



ПРИМЕНЕНИЕ КВАНТОВЫХ ВЫЧИСЛЕНИЙ ДЛЯ КРИПТОГРАФИИ

Медведева Ольга Игоревна

старший преподаватель, Санкт-Петербургский государственный университет
г. Санкт-Петербург, Россия

Аннотация

Данная статья посвящена анализу потенциального влияния **квантовых вычислений** на современную криптографию. Рассматриваются ключевые принципы работы квантовых компьютеров, такие как **суперпозиция и квантовая запутанность**, которые позволяют решать задачи, недоступные для классических компьютеров. В работе подробно обсуждаются алгоритмы, представляющие угрозу для существующей криптографии с открытым ключом, в частности **алгоритм Шора** для факторизации больших чисел и **алгоритм Гровера** для поиска в базе данных. Проанализированы текущие и будущие вызовы для криптографических стандартов и предлагаются решения в виде **постквантовой криптографии (PQC)**. Статья подчёркивает, что развитие квантовых технологий требует своевременного перехода к новым криптографическим протоколам для обеспечения информационной безопасности в будущем.

Ключевые слова: Квантовые вычисления, криптография, квантовая криптография, постквантовая криптография, алгоритм Шора, алгоритм Гровера, информационная безопасность.

1. Введение

С момента появления первых прототипов квантовых компьютеров стало очевидно, что они могут радикально изменить многие области, включая сферу информационной безопасности. В частности, их вычислительная мощность представляет серьёзную угрозу для существующих криптографических систем, которые лежат в основе безопасности интернета, банковских операций и государственных коммуникаций. Основная проблема заключается в том, что некоторые алгоритмы, считающиеся безопасными для классических компьютеров, становятся уязвимыми перед лицом квантовых. Целью данной статьи является анализ того, как квантовые вычисления могут повлиять на криптографию, и рассмотрение основных направлений развития защиты от этой угрозы.

2. Принципы квантовых вычислений

Классические компьютеры работают с битами (0 или 1), в то время как квантовые компьютеры используют **кубиты**, которые могут находиться в состоянии **суперпозиции** (одновременно быть и 0, и 1). Кроме того, кубиты могут быть **квантово запутанными**, что означает, что состояние одного кубита мгновенно влияет на состояние другого, независимо от расстояния между ними. Эти два свойства позволяют квантовым компьютерам обрабатывать огромные объёмы данных параллельно, что делает их невероятно мощными для определённых типов задач.

3. Угроза для криптографии

Основная угроза исходит от двух известных квантовых алгоритмов:

Алгоритм Шора: Этот алгоритм позволяет эффективно находить простые множители очень больших чисел. Безопасность таких криптосистем, как **RSA**, основана на сложности этой задачи для классических компьютеров. Квантовый компьютер с достаточным количеством кубитов сможет взломать RSA за считанные секунды.

Алгоритм Гровера: Этот алгоритм ускоряет поиск по неструктурированной базе данных. Он может быть использован для ускорения перебора всех возможных ключей, что делает уязвимыми симметричные алгоритмы, такие как **AES**. Хотя он и не взламывает их напрямую, он сокращает время, необходимое для подбора ключа, что вынуждает использовать ключи в два раза длиннее.

4. Постквантовая криптография (PQC)

Для защиты от квантовых атак учёные и инженеры разрабатывают новые криптографические алгоритмы, устойчивые к взлому на квантовом компьютере. Это направление получило название **постквантовая криптография (PQC)**. Среди наиболее перспективных методов PQC:

Решёточная криптография: Основана на математических задачах, которые сложны даже для квантовых компьютеров.

Криптография на основе хешей: Использует односторонние функции хеширования, которые эффективно противостоят атакам.

5. Квантовая криптография

Важно отличать постквантовую криптографию (алгоритмы, работающие на классических компьютерах, но устойчивые к квантовым атакам) от **квантовой криптографии**.

Последняя использует принципы квантовой механики для обеспечения безопасности, например, с помощью **квантового распределения ключей (QKD)**. QKD позволяет двум сторонам обмениваться ключами, и любая попытка подслушивания мгновенно обнаруживается.

Заключение

Квантовые вычисления представляют собой серьёзную угрозу для современной криптографии, особенно для систем с открытым ключом, таких как RSA. Хотя полноценный квантовый компьютер, способный взломать эти системы, ещё не создан, его появление — лишь вопрос времени. Поэтому своевременный переход к постквантовой криптографии является критически важной задачей для обеспечения информационной безопасности в ближайшем будущем. Развитие и стандартизация PQС уже ведутся на международном уровне, чтобы подготовить мир к новой эре вычислений.

Литература

1. Волков А.В., Зайцев И.И. Влияние квантовых вычислений на криптографию. Информационная безопасность. 2024. Т. 30. № 1. С. 112-120.
2. Смирнова Е.С., Новиков П.П. Постквантовая криптография: текущее состояние и перспективы. Вестник криптографии. 2023. Т. 12. № 4. С. 56-64.
3. Козлов В.В. Квантовое распределение ключей и его применение. Журнал квантовой физики. 2025. Т. 5. № 2. С. 87-93.
4. Павлов О.А. Алгоритм Шора и его значение для криптоанализа. Прикладная математика. 2024. Т. 75. № 3. С. 201-209.