**Вимоги та результати оцінки захищеності перспективного ЕЦП від спеціальних атак.**

**Дерев’янко Я.А., Горбенко І.Д., …**

**Анотація:**

Falcon – алгоритм електронно-цифрового підпису, що заснований на математиці алгебраїчних решіток. Він є одним з кандидатів для NIST з гарними показники швидкодії. Мінусом даного алгоритму є мала кількість досліджень стійкості проти спеціальних атак.

**1. Вступ**

Незважаючи на значні переваги, схеми на основі алгебраїчних решіток мають і недоліки.. Основною проблемою є те, що постквантові схеми так само вразливі до атак по бічних каналах, як і актуальні криптопримітиви. Саме тому слід враховувати можливі атаки та розглядати необхідні контрзаходи щодо них. На даний момент актуальними проти алгебраїчних решіток є часові атаки та атаки помилками. Тому це дослідження зосереджено саме на аналізі подібних атак на схему ЕЦП Falcon та можливих контрзаходах, які змогли б забезпечити захист від них.

Хоча відбірник алгоритму Falcon є вразливим до атак помилками, і це дає змогу отримати приватний ключ, ефективність компонентів даного алгоритму сприяє тому, що він є конкурентноспроможним, навіть при застосуванні контрзаходів.

**2 Часові атаки на Falcon**

Деякі математичні компоненти, які використовуються в алгоритмі ЕЦП Falcon, є вразливими до атак, заснованих на аналізі часових показників. Це пов’язано з певними складнощами реалізації цих компонентів за постійний час.

**2.1 Відбірник Гауса**

Саме Гаусові відбірники, як правило, є вразливим місцем для часових атак проти криптографії на решітках. Для схеми Falcon Гаусів відбірник виконує роль відбірника коротких векторів у решітках.

**2.2 Теоретичне перетворення числа (NTT)**

NTT є потенційно вразливим до часових атак, оскільки використовує велику кількість модульної арифметики, яку важко реалізувати за постійний час. У схемі Falcon NTT використовується для пришвидшення множення кільцевих многочленів.

**2.3 HashtoPoint**

Процес гешування повідомлення до точки в кільці поліномів „може бути складно здійсненним при постійному часі” – зазначають автори алгоритму Falcon. Тому функція є потенційно вразливою до часових атак.

**2.4 Запропоновані контрзаходи проти часових атак**

Одним з ефективних на даний момент заходів проти часових атак є алгоритм BlindVector, запроваджений Saarinen (2017). У BlindVector покращено випадкові перемішування для протистояння атакам по бічних каналах. Цей алгоритм використовується у даній реалізації, крім того гарантується постійна за часом реалізацію навіть для подальшого збільшення складності атак.

Для протидії часовим атакам, функції NTT та FFT також реалізовані постійними за часом. Дані операції є послідовними та безумовними, тому можна говорити про їх усталеність у часі. Ще однією особливістю є те, що у перетворенні застосовується вдосконалений NTT алгоритм Cooley-Tukey.

Також серед запропонованих заходів є відкидання зразку. Діапазон норм відкидань у реалізації, що розглядається, обрано на рівні 6,25%, 12,5% та 25%.

Ще одним нововведенням є ефективна конструкція методики гаусової вибірки (CDT) з постійним часом.

**3 BEARZ атака на Falcon**

BEARZ – атака помилками на схему ЕЦП Falcon, запропонована Sarah McCarthy та ін. (2019). Принцип дії атаки полягає у вилученні базису через переривання рекурсії або обнулення. Атака добуває закриту ключову інформацію, шляхом спричинення помилок в роботі. Модель зловмисника передбачає, що він може пропускати команди та обнуляти змінні.

**3.1 Рекурсія алгоритму Falcon**

Спираючись на структуру рекурсії Falcon, для успішної атаки слід було б перервати рекурсивний виклик у необхідній точці, щоб тільки місць були б заповнені. На жаль це не є можливим через характер функцій FFT.

**3.2 FFT: злиття та розділення**

Атаки шляхом переривання рекурсії можна класифікувати, в залежності від місця переривання. Але усі методи атаки призводять до однакового вихідного векторного формату для ; перші коефіцієнів примусово задаються нулями.

* Переривання другої рекурсії (для )
* Обнулення або атака пропуску (для )
* Переривання середньої рекурсії ( )

**3.3 Обробка після нападу**

Після отримання недійсного підпису атака передбачає відновлення таємного базису з нього. Тим самим отримується підрешітка решітки, згенерованої за допомогою F. Таким чином, з кількома недійсними підписами можна знайти решітку, породжену , (де є коротким вектором у цій решітці), а завдяки алгоритму BKZ можна знайти цей короткий вектор. Після цього можна отримати з відкритого ключа , і таким чином можна знайти таємний базис NTRU решітки.

**4 Ефективність контрзаходів**

**4.1 Часові атаки**

Для перевірки контрзаходу проти атак помилками, було 100 разів проведено процедуру підписання та визначено, що для набору 1, він потрапляв в діапазон 50 операцій на секунду, а для набору 2 - 20 операцій на секунду. Це свідчить про його ефективність проти часових атак.

**4.2 BEARZ Атака**

Перевірка після підписування може не виявити атаки помилками, яка націлена на вибірку, якщо одна і та ж помилка успішно реалізована двічі. Тому атака все ще може сформувати дійсний підпис і залишитись невиявленою. Однак контрзахід нульової перевірки повинен виявити атаку зі 100% успіхом. Тому його можна рекомендувати як мінімальний і достатній контрзахід.

**4.3 Порівняння з іншими схемами підписів на основі решітки**

Застосування перевірки після підпису спричиняє менші втрати продуктивності для алгоритму Falcon порівняно з алгоритмом Dilithium. Навіть при високому рівні безпеки його продуктивність знижується не так помітно, як у BLISS-B. Це можна пояснити ефективністю компонентів алгоритму ЕЦП Falcon. BLISS-B пропонує широкий спектр контрзаходів для захисту від запропонованих атак, і їх вплив на продуктивність може коливатися від додаткових 10% до 50%, залежно від реалізації. Однією з переваг схеми Dilithium є захищеність від атак на відбірник Гауса, проте його захист від атак помилками Bruinderink та Pessl (2018) залишається проблемою. При застосуванні до нього контрзаходів, його ефективність сповільнюється майже на 20%. А це є навіть гіршими показниками, ніж показники BLISS-B при застосуванні контрзаходу для захисту Гаусового відбірника.

**5 Висновки**

У цьому дослідженні було розглянуто атаку на схему підпису Falcon - BEARZ. Було показано, що певні математичні компоненти, які використовуються в алгоритмі ЕЦП Falcon, є вразливими до атак, заснованих на аналізі часових показників, а також, що Falcon є вразливим до атак помилками на відбірник Гауса. Через це при стандартизації чи впровадженні слід розглядати можливість фізичних атак. Було розглянуто можливі контрзаходи для протидії спеціальним атакам, показано вплив даних контрзаходів на швидкодію алгоритму. Крім того, було порівняно швидкодію різних схем, заснованих на решітках, і показано, що Falcon є конкурентним кандидатом другого раунду, навіть із застосуванням запропонованих контрзаходів.