SCIENCE CHINA
Information Sciences

• LETTER •

February 2025, Vol. 68, Iss. 2, 129501:1–129501:2
https://doi.org/10.1007/s11432-024-4163-6

# Quantum attack on RSA by D-Wave Advantage: a first break of 80-bit RSA

Chunlei HONG[1,2], Zhi PEI[1,2], Qidi WANG[1,2], Shuxiao YANG[1,2], Jingjing YU[1,2] & Chao WANG[1,2*]

[1]*School of Communication and Information Engineering, Shanghai University, Shanghai 200444, China*
[2]*Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Shanghai 200444, China*

Received 28 February 2024/Revised 27 May 2024/Accepted 10 September 2024/Published online 17 January 2025

**Citation** Hong C L, Pei Z, Wang Q D, et al. Quantum attack on RSA by D-Wave Advantage: a first break of 80-bit RSA. Sci China Inf Sci, 2025, 68(2): 129501, https://doi.org/10.1007/s11432-024-4163-6

RSA [1], a cryptographic system essential for securing network communications, relies on the difficulty of factorizing an integer into two primes (factorizing an integer $N = P \times Q$, where $P$ and $Q$ are prime numbers). In theory, quantum computers can factorize RSA integers in polynomial time. However, under the current limitations of quantum hardware, the practical ability of quantum algorithms to attack RSA remains unsatisfactory. In this study, we combine the advantages of quantum and classical computing, employing a hybrid architecture of quantum computing and classical algorithms to attack RSA. Based on the D-Wave Advantage quantum computer, we successfully conducted an attack on RSA with up to 80-bit, significantly improving the experimental indicators for quantum computing attacks on RSA.

The core algorithm of D-Wave quantum computer, quantum annealing algorithm [2], is an optimization algorithm with quantum tunneling effect. It can escape the local minima that traditional intelligent algorithms frequently fall into, and approach the global minimum quickly. In this study, we leverage the quantum annealing algorithm to explore problems within exponential solution spaces, thereby improving the Babai algorithm [3] for solving the closest vector problem (CVP). It yielded superior solutions compared to the Babai algorithm, enhanced the search efficiency for smooth pairs, and consequently accelerated the integer factorization of RSA.

*The framework of integer factorization.* The hybrid framework, combining quantum annealing and classical algorithms for integer factorization, is shown in Figure 1. The core innovation involves the tunneling effect of quantum annealing to improve Babai's algorithm for solving the CVP, thereby accelerating the factorization of RSA integers. Next, we introduce the process of integer factorization in our framework through three stages.

• The relationship between the solution quality of CVP and smooth pairs.

In this study, finding smooth pairs is a crucial and time-consuming step in the factorization of RSA integers. Therefore, optimizing the search algorithm for smooth pairs can significantly accelerate the factorization process. In the following, we will present the definition of smooth pairs.

**Smooth pair:** Let $p_1, p_2, ..., p_n$ be the smallest $n$ primes. An integer $u$ is $p_n$-smooth if it can be expressed as $u = \prod_{i=1}^{n} p_i^{e_i}$, where $e_i \geqslant 0$. A relation pair $(u, v)$ is $p_n$-smooth if both $u$ and $v$ are $p_n$-smooth. If $u$ is $p_n$-smooth and $v$ is $p'_n$-smooth, then $(u, v)$ is called $p_{n,n'}$-smooth.

The integer factorization problem can be expressed as a CVP of finding a target vector consisting of integers $N$. Assuming that there exists a set of integer $e_i$ that satisfies the following conditions:

$$\varphi := \left| \sum_{i=1}^{m} e_i \ln p_i - \ln N \right| \approx 0.$$

To facilitate computational, $u$ and $v$ can be characterized by the following mathematical expression:

$$u = \prod_{e_i \geqslant 0}^{m} p_i^{e_i}, v = \prod_{e_i < 0}^{m} p_i^{-e_i}.$$

Subsequently, it can be derived through analysis:

$$\left| \ln \left( \frac{u}{vN} \right) \right| = \varphi.$$

According to the Taylor's theorem, we can obtain $u - vN = vN\left(e^{\varphi} - 1\right) \approx \varphi vN$. If $\varphi$ is smaller, then $u - vN$ is also smaller, making it more probable that $(u, |u - vN|)$ will be a smooth pair. As a result, the higher the quality of the solution to the CVP, the greater the probability of it being identified as a smooth pair.

• Optimizing CVP solutions by quantum annealing algorithm.

Given a lattice $\mathcal{L}(\boldsymbol{B}_n) \in \mathbb{R}^{n+1}$ and the corresponding target vector $\mathbf{T} \in \mathbb{R}^{n+1}$. Assuming that $\boldsymbol{B}_n = [\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n] \in \mathbb{R}^{n+1,n}$ is an initial lattice basis, the LLL algorithm [4] is applied to obtain an approximately orthogonal lattice basis $\boldsymbol{D}_n = [\boldsymbol{d}_1, \cdots, \boldsymbol{d}_n] \in \mathbb{R}^{n+1,n}$. Subsequently, the Schmit orthogonalized vector $\widehat{\boldsymbol{D}}_n = \left[\widehat{\boldsymbol{d}}_1, \cdots, \widehat{\boldsymbol{d}}_n\right] \in \mathbb{R}^{n+1,n}$ can be calculated. Furthermore, we can use the Babai algorithm to

* Corresponding author (email: wangchao@shu.edu.cn)

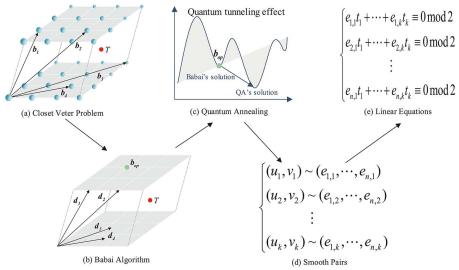


**Figure 1** (Color online) The hybrid architecture combining quantum annealing and classical algorithms for integer factorization.

find $\boldsymbol{b} \in \mathcal{L}(\boldsymbol{B}_n)$ that is closest to the target vector $\boldsymbol{T}$. It can be expressed as $\boldsymbol{b} = \sum_{i=1}^{n} k_i \boldsymbol{d}_i$, where $k_i = \lceil u_i \rfloor = \left\lceil \left\langle \boldsymbol{d}, \widehat{\boldsymbol{d}}_i \right\rangle, \left\langle \widehat{\boldsymbol{d}}_i, \widehat{\boldsymbol{d}}_i \right\rangle \right\rfloor$.

From the above formula, it is observed that the value of $k_i$ is obtained by rounding the value of $u_i$ in one direction, which means that the quality of vector $\boldsymbol{b}$ cannot be guaranteed. Therefore, considering both rounding up and rounding down $u_i$ simultaneously may yield a higher-quality solution. However, it would increase the computational complexity of classical computing exponentially. In order to solve this problem, we exploit the superposition effect of qubits to encode the coefficient values obtained by rounding up and down at the same time, thus constructing a lattice vector $\boldsymbol{b}_{new}$ that is closer to the target vector $\boldsymbol{T}$:

$$\boldsymbol{b}_{new} = \sum_{i=1}^{n} (k_i + x_i)\, \boldsymbol{d}_i = \sum_{i=1}^{n} x_i \boldsymbol{d}_i + \boldsymbol{b},$$

where $x_i \in \{0, 1, -1\}$. The Euclidean distance between $\boldsymbol{b}_{new}$ and the target vector $\boldsymbol{T}$ can be expressed as the function $F(x_1, \cdots, x_n)$:

$$F(x_1, \cdots, x_n) = \|\boldsymbol{T} - \boldsymbol{b}_{new}\|^2 = \left\| \boldsymbol{T} - \boldsymbol{b} - \sum_{i=1}^{n} x_i \boldsymbol{d}_i \right\|^2.$$

It can be observed that the smaller the value of $F(x_1, \cdots, x_n)$, the closer the vector $\boldsymbol{b}_{new}$ will be to the target vector $\boldsymbol{T}$. By mapping the variable $x_i$ to the Pauli matrix, the Hamiltonian function for $F(x_1, \cdots, x_n)$ can be constructed as follows:

$$H_b = \left\| \boldsymbol{T} - \boldsymbol{b} - \sum_{i=1}^{n} \widehat{x}_i \boldsymbol{d}_i \right\|^2 = \sum_{j=1}^{n+1} \left| \boldsymbol{N}_j - b_j - \sum_{i=1}^{n} \widehat{x}_i d_{i,j} \right|^2,$$

where $\widehat{x}_i \in \{0, 1, -1\}$ is a quantum operator mapped to the Pauli matrix according to the single qubit encoding rule. And it is determined by the value of orthogonal coefficients $u_i$ and $k_i$ in Babai algorithm, namely:

$$\hat{x}_i = \begin{cases} \left(I - \delta_z^i\right)/2, & \text{if } k_i \leqslant \mu_i; \\ \left(\delta_z^i - I\right)/2, & \text{if } k_i > \mu_i. \end{cases}$$

In this study, the quantum annealing algorithm is used to solve the Hamiltonian function $H_b$. This process can obtain a lattice vector $\boldsymbol{b}_{new}$, which may be closer to the target vector $\boldsymbol{T}$ than the Babai algorithm, thereby enhancing the probability of obtaining a smooth pair.

• Integer factorization.

Given a sufficient number of smooth pairs, we can construct a corresponding system of equations, which upon resolution yields a set of $n$ linearly dependent vectors. From these vectors, the relations $X^2 = \prod_{t_j=1}^{j\in\{1,\cdots,n'+2\}} u_j, Y^2 = \prod_{t_j=1}^{j\in\{1,\cdots,n'+2\}} |u_j - v_j N|$ can be established. Finally, we can factorize the integer $N$ into two primes $P$ and $Q$ by the condition $gcd(X \pm Y, N) \notin \{1, N\}$.

*Experimental results.* In this study, we used a random program to generate RSA integers ranging from 4-bit to 80-bit and conducted integer factorization experiments on these integers using the D-Wave Advantage_system4.1, equipped with a Pegasus topology of 5760 qubits. The default annealing schedule of [[0,0],[20,1]] was applied. Notably, we successfully factorized an 80-bit RSA integer: 1034879359475633166138643=1001721172891 × 1033101213673, which significantly exceeds the largest 48-bit RSA integer factorized in reference [5]. More experimental data and details are provided in Appendix B.

Ref. [5] employed the Quantum Approximate Optimization Algorithm (QAOA), based on the quantum gate model, for integer factorization. In contrast, we used the quantum annealing algorithm, which relies on quantum adiabatic evolution and significantly differs from QAOA in implementation and operation. Compared to this reference, our ability to factorize 80-bit RSA integers derives primarily from the following factors:

(1) Hardware conditions: The D-Wave Advantage, with over 5000 qubits, enhanced connectivity and improved error correction capabilities, enables the exploration of a larger solution space, making it better suited for solving complex problems.

(2) Annealing schedule: The D-Wave Advantage allows for flexibility in adjusting the annealing schedule to specific problem characteristics, enhancing the efficiency and accuracy of solving large-scale problems.

(3) Theoretical advantage: Quantum annealing leverages tunneling effects to escape local minima, increasing the likelihood of finding better solutions for complex problems.

*Conclusion.* In this study, we proposed a hybrid architecture that integrates quantum annealing with classical algorithms for integer factorization. Our framework enhanced the Babai algorithm's performance in solving the CVP, enabling it to search for smooth pairs with greater probability and higher efficiency, thus accelerating the factorization of RSA integers. Based on the D-Wave Advantage, our experimental results for RSA integer factorization far exceed those of other quantum computing attacks on RSA in the current public literature.

**Acknowledgements** We would like to express our gratitude to Academician Jianhua Zheng of the Chinese Academy of Sciences, and Qin Jing, Lan Luo and Bao Yan from the State Key Laboratory of Mathematical Engineering and Advanced Computing, for their guidance in the design of the algorithm architecture. This research was sponsored by CAAI-Huawei MindSpore Open Fund.

**Supporting information** Appendixes A and B. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

**References**

1 Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM, 1978, 21: 120–126
2 Finnila A B, Gomez M A, Sebenik C, et al. Quantum annealing: a new method for minimizing multidimensional functions. Chem Phys Lett, 1994, 219: 343
3 Babai L. On Lovasz' lattice reduction and the nearest lattice point problem. Combinatorica, 1986, 6: 1–13
4 Lenstra A K, Lenstra H W, Lovasz L. Factoring polynomials with rational coefficients. Math Ann, 1982, 261: 515–534
5 Yan B, Tan Z, Wei S, et al. Factoring integers with sublinear resources on a superconducting quantum processor. arXiv:2212.12372