НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

Реферат на тему
Криптографічні примітиви

Роботу виконав:
Юрчук Олексій, ФІ-52мн

2 грудня 2025 р.
м. Київ

ЗМІСТ

Розділ 1

Рівні стійкості криптографічних примітивів

Сучасна криптографія базується на формальних визначеннях безпеки, які дозволяють математично доводити стійкість криптографічних схем [1]. Ці визначення формулюються у вигляді *ігор безпеки* (security games) між супротивником (adversary) та челенджером (challenger), де супротивник намагається порушити якусь властивість криптосистеми [2]. В першому розділі розглянемо основні рівні стійкості криптографічних примітивів: односторонність (one-wayness), нерозрізненість (indistinguishability), семантична стійкість (semantic security) та стійкість до перетворень (non-malleability). Ці поняття аналізуються в контексті різних моделей атак, зокрема атак на основі обраного відкритого тексту (CPA), неадаптивних атак на основі обраного шифротексту (CCA-1) та адаптивних атак на основі обраного шифротексту (CCA-2) [3].

1.1 Моделі атак

Перед переходом безпосередньо до рівнів стійкості необхідно визначити моделі атак, які характеризують спектр можливостей супротивника. Нехай $\mathsf{PKE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ – асиметрична схема шифрування (Public Key Encryption) з простором повідомлень $\mathcal{M}$ та простором шифротекстів $\mathcal{C}$ [1].

1.1.1 Chosen Plaintext Attack (CPA)

В моделі атаки на основі обраного відкритого тексту супротивник має доступ до відкритого ключа pk і може обчислювати шифротексти для довільних повідомлень за власним вибором. Формально, супротивник $\mathcal{A}$ має оракульний доступ до функції шифрування $\mathsf{Enc}_{\mathsf{pk}}(\cdot)$ (тобто має можливість надсилати запити до функції/алгоритму оракула і отримувати коректні відповіді без знання внутрішнього ключа або його механізму роботи) [4].

Означення 1.1.1 (CPA-супротивник [5])**.**
CPA-супротивником називається ймовірнісний поліноміальний алгоритм $\mathcal{A}$, який отримує на вхід відкритий ключ pk та має доступ до оракула шифрування $\mathsf{Enc}_{\mathsf{pk}}(\cdot)$.

Для детермінованих схем шифрування з відкритим ключем доступ до оракула шифрування не надає додаткової переваги, оскільки супротивник може самостійно обчислити $\mathsf{Enc}_{\mathsf{pk}}(m)$ для будь-якого m [1].

1.1.2 Non-adaptive Chosen Ciphertext attack (CCA-1)

В моделі CCA-1 (також відомій як ”lunchtime attack” або Naor-Yung attack), супротивник додатково має доступ до оракула дешифрування $\mathsf{Dec}_{\mathsf{sk}}(\cdot)$, але лише *до* отримання challenge-шифротексту [6].

Означення 1.1.2 (CCA-1 супротивник [5]).
CCA-1 супротивником називається ймовірнісний поліноміальний алгоритм $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, *де:*

- $\mathcal{A}_1$ *отримує* pk *та має доступ до* $\mathsf{Dec}_{\mathsf{sk}}(\cdot)$, *генерує стан* state*;*
- $\mathcal{A}_2$ *отримує challenge та* state, *але* не має *доступу до* $\mathsf{Dec}_{\mathsf{sk}}(\cdot)$.

1.1.3 Adaptive Chosen Ciphertext attack (CCA-2)

Модель CCA-2, запропонована Рекоффом і Саймоном, є ”найсильнішою”(найгіршою з точки зору захисту) стандартною моделлю атаки [7]. Супротивник має доступ до оракула дешифрування як до, так і після отримання challenge-шифротексту, з єдиним обмеженням – він не може запитувати дешифрування самого challenge-шифротексту.

Означення 1.1.3 (CCA-2 супротивник [5]).
CCA-2 супротивником називається ймовірнісний поліноміальний алгоритм $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, *де обидві фази мають доступ до* $\mathsf{Dec}_{\mathsf{sk}}(\cdot)$, *з обмеженням, що* $\mathcal{A}_2$ *не може запитувати дешифрування challenge-шифротексту* c^*.

Згрупуємо ці атаки у порівняльну таблицю 1.1.

Привілегії	**CPA**	**CCA-1**	**CCA-2**
Доступ до pk	Так	Так	Так
Оракул $\mathsf{Enc}_{\mathsf{pk}}(\cdot)$	Так	Так	Так
Оракул $\mathsf{Dec}_{\mathsf{sk}}(\cdot)$ до challenge	Ні	Так	Так
Оракул $\mathsf{Dec}_{\mathsf{sk}}(\cdot)$ після challenge	Ні	Ні	Так (крім c^*)

Таблиця 1.1: Порівняння моделей атак за можливостями супротивника

1.2 Односторонність (One-Wayness)

Односторонність є *найслабшим* рівнем стійкості для схем шифрування. Вона вимагає, щоб супротивник не міг повністю відновити відкритий текст із шифротексту [3].

Означення 1.2.1 (OW-CPA стійкість).
Нехай $\mathsf{PKE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *– асиметрична схема шифрування, простір можливих атак:* $\mathsf{CPA} \in \{\mathsf{CPA}, \mathsf{CCA1}, \mathsf{CCA2}\}$. *Схема* PKE *називається OW-CPA стійкою, якщо для будь-якого* PPT *(Probabilistic Polynomial-Time)-супротивника* $\mathcal{A}$ *типу CPA:*

$$\mathsf{Adv}^{\mathsf{OW-CPA}}_{\mathsf{PKE},\mathcal{A}}(\lambda) = \Pr\left[\mathcal{A}(\mathsf{pk}, c^*) = m : \begin{array}{c}(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)\\ m \xleftarrow{p} \mathcal{M}\\ c^* \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m)\end{array}\right] \leq \mathsf{negl}(\lambda),$$

де λ – параметр безпеки.

Security game для OW-CPA наведена в алгоритмі 1.

Algorithm 1 Game OW-CPA для асиметричного шифрування

Require: Параметр безпеки 1^λ, супротивник $\mathcal{A}$
Ensure: Біт $b \in \{0, 1\}$
1: $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$
2: $m \xleftarrow{p} \mathcal{M}$
3: $c^* \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m)$
4: $m' \leftarrow \mathcal{A}(\mathsf{pk}, c^*)$
5: **if** $m' = m$ **then**
6:     **return** 1 ▷ guess successful
7: **else**
8:     **return** 0 ▷ guess failed
9: **end if**

Механізм інкапсуляції ключів (Key Encapsulation Mechanism, KEM) є криптографічним примітивом, що складається з трьох алгоритмів $\mathsf{KEM} = (\mathsf{KeyGen}, \mathsf{Encaps}, \mathsf{Decaps})$ [8].

Означення 1.2.2 (OW-CPA стійкість KEM)**.**
KEM $= (\mathsf{KeyGen}, \mathsf{Encaps}, \mathsf{Decaps})$ *називається OW-CPA стійким, якщо для будь-якого* PPT*-супротивника $\mathcal{A}$:*

$$\mathsf{Adv}^{\mathsf{OW-CPA}}_{\mathsf{KEM},\mathcal{A}}(\lambda) = \Pr\left[\mathcal{A}(\mathsf{pk}, c^*) = K : \substack{(\mathsf{pk},\mathsf{sk})\leftarrow\mathsf{KeyGen}(1^\lambda) \\ (K,c^*)\leftarrow\mathsf{Encaps}(\mathsf{pk})}\right] \le \mathsf{negl}(\lambda).$$

1.3 Нерозрізненість (Indistinguishability)

Нерозрізненість є значно сильнішим поняттям безпеки, ніж односторонність. Вона вимагає, щоб супротивник не міг отримати *жодної* інформації про відкритий текст із шифротексту [4].

Означення 1.3.1 (IND-CPA стійкість)**.**
Схема шифрування $\mathsf{PKE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *називається IND-CPA стійкою (Indistinguishability under Chosen Plaintext Attack),* $\mathsf{CPA} \in \{\mathsf{CPA}, \mathsf{CCA1}, \mathsf{CCA2}\}$*, якщо для будь-якого* PPT*-супротивника $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$:*

$$\mathsf{Adv}^{\mathsf{IND-CPA}}_{\mathsf{PKE},\mathcal{A}}(\lambda) = \left|\Pr[b' = b] - \frac{1}{2}\right| \le \mathsf{negl}(\lambda),$$

де "Гра" визначена в алгоритмі 2.

Означення 1.3.2 (IND-CPA стійкість KEM)**.**
KEM називається IND-CPA стійким, якщо для будь-якого PPT*-супротивника $\mathcal{A}$:*

$$\mathsf{Adv}^{\mathsf{IND-CPA}}_{\mathsf{KEM},\mathcal{A}}(\lambda) = \left|\Pr[\mathcal{A}(\mathsf{pk}, c^*, K_b) = b] - \frac{1}{2}\right| \le \mathsf{negl}(\lambda),$$

де $K_0 = K$ – справжній ключ з $(K, c^*) \leftarrow \mathsf{Encaps}(\mathsf{pk})$, а $K_1 \xleftarrow{p} \mathcal{K}$ – випадковий ключ.

Algorithm 2 Game IND-CCA2 для асиметричного шифрування

Require: Параметр безпеки 1^λ, супротивник $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$

Ensure: Біт $b' \in \{0,1\}$

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$

$(m_0, m_1, \mathsf{state}) \leftarrow \mathcal{A}_1^{\mathsf{Dec}_{\mathsf{sk}}(\cdot)}(\mathsf{pk})$ $\quad \triangleright\ |m_0| = |m_1|$

$b \xleftarrow{p} \{0,1\}$

$c^* \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_b)$

$b' \leftarrow \mathcal{A}_2^{\mathsf{Dec}_{\mathsf{sk}}(\cdot)}(c^*, \mathsf{state})$ $\quad \triangleright$ $\mathcal{A}_2$ не може запитувати $\mathsf{Dec}_{\mathsf{sk}}(c^*)$

return b'

1.4 Семантична стійкість (Semantic Security)

Семантична стійкість, введена Голдвассер та Мікалі [4], є симуляційним означенням безпеки. Інтуїтивно: схема є семантично стійкою, якщо будь-яку інформацію про відкритий текст, яку можна ефективно обчислити з шифротексту, можна також ефективно обчислити без шифротексту.

Означення 1.4.1 (SS-CPA стійкість).

Схема шифрування PKE *називається SS-CPA стійкою, якщо для будь-якого* PPT*-супротивника $\mathcal{A}$ існує* PPT*-симулятор $\mathcal{S}$ такий, що для будь-якої функції $f : \mathcal{M} \to \{0,1\}^*$ та розподілу $\mathcal{D}$ на $\mathcal{M}$:*

$$\left|\Pr[\mathcal{A}(\mathsf{pk}, \mathsf{Enc}_{\mathsf{pk}}(m)) = f(m)] - \Pr[\mathcal{S}(\mathsf{pk}, 1^{|m|}) = f(m)]\right| \leq \mathsf{negl}(\lambda),$$

де $m \leftarrow \mathcal{D}$.

Твердження 1.4.1 (Еквівалентність IND та SS [4, 9]).

Для моделі Chosen Plaintext Attack (CPA) маємо: IND-CPA $\Leftrightarrow$ SS-CPA.

Цей результат був розширений Белларе та ін. [3] на моделі CCA-1 та CCA-2:

$$\mathsf{IND\text{-}CCA1} \Leftrightarrow \mathsf{SS\text{-}CCA1}, \quad \mathsf{IND\text{-}CCA2} \Leftrightarrow \mathsf{SS\text{-}CCA2}.$$

1.5 Стійкість до перетворень (Non-Malleability)

Стійкість до перетворень (non-malleability) є напрямком захисту від атак, де супротивник намагається створити шифротекст, пов'язаний із challenge-шифротекстом [10].

Означення 1.5.1 (NM-CPA стійкість).

Схема PKE *називається NM-CPA стійкою, якщо для будь-якого* PPT*-супротивника $\mathcal{A}$, для будь-якого відношення R та розподілу $\mathcal{D}$:*

$$\Pr\left[R(m,\mathbf{m}')=1 \wedge c^* \notin \mathbf{c}' : \begin{array}{c} (\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda) \\ m \leftarrow \mathcal{D} \\ c^* \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m) \\ \mathbf{c}' \leftarrow \mathcal{A}(\mathsf{pk}, c^*) \\ \mathbf{m}' \leftarrow \mathsf{Dec}_{\mathsf{sk}}(\mathbf{c}') \end{array} \right] \approx \Pr\left[R(m, \mathbf{m}') = 1 : \begin{array}{c} m \leftarrow \mathcal{D} \\ \mathbf{m}' \leftarrow \mathcal{S}(\mathsf{pk}, 1^{|m|}) \end{array} \right].$$

В моєму розумінні означення [3], схема є NM-стійкою, якщо маючи шифротекст c^*, супротивник не може створити такий вектор шифротекстів $\mathbf{c}'$, дешифрування яких утворює вектор $\mathbf{m}'$, що є лінійною комбінацією оригінального повідомлення m.

1.6 Порівняльний аналіз означень

Означення	На що спрямований захист	Тип означення
OW (односторонність)	Повне відновлення повідомлення	Обчислювальне
IND (нерозрізненість)	Будь-яка інформація про повідомлення	Game-based
SS (семантична стійкість)	Будь-яка функція від шифротексту	Simulation-based
NM (стійкість до перетворень)	Створення пов'язаних шифротекстів	Simulation-based

Таблиця 1.2: Властивості різних рівнів стійкості

1.7 Ієрархія та імплікації між рівнями стійкості

Між різними рівнями стійкості існують певні імплікаційні співвідношення, які формують ієрархію стійкості [3, 11].

1.7.1 За типом атаки

Для фіксованого рівня стійкості $X \in \{\mathsf{OW}, \mathsf{IND}, \mathsf{SS}, \mathsf{NM}\}$:

$$X\text{-}\mathsf{CCA2} \Rightarrow X\text{-}\mathsf{CCA1} \Rightarrow X\text{-}\mathsf{CPA}.$$

Ці імплікації є односторонніми (зворотні імплікації не виконуються в загальному випадку) [3].

1.7.2 За рівнем стійкості

Для фіксованого типу атаки $\mathsf{CPA} \in \{\mathsf{CPA}, \mathsf{CCA1}, \mathsf{CCA2}\}$ [3, 11]:

$$\mathsf{NM\text{-}CPA} \Rightarrow \mathsf{IND\text{-}CPA} \Leftrightarrow \mathsf{SS\text{-}CPA} \Rightarrow \mathsf{OW\text{-}CPA}.$$

(!) Важливим фактом є те, що для CCA-2 атак нерозрізненість та стійкість до перетворень є еквівалентними поняттямм [11]:

$$\mathsf{IND\text{-}CCA2} \Leftrightarrow \mathsf{NM\text{-}CCA2}.$$

А для CPA ця еквівалентність не виконується:

$$\mathsf{NM\text{-}CPA} \Rightarrow \mathsf{IND\text{-}CPA}, \quad \text{але} \quad \mathsf{IND\text{-}CPA} \not\Rightarrow \mathsf{NM\text{-}CPA}.$$

1.7.3 Загальна ієрархія

Ієрархію рівнів стійкості для асиметричного шифрування можна гарно відобразити рисунком 1.1.

Стрілками позначимо імплікації. IND-CCA2 $\Leftrightarrow$ NM-CCA2 – єдина еквівалентність між IND та NM.

Найвищим рівнем стійкості для схем асиметричного шифрування є IND-CCA2 (еквівалентно NM-CCA2). Цей рівень є "золотим стандартом" для практичних криптосистем [11].

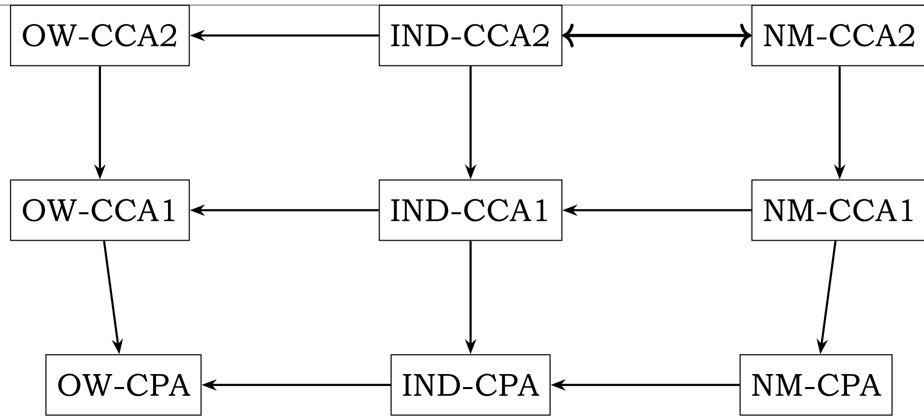

Рис. 1.1: Ієрархія рівнів стійкості

1.8 Приклади криптопримітивів

1.8.1 Криптопримітиви з доведеною стійкістю

RSA-OAEP (IND-CCA2)

RSA-OAEP (Optimal Asymmetric Encryption Padding) є стандартизованою схемою шифрування з відкритим ключем [12]. Схема використовує RSA-функцію з використанням оптимального падінгу, що базується на двох різних геш-функціях. Алгоритм шифрування RSA-OAEP є наступним:

Algorithm 3 RSA-OAEP шифрування

Require: Повідомлення m, відкритий ключ (n, e), геш-функції G, H
Ensure: Шифротекст c

$r \xleftarrow{p} \{0,1\}^{k_0}$ ▷ Випадкове значення
$s \leftarrow (m \| 0^{k_1}) \oplus G(r)$
$t \leftarrow r \oplus H(s)$
$w \leftarrow s \| t$
$c \leftarrow w^e \pmod{n}$
return c

Твердження 1.8.1 (Стійкість RSA-OAEP [13]).
RSA-OAEP є IND-CCA2 стійкою в моделі випадкового оракула за припущення складності RSA-задачі.

Cramer-Shoup (IND-CCA2 без ROM)

Схема Крамера-Шоупа є першою практичною схемою шифрування з відкритим ключем, для якої доведена IND-CCA2 стійкість у стандартній моделі (без випадкового оракула) [14].

Твердження 1.8.2 (Стійкість Cramer–Shoup [15]).
Схема Cramer–Shoup є IND-CCA2 стійкою за припущення DDH (Decisional Diffie–Hellman assumption).

ML-KEM (a.k.a Kyber)

ML-KEM (Module-Lattice-based Key Encapsulation Mechanism), раніше відомий як CRYSTALS-Kyber, є стандартизованим постквантовим КЕМ [16]. Він був обраний NIST (National Institute of Standards and Technology) як стандарт для постквантової криптографії.

Твердження 1.8.3 (Стійкість ML-KEM [17])**.**
ML-KEM є IND-CCA2 стійким за припущення складності задачі MLWE (Module Learning with Errors).

1.8.2 Криптопримітиви, що не задовольняють певним рівням стійкості

Textbook RSA

"Підручникова" схема RSA (Rivest-Shamir-Adleman without padding) не задовольняє навіть найслабшому рівню нерозрізненості IND-CPA [1].

Доведення:
Нехай $(\mathsf{pk}, \mathsf{sk}) = ((n, e), d)$ – ключова пара RSA. Розглянемо супротивника $\mathcal{A}$, який:

1. Вибирає повідомлення m_0, m_1;
2. Отримує challenge-шифротекст $c^* = m_b^e \pmod n$;
3. Обчислює $c_0 = m_0^e \pmod n$;
4. Якщо $c^* = c_0$, виводить $b' = 0$, інакше $b' = 1$.

Оскільки RSA є детермінованим алгоритмом, то зловмисник $\mathcal{A}$ вгадує правильно з ймовірністю $\mathsf{Adv}^{\mathsf{IND-CPA}}_{\mathsf{RSA},\mathcal{A}} = 1/2$. Окрім цього, Textbook RSA має властивість *мультиплікативності*, що робить її вразливою до атак на перетворення (NM-CPA) [18, 19].

$$\mathsf{Enc}(m_1) \cdot \mathsf{Enc}(m_2) = m_1^e \cdot m_2^e = (m_1 \cdot m_2)^e = \mathsf{Enc}(m_1 \cdot m_2) \pmod n,$$

□

ElGamal

Схема ElGamal є прикладом криптосистеми, яка задовольняє IND-CPA, але не задовольняє IND-CCA1 [20].

Твердження 1.8.4 (Стійкість ElGamal [21])**.**
Схема ElGamal є IND-CPA стійкою за припущення DDH, але не є IND-CCA2 стійкою (і, як наслідок, не є IND-CCA1 стійкою).

Доведення: Нехай $\mathsf{pk} = (G, g, h = g^x)$. Супротивник $\mathcal{A}$ діє наступним чином:

1. Вибирає два повідомлення $m_0, m_1 \in G$;
2. Отримує challenge-шифротекст $c^* = (c_1, c_2) = (g^r, m_b \cdot h^r)$;
3. Формує модифікований шифротекст $c' = (c_1, c_2 \cdot g) = (g^r, m_b \cdot h^r \cdot g)$;
4. Запитує $\mathsf{Dec}(c')$ у фазі після отримання c^* (це дозволено в CCA-2, оскільки $c' \neq c^*$);
5. Отримує $m' = m_b \cdot g$ та обчислює $m_b = m' \cdot g^{-1}$;
6. Виводить $b' = 0$, якщо $m_b = m_0$, інакше $b' = 1$.

Супротивник вгадує правильно з ймовірністю $\mathsf{Adv}^{\mathsf{IND-CCA2}} = 1/2$. $\square$

Ця вразливість пов'язана з malleability. Якщо $(c_1, c_2) = (g^r, m \cdot h^r)$ є шифротекстом для m, то для будь-якого відомого $\delta \in G$:

$$(c_1, c_2 \cdot \delta) = (g^r, m \cdot \delta \cdot h^r) = \mathsf{Enc}(m \cdot \delta),$$

тобто можна отримати валідний шифротекст для $m \cdot \delta$ без знання m. Ця властивість є наслідком мультиплікативності алгоритму ElGamal:

$$\mathsf{Enc}(m_1) \cdot \mathsf{Enc}(m_2) = (g^{r_1+r_2}, m_1 \cdot m_2 \cdot h^{r_1+r_2}) = \mathsf{Enc}(m_1 \cdot m_2).$$

1.8.3 Порівняльна таблиця перелічених алгоритмів

Крипто-примітив	**OW-CPA**	**IND-CPA**	**IND-CCA1**	**IND-CCA2**	**NM-CPA**	**NM-CCA2**
RSA-OAEP	Так	Так	Так	Так***	Так	Так***
Cramer–Shoup	Так	Так	Так	Так**	Так	Так**
ML-KEM (Kyber)	Так	Так	Так	Так*	Так	Так*
Textbook RSA	Так*	Ні	Ні	Ні	Ні	Ні
ElGamal	Так	Так**	Ні†	Ні	Ні	Ні

* — за припущення складності RSA-задачі; ** — за припущення DDH; *** — у моделі випадкового оракула; $\star$ – за припущення MLWE.
† — для ElGamal доведено нестійкість до CCA-2; нестійкість до CCA-1 не має явної простої атаки, але й доказу стійкості немає.

Таблиця 1.3: Порівняння рівнів стійкості криптопримітивів

Можна підбити коротенький підсумок:

1. Ієрархія рівнів стійкості: IND-CCA2 (еквівалентно NM-CCA2) є найвищим рівнем стійкості для схем асиметричного шифрування та механізмів інкапсуляції ключів.
2. Нерозрізненість та семантична стійкість еквівалентні для всіх розглянутих моделей атак (CPA, CCA-1, CCA-2).
3. Для CCA-2 атак IND та NM еквівалентні, але для CPA атак NM є строго сильнішою вимогою.
4. Сучасні криптосистеми (RSA-OAEP, Cramer–Shoup, ML-KEM) розробляються з метою досягнення IND-CCA2 стійкості так званого "золотого стандарту" безпеки.
5. Приклад Textbook RSA демонструє критичну важливість використання падінгу як такового для досягнення навіть найбазовіших рівнів стійкості.

Розділ 2

Рівні стійкості схем цифрового підпису

Схеми цифрового підпису(ЦП) є фундаментальним криптографічним примітивом, що забезпечує автентичність та цілісність повідомлень [2, 22]. На відміну від схем шифрування, де основною метою є конфіденційність, для схем підпису ключовою властивістю є захист від підробок (unforgeability) – неможливість створення валідного підпису без знання секретного ключа [23].

Формально, схема цифрового підпису складається з трьох алгоритмів [1]:

$\Sigma = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$:

- $\mathsf{KeyGen}(1^\lambda) \to (\mathsf{pk}, \mathsf{sk})$ — генерація ключової пари;
- $\mathsf{Sign}_{\mathsf{sk}}(m) \to \sigma$ — створення підпису для повідомлення m;
- $\mathsf{Verify}_{\mathsf{pk}}(m, \sigma) \to \{0, 1\}$ — перевірка підпису.

2.1 Моделі атак на схеми цифрового підпису

Існують багато рівнів стійкості, розглянемо два основних – універсальна непідробність (universal unforgeability, UU) та екзистенційна непідробність (existential unforgeability, EU). Їх доцільно розглядати в контексті різних моделей атак, наприклад: KOA (key-only attack), RMA (random message attack) та CPA (chosen message attack). Моделі атак на схеми ЦП класифікуються за обсягом інформації, яка доступна супротивнику [1, 23].

2.1.1 Атака лише з відкритим ключем (KOA)

В моделі KOA (Key-Only Attack) супротивник має доступ лише до відкритого ключа pk. Це найслабша модель атаки, оскільки супротивник не має жодних прикладів валідних підписів [23].

Означення 2.1.1 (KOA-супротивник)**.**

KOA це PPT *(Probabilistic Polynomial-Time)-алгоритм $\mathcal{A}$, який отримує на вхід лише відкритий ключ користувача* pk *та намагається створити валідний підпис.*

2.1.2 Атака з випадково обраними повідомленнями (RMA)

В моделі RMA (Random Plaintext Attack), також відомій як KPA (Known Plaintext Attack), супротивник перехоплює набір пар (m_i, σ_i), де повідомлення m_i обрані випадковим чином [23].

Означення 2.1.2 (RMA-супротивник)**.**

RMA-супротивником називається PPT*-алгоритм $\mathcal{A}$, який отримує:*

- *відкритий ключ* pk*;*
- *набір пар* $\{(m_1, \sigma_1), \ldots, (m_q, \sigma_q)\}$, *де* $m_i \overset{p}{\leftarrow} \mathcal{M}$ *та* $\sigma_i = \mathsf{Sign}_{\mathsf{sk}}(m_i)$.

2.1.3 Атака на основі вибраного plaintext (CPA)

Модель CPA (Chosen Plaintext Attack) є найсильнішою стандартною моделлю атаки. Супротивник має адаптивний (ґрунтуючись на попередньо отриманих результатах) оракульний доступ до функції підпису $\mathsf{Sign}_{\mathsf{sk}}(\cdot)$ і може запитувати підписи для довільних повідомлень за власним вибором [23].

Означення 2.1.3 (CPA-супротивник)**.**
CPA-супротивником називається такий поліноміальний алгоритм $\mathcal{A}^{\mathsf{Sign}_{\mathsf{sk}}(\cdot)}$, *який:*

- *отримуючи відкритий ключ* pk*;*
- *і маючи адаптивний оракульний доступ до* $\mathsf{Sign}_{\mathsf{sk}}(\cdot)$*;*
- *може робити поліноміальну кількість запитів до оракула для витягання деталей про* sk.

Всі перелічені атаки можна ґарненько звести до таблиці 2.1.

Преференція	**KOA**	**RMA**	**CPA**
Sign examples	Ні	Так (випадкові m_i)	Так (обрані m_i)
Адаптивність запитів	Ні	Ні	Так
Загроза	Найслабша	Середня	Найсильніша

Таблиця 2.1: Порівняння моделей атак на схему цифрового підпису

Ієрархія моделей атак

Між моделями атак існує певна ієрархія залежно від їх сили [23]:

$$\mathsf{CPA} \succ \mathsf{RMA} \succ \mathsf{KOA},$$

де під позначенням $A \succ B$ розуміємо, що модель A надає супротивнику більше можливостей, ніж модель B. І відповідно стійкість до більш сильної атаки (позначимо її X) включає в себе і стійкість до слабшої:

$$X\text{-}\mathsf{CPA} \Rightarrow X\text{-}\mathsf{RMA} \Rightarrow X\text{-}\mathsf{KOA}$$

2.2 Рівні непідробності

Рівні непідробності розрізняють залежно від того, що саме вважається успішною підробкою. Розглянемо три основні види.

2.2.1 Універсальна непідробність (Universal Unforgeability)

Універсальна непідробність (UU) вимагає, щоб супротивник не міг підробити підпис для *заданого* повідомлення m^*, яке обирається челенджером [23].

Означення 2.2.1 (UU-ATK стійкість)**.**

Схема підпису $\Sigma = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ *називається UU-ATK стійкою, де* $\mathsf{ATK} \in \{\mathsf{KOA}, \mathsf{RMA}, \mathsf{CPA}\}$*, якщо для будь-якого* PPT*-супротивника* $\mathcal{A}$*:*

$$\mathsf{Adv}^{\mathsf{UU-ATK}}_{\Sigma,\mathcal{A}}(\lambda) = \Pr\left[\mathsf{Verify}_{\mathsf{pk}}(m^*, \sigma^*) = 1 : \substack{(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda) \\ m^* \overset{p}{\leftarrow} \mathcal{M} \\ \sigma^* \leftarrow \mathcal{A}^{\mathcal{O}}(\mathsf{pk}, m^*)}\right] \leq \mathsf{negl}(\lambda),$$

де $\mathcal{O}$ *– оракул, визначений моделлю ATK.*

P.S. В моделі CPA супротивник не може запитувати $\mathsf{Sign}_{\mathsf{sk}}(m^*)$.

Алгоритм ”гри” UU-CPA наведемо в алгоритмі 4.

Algorithm 4 Game UU-CPA для схеми цифрового підпису

Require: Параметр безпеки 1^λ
Ensure: Біт $b \in \{0, 1\}$

$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$
$m^* \overset{p}{\leftarrow} \mathcal{M}$ ▷ Челенджер обирає цільове повідомлення
$Q \leftarrow \emptyset$ ▷ Множина запитаних повідомлень
$\sigma^* \leftarrow \mathcal{A}^{\mathsf{Sign}_{\mathsf{sk}}(\cdot)}(\mathsf{pk}, m^*)$ ▷ $\mathcal{A}$ не може запитувати $\mathsf{Sign}_{\mathsf{sk}}(m^*)$
if $\mathsf{Verify}_{\mathsf{pk}}(m^*, \sigma^*) = 1$ **and** $m^* \notin Q$ **then**
    return 1 ▷ Успішна підробка підпису
else
    return 0
end if

2.2.2 Екзистенційна непідробність (Existential Unforgeability)

Екзистенційна несфальсифікованість (EU) є більш сильним поняттям. Вона вимагає, щоб супротивник не міг підробити підпис для *будь-якого* повідомлення, яке підписант раніше не підписував [24]. Це є ”золотим стандартом” безпеки для цифрових підписів.

Означення 2.2.2 (EU-ATK стійкість)**.**

Схема підпису Σ *є EU-ATK стійкою, якщо для будь-якого* PPT*-algorithm* $\mathcal{A}$*:*

$$\mathsf{Adv}^{\mathsf{EU-ATK}}_{\Sigma,\mathcal{A}}(\lambda) = \Pr\left[\substack{\mathsf{Verify}_{\mathsf{pk}}(m^*,\sigma^*)=1 \\ \wedge\, m^* \notin Q} : \substack{(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda) \\ (m^*,\sigma^*) \leftarrow \mathcal{A}^{\mathcal{O}}(\mathsf{pk})}\right] \leq \mathsf{negl}(\lambda),$$

де Q *– множина повідомлень, для яких атакуючий* $\mathcal{A}$ *отримав підписи.*

EU-CPA також доволі часто позначають в літературі як EUF-CMA (Existential Unforgeability under Chosen Message Attack) [1].

Algorithm 5 Game EU-CPA (EUF-CPA) для схеми цифрового підпису

Require: Параметр безпеки 1^λ, супротивник $\mathcal{A}$
Ensure: Біт $b \in \{0,1\}$

```
(pk, sk) ← KeyGen(1^λ)
Q ← ∅
(m*, σ*) ← A^{Sign_sk(·)}(pk)                ▷ A сам обирає m*
if Verify_pk(m*, σ*) = 1 and m* ∉ Q then
    return 1                                 ▷ Успішна підробка
else
    return 0
end if
```

2.2.3 Сильна екзистенційна непідробність (sEU)

Виділяють також ще одне поняття – *сильна екзистенційна непідробність* (Strong Unforgeability under Chosen Message Attack, sEU a.k.a. SUF), яке додатково запобігає підробці зловмисником дійсного підпису для будь-якого нового повідомлення, включаючи те, яке вже було підписано законним підписувачем [25].

Означення 2.2.3 (sEU-CPA стійкість)**.**
Схема Σ *є sEU-CPA стійкою, якщо супротивник не може створити таку пару* (m^*, σ^*)*, що* $\mathsf{Verify}_{\mathsf{pk}}(m^*, \sigma^*) = 1 \wedge (m^*, \sigma^*) \notin Q$*, де* Q *– множина всіх пар (повідомлення, підпис), отриманих від оракула.*

Зв'язок між рівнями непідробності

Для фіксованого типу атаки ATK [23, 1]:

$$\mathsf{sEU\text{-}ATK} \Rightarrow \mathsf{EU\text{-}ATK} \Rightarrow \mathsf{UU\text{-}ATK}.$$

Ці імплікації є строгими – зворотні імплікації не виконуються в загальному випадку.

2.3 Ієрархія рівнів стійкості

Найвищим стандартним рівнем стійкості для схем цифрового підпису вважають sEU-CPA (SUF-CPA), а практичним "золотим стандартом" є EU-CPA (EUF-CPA) [1].

Повна ієрархія рівнів стійкості для схем підпису зображена на рисунку 2.1.

$$
\begin{tikzcd}
\boxed{\text{sEU-CPA}} \arrow[r] \arrow[d] & \boxed{\text{sEU-RMA}} \arrow[r] \arrow[d] & \boxed{\text{sEU-KOA}} \arrow[d] \\
\boxed{\text{EU-CPA}} \arrow[r] \arrow[d] & \boxed{\text{EU-RMA}} \arrow[r] \arrow[d] & \boxed{\text{EU-KOA}} \arrow[d] \\
\boxed{\text{UU-CPA}} \arrow[r] & \boxed{\text{UU-RMA}} \arrow[r] & \boxed{\text{UU-KOA}}
\end{tikzcd}
$$

Рис. 2.1: Ієрархія рівнів стійкості схем цифрового підпису. Стрілки позначають імплікації (від сильнішого до слабшого).

2.4 Приклади криптопримітивів

2.4.1 Схеми з доведеною EU-CPA стійкістю

RSA-PSS (EU-CPA)

RSA-PSS (Probabilistic Signature Scheme) є стандартизованою схемою підпису, розробленою Белларе та Рогавеєм [26]. На відміну від детермінованого RSA-підпису, PSS використовує рандомізацію. Алгоритм підпису RSA-PSS є наступним:

Algorithm 6 RSA-PSS підпис

Require: Повідомлення m, секретний ключ d, модуль n, геш-функції H, G
Ensure: Підпис σ

$r \xleftarrow{p} \{0,1\}^{k_0}$ ▷ Випадкове значення рандомізації
$w \leftarrow H(m \| r)$
$r^* \leftarrow G(w) \oplus r$
$y \leftarrow 0 \| w \| r^*$
$\sigma \leftarrow y^d \mod n$
return σ

Твердження 2.4.1 (Стійкість RSA-PSS [26]).
RSA-PSS є EU-CPA стійкою в моделі випадкового оракула (Random Oracle Model (ROM)) за припущення складності RSA-задачі.

Schnorr (EU-CPA)

Схема Шнорра є схемою підпису на основі розв'язанні задачі дискретного логарифма [27]. Вона є основою для багатьох сучасних схем підпису, наприклад, EdDSA.

Твердження 2.4.2 (Стійкість Schnorr [28]).
Схема Schnorr є EU-CPA стійкою в моделі випадкового оракула за припущення складності задачі дискретного логарифма (DL).

Схема виглядає наступним чином:

Algorithm 7 Схема підпису Schnorr

Генерація ключів $\mathsf{KeyGen}(1^\lambda)$:

$x \xleftarrow{\$} \mathbb{Z}_q$

return $(\mathsf{pk} = g^x,\ \mathsf{sk} = x)$

Підпис $\mathsf{Sign}_{\mathsf{sk}}(m)$:

$k \xleftarrow{\$} \mathbb{Z}_q$

$r \leftarrow g^k$

$e \leftarrow H(r \| m)$

$s \leftarrow k + x \cdot e \mod q$

return $\sigma = (e, s)$

Верифікація $\mathsf{Verify}_{\mathsf{pk}}(m, \sigma = (e, s))$:

$r' \leftarrow g^s \cdot \mathsf{pk}^{-e}$

return $(H(r' \| m) \stackrel{?}{=} e)$

ECDSA (EU-CPA)

Згадана мною раніше ECDSA (Elliptic Curve Digital Signature Algorithm) є широко використовуваною схемою підпису, стандартизованою у вже застарілому FIPS 186-4 [29]. (Буквально на початку 2024 року вийшло оновлення)

Твердження 2.4.3 (Стійкість ECDSA [30])**.**
ECDSA є EU-CPA стійкою в моделі generic group за припущення складності ECDLP (Elliptic Curve Discrete Logarithm Problem).

ML-DSA (Dilithium) – постквантовий підпис

ML-DSA (Module-Lattice-based Digital Signature Algorithm), раніше відомий як CRYSTALS-Dilithium, є стандартизованим NIST постквантовим підписом (той самий новий, 24 року стандарт) [31].

Він є EU-CPA стійким у припущені складності задач MLWE (learning with errors) та MSIS (short integer solution).

Список використаних джерел

[1] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. 2nd ed. Boca Raton, FL: CRC Press, 2020. ISBN: 978-0815354369.

[2] Oded Goldreich. *Foundations of Cryptography: Volume 1, Basic Tools*. Cambridge, UK: Cambridge University Press, 2001. ISBN: 978-0521035361.

[3] Mihir Bellare et al. "Relations Among Notions of Security for Public-Key Encryption Schemes". In: *Advances in Cryptology – CRYPTO '98*. Vol. 1462. Lecture Notes in Computer Science. Springer, 1999, pp. 26–45. DOI: 10.1007/BFb0055718.

[4] Shafi Goldwasser and Silvio Micali. "Probabilistic Encryption". In: *Journal of Computer and System Sciences*. Vol. 28. 2. 1984, pp. 270–299. DOI: 10.1016/0022-0000(84)90070-9.

[5] Alfred J. Menezes, Paul C. van Oorschot, and Scott Vanstone. *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 1996. ISBN: 978-0849385230.

[6] Moni Naor and Moti Yung. "Public-Key Cryptosystems Provably Secure against Chosen Ciphertext Attacks". In: *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*. STOC '90. ACM, 1990, pp. 427–437. DOI: 10.1145/100216.100273.

[7] Charles Rackoff and Daniel R. Simon. "Non-Interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack". In: *Advances in Cryptology – CRYPTO '91*. Vol. 576. Lecture Notes in Computer Science. Springer, 1991, pp. 433–444. DOI: 10.1007/3-540-46766-1_35.

[8] Victor Shoup. "A Proposal for an ISO Standard for Public Key Encryption". In: *IACR Cryptology ePrint Archive*. 2001. URL: https://eprint.iacr.org/2001/112.

[9] Silvio Micali, Charles Rackoff, and Bob Sloan. "The Notion of Security for Probabilistic Cryptosystems". In: *SIAM Journal on Computing* 17.2 (1988), pp. 412–426. DOI: 10.1137/0217025.

[10] Danny Dolev, Cynthia Dwork, and Moni Naor. "Non-Malleable Cryptography". In: *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*. STOC '91. ACM, 1991, pp. 542–552. DOI: 10.1145/103418.103474.

[11] Mihir Bellare and Amit Sahai. "Non-Malleable Encryption: Equivalence between Two Notions, and an Indistinguishability-Based Characterization". In: *Advances in Cryptology – CRYPTO '99*. Vol. 1666. Lecture Notes in Computer Science. Springer, 1999, pp. 519–536. DOI: 10.1007/3-540-48405-1_33.

[12] Mihir Bellare and Phillip Rogaway. "Optimal Asymmetric Encryption". In: *Advances in Cryptology – EUROCRYPT '94*. Vol. 950. Lecture Notes in Computer Science. Springer, 1994, pp. 92–111. DOI: 10.1007/BFb0053428.

[13] Eiichiro Fujisaki et al. “RSA-OAEP Is Secure under the RSA Assumption”. In: *Journal of Cryptology* 17.2 (2004), pp. 81–104. DOI: 10.1007/s00145-002-0204-y.

[14] Ronald Cramer and Victor Shoup. “A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack”. In: *Advances in Cryptology – CRYPTO ’98*. Vol. 1462. Lecture Notes in Computer Science. Springer, 1998, pp. 13–25. DOI: 10.1007/BFb0055717.

[15] Ronald Cramer and Victor Shoup. “Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack”. In: *SIAM Journal on Computing* 33.1 (2003), pp. 167–226. DOI: 10.1137/S0097539702403773.

[16] National Institute of Standards and Technology. *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. Federal Information Processing Standards Publication FIPS 203. NIST, 2024. DOI: 10.6028/NIST.FIPS.203.

[17] Roberto Avanzi et al. “CRYSTALS-Kyber: Algorithm Specifications and Supporting Documentation”. In: *NIST Post-Quantum Cryptography Standardization*. Round 3 Submission. 2021. URL: https://pq-crystals.org/kyber/.

[18] Dan Boneh. “Twenty Years of Attacks on the RSA Cryptosystem”. In: *Notices of the American Mathematical Society* 46.2 (1999), pp. 203–213.

[19] Daniel Bleichenbacher. “Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1”. In: *Advances in Cryptology – CRYPTO ’98*. Vol. 1462. Lecture Notes in Computer Science. Springer, 1998, pp. 1–12. DOI: 10.1007/BFb0055716.

[20] Taher ElGamal. “A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms”. In: *IEEE Transactions on Information Theory* 31.4 (1985), pp. 469–472. DOI: 10.1109/TIT.1985.1057074.

[21] Yiannis Tsiounis and Moti Yung. “On the Security of ElGamal Based Encryption”. In: *Public Key Cryptography – PKC ’98*. Vol. 1431. Lecture Notes in Computer Science. Springer, 1998, pp. 117–134. DOI: 10.1007/BFb0054019.

[22] Oded Goldreich. *Foundations of Cryptography: Volume 2, Basic Applications*. Cambridge, UK: Cambridge University Press, 2004. ISBN: 978-0521830843.

[23] Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. “A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks”. In: *SIAM Journal on Computing* 17.2 (1988), pp. 281–308. DOI: 10.1137/0217017.

[24] Jason Chia, Ji-Jian Chin, and Sook-Chin Yip. “Digital signature schemes with strong existential unforgeability”. In: *F1000Research* 10 (Sept. 2021). ISSN: 2046-1402. DOI: 10.12688/f1000research.72910.1.

[25] Michel Abdalla et al. “From Identification to Signatures via the Fiat-Shamir Transform: Minimizing Assumptions for Security and Forward-Security”. In: *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology*. EUROCRYPT ’02. Berlin, Heidelberg: Springer-Verlag, 2002, pp. 418–433. ISBN: 3540435530. URL: https://dl.acm.org/doi/10.5555/647087.715838.

[26] Mihir Bellare and Phillip Rogaway. "The Exact Security of Digital Signatures – How to Sign with RSA and Rabin". In: *Advances in Cryptology – EUROCRYPT '96*. Vol. 1070. Lecture Notes in Computer Science. Springer, 1996, pp. 399–416. DOI: 10.1007/3-540-68339-9_34.

[27] Claus-Peter Schnorr. "Efficient Signature Generation by Smart Cards". In: *Journal of Cryptology*. Vol. 4. 3. 1991, pp. 161–174. DOI: 10.1007/BF00196725.

[28] David Pointcheval and Jacques Stern. "Security Proofs for Signature Schemes". In: *Advances in Cryptology – EUROCRYPT '96*. Vol. 1070. Lecture Notes in Computer Science. Springer, 1996, pp. 387–398. DOI: 10.1007/3-540-68339-9_33.

[29] National Institute of Standards and Technology. *Digital Signature Standard (DSS)*. Federal Information Processing Standards Publication FIPS 186-4. NIST, 2013. DOI: 10.6028/NIST.FIPS.186-4.

[30] Daniel R. L. Brown. "Generic Groups, Collision Resistance, and ECDSA". In: *Designs, Codes and Cryptography* 35.1 (Apr. 2005), pp. 119–152. DOI: 10.1007/s10623-003-6154-z.

[31] National Institute of Standards and Technology. *Module-Lattice-Based Digital Signature Standard*. Federal Information Processing Standards Publication FIPS 204. NIST, 2024. DOI: 10.6028/NIST.FIPS.204.