УДК 004.056.55

doi.org/10.15407/fmmit2023.36.063

Методологія та механізми розробки, оцінки та порівняння міжнародних та національних постквантових стандартів асиметричних криптоперетворень

Іван Горбенко[1], Марина Єсіна[2], Володимир Пономар[3]

[1] д.т.н., професор, АТ «Інститут Інформаційних технологій» вул. Коломенська, 15, 61166, Харків, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, 61022, Харків, e-mail: i.d.gorbenko@karazin.ua
[2] к.т.н., АТ «Інститут Інформаційних технологій» вул. Коломенська, 15, 61166, Харків, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, 61022, Харків, e-mail: m.v.yesina@karazin.ua
[3] к.т.н., АТ «Інститут Інформаційних технологій» вул. Коломенська, 15, 61166, Харків, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, 61022, Харків, e-mail: laedaa@gmail.com

Наразі інтенсивно проводяться теоретичні та практичні дослідження, що пов'язані з розробкою, оцінкою, порівнянням та стандартизацією перспективних асиметричних криптографічних перетворень. Згідно існуючих поглядів, асиметричні стандарти криптографічного захисту інформації (КЗІ) повинні відповідати вимогам постквантовості, забезпечувати захист від класичних, квантових атак, а також бажано забезпечувати певний захист від атак на основі помилок та атак сторонніми каналами від порушника (криптоаналітика) 3-го рівня, для якого практично не існує матеріально-технічних та фінансових обмежень, та їх використання на практиці. Проблема постквантової стандартизації вирішується в декілька етапів: обґрунтування вимог; обґрунтування та вибір математичних методів розробки постквантових стандартів асиметричного шифрування (АСШ); протоколів інкапсуляції ключів (ПІК) та електронного підпису (ЕП). Для вирішення вказаних проблемних завдань необхідні теоретичні та практичні дослідження щодо експериментального підтвердження відповідності вимогам засобом використання комплексної методології оцінки та порівняння постквантових проєктів та стандартів АСШ, ПІК та ЕП.

Ключові слова: АСШ, ЕП, криптографічна стійкість, критерії, комплексна методологія оцінки та порівняння, методики оцінки та порівняння на основі безумовних, умовних та прагматичних критеріїв, ПІК.

Вступ. На міжнародному та національному рівнях суттєво жорсткіші вимоги висунуті стосовно безпеки інформації, техніко-економічних та техніко-експлуатаційних характеристик ІКС та інформаційних технологій (ІТ) стосовно КЗІ. На міжнародному рівні обґрунтовані та рекомендовані у якості міжнародних постквантових стандартів АСШ, ПІК та ЕП з використанням новітніх математичних методів – алгебраїчних решіток та систем із асиметричними ЕП на основі одноразових ключів. Для цього на міжнародному рівні вводяться стандарти асиметричного перетворення АСШ, ПІК Crystals-Kyber, ЕП Crystals-Dilithium, Falcon та Sphincs+. На національному рівні також проведені

дослідження та розробки з прийняттям національних постквантових асиметричних стандартів ЕП. Прийнято національний стандарт АСШ, ПІК ДСТУ 8961-2019, що ґрунтується на алгебраїчній решітці, на етапі прийняття проєкти ЕП «Вершина» та «Сокіл», що також ґрунтуються на різних алгебраїчних решітках. У цій доповіді показується, що вказані стандарти не поступаються за характеристиками та перевершують АСШ, ПІК Crystals-Kyber та ЕП Crystals-Dilithium і Falcon щодо безпеки інформації, техніко-економічних та техніко-експлуатаційних вимог, так як забезпечують захист від класичних атак включно 512 біт та квантових атак 256 біт, а вказані міжнародні – 256 біт від класичних та 128 біт від квантових атак [1-3].

1. Сутність комплексної методики оцінки та порівняння АСШ, ПІК та ЕП

Реалізація моделей безпеки для постквантового ЕП EUF-CMA (екзистенційна непідроблюваність при атаці на основі адаптивно вибраних повідомлень) та IND-CPA та IND-CCA2 стосовно протоколів АСШ та ПІК "семантично безпечного" шифрування або інкапсуляції ключів, дозволяє виконати необхідні умови їх постквантовості, а захист від класичних атак включно 512 біт та квантових атак 256 біт забезпечить достатні умови безпеки. Їх реалізація дозволяє оцінити та порівняти криптографічні примітиви АСШ, ПІК та ЕП з використанням трьох сукупностей критеріїв: безумовних, умовних та прагматичних. На першому етапі спочатку перевіряється відповідність криптопримітиву системі часткових безумовних критеріїв, а потім для кожного криптопримітиву на основі часткових обчислюється безумовний інтегральний критерій. На другому етапі отримуються відповідні оцінки з використанням спочатку системи часткових умовних критеріїв, а потім на їх основі обчислюється інтегральний умовний критерій. На третьому етапі отримуються відповідні оцінки з використанням системи прагматичних критеріїв [1].

2. Безумовні критерії оцінки та порівняння АСШ, ПІК та ЕП

Безумовним критерієм добору є логічна зміна так/ні (1/0), тому безумовний критерій можна записати у вигляді (1) [4]:

$$\left(W_{\delta 1}, W_{\delta 2}, W_{\delta 3}, W_{\delta 4}, W_{\delta 5}, W_{\delta 6}, W_{\delta 7}\right) \in (1,0) \tag{1}$$

з урахуванням наведених вище часткових безумовних критеріїв $W_{\delta 1}$–$W_{\delta 7}$ та умови (1) функція відповідності криптоперетворення може бути подана у вигляді (2) [4]:

$$f_{фв} = W_{\delta 1} \wedge W_{\delta 2} \wedge W_{\delta 3} \wedge W_{\delta 4} \wedge W_{\delta 5} \wedge W_{\delta 6} \wedge W_{\delta 7} = W_{\delta}. \tag{2}$$

Для отримання позитивного висновку щодо кожного безумовного критерію необхідно на основі моделей порушника, загроз та моделі безпеки довести, що для них можна реалізувати відповідний рівень безпеки. По суті, вирішення цієї проблеми, у загальному випадку зводиться до того, що для даних моделей (комплексної моделі) гарантовано забезпечується по кожному

безумовному критерію криптографічна стійкість від усіх класичних та квантових атак, а також забезпечується певний захист від атак на основі помилок та на основі витоку по технічним каналам.

3. Умовні критерії оцінки та порівняння АСШ, ПІК, ЕП

У якості прикладу розглядається оцінка та порівняння існуючих стандартів ЕП ДСТУ ISO/IEC 14888-3:2014 та ДСТУ 4145-2002. Порівняння алгоритмів ЕП пропонується проводити методом аналізу ієрархій. Виберемо, як умовні критерії оцінки ЕП, часткові критерії W_{y1}, $W_{y2,}$ $W_{y3.}$ $W_{y4,}$ $W_{y5,}$ $W_{y6.}$ $W_{y7,}$ W_{y8}. Порівняємо алгоритми ЕП відносно умовних критеріїв, для цього побудуємо дерево цілей, що наведено на рис. 1 [4].

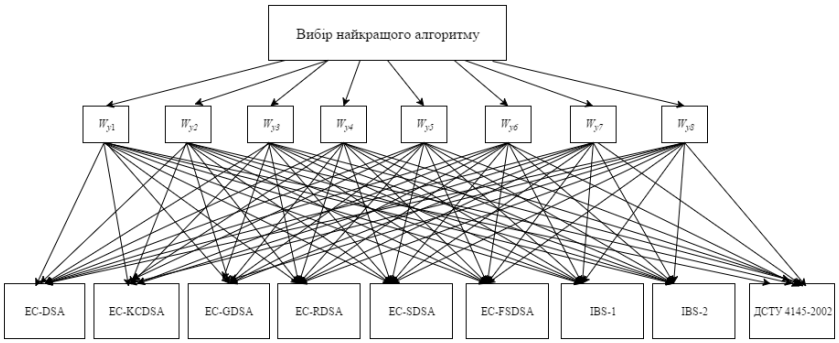

Рис. 1. Дерево цілей

4. Прагматичні критерії оцінки та порівняння АСШ та ПІК

На третьому етапі у залежності від вимог, що висуваються до криптопримітивів, при необхідності потрібно оцінювати та порівнювати альтернативні примітиви по техніко-економічним та техніко-експлуатаційним критеріям (характеристикам) У якості основних, скоріше всього, можливо використовувати такі характеристики: довжини особистих та відкритих ключів, довжини електронних підписів та довжини блоків, що шифруються, складність (швидкодія) основних – прямих та зворотних криптоперетворень, складність генерування (обчислення) ключів та параметрів, а також залежність від видів математичних методів реалізації АСШ, ПІК тощо.

У якості криптопримітивів АСШ, ПІК виберемо кандидати, що пройшли 3-й етап відбору NIST США. На цьому етапі оцінюються можливості виконання прагматичних вимог на основі використання методів – Crystals-Kyber, BIKE, Classic McEliece. Тобто визначаються прагматичні критерії вказаних АСШ, ПІК, наприклад, залежність довжини відкритого ключа від довжини особистого ключа (рис. 2). У цьому випадку, хоча в алгоритмі «Скеля» довжини ключів менші, ніж у Kyber, але залежність більш висока, в подальшому при меншому зростанні довжини особистого ключа – довжина відкритого буде зростати [1, 2].

На рис. 3 показана залежність часу шифрування від довжини відкритого ключа. Для Kyber залежність спадаюча, бо алгоритм Kyber1024 більш складний, ніж Kyber768, але при цьому має менший фінальний розмір ключів.

З рисунків видно, що в усіх оцінках крім генерації ключів, алгоритм «Скеля» має менші значення, ніж Kyber, при тому, що забезпечує той самий чи більший рівень безпеки (стійкості) [1, 2].

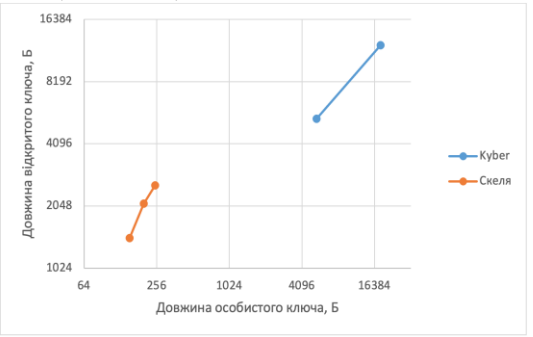

Рис. 2. Залежність довжини відкритого ключа від довжини особистого ключа

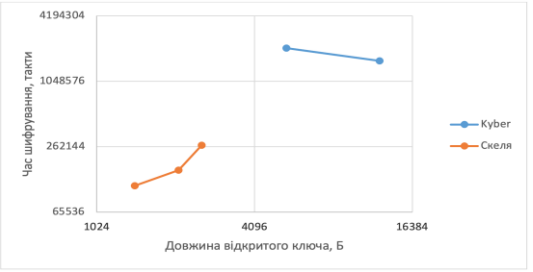

Рис. 3. Залежність часу шифрування від довжини відкритого ключа

5. Оцінка та порівняння проєктів та стандартів криптографічних перетворень типу АСШ, ПІК «Скеля» та Kyber

На рис. 4 наведено гістограму загальної відносної переваги алгоритмів АСШ. Найбільшу перевагу має алгоритм «Скеля», друге місце у SIKEp751, а серед

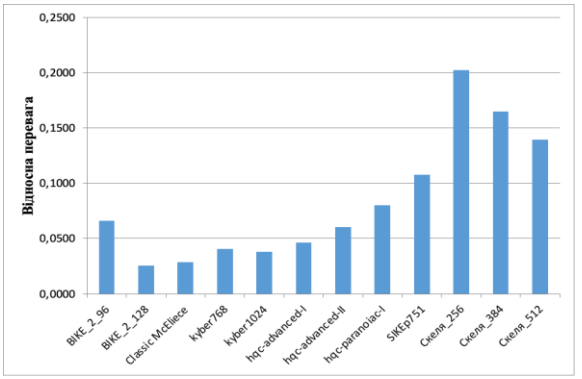

Рис. 4. Переваги алгоритмів АСШ

алгоритмів, що задовольняють високий рівень стійкості друге місце посідає HQC [1-4].

Висновки. 1. Комплексна методика аналізу існуючих та постквантових АСШ, ПІК та ЕП визначає методики оцінки та порівняння існуючих та постквантових АСШ, ПІК та ЕП на основі послідовного застосування безумовних, умовних та прагматичних критеріїв оцінки та порівняння їх якості. 2. Основним завданням комплексної методики є формалізація процесів прийняття рішень відносно виконання висунутих до них вимог АСШ, ПІК та ЕП, врахування переваг та недоліків примітивів, що є кандидатами на постквантовий стандарт. 3. Національний постквантовий стандарт АСШ, ПІК ДСТУ 8961-2019 не уступає і перевершують АСШ, ПІК Crystals-Kyber, а проєкти стандартів ЕП «Вершина» та «Сокіл» не поступаються міжнародному стандарту ЕП Crystals-Dilithium.

Література

[1] NIST IR 8413 Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process.

[2] ДСТУ 8961:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів.

[3] Crystals-Kyber: a CCA-secure module-lattice-based KEM / Leo Ducas., and other. // URL: https://eprint.iacr.org/2017/634.pdf.

[4] *Горбенко І. Д.* Методи, методика та результати порівняльного аналізу електронних підписів згідно ДСТУ ISO/IEC 14888-3:2014 / І. Д. Горбенко, М. В. Єсіна // Вісник Національного університету “Львівська політехніка”: серія “Автоматика, вимірювання та керування”. – Л. : Національний університет “Львівська політехніка”, 2016. – № 852 – С. 9–22.

Methodology and mechanisms of the development, assessment and comparison of international and national post-quantum standards

Ivan Gorbenko, Maryna Yesina, Volodymyr Ponomar

Theoretical and practical studies related to the development, evaluation, comparison and standardization of promising asymmetric cryptographic transformations are currently conducted. According to existing views, asymmetric standards of cryptographic protection of information (CPI) must meet the requirements of post -quantity, provide protection against classic, quantum attacks, it is also advisable to provide some protection against attacks and attacks by side channels from the offender (cryptoanalyst) of the 3rd level, for which there is practically no logistical and financial constraints and their use in practice. The problem of post-quantum standardization is solved in several stages: substantiation of requirements; substantiation and choice of mathematical methods of development of post-quantum standards of asymmetric encryption (AE); key encapsulation protocols (KEP) and electronic signature (ES). Theoretical and practical research is required to experiment with these problematic problems on experimental confirmation with the requirements of the use of a comprehensive assessment methodology and comparison of post-quantum drafts and standards of AE, KEP and ES.

Отримано 20.03.23