**УДК 004.056.55**

*І.Д. ГОРБЕНКО, д-р техн. наук, І.С. КУДРЯШОВ, В.В. ОНОПРІЄНКО*

# ПОРІВНЯЛЬНИЙ АНАЛІЗ ПОСТКВАНТОВИХ СТАНДАРТІВ ЕЛЕКТРОННОГО ПІДПИСУ НА ОСНОВІ МУЛЬТИВАРІАТИВНИХ КВАДРАТИЧНИХ ПЕРЕТВОРЕНЬ

## Вступ

Наприкінці 2016 року NIST (Національний інститут стандартів та технології) США оголосив конкурс на нові стандарти постквантової асиметричної криптографії [1]. До таких систем належать, зокрема, механізми електронного підпису(ЕП), направленого шифрування(НШ) та протоколи інкапсуляції ключів(ПІК). Значне число кандидатів на ЕП розроблено на основі застосування мультиваріативних квадратичних перетворень (Multivariate Quadratic Transformations, MQ-transformations) [3 – 10]. Механізми MQ-перетворень дозволяють забезпечити необхідні рівні стійкості, швидкодію та застосування в малоресурсних системах. Такі властивості MQ-перетворень мають суттєве значення для практичних додатків, тому їх аналіз та порівняння є важливою проблемною задачею, тим більше, що вона вирішується NIST США на міжнародному рівні.

Метою статі є розгляд та аналіз механізмів електронного підпису, які були запропоновані на конкурс NIST PQC, а також порівняння їх властивостей згідно з вимогами NISN щодо технічних, техніко-економічних та техніко-експлуатаційних.

У роботі розглянуті 8 з 9 MQ-схем, а саме: LUOV [3], Gui [4], Rainbow [5], MQDSS [6], TPSig [7], DualModeMS [8], HiMQ-3 [9] та GeMSS [10]. Для первинної оцінки криптографічної стійкості було проведено аналіз відповідності алгоритмів ЕП вимогам до криптосистем з відкритим ключем, а саме – до забезпечення захищеності від підробки [11, 12]. Сутність такої захищеності зведена до оцінки захищеності до атак на основі адаптивного підбору повідомлень (UF-CMA)[12] та стійкості від екзестенційної підробки з адаптивним підбором повідомлень (EUF-CMA).

При описі вимог до алгоритмів-кандидатів конкурсу були визначені такі рівні криптографічної стійкості, що визначені в [1, 2]:

Рівень 1: коли атака, яка зламує EUF-CMA-стійкий алгоритм, повинна вимагати для своєї реалізації пошуку ключа аналогічно AES-128; рівень 2 – потребує пошуку колізії для 256-бітної геш-функції аналогічно SHA256/SHA3-256; рівень 3 – аналогічний пошук ключа AES-192; рівень 4 – пошук колізії для 256-бітної геш-функції, наприклад SHA384/SHA3-384; рівень 5: коли атака на EUF-CMA-стійкий алгоритм ЕП вимагає обчислювальних ресурсів, аналогічних пошуку ключа AES-256.

Ми висуваєм також перспективні вимоги забезпечення 6 та 7 рівнів безпеки, маючи на увазі забезпечення 364 та 512 біт класичної та відповідно 192 та 256 біт квантової безпеки.

Проведений аналіз показників має початковий характер. Усі результати показників були отримані експериментальним шляхом засобом программного моделювання. Але уже на початковому етапі досліджень визначені основні проблеми, що повязані зі складністю та вартістю у широкому змісті – як вартості застосування, так і вартості криптоаналізу, так як ці характеристики є антагоністичними. Зменшення розмірів параметрів та ключів дозволяє зменшити складність криптографічних перетворень, але при цьому, як правило, зменшується складність криптоаналізу. Тому, уже на цьому етапі досліджень проекту NIST постала проблема мінімізації вартості асиметричних криптоперетворень типу АСШ, ЕП та ПІК. Тому будемо розглядати і цю проблему, по аналогії, як безумовну при дослідженні.

## 1. Сутність та загальна характеристика MQ-механізмів

Серед кандидатів на асиметричні перетворення типу АСШ, ЕП та ПІК 10 пропозицій грунтуються на механізмах багатовимірних 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, ключі, складність асиметричних перетворень та невеликі обчислювальні ресурси здійснення перетворень. Як наслідок, вказане дозволяє реалізувати MQ-перетворення у відносно простих засобах ЕП.

Розглянемо сутність MQ-перетворенння. Нехай $\mathrm{F}_q$ є скінченне поле з $q$ елементами. Також, нехай система мультиваріативних квадратичних поліномів $P=(P^{(1)},...,P^{(m)})$, з $m$ рівняннями та $n$ змінними визначена як:

$$P^{(k)}(x_1,...,x_n)=\sum_{i=1}^{n}\sum_{j=1}^{n}\gamma_{ij}^{(k)}x_ix_j+\sum_{i=1}^{n}\beta_i^{(k)}x_i+\alpha_0^{(k)},$$
$$k=1...m,\gamma_{ij}^{(k)},\beta_i^{(k)},\alpha_0^{(k)}\in \mathrm{F}_q \qquad (1)$$

Основна ідея для конструкції MQ-схем полягає у тому, що необхідно обрати **секретну** систему $F=(F^{(1)},...,F^{(m)}):\mathrm{F}_q^n\to\mathrm{F}_q^m$ (так зване центральне відображення), яка складається з $m$ мультиваріативних квадратичних поліномів, $n$ змінних, яка може бути інвертована з поліноміальною складністю.

Для того щоб сховати структуру центрального відображення $F$ у публічному ключі, необхідно обрати два афінних лінійних відображення $S:\mathrm{F}_q^m\to\mathrm{F}_q^m$ та $T:\mathrm{F}_q^n\to\mathrm{F}_q^n$. В якості публічного ключа використовується композиція квадратичних відображень $P=S\circ F\circ T$, яку важко відрізнити від випадкової системи і, тому складно інвертувати. В якості приватного ключа використовується сукупність відображень $(S,F,T)$, при знанні яких можна інвертувати публічний ключ $P$.

Послідовність (схема) генерації та перевірки ЕП [9], що базується на MQ-перетвореннях, наведено на рис. 1.

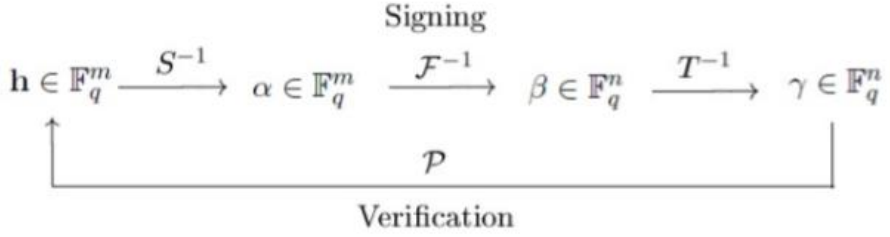


Рис. 1. Схеми вироблення та перевірки ЕП на основі MQ-схеми

## 2. Характеристика та властивості відомих механізмів ЕП

На конкурс NIST було подано вісім кандидатів, що грунтуються на MQ-перетвореннях – **LUOV** [3], **Gui** [4] , **Rainbow** [5], **MQDSS** [6], **TPSig** [7], **DualModeMS** [8] , **HIMQ-3** [9] та **GeMSS** [10] . Розглянемо їх та виберемо параметри, що необхідні для порівняння.

**Механізм (схема) LUOV** [3] (автор Ward Beullens) – Lifted Unbalanced Oil and Vinegar – є простим удосконаленням схеми UOV, у якому значно зменшено розмір відкритих ключів. Схема ЕП Unbalanced Oil and Vinegar (UOV) є однією з найстаріших і найкраще вивчених криптосистем. Схема UOV дуже проста. Має невеликі розміри ЕП та є достатньо швидкою. Основним недоліком UOV є те, що в ній відкриті ключі досить великі. В ній використовується операція піднесення публічного ключа (lifted – означає піднесений) до розширення поля таким чином, щоб зменшити розмір ключа. Схема LUOV може бути використана в двох режимах. Звичайний режим ЕП, в якому повідомлення аутентифікуються шляхом безпосередньо додавання ЕП. Іншим є режим відновлення повідомлень, який

дозволяє зменшити розміри ЕП та повідомлення. Причому, у режимі відновлення повідомлення частина повідомлення не передається, вона може бути відновлена безпосередньо на основі ЕП. Автори представили шість різних модифікацій схем ЕП, які, використовуючи відповідні параметри, реалізують 2, 4, та 5 рівні захисту. До особливостей запропонованих модифікації необхідно віднести можливості зменшення розміру ЕП та публічного ключа. Це досягається за рахунок зміни степеня розширення поля, коли чим менший степінь, тим більше розмір публічного ключа, а ЕП менші. Причому розмір секретного ключа залишається незмінним. Модель EUF-CMA безпеки в схемі LUOV гарантується за рахунок використання для реалізації механізму ЕП схеми UOV.

**Механізм (схема) Gui** [4] (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, що дозволяє зменшити порівняно з оригінальним дизайном HFEv розміри ЕП. В Gui застосовується інший підхід. Він зводиться до зниження степені поліномів HFE та одночасно зменшенні числа рівнянь та змінних vigenar. Вказане дозволяє різко прискорити процес розробки (створення) схеми ЕП без послаблення його безпеки. Але стандартна схема Gui гарантує лише універсальну непідробність. Для того щоб отримати EUF-CMA захист, необхідно ввести деякі додаткові перетворення. При цьому основна різниця полягає у тому, що необхідно використовувати випадковий бінарний вектор $r$, або так звану сіль. Крім того, замість генерації ЕП для ґеш-значення $h = H(d)$, ЕП виробляється для $H(H(d) \| r)$. Результатом ЕП є значення, $\sigma^* = (\sigma, r)$, де $\sigma$ – це стандартний підпис Gui. Щодо нього гарантується, що зловмисник не може підробити пару ґеш-підписів [4]. У цілому на конкурс було представлено три модифікації Gui-184, Gui-312, та Gui-448, з відповідними параметрами, які забезпечують 1, 3, та 5 рівні захисту, як і у HFEv.

**Механізм ЕП Rainbow** [5] (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 було створено у 2005 році та дороблено для захисту від знайденої атаки у 2008 році засобом зміни параметрів. Стандартна схема Rainbow надає лише універсальну непідробність. Для того, щоб отримати EUF-CMA захист, необхідно ввести параметри, що схожі з Gui перетворення. В Rainbow запропоновано найбільшу кількість модифікацій алгоритму – всього 9. Показано, що запропоновані варіанти параметрів відповідають, вірніше забезпечують 1, 3, 4 та 5 рівні захисту.

**Механізм MQDSS** [6] (автори – Ming-Shing Chen, Andreas Husing, Joost Rijneveld, Simona Samardjiska, Peter Schwabe) є механізмом ЕП, що грунтується на мультваріативних квадратичних перетвореннях. Механізм розроблений шляхом застосування до 5-крокової схеми ідентифікації перетворення Фіата-Шаміра (Fiat-Shamir transformation, FST). Якщо застосувати щодо схеми ідентифікації з $2q+1$ кроками схему FST, то отримаємо схему ЕП MQDSS. Вона адаптована до вирішення MQ-проблеми. Алгоритм генерації ключа MQDSS-q-n формально відповідає MQ. Доказ EUF-CMA безпеки ґрунтується на доказі безпеки будь-якої схеми, до якої було застосовано у FST (детальніше у [6]). Всього було запропоновано 15 варіацій схеми, але експериментальні дослідження показників виконані лише для двох схем: MQDSS-31-48 та MQDSS-31-64. Вони забезпечують тільки 2 та 4 рівні захисту відповідно. Необхідно відмітити, що ця схема має найменшу обчислювальну складність генерації ключової пари.

**Механізм TPSig** [7] (автори – Yossi (Joseph) Peretz, Nerya Granot) – є схемою ЕП, що базується на рішенні MQ-проблеми та проблеми NSARE(Асиметричні Алгебраїчні Рівняння Рікатті). Ця схема вже відхилена на конкурсі через те, що складність встановлення секретного ключа з підпису була лінійною. Схема **TPSig** має 2 модифікації для 1 та 5 рівнів захисту відповідно.

**Механізм DualModeMS** [8] (автори – J.-C. Faug`ere, L. Perret, J. Ryckeghem) – A Dual Mode for Multivariate-based Signature – є ЕП на основі мультиваріативних перетворень з

доволі нестандартною властивістю. Властивість ця полягає у тому, що публічний ключ має дуже маленький розмір, у той час коли сам підпис є великим. Цей підпис базується на HFEv схемі, яка модифікується за допомогою методу SBP, що дозволяє перетворити будь-який мультиваріативний підпис на основі MI на новий підпис, але з меншим публічним ключем, та більшим підписом. Таким чином, цей механізм поділяється на дві модифікації. На першому рівні (внутрішньому) – Inner.DualModeMs – рівні здійснюється ЕП, який базується на HFEv схемі, а на другому(зовнішньому) виконуються операції методу SBP. Цей підпис свого роду є підписом GeMSS з перетворенням SBP [11]. При використанні механізму забезпечується модель EUF-CMA захисту. Він грунтується на HFEv схемі, як на внутрішньому рівні так і на зовнішньому. Всього запропоновано три модифікації алгоритму: DualModeMS128, DualModeMS192, DualModeMS256, які повинні забезпечувати 1, 3, та 5 рівні безпеки відповідно. Для кожної з цих модифікацій наведено вхідні параметри системи, але показники щодо розміру ключів, ЕП та обчислювальної ефективності наведені лише для варіанту DualModeMS128.

**Механізм HIMQ-3** [9] (автор – Kyung-Ah Shim ) – A High Speed Signature Scheme based on Multivariate Quadratic Equations – є ЕП, що базується на модифікації стандартної MQ-схеми ЕП з парадигмою MQ+IP. Її сутність полягає у тому, що складність базується не тільки на вирішенні MQ-проблеми, а також на проблемі невизначеності ізоморфізму поліномів (IP-problem). В механізмі при виробленні ЕП, спочатку необхідно ввести деякі модифікації центрального відображення. Математичний доказ EUF-CMA було представлено у поданій на конкурс документації. Існують дві модифікації ЕП HiMQ-3 та HiMQ-3F, обидві забезпечують перший рівень захисту, і, мабуть, їх можна використовувати у смарт-картках.

**Механізм GeMSS** [10] (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 в тому, що ЕП при використанні має малий розмір, в той час, коли публічний ключ має великий розмір, а процес верифікації ЕП доволі швидкий. Цей ЕП базується на HFEv-схемі, оскільки HFE схема є доволі дослідженою в мультиваріативній криптографії. По суті GeMSS походить від QUARTZ, але має більш швидкі алгоритми, разом з тим ЕП є більш захищеним. Ця схема має три модифікації – GeMSS128, GeMSS192, GeMSS256 алгоритми. Для кожної модифікації визначені відповідні параметри, при застосуванні яких забезпечують 1, 3, 5 рівні захисту відповідно. Відмінність м**еханізму GeMSS** від ЕПА DualModeMS в тому, що він має відносно малі розміри відкритого ключа, але великі розміри ЕП. В той же час в механізмі модель EUF-CMA забезпечується за рахунок використаної схеми HFEv.

### 3. Порівняльний аналіз розміру ключів та підпису

Проведений аналіз дозволив визначити розміри публічного та секретного ключів та ЕП відповідно до вказаних авторами даних. В табл. 1 наведені модифікації різних алгоритмів, їх відповідний рівень безпеки, розміри ключів та ЕП. Для зручності порівнювальні характеристики були нормовані в вигляді байтів.

Так як значення параметрів відрізняються на декілька порядків, для більшої зручності на рис. 1 – 4 довжини ключових даних та ЕП наведені у логарифмічному масштабі. Сутність такого методу полягає в перетворенні величин даних наступним чином: $n = \log_{10} N$, де $N$ – початкове значення, тобто довжини публічного та секретного ключів, а також ЕП, які підлягають масштабуванню, причому $n$ є результатом обчислення десяткового логарифму над значенням, яке підлягає масштабуванню.

Слід зазначити, що дані наведені у гістограмах, відповідають усім вказаним вище варіаціям, та вони є впорядковані за зменшенням довжини. Відповідно до вимог системи, яка буде використовувати механізми ЕП, якщо зафіксувати рівень захисту, будуть змінюватися переваги на користь використання меншого публічного ключа, або секретного ключа. Так,

наприклад, у малоресурсних системах переважними будуть алгоритми, які використовують менші розміри ключових даних.

Таблиця 1

Характеристика основних криптографічних параметрів (у байтах)

| № | Схема | Модифікація | Рівень захисту | Розмір публічного ключа | Розмір секретного ключа | Розмір підпису |
|---|---|---|---|---|---|---|
| 1 | LUOV | LUOV-8-63-256 | 2 | 15,872 | 32 | 319 |
| | | LUOV-8-90-351 | 4 | 46,080 | 32 | 441 |
| | | LUOV-8-117-404 | 5 | 100,967 | 32 | 521 |
| | | LUOV-48-49-242 | 2 | 7,476 | 32 | 1,741 |
| | | LUOV-64-68-330 | 4 | 19,968 | 32 | 3,175 |
| | | LUOV-80-86-399 | 5 | 40,244 | 32 | 4,813 |
| 2 | GUI | Gui-184 | 1 | 426,292 | 19,559 | 45 |
| | | Gui-312 | 3 | 2,002,023 | 60,724 | 63 |
| | | Gui-448 | 5 | 5,928,141 | 159,642 | 83 |
| 3 | Rainbow | Ia | 1 | 152,064 | 100,250 | 64 |
| | | Ib | 1 | 151,860 | 106,189 | 78 |
| | | Ic | 1 | 192,205 | 143,360 | 104 |
| | | IIIb | 3 | 524,391 | 380,314 | 112 |
| | | IIIc | 3 | 720,794 | 538,112 | 156 |
| | | IVa | 4 | 565,453 | 376,116 | 92 |
| | | Vc | 5 | 1,723,700 | 1,274,266 | 204 |
| | | VIa | 5 | 1,351,373 | 892,109 | 118 |
| | | VIb | 5 | 1,352,704 | 944,538 | 147 |
| 4 | MQDSS | MQDSS-31-48 | 2 | 62 | 32 | 32,882 |
| | | MQDSS-31-64 | 4 | 88 | 48 | 67,800 |
| 5 | TPSig | TPSig-1 | 1 | 86,324 | 973 | 84,224 |
| | | TPSig-2 | 5 | 266,240 | 1,690 | 512 |
| 6 | DualMo-deMS | DualModeMS128 | 1 | 528 | 18,038,184 | 32,640 |
| 7 | HiMQ-3 | HiMQ-3 | 1 | 128,744 | 12,074 | 75 |
| | | HiMQ-3F | 1 | 100,878 | 14,878 | 67 |
| 8 | GeMSS | GeMSS128 | 1 | 417,408 | 14,208 | 48 |
| | | GeMSS192 | 3 | 1,304,192 | 39,440 | 88 |
| | | GeMSS256 | 5 | 3,603,792 | 82,056 | 104 |

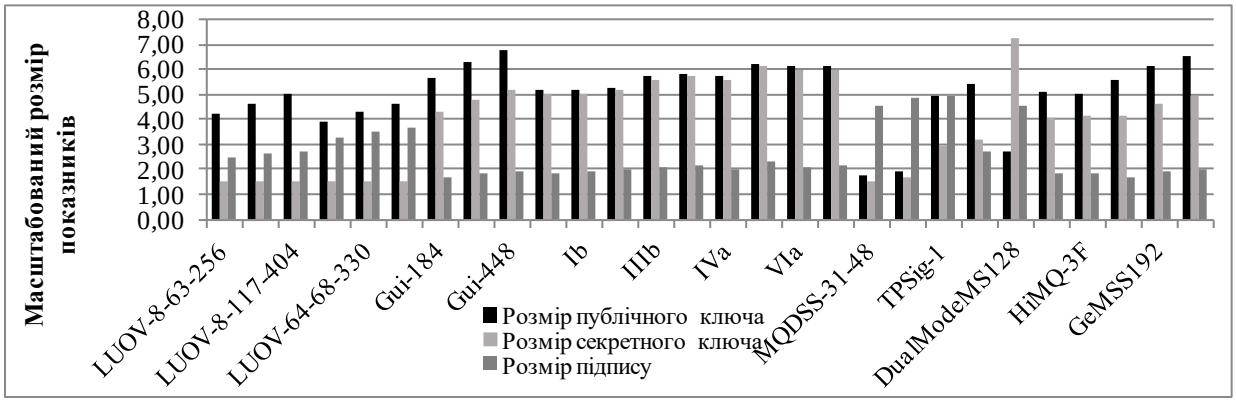


Рис. 2. Зведена гістограма показників розмірів ключових даних та ЕП
(байтів у логарифмічному масштабі)


Рис. 3. Гістограма порівнювального аналізу показників розміру публічного ключа
(байтів у логарифмічному масштабі) для ЕП


Рис. 4. Гістограма порівнювального аналізу показників розміру секретного ключа
(байтів у логарифмічному масштабі) для ЕП

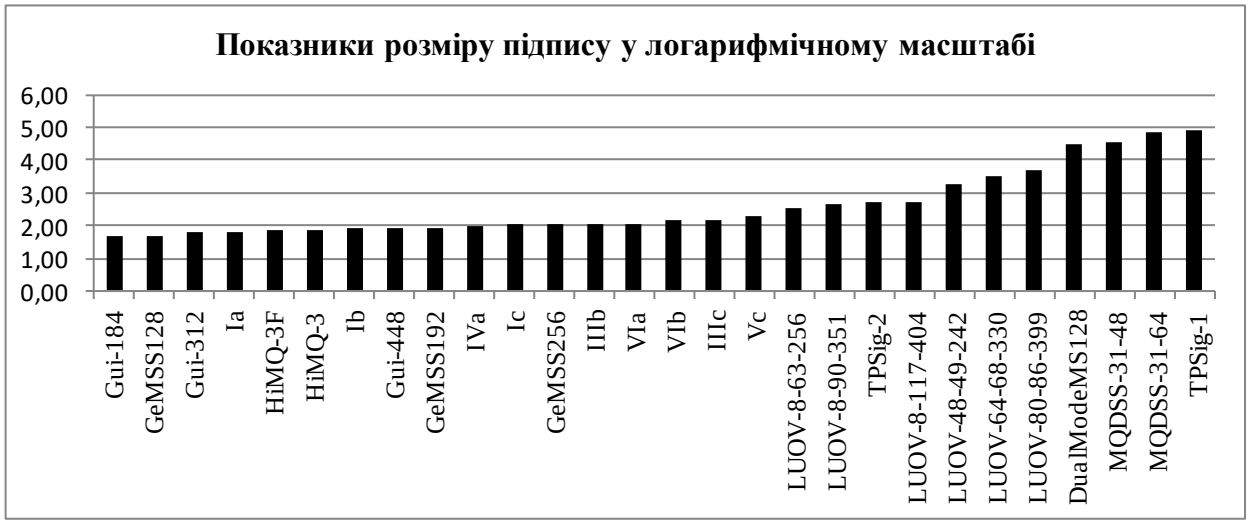


Рис. 5. Гістограма порівнювального аналізу показників розміру підпису (байтів у логарифмічному масштабі) для ЕП

Відповідно до даних, які показані на рис. 2, можна зробити висновок, що найменші довжини публічного ключа має MQDSS. В одній модифікації алгоритму – 62 байти (для рівня захисту 2), у другій – 88 (рівень захисту 4). Найбільші довжини публічного ключа мають Gui та GeMSS для рівня захисту 5 (для Gui також рівень захисту 3) – 5,928,141 байтів для Gui-448, 3,603,792 байтів для GeMSS256, та 2,002,023 для Gui-312. Також відносно малі довжини публічного ключа мають модифікації алгоритму LUOV для усіх представлених рівнів захисту. Усі інші представники мають приблизно рівні показники відповідно до забезпечених рівнів захисту.

Порівняльний аналіз для секретних (або приватних) ключів (рис. 3) показав, що серед представлених кандидатів найменші показники характерні для схеми підпису LUOV та MQDSS – в обох випадках по 32 байти. Однак слід зазначити, що LUOV реалізує 2, 4 та 5 рівні захисту, у той час, коли MQDSS має такий розмір лише для захисту рівня 1. Найбільші розміри секретних ключів мають DualModeMS та Rainbow схеми 18,038,184 та 1,274,266 байтів відповідно. Інші алгоритми мають приблизно однакові показники відповідно до реалізованих рівнів захисту.

Варто зауважити, що для усіх алгоритмів розміри підпису не перебільшують 100,000 байтів. Найменші показники відповідно до рівнів захисту мають Gui, GeMSS, та Rainbow, 45-83, 48-104, та 64-204 байти відповідно. При цьому вони можуть реалізовувати найвищий ступінь захисту. Найбільші розміри ЕП мають TpSig, DualModeMS та MQDSS, хоча ці показники відповідають рівням захисту 1 та 2. Відносно малі показники розміру підпису має також HiMQ-3, а LUOV розташувався посередині, хоча розмір підписів цього алгоритму значно перевищує лідерів у цьому показнику.

### 4. Порівняльний аналіз показників швидкодії

Оцінка показників швидкодії алгоритмів ЕП проведена авторами на різних обчислювальних платформах та представлена у табл. 2. Така оцінка наведена у циклах процесору, які необхідні для виконання операцій генерації ключової пари, створення ЕП, та його верифікації. Варто зазначити, що показники були отримані в процесі виконання алгоритмів без використання технологій оптимізації продуктивності. Деякі показники були вказані у мілісекундах та секундах, витрачених на виконання тієї чи іншої операції на зазначених обчислювальних платформах. Для того щоб проаналізувати обчислювальну ефективність алгоритмів, такі результати були переведені у кількість затрачених циклів процесору, визначену виходячи з характеристик обчислювальної платформи.

Така оцінка може дозволити провести порівняльний аналіз, не беручи до уваги обчислювальне середовище, з іншого боку вона носить лише первинний ознайомчий характер обчислювальної ефективності наведених вище алгоритмів.

Таблиця 2

Показники обчислювальної ефективності алгоритмів електронного підпису
(данні таблиці наведені у циклах процесору, які необхідно виконати для проведення кожної операції)

| № | Схема | Модифікація | Генерація ключової пари | Вироблення ЕП | Перевірка ЕП |
|---|---|---|---|---|---|
| 1 | LUOV | LUOV-8-63-256 | 39,421,493 | 26,714,796 | 15,123,202 |
| | | LUOV-8-90-351 | 154,498,995 | 81,889,845 | 49,173,941 |
| | | LUOV-8-117-404 | 276,912,036 | 144,203,736 | 84,564,465 |
| | | LUOV-48-49-242 | 27,419,223 | 88,046,948 | 50,301,626 |
| | | LUOV-64-68-330 | 90,548,276 | 259,662,473 | 125,317,813 |
| | | LUOV-80-86-399 | 192,475,607 | 595,199,427 | 273,408,571 |
| 2 | GUI | Gui-184 | 2,408,000,000 | 1,910,000,000 | 252,517 |
| | | Gui-312 | 43,817,000,000 | 25,436,000,000 | 724,044 |
| | | Gui-448 | 239,502,000,000 | 872,949,000,000 | 2,004,155 |
| 3 | Rainbow | Ia | 1,302,000,000 | 601,000 | 350,000 |
| | | Ib | 4,578,000,000 | 2,044,000 | 1,944,000 |
| | | Ic | 4,089,000,000 | 1,521,000 | 939,000 |
| | | IIIb | 26,172,000,000 | 5,471,000 | 4,908,000 |
| | | IIIc | 31,612,000,000 | 4,047,000 | 2,974,000 |
| | | IVa | 11,176,000,000 | 1,823,000 | 1,241,000 |
| | | Vc | 116,046,000,000 | 8,688,000 | 6,174,000 |
| | | VIa | 45,064,000,000 | 3,916,000 | 2,897,000 |
| | | VIb | 164,689,000,000 | 16,755,000 | 11,224,000 |
| 4 | MQDSS | MQDSS-31-48 | 2,957,276 | 266,840,340 | 191,666,288 |
| | | MQDSS-31-64 | 6,680,606 | 776,183,461 | 571,665,382 |
| 5 | TPSig | TPSig-1 | 212,676,920 | 864,000 | 1,387,800 |
| | | TPSig-2 | 302,400,000 | 1,228,500 | 2,160,000 |
| 6 | DualMo-deMS | DualModeMS128 | 2,072,200,000,000 | 6,006,000,000 | 6,994,000 |
| № | Схема | Модифікація | Генерація ключової пари | Створення підпису | Перевірка підпису |
| 7 | HiMQ-3 | HiMQ-3 | 157,899,562 | 321,443 | 614,735 |
| | | HiMQ-3F | 232,452,977 | 162,823 | 527,330 |
| 8 | GeMSS | GeMSS128 | 1,398,800,000 | 3,172,000,000 | 19,656,000 |
| | | GeMSS192 | 6,422,000,000 | 7,904,000,000 | 65,494,000 |
| | | GeMSS256 | 18,174,000,000 | 12,740,000,000 | 160,420,000 |

На рис. 5 – 8 наведені гістограми швидкодії для усіх модифікацій алгоритмів. Найменша кількість циклів, затрачених на виконання операцій, є більш кращим показником. Якщо кількість циклів має більше значення – це означає, що виконання операції займає багато часу і потребує більш потужної обчислювальної платформи.

На рис. 5 наведено зведену гістограму усіх показників швидкодії, яка показує загальне співвідношення ефективності обчислення кожної з трьох операцій (формування ключових даних, вироблення та перевірка ЕП) для кожної з наведених варіацій. Усі дані наведено у кількості циклів процесору, які необхідно використати при виконанні тієї чи іншої операції.

Майже однакову швидкість виконання всіх операцій має алгоритм LUOV. Невелика різниця між трьома операціями також є у GeMSS, MQDSS, та TPSig які мають невеликі аномалії у процесі перевірки підпису для першого кандидату, та генерації ключової пари для двох останніх. Суттєво більше часу на генерацію ключової пари вимагає Rainbow, хоча він

виконує операції з ЕП значно швидше більшості алгоритмів. Gui вимагає малих затрат на перевірку підпису, проте для створення підпису і ключової пари навпаки – великих.

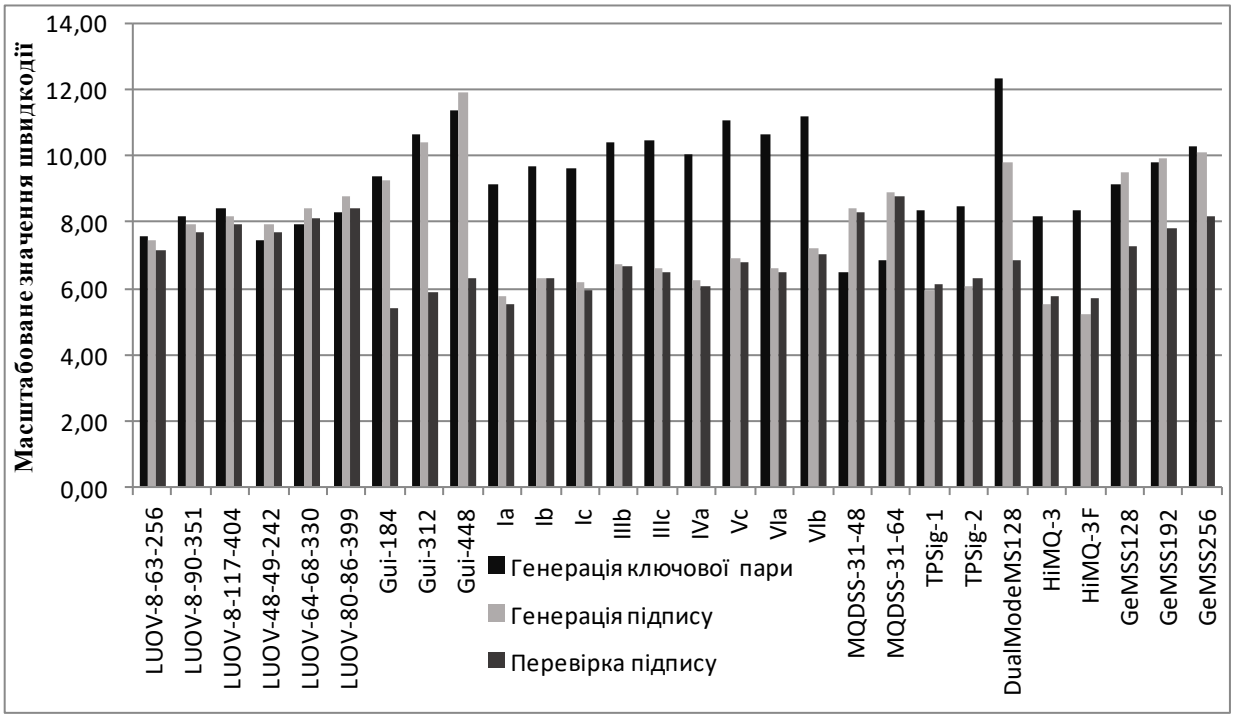


Рис. 6. Зведена гістограма показників швидкодії (циклів у логарифмічному масштабі)

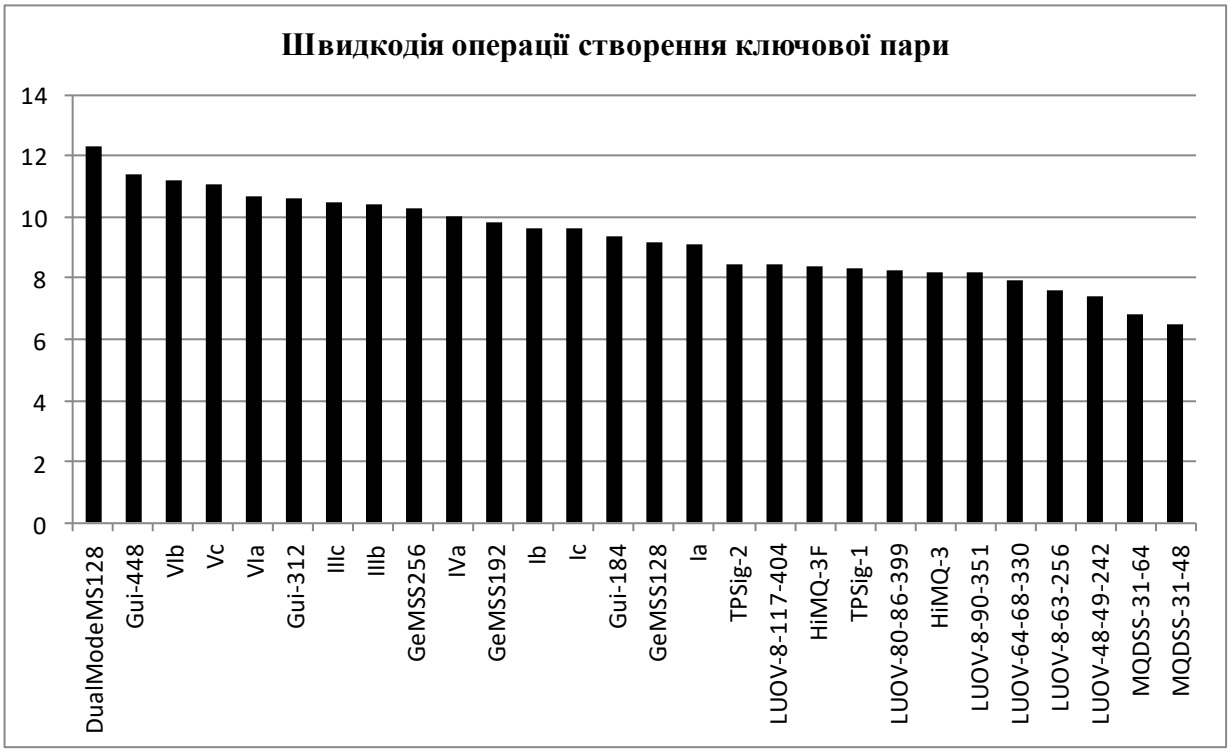


Рис. 7. Гістограма порівнювального аналізу показників швидкодії операції створення ключової пари (циклів у логарифмічному масштабі) для алгоритмів електронного підпису


Рис. 8. Гістограма порівнювального аналізу показників швидкодії операції генерації підпису (циклів у логарифмічному масштабі) для алгоритмів електронного підпису


Рис. 9. Гістограма порівнювального аналізу показників швидкодії операції перевірки підпису (циклів у логарифмічному масштабі) для алгоритмів електронного підпису

Оцінка швидкості операції створення ключової пари (рис. 6) показала, що найшвидшими схемами є MQDSS та LUOV, у той час, коли DualModeMS демонструє найгірші показники через додаткове SBP перетворення. Варто зазначити, що MQDSS та LUOV мають також і малі розміри ключових даних, а DualModeMS навпаки має великий розмір секретного ключа, який отримується шляхом «перенесення» ключових даних з публічного ключа до секретного.

Гістограма аналізу швидкодії операції вироблення ЕП вказує на те, що найшвидшим є HiMQ-3, але він реалізує лише 1 рівень захисту. Середні показники демонструє LUOV, а найгіршими за показником швидкодії створення ЕП є Gui та GeMSS.

Показники швидкодії операції перевірки ЕП демонструють такі результати: швидкими є Gui, Rainbow, та HiMQ-3 (що характерно, тому що HiMQ-3, як вже зазначалось, реалізує лише 1 рівень захисту), повільними є MQDSS, LUOV та GeMSS.

## 5. Обгрунтування вибору перспективних алгоритмів

Усі отримані результати узагальнені для кожного показника та наведені в табл. 3.

Таблиця 3

Показники зайнятих місць, відповідно до зазначених показників, модифікацій схем ЕП на основі MQ-перетворень

| Модифікація | Розмір публічного ключа | Розмір секретного ключа | Розмір підпису | Створення ключової пари | Створення підпису | Перевірка підпису | Сума |
|---|---|---|---|---|---|---|---|
| HiMQ-3 | 12 | 11 | 6 | 7 | 2 | 4 | 42 |
| HiMQ-3F | 11 | 13 | 5 | 10 | 1 | 3 | 43 |
| Ia | 13 | 18 | 4 | 13 | 3 | 2 | 53 |
| LUOV-8-63-256 | 5 | 1 | 18 | 4 | 14 | 18 | 60 |
| TPSig-1 | 9 | 9 | 28 | 9 | 4 | 8 | 67 |
| LUOV-8-90-351 | 8 | 2 | 19 | 6 | 15 | 20 | 70 |
| LUOV-48-49-242 | 4 | 4 | 22 | 3 | 16 | 21 | 70 |
| Gui-184 | 18 | 14 | 1 | 15 | 22 | 1 | 71 |
| Ib | 14 | 19 | 7 | 17 | 8 | 9 | 74 |
| TPSig-2 | 16 | 10 | 20 | 12 | 5 | 11 | 74 |
| Ic | 15 | 20 | 11 | 16 | 6 | 6 | 74 |
| LUOV-64-68-330 | 6 | 5 | 23 | 5 | 18 | 24 | 81 |
| MQDSS-31-48 | 2 | 7 | 26 | 1 | 19 | 26 | 81 |
| LUOV-8-117-404 | 10 | 3 | 21 | 11 | 17 | 23 | 85 |
| IVa | 20 | 23 | 10 | 19 | 7 | 7 | 86 |
| MQDSS-31-64 | 1 | 8 | 27 | 2 | 21 | 28 | 87 |
| GeMSS128 | 17 | 12 | 2 | 14 | 23 | 19 | 87 |
| LUOV-80-86-399 | 7 | 6 | 24 | 8 | 20 | 27 | 92 |
| Gui-312 | 26 | 16 | 3 | 23 | 27 | 5 | 100 |
| IIIb | 19 | 22 | 13 | 21 | 11 | 14 | 100 |
| IIIc | 21 | 24 | 16 | 22 | 10 | 13 | 106 |
| VIa | 23 | 25 | 14 | 24 | 9 | 12 | 107 |
| GeMSS192 | 22 | 15 | 9 | 18 | 25 | 22 | 111 |
| Vc | 25 | 27 | 17 | 25 | 12 | 15 | 121 |
| VIb | 24 | 26 | 15 | 26 | 13 | 17 | 121 |
| Gui-448 | 28 | 21 | 8 | 27 | 28 | 10 | 122 |
| DualModeMS128 | 3 | 28 | 25 | 28 | 24 | 16 | 124 |
| GeMSS256 | 27 | 17 | 12 | 20 | 26 | 25 | 127 |

Наведені в таблиці дані дозволяють зробити висновок, що сумарними оцінками показників швидкодії та розмірів ключів і підпису, перспективними кандидатами на пост-квантовий стандарт електронного підпису можуть бути HiMQ-3, Rainbow та LUOV. Перевага належить схемам Rainbow та LUOV тому, що вони можуть реалізувати декілька рівнів захисту, тим самим підлаштовуючись під потреби. Також ці механізми мають різні перспективи використання. Так, наприклад, LUOV має малі розміри ключів, що дозволить

використовувати цей алгоритм у криптографії для пристроїв з обмеженими ресурсами. У той самий час, Rainbow має одні з найменших показників розміру підпису.

**6. Схема підпису RAINBOW**

Пропонується розглянути схему Rainbow[5] як приклад реалізації схеми підпису на базі мультиваріативних багатовимірних перетворень. Цей механізм базується на схемі UOV [13]. Сутність таких схем полягає у тому, що існують два типи змінних – vinegar (змінні O) та oil (змінні M). Перші при обчисленні центрального відображення (1) обираються випадковим чином, а інші – використовуються як значення геш-функції від повідомлення. Особливістю схеми UOV є те, що зазвичай кількість $v$ змінних O має складати $v = 2o...3o$ від кількості $o$ змінних M.

Для схеми підпису Rainbow існують такі загальносистемні параметри [5]: $(q, v_1, o_1, o_2)$, де $q$ – порядок поля (зазвичай береться розширення поля ступеню 2, у поданих специфікаціях – 16 для модифікацій «a», 31 для модифікацій «b», 256 для модифікацій «c»); $v_1$ – кількість змінних O на першому рівні; $o_1, o_2$ – таке, що $o_1 + o_2 = m$, розміри рівнів Rainbow (кількість рівнянь на кожному рівні); $U$ – кількість рівнів; $m = n - v_1$ – кількість рівнянь, де $n$ – кількість змінних.

Для модифікації Ib маємо такі параметри (31, 36, 28, 28). Можна визначити, що $m = 28 + 28 = 56$ – кількість рівнянь для цієї модифікації. $n = v1 + m = 36 + 56 = 92$ – кількість змінних.

**Генерація ключової пари**

Для створення центрального відображення будується система індексів: нехай $V = \{1, 2, 3, \ldots, n\}$ – множина індексів. Також нехай існує $v_1, ..., v_{u+1}$ – $u+1$змінних, таких, що задовольняють вимозі $0 < v_1 < v_2 \ldots < v_{u+1} = n$. Також для кожного $\ell = 1, \ldots, u+1$ існує множина індексів $V_\ell = \{1, 2, \ldots, v_\ell\}$. Таким чином, кількість елементів множини $V_i$, або її потужність, складає $|V_i| = v_i$.

Нехай $o_i = v_{i+1} - v_i$ для $i = 1, \ldots, u$

Також визначимо множини індексів змінних Oil $O_i$ такі, що $O_i = V_{i+1} - V_i$ для кожного $i = 1, \ldots, u$.

Далі будуються поліноми центрального відображення (1):

$$f^{(k)}(x_1, ..., x_n) = \sum_{i, j \in V_\ell, i \le j} \alpha_{ij}^{(k)} x_i x_j + \sum_{i \in V_\ell, j \in O_\ell} \beta_{ij}^{(k)} x_i x_j + \sum_{i \in V_\ell \cup O_\ell} \gamma_i^{(k)} x_i + \delta^{(k)},$$

Відповідно можна визначити, що для кожного $k \in \{v_1 + 1, ..., n\}$ існує лише одне $\ell \in \{1, ..., u\}$ таке, що $k \in O_\ell$. Кожний з рівнів $\ell = 1, \ldots, u$ можна описати райдугою (rainbow) змінних [14]:

$[x_1, \ldots, x_{v1}]$, $\{x_{v1+1}, \ldots, x_{v2}\}$

$[x_1, \ldots, x_{v2}], \{x_{v2+1}, \ldots, x_{v3}\}$

……

$[x_1, \ldots, x_{v_{u-1}}] \{x_{v_{u-1}} + 1, \ldots, x_n\}$

Для кожного рівня l змінні у квадратних дужках «[]» є змінними Vinegar, а у фігурних дужках «{}» – змінними Oil.

Таким чином, для модифікації (31, 36, 28, 28) можна визначити, що:

$v_1 = 36, v_2 = 64, v_3 = 92$ – кількість змінних Vinegar на різних рівнях;

$o_1 = 28, o_2 = 28$ – кількість змінних Oil на різних рівнях;

$V_1 = \{1,...,36\}, V_2 = \{1,...,64\}, V_3 = \{1,\ldots,92\}$ – індекси змінних Vinegar;

$O_1 = \{37,...,64\}, O_2 = \{65,\ldots,92\}$ – індекси змінних Oil.

Оскільки подані специфікації мають лише 2 рівня, відповідно для них можна легко описати таку райдугу. Для модифікації Ib:

$[x_1,...,x_{36}]\{x_{37},\ldots,x_{64}\}$

$[x_1,\ldots,x_{64}]\{x_{65},\ldots,x_{92}\}$

Легко бачити, що кількість поліномів $f^{(k)}$ буде дорівнювати $n-(v_1+1)+1=n-v_1=m$. Коефіцієнти $\alpha_{ij}^{(k)}, \beta_{ij}^{(k)}, \gamma_i^{(k)}$ та $\delta^{(k)}$ є випадково вибраними елементами поля $F_q$.

Далі випадковим чином з елементів поля генерується $F_q$ матриця $M_S$ розміром $m \times m$ таким чином, що в полі $F_q$ існує матриця $InvS$ така, що $M_S * InvS = E$, де $E$ – одинична матриця.

Випадковим чином генерується вектор-стовпець $c_S$ із елементів поля $F_q$ розміром *m*.

Можна стверджувати, що $S = M_S x + c_S$ є афінним відображенням.

Далі випадковим чином генерується з елементів поля $F_q$ матриця $M_T$ розміром $n \times n$ таким чином, що в полі $F_q$ існує матриця $InvT$ така, що $M_T * InvT = E$, де $E$ – одинична матриця.

Випадковим чином генерується вектор-стовпець $c_T$ із елементів поля $F_q$ розміром *n*.

Тому можна стверджувати, що $T = M_T x + c_T$ є афінним відображенням.

Приватний ключ складається з ($InvS, c_S, F, InvT, c_T$).

Публічним ключом є композиція відображень $P = S \circ F \circ T$. Для того щоб забезпечити захист EUF-CMA, необхідно до секретного та публічного ключа додати розмір $\ell$ випадкової послідовності [5]. Отже, ключевою парою є $(sk, pk) = ((InvS, c_S, F, InvT, c_T, \ell), (S \circ F \circ T, \ell))$

**Вироблення ЕП**

Нехай для підпису поданий документ $d$. Для цього документу обчислюється геш-значення $h = H(d)$. Легко можна обчислити $x = S^{-1}(h)$. Сутність вироблення ЕП полягає у тому, що необхідно знайти прообраз $y$ центрального відображення $F$ для значення $x$, тобто $F(y) = x$.

Підпис створюється наступним чином. Маємо особистий ключ ($InvS, c_S, F, InvT, c_T$), та повідомлення $d$:

1. Заповнюються перші $v_1$ значень вектору $y$ як змінні Оцту (тобто їх заповнення дозволить знайти однозначне рішення системи):

   *a*) випадковим чином генеруються $v_1$ елементів поля $F_q$ $y_1,...,y_{v_1}$ і підставляються замість змінних Оцту у рівняння $f^{(k)}$. Таким чином отримуємо нову систему рівнянь:

   $$\hat{f}^{(k)} = f^{(k)}(y_1,...,y_{v_1}), k = v_1+1,...,n;$$

   *b*) для відображення $\hat{f}^{(k)}$, яке є афінним, знаходимо такі $\hat{F}$ та $c_F$ що $\hat{F}^{(k)} = \hat{F}x + c_F$;

   *c*) якщо матриця $\hat{F}$ не є зворотною, перейти до кроку 1, *a*.
2. Нехай є повідомлення $d$. Обчислюється значення $h = H(d)$.
3. Необхідно значення $h = H(d)$ перетворити на *m* елементів поля $F_q$.
4. Обчислюється $x = InvS(d - c_S)$.

5. Обчислимо $y_{v_1+1},\ldots,y_{v_2}$ що $y_{v_1+1},\ldots,y_{v_2} = InvF((x_{v_1+1},\ldots,x_{v_2}) - c_F)$.
6. Підставимо ці значення у систему рівнянь $\widehat{f}^{(v_2+1)},...,\widehat{f}^{(n)}$, отримаємо нову систему:

$$\widehat{f}^{(v_2+1)},...,\widehat{f}^{(n)} = \widehat{f}^{(v_2+1)}(y_{v_1+1},\ldots,y_{v_2}),...,\widehat{f}^{(n)}(y_{v_1+1},\ldots,y_{v_2})$$

7. Знайдемо останні $y_{v_2+1},\ldots,y_n$ як рішення системи рівнянь

$$y_{v_2+1},\ldots,y_n = (\widehat{f}^{(v_2+1)} = x_{v_2+1},\ldots,\widehat{f}^{(n)} = x_n)$$

8. Якщо не існує таких рішень або рішення не є випадковим, повернутись до кроку 2.
9. Обчислити $z = InvT(y - c_T)$.
10. Підписом є документ $d$ є $z$.

**Перевірка підпису**

Перевірка підпису здійснюється наступним чином. Маємо публічний ключ $P = S \circ F \circ T$, повідомлення $d$ та підпис $\sigma = z$:

1. Обчислимо $h = H(d)$.
2. Знайдемо рішення $h' = P(z)$.
3. Якщо h та h` співпадають $h = h'$, підпис є коректним.

Для досягнення захисту EUF-CMA підпис та перевірка підпису здійснюються для $h = H(H(d) \| r)$, де $r$ – випадково генерована послідовність довжиною $\ell$ біт. Підписом у цьому випадку є $\sigma = (z, r)$ [5].

**Висновки**

1. Як показав аналіз, 8 із 9 MQ- схем ЕП, а саме: LUOV [3], Gui [4], Rainbow [5], MQDSS [6], TPSig [7], DualModeMS [8], HiMQ-3 [9] та GeMSS [10] заслуговують уваги з точки зору можливого застосування в якості схеми ЕП.

2. В процесі первинної оцінки криптографічної стійкості було проведено аналіз відповідності алгоритмів ЕП вимогам до криптосистем з відкритим ключем, а саме – до забезпечення захищеності від підробки [11, 12]. Сутність такої захищеності зведена до оцінки захищеності до атак на основі адаптивного підбору повідомлень (UF-CMA)[12] та стійкості від екзестенційної підробки з адаптивним підбором повідомлень (EUF-CMA).

3. Серед кандидатів на асиметричні перетворення типу 10 пропозицій грунтуються на механізмах багатовимірних 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, ключі, складність асиметричних перетворень та невеликі обчислювальні ресурси здійснення перетворень.

4. Порівняльний аналіз для секретних (або приватних) ключів (рис. 3) показав, що серед представлених кандидатів найменші показники характерні для схеми підпису LUOV та MQDSS – в обох випадках по 32 байти. Однак слід зазначити, що LUOV реалізує 2, 4 та 5 рівні захисту, у той час, коли MQDSS має такий розмір лише для 1 рівня

5 Найбільші розміри ЕП мають TpSig, DualModeMS та MQDSS, хоча ці показники відповідають рівням захисту 1 та 2. Відносно малі показники розміру ЕП має також HiMQ-3, а LUOV розташувався посередині, хоча розмір ЕП цього алгоритму значно перевищує лідерів у цьому показнику.

6. Майже однакову швидкість виконання всіх операцій має алгоритм LUOV. Невелика різниця між трьома операціями також є у GeMSS, MQDSS, та TPSig які мають невеликі аномалії у процесі перевірки підпису для першого кандидату, та генерації ключової пари для

двох останніх. Суттєво більше часу на генерацію ключової пари вимагає Rainbow, хоча він виконує операції з ЕП значно швидше більшості алгоритмів.

7. Механізм Rainbow базується на схемі UOV [13]. Сутність таких схем полягає у тому, що існують два типи змінних – vinegar (змінні O) та oil (змінні M). Перші при обчисленні центрального відображення (1) обираються випадковим чином, а інші – використовуються як значення геш-функції від повідомлення.

8. В ході досліджень було встановлено, що практично всі схеми відповідають формальним вимогам до кандидатів на постквантові схеми електронного підпису, тобто мають різні модифікації алгоритмів, які забезпечують різні рівні захисту (від одного рівня до чотирьох).

9. Попередні дослідження дозволили визначити в якості перспективних ЕП схеми Rainbow, LUOV та HiMQ-3, але слід зазначити, що вимірювання цих показників проводилися з використанням неоптимізованих алгоритмів у операційних системах. Подальші дослідження оптимізованих реалізацій є перспективним напрямом.

**Список літератури:**


1. Post-Quantum Cryptography, Round 1 Submissions, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

2. Post-Quantum Cryptography, Call for Proposals, 2016. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization/Call-for-Proposals

3. Ward Beullens, Bart Preneel, Alan Szepieniec, Frederik Vercauteren. LUOV: Lifted Unbalanced Oil and Vinegar, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

4. Jintai Ding, Ming-Shen Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang. Gui, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

5. Jintai Ding, Ming-Shen Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang. Rainbow. NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

6. Simona Samardjiska, Ming-Shing Chen, Andreas Hulsing, Joost Rijneveld, Peter Schwabe. MQDSS, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

7. Joseph Peretz, Nerya Granot. TPSig, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

8. J.-C. Faugère, L Perret, J Ryckeghem. DualModeMS: A Dual Mode for Multivariate-based Signature, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

9. Kyuang-Ah Shim, Cheol-Min Park, Aeyoung Kim. HiMQ-3: A High Speed Signature Scheme based on Multivariate Quadratic Equations, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

10. A. Casanova, J.-C. Faugère, G. Macario-Rat, J Patarin, L Perret, J Ryckeghem. GeMSS: A Great Multivariate Short Signature, NIST Submission, 2017. [On-line]. Internet: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

11. Katz, Jonathan; Lindell, Yehuda. Introduction to Modern Cryptography: Principles and Protocols. Chapman & Hall / CRC Press, 2007. 404 p.

12. Bellare, Mihir; Rogaway, Phillip. Introduction to Modern Cryptography. [On-line]. Internet: http://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf, September 21, 2005.

13. Kipnis, Aviad. Unbalanced Oil and Vinegar Signature Schemes – extended version. EURO-CRYPT, 1999.

14. Jintai Ding, Dieter Schmidt. Rainbow, a New Multivariable Polynomial Signature Scheme. Springer-Verlag Berlin Heidelberg, 2005.



*Харківський національний*
*університет імені В.Н. Каразіна;*
*АТ «Інститут інформаційних технологій», Харків*



*Надійшла до редколегії 03.11.2018*