РЕАЛІЗАЦІЯ АРИФМЕТИЧНИХ ОПЕРАЦІЙ В СКІНЧЕННИХ ПОЛЯХ НА МЕРЕЖАХ КЛІТИННИХ АВТОМАТІВ

ГОРМАКОВА І.В., ДЕРБУНОВИЧ Л.В.
Національний технічний університет "Харьківський політехнічний інститут", м.Харків

Сучасні технології виробництва електронних елементів дозволяють створювати економічні обчислювальні та інформаційні мережі, потужність яких можна порівняти із потужністю суперкомп'ютерів типу n-Cube, Cray та їм подібних, але з ціною значно меншою. Застосовують такі мережі для реалізації різноманітних протоколів у сучасних мережах обробки інформації, завадостійкого кодування, криптографії, при спектральному аналізі та т.п.

У перерахованих вище мережах та системах одними з найбільш часто вживаних є арифметичні операції складання, множення та піднесення у квадрат елементів скінченних полів Галуа за модулем чисел великої розрядності. Інші арифметичні операції, такі як піднесення до степені або інверсія, можуть бути виражені через операції множення або піднесення у квадрат.

У доповіді представлено метод побудови помножувача, що оперує у скінченних полях Галуа.

Запропоновано архітектуру послівно-послідовного помножувача у полі $GF(2^p)$, в якій використовують уніфіковані блоки із мереж клітинних автоматів, комбінаційні модулі та регістри, що дозволяє без додаткових розрахункових операцій змінювати архітектуру помножувача відповідно до змін генеруючого полінома поля, довжини операндів або довжини слова. Зміна генеруючого полінома при збереженні степені полінома p вимагає тільки зміни правил настроювання мережі клітинних автоматів при повному збереженні їх структури. При зміні довжини операндів чи довжини слова змінюється розрядність уніфікованих блоків при повному збереженні їх структури.

Загальний час роботи запропонованого помножувача складає $(\lceil p/\omega \rceil+\omega)$ тактів, де ω – довжина слова, p – довжина операндів. Архітектура помножувача розрахована на реалізацію на ПЛІС типу FPGA та є такою, що легко тестується.