УДК 003.026:004.056

Ю.І. ГОРБЕНКО, канд. техн. наук, Т.В. МЕЛЬНИК, І.Д. ГОРБЕНКО, д-р техн. наук

АНАЛІЗ ПОТЕНЦІЙНИХ ПОСТКВАНТОВИХ МЕХАНІЗМІВ ЕЛЕКТРОННИХ ПІДПИСІВ НА ОСНОВІ ГЕШ-ФУНКЦІЙ

Вступ

В 2015 – 2017 рр. відбувся ряд значущих подій та прийняті на світовому рівні рішення, які визначили необхідність розробки та стандартизації постквантової асиметричної криптографії. До них необхідно віднести Інтернет – статтю [1], VII міжнародної конференцію з постквантової криптографії та її рекомендації, звіт «Report on Post – Quatum Cryptography. NISTIR 8105 (DRAFT) [2]», а також оголошення NIST США конкурсу на постквантові стандарти електронного підпису(ЕП) та асиметричного шифрування (АШ) [3] тощо. Серед можливих кандидатів на стандарт ЕП певні переваги мають методи, що грунтуються на використанні функцій гешування (НВ криптографія) [4 – 8]. Основні переваги НВ криптографії у використанні існуючих криптографічно стійких функцій гешування, значною швидкодією, прозорістю математичних перетворень та випробуванням функцій гешування часом. В той же час висунуті в [3] вимоги до постквантових ЕП вимагають проведення значних досліджень та порівняння потенційних кандидатів, що будуються на основі НВ криптографії та і інших математичних основ[4, 9] .

В [3] наведено основні вимоги до постквантових криптографічних примітивів – з безпеки застосування, техніко-економічні та техніко-експлуатаційні вимоги. Там же запропоновано критерії та показники відбору серед можливих кандидатів.

Мета цієї статі – відбір, розгляд сутностей та порівняльний аналіз, а також розробка пропозицій з удосконалення та застосування ЕП в обмеженому класі тільки НВ перетворень. В процесі досліджень використовуються визнані чи рекомендовані критерії та показники оцінки та відповідні методики.

Таким чином, нині вирішується проблема створення та стандартизації постквантових криптографічних примітивів типу ЕП. Вона надзвичайно актуальна і вимагає свого розв’язання в найближчі декілька років у відповідності з вимогами NIST США [2 – 4] та ETSI ЄС [10]. Отримані результати досліджень та пропозиції планується подати у вигляді серії статей.

1. Сутність та властивості постквантових ЕП Лампорта

На сьогодні існує декілька механізмів (схем) та складових ЕП, заснованих на геш-функціях. Серед них необхідно відмітити механізми Лампорта [5], Лампорта – Діффі [7], Вінтерніц [6], MSS (Merkle), XMSS, SPHINC, HORS та їх певні модифікації – XMSS-T, SPHINCS, SPHINCS-256, HORST [4, 8, 9]. Особливістю вказаних підписів є те, що їх криптографічна стійкість грунтується на колізійній стійкості функцій гешування та /чи стійкості до знаходження прообразу, так як нині уже розроблено та прийнято у якості геш-функцій ряд по суті стандартизованих постквантових геш-функцій. Запропоновані механізми, що названі вище, на наш погляд, є перспективними [9, 11]. Але залишається ряд проблемних питань, що повинні певною мірою бути вирішеними до початку етапу стандартизації: доведення криптографічної стійкості; мінімізація розмірів загальних параметрів та ключів; мінімізація довжини підпису та підвищення швидкодії ; вироблення та перевіряння ЕП тощо згідно вимог [2 – 7, 8 – 13].

Розглянемо у загальному вигляді сутності та властивості (переваги і недоліки), а також умови, відповідність вимогам, можливості удосконалення та застосування механізмів ЕП на основі НВ криптоперетворень в історичному ракурсі, але розглядаючи цю статтю як першу в досягненні поставленої мети.

1.1. Сутність та особливості механізму ЕП Лампорта

В [4, 5, 9] запропоновані криптографічні перетворення типу електронний підпис (ЕП) для постквантового періоду. Усі вони грунтуються на механізмах ЕП з використанням геш-функцій. Серед перших із них є механізм Лампорт ЕП, який уже раніше досліджувався, але потребує, на наш погляд, додаткового дослідження у зв'язку з новими вимогами та можливими застосуваннями в критичних додатках. Розглянемо та проведемо його аналіз у такій послідовності: узгодження геш-функції та загальних параметрів; генерування ключів; підпис та перевірка підпису; стійкість да потенційних атак та складність реалізації.

Загальні параметри. Підписувач А та перевірник Б узгоджують стандартизовану геш-функцію та її параметри, довжину геш-значення та генератори випадкових чи псевдовипадкових послідовностей (наявність та відповідність вимогам).

Генерування ключів. З використанням генератора чи генераторів випадкових чи псевдовипадкових послідовностей підписувач А генерує *n* секретних ключових пар (X, Y):

$$\begin{aligned} X &= (x_1,\ldots, x_i, \ldots, x_n) \\ Y &= (y_1,\ldots, yi, \ldots, y_n) \end{aligned} \quad (1)$$

з довжиною кожного із секретних ключів l_h, де l_h – довжина геш-значення вибраної геш-функції. При цьому кожна пара (x_i, y_i) є *i*-ю частиною секретного (особистого) ключа.

Відкритий ключ обчислюється засобом гешування секретних ключів (1), як наслідок отримуємо *n* пар відкритих ключів:

$$\begin{aligned} H(X) &= (H(x_1), \ldots, H(x_i), \ldots, H(x_n)) \\ H(Y) &= (H(y_1), \ldots, H(y_i), \ldots, H(y_n)), \end{aligned} \quad (2)$$

з довжиною геш-значення l_h .

Секретні ключі (1) загалом є обов'язково конфіденційними (особистими) та повинні бути доступними тільки підписувачу *A*. Відкриті ключі (2) опубліковуються чи є доступними усім користувачам Б іншим чином, що можуть отримувати від *A* підписані повідомлення.

Підпис повідомлення. При підписі повідомлення *M* підписувач *A* гешує повідомлення *M* з використанням узгодженої (як правило криптографічної) геш-функції з параметрами *Pr* та отримує геш-значення

$$h_M = H(M, Pr)) \quad (3)$$

Далі значення h_M, по суті, зашифровується засобом заміни бітів геш-значення h_M секретними одноразовими ключами із (1), причому кожен h_{Mi} біт, що приймає значення «0», замінюється послідовно секретним ключем із множини (1) X, а h_{Mi} біт, що приймає значення «1» заміняється послідовно секретним ключем із множини (1) Y. Процес такого зашифрування продовжується для усіх бітів геш-значення h_{Mi} .

Таким чином, l_h бітів геш-значення h_{Mi} заміняються (зашифровуються) по суті безумовно стійким шифром, оскільки послідовність бітів h_{Mi} заміняється одноразовими секретними ключами (x_i, y_i). Вказана послідовність l_h секретних ключів і є S ЕП повідомлення M, він разом з вибраними із x_i чи y_i стає відкритим та доступним як користувачам (перевірникам) відповідного домену так і порушнику (криптоаналітику). В подальшому такий ЕП у відповідному форматі передається та зберігається разом з повідомленням і є його ЕП.

У загальному випадку підписане повідомлення можна подати у такому вигляді

$$\{M; Z = (\{x_1 \mid y_1\}), \{x_2 \mid y_2\}, ..., \{x_i \mid y_i\}, ..., \{x_n \mid y_n\}) = \{M, Z = (z_1, z_2, ..., z_i, ..., z_n)\} \quad (4)$$

В (4) символ «|» означає, що при зашифрування в ЕП появляється один із використаних секретних сигналів – x_i чи y_i, що визначається *i*-м бітом геш-значення h_{Mi}. Таким чином, випадкові послідовності $(z_1, z_2, ..., z_i, ..., z_n)$ із секретного ключа стають ЕП повідомлення М.

Зрозуміло, що після зашифрування використані, що були секретними, ключі x_i чи y_i стають відкритими. Але в подальшому будемо враховувати, що відкритими із множини (1) стають лише *n* ключів, а *n* залишились секретними, вони в механізмі Лампорта після вироблення ЕП повинні бути знищеними та більше не використовуватись.

Перевірка ЕП повідомлення. При перевірянні ЕП підписане повідомлення $M*$ має такий вигляд

$$\{M^*; Z^* = (\{x_1 \mid y_1\}), \{x_2 \mid y_2\}, ..., \{x_i \mid y_i\}, ..., \{x_n \mid y_n\}) =$$
$$Z* = (z^*_1, z^*_2, ..., z^*_i, ..., z^*_n), \quad (5)$$

де символ «*» означає, що як повідомлення М, і підпис Z можуть бути викривленими чи підробленими тощо.

Нехай користувач Б хоче перевірити ЕП повідомлення (5). Це він може здійснити у такій послідовності.

1. Здійснює гешування повідомлення M^*, в результаті отримує геш-значення

$$h_{Mi*} = H(M^*, \Pr) \quad (6)$$

2. У відповідності зі значеннями h_{Mi*} із ЕП Z^* у відповідності з усіма значеннями бітів h_{Mi*} із відкритого ключа (2) вибираються геш-значення $H(x_i)$ чи $H(y_i)$.

Причому, якщо обчислене значення h_{Mi*} приймає значення «0», то із відкритого ключа ЕП підписувача А (2) вибирається відповідне значення $H(x_i)$, а якщо «1», то із відкритого ключа ЕП (2) підписувача А вибирається відповідне значення $H(y_i)$. Вказане виконується для усіх значень блоків бітів геш-значення (6) і користувач Б отримує

$$Z' = (\{H(x_1) \mid H(y_1)\}), \{H(x_2) \mid H(y_2)\}, ..., \{H(x_i) \mid H(y_i)\}, ..., \{H(x_n) \mid H(y_n)\}) =$$
$$= (z'_1, z'_2, ..., s'_i, ..., s'_n) \quad (7)$$

3. Користувач Б послідовно гешує усі ключі ЕП (4) та порівнює отримані значення зі значеннями (7) $(z'_1, z'_2, ..., z'_i, ..., z'_n)$. Якщо усі *n* значень при порівнянні співпали, то ЕП вважається справжнім, в іншому випадку ЕП вважається викривленим. Формально перевіряється, що для кожного *i* виконується вимога

$$z'_i = H(z_i). \quad (8)$$

Із наведеного механізму Лампорта слідує, що після зашифрування (4) половина секретних ключів із множин (Х, У) залишились секретними, так як вони знищуються після здійснення ЕП (зашифрування).

Нижче наводяться результати попереднього аналізу криптографічної стійкості ЕП Лампорта. Тут відмітимо основний недолік чи, скоріше всього, проблему реалізації ЕП Лампорта, яка зводиться до великих довжин ключів – як секретного, так і відкритого. Вважаємо, що для застосування ЕП Лампорта основні зусилля повинні бути направленими на її практичне вирішення.

1.2. Особливості одноразового механізму ЕП Лампорта – Діффі

Одною із перших модифікацій механізму ЕП Лампорта є механізм Лампорта – Діффі (LD-OTS) [7 – 9]. Особливістю модифікації механізму є уточнення вимог до геш-функцій. Так, геш-функція, що використовується для обчислення відкритих ключів (2) підписувачем та перевірником при перевірці підпису, є однонаправленою, а геш-функція, що використовується для гешування повідомлення *M* при виробленні ЕП, повинна бути криптографічною.

Загальні параметри. Нехай *l* – додатне ціле число, довжина геш-значення, яке є параметром безпеки механізму. В механізмі використовується однонаправлена геш-функція

$$f :\{0, 1\}^l \to \{0, 1\}^l \quad (9)$$

та криптографічна геш-функція

$$g :\{0, 1\}^* \to \{0, 1\}^l \quad (10)$$

Генерація ключової пари. Секретний ключ ЕП *X* механізму LD-OTS, як і у механізму Лампорта, складається з *2n* випадкових бітових строчок довжини l_h, причому не виключається, що $l_h = n$, тому

$$X= (x_{n-1}[0], x_{n-1}[1], \ldots, x_1[0], x_1[1], x_0[0], x_0[1]) \in R\{0, 1\}^{(n, 2n)} \quad (11)$$

Відкритим ключем підпису *Y* є послідовність строчок

$$Y= (y_{n-1}[0], y_{n-1}[1], \ldots, y_1[0], y_1[1], y_0[0], y_0[1]) \in R\{0, 1\}^{(n, 2n)}, \quad (12)$$

що отримана засобом гешування строчок секретного ключа (11), тобто як

$$y_i[j]= f(x_i[j]),\ 0 \le i \le n-1,\ j =0,1.$$

Таким чином, секретні ключі та відкриті ключі перевірки ЕП Лампорта – Діффі кожен складаються з *2n* строчок довжини *l*.

Підпис повідомлення. Повідомлення M = $\{0, 1\}^*$ підписується з використанням секретного ключа X (11). Спочатку за допомогою криптографічної геш-функції *g* обчислюється геш-значення повідомлення *M*

$$g(M) = h= (h_{l-1}, \ldots, h_0) \quad (13)$$

Безпосередньо ЕП повідомлення *M* буде, аналогічно (4), *n* строчок:

$$\sigma = (x_{n-1}[h_{n-1}], \ldots, x_1[h_1], x_0[h_0]) \in R\{0, 1\}^{(l, n)} \quad (14)$$

Таким чином, ЕП з використанням механізму LD-OTS є послідовність з *n* бітових рядків, кожен з яких довжиною *l*. Тобто ЕП механізму LD-OTS здійснюється аналогічно як і в механізмі Лампорта згідно з (4), *i*-й біт підпису є $x_i[0]$, якщо *i*-й біт геш-значення *h* дорівнює 0, інакше $x_i[1]$, якщо *i*-й біт геш-значення *h* дорівнює 1. *Всього довжина ЕП* складає $l \times n$ бітів, а при *l*=*n* буде $l^2 = n^2$.

Перевірка підпису. Перевірка ЕП механізму LD-OTS здійснюється аналогічно як і в механізмі Лампорта (6) та (8). Спочатку обчислюється геш-значення від повідомлення $h(M^*)$, підпис щодо якого перевіряється. Потім у відповідності зі значеннями h_{Mi*} із ЕП Z^* у відповідності з усіма значеннями бітів h_{Mi*}(0 чи 1) із відкритого ключа (12) вибираються геш-значення *yi[0]* чи *yi[1]*. *Наприкінці за допомогою однонаправленої геш-функції обчислюються геш-значення ЕП* (14), *які порівнюються з отриманими вище з* (12).

Необхідно підкреслити, що особливістю механізму ЕП Лампорта – Діффі у порівнянні з механізмом Лампорта є визначення функцій гешування (9) та (10), а також інший формат запису та використання секретного та відкритого ключів – в зворотному порядку. Тобто, в ньому зроблені уточнення.

1.3. Одноразовий ЕП Вінтерніц

Аналіз показує, що генерація ключа і підпису для механізму LD-OTS є ефективною, але розмір ЕП досить великий. Зменшення розміру ЕП досягається в механізмі одноразового ЕП, що запропонована в [6, 7], яка отримала назву механізму Вінтерніц (W-OTC). Ідея механізму Вінтерніц полягає в тому, щоб підписувати декілька бітів геш-значення, використовуючи один рядок одноразового ключа. Така пропозиція була запропонована вперше Merkle [7] як узагальнення його одноразового механізму. Однак, як слідує із [7], вона була описана в ній вперше.

Потрібно відмітити, що така ідея значний час застосовується в системах зв'язку при основному кодуванні, коли декілька бітів *w* при модуляції кодуються відповідним числом сигналі – переносників [12].

Загальні положення. Як і в механізмі Лампорта – Діффі – (LD-OTS) в механізмі Вінтерніц (W-OTS) використовуються одностороння геш-функція (6) та криптографічна геш-функція (10). Параметр Вінтерніц ЕП w ≥ 2 обирається як кількість бітів, що повинні бути підписані одночасно з використанням одноразового ключа.

У загальному випадку в механізмі Вінтерніц введено параметри t_1, t_2, t [6, 8], причому

$$t_1 = \lceil l / w \rceil, t_2 = \lceil \log_2 t_1 / w \rceil, t = t_1 + t_2, \tag{15}$$

де *l* довжина геш-значення, $w \geq 2$ – параметр, що визначає кількість бітів, які підписуються одним рядком одноразового ключа (LD-OTS). Параметр t_2 визначає необхідне число нулів, які потрібно добавити на початку геш-значення, щоб отримана в результаті нова довжина *t* була кратна w.

Для спрощення та з урахування практичного застосування параметр *w* можна визначити з обмеженням у вигляді (але не обов'язково)

$$w = 2^{\partial}, \ \partial = 1, 2, 3, 4, 5, 6, 7, 8... , \tag{16}$$

Генерування ключів. По аналогії з (11) у загальному випадку секретним ключем ЕП є $t_1 2^w$ випадкових бітових строчок довжини *l*

$$X = (x_{t1-1}, \ldots xi, \ldots, x_1, x_0) \in R\{0, 1\}^{(l,\ t_1 2^w)} \tag{17}$$

Таким чином, секретним ключем (17) є $t_1 2^w$ секретних ключів довжини *l*.

Відкритим ключем ЕП *Y* є послідовність строчок, що обчислюється шляхом застосування геш-функції *f*, по аналогії з (12), до кожного бітового рядку (17), внаслідок маємо

$$Y = (y_{t1-1}, \ldots, y_i, \ldots, y_1, y_0) \in \{0, 1\}^{(l,\ t_1 2^w)}, \tag{18}$$

де

$$y_i = f(x_i), 0 \leq i \leq t_1 2^w - 1. \tag{19}$$

Тобто, при генеруванні відкритого ключа необхідно виконати $t_1 2^w$ викликів однонаправленої геш-функції *f*. Необхідно підкреслити, що число секретних та відкритих ключів, які потрібні для виконання ЕП, залежить від величини *w*. Тому, змінюючи обгрунтувано w,
можна змінювати довжини секретного та відкритого ключів. Вказане досліджується нижче для ЕП, що розглядаються.

Вироблення ЕП W-OTC. Нехай необхідно підписати повідомлення *M* з геш-значенням g (*M*) = *d* = (d_{l-1}, ..., d_0). Для того щоб довжина *d* ділилась на *w*, спочатку необхідно встановити

мінімальне число нулів таким чином, щоб довжина d геш-значення ділилась на w. За цієї умови розширений рядок d розділяється на t_1 бітових блоків довжини w, тобто

$$d = b_{t1-1} \,||\, .bi\, .\, .\, ||\, b_0, \tag{20}$$

де знак || означає конкатенацію.

Засобом заміни кожного bi блоку геш-значення повідомлення g (M) зашифровується з використанням секретного ключа (17). Як результат ЕП повідомлення, тобто зашифроване геш-значення g (M), має такий вигляд

$$g(M) = S^* = \left(f^{b_{t1-1}}(x_{t1-1}), \ldots f^{bi}(x_i), \ldots, f^{b_1}(x_1), f^{b_0}(x_0)\right) = \\ = (s^*_{t1-1}, \ldots, s^*_i, \ldots, s^*_1, s^*_0) \tag{21}$$

Необхідно відмітити, що в (21) $s^*_{t1-1}, \ldots, s^*_i, \ldots, s^*_1, s^*_0$ – це ключі, які до вироблення ЕП були секретними. Але після вироблення ЕП вони стають відкритими, як і підписане повідомлення M , разом з ЕП.

Перевірка ЕП W-OTS. Для перевірки ЕП отриманого повідомлення M^*, що має вигляд

$$S^* = (s^*_{t1-1}, \ldots, s^*_i, \ldots, s^*_1, s^*_0) \tag{22}$$

спочатку аналогічно (20) обчислюється геш-значення $g(M^*)$, що має такий вигляд

$$d^* = b^*_{t1-1}, \ldots, b^*_i, \ldots, b^*_0. \tag{23}$$

Наявність символу (*) у M^* та у всіх b^*_i елементах означає, що вони могли бути викривленими штучно чи в результаті помилок при обробленні, передаванні та прийманні.

Далі, для всіх b^*_i (23) із відкритого ключа (18) у відповідності з їх значеннями вибираються певним чином геш-значення, що є складовими відкритого ключа. В результаті отримуємо

$$Y = (y_{t1-1}, \ldots, y_i, \ldots, y_1, y_0) \in \{0, 1\}^{(l,\, t_1)} \tag{24}$$

Потім здійснюється гешування значень $s^*_{t1-1}, \ldots, s^*_i, \ldots, s^*_1, s^*_0$, тобто ключів безпосередньо ЕП (22), в результаті отримуємо

$$Y^* = (y^*_{t1-1}, \ldots, y^*_i, \ldots, y^*_1, y^*_0) \in \{0, 1\}^{(l,\, t_1)} \tag{25}$$

Наостанок порівнюємо значення (24) y_i та (25) y^*_i для j = 0, 1, ...,i,…, t1 – 1.

Якщо $y_i = y^*_i$ для усіх j = 0, 1, ...,i,…, t1 – 1, то ЕП правильний, що підтверджує цілісність та справжність ЕП та підписане за його допомогою повідомлення M, а також дозволяє встановити авторство повідомлення M.

На наш погляд, викладений вище механізм одноразового ЕП *W-OTS* має суттєвий недолік – число секретних та відкритих ключів згідно (17) та (18) зі збільшенням параметра w зростає експоненційно. Крім того, довжина ЕП у залежності від значення w також э суттєвою. Вказане практично виключає можливість застосування механізму Вінтерніц на практиці, навіть у особливих технологіях з малим числом користувачів – підписувачів. Нижче наводиться удосконалений механізм Вінтерніц – Лампорта

1.4. Сутність та реалізація удосконаленого ЕП Вінтерніц – Лампорта

Аналіз підтверджує, що ключі і підписи Лампорта та Лампорта – Діффі (LD-OTS) є безумовно стійкими, але розмір ЕП досить великий, а також в Вінтерніц OTS (W-OTS) механізмі ЕП, що розглянуто вище, існує можливість виробляти коротші ЕП, але число секретних та відкритих ключів зі збільшенням параметра w зростає експоненційно. Особливість механізму Вінтерніц W-OTS в тому, що існує можливість використати секретний ключ одночасно для підпису декількох та значно більше бітів геш-значення [8, 9,

13]. Використовуючи цю ідею, розглянемо удосконалений механізм W-OTS з одноразовими ключам, основними перевагами якого є можливість суттєвого зменшення довжин секретних та відкритих ключів, а також довжини ЕП.

Як і в LD-OTS в W-OTS будемо використовувати односторонню геш-функцію

$$f : \{0, 1\}^{l} \rightarrow \{0, 1\}^{l}$$

та криптографічну геш-функцію

$$g : \{0, 1\}^{*} \rightarrow \{0, 1\}^{l}.$$

Генерація ключів для механізму W-OTS. Будемо вважати, що параметр $w \geq 2$ визначає кількість бітів геш-значення, що повинна бути підписано одночасно, тобто замінена одним секретним ключем. Цей механізм схожий на багатослівне кодування, що застосовується у системах зв'язку [12].

Для здійснення ЕП спочатку уточнимо параметри підпису – t_1 та t. Якщо довжина ЕП l кратна w, то $t1$ визначає кількість блоків бітів геш-значення, що будуть підписуватись (зашифровуватись) одним секретним ключем, причому

$$t = t1 = n / w \tag{26}$$

Якщо n не кратне w, то в останньому блоці буде менше чим w бітів, тому число блоків які потрібно підписати, необхідно збільшити на $t_{2=1,}$ записавши в перший блок додатково необхідне число нулів. У загальному випадку

$$t = t_1 + t_2 \tag{27}$$

Секретним ключем ЕП по аналогії з (1) є (X, Y) послідовність t множин 2^w секретних ключів (x_i, y_i) як і у механізмі Лампорта (1) та (2) , тобто

$$X = (x_{t-1}, \ldots, x_i, \ \ldots, x_0), \ Y = (y_{t-1}, \ldots, yi, \ \ldots, y_0) \tag{28}$$

з довжиною кожного із секретних ключів l_h, де l_h – довжина геш-значення для однонаправленої геш-функції f. При цьому кожна із множин 2^w секретних ключів (x_i, y_i) є i-ю частиною секретного (особистого) ключа. Згідно з (27) в (28) число секретних множин ключів менше ніж для механізмів Лампорта та Лампорта – Діффі (1). Точні оцінки наводяться нижче.

Відкритий ключ перевірки ЕП обчислюється засобом гешування секретних ключів (28) з застосуванням однонаправленої геш-функції f, внаслідок отримуємо t множин 2^w відкритих ключів:

$$H(X) = H(x_{t-1}), \ldots, \mathrm{H}(x_i), \ \ldots, \mathrm{H}(x_0),$$
$$H(Y) = H(y_{t-1}), \ldots, \mathrm{H}(y_i), \ \ldots, \mathrm{H}(y_0) \tag{29}$$

також з довжиною l_h кожного відкритого ключа пари $(H(x_i), \mathrm{H}(y_i))$. Але у випадку (29) параметр t в w разів менше за l_h.

Вироблення ЕП для механізму W-OT. Нехай по аналогії з (13) повідомлення M має геш-значення

$$g(M) = h = (h_{t-1}, ..., h_i, ..., h_0), \tag{30}$$

яке потрібно підписати з використанням криптографічної функції g.

У загальному випадку, якщо l_h не кратно *w*, добавимо до *h* деяке число нулів, так, щоб довжина l_h була кратна *w*. Рядок *h*, бітів розділяється на *t* блоків $b_{t-1},...,b_i,...,b_0$ довжини *w* бітів кожний.

В подальшому для ЕП та перевірки ЕП застосовуємо інше правило зашифрування: якщо значення b_i блоку знаходиться в інтервалі

$$0 \le b_i \le (2^w / 2) - 1 \tag{31}$$

то b_i блок зашифровується (заміняється) послідовно секретним ключем із множини (28) X, інакше заміняється послідовно секретним ключем із множини (28) Y. Тоді підписане повідомлення має такий вигляд

$$\{M; Z = (\{x_{t-1} \mid y_{t-1}\}), \{x_{t-2} \mid y_{t-2}\},...,\{x_i \mid y_i\},...,\{x_0 \mid y_0\}) = \{M, Z = (z_t, z_{t-1},..., z_i,..., z_0)\} \tag{32}$$

В (32) символ « | » означає, що при зашифруванні в ЕП з'являється один із використаних секретних сигналів – x_i чи y_i, що визначається *i*-м блоком бітів довжини w.

Правило (31) будемо застосовувати принципово по-новому. На відміну від механізму Вінтерніц не зашифровуються усі можливі стани 2^w, коли потрібно 2^w секретних ключів для кожного блоку b_i. В нашому випадку для зашифрування b_i потрібно всього $r = 2$ секретних та відкритих ключів. Крім того, в якості довжин блоків можна розглядати значення

$$l_h, l_h / 2, l_h / 4, l_h / 8... \tag{33}$$

В цьому випадку необхідне число секретних та відкритих ключів, а також довжина ЕП суттєво скорочується. Детально покажемо це нижче.

Перевірка ЕП для механізму W-OT. Перевірка ЕП здійснюється аналогічно (5) – (8), тобто у такій послідовності.

1. Із використанням криптографічної геш-функції *g* здійснюється гешування повідомлення M^*, для якого робиться перевірка ЕП, в результаті отримується геш-значення

$$h_{Mi^*} = H(M^*, \Pr).$$

Якщо довжина h_{Mi^*} не кратна w, то до рядка бітів h_{Mi^*} у відповідності з домовленістю добавляється деяке число нулів, так, щоб довжина h_{Mi^*} була кратна w. Рядок h_{Mi^*} бітів розділяється на *t* блоків $b_{t-1},...,b_i,...,b^0$ довжини w бітів кожен.

2. У відповідності зі значеннями b_i блоків h_{Mi^*} згідно правила (31) із відкритого ключа перевірки ЕП (29) згідно з критерієм (31) вибираються геш-значення $H(x_i)$ чи $H(y_i)$, внаслідок отримуємо

$$Z^* = (\{H(x_1) \mid H(y_1)\}), \{H(x_2) \mid H(y_2)\},...,\{H(x_i) \mid H(y_i)\},...,\{H(x_n) \mid H(y_n)\}) =$$

$$= (z^*_{t-1}, z^*_{t-2},..., z^*_i,..., z^*_0) \tag{34}$$

3. Користувач Б послідовно гешує усі ключі ЕП (32) та отримує значення

$$(H(z_t), H(z_{t-1}),..., H(z_i),..., H(z_0) \tag{35}$$

та порівнює отримані значення зі значеннями (34), тобто $(z^*_{t-1}, z^*_{t-2},..., z^*_i,..., z^*_0)$. Якщо усі *t* значень при порівнянні співпали, то ЕП вважається справжнім, в іншому випадку ЕП вважається викривленим.

Нижче наводяться результати порівняльного аналізу криптографічної стійкості та складності розглянутих вище постквантових механізмів ЕП на основі геш-функцій.

2. Аналіз властивостей ЕП з одноразовими ключами на основі геш-функцій

2.1. Загальні положення щодо умов здійснення атак

Згідно з вимогами [3, 4, 8, 9] постквантові ЕП повинні бути стійкими проти усіх відомих постквантових та класичних атак. Попередній аналіз показав, що основними загрозами щодо ЕП Лампорта, Лампорта – Діффі, Вінтерніц та удосконаленого з разовими ключами є підробка ЕП та створення хибного ЕП. Такі загрози повинні бути здійсненими в умовах використанні при ЕП одноразового ключа (1), (11), (17) та (26). Вказані загрози можуть бути потенційно реалізованими засобом здійснення силових атак типу «брутальна сила» та аналітичного типу [11].

Відповідно до загальновизнаних підходів основною задачею вказаних атак будемо вважати визначення секретного (особистого) ключа користувача (підписувача), тобто наприклад відносно ЕП Лампорта – визначення секретного ключа (1), для механізму Лампорта – Діффі секретного ключа (11), удосконаленого механізму секретного ключа (28). Це пов'язане з тим, що знаючи секретний ключ ЕП, криптоаналітик може здійснювати як модифікацію підписаного, так і створювати хибне повідомлення з дійсним підписом.

Для проведення криптоаналізу введемо модель порушника та модель загроз. Особливістю розгляду в тому, що за основу моделі порушника беруться модель квантового та класичного комп'ютерів та їх можливості, а за основу моделі загроз – методи та алгоритми квантового та класичного криптоаналізу щодо постквантових ЕП на основі геш-функцій.

В якості основних вихідних даних візьмемо такі [2 – 4, 5 – 9].

1. В якості геш-функцій можуть застосовуватись : ДСТУ ISOIEC 10118 (SHA -2); FIPS 202 (SHA –3); ДСТУ 7564-2014.
2. Функції гешування є стійкими проти класичного та квантового криптоаналізу, в тому числі: до знаходження прообразу; до знаходження другого прообразу; до виникнення чи створення колізій.
3. Порушник має повний доступ до математичної та програмних моделей геш-функцій та може отримувати з високою ймовірністю підписані повідомлення;
4. В якості секретних (особистих) ключів ЕП використовуються випадкові чи псевдовипадкові послідовності, що задовольняють вимогам нормативно-правових документів, наприклад NIST SP 800 –22: 2009 тощо.
5. Усі n секретних послідовностей секретного ключа, що використані при виробленні ЕП, є відкритими та доступні криптоаналітику, а ті, що не використані, зменшились секретними та знищені після ЕП.
6. Відкритим ключем ЕП є геш-значення усіх секретних послідовностей секретного ключа.
7. ЕП, що задовольняють вимогам 1 – 6, наведеним вище, згідно з [3, 11] будемо називати повністю автентичними з мінімальною ймовірністю обману щодо усіх відомих атак.
8. Основними атаками при цих дослідженнях будемо вважати атаки типу модифікація чи підробка (створення хибного) підпису довільного повідомлення.

Для підтвердження «повної автентичності» стійкості до модифікації та підробки підписаних повідомлень наведемо наступне.

2.2. Метод оцінки складності атаки типу модифікація ЕП

Нехай за умов 1 – 8 підрозд. 2.1 криптоаналітик змінює хоча б один біт в підписаному повідомленні *M*. Але при цьому він хоче або змінити ЕП, так щоб перевірка ЕП дала позитивний результат, або щоб значення ЕП не змінилося. Нехай при перевірці, наприклад на приймальній стороні, отримується викривлене значення повідомлення *M*', тобто криптоаналітик реалізує атаку зі зміною змісту повідомлення *M*. При перевірці ЕП спочатку обчислюється геш-значення

$$H(M') = (b'_{t-1}, ..., b'_i, ..., b'_0) \tag{36}$$

Далі, якщо геш-функція, що застосовується, відповідає вимогам до криптографічних геш-функцій, то після модифікації одного біта в повідомленні *M* в середньому зміниться половина бітів геш-значення H(m'), тобто приблизно $l_h / 2$ бітів. Також криптоаналітик знає тільки ті *n* значень секретного ключа, що були в невикривленому ЕП. Тому для модифікації ЕП йому необхідно знати *n* інших випадкових послідовностей секретного ключа. Це необхідно для того, щоб мати можливість використати їх для підстановки у відповідні місця підпису S, для тих бітів геш-значення, що змінилися.

Відповідно до прийнятої моделі будемо вважати, що криптоаналітик знає все про геш-функцію та може обчислити геш-значення модифікованого повідомлення M'. Це означає , що криптоаналітик може визначити біти геш-значення, що змінились після модифікації повідомлення. Тоді сутність атаки згідно з (1), (11), (17), (26) зводиться до того, щоб визначити та підставити в ЕП в середньому *n* секретних послідовностей, що йому недоступні.

Ймовірність знаходження однієї послідовності визначимо, вважаючи, що атака типу модифікація здійснюється методом створення колізії (наприклад, методом Гровера) [11]. Дійсно, із [11] слідує, що одним із ефективних алгоритмів криптоаналізу симетричних криптоперетворень, в тому числі стосовно геш-функцій, є алгоритм Гровера. При його використанні секретний ключ симетричного криптоперетворення можна знайти засобом виконання (за час) $\sqrt{N}$ групових операцій, де *N* – число можливих ключів.

Показано, що в цьому випадку при застосуванні методу ρ- Полларда ймовірність виникнення колізії *P(N,k)* в *k* спробах, а значить знаходження ключа, при довжині геш-значення l_h та $N = 2^{l_h}$ можна визначити як

$$p_\rho(N,k) = 1 - \ell^{-(k^2-k)/(2^{l_h+1})}. \tag{37}$$

Вираз (37) після простих перетворень та логарифмування можна подати у такому вигляді [12]:

$$k^2 - k + 2^{l_h+1} ln\,(1 - p_\rho(N,k)) = 0 \tag{38}$$

При застосуванні λ-Полларда методу, по аналогії з (37) та (38), ймовірність виникнення колізії *P(N,k)* в *k* спробах, а значить знаходження ключа [11]:

$$p_\lambda(N,k) = 1 - \ell^{-(k^2-1)/(2^{l_h})}, \tag{39}$$

$$k^2 - 1 + 2^{l_h} ln\left(1 - p_\lambda\left(N,k\right)\right) = 0\ . \tag{40}$$

У цілому (37) – (40) є параметричними співвідношеннями, що зв'язують три параметри – $p\left(N,k\right)$, k та $N = 2^{l_h}$. Тому, задаючи два параметри, можна обчислити значення третього тощо. В нашому випадку необхідно визначити $p(N,k)$, тобто ймовірність визначення однієї послідовності секретного ключа відповідно (1), (11), (17) чи (26).

Зведемо (37) та (39) до основ 2 та 10.Тоді, використовуючи властивості степені та логарифму для (37), отримаємо

$$P(N,k)=1-2^{-\log_2 e\cdot(2^{2V}-2^{V})\cdot 2^{-(\ln+1)}}=1-2^{-(\log_2 e\cdot(2^{2V-\ln-1}-2^{V-\ln-1}))} \quad (41]$$

При $k^2 >> k$

$$P(N,k)=1-2^{-\log_2 e\cdot 2^{2V-\ln-1}}. \quad (42]$$

Зрозуміло, що (16) потрібно застосувати коректно.

Для основи степені 10 по аналогії із (41) та(42) маємо

$$P(N,k)=1-10^{-\log_{10} 2\cdot 10^{\log_{10}(2V-\ln-1-v+\ln+1)}} \quad (43)$$

або при $k^2 >> k$

$$P(N,k)=1-10^{-\log_{10} 2\cdot 10^{\log_{10}(2V-\ln-1)}}. \quad (44]$$

Формули (41) – (46) важливі тим, що вони дозволяють отримувати та робити інтерпретацію стійкості зразу в бітах(чи кубітах).

В табл. 1 наведені значення ймовірностей (37) при таких вихідних даних:

- l_h – довжина геш-значення;
- k – кількість спроб підібрати одну послідовність секретного ключа;
- $N = 2^{l_h}$ – кількість можливих (допустимих) секретних ключів (послідовностей);
- n кількість послідовностей, що можуть бути використані в якості одноразового секретного ключа;

В табл. 1 показана ймовірність модифікації $P_{\rho}(N,k)$ ЕП при n=1.

Таблиця 1

l_h\k	2^{32}	2^{64}	2^{128}	2^{256}	2^{512}
256	$7.965*10^{-59}$	$1.469*10^{-39}$	0,393	1	1
512	$6.879*10^{-136}$	$1.269*10^{-116}$	$4.318*10^{-78}$	0.393	1

Наведені в табл. 1 дані не протирічять теорії колізій, вони характерні в точках $2^{128}, 2^{256}$.

2.3. Метод оцінки складності атаки створення хибного повідомлення та ЕП

Розглянемо атаку на ЕП, сутність якої зводиться до аналізу можливості створити та нав'язати хибне повідомлення при застосуванні розглянутих в розд. 1 механізмів ЕП з одноразовими ключами. Будемо вважати, що в системі ЕП забезпечується довіра за рахунок третьої довірчої сторони чи між підписувачами безпосередньо. Аналіз будемо вести в узагальненому вигляді для усіх чотирьох механізмів, що наведені вище.

В якості моделі порушника та моделі загроз приймемо відповідні моделі, що наведені в підрозд. 2.1. За виключенням п.8 будемо розглядати атаку зі створення хибних повідомлення та ЕП.

Попередній аналіз показує, що атака зі створенням хибного з ЕП повідомлення може здійснюватись за таких умов: криптоаналітику відомий відкритий ключ, наприклад у вигляді сертифікату відкритого ключа; відкритий ключ криптоаналітику невідомий, але він володіє повною інформацією про ЕП, в тому числі може накопичувати та аналізувати одноразові ЕП. Розглянемо та проведемо аналіз стійкості ЕП проти атаки повне розкриття при відомому відкритому ключі, коли криптоаналітику достовірно є відомими відкриті ключі (2), (12), (18) та (29). Дану атаку називаємо атакою «повне розкриття» тому, що в результаті її реалізації компрометується секретний ключ, наприклад (Х, У), для випадку (2), (18) та (29).

Вирішення задачі «повне розкриття» в такій постановці зводиться до застосування методу створення колізій для тих *n* послідовностей, що будуть використані при підписуванні засобом шифрування бітів геш-значення хибного повідомлення, наприклад для (29) та (28). Тобто, знаючи $H(x_i)$, необхідно знайти x_i для усіх *n*, які згідно з геш-значенням хибного повідомлення M^* повинні бути використаними. Повний опис таких подій можна отримати з використанням формул (37) – (41). Наприклад, при застосуванні методу ρ-Полларда ймовірність створення колізій визначається (37), але вимагає виконання $k_{\min}$ групових операцій для того, щоб забезпечити мінімально допустиму ймовірність створення колізій $P_{\min}(N,k)$. Тобто, в цьому випадку формули (37) та (38) мають такий вигляд

$$p_{\min_\rho}(N,k_{\min}) = 1-\ell^{-(k^2{}_{\min}-k_{\min})/(2^{l_h+1})}, \quad (45)$$

$$k^2{}_{\min} - k_{\min} + 2^{l_h+1} ln\,(1- p_{\min_\rho}(N,k)) = 0\ . \quad (46)$$

Зробимо детально аналіз та постановку цієї задачі.

По перше, криптоаналітик обмежений часом створення колізій для усіх *n* відкритих ключів, наприклад часом $t_{\min}$. Знаючи час $t_{\min}$, визначимо через необхідну складність допустиме значення $k_{\min}$. Далі, знаючи, *N* (l_{min}) та $k_{\min}$, знаходимо конкретне значення *P**. Також будемо вважати, що створення колізій відбувається для усіх *n* паралельно.

В табл. 2 наведено значення часової складності T обернення (створення колізій) (років) для таких вихідних даних: потужність криптоаналітичної системи відповідно до $I = 10^{12}, 10^{14}, 10^{16}$ *гр.оп./сек* , $t_{\min} = 3.15 \bullet 10^7$ сек/рік, $l_h = 256(512)$ бітів.

Таблиця 2

$l \backslash I$	10^{12}	10^{14}	10^{16}
256	10^{19}	10^{17}	10^{15}
512	10^{56}	10^{54}	10^{52}

В табл. 3 наведено оціночні значення ймовірності визначення однієї послідовності секретного ключа з один рік.

Таблиця 3

$l \backslash I$	10^{12}	10^{14}	10^{16}
256	10^{-19}	10^{-17}	10^{-15}
512	10^{-56}	10^{-54}	10^{-52}

Аналіз даних табл. 2 та 3 дозволяє зробити висновок про практичну неможливість створення хибного повідомлення методом обернення навіть одного відкритого ключа. При оберненні *n* ключів та послідовному криптоаналізі відповідно часова складність збільшується в *n* разів, а ймовірність успішного криптоаналізу зменшується в *n* разів.

Розглянемо атаку за умови, що відкритий ключ невідомий. Дану атаку також назвемо атакою «повне розкриття» тому, що в результаті її реалізації компрометується секретний ключ, наприклад (X, У) для випадку (2), (18) та (29). Спроба вирішення задачі «повне розкриття» в такій постановці зводиться до наступного. При підписуванні засобом шифрування бітів геш-значення робиться спроба створити хибне повідомлення, наприклад при повному розкритті (28). Вона вирішується методом Гровера послідовно для кожної із послідовностей секретного ключа. За даних умов ймовірність створення колізії для розкриття однієї послідовності секретного ключа можна оцінити, використовуючи формули (37) та (38), але при цьому також задатись і допустимими значеннями $k_{\min}$ та $t_{\min}$.

2.4. Оцінка та порівняння розмірів одноразових ключів та ЕП

При розгляді та аналізі механізму Лампорта, Лампорта – Діффі, Вінтерніц та удосконаленого механізму ЕП з разовими ключами однією із задач, що ставилась та вирішувалась, є зменшення розмірів ключів та ЕП. На наш погляд, найбільш продуктивним є удосконалений механізм з одноразовими ключами. Орієнтуючись на викладене в підрозд.1.1 – 1.4 та 2.1 – 2.3, зробимо оцінки розмірів ключів та ЕП для усіх розглянутих механізмів.

В якості вихідних даних приймемо такі.

1. В механізмі Лампорта та Лампорта – Діффі використовуються значення $n = l_h$, w=1, а l_h =256 та 512 бітів.
2. В механізмі Вінтерніц використовуються значення $n = l_h$, w=2, 4, 6, 8, 16, причому аналіз будемо проводити для l_h =256 та 512 бітів.
3. В удосконаленому механізмі $l_h = \mu \times n, \mu = 2,4,8,16,32,128,256.$, а W використовується у змісті (19).

В табл. 4 наведено результати оцінки розмірів секретних та відкритих одноразових ключів та розмірів ЕП для механізмів Лампорта та Лампорта – Діффі. Довжина секретного та відкритого ключів визначається як $2 \times l_h \times n$, довжина ЕП $l_h \times n$.

Таблиця 4

Розміри даних l_h, n			Розмір секретного ключа	Розмір відкритого ключа	Розмір ЕП
256	256		2^{17}	2^{17}	2^{16}
512	512		2^{19}	2^{19}	2^{18}

В табл. 5 наведено результати оцінки розмірів секретних та відкритих одноразових ключів та розмірів ЕП для механізму Вінтерніц. Довжина секретного та відкритого ключів визначається як $2 \times w^2 \times n_i \times l_h$, довжина ЕП $n_i \times l_h$

Таблиця 5

Розміри даних\ l_h, n_i	w_i		Розмір секретного ключа	Розмір відкритого ключа	Розмір ЕП
256	128	2	2^{18}	2^{18}	2^{15}
	64	4	2^{19}	2^{19}	2^{14}
	32	8	2^{23}	2^{23}	2^{16}
512	256	2	2^{20}	2^{20}	2^{17}
	128	4	2^{21}	2^{21}	2^{16}
	64	8	2^{25}	2^{25}	2^{17}

В табл. 6 наведено результати оцінки розмірів секретних та відкритих одноразових ключів та розмірів ЕП для удосконаленого механізму. Довжина секретного та відкритого ключів визначається як $2 \times \mu_i \times l_h$, довжина ЕП $\mu_i \times l_h$

Таблиця 6

Розміри даних\ l_h,	w_i		Розмір секретного ключа	Розмір відкритого ключа	Розмір ЕП
256	μ_i	2	2^{10}	2^{10}	2^{9}
		4	2^{11}	2^{11}	2^{10}
		8	2^{12}	2^{12}	2^{11}
		16	2^{13}	2^{13}	2^{12}
		32	2^{14}	2^{14}	2^{13}
		128	2^{16}	2^{16}	2^{14}
		256	2^{17}	2^{17}	2^{16}
		2	2^{11}	2^{11}	2^{10}

512	μ_i	4	2^{12}	2^{12}	2^{11}
		8	2^{13}	2^{13}	2^{12}
		16	2^{14}	2^{14}	2^{13}
		32	2^{15}	2^{15}	2^{14}
		128	2^{17}	2^{17}	2^{16}
		256	2^{18}	2^{18}	2^{17}
		512	2^{19}	2^{19}	2^{18}

У цілому результати порівняння досліджених та запропонованого механізму дозволяють зробити такі висновки.

Розміри секретних та відкритих одноразових ключів та розмірів ЕП для механізму Вінтерніц у порівнянні з механізму Лампорта вимагають збільшення розмірів секретних та відкритих одноразових ключів від 2 до 64 разів, але розміри ЕП зменшуються в 2 рази.

Розміри секретних та відкритих одноразових ключів та розмірів ЕП для удосконаленого механізму у порівнянні з механізмом Лампорта можуть бути зменшені для довжини ЕП 256 від 2 до 128 разів, а для довжини ЕП 512 ві 2 до 512 разів. При цьому для μ_i 256 та 512 відповідні значення табл. 8 співпали з відповідними даними табл 6.

Розміри секретних та відкритих одноразових ключів та розмірів ЕП для удосконаленого механізму у порівнянні з механізмом Вінтерніц для довжини 256 можуть бути зменшені для довжини ЕП 256 від 64 до 256 разів, а для довжини ЕП 512 – в 64 до 512 разів. При цьому довжини ЕП зменшуються від 8 до 32 разів (для довжини геш-значення 256), а для довжини 512 – від 2 до 128 разів.

У цілому необхідно зробити висновок, що удосконалений механізм забезпечує зменшення розмірів секретних та відкритих ключів, а також розмір ЕП.

Але необхідно ще дослідити та порівняти криптографічну стійкість та визначити розміри параметрів, при яких можна застосовувати удосконалений алгоритм одноразового ЕП.

2.5. Оцінка стійкості ЕП на основі геш-функцій з одноразовими ключами

Для визначення ймовірності успішного знаходження усіх n із $2n$ секретних послідовностей $P(n, p(N,k))$ секретного ключа покладемо, що усі послідовності є випадковими, рівно ймовірними та незалежними (див. п.1 – 7), тому ймовірність правильного визначення усіх послідовностей є добутком n подій. З урахуванням (37) отримуємо, що ймовірності успішного знаходження усіх n із $2n$ секретних послідовностей

$$P(n, p_\lambda(N,k)) = (1-\ell^{-(k^2-k)/(2^{l_h+1})})^n. \quad (47)$$

По аналогії з (41) для λ-Полларда методу для загального випадку отримаємо

$$P(n, p_\rho(N,k)) = (1-\ell^{-(k^2-1)/(2^{l_h})})^n. \quad (48)$$

Ймовірності (47) та (48) можна трактувати як ймовірності несанкціонованого доступу в систему ЕП на основі одноразових ключів. Також необхідно відмітити, що на перший погляд формули (47) та (48) дають різні результати. Насправді це не так, оскільки складність групових операцій в обох випадках є різною. При застосуванні ρ-Полларда методу використовується один процес реалізації групових операцій, а при застосуванні λ-Полларда методу застосовуються два процеси. Хоча з цього питання ще потрібні деталізації.

Для зручності обчислень формули (47) та (48) наведемо для основ 2 та 10. В результаті маємо для (47)

$$P(n, p(N,k)) = (1-2^{-\log_2 e\cdot(2^{2V}-2^{V})\cdot 2^{-(\ln+1)}})^n = (1-2^{-(\log_2 e\cdot(2^{2V-\ln-1}-2^{V-\ln-1}))})^n \quad (49]$$

При $k^2 >> k$

$$P(n, p(N,k)) = (1-2^{-\log_2 e\cdot 2^{2V-\ln-1}})^n \quad (50]$$

Для основи степені 10 аналогічно (49) та(50) маємо

$$P(n, p(N,k)) = (1-10^{-\log_{10} 2\cdot 10^{\log_{10}(2V-\ln-1-v+\ln+1)}})^n, \quad (51)$$

а при $k^2 >> k$

$$P(n, p(N,k)) = (1-10^{-\log_{10} 2\cdot 10^{\log_{10}(2V-\ln-1)}})^n \quad (52]$$

В табл. 7 наведено значення ймовірності вироблення хибного ЕП згідно запропонованої методики при n = 2 та при k= $2^{32}, 2^{64}, 2^{128}, 2^{256}, 2^{512}$. Пояснимо, що при n=2 згідно з нашою моделлю геш-значення зашифровується всього двома одноразовими парами ключів.

В табл. 8 наведено значення ймовірності вироблення хибного ЕП при n = 8 та при k= $2^{32}, 2^{64}, 2^{128}, 2^{256}, 2^{512}$.

Таблиця 7

lh\k	2^{32}	2^{64}	2^{128}	2^{256}	2^{512}
256	6 *10-117	2*10-78	0.154	1	1
512	6.8 *10-136	1.6*10-232	1.8*10-155	0.154	1

Таблиця 8

lh\k	2^{32}	2^{64}	2^{128}	2^{256}	2^{512}
256	1.6*10-465	2.2*10-311	0.0237	1	1
512	2.2 *10-1087	6.7*10-928	1.2*10-619	0.154	1

При реалізації механізмів Ломпарта, Ломпарта – Діффі та Вінтерніц при n=256 для реальних значень k практично отримуємо, що $P(n, p_\rho(N,k)) = 0.$ Так, навіть при $k = 2^{128}$ та $l_h = 256$ згідно (49) та (50) отримуємо $P(n, p_\rho(N,k)) = (0.393)^{256} = \leq 10^{-52}$.

Висновки

1. Можливо, механізми ЕП на основі геш-функцій є найбільш перспективними. Стійкість таких механізмів грунтується на використанні однонаправлених та криптографічних геш-функцій та генераторів випадкових та/чи псевдовипадкових послідовностей. Щодо більшості механізмів на основі геш-функцій є докази криптографічної стійкості як до класичних так і квантових атак. Також ЕП на основі геш-функцій практично є прийнятними як щодо складності (швидкодії), так і довжини ЕП та ключів.

2. Особливістю механізмів ЕП на основі геш-функцій є те, що їх криптографічна стійкість грунтується на колізійній стійкості функцій гешування та/чи стійкості до знаходження прообразу. Так як нині уже розроблено та прийнято у якості геш-функцій ряд, по суті стандартизованих постквантових геш-функцій, то такі механізми, на наш погляд, є перспективними. Але залишається ряд проблемних питань, що повинні певною мірою бути вирішеними до початку етапу стандартизації, в тому числі: доведення криптографічної

стійкості; мінімізація розмірів загальних параметрів та ключів; мінімізація довжини підпису та підвищення швидкодії; вироблення та перевіряння ЕП тощо відповідно до вимог.

3. Механізми ЕП з одноразовими ключами Лампорта, Лампорта – Діффі та Вінтерніц дійсно забезпечують як практичну, так і теоретичну криптографічну стійкість проти існуючих атак і можуть бути віднесені до криптоперетворень з бездоганним ЕП. Основними недоліками, що характерні для вказаного класу ЕП з одноразовими ключами, є великі довжини секретних та відкритих ключів, а також довжина ЕП.

4. На наш погляд, запропоноване удосконалення ЕП на основі алгоритму Вінтерніц має суттєві переваги щодо зменшення довжин ключів та ЕП, в той же час при обґрунтованому виборі параметрів механізму забезпечується криптографічна стійкість до атак модифікації та створення хибних підписів. Але вказаний клас ЕП з одноразовими ключами є складним, та скоріше може бути застосований для захисту повідомлень критичного рівня.

5. Розміри секретних та відкритих одноразових ключів та розмірів ЕП для механізму Вінтерніц у порівнянні з механізму Лампорта вимагають збільшення розмірів секретних та відкритих одноразових ключів від 2 до 64 разів, але розміри ЕП зменшуються в 2 рази.

6. Розміри секретних та відкритих одноразових ключів та розмірів ЕП для удосконаленого механізму у порівнянні з механізмом Лампорта можуть бути зменшені для довжини ЕП 256 від 2 до 128 разів, а для довжини ЕП 512 – від 2 до 512 разів. При цьому для μ_i 256 та 512 відповідні значення табл. 8 співпали з відповідними даними табл 6.

7. Розміри секретних та відкритих одноразових ключів та розмірів ЕП для удосконаленого механізму у порівнянні з механізмом Вінтерніц для довжини 256 можуть бути зменшені для довжини ЕП 256 від 64 до 256 разів, а для довжини ЕП 512 – від 64 до 512 разів. При цьому довжини ЕП зменшуються ввід 8 до 32разів (для довжини геш-значення 256), а для довжини 512 від 2 до 128 разів.

8. У цілому необхідно зробити висновок, що удосконалений механізм забезпечує зменшення розмірів секретних та відкритих ключів, а також розмір ЕП. Удосконалення механізму Лампорта зводиться до застосування іншого правила зашифрування (31). Якщо значення b_i блоку знаходиться в інтервалі 931), то b_i блок зашифровується (заміняється) послідовно
секретним ключем із множини (28) X, інакше заміняється послідовно секретним ключем із множини (28) Y.

9. Попередній аналіз показав, що основними загрозами щодо ЕП Лампорта, Лампорта – Діффі, Вінтерніц та удосконаленого з разовими ключами є підробка ЕП та створення хибного ЕП. Вказані загрози можуть бути потенційно реалізованими засобом здійснення силових атак типу «брутальна сила» та аналітичного типу на основі квантових алгоритмів, наприклад Гровера.

10. Обґрунтовані співвідношення (37) – (44) отримані на основі математичних методів Полларда та, по суті, є реалізацією алгоритму Гровера. На основі їх використання отримані аналітичні оцінки складності криптоаналізу типу повне розкриття для усього класу ЕП з одноразовими ключами.

Список літератури: 1. *A RIDDLE* WRAPPED IN AN ENIGMA. NEAL KOBLITZ AND ALFRED J. MENEZES Department of Mathematics, Box 354350, University of Washington, Seattle, WA 98195 U.S.A. 2. *Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone.* Report on Post – Quatum Cryptography. NISTIR 8105 (DRAFT). https://www.google.com.ua/search? 3. DRAFT – DRAFT – DRAFT. Proposed Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process. http://www.nist.gov/pqcrypto. 4. *Горбенко, І.Д., Кузнєцов, О.О., Потій, О.В., Горбенко, Ю.І., Ганзя, Р.С., Пономар, В.А.* Постквантова криптографія та механізми її реалізації // Радиотехника. – 2016. – Вып. 186. – С. 32–52. 5. *Leslie Lamport.* Constructing digital signatures from a one way function. Technical. Report SRI-CSL-98, SRI International Computer Science Laboratory, 1979. 6. *Andreas Hülsing.* W-OTS+ – shorter signatures for hash-based signature schemes. In Amr Youssef, Abderrahmane Nitaj, and Aboul-Ella Hassanien, editors, Progress. in

Cryptology – AFRICACRYPT 2013, volume 7918 of LNCS, pages 173–188.Springer, 2013. 7. *Ralph Merkle*.
A certified digital signature. In Gilles Brassard, editor, Advances inCryptology – CRYPTO ’89, volume 435 of LNCS, pages 218–238. Springer, 1990. 8. *Daniel J. Bernstein;, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O’Hearn*. SPHINCS: practical stateless hash-based Signatures. djb@cr.yp.to. daira@leastauthority.com, zooko@leastauthority.com 9. *Gorbenko, I., Ponomar, V.* Examining a possibility to use and the benefits of post-quantum algorithms dependent on the conditions of their application // Eastern European Journal of Enterprise Technologies, Vol.2, Issue 9-86, 2017, Pages 21-32. http://journals.uran.ua/eejet/article/view/96321/94881. 10. *ETSI GR* QSC 001 V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework. 11. *Горбенко, Ю.І.* Методи побудування та аналізу, стандартизація та застосування криптографічних системи ; за заг. ред. Горбенка І.Д. – Харків : Форт, 2016. – 958с. 12. *Gorbenko, I., Kuznetsov, A., Gorbenko, Yu., Kavun, S., Kachko, O., Yesina, M.* Electronic Signature Mechanisms. The Current State, the Existing Contradictions and Prospects of Practical Use for the Post-Quantum Period: Monograph. – ASC Academic Publishing, USA, 2017. – 165 p. 13. *Grover’s Quantum* Search Algorithm [електронний ресурс] – Режим доступу: URL: http://twistedoakstudios.com/blog/Post2644_grovers-quantum-search-algorithm. 14. *Кузнецов, А.А., Пушкарев, А.И., Сватовский, И.И., Шевцов, А.В.* Несимметричные криптосистемы на алгебраических кодах для пост-квантового периода // Радиотехника. – 2016. – Вып. 186. – С. 70-90. 15. *Кузнецов, О., Горбенко, Ю., Шевцов, О., Кузнецова, Т.* Дослідження криптографічних атак на схеми електронного цифрового підпису в фактор-кільцях зрізаних поліномів // Захист інформації. – Київ : Національний авіаційний університет, 2016. – Т. 18, №4, жовтень-грудень 2016. – С. 293-300.

Харківський національний університет
імені В.Н. Каразіна
Надійшла до редколегії 20.04.2017