УДК 003.26.09; 519.688

А. Луцків, Ю. Кондрацький
(Тернопільський національний технічний університет імені Івана Пулюя)

ДОСЛІДЖЕННЯ КРИПТОСТІЙКОСТІ АЛГОРИТМУ UEA1 МЕРЕЖ ПЕРЕДАЧІ ДАНИХ СТАНДАРТУ UMTS

З розвитком та поширенням телекомунікаційних технологій постає задача забезпечення конфіденційності інформації. Одним із завдань, яке необхідно вирішувати, є верифікація існуючих систем захисту. На зміну другому поколінню безпровідних технологій зв'язку приходять стандарти третього покоління, зокрема UMTS (W-CDMA). Universal Mobile Telecommunications System (UMTS) – технологія стільникового зв'язку, розроблена Європейським інститутом телекомунікаційних стандартів (ETSI) для впровадження 3G в Європі.

Для забезпечення конфіденційності та цілісності даних у UMTS використовуються два набори алгоритмів: перший набір - UEA1 і UIA1 [1], який базується на блоковому шифрі KASUMI; другий - UEA2 і UIA2 — на потоковому шифрі SNOW 3G. Використання тих чи інших систем шифрування обумовлено апаратним забезпеченням оператора зв'язку, абонента, а також аспектами роумінгу абонентських терміналів покоління 2G. Тому досить часто використовуються алгоритми UEA1/UIA1, а це зумовлює актуальність розробки відповідних криптоаналітичних засобів для верифікації відповідних систем захисту.

Згідно архітектури безпеки 3GPP систем для забезпечення конфіденційності і цілісності даних використовуються алгоритми f8 і f9 відповідно, зокрема блоковий шифр KASUMI, який базується на мережі Фейстеля з 8 раундами і генерує 64-бітне вихідне значення з 64-бітного вхідного значення, використовуючи 128-бітний ключ [2].

У 2010-му році опубліковано "сендвіч-атаку" із пов'язаними ключами на 8-раундовий KASUMI, з часовою складністю 2^{32} [3]. Варто зазначити, що дані криптоаналітичні атаки носять теоретичний характер і задачі їх практичної реалізації та оптимізації в паралельних та розподілених обчислювальних системах є важливими з практичної точки зору. Розв'язанням даної задачі займаються автори доповіді.

1. 3GPP TS 35.201: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: f8 and f9 Specification".

2. 3GPP TS 35.202: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification".

3. Orr Dunkelman, Nathan Keller, Adi Shamir (2010-01-10). A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony, Weizmann Institute of Science 10 January 2010 [Електронний ресурс]. – Режим доступу: URL: http://eprint.iacr.org/2010/013.pdf