомогою використання виразу $s_n := \varphi(s_{n-1}) \in S$, після цього випадкове число $r_n := \psi(s_n)$ розраховується та подається на вхід перетворення.

Оскільки різні криптографічні системи висувають різні вимоги до випадкових чисел, то необхідно оцінювати відповідність конкретної системи до вимог, які встановлені для систем цього класу. Саме такий підхід було реалізовано в AIS 20. В цьому нормативному документі представлено чотири ієрархічних функціональних класи. Кожен наступний клас містить

більш високий рівень вимог до вихідних послідовностей, а саме він включає в себе усі вимоги попереднього класу і додає нові вимого до ДГВП. Ці класи також впорядковані в залежності від вимог до криптосистем, в яких ДГВП буде використовуватися.

1.1. Вимоги до ДГВП класу К1

К1 (i) вимагає щоб ймовірність того, що вектори $(r_1,\ldots,r_c),(r_{c+1},\ldots,r_{2c}),\ldots,(r_{M-c+1},\ldots r_M)$ попарно різні, повинна бути, принаймні, $1-\varepsilon$

Якщо $\varepsilon = 0$, то стійкість механізму визначається як " висока ".

В інших випадках застосовуються наступні умови:

- $M^2/c^2\varepsilon > 2^{52}$ та $\varepsilon < 2^{-16}$: стійкість механізму " висока ";
- $M^2/c^2\varepsilon > 2^{32}$ та $\varepsilon < 2^{-12}$: стійкість механізму " середня ";
- $M^2/c^2\varepsilon > 2^{20}$: стійкість механізму " низька ".

Вибір параметрів c, ε та M залежить від призначення криптографічної системи. Прикладом систем, в яких застосовується ДГВП такого класу, можуть бути будь які інтерактивні протоколи.

1.2. Вимоги до ДГВП класу К2

ДГВП повинен задовольняти вимозі К1 (i). А також К2 (ii), яка вимагає, щоб випадкові числа, які генеровані ДГВП, мали статистичні властивості такі, як і випадкові числа, які генеровані ідеальним ГВП.

К2 (ii) – послідовності випадкових чисел r1, r2, ... та їх бітові представлення повинні задовольняти статистичним тестам Т1 – Т5, які наведені в додатках до AIS 20. Якщо ДГВП проходить всі індивідуальні тести, тоді підтверджується, що ДГВП задовольняє вимозі К2 (ii). Якщо більш ніж один індивідуальний тест не пройдений, то вважають, що ДГВБ не задовольняє вимозі К2 (ii).

Якщо тільки один тест не пройдений, то весь порядок тестування повинен бути повторений, і якщо на цей раз ДГВП проходить всі тести, то підтверджується, що він задовольняє вимозі К2 (ii). Друге повторення тестування не дозволяється.

Метою застосування класу К2 є виключення кореляційних атак на криптографічні алгоритми, що засновані на використанні статистично слабких випадкових чисел (випадкових ключів).

Прикладом криптографічних систем з ДГВП класу К2 є потокові шифри.

1.3. Вимоги до ДГВП класу К3

ДГВП повинен задовольняти вимогам К1 (i) та К2 (ii). Крім того висуваються нові вимоги К3 (iii) та К3 (iv), які полягають в тому, що:

К3 (iii) Якщо стійкість механізму "висока", то $H(p) \geq 80$; для "середньої" стійкості механізму – $H(p) \geq 48$. Ентропія p_A обчислюється як: $H(p) = -\sum_{s \in S} p_A(s)\log_2(p_A(s))$.

К3 (iv) Повинне бути фактично неможливо обчислити або вгадати попереднє r_{i-1} або наступне r_{i+j+1} з відомої підпослідовності $r_i, r_{i+1},\ldots,r_{i+j}$, $(i + j \leq M)$, а також обчислити або вгадати внутрішній стан. Потенціал передбачуваних атак супротивника залежить від стійкості механізму. Навіть при використанні сучасних передових знань імовірність атаки (реалізована прийнятним частковим методом перебору) може бути незначно більше чим, якби підпослідовність була би невідомою. Передбачається, що супротивник знає параметри (S, R, φ, ψ, p_A), однак він не знає ніяких внутрішніх станів $s_0, s_1,\ldots,s_M$.

Метою К3 є захист проти відновлення попередніх випадкових чисел і вгадування наступних з відомої підпослідовності.

Можливі криптографічні системи, в яких можуть використовуватися ДГВП К3:

1. генерація ключів;
2. генерація підпису DSS (секретний ключ x або випадкове число k);
3. генерація паролів.

1.4. Вимоги до ДГВП класу К4

ДГВП повинен задовольняти вимогам К1 (i), К2 (ii), К3 (iii), К3 (iv), та висувається нова вимога К4 (v), яка полягає в тому, що має бути фактично неможливо виробити попереднє випадкове число r_{i-1} знаючи внутрішній стан s_i . Потенціал передбачуваних атак супротивника залежить тут від стійкості механізму. Навіть використовуючи сучасні передові знання, імовірність атаки (реалізована прийнятним частковим методом перебору) може бути незначно більше чим, якби s_i було б не відомо. Передбачається, що супротивник знає параметри (S, R, φ, ψ, p_A).

Метою К4 є захист проти відновлення попередніх випадкових чисел з відомого внутрішнього стану.

ДГВП класу К4, можуть використовуватися в наступних криптографічних системах:

4. генерація ключів;
5. генерація підпису DSS (секретний ключ x або випадкове число k);
6. генерація сеансових ключів для симетричних криптографічних механізмів;
7. генерація паролів.

1.5. Аналіз класів К1 – К4 та вимог що вони встановлюють

Аналізуючи класи ДГВП можна зробити висновок, що класи є ієрархічно залежними, тобто кожен наступний повністю включає в себе попередній та доповнює своїми новими вимогами (табл. 2).

Таблиця 2

Функціональний клас	Вимоги до ДГВП	Криптографічні системи в яких застосовуються ДГВП такого класу
К1	К1(i)	Інтерактивні протоколи
К2	К1(i) + К2(ii)	Потокові шифри
К3	К1(i) + К2(ii) + К3(iii) + К3(iv)	Генерація ключів, генерація цифрового підпису DSS (секретний ключ x або випадкове число k), генерація паролів.
К4	К1(i) + К2(ii) + К3(iii) + К3(iv) + К4(v)	Генерація ключів, генерація цифрового підпису DSS (секретний ключ x або випадкове число k). генерація сеансових ключів для симетричних криптографічних механізмів, генерація паролів.

Вказані вимоги встановлюють всі рівні захищеності, як від найменшого (використання ДГВП як лічильника), так і найвищого (аналітик, навіть при знанні певних внутрішніх станів генератора, не може скомпрометувати усю послідовність). Методика тестування, що викладена в AIS 20, може застосовуватись як в реальному часі, так і в процесі досліджень, а також для технологічного тестування.

2. Аналіз загальних положень AIS 31

В AIS 31 представлені критерії оцінки криптографічних властивостей генераторів випадкових чисел. Оцінка фізичних генераторів випадкових послідовностей (ФГВП) ґрунтується в основному на статистичних тестах. На основі різних можливих сценаріїв атак можна розробити вимоги до властивостей зовнішніх і відповідно внутрішніх випадкових чисел. Беручи до уваги ці обставини в AIS 31 уведені 2 класи функціональності (P1, P2).

В AIS 31 враховані вимоги якісного перевіряння на випадковість та можливості оперативного тестування. Перевірка здійснюється на відповідність функціональним класам P1 та P2.

При перевірці на відповідність P1 використовуються тести, що були взяті в FIPS 140-1, але додатково введено авто кореляційний тест, що дозволяє перевірити кореляції між послідовністю та зсувом цієї ж послідовності.

При перевірці на відповідність до Р2 додатково використовуються три тести: тест перевірки рівномірного закону розподілу, порівняльний тест для поліноміальних розподілів та ентропійного тестування.

2.1. Вимоги до ДГВП класу Р1

Для відповідності класу Р1 повинні виконуватися вимоги Р.1 (i) – Р.1 (vi) в відповідності до механізмів та функцій стійкості.

Р.1 (i) вимагає, щоб послідовність випадкових векторів, створена з внутрішніх випадкових чисел (ВЧ) r1, r2, ... з великою ймовірністю являються попарно різними.

Для верифікації вимоги Р.1 (ii) внутрішня послідовність ВЧ r1, r2, ... та їх проекції на окремі біти повинні задовольняти статичним тестам Т1-Т5.

Для Р.1 (iii), якщо при увімкненні ДГВП відбувається загальна зупинка джерела шуму, то ця зупинка повинна бути автоматично розпізнана та після зупинки не можуть бути подані зовнішні ВЧ.

Для Р.1 (iv), якщо під час роботи ДГВП виникає загальна зупинка джерела шуму, то після зупинки припиняється виробка випадкових значень, що вироблюються внутрішньою випадковою послідовністю. В якості заміни достатньо, щоб після загальної зупинки джерела шуму ДГВП вів себе для кожної постійної послідовності сигналів шуму як К2-ДГВП AIS 20, вихідні послідовності якого відповідають передбаченій меті застосування.

Р.1 (v) вимоги в Р.1 (i) і Р.1 (ii) повинні бути перевірені при наперед визначених зовнішніх впливах, так як вони можуть впливати на функціонування джерела шуму.

Для Р.1 (vi) ДГВП повинен містити *online*-тест, котрий по зовнішньому виклику перевіряє якість внутрішніх ВЧ.

Після запуску апаратний генератор шуму починає виготовляти блоки необроблених випадкових байтів. Для негайного виявлення несправностей фізичного джерела шуму на старті повинні застосовуються повні статичні випробування (*online*-тест). Тільки в випадку успіху ФГВП доходить до стандартного режиму роботи і стає доступним елементом криптографічної системи. В стандартному режимі *online*-тест застосовується до кожного генерованого блоку випадкових байтів. Якщо тестування пройдене, ФГВП повернеться до робочого режиму. Інакше ФГВП буде заблоковано, і, відповідно, усі запити, що використовують ФГВП, будуть повернені з відповідним кодом помилки. Під час роботи кінцевого об'єкту оцінки повинне виконуватися неперервне тестування ФГВП для перевірки коректності його роботи.

Можливі застосування ФГВП Р1:

- відкриті, змінні вектори ініціалізації (сінхро послідовності):
- генерація начального стану для ДГВП класів К1 та К2 AIS 20.

2.2. Вимоги до ДГВП класу Р2

ДГВП повинен належати класу Р1 як мінімум з такими ж механізмами та функціями стійкості.

Р.2 (i) Перевірка властивостей Р1.

Р.2 (vii) Дискретизовані послідовності шумових сигналів (ДПШС), задовольняють певним критеріям, повинні проходить статичні тести, котрі крім усього іншого повинні виключати багатокрокові залежності. Крім того, повинне бути пройдене ентропійне тестування Т8.

Р.2 (viii) Додаткова математична обробка не повинна зменшувати ентропію на біт.

Р.2 (ix) При кожному включені ФГВП повинен бути достовірні мінімальні статистичні властивості ДПШС. До тих пір, доки не закінчиться статичне тестування, ВЧ не можуть бути видані.

Р.2 (x) Якщо під час роботи ФГВП відбувається загальна зупинка джерела шуму, повинна виключатися видача випадкових чисєл, так як відповідні внутрішні випадкові послідовності були сгенеровані після зупинки.

Р.2 (xi) В роботу ФГВП повинен бути імплементован *online*-тест, з допомогою якого може бути перевірено статистичну якість дискретизованної послідовності шумового сигналу. *Online*-тест повинен бути викликаний ззовні або ФГВП повинен сам викликати його. Після

повинне здійснюватися постійно або принаймні через регулярні проміжки. *Online*-тест повинен розрізнювати в узгоджений час незначні статистичні дефекти або погіршення статичних властивостей дискретизованної шумової послідовності.

P.2 (xii) Вимоги P.2 (vii) повинні бути перевірені для передбачених зовнішніх умов використання, так як вони можуть впливати на функціонування джерела шуму.

P.2 (xiii) ФГВП повинен сам викликати *online*-тест.

Можливі застосування ФГВП класу P2:

- ключі та параметри шифрування;
- випадкове заповнення;
- паролі.

2.3. Порівняння AIS 31 з іншими стандартами

Попередні дослідження та тестування підтвердили, що AIS 31 є надійною методикою тестування і по своїй ефективності забезпечує результати, що і NIST STS. Перевагою AIS 31 є те, що він забезпечує тестування в реальному часі. Методика, що визначена в AIS 31, може застосуватися як в реальному часі, так і в процесі досліджень, та для технологічного тестування. В AIS 31 враховані вимоги якісного перевіряння на випадковість та можливості оперативного тестування.

Аналіз показав, що AIS 31 базується на математично-технічній основі AIS 20. Що стосується застосування, то класи P1 і P2 відповідають класам K1-K2 і K3-K4 AIS 20.

3. Оцінка ДГВП заснованного на спарюванні точок елуптичної кривої та гешуванні згідно AIS 20

Відповідно до аналізу, що наведений в [5], указаний генератор задовольняє вимогам K1(i), K3(iii) та K3(iv). Вимога K2 (ii), яка полягає в тому, що послідовності r1, r2, ... та їх бітові представлення повинні задовольняти статистичним тестам T1 – T5, які наведені в додатках до AIS 20, буде виконуватися якщо в якості фінального перетворення використовувати геш функцію із ISO/IEC 10118-2. По суті, вказана вимога забезпечує властивість непередбачуваності. Вимога K4(v) полягає в тому, що аналітик, навіть маючи дані про внутрішній стан генератора, не може обчислити наступне або попереднє вихідне значення. Використовуючи модель випадкового оракулу можна довести, що якщо аналітик може визначити сусіднє вихідне значення генератору, то оракул, який він для цього застосовує, можна використати в якості засобу ефективного криптографічного аналізу при вирішенні задачі дискретного логарифму в групі точок еліптичної кривої.

Тому генератор, що заснований на спарювання точок еліптичної кривої, можна віднести до функціонального класу K4. Для порівняння, запропонований в стандарті США X9.98 [6] генератор також належить до класу K4, але оскільки він заснований лише на багаторазовому використанні алгоритмів гешування, то складність пошуку сусідніх вихідних значень генератора має лише поліноміальний характер, тобто цей генератор може застосовуватися лише в умовах використання досить великих (тому безпечних) загально системних параметрів.

Висновки

Прийняті в Німеччині нормативні документи AIS 20 та AIS 31 [2] враховують основні положення й досвід застосування федеральних стандартів США FIPS 140-1 [3] і FIPS 140-2 [4]. Нормативний документ AIS 20 містить критерії, що ефективно можуть застосовуватись для оцінки ДГВП.

Наведені в статті дані дозволяють зробити висновок про те, що усі чотири класи K1 – K4 є ієрархічно залежними, коли кожен наступний повністю включає в себе попередній та доповнює своїми новими вимогами.

В AIS 31 представлені критерії оцінки криптографічних властивостей генераторів випадкових чисел. Причому, оцінка фізичних генераторів випадкових послідовностей (ФГВП) грунтується в основному на статистичних тестах.

ДГВП, що заснований на спарювання точок еліптичної кривої, можна віднести до функціонального класу К4, тому він має перспективу застосування, в тому числі в Україні.

ДГВП, що запропонований в стандарті США X9.98 [6], теж належить до класу К4, але оскільки він заснований лише на багаторазовому використанні алгоритмів гешування, то складність пошуку сусідніх вихідних значень генератора має лише поліноміальний характер.

Список літератури: 1. *Application* Notes and Interpretation of the Scheme (AIS) 20. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 1999, 23 p. 2. *Application* Notes and Interpretation of the Scheme (AIS) 31. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 2001, 38 pages. 3. *Federal* Information Processing Standards Publication (FIPS PUB) 140-1. Security requirements for cryptographic modules. NIST, 1994, 48 pages. 4. *Federal* Information Processing Standards Publication (FIPS PUB) 140-2. Security requirements for cryptographic modules. NIST, 1999, 58 pages. 5. *Гриненко Т.А., Горбенко Ю.И., Орлова С.Ю.* Метод формирования и свойства ПВП на эллиптических кривых // Радиотехника. – 2001. – Вып.119. – С. 119-123. 6. *Стандарт* США X9.98-2010

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 12.08.2011