ВИКОРИСТАННЯ ПОЛІНОМІВ ІЗ РОЗШИРЕНИХ ПОЛІВ ГАЛУА ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ШИФРУВАННЯ

Рисований О.М., Сухой Р.Д., Іванов В.Р.
Національний технічний університет "Харківський політехнічний інститут", м. Харків

Використання поліномів із розширених полів Галуа має широке значення в різних галузях - в криптографії, теорії кодових чисел, цифровій обробці сигналів й комп'ютерній алгебрі [1-2].

В роботі було проаналізовано вплив поліномів з GF(2) та поліномів кінцевого поля GF(3). В сучасний час багато елементів комп'ютерної техніки мають 3 стани: елементи пам'яті, шинні формувачі, контролери шин. Третій стан елементів поки що не контролюється в силу того, що відсутні окремі мікросхеми для такого контролю. А самостійний синтез таких елементів, хоча й не важкий, однак при цьому необхідно використовувати різні й багато інших логічних елементів.

Поліноми з поля GF(2) формують максимальний період генерації, що дорівнює $T - 2^n$, що для полінома при $n = 4$ мають $T = 16-1$, що дуже замало навіть для звичайного застосування. А з іншого боку, поліноми з кінцевого поля GF(3) формують максимальний період генерації, що дорівнює $T - 3^n$. І це за $n = 3$ формує цикл $T_{max} = 81-1$. Для шифрування серйозного повідомлення це також недостатньо, але цикл генерації збільшується вп'ятеро. Але поліноми з кінцевого поля GF(3) дозволяють контролювати й 3-й стан, який до теперішнього часу ще не знаходить широкого використання [1-2].

Арифметика поля GF(3) також використовує множення, як звичайне множення поліномів, але з модулем по незвідному поліному, інверсію та побітове XOR, але вже за mod3.

В роботі наводяться рекомендації по використанню поліномів за різними критеріями оцінювання.

Обґрунтовано висновок в доцільності використання як в комп'ютерній техніці модуля 3-й, поліномів відповідних ступенів, так й при шифруванні повідомлень.

Література:

1. Кудряшов В.Є., Коломійцев О.В., Рисований О.М., Мегельбей В.В., Жирна О.В. Методика числового моделювання визначення показника ефективності стрільби ракетою по різних цілях при відпрацюванні цілевказівки з батарейного командного пункту. Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки. 1(19) (2024). Харків. 2024. С. 107-116. https://doi.org/10.37701/dndivsovt.19.2024.13.

2. Рисований О.М., Ігнатьєв К.І., Рибалка Р.В., Рудаковський Д.Р. Механізм шифрування повідомлень з максимальною довжиною // Інформатика, управління та штучний інтелект. Тези одинадцятої міжнародної науково-технічної конференції. – Харків: НТУ "ХПІ", 2024. – 176 с. - С.127. https://web.kpi.kharkov.ua/ai/wp-content/uploads/sites/249/2024/10/TEZY_IUSHI_2024.pdf.