УДК 004.056
Т.Коркішко, Л.Коркішко, В.Карпінський
(Тернопільський національний економічний університет)

КРИПТОАТАКИ НА ПІДСТАВІ ВИТОКУ ІНФОРМАЦІЇ З ПОБІЧНИХ КАНАЛІВ І ПРОТИДІЯ ЇМ

Атаки SCA (Side-Channel Attacks) – це атаки, які ґрунтуються на SCI (Side Channel Information), тобто на витоку інформації з побічних каналів. Інформація SCI – інформація, яка може бути відновлена з шифрувального пристрою та походить з процесу зашифрування відкритого тексту або його розшифрування. Методи SCA є небезпечні, тому що ці атаки можуть проводитися швидко та іноді здійснюватися, використовуючи доступні апаратні компоненти. Кількість часу, потрібного для нападу та аналізу, залежить від типу атаки. Розглянуте стосується лише найзагальнішої інформації про побічні канали її витоку, якими є: часові атаки TA (Timing Attacks), атаки простого SPA та диференційного DPA аналізу споживання (Simple and Differential Power Analysis Attacks) та атаки помилок FA (Fault Attacks) – недиференційний аналіз помилок NDFA (Non-Differential Fault Analysis) і диференційний аналіз помилок DFA (Differential Fault Analysis) в поєднанні з іншими атаками, такими як диференційно-ключові атаки (Differential-Key Attacks) або криптоааналіз диференційно-пов'язаних ключів (Differential Related Key Cryptanalysis).

В подальшому оцінено підходи до протидії криптоатакам SCA з рекомендаціями врахування одержаних результатів для розробки відповідних криптографічних модулів, а саме:

1) спільні підходи проти всіх атак – а) загальні інформаційно-незалежні обчислення, б) засліплення, в) уникнення умовного переходу і таємних проміжних ланок, г) ліцензування змодифікованих алгоритмів;

2) методи протидії проти часових атак – а) додавання затримок -- можуть суттєво ускладнити атаку та зробити її набагато важчою, але все ще можливою, б) зрівнювання часу множення та піднесення до квадрата -- цей підхід запобігає часовим атакам проти операцій піднесення до степеня, які виконуються як частка операцій асиметричної схеми шифрування та підлягають найзагальнішим атакам;

3) методи протидії атакам енергетичного аналізу – а) зрівноважування енергетичного споживання -- такі підходи, за яких енергетичне споживання за межами модуля є постійне та незалежне від вхідних і ключових бітових послідовностей, запобігають всім типам атак енергетичного споживання, зокрема SPA і DPA, б) зменшення значення сигналу -- на жаль, загалом таке зменшення сигналу не може звести нанівець значення сигналу, оскільки нападник, володіючи значною низкою вибірок, все ще зможе виконати DPA на сильно погіршеному сигналі, в) додавання шуму -- одне із запропонованих вирішень полягає в доданні випадкових обчислень, які збільшують рівень шуму достатнім для неможливості виявлення DPA, причому основна мета полягає в доданні досить випадкового шуму, щоб зупинити напад, але ще також обмежити його мінімально зверху, г) екранування -- може зробити атаки нездійсненними, однак зумовлює суттєве зростання вартості пристрою та його габаритів, д) модифікація запроектованих алгоритмів -- цим можна досягти розв'язання задачі, але вимагаються зміни проекту в алгоритмах і протоколах, що, ймовірно, робить результуючий продукт невідповідним до стандартів і специфікацій;

4) заходи проти атак помилок – а) виконання подвійного шифрування -- лише зумовлює атаку DFA важчою для здійснення із-за необхідності більшої кількості вибірок, але не неможливою.