УДК 004.056.55

Ю.І. ГОРБЕНКО, канд. техн. наук, К.В. ІСІРОВА

УДОСКОНАЛЕНИЙ МЕХАНІЗМ ОДНОРАЗОВИХ КЛЮЧІВ ДЛЯ ПОСТКВАНТОВОГО ПЕРІОДУ НА ОСНОВІ ГЕШ-ФУНКЦІЙ

Вступ

Розробка та стандартизація постквантових асиметричних криптографічних перетворень є однією із важливих проблем сучасності. Провідні держави, в тому числі США, розуміючи необхідність пошуку нових асиметричних криптографічних примітивів електронного підпису(ЕП) та асиметричного направленого шифрування (НШ), які будуть актуальними та можуть застосовуватись у постквантовий період, оголосив конкурс на розробку стандартів постквантових асиметричних криптографічних примітивів [1 – 3]. Заявки приймались NIST до 30 листопада 2017 року. Вони стосуються в першу чергу асиметричних алгоритмів ЕП. Європейський Союз (ЄС) також веде активну роботу з розробки та досліджень постквантових стандартів асиметричних криптографічних перетворень , в тому числі стандартів постквантового ЕП. Вказане пояснюється їх широким застосуванням в значному числі додатків та можливими великими втратами у випадку компрометації ЕП, коли з'явиться квантовий комп'ютер з необхідними характеристиками та можливостями [1 – 5].

Дослідження, проведені в технологічно розвинутих державах, показали, що одним із перспективних напрямів створення постквантового ЕП, може бути напрям, що ґрунтується на використанні функцій гешування та дерева Мерклі [6]. В основу цього напряму покладено використання одноразових ключів та одноразових ЕП. На нинішній час запропоновані та суттєво досліджені такі механізми генерування та використання одноразових ключів ЕП на основі функцій гешування (симетричних криптографічних перетворень та функцій зчеплення):

- механізм Лампорта з одноразовими ключами LOTS [7];
- механізми Вінтерніц з одноразовими ключами *WOTS*, $WOTS^{CR}$, $WOTS^{PRF}$, $WOTS^{+}$ [8, 10];
- модифікації механізму з одноразовими ключами Biba, HORS, HORS+, HORS++ та HORST [10].

Нами запропоновано удосконалений механізм з одноразовими ключами, що названий POTS [13]. Мета статті – обґрунтування необхідності, детальне викладення сутності, дослідження властивостей за критеріями складність – криптографічна стійкість, визначення переваг та недоліків, а також умов і можливостей застосування удосконаленого механізму POTS в різних додатках постквантового періоду.

1. Постановка проблеми та можливості її вирішення

Суттєвим розвитком механізму ЕП на основі *OTS є* механізм Вінтерніц [4, 8]. Хоча механізми OTS Лампорта та LD-OTS Лампорта – Діффі забезпечують потенційні можливі властивості криптографічної стійкості ЕП, а по суті – зашифрування), але розміри ЕП та OTS ключів залишаються досить великими. Зменшення розміру ЕП досягається в механізмі одноразового ЕП з OTS, що запропонована в [4, 13], який отримав назву механізму Вінтерніц (W OTS) [8]. Ідея механізму Вінтерніц полягає в тому, щоб підписувати, на відміну від OTS Лампорта, уже декілька бітів геш-значення, використовуючи одну послідовність OTS секретного одноразового ключа. Іншою особливістю механізму Вінтерніц є застосування одно направлених фунцій, які, на наш погляд, можна назвати функціями зчеплення. Особливістю застосування функцій зчеплення є можливість виділення відкритого ключа безпосередньо із отриманого ЕП. На наш погляд, це є принциповою особливістю механізму Вінтерніц. Але, в цій статі ми будемо ставити механізм Вінтерніц в одинакові умови з механізмом Вінтерніц.

Як в механізмах OTS Лампорта та Лампорта – Діффі, в механізмі Вінтерніц (WOTS) використовуються одностороння геш-функція та криптографічна геш-функція. Параметр Вінтерніц ЕП $w \geq 2$ обирається як кількість бітів, що повинні бути підписані (зашифровані) одночасно з використанням одноразового ключа. Запропоновано також варіант ЕП Вінтерніц WOTS з використанням додаткового методу контролю цілісності на основі контрольної суми геш-значення, що зашифровується. Застосування додаткового методу контролю цілісності має на меті підсилення стійкості ЕП Вінтерніц WOTS.

Також аналіз показав, що у основних роботах, що стосуються одноразових ключів, в недостатній мірі використовуються «істинно» криптографічні критерії оцінки криптографічної стійкості та складності. На наш погляд, при оцінці та порівнянні різних механізмів ЕП з OTS, необхідно, як мінімум, використовувати [5]:

- Lc, Lв та Lп – відповідно довжини секретних Кс та відкритих ключів Кв та відкритого ЕП;

- число секретних Nк одноразових ЕП WOTS ключа, що можуть бути використані з рівною ймовірністю;

- ентропія джерела ключів H(Nк) відповідної модифікації одноразового ЕП WOTS ключа;

- безпечний час $T_б$ у вигляді математичного сподівання часу розкриття криптографічної системи при застосуванні відомих силових та аналітичних атак за допомогою як класичних та і квантових комп'ютерів, в нашому випадку наприклад визначення секретного ключа за умови ЕП та як наслідок одноразовому відкритого ключа ЕП OTS ;

- відстань єдності джерела l_0 одноразових OTS секретних ключів ЕП ;

- складність здійснення успішного криптоаналізу *Іс ЕП з OTS* при застосуванні силових методів;

- складність здійснення успішного криптоаналізу *Іа ЕП OTS* при застосуванні аналітичних методів.

Основні визначення та порядок застосування запропонованих критеріїв та показників оцінки *ЕП* на основі *OTS* повинні застосовуватись в необхідній при аналізі та порівнянні.

Проведений аналіз основних механізмів з одноразовими ключами – OTS Лампорта, OTS Вінтерніц (*WOTS*, $WOTS^{CR}$, $WOTS^{PRF}$, $WOTS^{+}$ [8, 9]) та модифікації механізму з одноразовими ключами (Biba, HORS, HORS+, HORS++ та HORST[ ]) не задовольняють вимогам просторової та часової складності, що суттєво ускладнює реалізацію постквантових ЕП на основі функцій гешування. Справа в тому, що при спробах зменшити розміри ключів та ЕП, робиться відхід від істинно бездоганних ЕП [13 – 15]. В той же час, на наш погляд, існує можливість побудування постквантових ЕП на основі OTS ключів, у вигляді perfekt OTS (POTS) [13], які за властивостями практично не уступали механізму Лампорта. Тому розглянемо *сутність, результати дослідження властивостей, переваги та недоліків, а також умови і можливостей застосування удосконаленого механізму* POTS *в різних додатках постквантового періоду*.

2. Удосконалена математична модель механізму постквантового ЕП POTS

Загальні положення. В Вінтерніц OTS (WOTS) механізмі ЕП існує, у порівнянні з механізмом Лампорта, можливість виробляти коротші ЕП, але число секретних та відкритих ключів зі збільшенням параметра *w* зростає суттєво. Також у загальному випадку механізму WOTS, що адекватний щодо властивостей механізму Лампорта, суттєво збільшується часова та просторова складності. Вказане обмежує застосування механізмів Вінтерніц (*WOTS,* $WOTS^{CR}$, $WOTS^{PRF}$, $WOTS^{+}$ [8, 9]) для випадку, коли мають бути виконаними вимоги, аналогічні, що виконуються механізмом Лампорта. Також немає можливості використовувати секретний ключ одночасно для підпису декількох та значно більшого числа геш-значення (WFTS) [9.]. Використовуючи цю ідею, розглянемо удосконалений механізму POTS з одноразовими ключами, основними перевагами якого є можливість зменшення

довжин одноразових ключів (секретних та відкритих ключів), а також довжини ЕП. Існують також варіанти його застосування і для WFTS.

Як і в механізмах LOTS Лампорта та Лампорта – Діффі LDOTS, в удосконаленому механізмі POTS будемо використовувати односторонню чи криптографічну геш-функцію

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

та обов'язково криптографічну геш-функцію

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

При ЕП повідомлення M спочатку здійснюється гешування повідомлення M з використанням узгодженої (як правило криптографічної) геш-функції з параметрами Pr та обчислюється геш-значення

$$h_M = H(M, Pr)) \tag{2}$$

Далі значення h_M зашифровується засобом заміни w блоків бітів геш-значення h_M секретними одноразовими ключами Процес такого зашифрування продовжується для усіх блоків бітів геш-значення h_{Mi}.

Таким чином, l_h бітів геш-значення h_{Mi} заміняються (зашифровуються) одноразовими ключами, по суті безумовно стійким шифром, оскільки послідовність бітів h_{Mi} заміняється одноразовими секретними випадковими послідовностями. Вказана послідовність l_k секретних послідовностей і є ЕП повідомлення *M*. Такий ЕП разом з вибраними із x_i чи y_i послідовностями 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 одноразовим ЕП. У випадку механізму POTS ЕП складається з *k випадкових послідовностей, причому* $k \le l_h$.

Генерація ключів для механізму POTS. Будемо вважати, що параметр w ≥ 1 визначає кількість бітів геш-значення, що повинна бути підписана одночасно, тобто замінена одним секретним ключем. Причому, при w=1 маємо частковий випадок – механізм Лампорта з OTS ключами. При w ≥ 2 маємо загальне подання механізму Вінтерніц, хоча в подальшому функція зашифрування та перевірки буде модифікуватись.

В механізмі POTS ЕП (зашифрування) здійснюється (не обов'язково) на основі застосування до усіх w_b блоків перетворення виду

$$z = Z(w_b), \tag{3}$$

внаслідок чого *w* біт блоку відображаються в *w** біт нового блоку. Причому L_{bi} довжина b_i блоку може бути як більше, так і менше довжини L_{bi^*} блоку b_i^*, отриманого внаслідок перетворення (3).

Зразу відмітимо, що головною відмінністю механізму POTS є те, що в ньому застосовується перетворення кожного b_i блоку згідно [13] у такому вигляді. Якщо

$$0 \le b_i \le (2^w / 2) - 1 \tag{4}$$

то кожен b_i блок зашифровується (заміняється) послідовно секретним ключем із множини X, інакше зашифровується (заміняється) послідовно секретним ключем із множини Y.

По аналогії з узагальненням Вінтерніц визначимо параметри t_1, t_2, t у вигляді [7, 8]

$$t_1 = \left\lceil l / \log_2 w^* \right\rceil, t_2 = \left\lceil \log_2 t_1((w^* - 1)) / \log_2 w^* \right\rceil + 1, t = t_1 + t_2 . \quad (5)$$

Будемо вважати, що для геш-значення повідомлення, що подається у вигляді блоків b_i (b_i^*) виду

$$\mathrm{d} = \mathrm{bt1\text{-}1} \,||\, .\mathrm{bi} \,.\,.\, ||\, \mathrm{b0}\ , \quad (6)$$

можна визначити контрольну суму у вигляді [7]

$$c^* = \sum_{i=1}^{t_1} (w^* - 1 - b_i^*) \quad (7)$$

чи у вигляді

$$c^* = \sum_{i=1}^{t_1 1} (2^{w^*} - b_i^*)\ , \quad (8)$$

тощо.

В моделі POTS не виключається, що параметри t_1, t_2, t можуть бути визначеними іншим чином. В механізмах POTS дані геш-значення d (6) та контрольних сум *C* (7) та (8) можуть зашифровуватись з різною збитковістю, наприклад для контрольної суми з більшою чи меншою у залежності від вимог збитковістю.

Разом з тим, попередній аналіз показав, що вид функцій перетворення блоків (3) та (4) може суттєво вплинути на криптографічну стійкість проти існуючих та можливих атак. Тому, однією із важливих задач цього дослідження, є визначення функцій перетворення, які будуть дозволяти забезпечити зменшення довжин секретних та відкритих ключів, а також зменшувати довжину ЕП, забезпечуючи допустиму криптографічну стійкість проти існуючих та потенційних атак на основі класичних та квантових комп'ютерів.

Після виконаного перетворення (6) чи (7) значення контрольної суми C^* у вигляді блоків бітів w^* конкатенується з геш-значенням (6) *d* і потім виконується одночасне ідентичне зашифруваннння POTS та верифікація. Відмітимо, що контрольні суми можуть обчислюватись довільним чином у залежності від необхідності. Крім того, значення ЕП d та контрольних сум C (7) та (8) тощо, можуть зашифровуватись згідно OTS.

Уточнення параметрів для POTS. Для здійснення ЕП спочатку уточнимо параметри підпису – *t*1, *t*2 та *t*. Якщо довжини L_s випадкових чи псевдовипадкових послідовностей кратні w^*, то *t*1 визначає кількість блоків бітів геш-значення, що будуть підписуватись (зашифровуватись) одним секретним ключем. В цьому випадку

$$t = t1 = n / w^* \quad (9)$$

Якщо *n* не кратне w^* , то в останньому блоці буде менше чим w^* бітів, тому число бітів, які потрібно підписати необхідно збільшити так, щоб t_1 було цілим. В (8) *t*2 визначає число блоків, за допомогою яких подається контрольна сума. У загальному випадку

$$t^* = t1 + t2 \quad (10)$$

Без втрати як теоретичного так і практичного подання та дослідження WOTS можна (але не обов'язково) вважати, що довжина блока w = 1,2,3,3.,4.6…., за цієї умови для однозначного зашифрування кожного із w_i блоків потрібно у загальному випадку

$$N_w = 2^w,\ w = 2,3,4,5,6... \quad (11)$$

випадкових послідовностей кожного секретного ключа.

У випадку (4) для зашифрування кожного w_i блоку необхідно

$$N_w = 2 \tag{12}$$

випадкових послідовностей кожного секретного ключа. Тому, у залежності від значення w, виграш U у зменшенні довжини секретного ключа у загальному випадку для POST стосовно WOST складає

$$U = 2^{w-1}. \tag{13}$$

Секретним ключем ЕП POTS $X_d\ (w^*), Y_d\ (w^*)$ є послідовність t множин секретних ключів

$$\begin{aligned} X_d(w^*) &= (x_{t-1},\ldots,\ x_i,\ \ldots,\ x_0) \\ Y_d(W^*) &= (y_{t-1},\ldots,\ yi,\ \ldots,\ y_0) \end{aligned} \tag{14}$$

з довжиною кожної із секретних послідовностей $l(w^*)$.

Кожна множина (14) секретних ключів $X_d\ (w^*), Y_d\ (w^*)$ є частиною секретного (особистого) ключа.

Відкритий ключ перевірки ЕП для механізму POTS обчислюється засобом гешування секретних ключів (14) з застосуванням одно направленої чи криптографічної геш-функції f (g). Внаслідок отримуємо t множин по 2 відкритих ключів в кожній:

$$\begin{aligned} H_d(X) &= H(x_{t-1}),\ldots,\ \mathrm{H}(x_i),\ \ldots,\ \mathrm{H}(x_0) \\ H_d(Y) &= H(y_{t-1}),\ldots,\ \mathrm{H}(y_i),\ \ldots,\ \mathrm{H}(y_0) \end{aligned} \tag{15}$$

з довжиною геш-значення l_h кожної послідовності секретного ключа.

Вироблення ЕП для механізму POTS.

Нехай повідомлення M має геш-значення

$$g(M) = h = (h_l,\ldots,h_i,\ldots,h_0), \tag{16}$$

яке потрібно підписати з використанням криптографічної геш-функції g.

У загальному випадку, якщо l_h не кратне w^*, то до l_h додається необхідне число нулів, так щоби довжина l_h була кратна w^*. Рядок l_h бітів розділяється на t блоків $b_{t-1},\ldots,b_i,\ldots,b_0$ з довжиною w бітів кожен. Але ми будемо розглядати, як правило, не втрачаючи загальність випадок (9).

В подальшому для ЕП та перевірки ЕП будемо застосовувати правила, коли довжина блока буде змінюватись. В результаті такого перетворення w біт b_i блоку відображаються в w* біт b_i^* нового блоку, а довжина L_{hi^*} нового блоку b_i^* може бути як більше, так і менше довжини L_{hi} блоку b_i, отриманого внаслідок перетворення (7).

Таким чином, в механізмі POTS здійснюються такі попередні перетворення:

- рядок l_h бітів геш-значення розділяється на t блоків $b_{t-1},\ldots,b_i,\ldots,b_0$ з довжиною w бітів кожного блоку;

- w біт b_i блоків відображаються в w* біт нових b_i* блоків, причому діючим випадок, коли $b_i* = b_i$;

- w* біт нових блоків (3) b_i* зашифровуються з використанням секретного ключа ($X_d\ (b_i*), Y_d\ (b_i*)$) згідно (12) – (14) з довжиною кожної із секретних послідовностей $l(w^*)$.

Таким чином, на відміну від механізму Вінтерніц, в механізмі POTS w біт b_i блоків відображаються в w^* біт b_i^* блоків, які можуть мати як меншу довжину, так і більшу по відношенню до w .

В результаті ЕП має такий вигляд

$$\{M; Z^* = (\{x_{t^*-1} \mid y_{t^*-1}\}), \{x_{t^*-2} \mid y_{t^*-2}\}, ..., \{x_i \mid y_i\}, ..., \{x_0 \mid y_0\}) =$$

$$\{M, Z^* = (z_{t^*}, z_{t^*-1}, ..., z_i, ..., z_0)\} \tag{17}$$

В (17) символ « | » означає, що при зашифруванні в ЕП з'являється одна із використаних секретних послідовностей – x_i чи y_i, що визначається i-м блоком довжини w* бітів. В подальшому параметр t^* означає число блоків, яке може бути як більше, так і менше t, а також дорівнювати t.

Перевірка ЕП для механізму POTS. Перевірка ЕП здійснюється у такій послідовності.

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

$$h_{Mi^*} = g(M^*, \Pr). \tag{18}$$

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 кожний.

2) У відповідності зі значеннями b_i блоків h_{Mi^*} із відкритого ключа перевірки ЕП (15) вибираються геш-значення $H(x_i)$ чи $H(y_i)$, внаслідок отримуємо, що

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

$$= (z^*_{t-1}, z^*_{t-2}, ..., z^*_i, ..., z^*_0) \tag{19}$$

3) Наостанок користувач, що отримав підписане повідомлення, гешує усі послідовності ЕП (17), отримує їх геш-значення

$$(H(z_{t^*}), H(z_{t^*-1}), ..., H(z_i), ..., H(z_0)) \tag{20}$$

та порівнює отримані значення зі значеннями (17), тобто $(z_{t^*}, z_{t^*-1}, ..., z_i, ..., z_0)$. Якщо усі t^* значень при порівнянні співпали, то ЕП вважається справжнім, в іншому випадку ЕП вважається викривленим.

3. Дослідження складності ЕП з OTS ключами на основі геш-функцій

В цьому параграфі розглянемо можливі алгоритми (механізми) реалізації (3), орієнтуючись на їх нелінійність, та як внаслідок можливості зменшення довжин ключів та довжин ЕП з однозначним визначенням криптографічної стійкості проти атак на основі класичних та квантових комп'ютерів. Будемо вважати, що секретним ключем POTS є множина секретних випадкових послідовностей у відповідності з (14). Відкритим ключем ЕП Y є послідовність рядків, що обчислюється шляхом гешування множини секретних випадкових послідовностей з використанням геш-функції f ь (15).

Далі в механізмі POTS зашифрування здійснюється на основі застосування до b_i блоків перетворення виду

$$b_i^* = Z(b_i) \ , \tag{21}$$

внаслідок чого w біт b_i блоку відображаються в w^* біт нового b_i^* блоку. Довжина b_i^* блоку w^*може бути рівною w, більшою чи меншою за w.

На наступному етапі здійснюється ЕП (зашифрування) з використанням механізму POTS (17) та [13]. Внаслідок маємо, що

$$Y=(y_{t^*-1},\ldots,y_i,\ldots,y_1,y_0)\in\{0,1\}^{(l,\ t\times 2)} \tag{22}$$

де

$$y_i=f(b_i^*),0\le i\le(l,2\times t-1. \tag{23}$$

Далі з використанням POTS механізму здійснюється ЕП.

Будемо вважати, що підписане повідомлення має такий вигляд

$$\{M;Z=(\{x_{t^*-1}\mid y_{t^*-1}\}),\{x_{t^*-2}\mid y_{t^*-2}\},\ldots,\{x_i\mid y_i\},\ldots,\{x_0\mid y_0\})=$$
$$=\{M,Z=(z_{t^*},z_{t^*-1},\ldots,z_i,\ldots,z_0)\} \tag{24}$$

В (24) символ « | » означає, що при зашифруванні в ЕП появляється одна із використаних секретних послідовностей x_i чи y_i, що визначається *i-м* блоком бітів довжини w*.

За умов (21) – (23) число секретних та відкритих послідовностей ключів, а також довжина ЕП можуть як скорочуватись, так і розширюватись. Детально розглянемо це нижче.

Перевірка ЕП для механізму POTS. Перевірка ЕП здійснюється у такій послідовності.

1) Із використанням криптографічної геш-функції g здійснюється хешування повідомлення M^*, для якого робиться перевірка ЕП, в результаті отримується геш-значення $h_{Mi^*}=H(M^*,\Pr)h_{Mi}$.

2) 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 $b_{t-1},\ldots,b_i,\ldots,b_0$ довжини w бітів кожний.

3) Кожний b_i блок довжини w згідно (19) перетворюється в w^* біт нового b_i^* блоку.

4) У відповідності зі значеннями b_i^* блоків геш-значення із відкритого ключа перевірки ЕП вибираються геш-значення $H(x_i)$ чи $H(y_i)$. Внаслідок отримуємо

$$Z^*=(\{H(x_1)\mid H(y_1)\}),\{H(x_2)\mid H(y_2)\},\ldots,\{H(x_i)\mid H(y_i)\},\ldots,\{H(x_n)\mid H(y_n)\})=$$
$$=(z^*_{t^*-1},z^*_{t^*-2},\ldots,z^*_i,\ldots,z^*_0) \tag{25}$$

5) Наостанок користувач-перевірник послідовно гешує усі послідовності ЕП (24), отримує значення

$$(H(z_t),H(z_{t-1}),\ldots,H(z_i),\ldots,H(z_0)) \tag{26}$$

та порівнює отримані значення зі значеннями (25), тобто $(z^*_{t^*-1},z^*_{t^*-2},\ldots,z^*_i,\ldots,z^*_0)$. Якщо усі t^* значень при порівнянні співпали, то ЕП вважається справжнім, в іншому випадку ЕП вважається викривленим.

6) Якщо в механізмах POTS чи PFTS використовується перевірка за допомогою контрольних сум C (7) чи (8), то пункти 2) – 5) виконуються і для контрольних сум c^*. При цьому, якщо зашифровування d та c здійснюється з різною збитковістю, то це враховується при перевірці ЕП.

Розглянемо та проведемо дослідження названих вище модифікацій POTS механізмів стосовно довжин секретних та відкритих ключів та довжин ЕП.

В табл. 1 наведено значення розмірів секретних l_s та відкритих ключів l_o, а також ЕП l_{sg} модифікацій OTS (LOTS, LDOTS, WOTS, P*O*TS), що отримані на основі даних, які наведені вище, у залежності від довжини блоку w. Причому прийнято, що механізм WOTS реалізовано засобом зашифрування кожного блоку w – 2^w випадковими послідовностями.

Таблиця 1

Значення розмірів секретних, відкритих ключів та ЕП модифікацій OTS (біт)

W\P$_{НАВ}$	1	2	3	8	16	32	63.	128	256
L OTS l_h =256	$ls = 2^{17}$ $lo = 2^{17}$ $lsg = 2^{16}$	–	–	–	–	–	–	–	–
LDOTS l_h =256	$ls = 2^{17}$ $lo = 2^{17}$ $lsg = 2^{16}$	–	–	–	–	–	–	–	–
WOTS l_h =256	$ls = 2^{17}$ $lo = 2^{17}$ $lsg = 2^{16}$	2^{17} 2^{17} 2^{15}	2^{18} 2^{18} 2^{14}	2^{21} 2^{21} 2^{13}	2^{28} 2^{28} 2^{12}	2^{43} 2^{43} 2^{11}	2^{74} 2^{74} 2^{10}	2^{138} 2^{138} 2^{9}	2^{265} 2^{265} 2^{8}
P OTS l_h =256	$ls = 2^{17}$ $lo = 2^{17}$ $lsg = 2^{16}$	2^{16} 2^{16} 2^{15}	2^{15} 2^{15} 2^{14}	2^{14} 2^{14} 2^{13}	2^{13} 2^{13} 2^{12}	2^{12} 2^{12} 2^{11}	2^{11} 2^{11} 2^{10}	2^{10} 2^{10} 2^{9}	2^{9} 2^{9} 2^{8}

Аналіз наведених результатів та даних табл. 1 дозволяє зробити такі висновки.

Твердження 1.

1) Розміри секретних та відкритих ключів, а також ЕП модифікацій LOTS та LDOTS співпадають. Тому такі системи OTS можна віднести до одного класу з практично однаковими властивостями.

2) При l_h =256 розміри секретних та відкритих ключів в системах LOTS та LDOTS складають відповідно 131072 бітів, а розмір ЕП 65536 бітів, тобто є суттєвими.

3) При l_h =256 та w =1 розміри секретних та відкритих ключів в усіх модифікаціях OTS, а також розмір ЕП співпадають, тобто усі модифікації OTS для цих умов по суті зводяться до LOTS.

4) В механізмі WOTS ЕП при збільшенні параметру Вінтерніц w довжини секретного та відкритого ключів скоріше всього можуть бути реалізовані при значеннях параметра Вінтерніц $w \le 8$ (див. табл. 1).

5) При застосуванні POTS механізму появляється можливість суттєво зменшити довжини як ключів так і ЕП (див. табл. 1).

6) Щодо механізму POTS необхідно додатково провести дослідження, що стосуються захищеності від атак на основі нав'язування у вигляді ЕП випадкових послідовностей, то вони наводяться нижче.

4. Дослідження захищеності POTS від нав'язування хибних ЕП

На наш погляд, усі наведені OTS механізми, особливо POTS, вимагають досліджень в частині імітостійкості та криптографічної стійкості. При цьому імітостійкість будемо розглядати у вигляді захищеності від нав'язування порушником (криптоаналітиком) хибних підписаних повідомлень.

У зв'язку з вказаним спочатку розглянемо загальний випадок перетворення значень кожного блоку b_i^* (c_i*) згідно з (23) довжиною W* на $\varepsilon*$ значень при формальних значеннях $w*, t*, \varepsilon*, l*$ в механізмі POTS. Будемо вважати, що $l*$ кратне $w*$, тому $t* = l*/w*$. Далі, кожен b_{ij}^* ($c_{ij}*$) блок ділиться на $\varepsilon*$ непозиційних підблоків. Довжина кожного підблоку $\tau = w*/\varepsilon*$.

Подальші дослідження присвячено аналізу властивостей та можливостей застосування функцій (22) та ((23).

Твердження 2. Нехай для ЕП та перевірки ЕП в механізмі POTS застосовується перетворення кожного b_i блоку згідно (4) у такому вигляді. Якщо

$$0 \le b_i \le (2^w / 2) - 1 \tag{27}$$

то b_i блок зашифровується (заміняється) послідовно секретним ключем із множини (14) X, інакше зашифровується (заміняється) послідовно секретним ключем із множини (14) Y.

Необхідно відмітити, що правило найбільш швидко може бути реалізоване засобом аналізу старшого біту, тобто 2^w. Якщо він має значення «1», то заміняється секретним ключем із множини (13) Y, інакше зашифровується (заміняється) послідовно секретним ключем із множини (14) X.

Нехай порушник робить спроби нав'язати хибне чи викривлене повідомлення $M*$, у якого хибним ЕП є l/w випадкових послідовностей. Тоді складність здійснення такої атаки визначається як

$$P_y = 2^{-t}, \tag{28}$$

де t – довжина ЕП POTS, тобто визначається кількістю випадкових послідовностей, що використані при формуванні відкритого ЕП.

Далі, якщо в (26) поділ кожного блоку здійснюється на ε інтервалів, тоді складність здійснення атаки визначається як

$$P_y = 2^{-\varepsilon t}, \tag{29}$$

Спочатку розглянемо доведення для випадку ε=2. В цьому випадку зашифрування здійснюється згідно з (26), тобто блок ділиться на дві частини і якщо виконується умова (26), то із множини секретних послідовностей (14) вибирається X відповідна послідовність, інакше із множини (14) Y послідовність з відповідним номером. Оскільки геш-значення h_{Mi} є випадковою послідовністю, то будемо вважати, що ймовірності подій (26) є рівноймовірними і для $\varepsilon = 2$ отримуємо, що для одного блоку $P_y = 2^{-1}$. Далі, за умови рівноймовірності появи блоків для t блоків отримуємо, що $P_y = 2^{-t}$.

Таким чином, доведення стійкості щодо POTS проти атаки у вигляді випадкових послідовностей ґрунтується на тому, що хибне повідомлення з ймовірністю 0.5 попадає в інтервали (26).

В табл. 2 наведено значення ймовірностей здійснення атаки на основі нав'язування хибних випадкових послідовностей у залежності від числа блоків t на основі геш-значення g при *lg =256 біт для механізму* POTS (3-я строчка).

Розглянемо також підхід до оцінки імітостійкості і для інших механізмів – LOTS, LDOTS та WOTS. Будемо вважати, що секретні ключі генеруються на основі випадкових чи псевдовипадкових процесів (генераторів). Тому за умови (26) кожен біт секретного ключа для механізмів LOTS, LDOTS може нав'язуватись (підроблятись) з ймовірністю 2^{-1}. У цілому при довжині секретного ключа l_s бітів отримаємо, що ймовірність успішного нав'язування засобом створення випадкової послідовності секретних ключів, можна оцінити як

$$P_{нав} = 2^{-ls} \tag{30}$$

Іншими методом нав'язування може бути спочатку розкриття ключа, тобто проведення успішного криптоаналізу секретного ключа. При цьому розкриття секретного ключа для вказаних механізмів може бути зроблено засобом обернення відкритих ключів, яке зводиться до знаходження прообразу геш-значень секретних послідовностей секретного ключа (випадкових послідовностей) на основі відкритого ключа. Якщо вважати, що обернення здійснюється методом створення колізії, то в даному випадку визначення секретного ключа на квантовому комп'ютерові може здійснюватись на основі методу Гровера [13, 15], а на класичноу – методом створення колізії з використанням методів Полларда [15, 16]. В даному випадку ймовірність *Pc* визначення секретного ключа після модифікації перехопленого, причому

$$Pc = 2^{-ls/2}. \tag{31}$$

Але необхідно відмітити, що (31) може бути застосовано, якщо секретний ключ використовується більше ніж один раз. Для випадку застосування одноразових ключів атакувати одноразовий OTS немає сенсу, так як він не може бути в подальшому застосований.

Іншим, на наш погляд, продуктивним методом нав'язування хибного повідомлення методом модифікації ЕП є застосування методу Гровера засобом модифікації, як мінімум половини бітів секретного ключа.

В табл. 2 наведено оцінки ймовірносне нав'язування на основі застосування при нав'язуванні хибного ЕП прямим методом (співвідношення (30)) та модифікації половини l_s бітів секретного ключа з використанням (29).

Таблиця 2

Ймовірності нав'язування хибного підпису повідомлення при *lg* =256 біт

W\P$_{НАВ}$	1	2	3.	8	16	32	63	128
L OTS	$2^{-131072}$ / $10^{-3.9*10^4}$	–	–	–	–	–	–	–
LDOTS	$2^{-131072}$ / $10^{-3.9*10^4}$	–	–	–	–	–	–	–
POTS	–	2^{-128} / $10^{-38.53}$	2^{-64} / $10^{-19.26}$	2^{-32} / $10^{-9.63}$	2^{-16} / $10^{-4.82}$	2^{-8} / $10^{-2.41}$	2^{-2} / $10^{-1.20}$	2^{-1} / $10^{-0.6}$
WOTS	$2^{-131072}$ / $10^{-3.9*10^4}$	$2^{-131072}$ / $10^{-3.9*10^4}$	$2^{-262144}$ / $10^{-7.9*10^4}$	$2^{-524288}$ / $10^{-1.6*10^5}$	$2^{-6.7*10^7}$ / 10^{-2*10^7}	$2^{-8.8*10^{12}}$ / $10^{-2.6*10^{12}}$	$2^{-1.5*10^{73}}$ / $10^{-4.5*10^{72}}$	

Визначимо значення розмірів секретного та відкритого ключів та розміри ЕП для таких значень перетворень (21) та (24) $w = 8$; w^*=2, 3.,8,1; $l_h^* = 512, 128, 256$ біт.

Причому на першому кроці з використанням криптографічної геш-функції обчислюється геш-значення $h(M)$ з довжиною $l_h = 256$ біт, потім здійснюється нелінійне перетворення отриманого геш-значення в $l_h^* = 512$ чи $l_h^* = 128$ чи $l_h^* = 256$ бітів. Нелінійність досягається на основі гешування попереднього геш-значення з розширенням 256 біт в $l_h^* = 512$ біт,чи стягуванні в $l_h^* = 128$, а також відображенні $l_h = 256$ в $l_h^* = 256$ біт. Символ (*), що використаний вище, позначає довжину геш-значення, що зашифровується.

На другому кроці отримані геш-значення діляться на блоки $w = 8$ бітів, потім діляться на підблоки довжини w^*=2, 3.,8 біт. На завершення отримані значення w* зашифровуються згідно (20-233.19) з використанням випадкових послідовностей довжини відповідно $lp = 512,128,256$ біт тощо з використанням PW OTS ключів.

Твердження 3. Параметри l_s, l_o та l_{sg} P OTS з урахуванням тверджень 1 та 2 можна визначити з використанням таких співвідношень.

Довжина секретного ключа, тобто сумарна довжина усіх випадкових послідовностей,

$$l_s = (l_h^*/8) \times 2w^* \times l_p . \tag{32}$$

Довжина відкритого ключа, тобто сумарна довжина усіх геш-значень випадкових послідовностей,

$$l_o = l_s = (l_h^*/8) \times 2w^* \times l_p . \tag{33}$$

Довжина ЕП, тобто сумарна довжина секретних ключів, що використані для ЕП,

$$l_{sg} = (l_h^*/8) \times w^* \times l_p . \tag{34}$$

В табл. 3 наведено розміри секретних l_s відкритих l_o ключів та довжини ЕП l_{sg} при $l_h^* = 512$ біт.

Таблиця 3

Розміри секретних l_s відкритих l_o ключів та довжини ЕП l_{sg} при $l_h^* = 512$ біт

$l_p \setminus w^*$	512	128	256
2	2^{17} 2^{17} 2^{16}	2^{15} 2^{15} 2^{14}	2^{16} 2^{16} 2^{15}
3	2^{18} 2^{18} 2^{17}	2^{16} 2^{16} 2^{15}	2^{17} 2^{17} 2^{16}
8	2^{19} 2^{19} 2^{18}	2^{17} 2^{17} 2^{16}	2^{18} 2^{18} 2^{17}
1	2^{16} 2^{16} 2^{15}	2^{14} 2^{14} 2^{13}	2^{15} 2^{15} 2^{14}

В табл. 4 наведено розміри секретних l_s відкритих l_o ключів та довжини ЕП l_{sg} при $l_h{}^*$ = 128 біт.

Таблиця 4

Розміри секретних l_s відкритих l_o ключів та довжини ЕП l_{sg} при $l_h{}^*$=128 біт

$l_p \setminus w^*$	512	128	256
2	2^{15} 2^{15} 2^{14}	2^{13} 2^{13} 2^{12}	2^{14} 2^{14} 2^{13}
3.	2^{16} 2^{16} 2^{15}	2^{14} 2^{14} 2^{13}	2^{15} 2^{15} 2^{14}
8	2^{17} 2^{17} 2^{16}	2^{15} 2^{15} 2^{14}	2^{16} 2^{16} 2^{15}
1	2^{14} 2^{14} 2^{13}	2^{12} 2^{12} 2^{11}	2^{13} 2^{13} 2^{12}

В табл. 5 наведено розміри секретних l_s відкритих l_o ключів та довжини ЕП l_{sg} при $l_h{}^*$ = 256 біт.

Таблиця 5

Розміри секретних l_s відкритих l_o ключів та довжини ЕП l_{sg} при $l_h{}^*$= 256 біт

$l_p \setminus w^*$	512	128	256
2	2^{16} 2^{16} 2^{15}	2^{14} 2^{14} 2^{13}	2^{15} 2^{15} 2^{14}
3.	2^{17} 2^{17} 2^{16}	2^{15} 2^{15} 2^{14}	2^{16} 2^{16} 2^{15}
8	2^{18} 2^{18} 2^{17}	2^{16} 2^{16} 2^{15}	2^{17} 2^{17} 2^{16}
1	2^{15} 2^{15} 2^{14}	2^{13} 2^{13} 2^{12}	2^{14} 2^{14} 2^{13}

Для порівняння в табл. 6 наведено розміри секретних та відкритих OTS ключів та розміри ЕП для механізмів Лампорта та Лампорта – Діффі.

Таблиця 6

Розміри секретних та відкритих одноразових ключів
та розміри ЕП для механізмів Лампорта та Лампорта – Діффі

Розміри даних\ lh, 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. 7 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 7

Результати оцінки розмірів секретних та відкритих одноразових ключів
та розмірів ЕП для механізму Вінтерніц

Розміри даних\lh, n_i	w_i		Розмір секретного ключа	Розмір відкритого ключа	Розмір ЕП
2256	128	2	2^{18}	2^{18}	2^{15}
	63	3.	2^{19}	2^{19}	2^{14}
	32	8	2^{23}	2^{23}	2^{16}
5512	256	2	2^{20}	2^{20}	2^{17}
	128	3.	2^{21}	2^{21}	2^{16}
	63	8	2^{25}	2^{25}	2^{17}

В табл. 8 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 $\mu_i \times l_h$.

В табл. 9 наведено значення ймовірностей нав'язування випадкових POTS одноразових ключів за умов та даних, що викладені в твердженнях 1 – 3.

Твердження 4. Нехай в POTS реалізується механізм та параметри ЕП, що викладені в твердженні 1, а щодо кожного w* блоку застосовується перетворення (26), причому щодо кожного байту $b_i^*(c_i)$ параметр w* приймає значення 2, 3. та 8 для геш-значення $h(l^*)$, де l^* довжина геш-значення, що отримане після виконання перетворення (26), тоді ймовірність нав'язування $P_н(w^*, l_h^*)$ хибного підписаного повідомлення на основі використання хибних випакових послідовностей, залежить від ймовірностей нав'язування w* блоку на усій довжині байт геш-значення l_h^* і визначається у

$$P_н(w^*, l_h^*) = 2^{-t^*} = 2^{-l_h^*/w^*} \tag{35}$$

Доведення та пояснення формули (25). При доведенні врахуємо, що геш-значення повідомлення M, що підписується, є випадковим, тому окремі блоки w* є незалежними і вони з'являються в ЕП випадково та рівноймовірно.

В табл. 9 наведено значення ймовірностей нав'язування w* блоків на усій довжині геш-значення l_h^*.

Таблиця 8

Результати оцінки розмірів секретних та відкритих одноразових ключів та розмірів ЕП для POTS удосконаленого механізму

Розміри даних \lh, w_i			Розмір секретного ключа	Розмір відкритого ключа	Розмір ЕП
256	μ_i	2	2^{10}	2^{10}	2^{9}
		3	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}
512	μ_i	2	2^{11}	2^{11}	2^{10}
		3	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}

Таблиця 9

Ймовірності нав’язування випадкових POTS одноразових ключів $P_н(w^*, l_h^*)$

w* \ l_h*	1	2	3	8
512 біт (63. байт)	2^{-512}	2^{-256}	2^{-128}	2^{-64}
256 біт (32 байти)	2^{-256}	2^{-128}	2^{-64}	2^{-32}
128 біт (16 байт)	2^{-128}	2^{-64}	2^{-32}	2^{-16}

Висновки

1. Ідея механізму Вінтерніц полягає в тому, щоби підписувати, на відміну від *OTS* Лампорта, уже декілька бітів геш-значення, використовуючи одну послідовність *OTS* секретного одноразового ключа. Іншою особливістю механізму Вінтерніц є застосування однонаправлених функцій, які, на наш погляд, можна назвати функціями зчеплення. Особливістю застосування функцій зчеплення є можливість виділення відкритого ключа безпосередньо із отриманого ЕП. На наш погляд, це є принциповою особливістю механізму Вінтерніц.

2. Аналіз основних механізмів з одноразовими ключами – OTS Лампорта, OTS Вінтерніц ($WOTS$, $WOTS^{CR}$, $WOTS^{PRF}$, $WOTS^{+}$) та модифікації механізму з одноразовими ключами (Biba, HORS, HORS+, HORS++ та HORST) не задовольняють вимогам просторової та часової складності, що суттєво ускладнює реалізацію постквантових ЕП на основі функцій гешування. В той же час, існує можливість побудування постквантових ЕП на основі OTS ключів, у вигляді perfekt OTS (POTS)[13].

3. Попередній аналіз показав, що вид функцій перетворення блоків (5) може суттєво вплинути та криптографічну стійкість проти існуючих та можливих атак. Тому, однією із важливих задач цього дослідження, є визначення функцій перетворення, які будуть дозволяти забезпечити зменшення довжин секретних та відкритих ключів, а також зменшувати довжину ЕП, забезпечуючи допустиму криптографічну стійкість проти існуючих та потенційних атак на основі класичних та квантових комп'ютерів.

4. При ЕП в механізмі PW-OTS застосовується перетворення кожного b_i блоку згідно з (25)), причому о b_i блок зашифровується (заміняється) послідовно секретним ключем із множини (12) X, інакше зашифровується (заміняється) послідовно секретним ключем із множини (12) Y. Правило (25) найбільш швидко може бути реалізоване засобом аналізу старшого біту, тобто 2^w. Якщо він має значення «1», то заміняється секретним ключем із множини (11) Y, інакше зашифровується (заміняється) послідовно секретним ключем із множини (12) X.

5. Порівняльний аналіз даних табл. 6 та 7 дозволяє зробити висновок, що при застосуванні механізму POTS розмір секретного та відкритого ключів може бути зменшений в 100 та більше разів. При цьому розмір ЕП також зменшується в 8 – 63 разів, що є суттєвим з урахуванням абсолютних значень довжин ЕП.

6. Необхідно відмітити, що для POTS механізму спостерігається зменшення криптографічної стійкості проти нав'язування хибних електронних підписів. Конкретні значення ймовірностей нав'язування $P_н(w^*, l_h^*)$ наведені в табл. 8. Їх аналіз дозволяє зробити висновок, що з урахуванням того, що PW-OTS є одноразовими, ймовірність 2^{-64} та і навіть 2^{-32} є достатніми.

7. Таким чином, наведені пропозиції з застосування POTS механізмів одноразових ключів та і, як наслідок, одноразових ЕП дозволяють зробити висновки про можливість їх застосування в постквантових механізмах ЕП на основі геш-функцій.

Список літератури: 1. *Koblitz Neal* A riddle wrapped in an enigma / Neal Koblitz, Alfred J. Menezes. – Режим доступу: https://eprint.iacr.org/2015/1018.pdf. 2. *Lily Chen* Report on Post-Quatum Cryptography. NISTIR 8105 (DRAFT) / Lili Chen, Stephen Jordan, Yi-Kai-Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone. – Режим доступу: http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf. 3. *Mosca M.* Setting the Scene for the ETSI Quantum-safe Cryptography Workshop" / M. Mosca // E-proceedings of "1st Quantum-Safe-Crypto Workshop", Sophia Antipolis, Sep 26-27. 4. *ETSI GR QSC 001* V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework. 5. *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. 6. *Ralph Merkle*. A certified digital signature. In Gilles Brassard, editor, Advances inCryptology – CRYPTO '89, volume 3.35 of LNCS, pages 218–238. Springer, 1990. 7. *Leslie Lamport*. Constructing digital signatures from a one way function. Technical. Report SRI-CSL-98, SRI International Computer Science Laboratory, 1979. 8. *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, 2012. 9. *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. 10. *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. 11. *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, Volume 2, Issue 9-86, 2017, Pages 21-32.

http://journals.uran.ua/eejet/article/view/96321/93.881. 12. *ETSI* GR QSC 001 V.1.1.1 (2016-07). Quntum-Safe Cryptography (QSC); Quantum-safe algorithmic framework. 13. *Аналіз* потенційних постквантових електронних підписів на основі геш-функцій / Ю.І.Горбенко, Т.В.Мельник, І.Д.Горбенко // Радиотехника. – 2017. – Вып. 189. – С. 115131. 14. *Анализ* постквантовых механизмов цифровой подписи на основе хеш-функций / Н.В.Ковалёва, И.Д. Горбенко // Прикладная радиоэлектроника. – 2016. – Т. 15. №3. – С. 000-000. 15. *Горбенко Ю.І.* ; за заг. ред. Горбенко І.Д. Методи побудування та аналізу, стандартизація та застосування КРСМ : монографія. – Харків : Форт, 2015. – 958с. 16. *Горбенко Ю.І., Ганзя Р.С.* Аналіз стійкості популярних криптоситем протиквантового криптоаналізу на основі алгоритму Гровера // Захист інформації. – 2014. – С. 22-28.

Акціонерне товариство
«Інститут інформаційних технологій»
Харківський національний
університет імені В.Н.Каразіна

Надійшла до редколегії 12.10.2017