МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Лабораторна робота №3

на тему: «Семантична стійкість, нерозрізненність для атак IND-CCA & IND-CPA»

Перевірив:

_____
(посада, ініціали та прізвище)

_____ _____
(дата захисту) (підпис)

Кількість балів:
Відпов. темі: _____
Оформлення: _____
Оригінальність: _____
Захист: _____
Сума: _____

Виконав
ст. групи: ФІ-02мп
Стасюкевич А.Т.
(ініціали та прізвище)

_____
(підпис)

Київ — 2021р.

ЗМІСТ

1 СЕМАНТИЧНА СТІЙКІСТЬ. ПОНЯТТЯ НЕРОЗРІЗНЕНОСТІ

Семантична стійкість, як характеристика криптосистем в криптографії, подібна до концепції безпеки Шеннона, але з деяким уточненням.

Твердження 1.1. *Нехай пара* (E, D) *є шифром над* (K, M, C). *Відповідно до концепції Шеннона,* (E, D) *має досконалу секретність, якщо*

$$\{E(k, m_0)\} = \{E(k, m_1)\}, \forall\ m_0\ ,\ m_1 \in M(|m_0| = |m_1|)\ \ , k \leftarrow K \quad (1.1)$$

Твердження означає, що шифртекст не розкриває жодної інформації стосовно відкритого тексту. Змінивши знак рівності в твердженні (а саме в формулі 1.1), ми отримаємо поняття семантичної стійкості.

Означення 1.1. Шифр (E, D) являється семантично стійким, якщо

$$\{E(k, m_0)\} \approx_p \{E(k, m_1)\}, \forall\ m_0\ ,\ m_1 \in M(|m_0| = |m_1|)\ \ , k \leftarrow K \quad (1.2)$$

В формулі 1.2 $\approx_p$ означає те, що зловмисник може заволодіти мізерно малою інформацією з шифр тексту, якої недостатньою для судження про відкритий текст. Ввівши поняття семантичної стійкості, Гольдвассер та Мікалі показали, що це є еквівалентом поняттю нерозрізненності шифротексту під час атаки з підібраним відкритим текстом. Дамо інтуітивне визначення нерозрізненності:

Означення 1.2. Криптосистема являється стійкою з точки зору нерозрізненності, якщо жоден зловмисник, отримавший шифртекст, випадково вибраний з двоелементної множини повідомлень, визначеної противником, не може ідентифікувати відповідний цьому шифротексту відкритий текст з ймовірністю значно краще, ніж при випадковому

вгадуванні (1/2). Розглянемо найбільш поширенні поняття, а саме нерозрізненність для атак на основі вибраного відкритого тексту (IND-CPA) та нерозрізненність для атак на основі підібраного шифртексту (IND-CCA).

1.1 IND-CPA

IND-CPA розшифровується, як INDistinguishability under Chosen Plaintext Attack, нерозрізненність для атак на основі вибраного відкритого тексту. Задамо певний алгоритм генерації ключів KG, що генерує пару K_E, K_D. Алгоритм шифрування E та дешифрування D. Задамо певний алгоритм, що відповідає правилу: the adversary генерує два повідомлення однакової довжини. The challenger вирішує випадковим чином зашифрувати одне з них. The adversary намагається вгадати, яке з повідомлень було зашифровано.

Алгоритм

1) Challenger: $K_E, K_D = KG$(секретні параметри);

2) Adversary: m_0, m_1= вибирає два повідомлення однакої довжини. Відправляє m_0, m_1 до challenger.Виконує додаткові операції за поліноміальний час, включаючи виклики до оракула;

3) Challenger: b = випадковим чином вибирає значення з 0 та 1;

4) Challenger: $C = E(K_E, m_b)$. Відправляє C до adversary.

5) Adversary: надає відповідь стосовно b;

6) Якщо відповідь = b, то the adversary переміг.

Криптосистема стійка в сенсі IND-CPA, якщо будь-який ймовірний зловмисник за поліноміальний час має лише незначну "перевагу" в розрізненні шифротекста над випадковим вгадування.

1.2 IND-CCA

IND-CCA розшифровується, як INDistinguishability under Chosen Ciphertext Attack, нерозрізненність для атак на основі вибраного шифрованого тексту. Головна ідея IND-CCA така ж як в IND-CPA, але різниця в тому, що для IND-CCA The adversary додається додаткова можливість: викликати оракула шифрування або дешифрування. Це означає: The adversary може зашифрувати або розшифрувати довільні повідомлення, до отримання зашифрованого тексту.

Алгоритм

1) Challenger: $K_E, K_D = KG$(секретні параметри);

2) Adversary (поліноміально обмежене кількість разів): викликати оракул шифрування або дешифрування для довільних відкритих текстів або зашифрованих текстів відповідно;

3) Adversary: m_0, m_1= вибирає два повідомлення однакої довжини. Відправляє m_0, m_1 до challenger.Виконує додаткові операції за поліноміальний час, включаючи виклики до оракула;

4) Challenger: b = випадковим чином вибирає значення з 0 та 1;

5) Challenger: $C = E(K_E, m_b)$. Відправляє C до adversary.

6) Adversary: надає відповідь стосовно b;

7) Якщо відповідь = b, то the adversary переміг.

Криптосистема стійка в сенсі IND-CCA, якщо Adversary не має істотної переваги в даній грі.

ВИСНОВКИ

Було розглянуто поняття семантичної стійкості, нерозрізненності для атак IND-CPA IND-CCA. Визначенно, яка криптосистема являється IND-CPA або IND-CCA стійкою.

ПЕРЕЛІК ПОСИЛАНЬ

1. https://crypto.stackexchange.com/questions/26689/easy-explanation-of-ind-security-notions [Електронний ресурс].

2. https://www.coursera.org/lecture/crypto/semantic-security-q0h9g – Dan Boneh

3. https://en.wikipedia.org/wiki/Ciphertext_indistinguishability#IND-CPA [Електронний ресурс].