КРИПТОНИТ

Постквантовая схема инкапсуляции ключа «Кодиеум»

Виктория Высоцкая, Иван Чижов

21 марта 2024

Актуальность

1. Ежегодно растет мощность квантовых компьютеров, поэтому необходима стандартизация постквантовых алгоритмов «на опережение».
2. Задачи на кодах, исправляющих ошибки, являются стойкими к квантовым атакам Шора.
3. Ни одна схема KEM пока не проходит процесс стандартизации в рамках ТК26.

λ	— уровень стойкости,
n	— длина кода,
t	— вес вектора ошибки,
$q = 2^m$	— размер поля,
$k = n - mt$	— размерность кода,
$\mathrm{H}(\cdot) : \{0,1\}^* \to \{0,1\}^{512}$	— хэш-функция Стрибог-512.

$\widetilde{\mathrm{KGen}}(1^\lambda)$

1 : $g(x) \xleftarrow{U} \mathrm{GF}(2^m)[x] : g(x) -$ неприводимый, $\deg(g) = t$;

2 : $(\alpha_1, \dots, \alpha_n) \xleftarrow{U} \mathrm{GF}(2^m)^n$, для $\alpha_i \neq \alpha_j, i, j \in [0, n-1], i \neq j$

3 : $h_{i,j} = \alpha_j^i, i \in [0, t-1], j \in [0, n-1]$

4 : $\widetilde{H} \leftarrow \{h_{i,j}\}, \widetilde{H} \in \mathrm{GF}(2^m)^{t \times n}$

5 : представить $h_{i,j}$ как столбец $(\beta_{i,j,0}, \dots, \beta_{i,j,m-1})^T, i \in [0, t-1], j \in [0, n-1]$

6 : $\widehat{h}_{it+k,j} = \beta_{ij,k}$

7 : $\widehat{H} \leftarrow \{\widehat{h}_{i,j}\}, \widehat{H} \in \mathrm{GF}(2)^{mt \times n}$

8 : представить $\widehat{H}$ в виде $[H' \mid I_{n-k}], H' \in \mathrm{GF}(2)^{mt \times mt}$

9 : **return** $(\mathsf{pk} = H', \mathsf{sk} = (g, \alpha_1, \dots, \alpha_{n-1}))$

Описание схемы шифрования Нидеррайтера[1]

Enc(pk, m)

1 : $c \leftarrow [H' \mid I_{n-k}]m^T$

2 : **return** c

Dec(sk, c)

1 : $H \leftarrow [H' \mid I_{n-k}]$

2 : $\hat{c} \leftarrow \tilde{0}^{n-k} \| c$

3 : найти c' : $Hc'^T = 0 \wedge \mathrm{wt}(c \oplus c') \leqslant t$

4 : (алгоритм Берлекэмпа–Мэсси)

5 : $m \leftarrow c \oplus c'$

6 : **if** $\mathrm{wt}(m) = t \wedge c = Hm^T$:

7 : **return** m

8 : **return** $\perp$

[1] H. Niederreiter, “Knapsack-type cryptosystems and algebraic coding theory,” *Problems of Control and Information Theory*, vol. 15, no. 2, pp. 159–166, 1986

KGen(1^λ)

1 : $(\mathsf{pk}, \mathsf{sk}) \leftarrow \widetilde{\mathsf{KGen}}(1^\lambda)$

2 : $s \xleftarrow{u} \mathcal{M}$

3 : $\mathsf{sk}' \leftarrow (\mathsf{sk}, s)$

4 : **return** $(\mathsf{pk}, \mathsf{sk}')$

Encaps(pk)

1 : $m \xleftarrow{u} \mathcal{M}$

2 : $c \leftarrow \mathsf{Enc}(\mathsf{pk}, m)$

3 : $K \leftarrow \mathsf{H}(0 \| m)$

4 : **return** (K, c)

Decaps(sk, c)

1 : **parse** $\mathsf{sk}' = (\mathsf{sk}, s)$

2 : $m' \leftarrow \mathsf{Dec}(\mathsf{sk}, c)$

3 : **if** $m' \neq \perp$ **then**

4 : **return** $K \leftarrow \mathsf{H}(0 \| m')$

5 : **else return** $K \leftarrow \mathsf{H}(1 \| s \| c)$

$$\mathcal{M} = \{x \in \{0,1\}^n : \mathrm{wt}(x) = \omega\}$$

Теорема
Пусть $\mathcal{B}$ — противник, решающий задачу IND-CCA *для* KEM *«Кодиеум», делая не более q_D запросов к оракулу декапсуляции* Decaps *и не более q_H запросов к случайному оракулу* H. *Тогда существуют противник $\mathcal{A}$ с такими же вычислительными ресурсами, решающий задачу* OW-CPA *для схемы шифрования Нидеррайтера, и противник $\mathcal{A}'$ функции* PRF H, *делающий не более q_D запросов, такие что*

$$\mathrm{Adv}^{\text{IND-CCA}}_{\text{Codiaeum}}(\mathcal{B}) \leqslant \mathrm{Adv}^{\text{OW-CPA}}_{\text{Nieder}}(\mathcal{A}) + \mathrm{Adv}^{\text{PRF}}_{\text{H}}(\mathcal{A}').$$

Теорема

Пусть $\mathcal{B}$ — противник, решающий задачу IND-CCA *для* KEM *«Кодиеум». Тогда существует противник $\mathcal{A}$, решающий задачу* OW-CPA *для схемы шифрования Нидеррайтера, и противник $\mathcal{A}'$, решающий задачу* PRF *для функции* H*, обладающие такими же вычислительными ресурсами. При этом*

$$\mathrm{Adv}^{\text{IND-CCA}}_{\text{Codiaeum}}(\mathcal{B}) \leqslant 2\sqrt{\mathrm{Adv}^{\text{OW-CPA}}_{\text{Nieder}}(\mathcal{A})} + 2\mathrm{Adv}^{\text{PRF}}_{\text{H}}(\mathcal{A}').$$

[2] N. Bindel, M. Hamburg, K. Hövelmanns, A. Hülsing, E. Persichetti, “Tighter proofs of CCA security in the quantum random oracle model” in “Theory of Cryptography”, pp. 61-90, 2019

При выборе параметров мы опирались на следующие замечания:

1. Лучшее семейство алгоритмов, решающих задачу синдромного декодирования — алгоритмы декодирования информационными множествами (ISD). Известна реализация[3], позволяющая сопоставить функционирование алгоритмов на заданном наборе параметров.
2. Существует[4] модификация этого алгоритма (QISD) на основе квантового алгоритма Гровера.

[3] `https://github.com/Crypto-TII/syndrome_decoding_estimator`
[4] D.J. Bernstein, “Grover vs. McEliece” in LNCS, vol. 6061, pp. 73–80, 2010

При выборе параметров мы опирались на следующие замечания:

3. Хэш-функция Стрибог может быть использована как псевдослучайная функция в модели ROM[5].
4. Хэш-функция Стрибог может быть использована как псевдослучайная функция в модели QROM[6].

[5] V. Kiryukhin, “About k-bit security of MACs based on hash function Streebog” in Cryptology ePrint Archive 2023/1305, 2023

[6] N. Bindel, M. Hamburg, K. Hövelmanns, A. Hülsing, E. Persichetti, “Tighter proofs of CCA security in the quantum random oracle model” in “Theory of Cryptography”, pp. 61-90, 2019

Параметры схемы «Кодиеум» в классической модели

$\lambda_{\mathrm{ROM}} = \lambda_{\mathrm{ISD}}$	m	n	k	t	откр. ключ, МБ	секр. ключ, КБ	шифр-текст, байт	ключ сессии, байт
128	11	3072	2352	60	0.19	4.58	82.5	64
192	11	4416	3360	96	0.42	6.60	132	64
256	12	6976	5536	120	0.95	11.25	180	64

Параметры схемы «Кодиеум» в квантовой модели

λ_{QISD}	m	n	k	t	откр. ключ, МБ	секр. ключ, КБ	шифр-текст, байт	ключ сессии, байт
128	12	6944	5456	124	0.97	11.20	186	64
192	13	13680	11873	139	2.56	23.60	226	64
256	13	16960	14230	210	4.63	29.32	341	64

Параметры схемы «Кодиеум» в квантовой модели

λ_{QROM}	m	n	k	t	откр. ключ, МБ	секр. ключ, КБ	шифр-текст, байт	ключ сессии, байт
128	13	16960	14230	210	4.63	29.32	341	64
192	13	31620	27902	286	12.37	54.49	465	64
256	13	51980	47404	352	25.75	95.12	574	64

BIKE/HQC:

- строятся на квазициклических кодах:
  - короткие ключи,
  - не известна сложность базовых задач,
- в схеме HQC менялся базовый код,
- у схемы HQC отсутствует доказуемая стойкость в модели QROM.

Classic McEliece:

- строится на кодах Гоппы,
- до 4 раунда отсутствовала доказуемая стойкость,
- на основе известных оценок в модели ROM:

$$\mathrm{Adv}^{\text{IND-CCA}}_{\text{Codiaeum}}(\mathcal{A}) \approx \mathrm{Adv}^{\text{IND-CCA}}_{\text{ClassicMcEliece}}(\mathcal{B}),$$

- доказано[7], что в модели QROM:

$$\mathrm{Adv}^{\text{IND-CCA}}_{\text{Codiaeum}}(\mathcal{A}) = \mathrm{Adv}^{\text{IND-CCA}}_{\text{ClassicMcEliece}}(\mathcal{B}).$$

[7] N. Bindel, M. Hamburg, K. Hövelmanns, A. Hülsing, E. Persichetti, “Tighter Proofs of CCA Security in the Quantum Random Oracle Model” in “Theory of Cryptography Conference”, pp. 61–90, 2019

СПАСИБО ЗА ВНИМАНИЕ!

Высоцкая Виктория
v.vysotskaya@kryptonite.ru

Чижов Иван
i.chizhov@kryptonite.ru