QApp

Перспективные подходы к аппаратному ускорению постквантовой криптографии

Олег Турченко, Александр Данько

QApp.tech

Sk КиберХаб

АКТУАЛЬНОСТЬ

QApp

В настоящее время активно ведутся исследования в области постквантовой криптографии. Несмотря на обширную теоретическую базу, возникает также необходимость устранения технологических препятствий для внедрения постквантовых криптографических алгоритмов в существующие системы.

АКТУАЛЬНОСТЬ

QApp

Основные недостатки относительно классических криптосистем:

- **В среднем размер ключа и размер подписи больше.**
  Можно нивелировать за счет правильного выбора схемы, либо тривиального технического решения.
- **В среднем скорость шифрования/подписи ниже.**
  Можно решить большим множеством способов. Выбор конкретного решения зависит от используемого алгоритма, области применения и прикладных характеристик целевого устройства.

ПОДХОДЫ К УСКОРЕНИЮ

QApp

- **Использование SIMD инструкций.**
  SIMD инструкции являются наиболее популярным способом ускорения из-за простоты внедрения. Недостатком является то, что не все процессоры поддерживают SIMD.
- **Параллельное вычисление.**
  Параллельное вычисление может быть реализовано как аппаратно, так и программно. Потенциальная эффективность распараллеливания сильно зависит от рассматриваемого алгоритма.
- **Аппаратный ускоритель.**
  Наиболее эффективный способ ускорения, но имеющий недостатки:
  1. Сложность и стоимость внедрения.
  2. Сложность оценки эффективности. Большинство работ по аппаратному ускорению не учитывают вычислительные затраты ввода-вывода и целевое место применения.

АЛГОРИТМ KYBER

QApp

Kyber - схема инкапсуляции ключа, стойкость которой основана на сложности решения проблемы обучения с ошибками над модульными решетками. С 2023 г. - проект стандарта ML-KEM (FIPS 203).
Для референсной реализации наиболее узкими местами являются:

- Хэширование ($\sim 25\%$)
- Операции быстрого умножения NTT/INTT ($\sim 25\%$)

УСКОРЕНИЕ KYBER

QApp

- **Использование SIMD инструкций.**
  Хэширование и операции быстрого умножения NTT/INTT отлично векторизуются. Применение только SIMD инструкций позволяет ускорить алгоритм до 4 раз.
- **Аппаратный ускоритель.**
  Применение классических аппаратных ускорителей не дает существенного прироста за счет дополнительных преобразований. Однако при использовании аппаратного ускорителя NTT и функции хэширования в системе на кристалле можно достичь ускорения в 40 раз (28 нм).
- **Параллельное вычисление.**
  Kyber не обладает большим потенциалом для параллельного вычисления, но вычисление нескольких узких мест может быть ускорено в 2-3 раза.

АЛГОРИТМ DILITHIUM

QApp

Dilithium - схема ЭЦП, стойкость которой основана на сложности решения проблемы обучения с ошибками над модульными решетками. С 2023 г. - проект стандарта ML-DSA (FIPS 204).
В основе алгоритма Dilithium лежат те же примитивы, что и в Kyber. Для различных параметров может незначительно изменяться соотношение узких мест. Эффективность применения SIMD инструкций и большинства аппаратных ускорителей одинакова для Kyber и Dilithium.

АЛГОРИТМ FALCON

QApp

Falcon - схема ЭЦП, стойкость которой основана на сложности задачи поиска короткого целочисленного решения над решетками NTRU.
Для референсной реализации наиболее узким местом является:

- Умножение Монтгомери по модулю q ($\sim 12\%$)

УСКОРЕНИЕ FALCON

QApp

- **Использование SIMD инструкций.**
  В силу дизайна алгоритма Falcon отлично векторизуется. Наиболее эффективная реализация показывает прирост скорости в 18-19 раз.
- **Аппаратный ускоритель.**
  Классических аппаратные ускорители неприменимы для Falcon из-за операций с плавающей точкой. При реализации на ПЛИС можно достичь ускорения в 2-3 раза.
- **Параллельное вычисление.**
  При использовании GPU и небольших модификаций можно добиться 29-кратного ускорения относительно оптимизированной AVX2 реализации.

АЛГОРИТМ SPHINCS$^+$

QApp

SPHINCS$^+$ - схема ЭЦП, стойкость которой основана на криптографических хэш-функциях. С 2023 г. - проект стандарта SLH-DSA (FIPS 205).
Для референсной реализации наиболее узким местом является:

- Вычисление хэш функции($\sim 90\%$)

УСКОРЕНИЕ SPHINCS$^+$

QApp

- **Использование SIMD инструкций.**
  Для хэш функций SIMD инструкции дают прирост производительности в 4 раза.
- **Аппаратный ускоритель.**
  Классических аппаратные ускорители SHA позволяют ускорить алгоритм в 4 раза. При этом комбинированный метод SHA+AXV2 быстрее оптимизированной реализации только на 8.7%.
- **Параллельное вычисление.**
  SPHINCS$^+$ обладает крайне высоким потенциалом для параллельных вычислений. Используя 8 ядер, можно достичь ускорения в 7,3 раза. А при 64 ядрах - в 60.3 раз.

НОВЫЕ ОТЕЧЕСТВЕННЫЕ СХЕМЫ

QApp

Гиперикум[1] - схема ЭЦП, стойкость которой основана на криптографических хэш функциях. Представляет собой модифицированную версию SPHINCS$^+$.

Шиповник[2] - схема ЭЦП, стойкость которой основана на сложности декодирования случайного линейного кода.

[1] https://qapp.tech/research/hypericum
[2] https://kryptonite.ru/articles/postkvantovaia-kriptografiia-kak-novy-standart/

ГИПЕРИКУМ

QApp

Главным отличием с технической точки зрения является использование хэш-функции "Стрибог" вместо SHA.
Для референсной реализации наиболее узким местом является:

- Вычисление хэш функции($\sim 97\%$)

УСКОРЕНИЕ ГИПЕРИКУМ

QApp

- Для хэш-функции "Стрибог" SIMD инструкции дают прирост производительности в 2-4 раза.
- Эффективность распараллеливания почти не изменяется. В связи с этим можно применять известные результаты для SPHINCS$^+$. То есть, используя 8 ядер можно достичь ускорения в 7,3 раза. А при 64 ядрах - в 60.3 раз.

УСКОРЕНИЕ ГИПЕРИКУМ

Прототип реализации аппаратного ускорения на базе ALINX AX7Z100: Zynq 7000, позволяющий ускорить вычисление подписи в 16.8 раз относительно только программной реализации.

- WOTS+ и хэш-функция "Стрибог" вычисляются на ПЛИС
- Остальное вычисляется на процессорной части
- Тактовая частота ПЛИС: 100 МГц (макс. 250 МГц)
- Тактовая частота процессора: 667 МГц (макс. 800 МГц)
- Ширина шины AXI: 128 (32, 64)

АЛГОРИТМ ШИПОВНИК

QApp

Для референсной реализации[3] наиболее узкими местами являются:

- Выработка перестановок($\sim 62\%$)
- Функция хэширования($\sim 16\%$)
- Умножение матрицы на вектор($\sim 14\%$)

[3] Версия не окончательная и может измениться

УСКОРЕНИЕ ШИПОВНИК

QApp

- Для функции хэширования "Стрибог" SIMD инструкции дают прирост производительности в 2-4 раза.
- Обладает крайне высоким потенциалом для распараллеливания. Итеративная часть содержит 219 независимых между собой шагов и занимает почти все время выполнения подписи. Данные шаги можно выполнять параллельно, что позволит почти линейно ускорить вычисление подписи в зависимости от числа ядер.

НАИБОЛЕЕ ПЕРСПЕКТИВНЫЕ ПОДХОДЫ

QApp

- **Ускорители функции хэширования.**
  Функции хэширования встречаются во всех асимметричных схемах (даже в классических), а также являются узкими местами большинства постквантовых схем.
- **Быстрое умножение NTT/INTT.**
  NTT/INTT является узким местом наиболее популярных международных схем Kyber и Dilithium. На данный момент Kyber является единственным отобранным алгоритмом на роль KEM.

СПАСИБО ЗА ВНИМАНИЕ

QApp

QApp

Олег Турченко
Исследователь-криптограф

Email: oturchenko@qapp.tech

Телефон: +7-951-495-46-75

Telegram: @Oleg_Turchenko

Александр Данько
Разработчик

Email: adanko@qapp.tech

Телефон: +7-950-841-27-56

Telegram: @AlexanderDanko

QApp.tech

Sk КиберХаб

ГАЗПРОМБАНК