ПЕРСПЕКТИВНИЙ ГЕНЕРАТОР ВИПАДКОВИХ БІТІВ НА ГЕШ-ФУНКЦІЯХ ТА ЙОГО ВЛАСТИВОСТІ

Шапочка Н.В.
Науковий керівник – д.т.н., проф. Горбенко І.Д.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Леніна,14, каф. БІТ, тел. (057) 7021425)

The requirements to pseudorandom bit generators are proved and determined. The technique is offered and the result of research of statistical characteristics random bit generator on hash function is resulted.

Проаналізовані існуючі генератори випадкових бітів (ГВБ) та визначені вимоги до них. Визначено, що одним з ГВБ, що відповідає даним вимогам, являється ГВБ, реалізований на геш-функціях. Пропонується методика та наводиться результат дослідження статистичних характеристик ГВБ на геш-функціях, реалізованого згідно ISO/IEC 18031.

Детермінований ГВЧ може бути побудований на базі геш-функції, що є необоротною або однобічною, і може використовувати любу затверджену геш-функцію. Детерміновані ГВЧ на базі геш-функції можуть використовуватися в криптографічних додатках, у яких вимагаються різноманітні рівні стійкості захисту за умови використання підходящої геш-функції й одержання достатньої ентропії для початкового числа.

В результаті тестування ГВБ на геш-функціях показує не гірші результати, ніж визнаний «класичний» генератор BBS. А це є доказом надійності схем генерації, що реалізовані на геш-функціях.

На рис. 1 наведено статистичний портрет ГВБ на геш-функціях, отриманий за допомогою методики NIST STS, рекомендованої Національним інститутом по стандартизації й технологіям США.

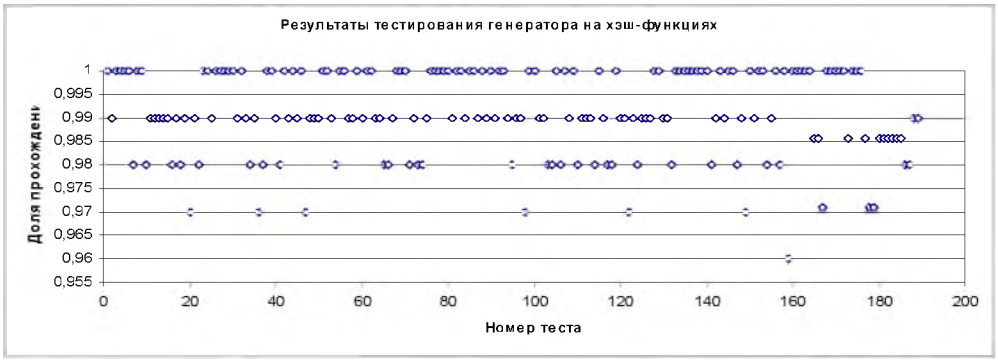

Рисунок 1 - Результати тестування ГВБ на геш-функціях

Тестування ГВБ, що базується на геш-функціях, підтвердило високий рівень випадковості формуємих ним послідовностей. ГВБ на геш-функціях володіє найнижчою вартістю, і, як наслідок, найвищою складністю. Даний генератор повністю задовольняє вимогам, які пред'являються до генераторів випадкових бітів.