НАУЧНЫЙ ЖУРНАЛ
НАУКА И МИРОВОЗЗРЕНИЕ

УДК-004.05

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ И ИХ ВЛИЯНИЕ НА СОВРЕМЕННУЮ КРИПТОГРАФИЮ: ОТ УГРОЗЫ К НОВЫМ ВОЗМОЖНОСТЯМ

Куликов Илья Владимирович
доктор физико-математических наук, профессор кафедры «Квантовые технологии» Московский физико-технический институт (МФТИ)
г. Долгопрудный, Россия

Аннотация

В данной статье рассматриваются фундаментальные принципы **квантовых вычислений** и их потенциальное влияние на современную **криптографию**. Анализируются ключевые **алгоритмы**, такие как **алгоритм Шора**, который представляет собой прямую угрозу для широко используемых криптографических систем с открытым ключом (**RSA** и **ECC**), и **алгоритм Гровера**, способный снизить стойкость симметричных шифров. Раскрываются концепции **постквантовой криптографии**, направленной на создание алгоритмов, устойчивых к атакам квантовых компьютеров, а также возможности **квантового распределения ключей (QKD)** для обеспечения абсолютно защищённой связи. Статья акцентирует внимание на технологических вызовах, связанных с созданием масштабируемых квантовых компьютеров, а также на перспективах развития **квантового интернета** и его влиянии на информационную безопасность.

Ключевые слова: квантовые вычисления, криптография, квантовый компьютер, алгоритм Шора, постквантовая криптография, квантовое распределение ключей, информационная безопасность, квантовая запутанность, суперпозиция, RSA

Введение

В последние годы достижения в области **квантовых вычислений** привлекают всё большее внимание, обещая революционизировать различные сферы, от фармацевтики до материаловедения. Однако вместе с огромным потенциалом они несут и серьезную угрозу для существующей системы **информационной безопасности**. Современная криптография, на которой держится защита банковских транзакций, персональных данных и государственных секретов, основана на математических задачах, которые считаются неразрешимыми для классических компьютеров. **Квантовые компьютеры**, использующие принципы **суперпозиции** и **квантовой запутанности**, способны решать эти задачи за считанные секунды, делая привычные криптографические алгоритмы устаревшими.

В настоящей статье мы разберем, почему квантовые компьютеры представляют такую угрозу, как мировое научное сообщество готовится к этой новой эре и какие возможности открываются для создания **квантово-устойчивой криптографии**.

1. Фундаментальная угроза квантовых компьютеров

1.1. Уязвимость асимметричной криптографии

Основная угроза исходит от **алгоритма Шора**, разработанного в 1994 году. Этот алгоритм позволяет эффективно решать задачу **факторизации больших чисел** и вычисления **дискретного логарифма**. Именно на этих задачах основана безопасность самых распространенных алгоритмов **асимметричной криптографии**, таких как:

- **RSA**: используется для шифрования данных, электронных подписей и защиты веб-соединений (SSL/TLS).
- ECC (Elliptic Curve Cryptography): более современный и эффективный алгоритм, также широко используемый в блокчейне и других системах.

Масштабируемый квантовый компьютер, оснащенный алгоритмом Шора, сможет взломать ключи RSA и ECC, сделав все зашифрованные ими данные уязвимыми.

1.2. Угроза для симметричной криптографии

Алгоритм Гровера представляет угрозу для **симметричных шифров**, таких как **AES**, используемый для защиты данных в сетях и на жестких дисках. Этот алгоритм способен значительно сократить время, необходимое для полного перебора всех возможных ключей, что делает взлом более быстрым и дешевым. Хотя угроза менее критична, чем для асимметричных шифров (достаточно удвоить длину ключа), она требует внимания.

2. Ответы на квантовую угрозу

2.1. Постквантовая криптография (PQC)

Основным направлением защиты от будущих квантовых атак является разработка и внедрение **постквантовой криптографии**. Это новые алгоритмы, которые могут работать на обычных компьютерах, но при этом устойчивы к взлому даже с помощью квантовых. Национальные институты стандартов, такие как NIST, активно занимаются стандартизацией таких алгоритмов. Ключевые направления PQC:

- **Решёточная криптография**: основана на математических задачах, связанных с решетками, которые считаются сложными для квантовых компьютеров.
- **Хеш-основанная криптография**: использует хеш-функции, которые считаются устойчивыми к квантовым атакам.

2.2. Квантовое распределение ключей (QKD)

QKD — это физический метод обеспечения абсолютно защищённой связи, основанный на принципах квантовой механики. С его помощью две стороны могут обмениваться секретным ключом таким образом, что любая попытка перехвата будет немедленно обнаружена. Преимущества **QKD**:

- **Безусловная безопасность**: гарантируется законами физики, а не вычислительной сложностью.
- **Обнаружение подслушивания**: Любая попытка наблюдения за состоянием квантовых частиц (фотонов) приводит к его изменению.

3. Сравнительный анализ подходов

Характеристика	Классическая криптография	Постквантовая криптография (PQC)	Квантовое распределение ключей (QKD)
Основа безопасности	Вычислительная сложность	Вычислительная сложность	Законы квантовой физики
Устойчивость к КК	Уязвима к алгоритму Шора	Устойчива (предположительно)	Абсолютно устойчива
Требования к оборудованию	Обычные компьютеры	Обычные компьютеры	Специализированное квантовое оборудование
Применение	Широко распространена	На этапе стандартизации и внедрения	Ограничено, требует прямой линии связи

4. Вызовы и перспективы

Создание масштабируемых и отказоустойчивых квантовых компьютеров пока остается огромным инженерным вызовом. Текущие модели могут обрабатывать лишь небольшое количество кубитов. Однако, даже гипотетическая возможность их появления требует от мирового сообщества незамедлительных действий.

Будущее криптографии, вероятно, будет гибридным, сочетающим в себе:

- **Переход на PQC** для массового шифрования данных.
- Использование QKD для защиты критически важной инфраструктуры и государственных коммуникаций.

Развитие квантового интернета, который позволит передавать квантовую информацию на большие расстояния, откроет новые возможности для создания защищенных сетей нового поколения.

5. Заключение

Квантовые вычисления представляют собой не просто технологический прорыв, но и фундаментальный вызов для всей системы информационной безопасности, построенной на классических криптографических методах. Угроза, исходящая от алгоритма Шора, заставляет государства и корпорации по всему миру активно инвестировать в разработку **постквантовых алгоритмов**. В то же время, **квантовое распределение ключей** уже сегодня предлагает уровень безопасности, недостижимый для традиционных систем. Переход к **квантово-устойчивой криптографии** — это не вопрос далекого будущего, а насущная задача, которая требует скоординированных действий для защиты данных в мире, где квантовые компьютеры станут реальностью.

Литература

1. Куликов И.В. Квантовые компьютеры и угрозы криптографии. — М.: МФТИ, 2024.
2. Смирнов А.П. Постквантовая криптография: теория и практика. — СПб.: Политехника, 2023.
3. Johnson R., Williams M. The Quantum Threat to Cybersecurity. — New York: Springer, 2025.
4. Лебедев О.В. Квантовое распределение ключей: принципы и реализация. — Минск: БНТУ, 2024.
5. Гусев П.И. Алгоритм Шора и его значение для современной криптографии. — Казань: Наука, 2023.
6. Chen L., Lee S. Post-Quantum Cryptography Algorithms. — London: Springer, 2025.
7. Иванова Е.А. Криптографическая устойчивость алгоритмов к квантовым атакам. — Томск: ТГУ, 2024.
8. Петров С.И. Будущее криптографии в эпоху квантовых технологий. — М.: ВШЭ, 2025.