РЕАЛІЗАЦІЯ УНІВЕРСАЛЬНИХ ПОМНОЖУВАЧІВ В СКІНЧЕННИХ ПОЛЯХ ГАЛУА НА ПЛІС ТИПУ FPGA

Гормакова І.В.

Національний технічний університет «Харківський політехнічний інститут», м.Харків

Під час проектування систем управління залізничним транспортом, банківською діяльністю, об'єктів АСУ ТП забезпечення по підвищення безпечності таких систем є однією з найважливіших умов. Найкращим рішення для забезпечення надійної передачі та зберігання інформації є застосування систем захисту інформації, особлива криптосистем.

Як відомо, при виконанні криптографічних алгоритмів найбільш часто вживаними є арифметичні операції в скінченних полях $GF(2^p)$: операції складання, множення та піднесення у квадрат елементів скінченних полів $GF(2^p)$ за модулем чисел великої розрядності.

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

Запропоновано архітектуру універсального 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.

Особливістю запропонованої архітектури помножувача є те, що за допомогою спеціального управляючого сигналу мається можливість налаштувати помножувач на виконання або прямої операції помноження елементів скінченного поля, або помноження елементів скінченного поля за методом Монтгомері.

Загальний час роботи запропонованого помножувача складає $(\lceil p/\omega \rceil+\omega)$ тактів, де ω – довжина слова, p – довжина операндів.

Наведено приклади реалізації запропонованої архітектури помножувача на ПЛІС типу FPGA. Проведений порівняльний аналіз запропонованої архітектури універсального помножувача та вже існуючих помножувачів відносно кількості використаних вентилів та площі на кристалі.