# Обґрунтування стійкості алгоритму ЕЦП FALCON

Денис Черниш[1], Антон Янко[2]

1. Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, УКРАЇНА, м. Харків, пр. Науки, 14,

2. Кафедра автоматизації проектування обчислювальної техніки, Харківський національний університет радіоелектроніки, УКРАЇНА, м. Харків, пр. Науки, 14, E-mail: denys.chernysh@nure.ua

***Коротка анотація – This article discusses the known cryptographic attacks on the electronic digital signature algorithm FALCON. We also consider such a weak point in the algorithm as floating point operations. We have considered the attacks that are most effective among existing attacks on electronic digital signature algorithms built on algebraic lattices. For the FALCON EDS algorithm, these attacks are ineffective when using the parameters given in the paper. We have also provided a justification for the floating point arithmetic algorithm used in the algorithm, which allows the algorithm to be immune to attacks related to this problem. Other algorithm vulnerabilities are currently being investigated within the NIST PQC competition.***

Ключові слова – алгоритм FALCON, решітки, NTRU, швидке перетворення фур'є, гешування, електронний цифровий підпис, семплер, структура GPV, постквантова криптографія

## V. Вступ

Криптосистеми на основі алгебраїчних решіток є перспективним напрямком постквантової криптографії. Основним класом решіток що використовуються у таких криптосистемх є решітки NTRU. Використання цих решіток дозволяє зробити алгоритм не лише швидким у порівнянні з іншими класами решіток, а й забезпечити порівняно високий рівень стійкості. Окрім цього, алгоритми електронного цифрового підпису засновані на алгебраїчних решітках мають порівняно малий розміру підпису та ключів. В даній роботі розглядається алгоритм ЕЦП FALCON[1] заснований саме на алгебраїчних решітках NTRU. В FALCON стійкість необхідний рівень стійкості забезпечується використанням NTRU-решіток у купі з структурою генерування цифрових підписів GPV.

Метою роботи є дослідження відомих атак на алгоритм ЕЦП FALCON та дослідження стійкості даного алгоритму.

## VI. Відомі атаки

Відновлення ключів. Найбільш ефективні атаки походять від зменшення решітки. Почнемо з розгляду решітки $\left(\mathbb{Z}[x]/(\phi)\right)^2\begin{bmatrix}0 & q\\ 1 & h\end{bmatrix}$. Після використання на цій основі редукції решітки перерахуємо всі точки решітки в області радіуса $\sqrt{2n}\sigma'$ з центром в початку координат. Таким чином, зі значною ймовірністю можна знайти $[g\ f]$. При використанні розміру блоку $B$, перерахування займає незначний час, якщо норма Грамма-Шмідта більше $0.75\sqrt{B}\sigma'$. Для найвідомішого алгоритму зменшення решітки, DBKZ, це $\left(\frac{B}{2\pi\mathrm{e}}\right)^{(1-n/B)}\sqrt{q}$.

Тоді легко вивести $B$ і показати, що $B=n+o(n)$. Це дає $B=652$, при $n=768$, і $B=921$, при $n=1024$. Передбачувана безпека докладно описана в таблиці 1 з використанням методології New Hope [2].

ТАБЛИЦЯ 1

ПЕРЕДБАЧУВАНА БЕЗПЕКА

| n | $B$ | Класичний | Квантовий |
|---|---|---|---|
| 512 | 392 | 114 | 103 |
| 768 | 652 | 195 | 172 |
| 1024 | 921 | 263 | 230 |

Підробка підпису. Підробка підпису може бути здійснена шляхом знаходження точки решітки на відстані, обмеженій $\beta$ від випадкової точки, в тій же решітці, що і вище. Це завдання також полегшується завдяки першому виконанню редукції решітки на вихідній основі. Одна можливість полягає в тому, щоб перерахувати всі точки решітки в кулі радіусом $\sqrt{\frac{nq}{\pi\mathrm{e}}}$. Оскільки ця куля більше, ніж в попередній атаці, ця атака буде повільніше. Може здатися, що це буде повільніше, ніж попередня атака через фактор $\Theta\left(\sqrt{n}\right)$ в радіусі. Це не той випадок, оскільки решітка має ортогональний базис, з чого випливає, що на відстані в $o\left(\sqrt{n}\right)$ мало точок $\left(2^{o(n)}\right)$. Мається на увазі, що запропонований спосіб починається з відновлення секретного ключа, так що він повільніше, ніж попередній алгоритм. Крім того, вкладення точки в решітку не допомагає: відстань до решітки $\Theta\left(\sqrt{n}\right)$ більше, ніж найкоротша ненульова точка.

Комбінаторна атака. При $q=O(n)$, розмір коефіцієнтів був би постійним. Тоді варіант Кирхнера-Фуке [3] BKW буде відпрацьовувати за час $2^{n/((2+o(1))\log\log n)}$, щоб відновити ключ, тобто асимптотично швидше, ніж попередні алгоритми. Це вказує на те, що найбільш компактна схема використовує $q=n^{1+\varepsilon+o(1)}$ для деякого $\varepsilon>0$. Однак, оскільки $n$ не велике, використаного $q$ досить, щоб зробити цю атаку неактуальною. Дійсно, навіть якщо припустити, що пошук найближчого сусіда виконується за постійний час і інші оптимістичні припущення, найкраща комбінаторна атака виконується за час $2^{135}$ для $n=512$.

Гібридна атака. Гібридна атака [4] поєднує в собі алгоритм зустрічі посередині і алгоритм відновлення ключа. Це дуже ефективно використовувалося проти

NTRU, через його вибір розріджених многочленів. Це, однак, не той випадок, так що його вплив набагато скромніший і врівноважується відсутністю сітчастого перерахування.

Щільна підрешітка високого рангу. Роботи показали, що, коли $f,g$ надзвичайно малі в порівнянні з $q$, легко атакувати криптографічні схеми, засновані на решітках NTRU. Навпаки, в FALCON $f,g$ приймаються не дуже малими, в той час як $q$ невеликий: побічний ефект полягає в тому, що це робить схему непроникною для так званих атак «надмірного навантаження NTRU». Зокрема, навіть якби $f,g$ були взяті в двійковому вигляді, довелося б обрати $q > n^{2.83}$, щоб ця властивість була корисною для криптоаналізу.

## VII. Точність арифметики з плаваючою точкою

Семплер з пасткою зазвичай вимагає використання арифметики з плаваючою точкою, і швидкий семплер Фур'є не є винятком. Це ставить питання про точність, необхідної для встановлення значущих кордонів безпеки. Наївний аналіз зажадав би точності $O(\lambda)$ бітів (незважаючи на логарифмічні фактори), але це привело б до істотно більш повільної процедурі генерації підпису.

Щоб проаналізувати необхідну точність, використовується аргумент розбіжності Рені. Як і в [5], через $a \prec b$ позначається той факт, що $a \le b + o(b)$, що дозволяє строго відкидати незначні фактори. Представлений швидкий семплер Фур'є є рекурсивним алгоритмом, заснованим на $2n$ дискретних семплерах $D_{\mathbb{Z},c_j,\sigma_j}$. Припускається, що значення $c_j$ (відповідно $\sigma_j$) відомі з абсолютною помилкою (відповідно, відносною похибкою), що не перевищує $\delta_c$ (відповідно $\delta_\sigma$), і через $\Upsilon$ (відповідно $\overline{\Upsilon}$) позначається вихідний розподіл семплера з нескінченної точністю. Потім стає можливим повторно використовувати точний аналіз семплера Кляйна. Для будь-якого виходу використаного семплера в гіршому випадку:

$$\left|\log\left(\frac{\overline{\Upsilon}(z)}{\Upsilon(z)}\right)\right| \prec 2n\left[\frac{\sqrt{154}}{1.312}\delta_c + (2\pi+1)\delta_\sigma\right] \le 20n(\delta_c + \delta_\sigma) \quad (1)$$

В середньому випадку значення $2n$ в рівнянні 1 можна замінити на $\sqrt{2}n$. Дотримуючись аргументів безпеки, це дозволяє стверджувати, що в середньому не очікується втрат безпеки, якщо $(\delta_c + \delta_c) \le 2^{-46}$.

Щоб перевірити, чи так це для FALCON, FALCON запускався з двома різними значеннями точності, високою точністю 200 біт і стандартної точністю 53 біта, і порівнювалися значення $c_j, \sigma_j$. Результатом цих експериментів є те, що завжди є $(\delta_c + \delta_c) \le 2^{-40}$: хоча це більше, ніж $2^{-46}$, різниця становить всього 6 біт. Тому можна вважати, що 53 біта точності досить для параметрів: рівень безпеки $\lambda \le 256$, кількість запитів $q_s \le 2^{64}$, і що можливість процедури підпису з витоком інформації про секретний базисі є суто теоретичною загрозою.

## VIII. Висновки

Розглянуті атаки є найефективнішими серед існуючих атак на алгоритми електронного цифрового підпису побудованих на алгебраїчних решітках. Для алгоритму ЕЦП FALCON наведені атаки є неефективними при використанні наведених у роботі параметрів. Також наведено обґрунтування використовуваної у алгоритмі точності арифметики з плаваючою точкою яка дозволяє алгоритму бути невразливим до атак пов’язаних з цією проблемою. Пошук інших вразливостей алгоритму на даний момент проводить у рамках конкурсу NIST PQC.

## Література


[1] Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. Specifications v1.0. Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, Zhenfei Zhang. https://falcon-sign.info/falcon.pdf.

[2] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange – A new hope. In 25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016., pages 327–343, 2016.

[3] Paul Kirchner and Pierre-Alain Fouque. An improved BKW algorithm for LWE with applications to cryptography and lattices. In Rosario Gennaro and Matthew J. B. Robshaw, editors, CRYPTO 2015, Part I, volume 9215 of LNCS, pages 43–62, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany.

[4] Nick Howgrave-Graham. A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. In Alfred Menezes, editor, CRYPTO 2007, volume 4622 of LNCS, pages 150–169, Santa Barbara, CA, USA, August 19–23, 2007. Springer, Heidelberg, Germany.

[5] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange – A new hope. In 25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016., pages 327–343, 2016.