УДК 004.056.55

О. БЕСПАЛОВ
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України,
Київ, Україна, e-mail: *alexb5dh@gmail.com*.

ПОБУДОВА CCA-СТІЙКОЇ МОДИФІКАЦІЇ АЛГОРИТМУ, ВИЗНАЧЕНОГО В ДСТУ 9041:2020

Анотація. Прийнятий у 2020 році Національний стандарт України ДСТУ 9041:2020 визначає алгоритм гібридного шифрування, який є стійким до атак, спрямованих на відновлення ключа та повідомлення, але не є IND-CCA-стійким, а також не є стійким до атак малих підгруп. У роботі побудовано модифікацію цього алгоритму, яка є стійкою як до IND-CCA, так і до атак малих підгруп, а також є узгодженою з чинними Національними стандартами України.

Ключові слова: ДСТУ 9041, скручені криві Едвардса, гібридне шифрування, IND-CPA, IND-CCA, DDHP, атаки малих підгруп.

DOI 10.34229/KCA2522-9664.26.3.13

ВСТУП

Український Національний стандарт ДСТУ 9041:2020 «Інформаційні технології. Криптографічний захист інформації. Алгоритм шифрування коротких повідомлень, що базується на скручених кривих Едвардса» [1] реалізує гібридне шифрування, що базується на KEM / DEM (Key Encapsulation Mechanism / Key Decapsulation Mechanism) парадигмі [2]. Назва «шифрування коротких повідомлень» пов'язана з основним призначенням цього стандарту — шифруванням ключів, однак його можна використовувати для шифрування повідомлень довільної довжини. Попри те, що цей алгоритм використовує симетричне шифрування та елементи асиметричної криптології, він вважається асиметричним алгоритмом, оскільки не потребує попереднього передавання секретних ключів.

Алгоритм гібридного шифрування, визначений в ДСТУ 9041 (далі — ДСТУ), є стійким до атак на відновлення ключа та/або відновлення повідомлення [3] за стандартного припущення про складність задачі дискретного логарифмування. Проте строго обґрунтованого аналізу його стійкості до так званих розрізнювальних атак наразі не існує.

Розрізнювальні атаки хоч і не несуть безпосередньої загрози відновлення ключа або повідомлення, поширені у сучасній криптології [4–8]. Згідно зі своєю назвою ці атаки призначені для розв'язання такої задачі: відрізнити величину, отриману в результаті певного перетворення з відомими вхідними даними, від випадково отриманої величини (прикладом такої задачі є розрізнювальна задача Діффі–Геллмана (Distinguishing Diffie–Hellman Problem (DDHP)) [9]).

Найбільшу увагу привертають розрізнювальні атаки з вибраним відкритим текстом (IND-CPA, Indistinguishability under Chosen Plaintext Attack) та з вибраним шифрованим текстом (IND-CCA, Indistinguishability under Chosen Ciphertext Attack) [2]. (Додавання IND до назви атаки підкреслює, що вона спрямована саме на задачу розрізнювання, а не відновлення ключа або повідомлення, надалі будемо випускати IND у назві атаки.)

У роботі [10] доведено стійкість алгоритму ДСТУ до CPA, а також, що він не є стійким до CCA, оскільки обидва компоненти цього алгоритму (KEM та симетричний алгоритм) не є стійкими до такої атаки. Тому метою цієї статті є побудова CCA-стійкої модифікації ДСТУ такої, що буде узгоджена із чинними Національними стандартами.