УДК 004.056.55 DOI: 10.46972/2076-1546.2019.16.02

М. В. Єсіна, С. Г. Вдовенко, І. Д. Горбенко

МОДЕЛІ БЕЗПЕКИ ПОСТКВАНТОВИХ АСИМЕТРИЧНИХ ШИФРІВ НА ОСНОВІ НЕРОЗРІЗНЮВАНОСТІ

У статті подано доведення еквівалентності властивості нерозрізнюваності (невизначеності) властивості семантичної безпеки для захисту криптосистем від криптоаналізу зловмисника на основі підібраного (вибраного) відкритого тексту.

Питання аналізу й дослідження моделей безпеки постквантових криптоалгоритмів відносно криптопримітивів усіх типів, визначення критеріїв оцінки їх відповідності різним моделям безпеки (згідно з різними типами криптоперетворень) є актуальними та такими, що мають практичне значення. Нерозрізнюваність (невизначеність) зашифрованого тексту – це важлива властивість безпеки багатьох схем шифрування, яка в разі атаки на основі підібраного (вибраного) відкритого тексту вважається основною вимогою для більшості достовірно захищених криптосистем із відкритим ключем. Деякі схеми також забезпечують нерозрізнюваність у ході атак на основі підібраного (вибраного) та адаптивно підібраного (вибраного) зашифрованого тексту. Використання властивості нерозрізнюваності (невизначеності) зашифрованого тексту на даний час дозволяє гарантовано здійснити захист усіх відомих симетричних та асиметричних криптосистем від класичного чи квантового криптоаналізу зловмисника.

Запропоновано три моделі безпеки, що стосуються шифрування, електронного підпису та механізмів інкапсуляції ключів. Розглянуті найпоширеніші сучасні види атак на безпеку механізмів шифрування, а саме: атака на основі адаптивно підібраних (вибраних) шифртекстів; атака на основі адаптивно підібраних (вибраних) відкритих текстів; атака на основі адаптивно підібраних (вибраних) відкритих текстів та адаптивно підібраних (вибраних) шифртекстів; атака на основі підібраних (вибраних) шифртекстів; атака на основі підібраних (вибраних) відкритих текстів; атака на основі підібраних (вибраних) відкритих текстів та підібраних (вибраних) шифртекстів; атаки розрізнення (розрізнюваності).

Ключові слова: *атака на основі адаптивно підібраних (вибраних) шифр текстів; атака на основі підібраних (вибраних) відкритих текстів; нерозрізнюваність (невизначеність) зашифрованого тексту; нерозрізнюваність ключів.*

Постановка проблеми в загальному вигляді. Національний інститут стандартів і технології (NIST) США проводить конкурс на постквантові криптографічні алгоритми. У критеріях відбору кандидатів є пункт, що стосується моделей безпеки, а саме: кожен тип криптоалгоритму повинен відповідати певній моделі безпеки. NIST наводить три моделі безпеки, що стосуються шифрування, електронного підпису та механізмів інкапсуляції ключів: моделі *IND-CPA*, *IND-CCA*, *IND-CCA2* стосуються механізмів шифрування; модель *EUF-CMA* – механізмів підпису; модель *CK* – механізмів інкапсуляції ключів. Тому актуальною є проблема узагальненого визначення та дослідження моделей безпеки щодо криптопримітивів усіх типів, зокрема визначення

умов застосування постквантових асиметричних шифрів у процесі здійснення класичного чи квантового криптоаналізу.

У термінах моделей безпеки щодо криптоперетворень асиметричного шифрування існують такі атаки: на основі адаптивно підібраних (вибраних) шифртекстів; на основі адаптивно підібраних (вибраних) відкритих текстів; на основі адаптивно підібраних (вибраних) відкритих текстів та адаптивно підібраних (вибраних) шифртекстів; на основі підібраних (вибраних) шифртекстів; на основі підібраних (вибраних) відкритих текстів; на основі підібраних (вибраних) відкритих текстів та підібраних (вибраних) шифртекстів; атаки розрізнення (розрізнюваності).

Нерозрізнюваність (невизначеність) у разі атаки на основі підібраного (вибраного) відкритого тексту еквівалентна властивості семантичної безпеки, тому багато криптографічних доказів використовують ці визначення як еквівалентні Якщо криптосистема володіє властивістю нерозрізнюваності, то зловмисник не зможе відрізнити пари шифрованих текстів на основі повідомлення, що вони шифрують [1].

Аналіз останніх досліджень і публікацій. Властивість нерозрізнюваності (невизначеності) розглянута в роботах Х. ван Тілборга та М. Білара [2, 5]. В опублікованих роботах не досліджено питання умов використання властивості нерорізнюваності (невизначеності) для захисту асиметричних криптосистем від класичного чи квантового криптоаналізу зловмисника.

Формулювання завдання. Метою статті є доведення еквівалентності властивості нерозрізнюваності (невизначеності) властивості семантичної безпеки для захисту криптосистем від криптоаналізу зловмисника на основі підібраного (вибраного) відкритого тексту.

Виклад основного матеріалу

1. Рекомендовані позначення та скорочення

Наведемо дефініції, позначення, допоміжні (довідкові) визначення та короткий опис атак у термінах цих моделей безпеки [2, 3].

IND – нерозрізнюваність (Indistinguishability);

IK – нерозрізнюваність ключів (Indistinguishability of keys);

IE – нерозрізнюваність зашифрованих текстів (Indistinguishability of encryptions);

CPA – атака на основі підібраних (вибраних) відкритих повідомлень (Chosen plaintext attack);

CCA2 – атака на основі адаптивно підібраних (вибраних) шифртекстів (Adaptive chosen ciphertext attack);

IE-CPA – нерозрізнюваність шифртекстів (зашифрованих текстів) у разі атаки на основі підібраних (вибраних) відкритих текстів;

IE-CCA – нерозрізнюваність шифртекстів (зашифрованих текстів) у разі атаки на основі підібраних (вибраних) шифртекстів.

PKE є *IND-CPA*, якщо шифртекст не розкриває жодної інформації про відкритий текст.

Оракул – це третя сторона, з якою ви спілкуєтеся, коли вам потрібні дані, які ви не хочете або не можете отримати самостійно. Це сторона, яка відповідає за підключення до джерела даних.

Роль оракула розшифрування може грати наївний користувач, змушений розшифровувати повідомлення зловмисника.

Випадковий оракул є потужною гіпотетичною детермінованою функцією, що ефективно обчислює рівномірно розподілені випадкові величини. Він точно імітується поліноміально обмеженим алгоритмом.

Модель із випадковим оракулом (*RAM*) – розширена математична модель криптографічного протоколу, у якій усі учасники мають доступ до оракула, що обчислює випадкову функцію. При кожному новому запиті значення функції на заданому аргументі вибирається випадковим чином. При цьому оракул запам'ятовує пару (аргумент – значення), у разі повторного запиту для цього аргументу, незалежно від того, хто з учасників його видав, буде повернено те ж саме запам'ятоване значення.

Оракул зашифрування забезпечує зашифрування запитуваного відкритого тексту, а оракул розшифрування – розшифрування запитуваного шифртексту.

2. Визначення моделі безпеки та нерозрізнюваності

Криптосистема вважається безпечною щодо нерозрізнюваності, якщо жоден зловмисник *A*, отримавши зашифрований текст, довільно вибраний з двоелементного простору повідомлень, визначеного ним самим, не може ідентифікувати свій вибір з імовірністю значно кращою, ніж у разі випадкових вгадувань (½). Якщо будь-який зловмисник може вдало відрізнити вибраний шифрований текст з імовірністю значно більшою, ніж ½, тоді він вважається таким, що має «перевагу» в розрізненні шифрованого тексту, а схема «не» вважається безпечною щодо нерозрізнюваності [1].

Безпека щодо нерозрізнюваності (невизначеності) розуміється як гра, де криптосистема вважається безпечною, якщо жоден зі зловмисників не може її виграти з значно більшою ймовірністю, ніж опонент, який повинен вгадати випадковим чином.

Найпоширеніші поняття, використовувані в криптографії [1, 2]:

нерозрізненість у разі атаки на основі підібраного (вибраного) відкритого тексту (*IND-CPA* безпека);

нерозрізненість у разі атаки на основі підібраного (вибраного) шифртексту (*IND-CCA* безпека);

нерозрізненість у разі атаки на основі адаптивно підібраного (вибраного) шифртексту (*IND-CCA2* безпека).

Безпека за будь-яким з останніх визначень передбачає безпеку за попередніми [1]:

схема, яка є *IND-CCA*-безпечною, також є *IND-CPA*-безпечною;

схема, яка *IND-CCA2*-безпечна, є як *IND-CCA*-безпечною, так і *IND-CPA*-безпечною.

Отже, *IND-CCA2* є найсуворішим із цих трьох визначень безпеки.

У разі нерозрізнюваності (невизначеності) відбувається захист від зловмисника *A*, який [4]: є ймовірнісною машиною Тюрінга поліноміального часу; має всі алгоритми; має повний доступ до засобів зв'язку.

3. Поняття семантичної безпеки

Семантична безпека – це поняття, яке описує безпеку схеми шифрування, позначається як *SEM-CPA* та фіксує ідею, що безпечна схема шифрування повинна приховувати всю інформацію про невідомий відкритий текст.

Зловмиснику дозволяється вибирати між двома відкритими текстами (m_0 та m_1), і він отримує зашифрування будь-якого з відкритих текстів.

Схема шифрування є семантично безпечною, якщо зловмисник не може здогадатися з кращою ймовірністю, ніж ½, чи даний шифртекст є зашифруванням повідомлення m_0 або m_1.

За Shannon схема шифрування є безпечною, якщо те, що можна визначити про відкритий текст із його шифртекстів, можна визначити за їх відсутності. Семантична безпека вимагає, щоб те, що можна ефективно обчислювати щодо деяких відкритих текстів з їх шифртекстів, можна було обчислювати так само легко, як за їх відсутності [5].

Поняття семантичної безпеки можна застосувати як до симетричних криптосистем, так і до криптосистем із відкритим ключем. Але, оскільки конкретний аналіз безпеки схеми шифрування на відкритому ключі є більш важливим, цей термін частіше використовується для обговорення безпеки схем шифрування з відкритим ключем [2].

Окрім семантичної безпеки, існують пов'язані поняття: «непідробленість» (Non-Malleability) та «поінформованість про відкритий текст» (Plaintext Awareness) [2].

Визначення 1. [Семантична безпека]. Нехай $SE=(K,E,D)$ – схема симетричного зашифрування; A – алгоритм, який має доступ до оракула. Розглянемо такі експерименти в сценарії семантичної безпеки [5]:

$Experiment\ Exp_{SE}^{SS\text{-}CPA\text{-}1}(A)$
$K \xleftarrow{\$} K, s \xleftarrow{\$} \varepsilon$
$for\ \ i \xleftarrow{} 1\ \ to\ \ q\ \ do$
$(M_{i,s}) \xleftarrow{\$} A(s)$
$M_i, M_i' \xleftarrow{\$} M_i$
$if\ |M_i| \neq M_i'\ \ then\ M_i \xleftarrow{} M_i' \xleftarrow{} \varepsilon$
$C_i \xleftarrow{\$} \varepsilon_K(M_i);\ s \xleftarrow{} \langle s, C_i \rangle$
$(f,Y) \xleftarrow{\$} A(s)$
$return\ f(M_1,...,M_q) = Y,$

$Experiment\ Exp_{SE}^{SS\text{-}CPA\text{-}0}(A)$
$K \xleftarrow{\$} K, s \xleftarrow{\$} \varepsilon$
$for\ \ i \xleftarrow{} 1\ \ to\ \ q\ \ do$
$(M_{i,s}) \xleftarrow{\$} A(s)$
$M_i, M_i' \xleftarrow{\$} M_i$
$if\ |M_i| \neq M_i'\ \ then\ M_i \xleftarrow{} M_i' \xleftarrow{} \varepsilon$
$C_i \xleftarrow{\$} \varepsilon_K(M_i');\ s \xleftarrow{} \langle s, C_i \rangle$
$(f,Y) \xleftarrow{\$} A(s)$
$return\ f(M_1,...,M_q) = Y.$

SEM-CPA перевагу алгоритму A визначаємо за таким виразом:

$$Adv_{SE}^{SEM-CPA}(A) = Pr[Exp_{SE}^{SS-CPA-1}(A) \Rightarrow 1] - Pr[Exp_{SE}^{SS-CPA-0}(A) \Rightarrow 1].$$

Отже, кожен експеримент ініціалізує свій оракул, вибравши випадковий ключ K. Усього q раз зловмисник вибирає простір повідомлень M_i, визначений імовірнісним алгоритмом, який завжди зупиняється (always-halting), написаним деякою фіксованою мовою програмування. Код для цього алгоритму – те, що насправді отримує зловмисник. Щоразу, коли виводиться простір повідомлення, дві випадкові вибірки M_i та M'_i виділяються з нього. Очікується, що M_i та M'_i мають однакову довжину, і якщо це не так, то обидва рядки «стираються». Зашифрування одного із цих повідомлень буде повернуто зловмиснику. Те, який рядок зашифрований, залежить від експерименту: M_i для експерименту 1 та M'_i для експерименту 0. За допомогою f позначають детерміністичну функцію. Її описує програма, яка завжди зупиняється (always-halting). Це програма для f, яку виводить зловмисник. За допомогою Y позначається рядок. Рядок s описує збережений стан, який за бажанням зловмисник може бути збережено.

Говорячи про термін виконання *A*, крім реального строку виконання, враховується ще максимальний час для виділення двох вибірок із кожного простору повідомлення *M*, що *A* виводить, і максимальний час для обчислення $f\left(M_1,...,M_q\right)$ над будь-яким вектором рядків. Характеризуючи довжину запитів *A*, підсумовується за всіма просторами повідомлень, що виводяться *A*, максимальна довжина рядка *M*, що знаходиться з ненульовою ймовірністю за допомогою *M*, і підсумовується також за довжинами кодувань кожного простору повідомлення функцією *f*, а рядок *Y* визначається за допомогою *A*.

Підкреслимо, що сказане вище виглядає як винятково сильне поняття безпеки. Зловмиснику надається можливість вибрати простір повідомлень, з якого буде взято кожне повідомлення. Йому дозволяється виокремити часткову інформацію про повідомлення, яку він вважає придатною для прогнозування. Він може повністю адаптуватися. Також вбудовано здатність виконувати атаку на основі підібраного (вибраного) повідомлення (просто виробляючи алгоритм *M*, який вибирає одну і тільки одну точку). Незважаючи на все це, покажемо далі, що безпека в розумінні нерозрізнюваності означає семантичну безпеку [5].

Теорема 1. [*IND-CPA ⇒SEM-CPA*]

Нехай $SE=\left(K,E,D\right)$ – схема симетричного за шифрування, *A* – зловмисник (для атаки *SEM-CPA* безпеки *SE*), який виконується за максимальний час t та здійснює щонайбільше *q* запитів, які в загальному мають μ бітів. Тоді тут існує і зловмисник *B* (для атаки *IND-CPA* безпеки *SE*), який досягає переваги за рахунок додаткової інформації про відкритий текст (1):

$$Adv_{SE}^{IND-CPA}\left(B\right)\geq Adv_{SE}^{SEM-CPA}\left(A\right), \tag{1}$$

де *B* виконує за час $t + O(\mu)$ щонайбільше *q* запитів, які в загальному мають μ бітів.

Доведення: зловмисника *B*, який має оракул *g*, опишемо за таким алгоритмом:

algoritm B^9

$s \xleftarrow{\$} \varepsilon$

for $i \longleftarrow 1$ *to* q *do*

$\left(M_{i,s}\right) \xleftarrow{\$} A\left(s\right)$

$M_i, M_i' \xleftarrow{\$} M_i$

if $\left|M_i\right| \neq M_i'$ *then* $M_i \longleftarrow M_i' \longleftarrow \varepsilon$

$C_i \longleftarrow g\left(M_i, M'\right),\ s \longleftarrow \left\langle s, C_i\right\rangle$

$\left(f,Y\right) \xleftarrow{\$} A\left(s\right)$

if $f\left(M_1,...,M_q\right)=Y$ *then return 1 else return 0.*

Припустимо спочатку, що *g* підтверджується (вказується) правим оракулом зашифрування, який повертає $C \xleftarrow{\$} E_K(M)$ у відповідь на запит (*M'*, *M*). Тоді алгоритм вище збігається з експериментом $Exp_{SE}^{SS-CPA-1}\left(A\right)$ [5]. Аналогічним чином, якщо *g* підтверджується (вказується) за допомогою лівого оракула зашифрування, то він повертає

$C \xleftarrow{\$} E_K(M')$ у відповідь на запит (M', M), тоді зазначений вище алгоритм збігається з експериментом $Exp_{SE}^{SS-CPA-0}(A)$. Звідси випливає, що $Adv_{SE}^{SEM-CPA}(B) = Adv_{SE}^{IND-CPA}(A)$. Щоб завершити теорему, необхідно звернути увагу на те, що час виконання B – це час виконання A та $O(\mu)$. B характеризує загальну кількість запитів q, загальна довжина яких не перевищує загальної довжини запитів A відповідно до нашої умови [5].

4. Сутність найпоширеніших атак

Розглянемо найпоширеніші сучасні види атак [2] на безпеку механізмів шифрування.

4.1. Атака на основі адаптивно підібраних (вибраних) шифртекстів – це сценарій, у якому зловмисник має можливість підібрати (вибрати) вхідні дані для функції розшифрування на основі попередніх запитів підібраних (вибраних) шифртекстів. Сценарій зазвичай є більш потужним, ніж основна атака на основі підібраних (вибраних) шифртекстів, а отже, менш реалістичним. Проте атака може бути досить практичною в налаштуваннях відкритого ключа. Наприклад, звичайний RSA є вразливим до атаки на основі вибраних (підібраних) шифртекстів, а деякі реалізації RSA можуть бути вразливими до атаки на основі адаптивно підібраних (вибраних) шифртекстів.

4.2. Атака на основі адаптивно підібраних (вибраних) відкритих текстів – це сценарій, у якому зловмисник має можливість підібрати (вибрати) вхідні дані для функції зашифрування на основі попередніх запитів підібраних (вибраних) відкритих текстів та їх відповідних шифртекстів. Сценарій зазвичай є більш потужним, ніж основна атака на базі підібраних (вибраних) відкритих текстів, але, ймовірно, менш практичним у реальному житті, оскільки ця атака вимагає взаємодії того, хто атакує, з пристроєм зашифрування.

4.3. Атака на основі адаптивно підібраних (вибраних) відкритих текстів та шифртекстів дозволяє зловмиснику одночасно застосувати запити на адаптивно підібрані (вибрані) відкриті тексти та адаптивно підібрані (вибрані) шифртексти. Вона є однією з найбільш потужних з огляду на можливості зловмисника.

4.4. Атака на основі підібраних (вибраних) шифртекстів – це сценарій, за якого зловмисник має можливість вибирати шифртексти C_i і переглядати їх відповідні розшифрування – відкриті тексти P_i. Це, по суті, такий самий сценарій, як атака на основі підібраних (вибраних) відкритих текстів, але застосована до функції розшифрування, а не до функції зашифрування. Атака вважається менш практичною в реальних ситуаціях, ніж варіант на основі підібраних (вибраних) відкритих текстів. Проте немає прямих відповідностей між складностями атак на основі підібраних(вибраних) відкритих текстів та підібраних(вибраних) шифртекстів. Шифр може бути вразливим до однієї атаки, але не до іншої або навпаки. Атака на основі підібраних (вибраних) шифртекстів є дуже важливою в криптографії з відкритим ключем, де сценарії відомих відкритих текстів і навіть підібраних (вибраних) відкритих текстів завжди доступні для зловмисника через загальновідомий ключ зашифрування. Наприклад, схема шифрування з відкритим ключем RSA не захищена від атаки на основі адаптивно підібраних (вибраних) шифртекстів.

4.5. Атака на основі підібраних (вибраних) відкритих текстів – це сценарій, у якому той, хто атакує, має можливість підбирати (вибирати) відкриті тексти P_i і переглядати їх відповідні зашифрування – шифртексти C_i. Ця атака вважається менш практичною, ніж на основі відомих відкритих текстів, але все ж таки небезпечною. Якщо шифр вразливий до атаки на основі відомих відкритих текстів, то він автоматично вразливий до атаки на основі підібраних(вибраних) відкритих текстів, але не обов'язково

навпаки. У сучасній криптографії типовий приклад подібного сценарію – диференційний криптоаналіз. Це також рідкісний метод, для якого перетворення з підібраного (вибраного) відкритого тексту до відомого відкритого тексту є можливим (через його роботу з парами текстів).

4.6. Атака на основі підібраних (вибраних) відкритих текстів та шифртекстів дозволяє зловмиснику комбінувати атаку на основі підібраних (вибраних) відкритих текстів і на основі підібраних (вибраних) шифртекстів, а також видавати підібрані (вибрані) запити як для функції зашифрування, так і для функції розшифрування.

4.7. Атаки розрізнення (розрізнюваності) – це алгоритм тестування, який намагається виявляти в криптосистемі невипадкову поведінку, що може надати певну інформацію зловмиснику. Розрізнювач – алгоритм тестування, пов'язаний або з ідеальною випадковою процедурою R, або з криптосистемою (або її частиною) C, яка повинна імітувати R. Якщо розрізнювач здатний розпізнати їх зі значною перевагою, то це призводить до атаки розрізнення (розрізнюваності). Це дуже загальний параметр, який може застосовуватися до будь-якої криптосистеми, але є актуальним для оцінки її безпеки.

В основі всіх шифрів лежать деякі детерміністичні функції (інакше було б важко розшифрувати), які приймають як параметр ключ, а як вхідні дані – повідомлення. Просте застосування детерміністичних функцій щодо ключа і повідомлення призводить до елементарної атаки розрізнення (розрізнюваності), оскільки всі повідомлення, що мають однакове значення, зашифруються в однаковий шифртекст за однакового ключа. Саме тому всі схеми шифрування включають елемент рандомізації.

4.8. Нерозрізнюваність у разі атаки на основі підібраних (вибраних) відкритих текстів. Основна ідея нерозрізнюваності полягає в тому, щоб розглянути зловмисника, який не володіє секретним ключем та обирає два повідомлення однакової довжини. Тоді одне з них зашифровується, а шифртекст надається зловмиснику. Схема вважається безпечною, якщо йому важко визначити, яке з двох повідомлень було зашифровано. Схема шифрування вважається захищеною від атаки на основі підібраних (вибраних) відкритих текстів, якщо зловмисник, який обмежується використанням «практичної» кількості ресурсів (обчислювальний час, кількість запитів), не може отримати значну перевагу.

Надамо зловмиснику трохи більше потужності (сили) для вибору цілої послідовності пар повідомлень рівної довжини. Далі деталізуємо цю гру.

Зловмисник вибирає послідовність пар повідомлень $\left(M_{0,1}, M_{1,1}\right),\ldots,\left(M_{0,q}, M_{1,q}\right)$, де в кожній парі два повідомлення мають однакову довжину. Ми надаємо йому послідовність шифртекстів $C_1,\ldots, C_q$, де C_i – це зашифрування $M_{0,I}$ для всіх $1 \le i \le q$ (1) або, C_i – це зашифрування $M_{1,I}$ для всіх $1 \le I \le q$ (2). Виконуючи зашифрування, алгоритм щоразу використовує ті самі ключі, крім свіжих додаткових випадкових бітів (coins) або оновленого стану. Зловмисник отримує послідовність шифртекстів, і тепер йому слід вгадати: були зашифровані $M_{0,1},\ldots, M_{0,q}$ чи $M_{1,1},\ldots, M_{1,q}$.

Щоб ще більше розширити можливості зловмисника, ми дозволимо йому вибрати послідовність пар повідомлень за допомогою атаки на основі підібраних (вибраних) відкритих текстів. Тобто зловмисник вибирає першу пару й отримує C_1, потім обирає другу пару й отримує C_2 тощо. Іноді це називається атакою на основі адаптивно

підібраних (вибраних) відкритих текстів, адже зловмисник може адаптивно підбирати (вибирати) кожен запит у такий спосіб, що відповідає більш раннім результатам.

4.9. Нерозрізнюваність у разі атаки на основі підібраних (вибраних) шифртекстів. Схема шифрування вважається захищеною від атаки на основі підібраних (вибраних) шифртекстів, якщо «розумний» зловмисник не може отримати «значну» перевагу, щоб відрізнити випадки $b = 0$ і $b = 1$, що мають доступ до оракулів, де розумно відображається використання його ресурсів. Технічне поняття називається нерозрізнюваністю в разі атаки на основі підібраних (вибраних) шифртекстів, позначається *IND-CCA*.

5. Моделі основних атак на основі нерозрізнюваності

Наведемо та розглянемо визначення та відповідні схеми виконання атак [2, 3].

5.1. Визначення *IND-CPA/CCA2*. Нехай $PKE = (Gen,\ Enc,\ Dec)$ є схемою шифрування з відкритим ключем. Розглянемо такий експеримент у сценарії *IND-CPA* [3]:

$$Expt\frac{IND-CPA}{PKE,\mathrm{A}}(\lambda)$$

$$(pk, sk) \longleftarrow Gen(1^{\lambda})$$
$$(m^0, m^1, state) \longleftarrow \mathrm{A}_1(pk)$$
$$b \longleftarrow \{0,1\}$$
$$c^* \longleftarrow Enc(pk, m^b)$$
$$b' \longleftarrow \mathrm{A}_2(c^*,\ state),$$

де pk – відкритий ключ;

sk – особистий ключ;

m – відкритий текст;

Gen – генерація ключів;

Enc – зашифрування;

Dec – розшифрування;

$state$ – деяка інформація про стан;

1^{λ} – параметр безпеки (може позначатися ще як k).

Алгоритм Gen на вхід приймає параметр безпеки 1^{λ}, виводить пару «відкритий – особистий ключ» (pk, sk).

Алгоритм Enc на вхід приймає відкритий ключ pk та відкритий текст m, обчислює шифртекст c.

Алгоритм Dec на вхід приймає особистий (секретний) ключ sk та шифртекст c, виводить відкритий текст m.

Потрібно, щоб для будь-якої пари (pk, sk) та m виконувалося рівняння $Dec(sk, Enc(pk, m)) = m$, тоді перевагу визначаємо за таким виразом:

$$Adv_{PKE.A}^{IND-CPA}(\lambda) = \left| Pr[b = b'] - \frac{1}{2} \right|.$$

Зауважимо, що *PKE* є *IND-CPA*-безпечним, якщо $Adv_{PKE.A}^{IND-CPA}(\lambda)$ є незначним.

Сценарій *IND-CCA2* повністю аналогічний *IND-CPA*, за винятком того, що зловмиснику дозволено запитувати *c* ($\neq c^*$) в оракула розшифрування $Dec(sk,\cdot)$.

5.2. Нерозрізнюваність ключів (визначення *IK-CPA/CCA2*). Конфіденційність ключа визначаємо в разі атак на основі підібраного (вибраного) відкритого тексту та підібраного (вибраного) шифртексту. Нехай зловмисник працює в два етапи [2, 3]. На етапі **find** він приймає два відкриті ключі pk_0 і pk_1 (відповідають секретним ключам sk_0 та sk_1) і виводить повідомлення *x* разом з деякою інформацією про стан *s*. На етапі **guess** він отримує виклик шифртексту *y*, який утворюється шляхом випадкового зашифрування повідомлень з одним із двох ключів. Він повинен визначити, який ключ був вибраний. У разі атаки на основі вибраного шифртексту зловмисник отримує оракули для $D_{sk_0}(\cdot)$ та $D_{sk_1}(\cdot)$ і може дозволити викликати їх у будь-якій точці з обмеженням (на обох оракулах), не запитуючи *y* під час етапу **guess.** Наведемо деякі основні позначення [3]:

$PE=(G,K,E,D)$ – схема шифрування з відкритим ключем;

G – загальний алгоритм генерації ключів: на вхід подається деякий параметр безпеки *k*, повертається деякий загальний ключ *I*;

K – рандомізований алгоритм генерації ключів, на вхід якого подається загальний ключ *I* та повертається пара ключів (pk,sk);

у $(pk,sk)\xleftarrow{R} K(I)$ *I* має бути тільки параметром безпеки *k* або містити додаткову інформацію;

E – рандомізований алгоритм зашифрування, який бере відкритий ключ *pk* та відкритий текст *x* для того, щоб повернути шифртекст *y*: $y\xleftarrow{R} E_{pk}(x)$;

D – детермінований алгоритм розшифрування, який приймає секретний ключ *sk* та шифртекст *y* для того, щоб повернути відповідний відкритий текст *x* або спеціальний символ $\perp$ та показати, що шифртекст є недійсним; записується $x\leftarrow D_{sk}(y)$, коли *y* є дійсним, та $\perp\leftarrow D_{sk}(y)$ – в іншому разі;

MsgSp(*pk*) – простір повідомлень, з якого вибирається *x*.

Необхідно, щоб $D_{sk}(E_{pk}(x))=y$ для всіх $x\in MsgSp(pk)$.

Далі наведемо визначення для варіантів нерозрізнюваності ключів [2, 3].

Визначення 2. Нехай $PKE=(Gen,\ Enc,\ Dec)$ є схемою шифрування на відкритому ключі. Розглянемо такий експеримент у сценарії *IK-CPA:*

$$Expt\frac{IK-CPA}{PKE,\mathrm{A}}(\lambda)$$

$$\left(pk^0, sk^0\right), \left(pk1, sk^1\right) \longleftarrow Gen\left(1^\lambda\right)$$
$$\left(m, state\right) \longleftarrow \mathrm{A}_1\left(pk^0, pk^1\right)$$
$$b \longleftarrow \{0,1\}$$
$$c^* \longleftarrow Enc\left(pk^b, m\right)$$
$$b' \longleftarrow \mathrm{A}_2\left(c^*, state\right).$$

Перевагу зловмисника визначаємо як

$$Adv_{PKE.A}^{IK-CPA}(\lambda) = \left| Pr[b = b'] - \frac{1}{2} \right|.$$

Припустимо, що *PKE* є *IK-CPA*-безпечним, якщо $Adv_{PKE.A}^{IK-CPA}(\lambda)$ є незначним.

Сценарій *IK-CCA2* повністю аналогічний *IK-CPA*, за винятком того, що зловмиснику дозволено запитувати c ($\neq c^*$) в оракулів розшифрування $Dec\left(sk^0, \cdot\right)$ та $Dec\left(sk^1, \cdot\right)$.

Визначення 3. [*IK-CPA, IK-CCA*]. Нехай $PE = \left(G, K, E, D\right)$ є схемою шифрування, $b \in \{0, 1\}$ та $k \in N$. При цьому A_{CPA}, A_{CCA} є зловмисниками. A_{CCA} має доступ до оракулів $D_{sk_0}(\cdot)$ та $D_{sk_1}(\cdot)$. Розглянемо такі експерименти в сценаріях *IK-CPA* та *IK-CCA*:

Experiment $Exp_{PE, A_{CPA}}^{SS\text{-}CPA\text{-}b}(k)$	*Experiment* $Exp_{PE, A_{CCA}}^{SS\text{-}CPA\text{-}b}(k)$
$I \xleftarrow{R} G(k)$	$I \xleftarrow{R} G(k)$
$\left(pk^0, sk^0\right) \xleftarrow{R} K(I); \left(pk^1, sk^1\right) \xleftarrow{R} K(I)$	$\left(pk_0, sk_0\right) \xleftarrow{R} K(I); \left(pk_1, sk_1\right) \xleftarrow{R} K(I)$
$(x, s) \longleftarrow A_{cpa}\left(find, pk_0, pk_1\right)$	$(x, s) \longleftarrow A^{D_{sk_0}(\bullet), D_{sk_1}(\bullet)}{}_{cca}\left(find, pk_0, pk_1\right)$
$y \longleftarrow \varepsilon_{pk_b}(x)$	$y \longleftarrow \varepsilon_{pk_b}(x)$
$d \longleftarrow A$	$d \longleftarrow A^{D_{sk_0}(\bullet), D_{sk_1}(\bullet)}{}_{cca}\left(guess, y, s\right)$
Return d,	*Return* d.

Вище передбачено, що A_{CCA} ніколи не запитує $D_{sk_0}(\cdot)$ або $D_{sk_1}(\cdot)$ на виклик шифртексту y. Для $\boldsymbol{atk} \in \{\boldsymbol{cpa}, \boldsymbol{cca}\}$ визначаємо переваги зловмисників за виразом

$$Adv_{PE.A_{ATK}}^{IK-ATK}(k) = Pr\left[Exp_{PE.A_{ATK}}^{IK-ATK-1}(k) = 1\right] - Pr\left[Exp_{PE.A_{ATK}}^{IK-ATK-0}(k) = 1\right].$$

Схема *PE* вважається *IK-CPA*-безпечною (відповідно, *IK-CCA*-безпечною), якщо функція $Adv_{PKE.A}^{IK-CPA}(\cdot)$ (а отже, $Adv_{PKE.A}^{IK-CCA}(\cdot)$) є незначною для будь-якого зловмисника A, часова складність якого поліноміальна за k.

Висновки. На сьогодні запропоновано три моделі безпеки, що стосуються шифрування, електронного підпису та механізмів інкапсуляції ключів: *IND-CPA*, *IND-CCA/CCA2* для механізмів шифрування; *EUF-CMA* для механізмів підпису; модель *CK* для інкапсуляції ключів.

Безпека за будь-яким із наступних визначень означає безпеку за попередніми, тобто: схема, яка є *IND-CCA*-безпечною, також є *IND-CPA*-безпечною; схема, яка є *IND-CCA2*-

безпечною, є як *IND-CCA*-безпечною, так і *IND-CPA*-безпечною. Отже, *IND-CCA2* є найсуворішим із цих трьох визначень безпеки.

Нерозрізнюваність (невизначеність) у разі атаки на основі підібраного (вибраного) відкритого тексту (*IND-CPA*) еквівалентна властивості семантичної безпеки (*SEM-CPA*). За нерозрізнюваності (невизначеності) шифртекстів відбувається захист усіх відомих криптосистем від зловмисника *A*, який: є імовірнісною машиною Тюрінга поліноміального часу; має всі алгоритми; володіє повним доступом до засобів зв'язку.

Подальші дослідження будуть спрямовані на вивчення властивостей криптографічної стійкості національних криптоалгоритмів.

СПИСОК ЛІТЕРАТУРИ

1. Ciphertext indistinguishability. URL: http://cse.iitkgp.ac.in/~debdeep/courses_iitkgp/FCrypto/scribes/scribe8.pdf (last accessed: 15.12.2018).
2. Henk C. A. van Tilborg, Sushil Jajodia. Encyclopedia of Cryptography and Security Springer. 2011. – 1416 p.
3. Yusuke Yoshida, Kirill Morozov, Keisuke Tanaka. CCA2 Key-Privacy for Code-Based Encryption in the Standard Model, Springer International Publishing AG 2017: PQCrypto 2017, LNCS 10346. P. 35–50. DOI: 10.1007/978-3-319-59879-6_3.
4. Dan Bogdanov. IND-CCA2 secure cryptosystems MTAT.07.006 // Research Seminar in Cryptography, 2005. URL: https://courses.cs.ut.ee/2005/crypto-seminar-fall/slides/S5.Bogdanov.indcca2.pdf (last accessed: 10.11.2018).
5. Bellare M. Symmetric encryption. URL: https://cseweb.ucsd.edu/~mihir/cse207/w-se.pdf (last accessed: 18.11.2018).

Подано 29.03.2019

М. В. Есина, С. Г. Вдовенко, И. Д. Горбенко

МОДЕЛИ БЕЗОПАСНОСТИ ПОСТКВАНТОВИХ АСИММЕТРИЧНЫХ ШИФРОВ НА ОСНОВЕ НЕРАЗЛИЧИМОСТИ

В статье приведено доказательство эквивалентности свойства неразличимости (неопределенности) свойству семантической безопасности для защиты криптосистем от криптоанализа нарушителя на основе подобранного (выбранного) открытого текста.

Вопросы анализа и исследования моделей безопасности постквантовых криптоалгоритмов по отношению к криптопримитивам всех типов, определение критериев оценки их соответствия различным моделям безопасности (согласно различным типам криптопреобразований) актуальны и имеют практическое значение. Неразличимость (неопределенность) зашифрованного текста является важным свойством безопасности многих схем шифрования, которое при атаке на основе подобранного (выбранного) открытого текста считается основным требованием для большинства достоверно защищенных криптосистем с открытым ключом. Некоторые схемы также обеспечивают неразличимость при атаке на основе подобранного (выбранного) и адаптивно подобранного (выбранного) зашифрованного текста. Использование свойства неразличимости (неопределенности) зашифрованного текста

в настоящее время позволяет гарантированно осуществить защиту всех известных симметричных и асимметричных криптосистем от классического или квантового криптоанализа злоумышленника.

Рассмотрены наиболее распространенные существующие сегодня виды атак на безопасность механизмов шифрования, а именно: атака на основе адаптивно подобранных (выбранных) шифртекстов; атака на основе адаптивно подобранных (выбранных) открытых текстов; атака на основе адаптивно подобранных (выбранных) открытых текстов и адаптивно подобранных (выбранных) шифртекстов; атака на основе подобранных (выбранных) шифртекстов; атака на основе подобранных (выбранных) открытых текстов; атаки различия (разрешения).

Ключевые слова: *атака на основе адаптивно подобранных (выбранных) шифртекстов; атака на основе подобранных (выбранных) открытых текстов; неразличимость (неопределенность) зашифрованного текста; неразличимость ключей.*

M. V. Yesina, S. G. Vdovenko, I. D. Gorbenko

MODELS OF SECURITY OF POST-QUANTUM ASYMMETRIC ENCUSSION BASED ON INDISTINGUISHABILITY

The article takes a verifier of equivalence of the quality of indistinguishability (uncertainty) of the semantic security for the cryptosystems defense against of attacker's cryptanalyses based on matched (selected) open text.

The issues of analysis and research of security models of post-quantum cryptoalgorithms in relation to cryptoprimitives of all types, the definition of criteria for assessing their compliance with different security models (according to different types of crypto-transformations) are relevant and of practical importance. The indistinguishability (uncertainty) of encrypted text is an important property of the security of many encryption schemes. The indistinguishability (uncertainty) property when attacking on the basis of matched (selected) plain text is considered a basic requirement for the majority of reliably protected public-key cryptosystems. Some schemes also provide an indistinguishability for attack based on selected (selected) encrypted text and attack based on adaptively picked (selected) encrypted text. The indistinguishability (uncertainty) of an attack on the basis of a selected (selected) open text is equivalent to the properties of semantic security. If the cryptosystem has the property of indistinguishability, the attacker will not be able to distinguish between pairs of encrypted texts based on the message that they encrypt. In the case of non-differentiation (uncertainty) of ciphertext protects all known cryptosystems from the intruder which: is a probabilistic Turing machine of polynomial time; has all algorithms; has full access to communications. Using the property of the indeterminacy (uncertainty) of the encrypted text at the present time, it is guaranteed to protect all known symmetric and asymmetric cryptosystems from the classical or quantum cryptanalysis of the intruder.

Here are a review of mostly attacks on the encryption security namely an attack based on adaptively matched (selected) ciphertexts, an attack based on adaptively matched (selected) open texts, an attack based on both of this types of texts, an attack based on matched (selected) ciphertexts, an attack based on matched (selected) open texts and a recognition attacks (recognizability).

Keywords: *an attack based on adaptively matched (selected) ciphertexts; an attack based on matched (selected) open messages; indistinguishability (uncertainty) of encrypted text; Indistinguishability of keys.*