ЗАХИСТ АЛГОРИТМУ ДІФФІ-ГЕЛЬМАНА ВІД АТАКИ ПО БОКОВОМУ КАНАЛУ

Абрамов Сергій Вадимович
аспірант групи ІБДдф-21-4.0д, спеціальності 125 "Кібербезпека",
Київського столичного університету імені Бориса Грінченка,
науковий керівник – к.т.н., доц.Соколов В.Ю.

Асиметричний алгоритм шифрування Діффі-Гельмана створений у 1976 році [1] для согласування ключів використовуючи відкрити канали зв'язку. Після появи повідомлень про створення незабаром квантових комп'ютерів, які легко зламують деякі шифри, виникла постквантова криптографія (PQC), що вивчає квантово-стійкі криптографічні алгоритми. Найбільш перспективним напрямом PQC є використання алгоритму CSIDH (Commutative Supersingular isogeny Diffie-Hellman key exchange) на ізогеніях еліптичних кривих [2, 3]. Пізніше було запропоновано використовувати в алгоритмах CSIDH еліптичні криві у формі Едвардса [2].

Одним з недоліків алгоритмів CSIDH є схильність до атаки по стороннім каналам [3]. Атака сторонніми каналами використовує непряму інформацію про фізичні процеси в пристроях. З параметрів процесів використовують час виконання операції на ґрунті спостереження за споживаною потужністю, електромагнітним випромінюванням тощо. В оригінальному алгоритмі усі ізогенії обчислюються по черзі. Атака ґрунтується на припущенні, що різні операції виконуються у пристрої за різний час, залежно від поданих вхідних даних. Таким чином, вимірюючи час обчислень та проводячи статистичний аналіз даних, можна отримати повну інформацію про секретний ключ. Особливо схильні до атак за часом алгоритми, що використовують множення, розподіл, зведення в ступінь і бітові операції над довільним числом біт [4].

Суть даної атаки полягає в тому, що крипто аналітик з високою точністю вимірює параметри (наприклад, енергоспоживання) пристрою і таким чином отримує інформацію про виконувані у пристрої операції. Під час аналізу цієї інформації визначаються секретні дані.

Щоб криптоаналітик не зміг провести атаку за часом виконання, всі етапи шифрування в пристрої повинні виконуватися за однаковий час. Наприклад, використовується метод вирівнювання часу виконання операцій. У зв'язку з цим у більшості статей з цієї теми [5] розглядаються різні варіанти «constant time CSIDH», в яких секретна кількість кроків по ізогенії нарощуються до верхньої межі фіктивними ланцюжками ізогеній. Такий захист досягається значною надмірністю та уповільненням алгоритму в середньому вдвічі.

У [6-9] пропонується альтернативний метод захисту від атаки бокового каналу. Для алгоритмів на нециклічних парах скручених кривих Едвардса пропонується метод рандомізації шляху по ізогенним ланцюжкам класів нецикличних кривих Едвардса. В орігінальному алгоритмі CSIDH на еліптичних кривих кроки по ізогеніям виконуються по черзі у межах кожної ізогенії. Пропонується метод, у якому кроки виконуються не по черзі, а у випадковому порядку, а вибір класу кривої теж здійснюється випадково. Враховується, що кроки по ізогеніям є комутативними і їх можна виконувати у будь якому порядку.

При цьому крипто аналітик не може чітко визначити по якої ізогенії здійснюється крок. У роботі [3] рекомендується для надійності використовувати кількость ізогеній 74, тоді ймовірність успішної роботи криптоаналітика дорівнює 2^{-74}

Необхідно враховувати що, в алгоритме CSIDH вже закладений природний захист від подібної атаки тім, що аналітик може вимірювати довжину кроку, але не може знати напрямок, тобто криву по якої здійснюється рух. В результате при рекомендованої в [3] кількості ізогеній 74 і кількості кроків по кожній з них 3, маємо середню довжину шляху по графу 3*74=222. Тоді загальна ймовірність успіху аналітика навіть в умовах безпомилково знайдених ізогєній дорівнює p^{-222} де p- ймовірність безпомилкового визначення ступеня ізогєнії аналітиком на одному кроці протоколу. Тоді, навить при ймовірності визначення кожного кроку p=1/2 ймовірність успіху при визначенні секретних даних буде $p= 2^{-222}$.

Враховуючи природний захист і рандомізацію маємо ймовірність успіху криптоаналітіка 2^{-296}. Що значно нижче за рівень безпеки 2^{-128}

ДЖЕРЕЛА

1. W. Di e and M.E. Hellman, \New Directions in Cryptography," IEEE Transactions on Information Theory, IT-22, n. 6, Nov 1976, pp. 644-654.

2. Bernstein D.J., Lange T. Faster Addition and Doubling on Elliptic Curves // Advancesin Cryptology—ASIACRYPT'2007 (Proc. 13th Int. Conf. On the Theory and Applicationof Cryptology and Information Security. Kuching, Malaysia. December 2–6, 2007). Lect. Notes Comp. Sci. V. 4833. Berlin: Springer, 2007. PP. 29–50.

3. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: An efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.)Advances in Cryptology { ASIACRYPT 2018. pp. 395{427. Springer International Publishing, Cham (2018).

4. Брюс Шнайер. Прикладна криптографія. Протоколи, алгоритми, ісходні тексти на языке Си Applied Cryptography. Protocols, Algorithms, and Source Code in C.—М.: Триумф, 2002.— 816 с.—3000 экз.—ISBN 5-89392-055-

5. H.Onuki, Y.Aikawa, T.Yamazaki, T.Takagi. A Faster Constant-time Algorithm of CSIDH keeping Two Points. ASIACRYPT, 2020.

6. Bessalov, A. ., Kovalchuk, L., Abramov , S. (2022). Рандомізація алгоритму CSIDH на квадратичних та скручених кривих Едвардса. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»,1(17), 128–144. https://doi.org/10.28925/2663-4023.2022.17.128144

7. A. Bessalov, et al., Implementation of the CSIDH algorithm model on supersingular twisted and quadratic Edwards curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3187, no. 1 (2022) 302–309.

8. A. Bessalov, et al., Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 1–10

9. A. Bessalov, et al., CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 36–45