УДК 004.056.55

О.Г. КАЧКО, канд. техн. наук, Ю.І. ГОРБЕНКО, канд. техн. наук, О.С. АКОЛЬЗІНА

АНАЛІЗ АТАК СПЕЦІАЛЬНОГО ТИПУ ЩОДО NTRU-ПОДІБНОГО АЛГОРИТМУ

Вступ

Розвиток та створення квантового комп'ютеру спричинили необхідність пошуку квантово стійких криптографічних механізмів та формування вимог до них. Так, NIST США восени 2017 року прийняв на конкурс постквантових 69 пакетів з кандидатами механізмів асиметричного криптоперетворення (електронні підписи (ЕП), асиметричні шифри(АСШ) та протоколи інкапсуляції ключів(ПІК)) [1], які пройшли попередні тестування. В процесі підготовки кандидатів розробниками враховано, що для практичного застосування механізми криптоперетворення мають задовольняти вимогам криптографічної стійкості, швидкодії та в певній мірі мають бути мало ресурсними. Серед висунутих вимог щодо криптографічної стійкості особливе значення мають спеціальні вимоги щодо каналів витоку по стороннім каналам та можливостям їх перекриття [2, 3]. З'ясувалось, що ця проблема є недостатньо добре вивченою, хоча і надзвичайно актуальною.

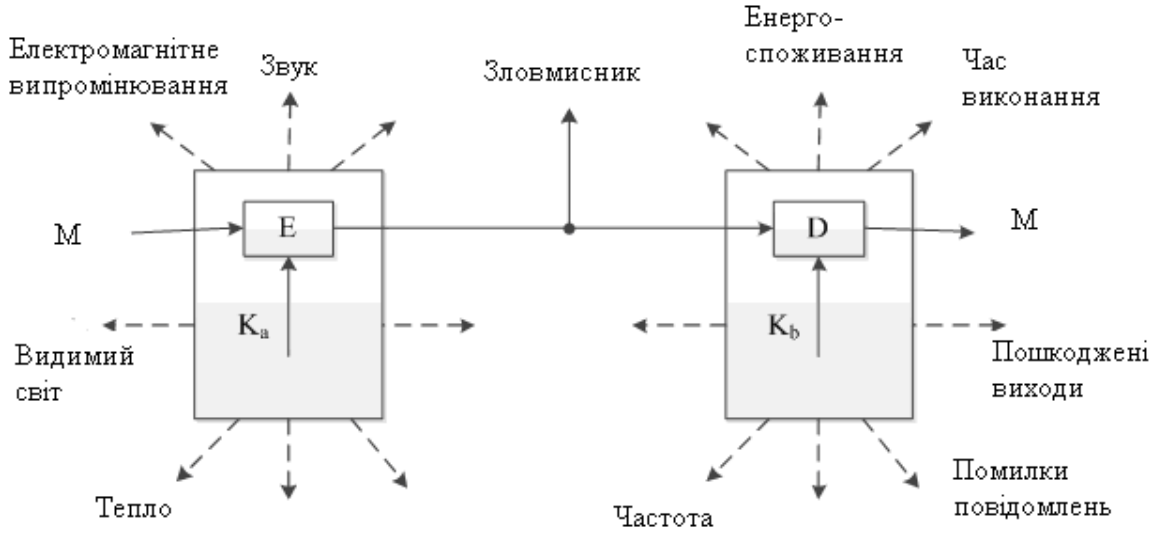
Мета статі – огляд та класифікація атак по стороннім каналам, а також викладення узагальнених підходів до перекриття або ослаблення впливу таких атак в постквантовий період в АСШ NTRU Prime IIT Ukraine [14 – 15].

1. Огляд та класифікація атак спеціального типу

Атаки спеціального виду (side-chanel attacks) можна віднести до атак аналітичного типу. Реалізація цих атак направлена на пошук вразливостей у практичній реалізації криптосистеми, в першу чергу засобу криптографічного захисту інформації (КЗІ). У [2, 3] запропоновано класифікацію спеціальних атак за такими ознаками:

- контроль над обчислювальним процесом;
- спосіб доступу до системи чи засобу;
- метод безпосереднього здійснення атаки.

На рисунку наведено модель, яка пояснює атаки спеціального виду [2, 3]. Розглянемо одну із можливих варіантів класифікації атак.



Криптографічна модель відносно атак спеціального виду

Класифікація спеціальних атак по степеню впливу на обчислювальний процес. Аналіз існуючих джерел [2, 3] показав, що по степеню впливу на обчислювальний процес спеціальні атаки можна поділити:

- на пасивні, коли зловмисник отримує необхідну інформацію без помітного впливу на систему, але система при цьому продовжує функціонувати як і раніше;
- активні, коли зловмисник реалізує деякий вплив на систему, у результаті якого змінюється поведінка системи, але зміни такого роду можуть бути «прозорими» для системи, на яку відбувається напад. При цьому зловмисник у змозі визначати та використати інформацію про систему.

Класифікація спеціальних атак по способу доступу до системи. В залежності від можливості доступу до апаратно-програмного чи апаратного засобу КЗІ можна виділити такі класи атак [2, 4 – 8]:

- агресивні (англ. *invasive*) – коли здійснюється спроба розкриття системи зловмисником та отримання прямого доступу до внутрішніх компонентів;
- напів агресивні (англ. *semi-invasive*) – коли вплив на внутрішні компоненти засобу КЗІ здійснюється без посереднього контакту;
- не агресивні (англ. *non-invasive*) – коли використовується тільки зовнішня інформація – наприклад час обчислення чи споживання енергії. Тобто безпосереднього впливу на систему, що досліджується, немає.

Класифікація спеціальних атак по методу здійснення атаки. Спеціальні атаки, в залежності від методів, які використовуються для аналізу отриманої інформації, можна поділити на [2, 3]:

- прості (англ. *simple side channel attack*) – коли здійснюється дослідження прямої залежності між процесами в пристрої та отриманої зловмисником інформації, а результатом атаки є виділення корисної інформації, наприклад, від рівня шумів;
- диференційні (англ. *differential side channel attack*) – коли використовуються статистичні методи дослідження залежностей між вхідними даними та інформацією, яка отримана під час спостереження. Як правило, при цьому здійснюються велика кількість вимірювань та спеціальна обробка сигналу і корекція помилок.

В процесі здійснення атак на реалізацію засобу КЗІ може здійснюватись аналіз усіх зовнішніх параметрів засобу, а також усі можливі методи порушення його нормального функціонування, аж до його руйнування з метою отримання секретного ключа.

При виконанні атак за часом [2, 3] вимірюється час виконання алгоритму криптоперетворення. У реалізаціях асиметричних алгоритмів час виконання операцій також може залежати як від оброблюваних даних, так і від ключа криптоперетворення (ЕП, АСШ, ПІК). При використанні апаратного рішення у вигляді автомата з жорсткою логікою, навіть час складання за деяким модулем може змінюватися у залежності від реалізації ланцюгів перенесення.

Атаки на реалізацію можуть ґрунтуватись на аналізі всіх споживаних потужностей сучасних обчислювальних пристроїв КЗІ, особливо таких, що побудовані на використанні елементів схемотехніки ТТЛ (англ. TTL), ТТЛШ (англ. TTL(S)), а також частково і КМОП (англ. CMOS). Вона також залежить від оброблюваних даних. Тому у зловмисника з’являється можливість отримати інформацію про внутрішній стан автомату, у тому числі секретний ключ, наприклад шляхом аналізу енергоспоживання при АСШ чи ЕП. Так, атака, що описана у [9], дозволяє на основі аналізу енергоспоживання обчислити вагу Хеммінга (кількість одиничних бітів) оброблюваного блоку. Ця інформація, а також знання виключно відкритих текстів (без знання шифртексту), дає зловмисникові можливість відтворити таємний ключ шифрування.

Крім того, якщо у порушника є можливість порушувати нормальну роботу пристрою (наприклад, вносити збої), то за допомогою спеціальних методів можна відновити практично будь-який секретний параметр системи.

Основною метою фізичної атаки є дослідження особливостей реалізації пристрою КЗІ (мікросхеми), що потрібно для отримання інформації відносно особистого або таємного ключів, наприклад, шляхом дослідження області всередині кристалу ПЛІС. Як правило, такі атаки орієнтовані на специфічні області ПЛІС, які в режимі нормального функціонування є не доступними.

2. Загальні пропозиції відносно протидії атакам спеціального виду

В основу захисту від атак спеціального виду можуть бути покладеними такі методи.

2.1. Фіксована кількість звернень до геш-функції

В роботі [10] показано атаку спеціального виду за часом, яка може розкрити секретний ключ NTRU. Ця атака можлива завдяки тому, що у розшифруванні різних шифротекстів використовується різна кількість звернень до геш-функції. Методом протидії таким атакам є використання механізму доповнення. Розмір доповнення повинен відповідати необхідному рівню криптостійкості. Так, в [10] використовується схема доповнення NAEP, а розмір доповнення дорівнює розміру геш значення, яке задовольняє умові

$$Hlen = \begin{cases} 160 & k \le 112 \\ 256 & k > 112 \end{cases} \quad (1)$$

де k – рівень криптостійкості.

За умови виконання (1) можна сподіватись, що криптоперетворення і, як наслідок, криптосистема, може бути захищеною від атак за часом.

2.2. Рандомізація даних

Метод рандомізації зводиться до «засліплення» даних [11 – 14]. По суті воно зводиться до зміни вхідних даних в деякий непередбачуваний стан. Залежно від характеристик функції «засліплення» вона може виключити деякі або всі витоки корисної інформації. Основною властивістю вхідних даних є їх псевдовипадковість. У криптосистемі «NTRU Prime IIT Ukraine» застосовується засліплюючий поліном, що запобігає витоку інформації про секретний ключ.

2.3. Незалежність від значень

Якщо усі перетворення із особистим ключем та поліномом засліплення при зашифруванні та розшифруванні не залежать від значень засліплюючого поліному та особистого ключа, то про них не можливо по стороннім каналам дізнатися будь-яку інформацію.

Також, якщо в операції множення не використовується значення секретного ключа, то не можливо отримати інформацію про секретний ключ аналізуючи операцію множення по стороннім каналам.

3. Вплив заходів стійкості на кількість ключів NTRU-подібного алгоритму

Аналіз показав, що в будь-якому разі ключі криптоперетворення повинні задовольняти властивостям випадкових послідовностей. До таких властивостей належать: випадковість, рівноймовірність та незалежність. В «NTRU Prime IIT Ukraine» [14, 15] це забезпечується за рахунок фіксованих значень кількостей ненульових елементів у секретних ключах f та g. Так, кількість 1, -1, 0 приблизно є рівною.

У табл. 1 у якості прикладу наведено конкретні значення параметрів для першого, середнього та останнього набору параметрів згідно [16].

Таблиця 1

Приклади параметрів NTRU Prime IIT Ukraine

Параметри				
n	q	t	рівень стійкості k	
439	6833	142	112	1
727	5827	121	205	2
1021	8819	183	298	3

У [14, 15] визначено наступне співвідношення (1, -1, 0) для секретних ключів f та g: для f: кількість 1 та -1 позначається як df та дорівнює $df = 2t$, для g кількість одиниць дорівнює $dg_1 = n/3+1$, кількість -1 дорівнює $dg_{-1} = n/3$.

Таблиця 2

Стійкість NTRU Prime IIT Ukraine

	Рівень стійкості		
	1	2	3
$df = 2t$	184	242	366
$dg_1 = n/3+1$	147	243	341
$dg_{-1} = n/3$	146	242	340

Для того щоб порахувати кількість можливих ключів, визначимо наступну формулу.

Нехай задані n_1 елементів першого типу, n_2 елементів другого типу, ... n_k елементів k-го типу, усього n елементів. Перестановки з повторенням – це варіанти їх розміщення по різним місцям. Їх кількість позначається як $P_n(n_1, n_2, ..., n_k)$.

В цьому випадку кількість перестановок з повторенням:

$$P_n(n_1, n_2, ..., n_k) = \frac{n!}{n_1! n_2! ... n_k!} \tag{2}$$

Ключі в NTRU представляють собою перестановки з повторенням довжини n, що складаються з елементів трьох типів $(1, 0, -1)$. У табл. 3 наведено значення кількості можливих ключів, які отримані при застосуванні формули (2).

Таблиця 3

Кількість ключів NTRU Prime IIT Ukraine

	Рівень стійкості		
	1	2	3
для f	$0,3*10^{193}$	$0,9*10^{344}$	$0,3*10^{482}$
для g	$0,5*10^{207}$	$0,9*10^{344}$	$0,1*10^{485}$

Якщо немає обмеження на кількість 1, -1 для ключів, наприклад як для схеми Crystals-Kyber [17], то для підрахунку треба використовувати формулу розміщення з повторенням:

$$A_n^{'m} = n^m, \tag{3}$$

де n – для ключів це кількість елементів, тобто 3, а m – кількість позицій, тобто розмір ключа.

У табл. 4 наведені значення кількості секретних ключів при відсутності обмежень на кількість коефіцієнтів.

Таблиця 4

Кількості секретних ключів без обмеження на кількість коефіцієнтів

	Рівень стійкості		
Кількість секретних ключів	1	2	3
	$0,3*10^{210}$	$0,7*10^{347}$	$0,1*10^{488}$

Аналіз показав, що при введенні обмежень розмір простору ключів зменшується. У табл. 5 наведені значення у скільки разів зменшується кількість ключів, якщо ввести обмеження на коефіцієнти згідно наведеному вище.

Таблиця 5

Зменшення розміру ключового простору

	Рівень стійкості		
	1	2	3
для f	10^{17}	$0,8*10^{3}$	$0,3*10^{6}$
для g	$0,6*10^{3}$	$0,8*10^{3}$	10^{3}

Таким чином, обмеження на кількість ненульових коефіцієнтів призводить до зменшення кількості ключів від 17-ти до 3-х десяткових порядків. Однак, ця міра є необхідною задля захисту перспективних криптоперетворень постквантового періоду від атак по стороннім каналам.

3. Висновки

В результаті проведених досліджень можна зробити наступні висновки:

1. У загальному випадку певну інформацію про особистий (таємний) ключі можна отримати по таким параметрам як час, енергоспоживання, та будь-яким іншим фізичним показникам обчислювального приладу.

2. Класифікацію спеціальних атак по стороннім каналам можна провести за такими основними ознаками: контролем над обчислювальним процесом, способом доступу до системи чи засобу та методом безпосереднього здійснення атаки.

3. При виконанні атак за часом вимірюється час виконання алгоритму шифрування. У реалізаціях асиметричних алгоритмів час виконання операцій також може залежати як від оброблюваних даних, так і від ключа шифрування. Основною ознакою, яка дозволяє здійснити атаку по значенню часу виконання криптоперетворення стороннім є, наприклад, асиметрія в числі символів (1, -1).

4. Для захисту криптосистеми «NTRU Prime IIT Ukraine» від атак за часом пропонується під час шифрування здійснювати фіксовану кількість звернень до геш-функції, а також здійснювати засліплення даних (що вносить додаткову випадковість). Також усі перетворення, що здійснюються з секретними параметрами, не повинні залежати від конкретних значень цих параметрів.

5. Для забезпечення випадковості, рівноймовірності та незалежності ключових даних можна використовуються поліноми з фіксованою кількістю символів (1, -1, 0). Однак такі обмеження призводять до зменшення кількості ключів від 17-ти порядків до 3-х десяткових порядків. Але використання ключів з фіксованою кількістю символів (1, -1, 0) ключів дозволяє в суттєвій мірі зменшити можливості криптоаналітика по здійсненню атак по спеціальним (стороннім) каналам.

Список літератури:

1. Електронний режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography.

2. Васильцов І. В. Атаки спеціального виду на криптопристрої та методи боротьби з ними ; за наук. ред. проф. В.П. Широчина. Кременець : Видавничий центр «КОГПІ», 2009. 264 с.

3. Kocher P. Differential Power Analysis/ P. Kocher, J. Jaffe, J. Benjamin // Proc. of Advances in Cryptology (CRYPTO '99). LNCS. 1999. T. 1666. P.388-397.

4. Горбенко Ю. І., Пасічник Р. О., Коряков І. В., Скуліш Є. Д. Організація атак спеціального виду на КРП в групі точок ЕК // Зб. наук. праць національної академії СБУ №4. 2011. С. 193-205.

5. Chnorr C.P. A Hierarchy of Polynomial Time Lattice Basis Reduction Algorithms / C.P. Schnorr // Theoretical Computer Science 53. 1987. P.201-224.

6. Smith K. J. Methodologies for Power Analysis Attacks on Hardware Implementations of AES: Master's thesis, Department of Computer Engineering, Rochester Institute of Technology / K. J. Smith. N: 2009. 109p.

7. D.AZTEC.2. Alternatives to RSA. – Access mode: http://www.ecrypt.eu.org/ecrypt1/documents/D.AZTEC.2-1.2.pdf.

8. Peeters E. Power and Electromagnetic Analysis: Improved Model, Consequences and Comparisons / E. Peeters, F.-X. Standaert, J.-J. Quisquater // Integr. VLSI J. vol. 40. 2007. P. 52-60.

9. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Харків : ХНУРЕ ;Форт, 2012. 868 с.

10.Oswald, E. Randomized addition-subtraction chains as a countermeasure against power attacks / E. Oswald, M. Aigner // Cryptographic Hardware and Embedded Systems – CHES 2001, LNCS, vol.2162. Springer. 2001. P.39-50.

11. Moeller B. Securing elliptic curve point multiplication against side-channel attacks / B. Moeller // Information Security – ISC 2001, LNCS, vol.2200. Springer. 2001. P.324-334.

12. Hasan M. Power analysis attacks and algorithmic approaches to their countermeasures for Koblitz curve cryptosystems / M. Hasan // IEEE Trans. Comput. 2001. Vol.50, no.10. P.1071-1083.

13. Lee M.K. Sliding window method for NTRU / M.K. Lee, J.W. Kim, J.E. Song, K. Park // Applied Cryptography and Network Security – ACNS 2007, LNCS. vol.4521. Springer. 2007. P.432-442.

14. Качко О.Г., Єсіна М.В., Акользіна О.С. Оптимізація алгоритму направленого шифрування NTRU Prime IIT Ukraine з урахуванням відомих атак // Радіотехніка. 2017. Вип. 191. С.11-23.

15. Горбенко І.Д., Качко О.Г., Єсіна М.В. Аналіз алгоритму направленого шифрування NTRU Prime // Радіотехніка. 2017. Вип. 191. С..5-10.

16. Bernstein D.J., Chuengsatiansup Ch., Lange T., van Vredendaal Ch. NTRU Prime // Cryptology ePrint Archive: https://ntruprime.cr.yp.to/ntruprime-20160511.pdf.

17. Joppe Bos, Leo Ducas, Eike Kiltz. CRYSTALS – Kyber: a CCA-secure module-lattice-based KEM // https://eprint.iacr.org/2017/634.

Акціонерне товариство
«Інститут інформаційних технологій»;
Харківський національний
університет радіоелектроніки;
Харківський національний
університет імені В.Н. Каразіна

Надійшла до редколегії 05.03.2018