де q – заряд електрона, i – середня сила струму (зокрема фоновий струм і струм сигналу), f – ширина частотної смуги. З рівняння (1) випливає, що дробовий шум підсилюється у разі приросту струму і ширини смуги.

Середнє значення квадрата напруги теплового шуму в будь-якому колі, за певної температури, у малому частотному інтервалі:

$$\overline{\Delta U^2} = 4kTR\Delta f, \qquad (2)$$

де k – стала Больцмана, що дорівнює $1,38 * 10^{-23}$ *Дж/град*; R – опір кола, Ом.

На основі цього розробляються структури виділення шумових сигналів та досліджуються впливи кожного з видів шумів на показник температури.

Передбачається використання сучасних методів опрацювання сигналів, зокрема вейвлет-перетворення, для виділення інформативних параметрів сигналу з метою оцінки температури.

Висновки. Як показують попередні дослідження вейвлет-перетворення доцільно та ефективно використовувати для виділення і оцінки шумових сигналів, а вдосконалення відповідних методів перетворення є актуальним напрямом подальших наукових досліджень.

С. Брао
Науковий керівник – д-р техн. наук, проф. В.М. Максимович

ПРИСТРОЇ АПАРАТНОГО ШИФРУВАННЯ ДАНИХ З ІНТЕРФЕЙСОМ USB

USB-ключі, або, як їх ще називають, USB-токени – це персональний засіб автентифікації та зберігання даних у комп'ютерних системах та мережах. Ззовні цей пристрій являє собою звичайний флеш-носій, але за своїми функціями він багато в чому відповідає смарт-карті.

Ці пристрої зручні у користуванні, оскільки не потребують запам'ятовувати безліч паролів і кодів доступу, вся інформація зберігається в USB-токені. Крім того, USB-ключі підтримують роботу з цифровими сертифікатами і електронними цифровими підписами (ЕЦП), можуть переносити цифрові підписи, сертифікати, конфідентційні файли та іншу інформацію, яку небезпечно зберігати на відкритих носіях інформації.

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua

Було запропоновано пристрій шифрування з USB-інтерфейсом, який має структуру USB-ключа. Оскільки в багатьох галузях, де ціна та витрати енергії виходять на передній план, обчислювальна потужність сконцентрована в малих, недорогих центральних процесорах, серед яких домінують 8-бітні мікроконтролери, для використання в пристрої був вибраний малопотужний недорогий мікроконтролерATmega16.

Під час вибору алгоритму шифрування, орієнтуючись на розроблення недорогого пристрою на мікроконтролері, для якого визначальними характеристиками буде розмір коду та час виконання, зосередимо увагу на симетричних шифрах, оскільки їх ідея значно більше підходить для реалізації в портативних пристроях з врахуванням вказаних критеріїв.

Опираючись на результати порівняння вимог до пам'яті реалізацій алгоритму ГОСТ 28147-89, наведеними в статті, у варіанті мінімального розміру коду необхідно затратити менший обсяг пам'яті, ніж для всіх інших алгоритмів. У порівнянні за продуктивністю алгоритму ГОСТ 28147-89 з відомими реалізаціями інших lightweight-алгоритмів, алгоритм ГОСТ 28147-89 у варіанті максимальної швидкодії демонструє достатньо високу продуктивність, поступаючись лише алгоритму AES і випереджаючи всі інші алгоритми.

Згідно з отриманими результатами, для використання в розроблюваному пристрої було вибрано алгоритм ГОСТ 28147-89, який має найвище співвідношення продуктивність/розмір коду з всіх розглянутих криптоалгоритмів, забезпечуючи при цьому високий рівень захисту.

Розроблену конструкцію можна вдосконалювати, збільшуючи функціональні можливості.

Н. Чикальська
Науковий керівник – канд. техн. наук, доц. А.В. Гунькало

ОЦІНЮВАННЯ ЗАДОВОЛЕНОСТІ СПОЖИВАЧІВ ЯКІСТЮ ПРОДУКЦІЇ (ПОСЛУГ)

Кожен із нас, купуючи продукцію, або користуючись послугами, хоче, щоб вони були якісними, тобто такими, які задовольняють наші вимоги.

Від того, наскільки споживачі задоволені продукцією або послугами, залежить успіх підприємства чи організації (деколи і авторитет), адже задоволені споживачі частіше звертаються в організацію, рекомен-

Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua