ПОДХОДЫ КВАНТОВОГО ОТЖИГА К ВЗЛОМУ ШИФРОВАНИЯ RSA

Холодов Я. А.[1], Саллум Х.[2], Агапова Н. А.[3]

DOI: 10.21681/2311-3456-2025-4-127-133

Цель исследования: *изучение трансформационного потенциала квантового отжига в решении проблемы простой факторизации.*

Метод(ы) исследования: *наш подход включает в себя всесторонний обзор последних экспериментальных прорывов и теоретических инноваций. В частности, мы анализируем такие методики, как память поверхностного кода, формулировки HUBO и QUBO, алгоритмы гамильтониана, зависящие от диапазона, модульные локально-структурированные методы встраивания и модифицированный метод таблицы умножения. Кроме того, для подтверждения наших выводов представлены предварительные эксперименты по генерации случайных чисел.*

Результат(ы) исследования: *исследование оценивает применение квантового отжига для факторизации простых чисел, показывая, что продвинутые техники отображения задач, такие как формулировки HUBO и QUBO, значительно повышают эффективность представления сложных задач факторизации на квантовом оборудовании. Примечательно, что включение памяти поверхностных кодов повышает стабильность состояний кубитов во время отжига, снижая количество ошибок и повышая точность вычислений. Исследование также демонстрирует, что алгоритмы гамильтониана, зависящие от диапазона, и модульные локально-структурированные методы встраивания способствуют оптимизации взаимодействия кубитов, обеспечивая более точное выполнение процесса факторизации. Представлен модифицированный метод таблицы умножения, обеспечивающий оптимизированную вычислительную стратегию, особенно эффективную для больших составных чисел. Предварительные эксперименты со случайными числами подтверждают теоретические выводы, указывая на то, что эти интегрированные методы позволяют повысить производительность по сравнению с традиционными подходами. В совокупности полученные результаты подчеркивают потенциал квантового отжига как надежной основы для решения сложных криптографических задач и закладывают основу для будущих исследований масштабируемых квантовых алгоритмов и аппаратных реализаций.*

Научная новизна: *эта работа объединяет несколько передовых методов квантового отжига для факторизации простых чисел, соединяя экспериментальные инновации с теоретическими разработками, чтобы предложить новую структуру, которая повышает эффективность криптографических вычислений.*

Ключевые слова: *Quantum Annealing, RSA, QUBO, Prime Factorization.*

Введение

Квантовые вычисления стали преобразующей областью, обладающей потенциалом превзойти классические вычислительные возможности в решении определенных классов задач. Недавние достижения в области квантовой коррекции ошибок, такие как продемонстрированные Google Quantum AI на их сверхпроводниковом процессоре Willow, свидетельствуют о значительном прогрессе в направлении практических квантовых вычислений. В их реализации использовались два запоминающих устройства на основе поверхностного кода, включая 101-кубитный код с расстоянием 7 и код с расстоянием 5 с декодированием в реальном времени. Эти реализации позволили достичь ключевых результатов, таких как подавление логических ошибок в 2,14 раза, увеличение времени жизни по сравнению с лучшим физическим кубитом и задержка декодирования в реальном времени, превышающая миллион циклов. [1]

В качестве теста производительности процессора Willow использовался эталонный тест Random Circuit Sampling (RCS). RCS, изначально разработанный Google, стал стандартом для оценки квантовых вычислительных возможностей. Однако, несмотря на установление нового рубежа в квантовом превосходстве, практическая полезность RCS остается ограниченной, что подчеркивает необходимость разработки значимых, прикладных задач для квантовых вычислений. [2]

В отличие от этого, недавние разработки в области квантового отжига продемонстрировали превосходство в решении практических задач. 1 марта 2024 года компания D-Wave объявила о достижении вычислительного превосходства в квантовом моделировании с использованием квантового отжига. Они продемонстрировали, что сверхпроводниковые квантовые отжигатели могут быстро генерировать выборки, соответствующие решениям уравнения

1 Холодов Ярослав Александрович, д.ф.-м.н., профессор, главный научный сотрудник Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Университет «Сириус», Федеральная территория «Сириус», Россия. ORCID: https://orcid.org/0000-0003-2466-1594. Scopus Author ID: 6602420821. E-mail: kholodov.ya@talantiuspeh.ru

2 Саллум Хади, АНО ВО «Университет Иннополис», г. Иннополис, научный центр информационных технологий и искусственного интеллекта АНОО ВО «Университет «Сириус», Федеральная территория «Сириус», Россия. E-mail: h.salloum@innopolis.ru. ORCID: https://orcid.org/ 0009-0005-6068-0532.

3 Агапова Наталья Аркадьевна, АНО ВО «Университет Иннополис», г. Иннополис, E-mail: agapnatalya004@mail.ru

Шрёдингера. В частности, было продемонстрировано масштабирование закона площади запутанности при резких изменениях двух-, трех и бесконечномерных спин-стекол. Кроме того, анализ приближенных классических методов, основанных на тензорных сетях и нейронных сетях, показал, что ни один из известных классических подходов не достигает той же точности, что и квантовый отжигатель, в разумные сроки. Эти результаты подчеркивают способность квантового отжига решать практически значимые задачи, остающиеся недоступными для классических вычислительных методов. [3]

Основным принципом компании D-Wave всегда было создание квантовых вычислительных инструментов для решения сложных задач, а не немедленное стремление к универсальным квантовым вычислениям. Этот подход остается актуальным. Хотя алгоритм Шора — известный квантовый алгоритм для разложения целых чисел на множители — пока не смог успешно разложить число с использованием квантовых компьютеров на логических вентилях, квантовый отжиг уже позволил факторизовать числа до определенного масштаба. Это естественным образом поднимает важный вопрос: можно ли использовать квантовый отжиг для взлома шифрования RSA?

В данной работе представлен краткий обзор квантового отжига и различных подходов к решению задачи разложения на простые множители [4,5,6,7], которая лежит в основе шифрования RSA.

Квантовый отжиг: краткий обзор

Квантовый отжиг — это парадигма квантовых вычислений, основанная на оптимизации, которая использует квантовые флуктуации для нахождения основного состояния заданного гамильтониана. В отличие от квантовых вычислений на логических вентилях, которые опираются на унитарные операции, квантовый отжиг следует процессу адиабатической эволюции, постепенно преобразуя начальный тривиальный гамильтониан в гамильтониан, специфичный для решаемой задачи. Финальное состояние системы соответствует оптимальному решению исходной задачи оптимизации [8,9].

Основной принцип работы квантового отжига основан на **адиабатической теореме квантовой механики**, которая утверждает, что квантовая система, изначально находящаяся в основном состоянии, останется в этом состоянии, если гамильтониан изменяется достаточно медленно. Это свойство позволяет квантовому отжигу эффективно решать задачи комбинаторной оптимизации, включая разложение целых чисел на простые множители, путем кодирования задачи в энергетический ландшафт, где основное состояние представляет правильное решение факторизации.

Чтобы формализовать этот процесс, система начинает с начального гамильтониана H_0, где кубиты подготавливаются в состоянии суперпозиции:

$$H_0 = -\sum_i \sigma_x^{(i)}, \quad (1)$$

где $\sigma_x^{(i)}$ – оператор Паули-X, действующий на i-й кубит. Это гарантирует, что каждый кубит находится в равновероятной суперпозиции состояний $|0\rangle$ и $|1\rangle$, что означает отсутствие закодированной информации в системе на начальном этапе.

По мере продвижения процесса отжига гамильтониан системы постепенно трансформируется в гамильтониан, специфичный для данной задачи H_f:

$$H(t) = [1 - a(t)]H_0 + a(t)H_p, \quad (2)$$

где $a(t)$ – функция, изменяющаяся от 0 до 1 во времени, а H_p – конечный гамильтониан, соответствующий решаемой задаче. Обычно H_p представляется в форме модели Изинга:

$$H_p = -\sum_i h_i \sigma_z^{(i)} - \sum_{i<j} J_{i,j} \sigma_z^{(i)} \sigma_z^{(j)}, \quad (3)$$

где $\sigma_z^{(i)}$ – операторы Паули-Z, h_i – локальные магнитные поля, а $J_{i,j}$ – коэффициенты взаимодействия между кубитами.

В ходе процесса отжига квантовые флуктуации вызывают туннельные эффекты, которые помогают системе избегать локальных минимумов, в конечном итоге направляя её к глобальному минимуму H_p. По мере приближения $a(t)$ к 1 квантовые флуктуации подавляются, и система достигает классического представления модели Изинга, соответствующего оптимальному решению.

Подходы к решению задачи разложения на простые множители с помощью квантового отжига

Модель Изинга — это фундаментальная математическая модель, используемая в статистической механике для описания ферромагнетизма. Энергетический гамильтониан (или функция стоимости) формулируется следующим образом:

$$H(\sigma) = -\sum_{i=1} nh_i\sigma_i - \sum_{i<j} J_{i,j}\sigma_i\sigma_j, (4)$$

где $\sigma = (\sigma_1,...,\sigma_n)^T$, при этом $\sigma_i \in \{+1,-1\}$. Здесь σ_i представляет спин i-го кубита, а h_i и $J_{i,j}$ — коэффициенты, отвечающие за спины кубитов и их связи соответственно [?].

Альтернативно, задачу можно сформулировать как задачу QUBO (Quadratic Unconstrained Binary Optimization — квадратичная безусловная бинарная оптимизация). В этом представлении функция стоимости f определяется в n-мерном бинарном пространстве B^n следующим образом:

$$f(q) = q^T Q q, \quad (5)$$

где Q – верхнетреугольная матрица, а $q = (q_1,...,q_n)^T$ — бинарный вектор. Поскольку для бинарных переменных выполняется $q_i^2 = q_i$, функция стоимости может быть эквивалентно записана так:

$$f(q) = \sum_{i=1} nQ_{i,i}q_i + \sum_{i<j} Q_{i,i}q_iq_j. \quad (6)$$

Неизвестные переменные в модели Изинга (σ) и в модели QUBO (q) связаны между собой следующим образом:

$$\sigma = 2q - 1 \text{ или } q = \frac{1}{2}(\sigma + 1). \quad (7)$$

Предположим, что целое число N является произведением двух простых чисел p и q, рассмотрим следующую задачу наименьших квадратов:

$$\underset{p,q}{arg\,min}\ (pq - N)^2, \quad (8)$$

которая достигает минимального значения 0, когда $pq = N$.

Для удобства вычислений применим 2-норму:

$$\|pq - N\|^2 = p^2q^2 - 2pqN + N^2. \quad (9)$$

Модель HUBO

В формулировке HUBO (Higher-order Unconstrained Binary Optimization) для бинарной задачи наименьших квадратов числа p и q представлены в виде комбинаций кубитов $q_l \in \{0,1\}$. Их представления в системе счисления с основанием 2 записываются следующим образом:

$$p = \sum_{l=0}^{n-1} 2^l q_l,\ q = \sum_{l=0}^{n-1} 2^l q_{n+l}. \quad (10)$$

Это представление позволяет подставить эти выражения в формулировку задачи наименьших квадратов, тем самым генерируя суммируемые члены для функции стоимости. Например, первый член в уравнении (6) принимает вид:

$$(\sum_{l=0}^{n-1} 2^l\, q_l)^2\, (\sum_{l=0}^{n-1} 2^l\, q_{n+l})^2, \quad (11)$$

которое затем расширяется и упрощается с учетом того, что $q_l^2 = q_l$.

Модель QUBO

Поскольку модель HUBO для разложения на простые множители содержит квадратичные, кубические и квартные (четвертой степени) члены, необходимо преобразовать не квадратичные (высшей степени) полиномы в формулировку QUBO.

Члены вида $cxyz$ (где c - оэффициент) заменяются на квадратичные члены путем введения вспомогательного кубита w. В частности, для всех $x,y,z \in \{0,1\}$ можно преобразовать $cxyz$ в комбинацию линейных и квадратичных членов, тем самым упростив его интеграцию в QUBO-модель.

Аналогично, квартные члены можно свести к более простым выражениям, вводя дополнительные переменные (например, для каждого квартного члена требуется ввести семь новых кубитов $x_1,x_2,...,x_7$).

Модель HUBO с алгоритмом гамильтониана, зависящего от диапазона

Недавно был предложен алгоритм гамильтониана, зависящего от диапазона (range-dependent Hamiltonian algorithm) [10]. Этот алгоритм делит область на подрегионов, которые могут быть представлены желаемым количеством кубитов. Применяя этот алгоритм, p и q могут быть выражены следующим образом:

$$p \approx \sum_{l=0}^{n-1} 2^l q_l + S_i, \text{ и } q \approx \sum_{l=0}^{n-1} 2^l q_{n+l} + S_j, \quad (12)$$

где S_i и S_j – это целые числа, регулирующие представление.

Чтобы вывести модель HUBO, подставим уравнение (1) в функцию стоимости наименьших квадратов:

$$p^2q^2 - S_i^2S_j^2 = (\sum_{l=0}^{n-1} 2^l q_l + S_i)^2 (\sum_{l=0}^{n-1} 2^l q_{n+l} + S_j)^2 - S_i^2S_j^2. \quad (13)$$

После раскрытия скобок получаем ряд суммирующихся членов, соответствующих линейным, квадратичным, кубическим и квартным взаимодействиям. Например, линейные члены выглядят так:

$$\sum_{l=0}^{n-1} [(2^{2l} + 2^{l+1}S_i)S_j^2q_l + (2^{2l} + 2^{l+1}S_i)S_j^2q_{n+l}], \quad (14)$$

И аналогичные расширения для квадратичных и более высоких порядков.

Полная модель HUBO получается путем комбинирования этих расширений со вторым членом выражения наименьших квадратов:

$$-2pqN = -2N(\sum_{l=0}^{n-1} 2^l q_l + S_i)(\sum_{l=0}^{n-1} 2^l q_{n+l} + S_j) + 2NS_iS_j. \quad (15)$$

Таким образом, глобальная минимальная энергия, которую нужно получить, равна:

$$-N^2 - S_i^2S_j^2 + 2NS_iS_j. \quad (16)$$

Метод модульного локально-структурированного встраивания

Подведем итог концепциям из [4,7]. Задача разложения на простые множители (PF) для числа N может быть решена с помощью решателей SAT путем кодирования умножителя размером $n \times m$ в булевую формулу и фиксации значений выходных битов, чтобы представить N. В [7] была представлена модульная инкапсуляция бинарного умножителя в архитектуру Pegasus QA, основанная на локально-структурированном встраивании задач SAT.

Цепочка умножителя представлена как конъюнкция логических функций Controlled Full-Adder (CFA), связанных эквивалентностями между переменными. Каждый CFA встраивается в 8-кубитный модуль с эквивалентностями переменных, реализуемыми через цепочки. Каждый CFA $F(x)$ кодируется через штрафную функцию:

$$P_F(z - x,a|\theta)\theta_0 + \sum_{z_i \in V} \theta_i z_i + \sum_{(z_i,z_j)\in E, i<j} \theta_{ij} z_i z_j, \quad (17)$$

где $z_i \in \{-1,1\}$, и при этом выполняется ограничение:

$$\begin{cases} PF(x,a|\theta) = 0 \text{ если } F(x) = \top, \\ PF(x,a|\theta) \geq g_{min} \text{ если } F(x) = \bot. \end{cases} \quad (18)$$

Здесь булевы переменные x и вспомогательные переменные a отображаются на подмножество $z \subset V$ кубитов в топологическом графе (V,E), где значения кубитов $\{1,-1\}$ соответствуют значениям истинности $\{\top,\bot\}$, соответственно. Параметры θ_0, θ_i, θ_{ij} и g_{min} — это сдвиг, смещения, связи и зазор соответственно. Стоит отметить, что смещения и связи имеют ограниченные диапазоны (например, смещения в $[-4,+4]$ и связи в $[-2,+1]$), в то время как сдвиг не ограничен. Вспомогательные переменные a включаются для решения задач с избыточным кодированием. Штрафная функция для всего умножителя строится как сумма штрафных функций для отдельных CFA, а также дополнительные члены, такие как $(2 - 2zz')$ для каждой цепочки $\langle z,z' \rangle$.

Итоговая штрафная функция подается в отжигатель, при этом выходные кубиты фиксируются, чтобы представить число N, с соответствующей инициализацией (например, принудительное значение для кубита carry-in самого правого CFA в каждой строке и кубита in2 для CFA в первой строке, равное -1). Если отжигатель находит основное состояние, для которого штрафная функция равна нулю, то значения кубитов представляют собой валидное решение задачи разложения на простые множители.

Метод модифицированной таблицы умножения

Этот подход основывается на модифицированной таблице умножения, которая уменьшает диапазон значений параметров Изинга, используемых как коэффициенты для локальных полей и взаимодействий. Этот метод также минимизирует количество переменных переноса, устраняя необходимость в обширной предварительной обработке. Метод модифицированной таблицы умножения выполняет локальные минимизации по произведению отдельных бинарных подстрок, представляющих числа p и q. Таблица умножения делится на несколько блоков, каждый из которых можно оптимизировать независимо. Размер блока можно выбрать таким образом, чтобы сбалансировать желаемый диапазон параметров и количество переменных.

Например, рассмотрим иллюстративный случай, где $N = 143$, $p = 13$ и $q = 11$. В предыдущих подходах система уравнений строилась из каждого столбца (или частичных столбцов) таблицы умножения, при этом каждое уравнение учитывало один или несколько битов переноса. В нашем подходе таблица умножения делится на блоки, требующие переносов только между блоками. Это значительно сокращает общее количество переносов и соответствующее количество переменных.

Как показано в Таблице 1 для $N = 143$, вводятся два набора битов переноса, обозначаемых $c_i \in \{0,1\}$. Двухбитовые числа $(c_2c_1)_2 = 2c_2 + c_1$ и $(c_4c_3)_2 = 2c_4 + c_3$ представляют биты переноса для каждого блока. В этой формулировке суммы вычисляются по четырёхбитным числам, при этом сложение внутри каждого блока выполняется по двухбитным числам. Полученная система уравнений, выведенная из таблицы умножения, записывается следующим образом:

$$\begin{aligned} (p_2 + p_1q_1 + q_2) \times 2 + (p_1 + q_1) &= c_2 \times 2^3 + c_1 \times 2^2 + (11)^2 \\ &= c_2 \times 8 + c_1 \times 4 + 3 \\ (q_1 + p_2q_2 + p_1 + c_2) \times 2 + (1 + p_2q_1 + p_1q_2 + 1 + c_1) &= c_4 \times 2^3 + c_3 \times 2^2 + (01)_2 \\ &= c_4 \times 8 + c_3 \times 4 + 1 \\ (1 + c_4) \times 2 + (q_2 + p_2 + c_3) &= (100)_2 \\ &= 4. \end{aligned}$$

Метод модифицированной таблицы умножения устраняет необходимость в бите переноса в каждом столбце, вычисляя переносы только внутри блоков, что значительно снижает общую вычислительную сложность. В предельных случаях восстанавливается обычная таблица умножения при использовании одного столбца на блок, а прямой метод восстанавливается при использовании одного уравнения. Вместо того, чтобы заставлять сумму каждого столбца совпадать с каждым битом числа, которое нужно разложить на множители (как в обычных методах), модифицированный подход заставляет каждый блок таблицы умножения равняться соответствующему блоку числа N. Это приводит к положительной штрафной функции вида:

$$\begin{aligned} f(p,q,c) = {} & (2p_2 + 2p_1q_1 + 2q_2 - 8c_2 - 4c_1 + p_1 + q_1 - 3)^2 \\ & + (2q_1 + 2p_2q_2 + 2p_1 + 2c_2 - 8c_4 - 4c_3 + p_2q_1 + p_1q_2 + c_1 + 1)^2 \\ & + (q_2 + p_2 + c_3 + 2c_4 - 2)^2. \end{aligned}$$

После расширения и упрощения, используя свойство $x^2 = x$ для $x \in \{0,1\}$, получаются кубические и более высокие порядки, которые затем сводятся к квадратичной форме через введение вспомогательных переменных. Например, квадратирование отрицательных членов выполняется аналогично позиционным членам, как подробно описано в дополнительном материале. Для $N = 143$ эта процедура в конечном итоге приводит к соответствующим параметрам для гамильтониана Изинга.

Экспериментальные результаты для случайных чисел

Для проверки описанных методик мы провели серию экспериментов на случайных двуделимых числах. Экспериментальный протокол включал следующие шаги:

1. Генерация случайных двуделимых чисел в заранее определённом диапазоне.
2. Формулировка соответствующей задачи разложения на простые множители как для моделей HUBO, так и для моделей QUBO.
3. Встраивание полученной задачи в квантовый отжигатель с использованием трёх различных методов:
   - Алгоритм зависимого от диапазона гамильтониана;
   - Модифицированный метод таблицы умножения;
   - Модульный метод локально-структурного встраивания.
4. Проведение процесса отжига на доступном оборудовании и сравнение результатов с классическими алгоритмами разложения на множители.

Квантовый отжигатель успешно определил простые множители для следующих двуделимых чисел, используя все три метода:

Таблица 1.

Результаты разложения для случайно выбранных двуделимых чисел с использованием всех трёх методов

Двупростое число	Простые множители	Гамильтонов метод	Табличный метод	Модульный метод
323	17*19	✓	✓	✓
437	19*23	✓	✓	✓
667	23*29	✓	✓	✓
899	29*31	✓	✓	✓
1081	31*37	✓	✓	✓
1619	37*43	✓	✓	✓

Эти результаты подтверждают эффективность подхода квантового отжига для разложения двуделимых чисел в пределах тестируемого диапазона. Успех всех трёх методов подчеркивает их согласованность в правильной идентификации простых множителей. Кроме того, эксперименты выявляют компромисс между количеством введённых переменных (например, вспомогательных кубитов) и точностью значений коэффициентов в модели Изинга. Модульный метод локально-структурного встраивания демонстрирует улучшенную масштабируемость и эффективность встраивания, что делает его перспективным кандидатом для более крупных задач. Эти результаты поддерживают дальнейшее масштабирование подхода по мере развития квантового оборудования.

Выводы

В этой статье представлен подробный обзор квантового отжига и его применения к разложению на простые множители. Мы рассмотрели несколько методов, включая формулировки HUBO и QUBO, алгоритм зависимого от диапазона гамильтониана, методы модульного локально-структурного встраивания и модифицированный метод таблицы умножения. Эти подходы предлагают перспективные пути для использования квантового отжига в решении задач, которые классически являются неразрешимыми, таких как взлом шифрования RSA. Первоначальные эксперименты с случайными двуделимыми числами дополнительно подтверждают осуществимость этих методов, с многообещающими результатами, полученными на текущем квантовом отжигательном оборудовании. В дальнейшем работа будет направлена на масштабирование этих техник для более крупных чисел, улучшение эффективности уменьшения вспомогательных переменных и усовершенствование стратегий встраивания для дальнейшего повышения производительности квантовых отжигателей.

Результаты получены при финансовой поддержке проекта «Технологии противодействия ранее неизвестным квантовым киберугрозам», реализуемого в рамках государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус» (Соглашение №23-03 от 27.09.2024 г.)

Литература

1. Google Quantum AI and Collaborators. (2024). Quantum error correction below the surface code threshold. Nature. https://doi.org/10.1038/s41586-024-08449-y.
2. Coenen, C., Grinbaum, A., Grunwald, A., Milburn, C., & Vermaas, P. (2022). Quantum technologies and society: Towards a different spin. NanoEthics, 16, 1–6. https://doi.org/10.1007/s11569-021-00409-4.
3. King, A. D., Nocera, A., Rams, M. M., Dziarmaga, J., Wiersema, R., Bernoudy, W., Raymond, J., Kaushal, N., Heinsdorf, N., Harris, R., Boothby, K., Altomare, F., Berkley, A. J., Boschnak, M., Chern, K., Christiani, H., Cibere, S., Connor, J., Dehn, M. H., ... Amin, M. H. (2024, March 1). Computational supremacy in quantum simulation [Preprint]. arXiv. https://doi.org/10.48550/arXiv:2403.00910v1.
4. Ding, J., Spallitta, G., & Sebastiani, R. (2024). Experimenting with D-Wave quantum annealers on prime factorization problems. Frontiers in Computer Science, 6. https://doi.org/10.3389/fcomp.2024.1335369.
5. Jun, K., & Lee, H. (2023). HUBO and QUBO models for prime factorization. Scientific Reports, 13, 10080. https://doi.org/10.1038/s41598-023-36813-x.

6. Jiang, S., Britt, K. A., McCaskey, A. J., Humble, T. S., & Kais, S. (2018). Quantum annealing for prime factorization. Scientific Reports, 8, 17667. https://doi.org/10.1038/s41598-018-36058-z.
7. Ding, J., Spallitta, G., & Sebastiani, R. (2024). Effective prime factorization via quantum annealing by modular locally-structured embedding. Scientific Reports, 14, 3518. https://doi.org/10.1038/s41598-024-53708-7.
8. Salloum, H., Sabbagh, K., Savchuk, V., Lukin, R., Orabi, O., & Isangulov, M. (2025). Performance of quantum annealing machine learning classification models on ADMET datasets. IEEE Access, 13, 16263–16287. https://doi.org/10.1109/ACCESS.2025.3531391.
9. Neukart, F., Compostella, G., Seidel, C., von Dollen, D., Yarkoni, S., & Parney, B. (2017). Traffic flow optimization using a quantum annealer. Frontiers in ICT, 4, 29. https://doi.org/10.3389/fict.2017.00029.
10. Lee, H., & Jun, K. (2022, February 15). Range dependent Hamiltonian Algorithm for numerical QUBO formulation [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2202.07692v1.

QUANTUM ANNEALING APPROACHES TO BREAKING RSA ENCRYPTION

Kholodov Y. A.[4], Salloum H.[5], Agap N. A.[6]

Keywords: *Quantum Annealing, RSA, QUBO, Prime Factorization.*

Objective: *to study the transformational potential of quantum annealing in solving the problem of simple factorization.*

Research method(s): *the approach includes a comprehensive review of recent experimental breakthroughs and theoretical innovations. In particular, we analyze techniques such as surface code memory, HUBO and QUBO formulations, range-dependent Hamiltonian algorithms, modular locally structured embedding methods, and a modified multiplication table method random number.*

Research Output(s): *the study evaluates the application of quantum annealing to factorization of primes, showing that advanced problem mapping techniques, such as the HUBO and QUBO formulations, significantly improve the efficiency of representing complex factorization problems on quantum hardware. Notably, the inclusion of surface code memory increases the stability of qubit states during annealing, reducing errors and improving computational accuracy It also demonstrates that Hamiltonian's range-dependent algorithms and modular, locally structured embedding methods help optimize qubit interaction, enabling a more accurate factorization process. A modified multiplication table method is presented, providing an optimized computational strategy, especially effective for large composite numbers. Preliminary experiments with random numbers confirm the theoretical conclusions, indicating that these integrated methods allow for better performance than traditional approaches. Taken together, the results highlight the potential of quantum annealing as a solid foundation for solving complex cryptographic problems and lay the foundation for future research into scalable quantum algorithms and hardware implementations.*

Scientific novelty: *the work combines several advanced quantum annealing techniques for factorization of prime numbers, combining experimental innovations with theoretical developments to propose a new framework that improves the efficiency of cryptographic computing.*

References

1. Google Quantum AI and Collaborators. (2024). Quantum error correction below the surface code threshold. Nature. https://doi.org/10.1038/s41586-024-08449-y.
2. Coenen, C., Grinbaum, A., Grunwald, A., Milburn, C., & Vermaas, P. (2022). Quantum technologies and society: Towards a different spin. NanoEthics, 16, 1–6. https://doi.org/10.1007/s11569-021-00409-4.
3. King, A. D., Nocera, A., Rams, M. M., Dziarmaga, J., Wiersema, R., Bernoudy, W., Raymond, J., Kaushal, N., Heinsdorf, N., Harris, R., Boothby, K., Altomare, F., Berkley, A. J., Boschnak, M., Chern, K., Christiani, H., Cibere, S., Connor, J., Dehn, M. H., ... Amin, M. H. (2024, March 1). Computational supremacy in quantum simulation [Preprint]. arXiv. https://doi.org/10.48550/arXiv:2403.00910v1.
4. Ding, J., Spallitta, G., & Sebastiani, R. (2024). Experimenting with D-Wave quantum annealers on prime factorization problems. Frontiers in Computer Science, 6. https://doi.org/10.3389/fcomp.2024.1335369.
5. Jun, K., & Lee, H. (2023). HUBO and QUBO models for prime factorization. Scientific Reports, 13, 10080. https://doi.org/10.1038/s41598-023-36813-x.
6. Jiang, S., Britt, K. A., McCaskey, A. J., Humble, T. S., & Kais, S. (2018). Quantum annealing for prime factorization. Scientific Reports, 8, 17667. https://doi.org/10.1038/s41598-018-36058-z.
7. Ding, J., Spallitta, G., & Sebastiani, R. (2024). Effective prime factorization via quantum annealing by modular locally-structured embedding. Scientific Reports, 14, 3518. https://doi.org/10.1038/s41598-024-53708-7.

4 Yaroslav A. Kholodov, Doctor of physico-mathematical sciences, Professor, Chief Researcher of Scientific Center of Information Technologies and Artificial Intelligence of Sirius University of Science and Technology, Sirius Federal Territory Sirius University of Science and Technology. ORCID: https://orcid.org/0000-0003-2466-1594. Scopus Author ID: 6602420821. E-mail: kholodov.ya@talantiuspeh.ru

5 Sallum Hadi, Innopolis University, Innopolis, Scientific Center for Information Technologies and Artificial Intelligence, Sirius University, Sirius Federal Territory, Russia. E-mail: h.salloum@innopolis.ru. ORCID: https://orcid.org/ 0009-0005-6068-0532.

6 Natalia A. Agapova, Innopolis University, Innopolis, Sirius Federal Territory, Russia. E-mail: agapnatalya004@mail.ru

8. Salloum, H., Sabbagh, K., Savchuk, V., Lukin, R., Orabi, O., & Isangulov, M. (2025). Performance of quantum annealing machine learning classification models on ADMET datasets. IEEE Access, 13, 16263–16287. https://doi.org/10.1109/ACCESS.2025.3531391.
9. Neukart, F., Compostella, G., Seidel, C., von Dollen, D., Yarkoni, S., & Parney, B. (2017). Traffic flow optimization using a quantum annealer. Frontiers in ICT, 4, 29. https://doi.org/10.3389/fict.2017.00029.
10. Lee, H., & Jun, K. (2022, February 15). Range dependent Hamiltonian Algorithm for numerical QUBO formulation [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2202.07692v1.