УДК 003.026:004.056
DOI: 10.32626/2308-5916.2019-19.69-74

І. С. Кудряшов*, студент,
Г. А. Малєєва,** аспірант

*Харківський національний університет імені В. Н. Каразіна, м. Харків,
**Харківський національний університет радіоелектроніки, м. Харків

АНАЛІЗ ВЛАСТИВОСТЕЙ ЕЛЕКТРОННИХ ПІДПИСІВ НА БАЗІ MQ-ПЕРЕТВОРЕНЬ

Останнім часом найбільш важливими дослідженнями у сфері криптографічного захисту інформації є дослідження, які пов'язані з можливістю використання існуючих алгоритмів у пост квантовий період, а також дослідження, які спрямовані на пошуки перспективних алгоритмів які будуть стійкими до квантових атак, а отже відповідатимуть усім вимогам пост квантового світу. Стаття присвячена аналізу алгоритмів електронного підпису на базі MQ (Multivariate Quadratic Transformations — мультиваріативні квадратичні перетворення). У статті представлена загальна схема створення електронного підпису із застосуванням мультиваріативних перетворень. Наведені результати оцінки механізмів електронного підпису відносно загальноприйнятих критеріїв. Як основні умовні критерії використані довжини ключових даних та результату криптографічного перетворення, тобто електронного підпису, а також обчислювальна ефективність створення підпису та його перевірки. Порівняння проводилося щодо електронних підписів LUOV, Gui, Rainbow, MQDSS, TPSig, DualModeMS, HiMQ-3, DME та GeMSS. Під час аналізу використана методика порівняння криптографічних механізмів на основі експертних оцінок за сукупністю умовних та безумовних критеріїв методом вагових коефіцієнтів. На основі проведених досліджень обрані найбільш перспективні кандидати на пост квантовий стандарт електронного підпису, а також запропоновані рекомендації щодо їх застосування.

Ключові слова: *асиметричний ключ, асиметричні криптоперетворення, багатовимірні перетворення, електронний підпис, квадратичні поля, постквантові електронні підписи, MQ перетворення, пост квантовий алгоритм.*

Вступ. У 2016 році Національний інститут стандартів та технологій (NIST) США оголосив конкурс на пошук нових стандартів криптографічного захисту інформації, які будуть стійкими до пост-квантових атак [1]. Доведено, що більшість існуючих криптографічних стандартів не будуть стійкими до квантових атак [2]. У зв'язку з цими фактами був оголошений конкурс NIST PQC основне завдання якого пов'язано з від-

бором алгоритмів, які планується прийняти в 2020–2022 рр. До таких віднесено стандарти електронного підпису (ЕП), стандарти направленого шифрування (НШ) та протоколи інкапсуляції ключів (ПІК).

Значна кількість механізмів запропонована на базі мультиваріативних квадратичних (MQ) перетворень — 13 з 71. На даний момент 2 кандидати відкликані, 3 кандидати атаковані, 2 з них вже запропонували шляхи усунення вразливостей. Таким чином з 13 запропонованих алгоритмів на даному етапі пропонується розглянути 9 алгоритмів електронного підпису — LUOV, Gui, Rainbow, MQDSS, TPSig, DualModeMS, HiMQ-3, DMT та GeMSS. У статті наводяться результати досліджень і порівнянь цих кандидатів відносно безумовних та умовних критеріїв та вимог технічних, техніко-економічних та техніко-експлуатаційних.

Сутність MQ-перетворень. Аналіз показує, що багатовимірна MQ криптографія ґрунтується на складності вирішення задач, що пов'язані з багатовимірними поліномами над кінцевими полями та вирішенням систем багатовимірних поліноміальних рівнянь. Основними особливостями MQ-перетворень є невеликі, у порівнянні з іншими, складність асиметричних перетворень та невеликі обчислювальні ресурси здійснення перетворень.

Детальний опис схеми електронного підпису на базі мультиваріативних перетворень описаний у [3]. У загальному випадку послідовність (схема) генерації та перевірки ЕП [4], що базується на MQ-перетвореннях, показано на рис. 1.

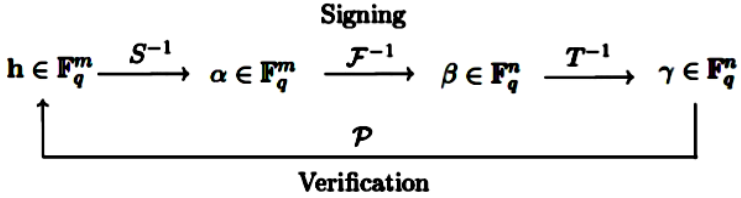

Рис. 1. *Схеми створення та перевірки підпису на основі MQ-схеми*

де $F = (F^{(1)},...,F^{(m)}) : F_q^{\,n} \to F_q^{\,m}$ — секретна система, або центральне відображення, $S : F_q^{\,m} \to F_q^{\,m}$ та $T : F_q^{\,n} \to F_q^{\,n}$ — афінні відображення, а $P = (S \circ F \circ T)$ — публічний ключ.

Опис запропонованих алгоритмів. На конкурс NIST подано 8 кандидатів, що ґрунтуються на MQ — перетвореннях — LUOV [5], Gui [6], Rainbow [7], MQDSS [8], TPSig [9], DualModeMS [10], HIMQ-3 [4], DME [11] та GeMSS [12]. Більш детально ці алгоритми розглянуті у [3].

Схема підпису LUOV [5], (автор Ward Beullens) — Lifted Unbalanced Oil and Vinegar — це просте удосконалення схеми UOV, у якому значно зменшено розмір відкритих ключів. В ній використовуєть-

ся відображення публічного ключа (lifted — означає піднесений) у розширене поле, таким чином зменшується розмір ключа. Схема LUOV може бути використана в двох режимах: класичному, та режиму з відновленням повідомлення.

Схема підпису Gui [6] (автори — Ming-Shing Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang) базується на HFEv — схемі ЕП, яку вперше запропонували Патарін, Куртуіз та Губін. В модифікованій схемі QUARTZ, як і в Gui, використовується спеціально розроблений процес вироблення ЕП за допомогою якого зменшується розмір самого підпису.

Схема підпису Rainbow [7] (автори — Ming-Shing Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang) базується на добре відомій UOV схемі, яка була запропонована ще у 1999 році. Безпосередньо ЕП Rainbow розроблено у 2005 році, останні зміни вносилися до цього механізму ще у 2008 році, у зв'язку з існуючою на той час атакою. Варто зазначити що Rainbow має найбільш привабливі показники швидкодії.

Схема підпису MQDSS [8] (автори — Ming-Shing Chen, Andreas Husing, Joost Rijneveld, Simona Samardjiska, Peter Schwabe) є схемою ЕП, що ґрунтується на застосуванні до 5-крокової схеми ідентифікації перетворення Фіата–Шаміра (Fiat-Shamir transformation, FST).

Схема підпису TPSig [9] (автори — Yossi (Joseph) Peretz, Nerya Granot) — це схема ЕП, яка базується на рішенні MQ-проблеми та проблеми NSARE (асиметричні алгебраїчні рівняння Рікатті).

Схема підпису DualModeMS [10] (автори — J.-C. Faug`ere, L. Perret, J. Ryckeghem) — A Dual Mode for Multivariate-based Signature — ЕП, основна властивість якого є те, що при його застосуванні використовуються малі за розміром публічні ключі. Цей підпис базується на HFEv схемі, з модифікацією методом SBP, який дозволяє перетворити будь-який мультиваріативний підпис на основі MI на новий підпис, але з меншим публічним ключем, та більшим підписом.

Механізм HIMQ-3 [4] (автор — Kyung-Ah Shim) — A High Speed Signature Scheme based on Multivariate Quadratic Equations — ЕП, що базується на модифікації стандартної MQ-схеми ЕП з парадигмою MQ+IP. Її сутність полягає у тому, що складність базується не тільки на вирішені MQ-проблеми, а також на проблемі невизначеності ізоморфізму поліномів (IP-problem).

Механізм DME [11] (автор — Ignacio Liengo) — a public key, signature and KEM system based on double exponentiation — ЕП, що базується на подвійному піднесенні з використанням матричних експонентів.

Механізм GeMSS [12] (автори — J.-C. Faug`ere, L. Perret, J. Ryckeghem, A. Casanova, G. Macario-Rat, J. Patarin) — Great Multivariate Signature Scheme — що має схожість з DualModeMS. Відмінність полягає у тому, що ЕП при використанні має малий розмір, водночас,

коли публічний ключ має великий розмір, а процес верифікації підпису доволі швидкий.

Аналіз механізмів відносно безумовних критеріїв. У роботі [13] проведено аналіз алгоритмів відносно безумовних критеріїв. Результати аналізу наведені у таблиці. За наведеними результатами були обрані механізми які, на наш погляд, задовольняють усім безумовним критеріям. Ця оцінка була спроектована у інтегральний безумовний критерій, який обчислюється наступним чином:

$$W_\delta = W_1 \wedge W_2 \wedge W_3 \wedge W_4 \wedge W_5 \wedge W_6 \wedge W_7$$

Якщо W_δ відповідає значенню 0, то приймається, що криптографічне перетворення не задовольняє безумовним критеріям, якщо 1 — задовольняє.

Таблиця

Результати аналізу відповідності безумовним критеріям пост-квантових перетворень типу ЕП на базі MQ-перетворень

Scheme	$W_{\delta 1}$	$W_{\delta 2}$	$W_{\delta 3}$	$W_{\delta 4}$	$W_{\delta 5}$	$W_{\delta 6}$	$W_{\delta 7}$	W_δ
TPSig	1	0	0	1	1	1	1	0
HiMQ3	1	0	0	1	1	1	1	0
DME	1	1	0	1	1	1	1	0
LUOV	1	1	1	1	1	1	1	1
GUI	1	1	1	1	1	1	1	1
Rainbow	1	1	1	1	1	1	1	1
MQDSS	1	1	1	1	1	1	1	1
DualModeMS	1	1	1	1	1	1	1	1
GeMSS	1	1	1	1	1	1	1	1

Таким чином можна зробити висновок, що на даному етапі досліджень лише 6 алгоритмів відповідають безумовним критеріям і є потенційними кандидатами на пост-квантовий стандарт ЕП.

Порівняння алгоритмів відносно умовних критеріїв. У роботах [3, 13] наведені порівняння алгоритмів відносно технічних, техніко-економічних та техніко-експлуатаційних умов їх використання. Узагальнені результати оцінок показано на рис. 2.

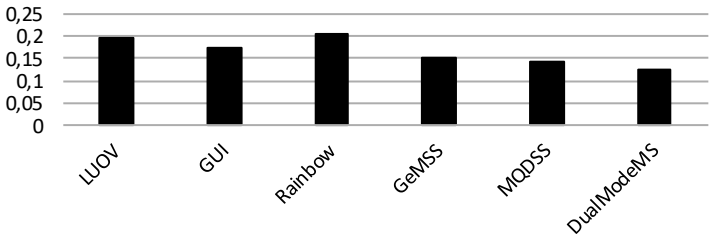

Рис. 2. *Відносна перевага алгоритмів ЕП на базі MQ перетворень*

Відповідно до рис. 2, який узагальнює дослідження [3, 13], можна стверджувати, що найбільш перспективними алгоритмами ЕП на базі MQ-перетворень є Rainbow та LUOV. Також, варто зазначити, що у 2-й раунд [14] конкурсу NIST PQC пройшли 4 з 6 алгоритмів, які задовольняють безумовним критеріям: це LUOV, Rainbow, GeMSS, та MQDSS.

Висновки. Розглянуті алгоритми електронного підпису на базі мультиваріативних квадратичних перетворень, які подані як кандидати на пост-квантовий стандарт, на конкурс NIST PQC. Представлено результат їх аналізу при застосуванні безумовних та умовних технічних, техніко-економічних та техніко-експлуатаційних критеріїв. На основі отриманих результатів можна зробити висновок, що лише 6 з 9-ти представлених механізмів на базі MQ-перетворень відповідають усім безумовним критеріям. Як показали дослідження [3, 13], з цих 6 алгоритмів найбільш перспективними, на думку авторів, є Rainbow та LUOV [3, 13]. До значимих у цьому напрямку варто віднести аналіз стійкості наведених алгоритмів від різних видів атак. Перспективність дослідницьких робіт у напрямку MQ-перетворень підтверджує той факт, що 4 з 9 механізмів електронного підпису, які пройшли у 2-й раунд конкурсу — це підписи на базі MQ-перетворень.

Список використаних джерел:

1. Post-Quantum Cryptography, Round 1 Submissions, 2017. URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.
2. Горбенко Ю. І. Методи побудування та аналізу, стандартизація та застосування криптографічних систем : монографія. Харків : Форт, 2016. 959 с.
3. Горбенко І. Д., Кудряшов І. С., Онопрієнко В. В. Порівняльний аналіз пост квантових стандартів електронного підпису на основі мультиваріативних квадратичних перетворень. *Радиотехника* : всеукр. межвед. науч.-техн. сб. Харьков : ХТУРЕ. 2018. Вып. 195. С. 46–60.
4. Kyuang-Ah Shim, Cheol-Min Park, Aeyoung Kim. HiMQ-3: A High Speed Signature Scheme based on Multivariate Quadratic Equations, NIST Submission, 2017. URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/-Round-1-Submissions.
5. Ward Beullens, Bart Preneel, Alan Szepieniec, Frederik Vercauteren. LUOV: Lifted Unbalanced Oil and Vinegar, NIST Submission, 2017. URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.
6. Jintai Ding, Ming-Shen Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang. Gui, NIST Submission, 2017. URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.
7. Jintai Ding, Ming-Shen Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang. Rainbow. NIST Submission, 2017. URL: https://csrc.nist.gov/Projects/-Post-Quantum-Cryptography/Round-1-Submissions.
8. Simona Samardjiska, Ming-Shing Chen, Andreas Hulsing, Joost Rijneveld, Peter Schwabe. MQDSS, NIST Submission, 2017. URL: https://csrc.nist.gov/-Projects/Post-Quantum-Cryptography/Round-1-Submissions.

9. Joseph Peretz, Nerya Granot. TPSig, NIST Submission, 2017. URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.
10. Faugère J.-C., Perret L., Ryckeghem J. DualModeMS: A Dual Mode for Multivariate-based Signature, NIST Submission, 2017. URL: https://csrc.nist.gov/-Projects/Post-Quantum-Cryptography/Round-1-Submissions.
11. Ignacio Luengo, Martin Avendano, Michel Marco. DME: DME a public key, signature and KEM system based on double exponentiation, NIST Submission, 2017. URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/-Round-1-Submissions. unpublished.
12. Casanova A., Faugère J.-C., Macario-Rat G., Patarin J., Perret L., Ryckeghem J. GeMSS: A Great Multivariate Short Signature, NIST Submission, 2017. URL: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.
13. Post-Quantum Cryptography, Round 2 Submissions, 2019. URL: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

ANALYSIS OF OPPORTUNITIES OF THE DS BASED ON THE MQ-TRANSFORMATION

Recently, the most critical studies in the field of cryptographic information security are studies that relate to the possibility of using existing algorithms in the post quantum period, as well as studies that seek to find promising algorithms that will be resistant to quantum attacks, and therefore meet all requirements of the post. quantum world. The paper is devoted to the analysis of MQ-based electronic signature algorithms (Multivariate Quadratic Transformations) of transformations relative to the unconditional and conditional criteria that were proposed as candidates for the post-quantum standard of the NIST PQC competition. The paper presented the general scheme of creating an electronic signature using multivariate transformations. The analysis of candidates and their peculiarities was also conducted. The results of the evaluation of the electronic signature mechanisms in relation to generally accepted unconditional criteria, as well as regarding the conditional criteria based on the techno-economic and technical-operational requirements for nominated candidates for the post-quantum standard are presented. The main conditional criteria were the lengths of key data and the result of the cryptographic transformation, that is, the electronic signature, as well as the computational efficiency of signature creation and verification. The comparison was made on the electronic signatures of LUOV, Gui, Rainbow, MQDSS, TPSig, DualModeMS, HiMQ-3, DME and GeMSS. During the analysis, the technique of comparing cryptographic mechanisms on the basis of expert evaluations using a combination of conditional and unconditional criteria by weighting coefficients method was used. On the basis of the conducted researches, the most perspective candidates for the post quantum standard of electronic signature were selected, as well as recommendations for their application were proposed.

Key words: *asymmetric key, asymmetric cryptographic transformations, multivariate transformations, digital electronic signature, quadratic fields, post-quantum electronic signatures, MQ transformation, post quantum algorithm.*

Одержано 01.02.2019