УДК 004.056.5

Михайло МАЧУЛЯК, Владислав КОНДРАТЮК, Роман ДУДАНЕЦЬ

Західноукраїнський національний університет

АЛГОРИТМ ЦИФРОВОГО ПІДПИСУ НА ОСНОВІ КРИПТОСИСТЕМИ НІДЕРРАЙТЕРА

Вступ. Розвиток квантових обчислень створює серйозну загрозу сучасним криптографічним алгоритмам, зокрема схемам цифрового підпису на основі RSA, DSA та ECC. Квантові алгоритми, такі як алгоритм Шора, здатні ефективно розв'язувати задачі факторизації та дискретного логарифма, що робить традиційні криптосистеми вразливими. У зв'язку з цим постає гостра потреба у впровадженні постквантових криптографічних методів, які забезпечують високий рівень безпеки навіть за наявності квантових обчислювальних потужностей [1]. Таким чином, дослідження алгоритму цифрового підпису на основі криптосистеми Нідеррайтера є актуальним, оскільки воно сприяє розвитку постквантової криптографії, забезпечує захист інформації у нових технологічних умовах.

Метою роботи є дослідити алгоритм цифрового підпису на основі криптосистеми Нідеррайтера для забезпечення високого рівня безпеки у постквантових обчислювальних середовищах.

1. Основи криптосистеми Нідеррайтера

Алгоритм цифрового підпису на основі криптосистеми Нідеррайтера є одним із перспективних рішень у галузі постквантової криптографії. Цей підхід базується на складності декодування лінійних кодів, зокрема, кодів Ріда-Соломона або кодів Goppa, що є NP-складною задачею навіть для квантових комп'ютерів. Завдяки цьому, алгоритм Нідеррайтера має високий рівень криптографічної стійкості та підходить для використання в довготривалих системах захисту інформації. Для алгоритму цифрового підпису на основі криптосистеми Нідеррайтера обчислення базуються на генераторній матриці та векторах синдрому. Підпис утворюється шляхом створення вектору помилок і перетворень з використанням приватного ключа. Алгоритм цифрового підпису Нідеррайтера виконується в три основні етапи [2, 3].

1. Генерація ключів: Публічний ключ G' приховує структуру базового коду, шляхом множення на матрицю скремблера S та матрицю перестановок P. Приватний ключ включає інформацію про S, P і початковий код.

2. Процес підпису:

- хешування повідомлення для отримання вектору-образу в просторі синдрому;
- декодування цього вектору за допомогою приватного ключа для отримання вектору помилок, який слугує підписом.

3. Перевірка підпису:

- підпис разом із повідомленням хешується для порівняння з відповідним вектором синдрому;
- якщо отримані результати збігаються, підпис вважається дійсним.

У порівнянні з алгоритмами, такими як RSA чи ECDSA, криптосистема

Нідеррайтера забезпечує менший розмір підпису, але більший розмір публічного ключа. Це робить її зручною для сценаріїв, де важлива швидкість перевірки підпису, наприклад, у системах Інтернету речей (IoT) (таблиця 1).

Таблиця 1 - Порівняння алгоритмів цифрового підпису на основі McEliece, Нідеррайтера та RSA

Критерій	McEliece	Нідеррайтер	RSA
Основна ідея	Використання кодів корекції помилок (Goppa-коди).	Використання кодів корекції помилок (Goppa, Ріда-Соломона).	Використання факторизації великих чисел.
Стійкість до квантових атак	Висока. Постквантовий алгоритм.	Висока. Постквантовий алгоритм.	Низька. Уразливий до атак квантових комп'ютерів.
Розмір ключів	Дуже великий (кілька сотень кілобайт).	Дуже великий (кілька сотень кілобайт).	Невеликий (кілька кілобайт).
Розмір підпису	Великий (порядку сотень байтів).	Великий (порядку сотень байтів).	Невеликий (кілька сотень бітів).
Придатність для систем із обмеженими ресурсами	Обмежена через великий розмір ключів і підписів.	Обмежена через великий розмір ключів і підписів.	Придатний через невеликі розміри ключів і швидкість роботи.
Складність математичних операцій	Базується на складності декодування лінійних кодів.	Базується на складності декодування лінійних кодів.	Базується на складності факторизації цілих чисел.

Хоча алгоритм має переваги, він стикається з викликами, пов'язаними з великим розміром публічних ключів. Для оптимізації продуктивності пропонуються такі підходи: 1) використання скорочених лінійних кодів для зменшення розміру ключів; 2) апаратна реалізація операцій для підвищення швидкості декодування.

Висновок. Алгоритм цифрового підпису на основі криптосистеми Нідеррайтера демонструє значний потенціал для використання у постквантових системах завдяки своїй математичній складності і стійкості до атак. Подальші дослідження спрямовані на зменшення розміру публічних ключів і оптимізацію обчислень, що відкриває нові перспективи її застосування у високонавантажених системах.

Перелік використаних джерел.

1. Vambol, A., Kharchenko, V., Potii, O., Bardis, N. Post-Quantum Network Security: McEliece and Niederreiter Cryptosystems Analysis and Education Issues. WSEAS Transactions on Systems and Control, 2020, *15*, 627-634.

2. Циганенко О. С. Development of digital signature algorithm based on the Niederriter crypto-code system. Системи обробки інформації, 2020, 3 (162): 86-94.

3. Погасій С.С., Мілевський С.В., Жученко, О.С., Томашевський Б.П., Рагімова, І.Р., Сергієв, С.В. Development of Niederriter crypto-code design models on LDPC-codes. Системи обробки інформації, 2021, 4 (167): 58-68.