УДК 004.056

ПОБУДОВА РОЗПІЗНАВАЧА ДЛЯ ШИФРУ SIMECK НА ОСНОВІ КРИПТОАНАЛІТИЧНОГО МЕТОДУ ОБЕРТАНЬ

М. М. Коломієць[1]

[1] *Національний технічний університет України «Київський політехнічний інститут»*

Анотація

В роботі запропоновано підхід до побудови статистичного розпізнавача шифротексту від випадкового тексту за схемою пов'язаних ключів для сімейства блокових шифрів Simeck.

Ключові слова: Simeck, легковагова криптографія, атака пов'язаних ключів, статистичний розпізнавач

Вступ

Шифр Simeck є представником легковагової криптографії. Він створений на основі шифрів Simon та Speck і поєднує в собі переваги цих шифрів. Simeck мало досліджений на даному етапі, тому є доцільними дослідження переносу атак на блокові шифри Simon та Speck [1].

1. Короткий опис шифру Simeck

Simeck спроектований таким чином, щоб бути максимально малим по апаратній частині та компактним в програмній реалізації. Раундова функція та алгоритм генерування ключа шифру Simeck наслідують структуру Фейстеля. Раундова функція визначена наступним чином:

$$R_{k_i}(l_i, r_i) = (r_i \oplus f(l_i) \oplus k_i, l_i),$$

де l_i та r_i – два слова внутрішнього стану Simeck, k_i – раундовий ключ, а функція f визначена як

$$f(x) = x\&(x <<< 5) \oplus (x <<< 1).$$

Схематично раунд шифру показаний на рис. 1.

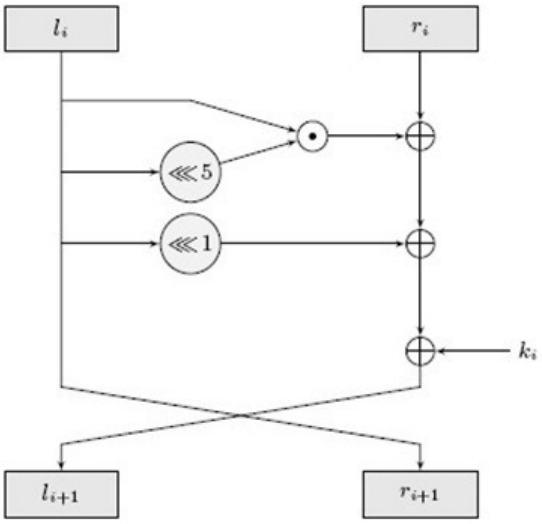

Рис. 1. Схема раунда шифру Simeck

2. Побудова статистичного розпізнавача

Шифр Simeck використовує операції XOR та AND у раундовій функції. Це дає можливість створення статистичного розпізнавача за схемою пов'язаних ключів. Розпізнавач відрізнятиме шифротекст, який видає шифр Simeck, від випадкового тексту.

Операції зсуву числа на r біт позначаються як $<<<_r$ та $>>>_r$. Зсунуті змінні позначаються $\overleftarrow{X}$ та $\overrightarrow{X}$ відповідно. Пару $(X, \overrightarrow{X})$ називають парою обертання.

В основу побудови статистичного розпізнавача покладено твердження про те, що пара обератння зберігає будь-яке побітове перетворення та будь-яке обертання, наприклад

$$\overrightarrow{X \oplus Y} = \vec{X} \oplus \vec{Y}, \vec{X}>>>_{r'} = \overrightarrow{X >>>_{r'}}$$

Розпізнавач застосовується до певного чорного ящика, визначаючи чи в ньому міститься шифр Simeck чи випадкова перестановка. Для цього необхідно взяти пару обертання $(A, \vec{A})$ та подати по черзі на вхід чорного ящика. Як результат виникає дві послідовності B та B'. Якщо при аналізі цих послідовностей виявиться, що B' та B є парою обертання з певним значенням r, то даний чорний ящик - це шифр Simeck, якщо ні – то на виході випадкова послідовність.

Висновки

В даній роботі запропоновано підхід до побудови статистичного розпізнавача на основі сценарію пов'язаних ключів. Даний статистичний розпізнавач дає змогу у майбутньому побудувати атаку часткового відновлення ключа на блоковий шифр Simeck.

Перелік використаних джерел

1. Jukov A. E. Lightweight cryptography // Cybersecurity questions. — 2015. — Т. 9, № 1. — С. 2–4.