УДК 004.056.55

Аналіз впливу квантових комп'ютерів на безпеку механізмів інкапсуляції ключів на прикладі ДСТУ 8961:2019 «Скеля»

Євгеній Каптьол[1]

[1] аспірант, Харківський національний університет ім. В.Н.Каразіна, Площа Свободи, 6, 61000, Харків, e-mail: kaptevg@gmail.com

У роботі наведено та проаналізовано вплив квантових комп'ютерів на безпеку механізмів інкапсуляції ключів. Розглянуто сучасний стан постквантової криптографії та постквантових алгоритмів криптоаналізу. Розглянуто та проаналізовано сучасний стан процесу стандартизації постквантової криптографії для використання в перехідний період та зроблено висновок про відсутність альтернатив серед кандидатів для стандартизації серед механізмів інкапсуляції ключів. Розглянуто розвиток методів постквантового криптоаналізу та зменшення необхідної для їх реалізації квантових ресурсів. Зроблено висновок про необхідність обрання та використання механізмів інкапсуляції ключів з доступних варіантів, що задовольняють вимоги постквантової криптографії. У роботі наведено опис та досліджено безпеку механізму інкапсуляції ключів ДСТУ 8961:2019 у моделі випадкового оракула.

Ключові слова: квантовий комп'ютер; постквантова криптографія; механізм інкапсуляції ключів; «Скеля»

Вступ. Розвиток потужностей квантових комп'ютерів, розмірів квантових регістрів та квантових алгоритмів ставить під загрозу сучасну криптографію з відкритим ключем. Особливо актуальною ця загроза стає з урахуванням факту початку комерціалізації квантових обчислень, про що свідчать широке поширення Quantum as a Service (QaaS) (таких як IBM Quantum[1]) та продаж окремих зразків квантових комп'ютерів (як наприклад продукція компанії D-wave[2]) Згідно з BSI[3], для практичного використання сучасних криптографічно релевантних алгоритмів необхідна успішна реалізація квантової корекції помилок (QEC). Таким чином, на час перехідного періоду одним з основних способів боротьби з цією загрозою є постквантова криптографія.

1. Аналіз стану постквантової криптографії

Постквантові алгоритми базуються на математичних задачах, які не мають ні класичних ні квантових ефективних алгоритмів розв'язку. Основною особливістю постквантової криптографії є можливість її реалізації на звичайних апаратних засобах. Постквантова криптографія може бути реалізована за допомогою різних підходів, серед яких можна виділити: криптографію на основі кодів, криптографію на основі решітки, криптографію на основі гешування, криптографію на основі

ізогенії та багатовимірну криптографію.

У зв'язку з потребою в постквантовій криптографії для застосування в перехідний та квантовий періоди та з метою стандартизації постквантових алгоритмів, з боку NIST було розпочато конкурс NIST PQC, в результаті котрого в липні 2022 було обрано для стандартизації 4 кандидати (механізм інкапсуляції ключа CRYSTALS-Kyber та цифрові підписи CRYSTALS-Dilithium, Falcon та SPHINCS$^+$) та було визначено кандидатів для четвертого раунду (механізми інкапсуляції ключів BIKE, Classic McEliece, HQC та SIKE)[4].

Розвиток алгоритмів криптоаналізу також не стоїть на місці. Так нещодавно в [5] було запропоновано універсальний квантовий алгоритм для факторизації цілих чисел, котрий базується на алгоритмі Шора та застосовує алгоритм квантової наближеної оптимізації (QAOA) для пришвидшення. Таким чином цей алгоритм потребує сублінійних квантових ресурсів для своєї роботи.

Квантові алгоритми криптоаналізу проходять вдосконалення щодо зменшення кількості квантових ресурсів, необхідних для їх застосування. Це призводить до наближенням практичного застосування квантових комп'ютерів для практичного криптоаналізу та зростання потреби в постквантових алгоритмах ще до їх стандартизації. Особливо варто зазначити потребу в механізмах інкапсуляції ключів, котрі не отримали багато альтернатив під час оцінки постквантових алгоритмів в ході визначення кандидатів на стандартизацію в ході третього раунду NIST PQC. У зв'язку з цим варто звернути увагу на існуючі варіанти механізмів інкапсуляції ключів для їх оцінки на придатність до застосування в якості постквантового алгоритму. Так, наприклад, розглянемо механізм інкапсуляції ключів ДСТУ 8961:2019 «Скеля».

2. Механізм інкапсуляції ключів та його безпека

Механізм інкапсуляції ключів «Скеля» використовує гібридний варіант перетворень Дента власної розробки для отримання IND-CCA2 безпечного механізму інкапсуляції ключів з ймовірнісної схеми асиметричного шифрування. Через це спочатку потрібно визначити загальні ймовірнісну схему асиметричного шифрування, механізм інкапсуляції ключів та безпеку механізму інкапсуляції ключів. Ймовірнісна схема асиметричного шифрування представляє собою трійку алгоритмів (Gen, Enc, Dec), де: Gen – поліноміальний за часом алгоритм генерації ключової пари, що приймає параметр безпеки 1^λ та повертає ключову пару (pk, sk); Enc – поліноміальний за часом алгоритм шифрування, що приймає повідомлення $m \in \mathrm{M}$, випадкове значення $r \in \mathrm{R}$ та відкритий ключ pk і повертає шифротекст $c \in \mathrm{C}$; Dec – поліноміальний за часом алгоритм розшифрування, що приймає шифртекст $c \in \mathrm{C}$, секретний ключ sk та повертає повідомлення $m \in \mathrm{M}$ або помилку розшифрування $\perp$.

Механізм інкапсуляції ключів представляє собою трійку алгоритмів $(Gen, Encaps, Decaps)$, де: Gen – поліноміальний за часом алгоритм генерації ключової пари, що приймає параметр безпеки 1^λ та повертає

ключову пару (pk, sk); *Encaps* – поліноміальний за часом алгоритм, що приймає відкритий ключ pk та повертає ключ K та його інкапсуляцію C; *Decaps* – поліноміальний за часом алгоритм, що приймає інкапсуляцію ключа C, секретний ключ sk та повертає ключ K.

Нарешті визначимо безпеку механізму інкапсуляції ключів. Нехай $\Pi = (Gen, Encaps, Decaps)$ позначає механізм інкапсуляції ключів, а A позначає супротивника. Для атаки $atk \in \{cpa, cca1, cca2\}$ і параметра безпеки λ ймовірність успіху супротивника визначається як

$$Adv_{A,\Pi}^{ind-atk}(\lambda) = |\Pr[Exp_{A,\Pi}^{ind-atk-1}(\lambda) = 1] - \Pr[Exp_{A,\Pi}^{ind-atk-0}(\lambda) = 1]|, \quad (1)$$

для $b \in \{0,1\}$, експеримент $Exp_{A,\Pi}^{ind-atk-b}(\lambda) = b'$ визначається як

$$\begin{array}{ccc} (pk, sk) & \leftarrow & Gen(1^{\lambda}) \\ (pk) & \rightarrow & A^{O_1}(pk) \\ b & \in_R & \{0,1\} \\ (K_0, C) & \leftarrow & Encaps(pk) \\ K_1 & \leftarrow_R & \{0,1\}^{KeyLen} \\ b' & \leftarrow & A^{O_2}(pk, K_b) \\ Повернути & b' & \end{array}, \quad (2)$$

де для $atk = cpa \Rightarrow O_1(\cdot) = \varepsilon, O_2(\cdot) = \varepsilon$, $atk = cca1 \Rightarrow O_1(\cdot) = O_{Decaps}(\cdot), O_2(\cdot) = \varepsilon$ та $atk = cca2 \Rightarrow O_1(\cdot) = O_{Decaps}(\cdot), O_2(\cdot) = O_{Decaps}(\cdot)$.

Механізм інкапсуляції ключів є безпечним в сенсі IND-ATK, де $atk \in \{cpa, cca1, cca2\}$, якщо $Adv_{A,\Pi}^{ind-atk}(\cdot)$ є незначною величиною, як функція від λ.

3. Формальний опис механізму інкапсуляції ключів ДСТУ 8961:2019 "Скеля"

Тепер час навести опис механізму інкапсуляції ключів ДСТУ 8961:2019 "Скеля". Для цього потрібно ввести деякі позначення.

Нехай $R_q = \mathbf{Z}_q[X]/(X^n - X - 1)$ – кільце поліномів над $\mathbf{Z}_q$ з твірним поліномом $X^n - X - 1$, а R_3 – множина поліномів кільця R_q, усі коефіцієнти яких належать до множини $\{-1, 0, 1\}$. Позначимо як $R_3^{a,b}$ множину усіх поліномів у R_3, що мають кількість ненульових елементів у діапазоні $[a, b]$.

Задля уникнення технічних деталей, які не впливають на аналіз у моделі випадкового оракула та для полегшення аналізу потрібно ввести наступні геш-

функції, які є еквівалентними до перетворень, що використовуються у ДСТУ 8961:2019:

$$BPGM : \{0,1\}^{8*maxMsgLenBytes+db} \times R_q \to R_3^t$$
$$MGF : R_q \to R_3$$
$$H : R_q \to \{0,1\}^{\lambda}$$
$$KDF : R_q \to \{0,1\}^{K\_bytes}$$

(3)

де λ – параметр безпеки, t – загальносистемний параметр, а $\max MsgLenBytes, db, K\_bytes$ є константами, що визначаються на основі загальносистемних параметрів. ДСТУ 8961:2019 має ймовірність помилок дешифрування (криптоаналізу). Загальносистемні параметри забезпечують, щоб вона була достатньо мала, і на практиці не виникало помилок дешифрування. Позначимо ймовірність виникнення помилки дешифрування як ε_{Dec}.

4. Аналіз механізму інкапсуляції ключів ДСТУ 8961:2019 "Скеля" у моделі випадкового оракула

Доказ IND-CCA2 безпеки SkelyaPKE у моделі випадкового оракула ґрунтується на стандартних техніках. Використовується наступна технічна лема.

Лема 1. Позначимо як A, B, E деякі події в ймовірністному просторі. Якщо $\Pr[A|\neg E]=\Pr[B|\neg E]$, то має місце нерівність $\left|\Pr[A]-\Pr[B]\right| \le \Pr[E]$.

Теорема 1. Нехай $PPKE=(Gen, Enc, Dec)$ – деяка ймовірнісна схема асиметричного шифрування, а SkelyaKEM – механізм інкапсуляції ключів, що побудований за допомогою застосування перетворення до $PPKE$. Якщо існує алгоритм A, що може перемогти у IND-CCA2 грі SkelyaKEM за поліноміальний час з ймовірністю ε та робить $q_{BPGM}, q_H, q_{KDF}, q_{Dec}$ запитів до випадкових оракулів BPGM, H, KDF та оракула дешифрування, то існує алгоритм B, що може інвертувати $PPKE$ з ймовірністю ε'.

$$\varepsilon' = \varepsilon - \frac{q_D}{\left|R_3^{2t,n-2t}\right|} - \frac{\gamma q_D}{2^{\lambda}} - \frac{\gamma q_D}{\left|R_3^t\right|}. \quad (4)$$

де $\frac{q_D}{\left|R_3^{2t,n-2t}\right|}$, $\frac{\gamma q_D}{2^{\lambda}}$ та $\frac{\gamma q_D}{\left|R_3^t\right|}$ - обмеження ймовірностей, пов'язаних з випадковим обранням шифротексту та помилками дешифрування.

Висновки. Розвиток потужностей квантових комп'ютерів, розмірів квантових регістрів та квантових алгоритмів ставить під загрозу сучасну криптографію з

відкритим ключем. Квантові алгоритми криптоаналізу проходять вдосконалення щодо зменшення кількості необхідних квантових ресурсів.

Механізми інкапсуляції ключів, котрі не отримали багато альтернатив під час оцінки постквантових алгоритмів в ході визначення кандидатів на стандартизацію в ході третього раунду NIST PQC.

Механізм інкапсуляції ключів «Скеля» використовує гібридний варіант перетворень Дента власної розробки для отримання IND-CCA2 безпечного механізму інкапсуляції ключів з ймовірнісної схеми асиметричного шифрування. Доказ IND-CCA2 безпеки SkelyaPKE у моделі випадкового оракула ґрунтується на стандартних техніках та показує, що механізм інкапсуляції ключів ДСТУ 8961:2019 "Скеля" задовольняє вимоги.

Література

[1] Docs directory - IBM Quantum; [accessed 2023 Mar 10]. https://quantum-computing.ibm.com/.
[2] D-Wave systems | The Practical Quantum Computing Company; [accessed 2023 Mar 12]. https://www.dwavesys.com/.
[3] Federal Office for Information Security (BSI). Quantum-safe cryptography – fundamentals, current developments and recommendations. 2021 Oct [accessed 2023 Mar 9]. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=4.
[4] NISTIR 8413. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. 2022 Jul [accessed 2023 Mar 13]. https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413-upd1.pdf.
[5] Bao Yan, Ziqi Tan, Shijie Wei, Haocong Jiang, Weilong Wang. Factoring integers with sublinear resources on a superconducting quantum processor. arXiv. 2022 Dec 23 [accessed 2023 Mar 13]. State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou. https://arxiv.org/abs/2212.12372. doi: https://doi.org/10.48550/arXiv.2212.12372.

Analysis of the impact of quantum computers on the security of key encapsulation mechanisms using an example of ДСТУ 8961:2019 «Скеля»

Yevhenii Kaptol

In the paper the influence of quantum computers on the security of key encapsulation mechanisms is presented and analyzed. The current state of post-quantum cryptography and post-quantum cryptanalysis algorithms is considered. The current state of the process of standardization of post-quantum cryptography for use in the transition period is considered and analyzed, and a conclusion is made that there are no alternatives among candidates for standardization among key encapsulation mechanisms. The development of post-quantum cryptanalysis methods and the reduction of quantum resources required for their implementation are considered. It is concluded that it is necessary to choose and use key encapsulation mechanisms from the list of available options that meet the requirements of post-quantum cryptography. In the paper the security of the DSTU 8961:2019 key encapsulation mechanism in the random oracle model is described and analyzed.

Отримано 15.03.23