РусКрипто XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

КуАпп

# Отличительные особенности отечественного постквантового механизма инкапсуляции ключа «Земляника»

Алексей Зеленецкий

Старший криптограф-исследователь, ООО «КуАпп»

Старший преподаватель, МГТУ им. Н.Э. Баумана

# Цели доклада



- Ответить на вопрос: «Земляника» = Kyber?
- Обсудить новые результаты и текущий статус работ в рамках РГ ПККМ ТК 26
- Обсудить перспективные направления дальнейших исследований

# Задачи M-LWE и M-LWR



Пусть

- $q, p, k \in \mathbb{N}$, $\phi(x) \in \mathbb{Z}[x]$ — круговой многочлен степени $\deg \phi = n$
- $\chi_s, \chi_e$ — вероятностные распределения над $\mathbb{Z}$ с $\mu = 0$ и «маленьким» $\sigma$
- $R = \mathbb{Z}[x]/(\phi(x))$, $R_q = R/(q)$

## Задача M-LWE

- $\boldsymbol{A} \leftarrow R_q^{k \times k}$, $\boldsymbol{s} \leftarrow \chi_s^{k \times n}$ и $\boldsymbol{e} \leftarrow \chi_e^{k \times n}$
- $\boldsymbol{b} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}$
- $\boldsymbol{s} - ?$
- Mod-SIVP$_\gamma \leq$ M-LWE $\leq$ PKE

## Задача M-LWR

- $\boldsymbol{A} \leftarrow R_q^{k \times k}$ и $\boldsymbol{s} \leftarrow \chi_s^{k \times n}$
- $\boldsymbol{b} = \lfloor p/q \cdot \boldsymbol{A} \cdot \boldsymbol{s} \rceil$
- $\boldsymbol{s} - ?$
- M-LWE $\overset{?}{\leq}$ M-LWR $\leq$ PKE

# Системы шифрования на основе задачи M-LWE/M-LWR

РусКрипто XXVIII научно-практическая конференция

КуАпп

Все современные системы асимметричного шифрования на основе задачи M-LWE/M-LWR следуют конструкции схемы LPR[1]:

**KeyGen():**

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

**Enc($pk, m \in R/(2)$):**

1: $\boldsymbol{r} \leftarrow \chi_s^{k \cdot n}$
2: $\boldsymbol{e_1} \leftarrow \chi_e^{k \cdot n}$
3: $e_2 \leftarrow \chi_e^{n}$
4: $\boldsymbol{u} := \boldsymbol{A}^T \cdot \boldsymbol{r} + \boldsymbol{e_1}$
5: $v := \boldsymbol{b}^T \cdot \boldsymbol{r} + e_2 + \lfloor q/2 \rceil \cdot m$
6: $c := (\boldsymbol{u}, v)$
7: **return** $c$

**Dec($sk, c$):**

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

[1] V. Lyubashevsky, C. Peikert, O. Regev. 2013. On Ideal Lattices and Learning with Errors over Rings. // Journal of the ACM

# Механизмы инкапсуляции ключа на основе задачи M-LWE/M-LWR

РусКрипто XXVIII научно-практическая конференция

КуАпп

МИК на основе M-LWE/M-LWR: LPR $\xrightarrow{\mathrm{FO}^{\mathrm{RT}}_{\mathrm{KT}}}$ KEM

## Принципы работы преобразования FO

- Вырабатывается $m \leftarrow \mathcal{M}$, затем оно зашифровывается:

$$c := \mathrm{Enc}(pk, m; G(m))$$

- Сеансовый ключ равен $H(m||c)$, если $KT = (m, c)$, и $H(m)$ в другом случае
- При декапсуляции выполняется последовательность действий:

1. $m' := \mathrm{Dec}(sk, c)$
2. $c' := \mathrm{Enc}(pk, m; G(m))$
3. $b = \begin{cases} 1, \text{ если } c' = c \\ 0, \text{ если } c' \neq c \end{cases}$

# Механизмы инкапсуляции ключа на основе задачи M-LWE/M-LWR



## Принципы работы преобразования FO

- Если $b = 1$, то возвращается $K = H(m'||c)$, если KT $= (m, c)$, и $K = H(m')$ в другом случае
- Если $b = 0$, то шифртекст отклоняется:
  - $K = \perp$, если RT $= \perp$
  - $K = H(\text{salt}|c)$ (либо $K = H(\text{salt})$), если RT $= \not\perp$
- Соль salt $\leftarrow \mathcal{M}$ вырабатывается в ходе работы KeyGen$()$ и хранится в секрете как часть $sk$

# Различные МИК на основе задачи M-LWE/M-LWR



Различие между МИК на основе M-LWE/M-LWR обеспечивается за счет:

- Выбора задачи
- Выбора параметров задачи/криптосистемы
- Выбора типа преобразования FO

Примеры различных МИК на основе M-LWE/M-LWR:

| **МИК** | **FO** | **Задача** | $\phi(x)$ | $q$ | $\chi_s$ | $\chi_e$ | **Умн. в** $R_q$ |
|---|---|---|---|---|---|---|---|
| ML-KEM (FIPS 203) | $\mathrm{FO}_m^{\not\perp}$ | M-LWE | $x^{256}+1$ | $3329$ | CB | CB | NTT |
| Saber | $\mathrm{FO}_{(m,c)}^{\not\perp}$ | M-LWR | $x^{256}+1$ | $2^{13}$ | CB | – | Toom-4-2-2 |
| Smaug-T | $\mathrm{FO}_m^{\not\perp}$ | M-LWE + M-LWR | $x^{256}+1$ | $2^{10}; 2^{11}$ | Sparse | DG | Special |
| Tyber | $\mathrm{FO}_{(m,c)}^{\not\perp}$ | M-LWE | $x^{324}-x^{162}+1$ | $2917; 3889$ | CB | CB | NTT |
| «Земляника» | $\mathrm{FO}_m^{\perp}$ | M-LWE | $x^{256}+1$ | $2^{10}; 2^{11}$ | CB | CB | Toom-4-4; Toom-4-2-2 |

# Выбор модуля $q$, равного степени двойки

РусКрипто XXVIII научно-практическая конференция КуАпп

**Преимущества:**

- Отсутствие дополнительных алгоритмов приведения по модулю — повышает производительность
- Эффективный алгоритм равномерного выбора из $\mathbb{Z}_q$ — повышает производительность
- Возможность использовать меньшие значения $q$ (из-за особенностей NTT) — снижает размер ключей и шифртекста

**Единственный недостаток** — невозможность использования NTT, однако

- Алгоритм Toom-4-4, используемый для наборов параметров Z512 и Z768, демонстрирует сравнимую с NTT производительность

# Явное оповещение об ошибке при декапсуляции

РусКрипто XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

КуАпп

**Преимущества:**

- В ходе выработки ключей не требуется генерировать соль
- Не требуется хранить соль как часть секретного ключа

**Обоснование безопасности «явного оповещения»:**

- Оценки теоретической стойкости получившегося МИК[1]
- Сведение теоретической стойкости МИК с «неявным оповещением» к теоретической стойкости МИК с «явным оповещением»[2]

[1] Hovelmanns, K., Hulsing, A., Majenz, C. (2022). Failing Gracefully: Decryption Failures and the Fujisaki-Okamoto Transform // Advances in Cryptology – ASIACRYPT 2022
[2] Hovelmanns, K., Kudinov, M. (2025). Treating Dishonest Ciphertexts in Post-quantum KEMs – Explicit vs. Implicit Rejection in the FO Transform // PQCrypto 2025

# Более точный способ оценки стойкости к атакам, эксплуатирующим ошибки при декапсуляции



- Ранее основной характеристикой МИК, отвечающей за стойкость к таким атакам, служил показатель корректности $\delta$ — вероятность возникновения ошибки при декапсуляции
- С точки зрения теоретической стойкости, для достижения стойкости в $\lambda$ бит достаточно, чтобы $\log_2 \delta \leq -\lambda$
- Уже для $\lambda = 192$ достичь этой границы можно либо за счет существенного ухудшения эксплуатационных характеристик, либо за счет существенного упрощения задачи M-LWE
- На практике выбор целевого значения для $\delta$ обосновывается эвристически

# Более точный способ оценки стойкости к атакам, эксплуатирующим ошибки при декапсуляции

В ходе анализа стойкости «Земляники» был предложен более точный способ оценки таких атак, в основе которого лежат:

- Более точная оценка теоретической стойкости МИК, построенных путем применения преобразования FO из работы [1]
- Предположение об отсутствии у атакующего информации о секретном ключе в силу вычислительной сложности M-LWE
- Предположение о пределе в $2^{64}$ запросов честному участнику со стороны атакующего

**Итог:** Увеличение показателя корректности $\delta$ для набора параметров Z768 улучшило эксплуатационные характеристики и сложность задачи M-LWE, лежащей в основе МИК

[1] Hovelmanns, K., Hulsing, A., Majenz, C. (2022). Failing Gracefully: Decryption Failures and the Fujisaki-Okamoto Transform // Advances in Cryptology – ASIACRYPT 2022

# «Земляника» = Kyber?



«КуАпп» отвечает на этот вопрос следующим образом:

> «Земляника» следует стандартной парадигме построения МИК на основе задачи M-LWE, однако при ее разработке использован ряд новых решений. Это, в совокупности с тщательно подобранными параметрами, позволяет ей превзойти свои аналоги по целому ряду эксплуатационных характеристик

# Точная оценка показателя рассеивания для системы шифрования на основе задачи M-LWE

В ходе анализа теоретической стойкости «Земляники» требовалось оценить показатель рассеивания $\gamma$ для лежащей в ее основе системы шифрования:

**Показатель рассеивания**

Система шифрования с множеством шифртекстов $\mathcal{C}$ является $\gamma$-рассеянной, когда для любой ключевой пары $(pk, sk) \leftarrow \mathsf{KeyGen}()$ и любого открытого текста $m$ выполнено:

$$\max_{c \in \mathcal{C}} \Pr[\mathsf{Enc}(pk, m) = c] \leq 2^{-\gamma}$$

- В работе[1] была получена нижняя оценка для $\gamma$ для системы шифрования на основе задачи LWE

[1] Hovelmanns, K., Hulsing, A., Majenz, C. (2022). Failing Gracefully: Decryption Failures and the Fujisaki-Okamoto Transform // Advances in Cryptology – ASIACRYPT 2022

# Точная оценка показателя рассеивания для системы шифрования на основе задачи M-LWE



В рамках обоснования стойкости «Земляники» установлено точное значение показателя рассеивания для систем шифрования на основе задачи M-LWE:

**Теорема**

Система асимметричного шифрования на основе задачи M-LWE с параметрами $R = \mathbb{Z}[x]/(x^n + 1)$, где $n$ — степень двойки, $k$, $q$, $\chi_s$ и $\chi_e$ является $\gamma$-рассеянной с показателем рассеивания

$$\gamma = \left( \max_{x \in \mathrm{supp}(\chi_e)} \chi_e(x) \right)^{n \cdot (k+1)}$$

# Реализация с использованием «Стрибог» для хэширования и выработки псевдослучайной последовательности

РусКрипто XXVIII научно-практическая конференция

КуАпп

| # | $\|sk\|$, Б | $\|pk\|$, Б | $\|ct\|$, Б | KG, мкс | Enc, мкс | Dec, мкс |
|---|---|---|---|---|---|---|
| Z512 | 832 | 672 | 768 | 28 | 32 | 30 |
| ML-KEM512 | 1632 | 800 | 768 | 21 | 25 | 28 |
| Z768 | 1216 | 992 | 1280 | 55 | 60 | 58 |
| ML-KEM768 | 2400 | 1184 | 1088 | 33 | 38 | 43 |
| Z1024 | 1856 | 1440 | 1568 | 107 | 114 | 112 |
| ML-KEM1024 | 3168 | 1568 | 1568 | 51 | 54 | 61 |

Тесты проводились на ARM 3.2 GHz 8 Gb RAM

# Работы в рамках РГ ПККМ ТК 26

РусКрипто XXVIII научно-практическая конференция

КуАпп

- Подготовлена первая редакция проекта МР
- Получены и отработаны замечания по проекту МР
- Подготовлена первая редакция обоснования стойкости

# Перспективные направления для дальнейших исследований



## Исследование стойкости:

- Получение результатов о сложности решения лежащей в основе «Земляники» задачи M-LWE в вычислительных моделях, отличных от core-SVP
- Дальнейшее исследование стойкости «Земляники» к атакам, эксплуатирующим ошибки при декапсуляции
- Исследование сложности задачи M-LWE с модулем $q = 2^l$

## Улучшение эксплуатационных характеристик:

- Применение других способов выработки псевдослучайных бинарных последовательностей
- Применение других алгоритмов умножения многочленов в кольце $\mathbb{Z}_q[x]/(x^n + 1)$ для $n$ и $q$, равных степени двойки

# Спасибо за внимание!

РусКрипто XXVIII научно-практическая конференция

КуАпп


**Алексей Зеленецкий**

Старший криптограф-исследователь, ООО «КуАпп»

Старший преподаватель, МГТУ им. Н.Э. Баумана

azelenetskiy@qapp.tech

@Leshachi


qapp.tech