конференция РусКрипто

QApp

Механизм инкапсуляции ключа на решетках «Земляника»

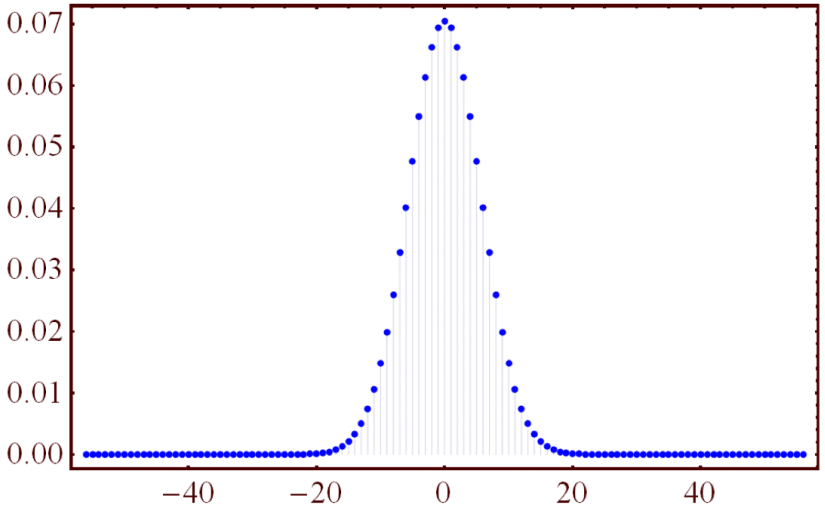
Алексей Зеленецкий
Старший криптограф-исследователь

qapp.tech

Участник

Задача LWE

- Задача S-LWE: Решить зашумленную систему уравнений $\boldsymbol{b} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e} \mod q$
- Задача D-LWE: Отличить вектор $\boldsymbol{b} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e} \mod q$ от случайного
- В обеих задачах будем считать, что $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{m \times n}$, $\boldsymbol{s} \leftarrow \chi^n$ и $\boldsymbol{e} \leftarrow \chi^m$
- Под χ обычно понимается дискретное распределение Гаусса χ_α с $\mu = 0$ и $\sigma = \dfrac{\alpha \cdot q}{\sqrt{2\pi}}$



Дискретное распределение Гаусса для $q = 113$ и $\alpha = 0.05$

Сложность и эффективность LWE

QApp

Теорема Регева (2005 г.) *

- Пусть $q = p^k$, $q = poly(n)$, $\alpha \cdot q > 2\sqrt{n}$
- S-LWE$_{n,q,\chi_\alpha} \leq$ D-LWE$_{n,q,\chi_\alpha}$
- Эффективный алгоритм для решения S-LWE$_{n,q,\chi_\alpha} \Rightarrow$ эффективный квантовый алгоритм для решения SIVP$_\gamma$ и GapSVP$_\gamma$ на **любой** решетке размерности n, где $\gamma = \tilde{O}(n/\alpha)$

Производительность МИК FrodoKEM, основанного на задаче LWE:

- Открытый ключ и шифртекст от 9 до 20 кбайт
- Производительность примерно в 100 раз ниже, чем у Kyber, Saber, NTRU
- Основные проблемы: генерация больших матриц и умножение больших матриц

* O. Regev “On lattices, learning with errors, random linear codes, and cryptography” // in Proceedings of the thirty-seventh annual ACM symposium on Theory of computing, 2005

LWE с дополнительной структурой

- Пусть $a \leftarrow R_q = \mathbb{Z}_q[x]/(x^n + 1)$, секрет $s \in R_q$ и ошибка $e \in R_q$, у обоих коэффициенты выбраны из χ_α
- Рассмотрим многочлен $b = a \cdot s + e$
- Перепишем данное выражение в матричном виде

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 & -a_n & \dots & -a_2 \\ a_2 & a_1 & \dots & -a_3 \\ \vdots & \vdots & \ddots & \vdots \\ a_n & a_{n-1} & \dots & a_1 \end{pmatrix} \cdot \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix}$$

В предположении сложности задачи LWE с матрицей вида $\mathrm{rot}(a)$ *, вектор b не отличим от случайного

* Матрица из выражения выше

Задача Module-LWE

- В задаче M-LWE: $\boldsymbol{A} \leftarrow R_q^{m \times k}$, $\boldsymbol{s} \leftarrow \chi_\alpha^{n \times k}$, $\boldsymbol{e} \leftarrow \chi_\alpha^{n \times m}$ и $\boldsymbol{b} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}$
- Задача M-LWE: Отличить вектор многочленов $\boldsymbol{b}$ от случайного вектора из R_q^k
- Эффективный алгоритм для решения M-LWE $\Rightarrow$ эффективный квантовый алгоритм для решения SIVP_γ на **любой модульной решетке** *
- Структура матрицы A в задаче M-LWE:

$$A = \begin{pmatrix} rot(a_{1,1}) & rot(a_{1,2}) & \dots & rot(a_{1,k}) \\ rot(a_{2,1}) & rot(a_{2,2}) & \dots & rot(a_{2,k}) \\ \vdots & \vdots & \ddots & \vdots \\ rot(a_{m,1}) & rot(a_{m,2}) & \dots & rot(a_{m,k}) \end{pmatrix}$$

* A. Langlois, D. Stehl´e. Worst-case to average-case reductions for module lattices // Designs, Codes and Cryptography, 2015

Описание МИК «Земляника»

Конструкция «Земляники»: LPR-based * схема шифрования Zem.PKE и МИК Zem.KEM

$$\text{Zem.PKE} \xrightarrow{\text{FO}_m^{\perp}} \text{Zem.KEM}$$

Стойкость «Земляники» основана на сложности задачи M-LWE с параметрами:

- $R_q = \mathbb{Z}_q[x]/(x^{256}+1)$, где $q \in \{2^{10}, 2^{11}\}$
- Матрица $\boldsymbol{A}$ имеет размер $k \times k$, где $k \in \{2, 3, 4\}$
- Коэффициенты векторов $\boldsymbol{s}$ и $\boldsymbol{e}$ выбираются из биномиального распределения, центрированного относительно нуля, B_η
- Если $\zeta \leftarrow B_\eta$, то $\zeta \in \{-\eta, \ldots, 0, \ldots, \eta\}$ и $\Pr[\zeta = t] = \dfrac{\binom{2\eta}{\eta+t}}{2^{2\eta}}$

* V. Lyubashevsky, C. Peikert, O. Regev On ideal lattices and learning with errors over rings // EUROCRYPT 2010

Zem.PKE.KeyGen — алгоритм выработки ключей

QApp

Алгоритм 1: Zem.PKE.KeyGen()

1: $\boldsymbol{A} \leftarrow R_q^{k \times k}$
2: $\boldsymbol{s} \leftarrow B_{\eta_s}^{n \cdot k}$
3: $\boldsymbol{e} \leftarrow B_{\eta_e}^{n \cdot k}$
4: $pk := (\boldsymbol{A}, \boldsymbol{b} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e})$
5: $sk := \boldsymbol{s}$
6: **return** (pk, sk)

Замечания:

- Для сокращения размеров pk матрица $\boldsymbol{A}$ генерируется из сида $seed_A \in \{0,1\}^{256}$ и фактически $pk = (seed_A, \boldsymbol{b})$
- η_s, η_e — параметры биномиального распределения для секрета $\boldsymbol{s}$ и $\boldsymbol{e}$, соответственно

Zem.PKE.Enc — алгоритм шифрования

QApp

Алгоритм 2: Zem.PKE.Enc($pk = (A, \boldsymbol{b})$, $m \in \{0,1\}^{256}$; $rnd \in \{0,1\}^{256}$)

1: $\boldsymbol{r} \leftarrow B_{\eta_s}^{n \cdot k}$
2: $\boldsymbol{e_1} \leftarrow B_{\eta_e}^{n \cdot k}$
3: $e_2 \leftarrow B_{\eta_2}^{n}$
4: $\boldsymbol{u} := \boldsymbol{A}^T \cdot \boldsymbol{r} + \boldsymbol{e_1}$
5: $v := \boldsymbol{b}^T \cdot \boldsymbol{r} + e_2 + \frac{q}{2} \cdot m$
6: $ct := (\boldsymbol{u}, v)$
7: **return** ct

Замечания:

- Аргумент rnd является секретным и используется для генерации $\boldsymbol{r}, \boldsymbol{e_1}$ и e_2
- Сообщение $m \in \{0,1\}^{256}$ можно рассматривать, как многочлен из R_q с бинарными коэффициентами

Zem.PKE.Dec — алгоритм расшифрования

QApp

Алгоритм 3: Zem.PKE.Dec($sk = s$, $ct = (u, v)$)

$m' := v - s^T \cdot u$
for $(i = 0; i < 256; i := i + 1)$ **do**
    if $\frac{q}{4} < m'[i] \leq 3 \cdot \frac{q}{4}$ **then**
        $m[i] = 1$
    else
        $m[i] = 0$
    end if
end for
return m

Корректность расшифрования

- Если раскрыть выражение $m' := v - \boldsymbol{s}^T \cdot \boldsymbol{u}$, то получим

$$m' := (\boldsymbol{e}^T \cdot \boldsymbol{r} - \boldsymbol{s}^T \cdot \boldsymbol{e_1} + e_2) + \frac{q}{2} \cdot m$$

- Сообщение m' будет равно изначальному сообщению m тогда и только тогда, когда

$$||\boldsymbol{e}^T \cdot \boldsymbol{r} - \boldsymbol{s}^T \cdot \boldsymbol{e_1} + e_2||_\infty < \frac{q}{4}$$

- Обозначим вероятность ошибки расшифрования за δ:

$$\delta = \mathrm{Pr}[||e^T \cdot r - s^T \cdot e_1 + e_2||_\infty \geq \frac{q}{4}]$$

IND-CPA стойкость Zem.PKE

- Заметим, что открытый ключ pk состоит из случайной матрицы $\boldsymbol{A}$ и вектора $\boldsymbol{b} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}$
- Если задача M-LWE трудна, то открытый ключ pk не отличим от случайного
- Шифртекст $ct = (\boldsymbol{u}, v)$, где $\boldsymbol{u} = \boldsymbol{A}^T \cdot \boldsymbol{r} + \boldsymbol{e}_1$ и $v = \boldsymbol{b}^T \cdot \boldsymbol{r} + e_2 + \frac{q}{2} \cdot m$
- Если задача M-LWE трудна, то шифртекст не отличим от случайного
- Таким образом, Zem.PKE является IND-CPA стойкой схемой шифрования с преимуществом противника A:

$$\mathrm{Adv}^{\text{IND-CPA}}_{\text{Zem.PKE}}(A) \leq 2\mathrm{Adv}^{\text{M-LWE}}_{n,q,k,B_{\eta s},B_{\eta e},k+1}(B)$$

Механизм инкапсуляции ключа Zem.KEM

Пусть $G : \{0,1\}^* \to \{0,1\}^{512}$ и $H : \{0,1\}^* \to \{0,1\}^{256}$ — криптографические хэш-функции

1. Алгоритм выработки ключа такой же, как в Zem.PKE

2. Алгоритм инкапсуляции Zem.KEM.Encaps:

Алгоритм 4: Zem.KEM.Encaps(pk)

1: $m \leftarrow \{0,1\}^{256}$
2: $(K, rnd) := G(m||H(pk))$
3: $c :=$ Zem.PKE.Enc(pk, m, rnd)
4: **return** (K, c)

Механизм инкапсуляции ключа Zem.KEM

3. Алгоритм декапсуляции Zem.KEM.Decaps:

Алгоритм 5: Zem.KEM.Decaps(sk, c)

1: $m' := \text{Zem.PKE.Dec}(sk, c)$
2: $(K', rnd') := G(m' || H(pk))$
3: $c' := \text{Zem.PKE.Enc}(pk, m', rnd')$
4: **if** $c \neq c'$ **then**
5: **return** $\perp$
6: **end if**
7: **return** K'

Замечания:

- Специальный символ $\perp$ сообщает об ошибке инкапсуляции
- Сессионный ключ K имеет длину 32 байта

Наборы параметров

QApp

На текущий момент предлагаются следующие наборы параметров для Zem.KEM:

#	q	n	k	η_s	η_e	$\lvert sk \rvert$, Б	$\lvert pk \rvert$, Б	$\lvert ct \rvert$, Б	$\log_2(\delta)$
Z512	1024	256	2	1	1	832	672	768	-149
Z768-R	1024	256	3	1	1	1216	992	1280	-125
Z768-C	2048	256	3	2	1	1408	1088	1152	-156
Z1024	2048	256	4	2	1	1856	1440	1568	-168

Замечания:

- Наборы параметров Z768-C и Z768-R отличаются подходом к требованиям к величине δ
- Мы предлагаем новый подход и демонстрируем его преимущество

IND-CCA стойкость Zem.KEM

Преимущество IND-CCA атакующего A против Zem.KEM *:

Против классического противника:

$$\mathsf{Adv}^{\text{IND-CCA}}_{\text{Zem.KEM}}(A) \leq 3\mathsf{Adv}^{\text{IND-CPA}}_{\text{Zem.PKE}}(B) + (q_D + 1) \cdot \mathsf{Adv}^{\text{FFP-CPA}}_{\text{Zem.PKE}}(C) + \frac{4(q+q_D+1)}{2^{256}}$$

Против квантового противника:

$$\mathsf{Adv}^{\text{IND-CCA}}_{\text{Zem.KEM}}(A) \leq 4 \cdot \sqrt{(q + q_D) \cdot \mathsf{Adv}^{\text{IND-CPA}}_{\text{Zem.PKE}}(B)} + (q_D + 1) \cdot \mathsf{Adv}^{\text{FFP-CPA}}_{\text{Zem.PKE}}(C) + \frac{8(q+q_D)}{2^{128}},$$

где:

- q — количество запросов к G и H
- q_D — количество запросов декапсуляции
- в игре FFP-CPA противник пытается сгенерировать сообщение, вызывающее ошибку расшифрования, имея при этом только открытый ключ

* K. Hövelmanns, A. Hülsing, and C. Majenz Fail-ing gracefully: Decryption failures and the Fujisaki-Okamoto transform. // ASIACRYPT 2022

Сложность известных атак на M-LWE

- На сегодняшний день все алгоритмы, решающие задачу M-LWE, решают ее, как задачу LWE
- Два основных алгоритма, primal и dual, решают LWE через сокращение базиса решеток $\Lambda = \{\mathbb{Z}^m \ni \boldsymbol{y} \equiv \boldsymbol{A} \cdot \boldsymbol{x} \mod q \mid \boldsymbol{x} \in \mathbb{Z}_q^n\}$ и $\Lambda^* = \{\boldsymbol{x} \in \mathbb{Z}^n : \boldsymbol{x} \cdot \boldsymbol{A} \equiv 0 \mod q\}$, соответственно
- Для сокращения базиса используется алгоритм BKZ, для оценки времени которого существует разные методы
- Мы используем наиболее консервативный подход core-SVP

Сложность известных атак на M-LWE

QApp

Сложности primal и dual атак в модели core-SVP для предложенных наборов параметров:

#	Primal (Cl.)	Dual (Cl.)	Primal(Q.)	Dual (Q.)
Z512	119	108	113	103
Z768-R	193	175	180	164
Z768-C	184	167	173	157
Z1024	257	233	240	218

Атаки, эксплуатирующие ошибку декапсуляции

QApp

Основные сведения:

- Каждая ошибка декапсуляции — источник информации о секретном ключе
- Идея атаки: вызвать достаточное количество ошибок декапсуляции $\rightarrow$ сделать оценку секретного ключа $\rightarrow$ решить упрощенную задачу M-LWE
- Защита — сделать δ очень маленькой (но насколько?)

Пересмотр требований к δ:

- Ранее, требования к δ предъявлялись исходя из другой оценки преимущества атакующего
- Мы впервые основываем наши требования (но только для набора параметров Z768-R) на оценке преимущества атакующего в игре FFP-CPA
- Это более практичный подход, поскольку данное преимущество можно считать оценкой сложности вызвать хотя бы одну ошибку декапсуляции

Атаки, эксплуатирующие ошибку декапсуляции

Оценка сложности вызвать ошибку декапсуляции:

1. В условиях сложности задачи M-LWE, атакующий не может отличить открытый ключ от случайного

2. В таком случае, ему ничего не остается, кроме как генерировать «слабые» шифртексты *, вызывающие ошибки декапсуляции чаще остальных

3. Пусть α — вероятность сгенерировать шифртекст с вероятностью вызвать ошибку декапсуляции β

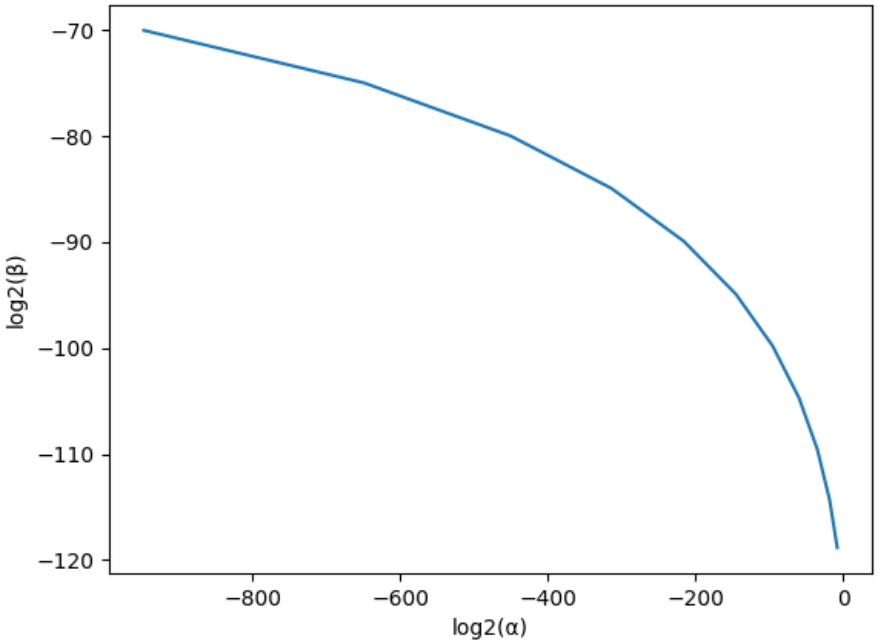
4. Сложность атаки:

   - Классическая: $\approx (\alpha \cdot \beta)^{-1}$ операций
   - Квантовая: $\approx (\sqrt{\alpha} \cdot \beta)^{-1}$ операций
   - В обоих случаях $q_D \approx \beta^{-1}$

* J.-P. D'Anvers, Q. Guo, T. Johansson, etc. Decryption failure attacks on ind-cca secure lattice-based schemes // Lecture Notes in Computer Science, 2019

Атаки, эксплуатирующие ошибку декапсуляции

Зависимость β от α для Z768-R:



Вывод: В текущих условиях такие атаки невозможны

Особенности «Земляники» и сравнение с Kyber

QApp

1. Модуль q — степень двойки:
   - Эффективнее и проще модульная арифметика и генерация матрицы
   - Использование нескольких уровней Toom-Cook вместо NTT
2. Использование FO с явным отказом:
   - Исключает лишнюю работу, выполняемую при неявном отказе
3. Пересмотр требований к параметру δ:
   - Повышение параметра δ без явного ущерба стойкости схемы $\Rightarrow$ улучшение эксплуатационных характеристик

Сравнение с Kyber

QApp

#	$\|sk\|$, Б	$\|pk\|$, Б	$\|ct\|$, Б	KG, мкс	Enc, мкс	Dec, мкс	Cl.	Q.
Z512	832	672	768	11.4	14.3	14.5	119	108
K512	1632	800	768	20.6	25.0	28.6	118	107
Z768-R	1216	992	1280	21.5	23.1	23.5	193	175
Z768-C	1408	1088	1152	23.8	23.8	28.0	184	167
K768	2400	1184	1088	32.2	36.9	41.1	182	165
Z1024	1856	1440	1568	33.2	38.4	40.7	257	233
K1024	3168	1568	1568	50.8	54.3	61.0	255	231

- Сравниваются реализации на языке программирования C
- Тесты проведены с использованием 8 ГБ RAM на процессоре архитектуры ARM с тактовой частотой 3.2 ГГц

QApp

Алексей Зеленецкий
Старший криптограф-исследователь

azelenetskiy@qapp.tech
@Leshachi

qapp.tech

Участник