УДК 004.056.55

Ю.І. ГОРБЕНКО, канд. техн. наук, О.В. ШЕВЦОВ, Т.Ю. КУЗНЕЦОВА

МОДЕЛЬ ПОРУШНИКА СИСТЕМ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ В УМОВАХ КВАНТОВОГО КРИПТОАНАЛІЗУ

Вступ

Досить суттєве значення мають автоматизовані засоби автентифікації та ідентифікації, що знайшли своє застосування в різних криптографічних протоколах [1 – 18]. Ключову роль в забезпеченні контроля цілісності та *неспростовності* для вказаних технологій відіграють електронні цифрові підписи (ЕЦП). Із появою квантового комп'ютера очікується значна зміна поглядів на криптоаналіз та, як наслідок, – на визначення кандидатів постквантового ЕЦП [4, 5]. Оцінку основних результатів щодо квантового криптоаналізу проведено в [4 – 8]. Найбільш перспективні розробки схем цифрового постквантового підпису представлені в роботах [13, 15, 18]. Проте, немає точного та *усталеного* сприйняття моделі загроз та моделі порушника в умовах появи квантового комп'ютера.

Метою даної роботи є підвищення ефективності розробки систем квантової криптографії за рахунок аналізу можливих методів квантового криптоаналізу на системи ЕЦП та побудови моделі порушника в постквантовому середовищі. Для досягнення поставленої мети вирішувалися наступні задачі:

- розробка моделі порушника ЕЦП та управління ключовими даними із доступом до квантового комп'ютера;
- розробка моделі порушника ЕЦП із доступом до квантового випадкового оракула;
- розробка моделі загроз на системи ЕЦП в умовах появи квантового комп'ютера;

При побудові моделі порушника та загроз застосовується методика, що ґрунтується спочатку на побудові моделі порушника (п. 1), виявленні усіх можливих загроз та визначенні способів їх реалізації, а наостанок – на побудові моделі загроз ЕЦП для конкретних умов застосування (п. 2). Представлені умови застосування ЕЦП моделюють використання квантового комп'ютера, що впливає на характер дій зловмисника та особливості загроз (п. 2). В п. 3 отримано кількісні оцінки захищеності ЕЦП від основних загроз. Побудовані моделі порушника та загроз дозволяють сформулювати вимоги до системи захисту інформації при автентифікації повідомлень засобами ЕЦП.

1. Загальна модель порушника та загроз ЕЦП

Орієнтуючись на [4], під моделлю порушника будемо розуміти абстрактний формалізований чи неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії тощо. Також може бути врахована наступна інформація, доступна противнику:

- криптографічні дані, доступні атакуючому (наприклад, атака з підібраним шифротекстом);
- визначені аспекти криптографічних алгоритмів (наприклад, чи доступно атакуючому визначення хеш-функції, використовуваної в алгоритмі, – це може бути важливим фактором в моделі випадкового оракула);
- визначені аспекти виконання (наприклад, чорний ящик);
- обчислювальні ресурси, доступні атакуючому.

Проведений аналіз показав [4], що порушник (супротивник) може здійснювати по відношенню до криптографічних примітивів пасивні або активні атаки. При пасивних атаках порушник може здійснювати:

- аналіз даних, перехоплених в процесі виконання криптографічного примітиву, наприклад визначення таємного сеансового ключа за перехопленим відкритим ключем;

- розв'язання задач повного або універсального розкриття по відношенню до статичного, сеансового або одночасно і статичного, і сеансового ключів.

При активних атаках порушник може створювати та передавати хибні повідомлення та підписи, що є імітацією роботи істинного криптографічного примітиву;

Поряд з тим, в моделі порушника необхідно задавати інші його можливості, наприклад [4]:

- міру доступу до каналу передачі даних між підписувачем та перевіряючим;

- можливості записування даних, що передаються в процесі виконання криптопримітиву ЕЦП;

- можливість зміни даних криптопримітиву (модифікування);

- можливість знищення даних;

- багаторазове використання даних примітиву;

- несанкціоновану ініціалізацію виконань алгоритму, перезапускання тощо.

Зловмисник в процесі протидії може знаходиться в різних умовах [4], враховуючи це, будемо розглядати наступних зловмисників:

-зовнішній, що має тільки загальнодоступні дані та відомості, наприклад повідомлення, підписи ЕЦП, відкриті ключі, загальносистемні параметри;

- зловмисник, що має постійний чи тимчасовий доступ до критичної інформації, наприклад до ключів сеансів, таємних даних тощо.

Крім вказаного, згідно з [4], будемо також розглядати порушника з чотирма рівнями можливостей:

- нульовий – випадкове навмисне ознайомлення зі змістом інформації (випадкове прослуховування в каналі);

- перший – порушник має обмежені кошти та самостійно створює засоби і методи атак на засоби криптографічного захисту інформації (КЗІ), а також інформаційно-телекомунікаційні системи із застосуванням широко розповсюджених програмних засобів та електронно-обчислювальної техніки;

- другий – порушник корпоративного типу має змогу створювати спеціальні технічні засоби, вартість яких співвідноситься з можливими фінансовими збитками при втраті, спотворенні та знищенні інформації, що захищається. У цьому разі для розподілу обчислень при проведенні атак можуть застосовуватися локальні обчислювальні мережі;

- третій – порушник має науково-технічний ресурс, який прирівнюється до науково-технічного ресурсу спеціальної служби економічно розвинутої держави.

Цілі порушника – створення нових та підвищення ефективності існуючих методів аналізу стійкості класичних та постквантових ЕЦП. Існує класифікація моделей порушника за мотивом. Підґрунтям цілеспрямованої реалізації порушником криптоаналізу є, найчастіше, корисливі мотиви. Раціональна модель мотивації зловмисника описує дії порушника в залежності від вигоди та витрат, які він отримує в результаті криптоаналізу. Наприклад, вибір стратегії дій зловмисником визначається прагненням одержати особисто максимальну вигоду та нанести максимальні втрати користувачеві (власникові). Існує також альтруїстична модель поведінки зловмисника, коли мотивація противника виходить за межі поняття вигоди і є більш руйнівною. Модель раціонально вмотивованого зловмисника представляється більш релевантною до обставин реального світу, ніж альтруїстична.

Захищеність ключів від дій зловмисників називається криптографічною живучістю. При цьому необхідно враховувати, що компрометація тільки довгострокових (статичних) ключів

не приводить до компрометації ключів сеансів, що уже були застосовані раніше. При здійсненні аналізу криптографічних примітивів типу ЕЦП необхідно зважати на наступне:

- якщо довгострокові особисті ключі ЕЦП скомпрометовані, то наступні сеанси здійснення протоколів не захищені від підробки;

- при компрометації статичних (довгострокових) ключів компрометація минулих ключів сеансів не відбувається.

В наукових колах розповсюджено різні підходи до моделювання дій порушника. Розглянемо деякі з них. Відповідно до моделі загроз Долева – Яо [0], будь-яке повідомлення, що передається у мережі, може бути прослухане зловмисником. Із цього слідує, що будь-яке повідомлення, отримане користувачем із мережі, спочатку було перехоплено зловмисником, а потім передано адресату.

Зауваження. За даними твердженнями зробимо припущення, що зловмисник має контроль над всією мережею. Аналіз мережі, в якій використовуються різні протоколи, що включають криптопримітиви ЕЦП, виходить за рамки даної роботи. Посилені припущення щодо дій зловмисника в мережі робляться для того, аби результати даної роботи могли бути застосовані для моделі загроз будь-якої мережі, а структура доведення загального протоколу включала би примітив ЕЦП у вигляді модуля, тобто, без врахування конкретних особливостей моделі загроз ЕЦП.

Необхідно зазначити також межі можливостей зловмисника. Якщо примітиви ЕЦП безпечні, то зловмисник не може вгадати випадкове число, обране із достатньо великого простору. Не маючи правильного особистого ключа, зловмисник не може відтворити підпис за його відкритим ключем або підписати повідомлення. Зловмисник не може знайти особистий ключ, знаючи тільки відкритий ключ.

Спочатку виділимо основну методику оцінки дій зловмисника, а потім застосуємо математичний апарат оцінки дій зловмисника щодо зламу основних постквантових ЕЦП. Визначимо такі кандидати ЕЦП на постквантовий період [4 – 8, 13, 15, 18]:

на основі хеш-функцій (Hash Based);

на основі завадостійких кодів (Code Based);

на основі решіток (Lattice Based);

на основі факторизації поліномів (Multivariate Polynomial Based).

Розгляд основних концепцій автентифікації з метою захисту від НСД ведеться, зазвичай, в частині криптографічних протоколів. Наведені концептуальні положення можуть бути застосованими й до примітивів ЕЦП.

Розглянемо спрощену модель середовища взаємодії [4] відправника та отримувача в умовах дій зловмисника. Ця узагальнена модель включає найкритичніший випадок, коли кожна сторона може бути зловмисником. Таким чином, гарантії безпеки взаємодії засновані не на довіреній стороні чи на припущенні, що більшість учасників є чесними, а на гарантії криптографічної стійкості ЕЦП. Таким чином, дана модель включатиме модель загроз ЕЦП, яку буде розглянуто далі. Такий підхід дасть змогу поширити результати моделі погроз ЕЦП й на середовище, де сторони не довіряють один одному. Учасники моделі середовища взаємодії:

- D_1, D_2: відправник та отримувач;

- КРА – криптоаналітик (зловмисник);

- випадковий оракул;

Оскільки сторони D_1 D_2 можуть виявитися зловмисниками, проаналізуємо основні погрози:

1) D_1 відмовляється від факту передачі повідомлення M_i в мережу;

2) D_1 намагається обманути, що він сформував та передав деяку інформацію M_i;

3) підміна джерелом D_1 часу передачі інформації M_i;

4) підміна передачі інформації M_i на інформацію $M_i^{'}$;

Основні погрози, що може реалізувати джерело D_2:

1) D_2 формує деяку інформацію $M_i^{'}$ та стверджує, що він отримав її від D_1;

2) підміна джерелом D_2 часу передачі інформації M_i;

3) D_2 відмовляється від факту отримання повідомлення M_i.

Основні погрози, що може реалізувати КРА:

1) імітація помилкового повідомлення M_i, КРА у момент часу, коли D_1 пасивний, створює помилкову M_i інформацію і передає її D_2 ;

2) модифікація правильної інформації M_i у випадку, якщо D_1 передає D_2 деяку інформацію M_i, КРА модифікує інформацію M_i в $M_i^{'}$ і передає її D_2;

3) нав'язування раніше створеної інформації (повтор), тобто КРА в будь-який момент часу t_j передає її ще раз D_2, коли D_1 пасивний;

В даній моделі представлений випадковий оракул. Всі учасники моделі мають доступ до оракула, який обчислює випадкову функцію. При кожному новому запиті значення функції на даному аргументі вибирається випадковим чином. При цьому оракул запам'ятовує пару (аргумент, значення) і при повторному запиті для цього аргументу, незалежно від того, хто з учасників його видав, буде повернуто те саме запам’ятоване значення. Модель із випадковим оракулом була введена для протоколів електронного підпису, де випадкова функція замінила хеш-функцію. Згодом модель було узагальнено на криптографічні протоколи різних типів, і в даний час в криптології значна частина результатів про стійкість доводиться в цій моделі. В класичному варіанті сам алгоритм підпису та всі інші учасники, крім зловмисника здійснюють доступ до випадкового оракула за допомогою класичних бітових рядків. Під класичним входом/виходом розуміється звичайний бітовий рядок. При цьому на вхід випадкового оракула подається один рядок, що представляє аргумент, а інший представляє вихідне значення.

Класичний комп’ютер працює зі скінченним числом біт. Кожен біт може знаходитися в одному з двох станів 0 чи 1. Стан всієї системи задається значенням всіх бітів. Тому множина станів класичного комп'ютера $B^n = \{0,1\}^n$ скінченна та має потужність 2^n.

Під позначенням $\{0;1\}^*$ будемо розуміти множину скінченних бінарних рядків, а під $\{0;1\}^\infty$ будемо розуміти нескінченні рядки. Тоді R – це відображення із $\{0;1\}^*$ на $\{0;1\}^\infty$, визначене вибором кожного біта $R(x)$ випадково та незалежно для кожного x. Відповідно, ЕЦП – це кортеж $(G, Sign, Verify)$ поліноміальних алгоритмів генерації ключів, підпису та перевірки. Перші два з них імовірнісні, а останні два мають доступ до випадкового оракула. Отримуючи на вхід строку 1^k (максимального обсягу інформації із довжиною k, де k параметр безпеки), генератор створює пару (pk, sk) публічний та секретний ключ за поліноміальний час. Зловмисник ЕЦП A – це невипадковий поліноміальний алгоритм F із доступом до R та оракула підписання. Вихід F – це пара (m, σ) повідомлення та підпис, причому, m не є результатом роботи оракула підписання.

Ґрунтуючись на наведеному, розглянемо модель порушника ЕЦП в умовах появи квантового комп’ютера, на основі якої побудуємо модель загроз ЕЦП.

2. Модель порушника та загроз ЕЦП в умовах появи квантового комп'ютера

Модель порушника ЕЦП в умовах появи квантового комп'ютера включає в себе наступні аспекти. Метою зловмисника є підробка підпису повідомлення та компрометація особистих ключів ЕЦП [4]. На відміну від протоколів автентифікації ми виключаємо випадки, коли зловмисник ненавмисно реалізує криптоаналіз [4]. Кваліфікація порушника – сукупність певних знань і вмінь порушника, які він використовує для порушення роботи криптопримітиву ЕЦП. Можна визначити кілька типів кваліфікації порушників, що дозволять успішно реалізувати загрози системам постквантової криптографії [18 – 21]:

- порушник володіє інформацією щодо математичного базису криптографічних перетворень конкретного ЕЦП, що дозволить створити нові методи криптоаналізу, відповідно до рівня криптографічного захисту;
- порушник володіє високим рівнем знань в галузі обчислювальної техніки (зокрема криптографії, теорії алгоритмів та паралельних обчислень тощо) і програмування криптографічних засобів автентифікації;
- порушник досконало володіє знаннями квантової фізики, квантової інформатики тощо, а також навичками роботи з обладнанням, що складає квантовий комп'ютер [2];
- порушник має доступ до глобальних обчислювальних мереж, суперкомп'ютера чи квантового комп'ютера, за допомогою якого може реалізувати, наприклад силову атаку, використовуючи відомі квантові алгоритми Шора, Гровера тощо [10].

Можливості порушника в умовах появи квантового комп'ютера представлені нижче.

1) Порушник має можливість запуску програмного забезпечення, що реалізує певні функції з обробки класичного та квантового криптоаналізу. Знання мов програмування дозволить порушнику реалізувати створені методи криптоаналізу, а також модифікувати існуючий програмний код легітимних користувачів.

2) Порушник може створювати нові алгоритми класичного та квантового криптоаналізу для подальшого одержання необхідної порушнику інформації шляхом створення програмного забезпечення та модифікування існуючого.

Теоретичний аналіз стійкості примітивів постквантової криптографії будемо проводити, виходячи з того, що порушник використовує технічні можливості не тільки квантової механіки та інформатики, а й класичні методи криптоаналізу, або їх поєднання, що поширює картину загроз, які треба враховувати.

Розробка моделі порушника ЕЦП із доступом до квантового випадкового оракула. В останні роки в літературі (особливо зарубіжній) робиться спроба знайти зручний та суворий математичний апарат доказу постквантової стійкості криптографічних примітивів за допомогою зведення доказів класичної стійкості до доказів постквантової стійкості, використовуючи апарат теорії ігор [10], формулювання умов, коли такі зведення є ефективними. Також вивчається модель зловмисника із доступом до квантового випадкового оракула та відмінність від моделі порушника із доступом до класичного випадкового оракула. Ці роботи також розглядають методику оцінки стійкості ЕЦП. Продемонстровано, як поняття криптографічної безпеки можуть бути представлені за допомогою використання принципів формалізації теорії ігор.

Особливістю ЕЦП як криптографічних перетворень є те, що ключі асиметричної пари генеруються особисто кожним власником цієї пари у складі особистого та відкритого ключів. Це означає, що власник ключової пари може згенерувати її, використовуючи спеціальні засоби, в тому числі такі, що створюються порушником для шахрайства. Будемо вважати, що ці шахрайські дії здійснює порушник 1, 2 або 3 рівнів. Будемо також вважати, що ЕЦП здійснюється з використанням криптографічних перетворень, які є постквантово стійкими.

В якості моделі порушника виберемо таку, що базується на спробі селективної або екзистенційної підробки повідомлень, що підписуються. Селективна підробка представляє

загрозу, спрямовану на створення правильного ЕЦП для попередньо вибраного повідомлення M_i. Екзистенційна підробка представляє погрозу, яка полягає в створенні порушником для повідомлення M_i, можливо навіть такого, що не має змісту, правильного ЕЦП.

Розглядається санкціонований користувач-порушник, який здійснює такі зловмисні дії. Робиться спроба для повідомлень M_i та M_j виробити ідентичний ЕЦП. Далі порушник (зловмисник) може маніпулювати цими підписаними повідомленнями, пред'являючи або передаючи при реалізації загроз те чи інше повідомлення.

Для моделювання дій зловмисника будемо оперувати поняттям модель випадкового оракула. Також вважатимемо, що всі сторони (підписувач, перевіряючий та зловмисник) можуть посилати запити до випадкового оракула, який обчислює хеш-функції для них та забезпечує послідовні та несуперечливі відповіді для всіх учасників взаємодії.

Питання моделювання випадкового оракула для квантового зловмисника досить важливе та складне. Для цього поняття суттєвим є визначення квантового комп'ютера та відмінності квантових обчислень від класичних. Квантовий комп'ютер працює зі скінченним набором елементарних станів, що називаються кубітами. Кожний кубіт має два виділених стани (якщо кубіти вважати спінами, то ці стани "спін вгору", "спін вниз"). Визначення виділених станів для кожного кубіта системи задає не всі можливі стани системи, а тільки базисні. Можливі також будь-які лінійні комбінації базисних станів із комплексними коефіцієнтами. Базисні стани будемо позначати $|x_1,...,x_n\rangle$, де $x_j \in B$ або $|x\rangle$, де $x \in B^n$. Довільний стан системи може бути представлений у вигляді

$$|\psi\rangle = \sum_{(x_1,...,x_n)\in B^n} c_{x_1,...,x_n} |x_1,...,x_n\rangle, \text{ де } \sum_{(x_1,...,x_n)\in B^n} \left|c_{x_1,...,x_n}\right|^2 = 1.$$

Простір станів для такої системи – скінченний (розмірності 2^n) простір над полем комплексних чисел. Визначимо відмінність станів класичного та квантового комп'ютера [0]:

- стан класичного комп'ютера, що складається із біт, виражається як – $x_1x_2...x_nx_j \in B$;

- стан квантового комп'ютера складається із кубіт. Існує базисний стан, що виражається як $|x_1,...,x_n\rangle$, $x_j \in B$, і довільний стан, який виражається як $\sum_{x\in B^n} c_x |x\rangle$, де $\sum_{x\in B^n} |c_x|^2 = 1$.

Обчислення можна представити як послідовність перетворень над множиною станів системи. Опишемо, які перетворення можливі в класичному, а які – в квантовому випадку [0]:

- для класичного випадку перетворення – це функція із B^n в B^n;

- для квантового випадку перетворення – це унітарні оператори, тобто оператори, які зберігають довжину вектору $\sum_{x\in B^n} |c_x|^2$.

Більшість сучасних моделей випадкових оракулів є доказово стійкими по відношенню до зловмисника із класичним доступом до випадкового оракула. В цих моделях зловмисник має доступ до оракула хеш-функції $O : \{0, 1\}^* \to \{0, 1\}^*$, він може дізнатися значення O (x) за допомогою подачі запитів до оракула O в класичному стані x. Для вивчення конкретної системи випадковий оракул заміняється конкретною хеш-функцією, що змушує зловмисника оцінювати цю хеш-функцію через квантовий стан x [2].

Для того щоб змоделювати цю властивість, ми дозволимо зловмиснику оцінювати випадкового оракула в суперпозиції (або через явище суперпозиції). Це означає, що зловмисник може відправляти квантові стани $\langle\varphi| = \sum c_x |x\rangle$ до оракула O та отримувати назад «оцінені» стани $\sum c_x |O(x)\rangle$ (у відповідному представленні для того, щоб зберегти унітарність перетворення). На вхід випадкового оракула подаються запити в суперпозиції, а на виході отримують

суперпозицію відповідей. Суперпозиція – це лінійна комбінація 2^n можливих векторів, взятих із комплексними коефіцієнтами, де кожен з 2^n векторів є точним аналогом класичного бітового рядка. Таку модель будемо називати модель *випадкового оракула із квантовим доступом* (ВОКД). У той же час сам алгоритм підпису та всі інші учасники, крім зловмисника, здійснюють доступ до випадкового оракула за допомогою класичних бітових рядків. Під класичним входом/виходом розуміється звичайний бітовий рядок, а під квантовим – набір кубіт.

Доказ безпеки в моделі ВОКД значно важчий, ніж в класичній моделі. В якості прикладу розглянемо цифровий підпис. Стандартна стратегія доказу безпеки в класичних налаштуваннях – зловмисник обирає запити до випадкового оракула, а відповіді оформляє як результат вирішеної ним задачі. Таким чином, ця відповідь може бути оформлена як вирішення задачі підробки підпису. Якщо зловмисник зробить q випадкових запитів до випадкового оракула, то задача вирішується із вірогідністю $1/q$, а оскільки q є поліноміальним алгоритмом, то вірогідність «успішного» результату є досить великою для доказу безпеки в класичному налаштуванні випадкового оракула. На жаль, така стратегія оцінки дій зловмисника в ВОКД повністю втрачає сенс [0]. Кожний запит до ВОКД потенційно оцінює випадкового оракула в експоненційно великій кількості точок.

Якщо в класичній схемі випадковий оракул може бути змодельований безпосередньо за допомогою ідеальної хеш-функції або абстрактної алгоритмічної моделі (запит – перевірка попереднього значення – вибір генерації випадкового числа із записом або читанням раніше існуючого значення – відповідь), то в квантовому випадковому оракулові вся функція повинна бути згенерована заздалегідь, адже у відповідь, навіть на одноразовий запит, квантовий оракул видає безліч відповідей одразу. Таким чином неможливо об'єднати відповіді від одного запиту. Це показує, що доказ безпеки в класичному випадковому оракулові не обов’язково доводить постквантову безпеку.

Нижче подані відмінності між квантовим та класичним оракулом.

Класичні випадкові оракули є адаптивними. Це дозволяє програмувати їх відповіді для зловмисника, який користується адаптивно підібраними відповідями. Оскільки ВОКД забезпечує експоненційно велику множину відповідей в суперпозиції їх станів на запит, то це ускладнює програмування адаптивного ВОКД.

Однією з відмінностей класичного випадкового оракула, порівняно з квантовим є те, що в його моделі симулюються прообрази (pre-images), потрібні криптоаналітику. В ВОКД відповідь на запит може бути схована в суперпозиції в експоненціно великому наборі квантових станів і не зрозуміло, як отримати необхідні відповіді.

В класичному випадку можна ефективно змоделювати експоненційного випадкового оракула, просто обираючи випадкові відповіді. У випадку оракула з квантовим доступом зловмисник може отримати всі відповіді одночасно на всі вхідні запити. Це ускладнює стратегію запит-відповідь, яка застосовується в класичних випадкових оракулах і яка є більш узгодженою.

Деякі докази, засновані на випадковому оракулові, застосовують тактику повернення в попередній стан алгоритму (Rewinding/Partial Consistency), коли певні хеш-значення залишаються незмінними й, принаймні, одне хеш-значення серед них змінюється. Для ВОКД існує чимало труднощів впровадження такої техніки, зокрема неможливо змінювати хеш-значення непомітно.

Далі наведемо модель зловмисника при екзистенційній підробці. Нехай є зловмисник A та чесна сторона C. Модель зловмисника у вигляді взаємодії цих двох сторін назвемо моделлю гри G^{FOR} (див. алгоритм 1) [4].

Алгоритм 1.

Схема підпису: $\Pi = (KGen, Sign, Vrfy)$.

1. C генерує $(pk, sk) \leftarrow KGen(1^n)$. Відправляє pk зловмиснику A.

2. A робить запити на формування підписів від повідомлень $\{m_i\}$. C повертає $\sigma_i := Sign(sk, m_i)$. Ці повідомлення обираються адаптивно самим A.

3. A формує $(m*, \sigma*)$. Якщо $Vrfy(pk, (m*, \sigma*)) = 1$ та $m* \notin \{m_i\}$, C оголошує успіх. Інакше оголошує невдачу.

В літературі широке розповсюдження знайшла наступна техніка. Якщо розглядати послідовність ігор, то кожна наступна гра схожа на попередню з невеликою різницею в постановці експерименту. Буквально моделюється декілька схожих моделей гри зловмисника і, на підставі схожості цих ігор, можна дійти до причино-наслідкових зав'язків у різних моделях зловмисника при доказі безпечності ЕЦП щодо всіх можливих варіантів поведінки зловмисника.

Врахуємо, що існує можливість вразливостей постквантових ЕЦП до класичного криптоаналізу. Тоді доцільно розглядати не послідовність ігор, як в роботах [1 – 3], а їх паралельну комбінацію. Тобто, нехай є класична гра G_c^{FOR} та квантова гра G_q^{FOR}, які обчислювально незначною мірою відрізняються від алгоритму 1. Тоді загальна вірогідність успіху зловмисника дорівнює 1, якщо він має успіх принаймні в одній з ігор, тобто $\Pr(G_c^{FOR}) + \Pr(G_q^{FOR}) = 1$. При цьому, в першій грі зловмисник використовує класичний комп'ютер, а в другій – квантовий.

Відповідна модель зловмисника має формалізований вигляд алгоритму 2.

Алгоритм 2.

Схема підпису: $\Pi = (KGen, Sign, Vrfy)$.

1. C генерує $(pk, sk) \leftarrow KGen(1^n)$. Відправляє pk зловмиснику A.

2. A робить запити на формування підписів від повідомлень $\{m_i\}$. C повертає $\sigma_i := Sign(sk, m_i)$. Ці повідомлення обираються адаптивно самим A.

3. A формує $(m*, \sigma*)$. Якщо $Vrfy(pk, (m*, \sigma*)) = 1$ та $m* \notin \{m_i\}$, $C_1 = 1$. Інакше $C_1 = 0$.

4. A формує $(m*, \sigma*)_{QuantComp}$. Якщо $Vrfy(pk, (m*, \sigma*)_{QuantComp}) = 1$, $C_2 = 1$. Інакше $C_2 = 0$.

5. Якщо $C_1 \vee C_2 = 1$, C оголошує успіх. Інакше оголошує невдачу.

Аналіз моделі загроз, наведеної в алгоритмі 2, показав що криптопримітиви ЕЦП потрібно конструювати з врахуванням вимог часу та використовувати математичний базис квантовостійкої однопрохідної функції. При цьому потрібно оцінювати загальну захищеність від зламу за допомогою класичних обчислень, що ускладнює і модель зловмисника.

Доказ різних випадків моделей зловмисника та зведення моделі із класичного випадку до квантового потребують подальших досліджень.

Розглянемо модель загроз ЕЦП, яка випливає із відомих класичних та квантових моделей загроз, та з'ясуємо особливості зазначених вище підходів за умови виникнення квантового комп'ютера. Для цього зробимо класифікацію за типом загрози, що несуть дії порушника:

1. *Атака на основі відомого відкритого ключа* (key-only attack). Практично завжди доступна криптоаналітику (порушнику), оскільки може виконуватися при знанні загальносистемних параметрів й діючих відкритих ключах.

2. *Атака на основі відомих підписаних повідомлень* (known-message attack). В розпорядженні криптоаналітика, разом із даними з попередньої атаки, є деяке число пар $(m, signature)$ підписаних повідомлень m, при цьому відсутня можливість вибору повідомлення m зловмисником.

3. *Проста атака з вибором підписаних повідомлень* (generic chosen-message attack). Криптоаналітик має можливість вибрати деяку кількість підписаних повідомлень, знає загальносистемні параметри і має після вибору підписаних повідомлень доступ до відкритих ключів.

4. *Спрямована атака з вибором повідомлення* (direct chosen-message attack). Криптоаналітик знає загальносистемні параметри, може на свій розсуд вибрати відкритий ключ і після цього вибрати підписані повідомлення.

5. *Адаптивна атака з вибором підписаного повідомлення* (adaptive chosen-message attack). При здійсненні атаки криптоаналітик може вибирати відкритий ключ, а також підписане повідомлення. При цьому вибір наступного підписаного повідомлення він може робити на основі знання припустимого підпису попереднього обраного повідомлення.

Проведений аналіз показав, що кожна атака спрямована на досягнення визначеної мети. З урахуванням цього, для всіх схем ЕЦП у порядку зростання небезпеки можна виділити такі види погроз [4].

1. *Екзистенційна підробка* (existential forgery). Загроза полягає в створенні підпису для будь-якого, можливо безглуздого повідомлення m', що відрізняється від дійсного повідомлення, що підписується.

2. *Селективна підробка* (selective forgery) – це можливість створення для заздалегідь обраного повідомлення m правильного ЕЦП.

3. *Універсальна підробка* (universal forgery) – знаходження криптоаналітиком алгоритму формування підпису, функціонально еквівалентному дійсному алгоритму ЕЦП, без використання або із використанням дійсного особистого ключа.

4. *Повне розкриття* (total break). При цій загрозі криптоаналітик може обчислити таємний ключ, який відповідає відкритому ключу Q. Це дозволяє криптоаналітику формувати цифрові підписи для будь-яких повідомлень і надалі нав'язувати ці повідомлення кореспондентам.

Розглянемо модель загроз ЕЦП у відповідності до наступної методики редукції доказів. Атакуючий намагається досягти певних зловмисних цілей (які складатимуть компрометацію системи). Компрометація може включати обчислення особистого ключа або підробку двох певних повідомлень. Редукція, яка становить доказ, – це доказ того, що якщо атакуючий може досягти мети компрометації, то атакуючий (з невеликим додатковим обсягом роботи) здатний досягти і деякої іншої мети, додаткової компрометації, можливо пов'язаних з "примітивом" нижчого рівня, на якому заснована схема. Твердження, що доводиться, має вигляд: "Якщо противник може зробити 'X', то він також повинен вміти робити 'Y'". Зазвичай конструюється такий доказ, щоб 'Y' було будь-яким видом обчислень, яке вважається важко здійснюваним. Якщо приймається припущення, що противник не може зробити 'Y', тоді витікає логічний висновок доказу, що приймається також і те, що противник не може зробити 'X' (принаймні якщо він діє в рамках даної моделі атаки).

Відповідно до вказаних методів редукції доказів безпеки досить просто класифікувати вказані погрози ЕЦП за додатковою складністю криптоаналіза в порівнянні із криптоаналізом більш загальної задачі зламу. Так, якщо противник може зробити атаку типу повне розкриття, то він також повинен вміти робити всі інші види атак із додатковою поліноміальною складністю. Очевидно, якщо противник може зробити атаку типу універсальна підробка, то він також повинен вміти робити всі інші види атак підробки із додатковою поліноміальною

складністю. У свою чергу, селективна підробка включає, за логікою редукції, можливість виконання екзистенційної підробки не вище, ніж із додатковою поліноміальною складністю. Дану редукційну модель представимо в вигляді однонаправленого графу, вершини якого представляють тип атаки (рис. 1). Стрілки позначають редукцію переходу із одного типу атаки до іншого.

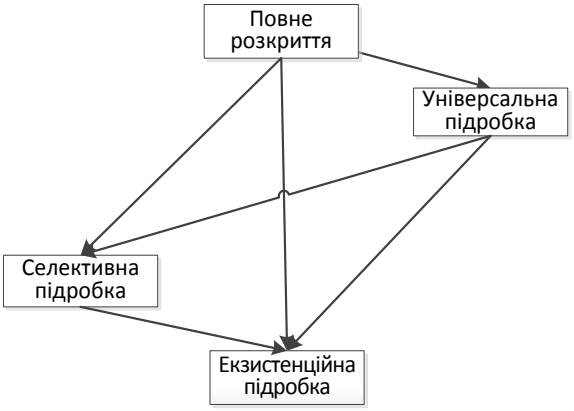

Рис. 1. Схема редукційної моделі атак на ЕЦП

Зв'язки в редукційній моделі для класичного криптоаналізу позначають відношення більш загального виду атаки до часткового випадку. Але якщо противник може зробити атаку типу екзистенційна підробка, то він не обов'язково зможе зробити атаку повного розкриття із додатковою поліноміальною складністю. В противному випадку підпис є нестійким.

Ця схема справедлива для загального випадку і є, скоріше, ідеальною моделлю, тому вона може змінюватися в залежності від різних умов. Порушення чи видозмінення цієї схеми залежать від існування тих чи інших атак на конкретний підпис та від базових параметрів ЕЦП. З'ясуємо ці зміни в редукційній моделі у випадку атак із застосуванням квантового алгоритму Гровера в загальному вигляді. Припустимо, зловмиснику доступний квантовий комп'ютер, який використовує алгоритм Гровера квантового пошуку із часовою складністю [20] $O(\sqrt{N})$, що зменшилась по відношенню до складності класичних алгоритмів як корінь квадратний від об'єму обчислень класичних алгоритмів. Оскільки алгоритм Гровера є атакою повного перебору, то відмінність в складності різних типів атак, що досліджуються, буде залежати від вхідних даних алгоритму. Множина вхідних даних для атаки повного розкриття визначається областю допустимих значень множини ключів, що кількісно виражається довжиною ключа. Множина вхідних даних для атак підробки визначається областю допустимих значень повідомлень чи підписів (довжина повідомлення чи підпису). Із цього слідує, що за умови, якщо конкретний алгоритм ЕЦП має однакову довжину ключа та підпису, то для атак на квантовому комп'ютері із використанням алгоритму Гровера змінюється схема зв'язків в редукційній моделі (див. рис. 1). Оскільки алгоритм грубого пошуку не оптимізований під яку-небудь конкретну задачу, то складність атак типу повне розкриття та універсальна підробка буде тією самою.

Так, повний перебір ключів алгоритмом Гровера змінює складність $O(N) \to O(\sqrt{N})$ у порівнянні з класичним повним перебором, а складність знаходження колізій зменшується у порівнянні із класичною атакою як $2^{n/2} \to 2^{n/3}$. Тобто, для алгоритму Гровера повний перебір ключа має складність $2^{n/2}$, яка не набагато більша, ніж складність знаходження колізій $2^{n/3}$. Відповідно до вищесказаного, атаки у загальному вигляді мають наступні оцінки:

- атака повного розкриття має складність $2^{n/2}$;
- атака універсальної підробки має складність $2^{n/2}$;
- атака селективної підробки має складність $2^{n/2}$;
- атака екзистенційної підробки має складність $2^{n/3}$.

Таким чином, редукційна модель буде мати вигляд, представлений на рис. 2.

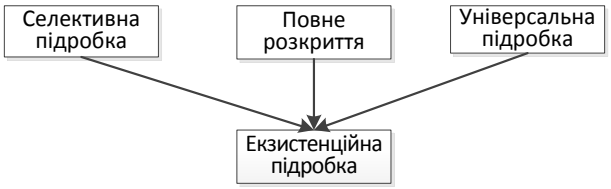

Рис. 2. Схема редукційної моделі атак на ЕЦП
у випадку застосування квантового алгоритму Гровера

Запропонована у даному пункті класифікація методів криптоаналізу дозволяє чітко визначити напрямки подальших досліджень щодо розробки методів та побудови систем захисту інформації. Урахування даних зауважень може бути корисними при розробці нових чи оцінці існуючих моделей захисту ЕЦП. Розроблена модель порушника в квантових системах захисту інформації дозволяє визначити напрямки підвищення безпеки постквантових криптопримітивів ЕЦП.

3. Оцінка загроз схеми ЕЦП для класичних та квантових атак

З метою завершення аналізу моделі порушника ЕЦП, що діє в умовах появи квантових обчислень та їх практичного застосування, зробимо основні кількісні оцінки загроз класичних і постквантових ЕЦП на основі складності відомих атак.

Для цього наведемо оцінки стійкості перетворень в кільці (RSA), скінченному полі (DSA) та групі точок еліптичних кривих (EC-DSA). Обрахуємо та занесемо результати оцінки складності криптоаналізу (оцінки стійкості) криптографічних перетворень в таблиці.

Спочатку визначимо складність криптоаналізу для перетворень у кільці. Очевидно, найменш складним буде криптоаналіз, що застосовується на факторизації модуля перетворення N з використанням загального решета числового поля [0]:

$$I_K = \exp\left\{\delta\left(\log N\right)^{\nu}\left(\log\log N\right)^{1-\nu}\right\}. \tag{1}$$

При криптоаналізі криптографічних перетворень у полі Галуа $GF(p)$ найбільш складною є задача розв'язання дискретного логарифмічного рівняння

$$Y_i = \theta_v^{X_i} \left(\mathrm{mod}\, p\right). \tag{2}$$

Складність розв'язання (2) також може бути оцінена з використанням формули [4]:

$$I_K = \exp\left\{\delta\left(\log N\right)^{\nu}\left(\log\log N\right)^{1-\nu}\right\}. \tag{3}$$

Якщо розв'язок базується на використанні решета числового поля, то для дискретного логарифмування у (3) треба застосовувати $\delta = 1/92, \nu = 1/3$, а для випадку факторизації у (1) застосовуються $\delta = 1,90, \nu = 1/3$ [4].

Складність криптоаналізу в групі точок ЕК при використанні оптимального методу ρ – Полларда можна оцінити як

$$I^2 - 1 + n\ln\left(1 - P_k\right) = 0 \tag{4}$$

або спрощеною формулою

$$I_\rho = \sqrt{\frac{\pi \cdot n}{4}} \text{ чи } I_\rho \approx \sqrt{-2n\ln\left(1-P_k\right)},$$

де n – порядок базової точки G в групі точок ЕК.

На основі перелічених оцінок приведемо аналіз існуючих ЕЦП.

Приклад. Необхідно порівняти криптоперетворення в кільцях (RSA), полях (DSA) та групі точок ЕК (EC-DSA) за критерієм складності виконання та визначити вартість криптоаналізу методом повного розкриття, при якому криптоаналітик знаходить секретний (особистий) ключ абонента, якщо довжини модулів криптоперетворень в кільці, полі та групі точок ЕК відповідно дорівнюють $l = 336$ бітів.

Розв'язання. Для випадку факторизації маємо:

$$I_K = \exp\left[1.90\left(\ln 2^{336}\right)^{\frac{1}{3}}\left(\ln\ln 2^{336}\right)^{\frac{2}{3}}\right] = \exp\left(1.90\cdot 6{,}17\cdot 3{,}1\right) = \exp\left(39{,}78\right) = 8\cdot 10^{15}.$$

Для випадку дискретного логарифмування маємо:

$$I_П = \exp\left[1{,}92\left(\ln 2^{336}\right)^{\frac{1}{3}}\left(\ln\ln 2^{336}\right)^{\frac{2}{3}}\right] = \exp\left[1{,}92\left(\frac{\log_2 2^{336}}{\log_2 e}\right)^{\frac{1}{3}}\left(\ln\left(\frac{\log_2 2^{336}}{\log_2 e}\right)\right)^{\frac{2}{3}}\right] =$$

$$= \exp\left[1{,}92\left(\frac{336}{1{,}43}\right)^{1/3}\left(\ln\left(\frac{336}{1{,}43}\right)\right)^{2/3}\right] = \exp\left[1{,}92\cdot\left(234{,}96\right)^{1/3}\left(\ln 234{,}96\right)^{2/3}\right] =$$

$$= \exp\left(1{,}92\cdot 6{,}17\cdot 3{,}1\right) = \exp\left(36{,}7\right) = 8{,}9\cdot 10^{15}.$$

Для дискретного логарифмування в групі точок ЕК маємо:

$$I = \sqrt{\frac{\pi\cdot n}{4}} = \sqrt{\frac{3{,}14\cdot 2^{336}}{4}} = 0{,}886\cdot 2^{168} = 8{,}86\cdot 10^{49}.$$

Порівняння отриманих результатів дозволяє зробити такі висновки:

- криптографічна стійкість проти атаки «повне розкриття» при застосуванні криптоперетворення в групі точок еліптичної кривої має експоненційний характер і суттєво перевищує стійкість криптоперетворень у кільці (факторизація) та в скінченному полі Галуа (дискретне логарифмування);

- стійкість криптоперетворень у кільці та в скінченному полі має суб'експоненційний характер і оцінки значень складності криптоаналізу практично співпадають.

В табл. 1 приведено аналогічні оцінки для основних стандартів ЕЦП, що застосовуються зараз:

– RSA (ДСТУ ISO/IEC 14888-2 на основі RSA) (число множень розміру N);

– DSA (ДСТУ ISO/IEC 14888-3 (DSA) та ДСТУ ISO/IEC 9796-2 (DSA)) (число множень розміру P);

– EC (ДСТУ 4145-2002, ДСТУ ISOIEC 14888-3 (ЕК) та ДСТУ ISOIEC 9796-3 (ЕК)) (число операцій складання на ЕК розміру n).

Для постквантових застосувань більшість відомих та стандартизованих алгоритмів ЕЦП є непридатними, бо складність квантового криптоаналізу дуже низька (див. таблицю). Тому основні перспективні дослідження і розробки криптографічних засобів захисту інформації в нинішній час спрямовані на пошуки рішень, які не мали б вразливостей по відношенню до квантових обчислень, будучи одночасно стійкими до атак за допомогою звичайних комп'ютерів.

В результаті аналізу стійкості криптопримітивів виділяють такі перспективні постквантові кандидати:

- криптографія на основі хеш-функцій (Hash Based);
- криптографія на основі перешкодостійких кодів (Code Based);
- криптографія на основі решіток (Lattice Based);
- криптографія на основі факторизації поліномів (Multivariate Polynomial Based).

Існують різні схеми ЕЦП, зокрема на основі перешкодостійких кодів (CFS, Paralell CFS); підписи на основі апарату хеш-функцій (Lamport та XMSS); схеми ЕЦП на решітках (BLISS та NTRU); ЕЦП на основі факторизації поліномів (Rainbow).

Стандарт/ оцінки	Алгоритм/ Складність КРА	Мінімальна довжина	Максимальна n	Мінімальна стійкість	Максимальна стійкість	Складні квантов алгорит
СТУ 4145-2002/ спон.	ДСТУ 4145-2002	2^{163}	2^{431}	$2^{24,5}$	$2^{64,5}$	10^{10}
СТУ ISOIEC 14888-3 К)\експон.	EC-DSA	2^{160}	2^{571}	2^{80}	$2^{285,5}$	6.7·10
	EC-GDSA	2^{160}	2^{571}	2^{80}	$2^{285,5}$	6.7·10
	EC-KCDSA	2^{160}	2^{571}	2^{80}	$2^{285,5}$	6.7·10
	EC-RDSA	2^{256}	2^{256}	2^{128}	2^{128}	$6\cdot10^{9}$
	EC-SDSA	2^{256}	2^{384}	2^{128}	2^{192}	$6\cdot10^{9}$
	EC-FSDSA	2^{256}	2^{384}	2^{128}	2^{192}	$6\cdot10^{9}$
ДСТУ ISOIEC 9796-3 (ЕК)/експон.	ECPV	2^{161}	2^{163}	$2^{80,5}$	$2^{81,5}$	1.6·10
	ECNR	2^{158}	2^{163}	2^{79}	$2^{81,5}$	1.6·10
	ECAO	2^{192}	2^{200}	2^{96}	2^{100}	1.6·10
	ECKNR	2^{160}	2^{163}	2^{80}	$2^{81,5}$	1.6·10
	ECMR	2^{160}	2^{163}	2^{80}	$2^{81,5}$	1.6·10
ДСТУ ISOIEC 14888-3 (Спарюв. точок ЕК)/ експон	IBS1	2^{512}	2^{1024}	2^{256}	2^{512}	3.8 ·10
	IBS2	2^{512}	2^{1024}	2^{256}	2^{512}	3.8 ·10
Стандарти RSA		Мінімальне N	Максимальне N	Мінімальна стійкість	Максимальна стійкість	
Стандарти ЕП 14888-2 на основі RSA / субекспон.	RSA/RW	2^{750}	2^{4999}	$2^{51,86}$	2^{116}	12·10
	GQ1/GQ2	2^{750}	2^{4999}	$2^{51,86}$	2^{116}	12·10
	GPS1	2^{750}	2^{4999}	$2^{51,86}$	2^{116}	12·10
	GPS2	2^{750}	2^{4999}	$2^{51,86}$	2^{116}	12·10
	ESIGN	2^{750}	2^{4999}	$2^{51,86}$	2^{116}	12·10
Стандарти DSA		Мінімальне P	Максимальне P	Мінімальна стійкість	Максимальна стійкість	
ДСТУ ISOIEC 14888-3 (DSA)/субексп.	DSA	2^{1024} (заборонено) 2^{2048} (дозволяється)	2^{3072} (використовується) (можна використовувати значення більше за 2^{3072})	2^{80}	$2^{96,01}$	2.9·10
	KCDSA	2^{1024} (заборонено) 2^{2048} (дозволяється)	2^{3072} (використовується) (можна використовувати значення більше за 2^{3072})	2^{80}	$2^{96,01}$	2.9·10
	Pointcheval/	2^{1024} (заборонено) 2^{2048} (дозволяється)	2^{3072} (використовується) (можна використовувати значення більше за 2^{3072})	2^{80}	$2^{96,01}$	2.9·10
	Vaudenay	2^{1024} (заборонено) 2^{2048} (дозволяється)	2^{3072} (використовується) (можна використовувати значення більше за 2^{3072})	2^{80}	$2^{96,01}$	2.9·10
	SDSA	2^{1024} (заборонено) 2^{2048} (дозволяється)	2^{3072} (використовується) (можна використовувати значення більше за 2^{3072})	2^{80}	$2^{96,01}$	2.9·10
ДСТУ ISOIEC 9796-3 (DSA)/експон.	NR	2^{1024}	2^{3072}	2^{80}	$2^{96,01}$	2.9·10

Стандарт/ оцінки	Алгоритм/ Складність КРА	Мінімальна довжина	Максимальна n	Мінімальна стійкість	Максимальна стійкість	Складність квантового алгоритму
Постквантові підписи	BLISS	2^{2000}	2^{3000}	$10^{206,36} = 2^{619,08}$	$10^{315,86} = 2^{947,58}$	$2^{n/2-1} =$
	CFS	m, t =(11,4)	m, t =(12,45)	2^{98}	2^{140}	2^{133}
	XMSS	n=256, H=85	n=512, H=170	$2^{n/2-1} = 2^{127}$	$2^{n/2-1} = 2^{255}$	$2^{n/3} = 2$ $2^{512/3} =$
	Rainbow	2^{561352}	-	2^{128} -	-	2^{280676}
	KCDSA	2^{1024} (заборонено) 2^{2048} (дозволяється)	2^{3072} (використовується) (можна використовувати значення більше за 2^{3072})	2^{80}	$2^{96,01}$	$2.9 \cdot 10^{10}$
	Pointcheval/	2^{1024} (заборонено) 2^{2048} (дозволяється)	2^{3072} (використовується) (можна використовувати значення більше за 2^{3072})	2^{80}	$2^{96,01}$	$2.9 \cdot 10^{10}$
	Vaudenay	2^{1024} (заборонено) 2^{2048} (дозволяється)	2^{3072} (використовується) (можна використовувати значення більше за 2^{3072})	2^{80}	$2^{96,01}$	$2.9 \cdot 10^{10}$
	SDSA	2^{1024} (заборонено) 2^{2048} (дозволяється)	2^{3072} (використовується) (можна використовувати значення більше за 2^{3072})	2^{80}	$2^{96,01}$	$2.9 \cdot 10^{10}$
OIEC 9796-3 (DSA)/експон.	NR	2^{1024}	2^{3072}	2^{80}	$2^{96,01}$	$2.9 \cdot 10^{10}$
остквантові підписи	BLISS	2^{2000}	2^{3000}	$10^{206,36} = 2^{619,08}$	$10^{315,86} = 2^{947,58}$	$2^{n/2-1} = 2^{999}$
	CFS	m, t =(11,4)	m, t =(12,45)	2^{98}	2^{140}	2^{133}
	XMSS	n=256, H=85	n=512, H=170	$2^{n/2-1} = 2^{127}$	$2^{n/2-1} = 2^{255}$	$2^{n/3} = 2^{84}$; $2^{512/3} = 2^{256}$
	Rainbow	2^{561352}	-	2^{128} -	-	2^{280676}

Де H – це висота дерева Меркля, n – розмір хеш-функції, 2^m – це розмір особистого ключа, де m – кількість біт, t – це виправляюча здатність лінійного коду.

Висновки

В ході досліджень розглянуто загальну модель порушника та загроз ЕЦП та спрощену модель середовища взаємодії відправника та отримувача в умовах дій зловмисника. В розглянутій моделі застосовується поняття випадкового оракула, до якого мають доступ всі учасники взаємодії. При кожному новому запиті значення функції вибирається випадковим чином і оракул запам'ятовує пару (аргумент, значення). При повторному запиті для цього аргументу, незалежно від того, хто з учасників його видав, буде повернуто те саме запам’ятоване значення. Модель із випадковим оракулом застосовується для протоколів ЕЦП, де випадкова функція замінила хеш-функцію. В класичному варіанті сам алгоритм підпису та всі учасники, крім зловмисника, здійснюють доступ до випадкового оракула за допомогою класичних бітових рядків.

На основі розглянутої моделі середовища взаємодії відправника та отримувача в умовах дій зловмисника із випадковим оракулом було досліджено модель порушника ЕЦП в умовах появи квантового комп’ютера. Для врахування особливостей квантових обчислень та, зокрема, можливостей щодо здійснення квантового криптоаналізу в дослідженій моделі порушника ЕЦП застосовано поняття *випадкового оракула квантовим із доступом.* Відповідно до розглянутої моделі зловмисник може оцінювати випадкового оракула через явище суперпозиції, тобто зловмисник може відправляти квантові стани $\langle\varphi| = \sum c_x |x\rangle$ до оракула O та отримувати назад "оцінені" стани $\sum c_x |O(x)\rangle$. У той же час сам алгоритм підпису та всі інші учасники, крім зловмисника, здійснюють доступ до випадкового оракула за допомогою класичних бітових рядків (без використання явища суперпозиції). Однією з відмінностей класичного випадкового оракула, порівняно з квантовим, є те, що в його моделі симулюються прообрази, потрібні криптоаналітику. Для випадкового оракула з квантовим доступом відповідь на запит може бути схована в суперпозиції в експоненційно великому наборі квантових станів, і не зрозуміло, як отримати необхідні відповіді. В класичному випадку можна ефективно змоделювати експоненційного випадкового оракула, просто обираючи випадкові відповіді. У випадку оракула з квантовим доступом зловмисник може отримати всі відповіді одночасно на всі вхідні запити. Це ускладнює стратегію запит-відповідь, яка застосовується в класичних випадкових оракулах і яка є більш узгодженою.

Із застосуванням моделі середовища взаємодії відправника та отримувача формалізовано поведінку зловмисника при екзистенційній підробці. При цьому застосовано моделі та методи теорії ігор. Зокрема, модель зловмисника у вигляді взаємодії двох сторін (зловмисника A та чесної сторони C) розглядається на основі паралельного об'єднання різних ігор: класичної гри G_c^{FOR} та квантової гри G_q^{FOR}. Загальна вірогідність успіху зловмисника дорівнює 1, якщо він має успіх принаймні в одній з ігор, тобто $\Pr(G_c^{FOR}) + \Pr(G_q^{FOR}) = 1$. При цьому, в першій грі зловмисник використовує класичний комп'ютер, а в другій – квантовий. Відповідну модель зловмисника подано у формалізованому вигляді обчислювального алгоритму.

Аналіз моделі загроз, заснованої на паралельному об'єднанні різних (класичних та квантових) ігор, показав що криптопримітиви ЕЦП потрібно конструювати з врахуванням вимог часу та використовувати математичний базис квантовостійкої однопрохідної функції. При цьому потрібно оцінювати загальну захищеність від зламу за допомогою класичних обчислень, що ускладнює і модель зловмисника. Доказ різних випадків моделей зловмисника та зведення моделі із класичного випадку до квантового потребують подальших досліджень.

Розглянута модель загроз ЕЦП, яка випливає із відомих класичних та квантових моделей загроз, дозволила ввести певну класифікацію різних атак за типом загрози, що несуть дії порушника. Відповідно до розглянутих методів редукції доказів безпеки зазначені загрози ЕЦП класифіковано за додатковою складністю криптоаналізу в порівнянні із більш загальної задачі криптоаналізу. Таку класифікацію подано як редукційну модель у вигляді однонапра-

вленого графіку, вершини якого представляють тип атаки, а стрілки позначають редукцію переходу із одного типу атаки до іншого. Зв'язки в редукційній моделі для класичного криптоаналізу позначають відношення більш загального виду атаки до часткового випадку.

Розглянута редукційна модель загроз ЕЦП є ідеалізованою моделлю, яка може змінюватися в залежності від різних умов, наприклад від існування тих чи інших атак на конкретний підпис та від базових параметрів ЕЦП. У випадку існування атак із застосуванням квантового алгоритму Гровера часова складність квантового пошуку зменшується по відношенню до складності класичних алгоритмів як корінь квадратний від об'єму обчислень класичних алгоритмів. Тобто, повний перебір ключів алгоритмом Гровера змінює складність $O(N) \to O(\sqrt{N})$ у порівнянні з класичним повним перебором, а складність знаходження колізій зменшується у порівнянні із класичною атакою, як $2^{n/2} \to 2^{n/3}$. Тобто, для алгоритму Гровера повний перебір ключа має складність $2^{n/2}$, яка не набагато більша, ніж складність знаходження колізій $2^{n/3}$. Відповідно до цього, складність атак у загальному вигляді змінюється, що призводить і до зміни редукційної моделі переходу із одного типу атаки до іншого. Урахування даних зауважень може бути корисним при розробці нових чи оцінці існуючих моделей захисту ЕЦП, зокрема розроблена модель порушника в квантових системах захисту інформації дозволяє визначити напрямки підвищення безпеки постквантових криптопримітивів ЕЦП.

З метою завершення аналізу моделі порушника ЕЦП, що діє в умовах появи квантових обчислень, та їх практичного застосування, в роботі отримано основні кількісні оцінки загроз класичних і постквантових ЕЦП на основі складності відомих атак. Порівняння отриманих результатів дозволило зробити такі висновки:

- криптографічна стійкість (в умовах класичних обчислень) проти атаки «повне розкриття» при застосуванні криптоперетворення в групі точок еліптичної кривої має експоненційний характер і суттєво перевищує стійкість криптоперетворень у кільці (факторизація) та в скінченному полі Галуа (дискретне логарифмування); стійкість криптоперетворень у кільці та в скінченному полі має суб'експоненційний характер і оцінки значень складності криптоаналізу практично співпадають;

- для постквантових застосувань більшість відомих та стандартизованих алгоритмів ЕЦП є неприйнятними, бо складність квантового криптоаналізу дуже низька. Тому перспективним є дослідження і розробка таких криптопримітивів, які не мали б вразливостей по відношенню до квантових обчислень та були одночасно стійкими до атак за допомогою звичайних комп'ютерів. До перспективних постквантових алгоритмів ЕЦП слід віднести: ЕЦП на основі перешкодостійких кодів (CFS, Paralell CFS); підписи на основі апарату хеш-функцій (Lamport та XMSS); схеми ЕЦП на решітках (BLISS та NTRU); ЕЦП на основі факторизації поліномів (Rainbow).

Список літератури: 1. *A Note* on Quantum Security for Post-Quantum Cryptography Fang Song Department of Combinatorics & Optimization and Institute for Quantum Computing University of Waterloo. https://eprint.iacr.org/2010/428.pdf 2. *Random* Oracles in a Quantum World Dan Boneh1, Ozgur Dagdelen2, Marc Fischlin2, Anja Lehmann3, Christian Schaner, and Mark Zhandry Stanford University, USA https://eprint.iacr.org/2014/709.pdf 3. *Towards* a Game Theoretic View of Secure Computation / Gilad Asharov, Ran Canetti, Carmit Hazay http://gir.bmstu.ru/data/ksbp_data/pdf/EUROCRYPT/EC_2011.00024_ Towards_a_Game_Theoretic_View_of_Secure_Computation.pdf 4. *Прикладна* криптологія. Теорія. Практика. Застосування : монографія / І. Д. Горбенко, Ю. І. Горбенко; Харк. нац. ун-т радіоелектрон., ЗАТ "Ін-т інформ. технологій". – Х. : Форт, 2012. – 868 с. 5. *ETSI White* Paper No. 8, Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges, June 2015. Режим доступу: http://www.etsi.org/ – 24.07.2016 – Загл. с экрана. 6. *Third* International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010, Proceedings NSA acknowledges need for quantum-safe crypto. [Електронний ресурс]. Режим доступу: http://www.idquantique.com/nsa-quantum-safe-crypto/-

24.07.2016 – Загл. с экрана. 7. *NISTIR 8105 DRAFT* Report on Post-Quantum Cryptography. National Institute of Standards and Technology Internal, Report 8105. [Електронний ресурс]. Режим доступу: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf – 24.07.2016 – Загл. с экрана. 8. *Evaluating* Post-Quantum Asymmetric Cryptographic Algorithm Candidates / Tolga Acar, Josh Benaloh, Craig Costello and Dan Shumow. – MSR Security and Cryptography Group. [Електронний ресурс]. Режим доступу: http://csrc.nist.gov/groups/ST/post-quantum-2015/presentations/session7-shumow-dan.pdf – 24.07.2016 – Загл. с экрана. 9. *Bernstein, D.* Post-quantum cryptography / D. Bernstein, J. Buchmann, E. Dahmen. – Berlin: Springer, 2009. – 246 p. 10. *Горбенко, Ю. І.* Аналіз шляхів розвитку криптографії після появи квантових комп'ютерів / Ю. І. Горбенко, Р. С. Ганзя // Вісник Національного університету "Львівська політехніка". 2014. № 806. С. 40-48. 11. *Daniel J. Bernstein, Daira Hopwood, Andreas Helsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Peter Schwabe, and Zooko Wilcox O'Hearn*. Sphincs: practical stateless hash-based signatures. Cryptology ePrint Archive, Report 2014/795, 2014/ Daniel J. Bernstein, Daira Hopwood, Andreas Helsing. [Електронний ресурс]. Режим доступу:http://eprint.iacr.org/- 24.07.2016 – Загл. с экрана. 12. *Ray, A.* Perlner and David A. Cooper Quantum resistant public key cryptography: a survey. In Proceedings of the 8th Symposium on Identity and Trust on the Internet (IDtrust '09), Kent Seamons, Neal McBurnett, and Tim Polk (Eds.). – New York, ACM, 2009. P. 85-93. 13. *Enhanced* Lattice-Based Signatures on Recon gurable Hardware Extended Version [Электронный ресурс]. – Режим доступа : https://eprint.iacr.org/2014/254.pdf. – Заглавие с экрана. 14. *Богданов, А.Ю.* Квантовые алгоритмы и их влияние на безопасность современных классических криптографических систем / А.Ю. Богданов, И.С. Кижватов. – М. : РГГУ, 2005. 15. *M. Finiasz* Parallel-CFS – Strengthening the CFS McEliece-Based Signature Scheme. In A. Biryukov, G. Gong, and D.R. Stinson, editors, Selected Areas in Cryptography, vol. 6544 of Lecture Notes in Computer Science. – Springer Berlin Heidelberg, 2011. P. 159 – 170. 16. *Берлекэмп, Э.* Алгебраическая теория кодирования. – М. : Мир, 1971. – 234 с. 17. *McEliece R.J.* A Public-Key Criptosystem Based on Algebraic Theory // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January – February, 1978. – P. 114-116. 18. *W. Whyte*. IEEE P1363.1 Draft 10: Draft Standard for Public Key Crypto-graphic Techniques Based on Hard Problems over Lattices [Електронний ресурс] / N. Howgrave-Graham, J. Hostein, J. PIpher, J.H. Silverman. Режим доступу: http://grouper.ieee.org/groups/1363/ WorkingGroup/contact.html. 19. *Shor, P.* (1997), «Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer», SIAM J. Comput., 26 (5), pp.1484-1509. 20. *Grover, L.* (1996), «A fast quantum mechanics algo- rithm for database search», Proceeding of the 28th ACM Symposium on Theory of Computation. New York: ACM Press, pp. 212-219. 21. *Китаев, А. Шень, А., Вялый, М.* Классические и квантовые вычисления. – М. : МЦНМО, 1999. – 192 с.

Харківський національний
університет імені В. Н. Каразіна

Надійшла до редколегії 11.09.2016