АНАЛІЗ ЕФЕКТИВНОСТІ АПАРАТНОЇ РЕАЛІЗАЦІЇ АЛГОРИТМУ ШИФРУВАННЯ «КАЛИНА» НА ПЛІС

Караман Д. Г., Божок О. І.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

«Калина» — кодова назва блочного симетричного алгоритму шифрування, який став лідером за результатами відкритого конкурсу на національний стандарт симетричного алгоритму шифрування, що проводився з 2007 по 2010 рік. Після незначних змін він був прийнятий у якості національного стандарту ДСТУ 7624:2014 і введений в дію з 1 липня 2015 року.

Алгоритм шифрування «Калина» побудований на базі структури SPN (substitution-permutation network) зі збільшеним розміром MDS-матриці, з набором з чотирьох підстановлювальних блоків, попереднім і фінальним забілюванням за допомогою операції додавання по модулю 2^{64}, а також оригінальною конструкцією схеми розширення ключа шифрування розміром аж до 512 біт.

Основними вимогами конкурсу для кандидатів на національний стандарт були високий ступінь криптографічного стійкості і високий рівень продуктивності програмних реалізацій на 64-бітних процесорах загального призначення. Однак прийняття алгоритму в якості національного стандарту означає проходження сертифікаційних процедур для систем криптографічного захисту інформації з будь-якою формою реалізації алгоритму шифрування, в тому числі і апаратною.

Всі найбільш популярні алгоритми шифрування мають безліч варіантів апаратних реалізацій в різних базисах. Одним з найбільш популярних базисів є програмовані логічні інтегральні схеми (ПЛІС) типу FPGA. Цей базис дозволяє отримувати прийнятні за ефективністю і швидкодією рішення при мінімальних матеріальних і часових витратах на розробку. Ще однією особливістю проектування пристроїв на ПЛІС є отримання платформонезалежного опису реалізованого функціонального блоку, який, згодом, можна модифікувати і покращувати, конвертувати для реалізації в інших базисах, а також використовувати для моделювання роботи пристрою задля освітніх цілей і проведення наукових досліджень.

У доповіді представлена функціональна модель блокового симетричного алгоритму шифрування «Калина», опис якої виконано за допомогою мови опису апаратури VHDL, розглянуті особливості реалізації перетворень даного алгоритму, наведено попередні оцінки апаратних витрат і статичні часові характеристики реалізації представленої моделі в базисі ПЛІС різних виробників.