АНАЛІЗ МОЖЛИВОСТІ РЕАЛІЗАЦІЇ АЛГОРИТМУ ПОТОКОВОГО ШИФРУВАННЯ «MICKEY» НА ОСНОВІ ПРОГРАМУЄМИХ ЛОГІЧНИХ МАТРИЦЬ

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

Розробка нових стандартів і швидкий розвиток криптографічних засобів захисту дає нам можливість реалізовувати їх на сучасних платформах. За допомогою апаратного проектування цифрових систем можливо збільшити швидкодію, а нові алгоритми криптографічного захисту дозволяють підвищити стійкість і при цьому використовувати їх в системах з обмеженою кількістю ресурсів. Об’єктами дослідження можуть бути алгоритм потокового шифрування «MICKEY»; симетричні алгоритми шифрування; платформа САПР «MAX + PLUS II».

Метою даної роботи був аналіз можливості реалізації алгоритму потокового шифрування «MICKEY» на сучасній елементній базі. Алгоритм «MICKEY» може ефективно бути реалізований на всіх сучасних апаратних платформах. Він має просту реалізацію при високому ступені захищеності. У ньому використовується нерегулярне тактування, а також нові методи, що забезпечують досить велику стійкість до атак. Використовуючи алгоритм «MICKEY», можливо дослідження характеристик ентропії та кореляції; аналіз ефективності реалізації алгоритму на ПЛІС.

На відміну від звичайних цифрових мікросхем логіка роботи ПЛІС не визначається при виготовленні, а задається за допомогою програмування. Структури ПЛІС мають високий рівень регулярності: основу кристала ПЛІС становить матриця однотипних функціональних вузлів, на базі яких користувач може створювати цілі системи керування складними технологічними об'єктами. Завдяки цьому ПЛІС характеризуються високою швидкодією і надійністю, а також широкими можливостями в частині резервування і діагностики. Окремою сферою застосування ПЛІС є пристрої для захисту від копіювання та модифікації інформації. Застосування ПЛІС середнього ступеня інтеграції виявляється достатнім для надійного «закриття» інформації. Сучасні ПЛІС мають такі характеристики, як властивість багаторазової переконфігурації, низька вартість виготовлення, низька енергія споживання, висока швидкодія. Оскільки ПЛІС має можливість швидкого перепрограмування та перебудови обчислювальної структури, то це дозволяє реалізовувати довільні алгоритми обробки даних.

У рамках досліджень програмно-апаратна реалізація «MICKEY» була виконана мовою AHDL. Такий програмно-апаратний підхід дозволить забезпечити ефективне та просте користування, підтримку та реалізацію методів паралельного програмування, широку функціональність виготовленого пристрою та економічну привабливість.