УДК 004.38
DOI: https://doi.org/10.17721/ISTS.2024.7.31-38

Андрій ФЕСЕНКО, канд. техн. наук , доц.
ORCID ID: 0000-0001-5154-5324
e-mail: andrii.fesenko@knu.ua
Київський національний університет імені Тараса Шевченка, Київ, Україна

Марія МИРОШНІЧЕНКО, студ.
ORCID ID: 0009-0008-3535-661X
e-mail: mrshnchnkmaria@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

ПОРІВНЯННЯ ПОСТКВАНТОВИХ СТАНДАРТІВ У РОЗРІЗІ ВПРОВАДЖЕННЯ У КЛАСИЧНІ АЛГОРИТМИ ЕЛЕКТРОННОГО ПІДПИСУ

Вступ. *Дослідження розробки й упровадження постквантових стандартів, а також аналіз і порівняння вже існуючих алгоритмів, на основі яких може засновуватись функціонування стандартів у сфері електронного цифрового підпису. Одним з основних питань стало вивчення міграції класичної криптографії до постквантової. Наведено порівняння трьох популярних постквантових стандартів: CRYSTALS-Dilithium, Falcon та SPHINCS+. В результаті дослідження обрано найоптимальніший із стандартів до впровадження у класичні схеми електронного підпису.*

Зазначене дослідження є актуальним у зв'язку зі зростанням інтересу до квантових технологій і потребою у забезпеченні безпеки електронних комунікацій у майбутньому квантовому світі.

Методи. *Використано методи міграції класичної криптографії до постквантової. Це важливе питання, оскільки потужність квантових комп'ютерів може вразити деякі існуючі криптографічні алгоритми. Проведено аналіз можливостей переходу до нових стандартів та їхньої відповідності вимогам безпеки. Наведено порівняння трьох популярних постквантових стандартів: CRYSTALS-Dilithium, Falcon та SPHINCS+. Це дозволяє визначити найоптимальніший та найнадійніший стандарт для впровадження у класичні схеми електронного підпису. Автори обґрунтовують вибір оптимального стандарту, враховуючи його властивості та відповідність вимогам безпеки.*

Результати. *Стаття містить важливі результати дослідження у галузі постквантових стандартів для електронного цифрового підпису, що можуть бути корисними для розробників криптографічного програмного забезпечення й інженерів з інформаційної безпеки.*

Додатково розглянуто питання щодо викликів і перешкод у впровадженні постквантових стандартів, таких як складність реалізації, вартість інфраструктури та задачі стандартизації. Висвітлено перспективи майбутнього розвитку постквантової криптографії та вплив її впровадження на сучасні системи електронного підпису. Це допоможе читачам отримати повніше розуміння та контекст щодо важливості й потенційних викликів у цій області.

Висновки. *Falcon і CRYSTALS-Dilithium відомі високою швидкістю підписування і помірнішим розміром ключа, що робить їх практичними для багатьох застосувань. SPHINCS+, незважаючи на свою відмовостійкість, має меншу швидкість і вимагає більшого розміру ключа. Вибір між CRYSTALS-Dilithium, Falcon і SPHINCS+ залежатиме від конкретних потреб застосування, а також від компромісів між швидкістю, розміром ключа та відмовостійкістю. Зазвичай ці системи пропонують високу швидкість підписування, і це одна з їхніх ключових переваг. Вони призначені для використання у швидких операціях, наприклад, на серверах чи вбудованих системах.*

Ключові слова: *електронний підпис, постквантова криптографія, криптогнучкість, постквантові стандарти.*

Вступ

Криптографія є вирішальним інструментом для безпеки нашого цифрового суспільства і використовується практично всюди. Наприклад, вона захищає наші онлайн-комунікації, зберігає дані на пристроях у секреті, навіть, якщо ми їх втратимо, і захищає цілісність та автентичність цифрових записів.

Нині безпека цифрових інфраструктур значною мірою базується на криптографії з відкритим

ISSN 2707-1758

ключем (також відомій як "асиметрична криптографія"). Актуальність теми полягає у тому, що з кожним новим етапом розвитку квантових технологій зростає загроза сучасній криптографії, на якій заснована безпека функціонування більшості державних установ. Для попередження злому сучасної системи шифрування інформації впровадження постквантових стандартів уже зараз є нагальною потребою, поки квантовий комп'ютер все ще перебуває на стадії розробки.

Щоб попередити загрозу сучасній асиметричній криптографії з боку квантових комп'ютерів, неминучим стало виникнення галузі криптографічних досліджень – постквантової криптографії. Названа галузь передбачає розроблення та дослідження асиметричних криптосистем, які не можуть бути зламані навіть за допомогою потужних квантових комп'ютерів. Методи переважно базуються на розв'язанні математичних задач, для яких сьогодні невідомі як класичні алгоритми, так і квантові.

Електронний підпис – це електронні дані у зашифрованій формі, які додаються підписантом до інших електронних даних, наприклад електронних документів, звітності, або ж логічно з ними пов'язуються та використовуються ним як замінник справжнього особистого підпису. Отже, ключів при застосуванні ЕП існує два – особистий і відкритий. Відкритий ключ використовують для зчитування особистого ключа, до якого підписант подав звітність. Особистий може бути записаний, наприклад, на флешку чи інший носій.

У схемі електронного підпису (рис. 1) повідомлення надається зі значенням, яке дозволяє перевірити автентичність, цілісність і незаперечне авторство повідомлення. Схеми цифрового підпису є асиметричними криптосистемами. Закритий ключ використовують для генерування підпису, відкритий ключ можна застосувати для перевірки підпису.

Рис. 1. Схема електронного підпису

Мета. Необхідність досліджень указаної теми полягає у систематизації знань і результатів, отриманих у процесі опрацювання інформації, оскільки дослідження і розвиток постквантових методів допомагають розв'язувати багато ключових проблем, пов'язаних із постквантовими технологіями. Аналіз методів створення постквантових стандартів сприяє розробленню потужніших квантових комп'ютерів та ефективніших квантових алгоритмів. Це відкриває нові можливості для розв'язання складних обчислювальних задач. Аналіз методів створення постквантових стандартів допомагає розробити нові квантові криптографічні протоколи, які можуть стати основою майбутньої безпеки мереж та інформаційних систем. Розвиток постквантових стандартів є ключовим для квантової комунікації, яка може забезпечити надійне передавання даних захищеними від перехоплення зловмисниками.

Методи

У роботі використано методи міграції класичної криптографії до постквантової. Це важливе

питання, оскільки потужність квантових комп'ютерів може вразити деякі існуючі криптографічні алгоритми. Також проведено аналіз можливостей переходу до нових стандартів та їхньої відповідності вимогам безпеки.

Крім того, наведено порівняння трьох популярних постквантових стандартів: CRYSTALS-Dilithium, Falcon та SPHINCS+. Це дозволяє визначити найоптимальніший і найнадійніший стандарт для впровадження у класичні схеми електронного підпису. Автори обґрунтовують вибір оптимального стандарту, враховуючи його властивості та відповідність вимогам безпеки.

Результати

Класичну схему електронного підпису використовують для забезпечення автентичності та цілісності електронної інформації, яку надає або підписує особа, чи сутність у цифровому форматі. Основні кроки цієї схеми такі.

1. Генерування ключів. Спочатку сторона, яка буде підписувати повідомлення, створює пару ключів – приватний ключ і відкритий ключ. Приватний ключ залишається суто конфіденційним і не повинен розголошуватися.

2. Підписання даних. Для підпису повідомлення суб'єкт використовує свій приватний ключ і криптографічний алгоритм, щоб створити цифровий підпис. Цей підпис додається до повідомлення.

3. Передавання повідомлення і підпису. Спільно з підписаним повідомленням суб'єкт також може надіслати свій відкритий ключ іншій стороні або опублікувати його в загальнодоступному реєстрі, якщо це необхідно для перевірки підпису.

4. Перевірка підпису. Отримуючи підписане повідомлення і відкритий ключ, інша сторона може використовувати криптографічний алгоритм, щоб перевірити цифровий підпис. Якщо підпис правильний, то це свідчить про те, що повідомлення не було змінене після підписування і було підписане особою з відповідним приватним ключем.

5. Довіра до ключа. Один із важливих аспектів класичної схеми електронного підпису – це підтвердження довіреності відкритого ключа, що використовується для перевірки підпису. Це може включати використання довірених центрів сертифікації ключів (ЦСК) або мережу блокчейну для підтвердження відповідності відкритого ключа конкретній особі або сутності.

Класичні алгоритми електронного підпису базуються на обчислювальній складності певних математичних завдань, таких як факторизація великих чисел, обчислення дискретного логарифма тощо. Нині ці алгоритми вважають безпечними завдяки складності вказаних обчислень на класичних комп'ютерах.

Проте квантові обчислення можуть потенційно стати загрозою для безпеки цих класичних алгоритмів електронного підпису. Квантові комп'ютери мають здатність розв'язувати деякі математичні завдання, які є важкими для класичних комп'ютерів, набагато швидше. Зокрема, алгоритм Шора може дуже ефективно факторизувати великі числа і зламувати RSA-шифрування. Це означає, що, коли в майбутньому буде побудований потужний квантовий комп'ютер, то класичні алгоритми електронного підпису, які засновані на розглянутих математичних задачах, можуть бути вразливими (Горбенко та ін., 2017).

CRYSTALS-Dilithium

Загальна оцінка. Dilithium є схемою підпису з високою ефективністю, порівняно простою реалізацією, сильним теоретичним обґрунтуванням – довгою історією вивчення. Вказана схема є гарним вибором для великої кількості криптографічних застосувань. Тому NIST обрав цю схему для стандартизації.

Безпека. Безпека Dilithium ґрунтується на Module-LWE, чого вже достатньо для того, щоб показати, що відкритий ключ не розкриває інформації про секретний ключ.

Механізм Crystals-Dilithium є ЕП, що має надійну безпеку від атак на вибране повідомлення, його стійкість базується на складності проблем ґратки над модульними ґратками. Поняття безпеки означає, що порушник, який має доступ до "оракула" підпису, не може виробити підпис повідомлення, підпис якого він ще не бачив, а також не може створити інший підпис повідомлення, яке він уже бачив підписаним.

Механізм ЕП Crystals-Dilithium є консервативний за параметрами і дозволяє зменшити розмір відкритого ключа та відносно легко дозволяє змінювати рівень криптостійкості, змінюючи розміри параметрів і ключів.

Функціональну реалізацію алгоритму зображено на рис. 2. Оскільки багато програм вимагають передавання як відкритого ключа, так і підпису (напр., ланцюжки сертифікатів), розроблена схема мінімізує суму цих параметрів. Відповідно до обмеження, щодо уникнення дискретної вибірки Гаусса, відомо, що Dilithium має найменшу комбінацію розмірів підпису та відкритого ключа з усіх схем постквантового підпису (Горбенко, & Ганзя, 2014).

ISSN 2707-1758

Gen

$\mathbf{A} \leftarrow R_q^{k \times \ell}$
$(\mathbf{s}_1, \mathbf{s}_2) \leftarrow S_\eta^\ell \times S_\eta^k$
$\mathbf{t} := \mathbf{A}\mathbf{s}_1 + \mathbf{s}_2$
return $(pk = (\mathbf{A}, \mathbf{t}), sk = (\mathbf{A}, \mathbf{t}, \mathbf{s}_1, \mathbf{s}_2))$

Sign(sk, M)

$\mathbf{z} := \perp$
while $\mathbf{z} = \perp$ do
  $\mathbf{y} \leftarrow S_{\gamma_1 - 1}^\ell$
  $\mathbf{w}_1 := \mathsf{HighBits}(\mathbf{A}\mathbf{y}, 2\gamma_2)$
  $c \in B_{60} := \mathsf{H}(M \parallel \mathbf{w}_1)$
  $\mathbf{z} := \mathbf{y} + c\mathbf{s}_1$
  if $\|\mathbf{z}\|_\infty \geq \gamma_1 - \beta$ or $\|\mathsf{LowBits}(\mathbf{A}\mathbf{y} - c\mathbf{s}_2, 2\gamma_2)\|_\infty \geq \gamma_2 - \beta$, then $\mathbf{z} := \perp$
return $\sigma = (\mathbf{z}, c)$

Verify$(pk, M, \sigma = (\mathbf{z}, c))$

$\mathbf{w}_1' := \mathsf{HighBits}(\mathbf{A}\mathbf{z} - c\mathbf{t}, 2\gamma_2)$
if return $[\![\|\mathbf{z}\|_\infty < \gamma_1 - \beta]\!]$ **and** $[\![c = \mathsf{H}(M \parallel \mathbf{w}_1')]\!]$

Рис. 2. Шаблон для схеми підпису Crystals-Dilithium

Falcon

Falcon (Fast Fourier Lattice-based Compact Signatures over NTRU) – схема на ґратках, що використовує підхід Hash-And-Sign. Теоретична безпека Falcon підтверджується доказом у моделі QROM на основі складності SIS над NTRU ґратками. Консервативні оцінки складності підробки підпису Falcon мають ті самі значення, що і для Dilithium. В ньому ідеалізовано швидкі компактні підписи на основі ґратки Фур'є. Конструкція ЕП Falcon є простою, в ньому реалізуються теоретичні межі для хешування й ЕП на основі ґратки. В механізмі використовують клас криптографічних ґраток (клас граток NTRU) та зразок "лазівки", реалізуючи швидку вибірку Фур'є.

Falcon має найменші розміри відкритого ключа та підпису серед кандидатів третього раунду. Falcon дуже швидко перевіряє підпис. Вироблення підпису відбувається дещо повільніше за Dilithium, а генерування ключів – значно повільніше. З урахуванням цієї інформації, можна сказати, що Falcon може бути гарним вибором у деяких спеціалізованих протоколах, проте у загальному випадку поступається Dilithium згідно з Post-Quantum Cryptography. Round 2 Submissions. (https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions).

Блок-схему генерування ключів алгоритму Falcon зображено на рис. 3.

Алгоритм генерування ключів зображено на рис. 4. Ця процедура є основним алгоритмом формування підпису.

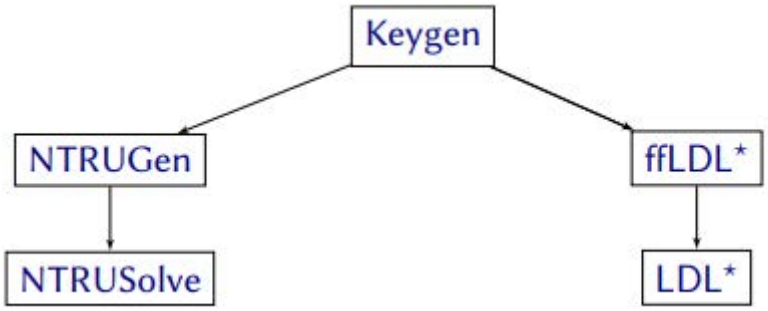

Рис. 3. Блок-схема генерування ключів

Require: A monic polynomial $\phi \in \mathbb{Z}[x]$, a modulus q
Ensure: A secret key sk, a public key pk
1: $f, g, F, G \leftarrow \mathsf{NTRUGen}(\phi, q)$ ▷ Solving the NTRU equation
2: $\mathbf{B} \leftarrow \left[\begin{array}{c|c} g & -f \\ \hline G & -F \end{array}\right]$
3: $\hat{\mathbf{B}} \leftarrow \mathsf{FFT}(\mathbf{B})$ ▷ Compute the FFT for each of the 4 components $\{g, -f, G, -F\}$
4: $\mathbf{G} \leftarrow \hat{\mathbf{B}} \times \hat{\mathbf{B}}^{\star}$
5: $\mathsf{T} \leftarrow \mathsf{ffLDL}^{\star}(\mathbf{G})$ ▷ Computing the LDL* tree
6: for each leaf leaf of T do ▷ Normalization step
7: leaf.value $\leftarrow \sigma / \sqrt{\text{leaf.value}}$
8: $\mathsf{sk} \leftarrow (\hat{\mathbf{B}}, \mathsf{T})$
9: $h \leftarrow g f^{-1} \bmod q$
10: $\mathsf{pk} \leftarrow h$
11: return sk, pk

Рис. 4. Алгоритм генерування ключів

Falcon був обраний для стандартизації тому, що NIST має впевненість у його безпеці (якщо реалізація виконана правильно з урахуванням атак) та тому, що він має малий розмір відкритого ключа та підпису, що важливо у багатьох застосуваннях.

SPHINCS+

SPHINCS+ – це схема підпису без збереження стану на основі хешу.

Конструкція. Схема поєднує використання одноразових підписів, кількох підписів, дерев Меркла та гіпердерев для створення схеми цифрового підпису, яка підходить для загального застосування.

Зауважимо, що криптографічна безпека SPHINCS+ ґрунтується лише на безпеці використовуваних базових хеш-функцій. Це припущення щодо безпеки не залежить від того, на яких базуються інші схеми підписів фіналістів (напр., Dilithium і Falcon), тому SPHINCS+ забезпечує успішний **запасний варіант у разі непередбачених криптоаналітичних атак.**

Продуктивність. Через спосіб формування підписів SPHINCS+ генерування та перевірка ключів відбувається набагато швидше. Навіть для безпеки Категорії 1 найменші (і найповільніші) вибори параметрів дають підпис, розмір якого становить близько 8 кБ і є набагато більшим, ніж у альтернативних схемах підпису, таких як Falcon або Dilithium (Горбенко та ін., 2018):

- w: розмір слів, які використовуються;
- l_1: фіксована кількість слів, розмір яких становить w, повідомлень, які потрібно підписати;
- l_2: фіксована кількість слів, розмір яких становить w, значення перевірки парності, що використовується в алгоритмі підпису (рис. 5).

- Keygen()
  1. Let $\mathsf{sk} = (s_i)_{i=1,\ldots,\ell}$ where the s_i are uniformly random w-bits words;
  2. For $1 \leqslant i \leqslant \ell$, $p_i \leftarrow H^{w-1}(s_i)$;
  3. *public key:* $\mathsf{pk} \leftarrow (p_1, \ldots, p_\ell)$, *private key:* sk.
- Sign(m, sk)
  1. Express m in base w: $\mathsf{m} = (\mathsf{m}_1 \mathsf{m}_2 \ldots \mathsf{m}_{\ell_1})_w$;
  2. Compute the parity-check value $C \leftarrow \sum_{i=1}^{\ell_1} (w - 1 - \mathsf{m}_i)$;
  3. Express C in base w: $C = (C_1 C_2 \ldots C_{\ell_2})_w$;
  4. $\mathbf{b} = (b_1, b_2, \ldots, b_\ell) \leftarrow (\mathsf{m}_1, \ldots, \mathsf{m}_{\ell_1}, C_1, \ldots, C_{\ell_2})$ – we will later call it the *b-vector* of m;
  5. For $1 \leqslant i \leqslant \ell$, $\sigma_i \leftarrow H^{b_i}(s_i)$;
  6. *signature:* $\boldsymbol{\sigma} \leftarrow (\sigma_1, \ldots, \sigma_\ell)$.
- Verify(m, $\boldsymbol{\sigma}$, pk)
  1. Compute the b-vector of m as in the signature algorithm (steps 1-4);
  2. Accept if and only if $\forall i \in [\![1, \ell]\!]$, $p_i = H^{w-1-b_i}(\sigma_i)$.

Рис. 5. Шаблон для схеми підпису SPHINCS+

Параметри пропонують хороший компроміс між розміром і швидкістю, і зазвичай є такими ті, що обрані в останніх конструкціях.

SPHINCS+ – це складна схема, що включає багато різних параметрів для кожної категорії безпеки. Кожен набір параметрів визначає певний компроміс між складністю різних етапів процесу підписання та перевірки й розміром остаточного підпису. Розробники SPHINCS+ розглянули широкий діапазон набору параметрів і запропонували два набори для кожної категорії безпеки. Один набір робить підписи швидшими за рахунок більших підписів, а інший набір робить підписи меншими за рахунок повільніших підписів. Хоча ці набори параметрів добре підходять для більшості загального використання SPHINCS+, можна зробити інші екстремальніші компроміси (напр., зробити підписи дуже повільними, щоб зробити підпис на пару тисяч байтів коротшим), які можуть бути чутливими в деяких випадках.

Складність SPHINCS+ є потенційною проблемою для безпеки впровадження, а також для оцінювання безпеки всієї схеми (оскільки помилку у специфікації або конструкції легше пропустити у складнішому алгоритмі). Криптографічна безпека SPHINCS+ покладається лише на безпеку використовуваних базових хеш-функцій. SPHINCS+ забезпечує успішний запасний варіант у разі непередбачених криптоаналітичних атак. Складність захисту SPHINCS+ від атак бічними каналами переважно визначається складністю захисту реалізації хешу з ключем від атак бічними каналами.

Через спосіб формування підписів SPHINCS+ генерування та перевірка ключів відбувається набагато швидше, ніж підписання. Відкриті ключі SPHINCS+ дуже короткі, але підписи SPHINCS+ досить довгі. Основною ідеєю SPHINCS+ є створення безпечного підпису, який неможливо підробити, навіть якщо той, хто атакує, отримає секретний ключ підписувача. Спосіб побудови підпису SPHINCS+ робить його дуже стійким до атак, таких як атака Гроша, і надійним для довготермінового використання (Ducas, Lepoint, & Lyubachevsky, 2024).

Наочне порівняння **характеристик алгоритмів ЕП** наведено в таблиці.

Таблиця

Характеристики алгоритмів ЕП

	CRYSTALS-Dilithium	**Falcon**	**SPHINCS+**
Механізм ЕП	Конструкція механізму ЕП Dilithium базується на підході "Fiat-Shamir з перериваннями"	Механізм Falcon є розвитком ЕП NTRU та позначається як NTRU – Falcon	SPHINCS+ використовує велику кількість хеш-функцій і дерево Горнера
Швидкодія	+++*	+++	++
Розмір ключа	++**	+	+++
Відмовостійкість	Стійкість механізму ЕП Dilithium ґрунтується на складності пошуку коротких векторів у алгебричних ґратках	Falcon розроблено з огляду на відмовостійкість і стійкість до різних типів атак, включно з квантовими атаками	SPHINCS+ має високий рівень відмовостійкості та стійкості до атак, включно з атаками Гроша та квантовими атаками

Примітки. +++*– висока швидкодія; ++ – помірна швидкодія; * – низька швидкодія; ** ++ – великі розміри ключа; ++ – помірні розміри ключа; + – невеликі розміри ключа.

Дискусія і висновки

Методи Falcon і CRYSTALS-Dilithium відомі високою швидкістю підписування і помірнішим розміром ключа, що робить їх практичними для багатьох застосувань. SPHINCS+, незважаючи на свою відмовостійкість, має меншу швидкість і вимагає більшого розміру ключа. Вибір між CRYSTALS-Dilithium, Falcon і SPHINCS+ залежатиме від конкретних потреб застосування, а також від компромісів між швидкістю, розміром ключа та відмовостійкістю. Зазвичай ці системи пропонують високу швидкість підписування, і це одна з їхніх ключових переваг. Вони призначені для використання у швидких операціях, наприклад, на серверах чи вбудованих системах. Falcon вирізняється високою швидкістю підписування та помірним розміром ключа. Цей метод підходить для застосувань, де важливо забезпечити високу продуктивність підписування. Falcon має достатню відмовостійкість і рівень

захисту від квантових атак, а також характеризується високою швидкістю підписування, схожою на Dilithium, він призначений для швидких операцій і вимагає менше часу для створення підпису.

SPHINCS+ відомий своєю високою відмовостійкістю та захистом від квантових атак. Цей метод підходить для застосувань, де відмовостійкість є першочерговою вимогою, навіть за високих витрат обчислювальних ресурсів. Зазвичай SPHINCS+ має меншу швидкість підписування та великий розмір ключа, що може бути обмеженням для деяких застосувань.

CRYSTALS-Dilithium характеризується високою швидкістю підписування та меншим розміром ключа. Цей метод підходить для застосувань, де важливі і висока швидкість підписування, і відмовостійкість. CRYSTALS-Dilithium є ефективним рішенням для багатьох застосувань, оскільки поєднує високу продуктивність і відмовостійкість. SPHINCS+ зазвичай має помірну швидкість підписування. Він вимагає значної кількості операцій для створення підпису, що робить його менш швидким порівняно з іншими методами. Зазвичай швидкість SPHINCS+ оцінюється в сотнях операцій за секунду.

Розмір ключа в CRYSTALS-Dilithium зазвичай менший порівняно з SPHINCS+, що дозволяє зберігати ключі й обробляти дані ефективніше. Розмір ключа у Falcon невеликий, що полегшує управління ключами та їхнє зберігання. SPHINCS+ вимагає великого розміру ключа, що може бути неефективним для деяких застосувань, особливо на обмежених ресурсах.

Внесок авторів: Андрій Фесенко – концептуалізація; методологія; аналіз джерел, підготування огляду літератури або теоретичних засад дослідження; Марія Мирошніченко – збір емпіричних даних та їх валідація; емпіричне дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Горбенко Ю., & Ганзя, Р. (2014). Аналіз шляхів розвитку криптографії після появи квантових комп'ютерів. *CSN*, 806. http://science.lpnu.ua/uk/csn/vsi-vypusky/nomer-806-2014/analiz-shlyahiv-rozvytku-kryptografiyi-pislya-poyavy-kvantovyh.

Горбенко, І., Качко, О., Єсіна, М., & Пономар, В. (2018). Методи, методика та результати порівняльного аналізу кандидатів на постквантовий стандарт електронного підпису. *XX Ювілейна міжнародна науково-практична конференція "Безпека інформації в інформаційно-телекомунікаційних системах"* (с. 96–97). м. Буча (Київська область), ГНЦ "Зелена Буча".

Горбенко, І., Кузнецов, О., Потій, О., Горбенко, Ю., Ганзя, Р., & Пономар, В. (2017). Модель зрілості можливостей системи кібербезпеки на об'єктах критичної інфраструктури енергетичного сектору ES-C2M2. *Кібербезпека: освіта, наука, техніка*, 2(10), 32–52.

Ducas, L., Lepoint, T., & Lyubachevsky, V. (2024). *Crystals – Dilithium: Digital Signatures from Module Lattices*. TCHES 2024 . https://cryptojedi.org/papers/dilithium- 20170617.pdf

REFERENCES

Ducas, L., Lepoint, T. & Lyubachevsky, V. (2024). *Crystals – Dilithium: Digital Signatures from Module Lattices*. TCHES 2024. https://cryptojedi.org/papers/dilithium-20170617.pdf.

Gorbenko, I., Kuznetsov, O., Potii, O., Horbenko, Yu., Ganzya, R., & Ponomar, V. (2017). Maturity model of cyber security system capabilities at critical infrastructure facilities of the energy sector ES-C2M2. *Cyber security: education, science, technology*, 2(10), 32–52 [in Ukrainian].

Horbenko, I., Kachko, O., Yesina, M., Ponomar, V. (2018). Methods, techniques and results of comparative analysis of candidates for the post-quantum electronic signature standard. *XX Jubilee International Scientific and Practical Conference "Information Security in Information and Telecommunication Systems"* (pp. 96–97). Bucha (Kyiv region), SSC "Zelena Bucha" [in Ukrainian].

Horbenko, Yu., & Ganzya, R. (2014). Analysis of the development of cryptography after the advent of quantum computers. *CSN*, 806. [in Ukrainian]. http://science.lpnu.ua/uk/csn/vsi-vypusky/nomer-806-2014/analiz-shlyahiv-rozvytku-/kryptografiyi-pislya-poyavy-kvantovyh.

Отримано редакцією журналу / Received: 12.04.24
Прорецензовано / Revised: 17.04.24
Схвалено до друку / Accepted: 13.05.24

Andrii FESENKO, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0001-5154-5324
e-mail: andrii.fesenko@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Maria MYROSHNICHENKO, Student
ORCID ID: 0009-0008-3535-661X
e-mail: mrshnchnkmaria@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

COMPARISON OF POST-QUANTUM STANDARDS AS IMPLEMENTED IN CLASSICAL ELECTRONIC SIGNATURE ALGORITHMS

Background. *The work examines the development and promotion of post-quantum standards, as well as the analysis and improvement of existing algorithms, on the basis of which the functioning of standards in the field of electronic digital signature can be based. One of the main reasons was also the migration of classical cryptography to post-quantum cryptography. The robot is aligning three popular post-quantum standards: CRYSTALS-Dilithium, Falcon and SPHINCS+. As a result of the investigation, the most optimal standards were selected before implementation of classical electronic signature schemes.*

The article is dedicated to the development and promotion of post-quantum standards in the field of electronic digital signature. It is also necessary to analyze and level up existing algorithms, on the basis of which the functioning of such standards can be based. The research is considered relevant due to the growing interest in quantum technologies and the need for secure electronic communications in the upcoming quantum world.

Methods. *Migrating classical cryptography to post-quantum cryptography. However, power is important, because the power of quantum computers can be affected by certain cryptographic algorithms. An analysis of the feasibility of transitioning to new standards and their existing security capabilities is also carried out.*

In addition, three popular post-quantum standards are being updated: CRYSTALS-Dilithium, Falcon and SPHINCS+. This allows us to determine the most optimal and reliable standard for implementation of classical electronic signature schemes. The authors of the work carry out the selection of the optimal standard, ensuring the safety and security of its authorities.

Results. *Contains important results from the study of post-quantum standards for electronic digital signatures, which may be useful for developers of cryptographic software and information security engineers.*

The power supply to the influences and changes in the advanced post-quantum standards, such as the complexity of implementation, the flexibility of infrastructure and power standardization, are thoroughly examined. The prospects for the future development of post-quantum cryptography and its influx into modern electronic signature systems have also been highlighted. This will help readers to take away the more common sense and context of the importance and potential contributions in this area.

Conclusions. *Falcon and CRYSTALS-Dilithium have a high signing fluidity and a larger key size, making them practical for rich stagnation. SPHINCS+, regardless of its viscosity, has less fluidity and requires a larger key size. The choice between CRYSTALS-Dilithium, Falcon and SPHINCS+ will depend on the specific drying needs, as well as compromises between fluidity, key size and viscosity. This demonstrates the high speed of subscription, and this is one of its key advantages. It is intended for use in quick operations, for example, on servers and industrial systems.*

Keywords: *electronic signature, post-quantum cryptography, cryptoflexibility, post-quantum standards.*

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.