Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"

Реферат на тему:

«Семантична стійкість, IND-CCA, IND-CPA»

Виконавець: Попов А., ФІ-02мн.

Київ 2021

ЗМІСТ

1 СЕМАНТИЧНА СТІЙКІСТЬ. ПОНЯТТЯ НЕРОЗРІЗНЕНОСТІ

Семантична безпека, яку Goldwasser та Micali запровадили для шифрування відкритим ключем, переносить сутність поняття К.Шеннонв про безпеку на обставини ситуації, коли безпека не є абсолютною але залежить від обчислювальних зусиль, докладених противником. Шеннон каже : "схема шифрування безпечна, якщо можна визначити те, що можна визначити щодо відкритого тексту з його зашифрованого тексту також повністю визначається за відсутності зашифрованого тексту. Семантична безпека вимагає, щоб те, що можна ефективно обчислити щодо деяких відкритих текстів з їх зашифрованих текстів, можна було обчислити так само легко, як і за відсутності цих шифротекстів.

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. Говорячи про час роботи нападника A, ми включаємо, крім фактичного часу роботи, максимальний час витягувати два зразки з кожного простору повідомлень M, який виводить A, і ми включаємо максимальний час для обчислення f (M1, ..., Mq) за будь-яким вектором рядків. Говорячи про тривалість запитів A. підсумовуємо по всіх просторах повідомлень, що виводяться A, максимальну довжину рядка M, що виводиться за допомогою ненульова ймовірність за M, і ми також підсумовуємо довжини кодування кожного повідомлення пробіл, функція

f і рядок Y, виведені A. Ми наголошуємо, що вищезазначене здавалося б надзвичайно сильним поняттям безпеки. Ми надали суперникові можливість вибору просторів повідомлень, з яких буде кожне повідомлення звертається. Ми дозволили суперникові вибрати часткову інформацію про повідомлення, які він знаходить зручно передбачати. Ми дозволили супернику бути повністю адаптивним. Ми вбудували здатність виконати атаку за вибраним повідомленням (просто створивши алгоритм M, який виконує вибірку одного і того самого один бал). Незважаючи на все це, ми тепер показуємо, що безпека в сенсі невідмінності означає семантична безпека.

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 (англ. INDistinguishability under Chosen Plaintext Attack) - нерозрізненність для атак на основі вибраного відкритого тексту. Всі підходи до задання криптосистеми (в основі якої лежить імовірнісний алгоритм асиметричного шифрування) та доведення IND-CPA для неї - використовується формальний опис криптосистеми та моделювання зловмисника, зазвичай його формалізують як ймовірнісну поліноміальну машину Тьюрінга. 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: зловмисник генерує два повідомлення однакової довжини. The challenger вирішує випадковим чином зашифрувати одне з них. Зловмисник 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. Ця перевага виражається ймовірністю "перемоги"$P(A) = 1/2 + delta(k)$, де $delta(k)$ - нескінченно мала функція.

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 зловмиснику додається додаткова можливість: викликати оракула шифрування або дешифрування. Це означає: зловмисник 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.

1.3 IND-CCA2

IND-CCA2 - сутність така ж сама як і в IND-CCA1, тільки в цій схемі зловмиснику дозволяється коритсуватись оракулом після того як було отримано шифртекст C. За умови, що забороняється подавати шифртекст C на вхід оракулу, адже тоді визначення тривіалізується і

мета побудови всієї системи доведення втрачається.

ВИСНОВКИ

Було розглянуто поняття семантичної стійкості, нерозрізненності для атак IND-CPA & IND-CCA & IND-CCA2. Визначенно, яка криптосистема являється IND-CPA або IND-CCA стійкою.

Поряд із установленою термінологією щодо семантичної стійкості (IND-CPA, IND-CCA1-2), напрацьовано загальні підходи до її забезпечення. Такі як додавання MAC (message authentication code) в початок повідомлення (за умови, що MAC стійкий, виклики оракула для зловмисника не дають жодної переваги) для забезпечення IND-CCA. При чому в даній схемі автентифікується відкритий текст, навідміну від рельних криптосистем, де намагаються забезпечити цілісність шифртексту використовуючи MAC.

Також можна зустріти приклади криптосистем, коли виконується IND-CPA і виконується IND-CCA [5].

ПЕРЕЛІК ПОСИЛАНЬ

1. https://eprint.iacr.org/2015/042.pdf [Електронний ресурс].

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

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

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

5. https://people.csail.mit.edu/alinush/cse508-spring-2011/03-03-cpa-and-cca.pdf [Електронний ресурс].

6. https://www.cs.princeton.edu/courses/archive/fall07/cos433/lec14comb.pdf [Електронний ресурс].