ДАТЧИКИ ВИПАДКОВИХ ЧИСЕЛ

Рогальов А.Г., студент, Нечитайло Ю.А., к.т.н.
(ДБТУ, м. Харків, Україна)

Random number sensors are described. Methods of generating random numbers are given. The fields of application of random number sensors are considered.

Датчики випадкових чисел є важливим елементом багатьох систем, що вимагають випадкових або псевдовипадкових чисел. Наприклад, криптографічні протоколи використовують випадкові числа для забезпечення безпеки, так як прогнозування послідовності випадкових чисел важко або неможливо. Моделювання складних процесів також вимагає випадкових чисел, щоб відтворити випадковість природних явищ.

Для створення випадкових чисел датчики використовують різні методи. Наприклад, деякі датчики використовують фізичні процеси, такі як шум електричних сигналів або квантові явища, щоб генерувати випадковість. Інші датчики використовують математичні алгоритми для створення псевдовипадкових чисел, які можуть бути використані у багатьох випадках, де випадковість не є критичною, але вимагається велика кількість випадкових чисел.

Один з найбільш відомих методів створення псевдовипадкових чисел - це лінійний конгруентний метод. Цей метод використовує формулу, яка генерує послідовність чисел, які виглядають як випадкові, але насправді є псевдовипадковими. Цей метод використовує початкове число, яке називається насінням (seed), та математичні операції для генерації наступних чисел у послідовності. Лінійний конгруентний метод - один із широко відомих методів генерації псевдовипадкових чисел. Застосовується у простих випадках і не має криптографічної стійкості. Входить до стандартних бібліотек різних компіляторів. Перевагою генераторів на основі цього методу є їхня швидкість за рахунок малої кількості операцій на біт.

Фізичні процеси, які використовуються для генерації випадкових чисел, можуть включати шум електричних сигналів, тепловий шум та радіоактивний розпад. Квантові датчики випадкових чисел використовують квантові явища, такі як суперпозицію та розбиття фотонів, щоб забезпечити випадковість. Ці методи забезпечують надійний рівень випадковості, оскільки їхні властивості не можуть бути передбачені.

Деякі датчики випадкових чисел також використовуються в іграх та інших додатках, щоб забезпечити випадковість подій. Наприклад, датчик випадкових чисел може використовуватись для визначення результуючої випадкової карти в грі, що забезпечує більш різноманітні та непередбачувані ігрові сценарії.

Насамкінець, слід зазначити, що датчики випадкових чисел не є абсолютно випадковими, оскільки вони генеруються за допомогою алгоритмів або фізичних процесів, які можуть бути передбачені та вивчені. Проте, вони забезпечують достатній рівень випадковості для більшості застосувань та дозволяють виконувати багато завдань, які потребують випадкових чисел.