QUANTUM COMPUTING AND QUANTUM INTERNET ay 2024 2025

Student

Lorenzo Menchini

Prof.

Luciano Lenzini

Leonardo Baciottini

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

INDEX

SHOR ALGORITHM

Shor's Algorithm is a quantum algorithm designed to efficiently factor large integers.
Classical factoring algorithms require exponential time, making factoring hard for very large numbers.
Shor's Algorithm solves this problem in polynomial time using quantum period finding.

General Number Field Sieve (GNFS)

$$\exp\left(\left(\frac{64}{9}\right)^{1/3}(\log N)^{1/3}(\log\log N)^{2/3}\right)$$

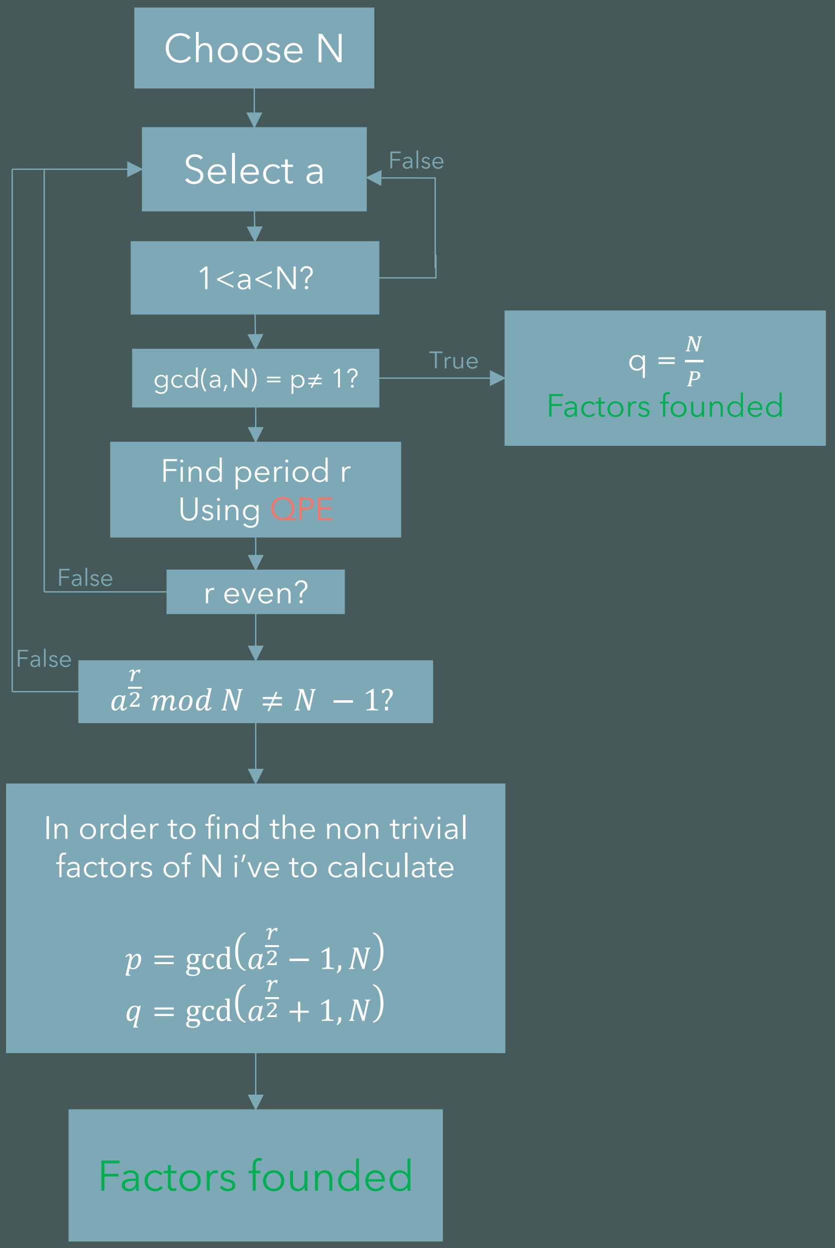
Sub-exponentia complexity

Shor algorithm

$$O((\log N)^3)$$

Polinomial complexity

ALGORITHM WORKFLOW



CIRCUIT IMPLEMENTATION:
Project requirements

Implementing Shor algorithm on Qiskit with $N = 21$:

choose 3 arbitrary values for a $(1<a<N)$ coprime with N and run the algorithm for each value

Evaluate on:
- a noiseless quantum simulator
- a real IBM quantum device

Performance metric: average number of quantum period finding shots required to successfully factor N

EXPERIMENTAL SETUP

- Phase register (m qubits)
- Working Register (n qubits)
- IQFT circuit
- U unitary gate
- Measuration for each qubit of the phase register

- Knowing that N=21 means that the working register must be of 5 qubits

- The values chosen for the experiment will be a = 2, 10, 19, all of them coprime with N

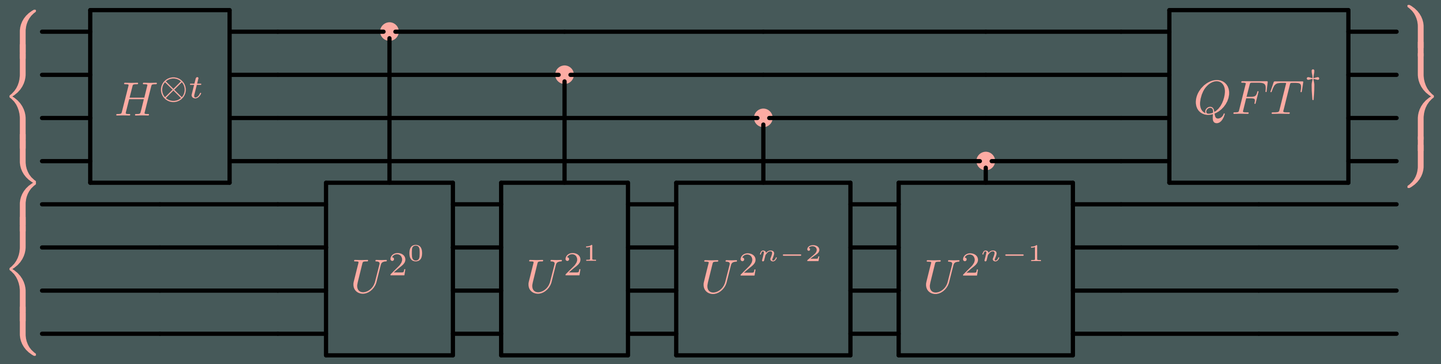
- The phase register has to be at least m = $\lfloor 2\log 2(N) \rfloor$ qubits, so i choose m = 10

Qiskit circuits

PHASE ESTIMATION CIRCUIT

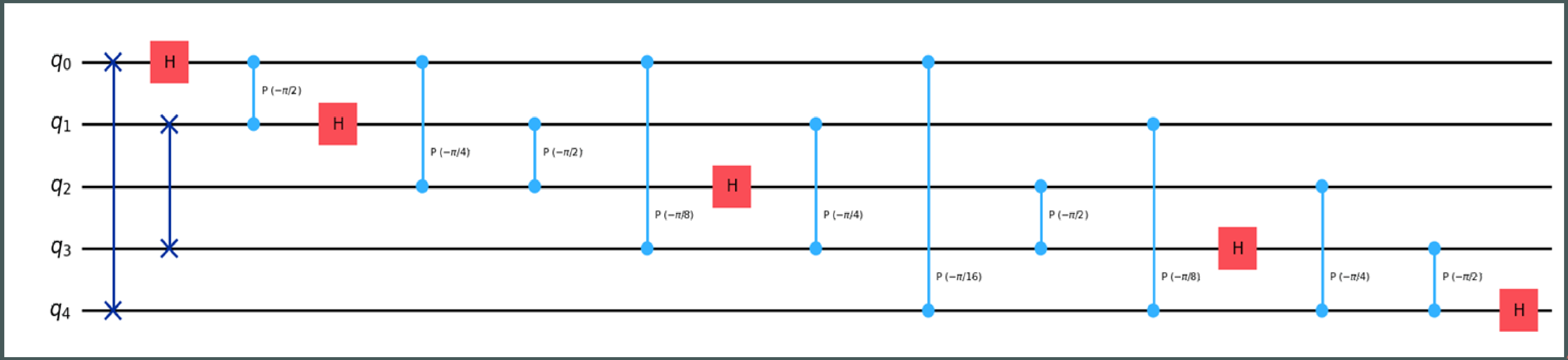
$|0\rangle$

$|1\rangle = \frac{1}{\sqrt{r}}(|u_0\rangle + |u_1\rangle + \cdots \cdots |u_{r-1}\rangle)$



$\frac{1}{\sqrt{r}}(|2^n \cdot \frac{1}{r}\rangle + |2^n \cdot \frac{2}{r}\rangle + \cdots \cdots |2^n \cdot \frac{r-1}{r}\rangle)$

IQFT



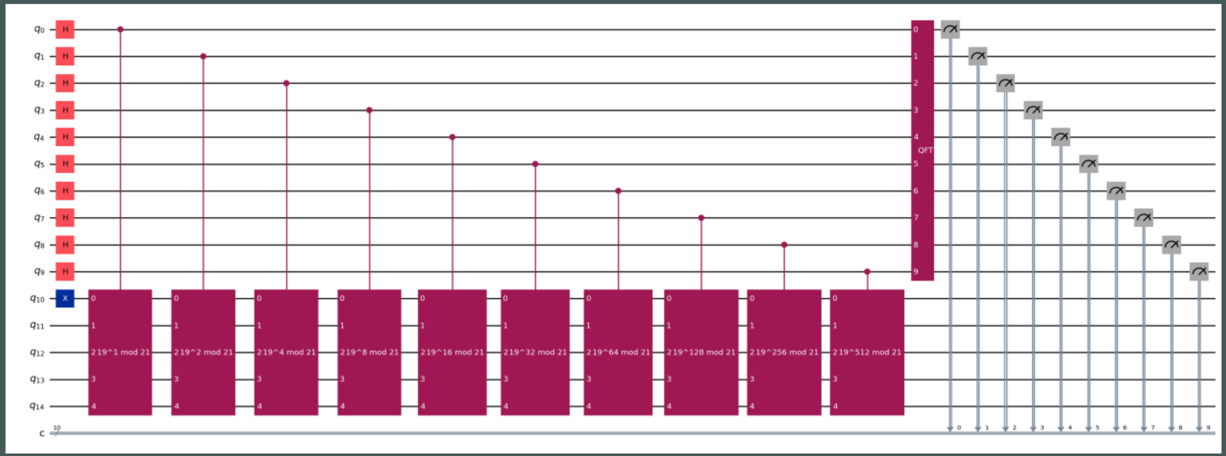
QPE CONSTRUCTION

In Shor is crucial the period finding, which is done
By appling the quantum phase estimation.
The period r is defined as the smallest r such as:

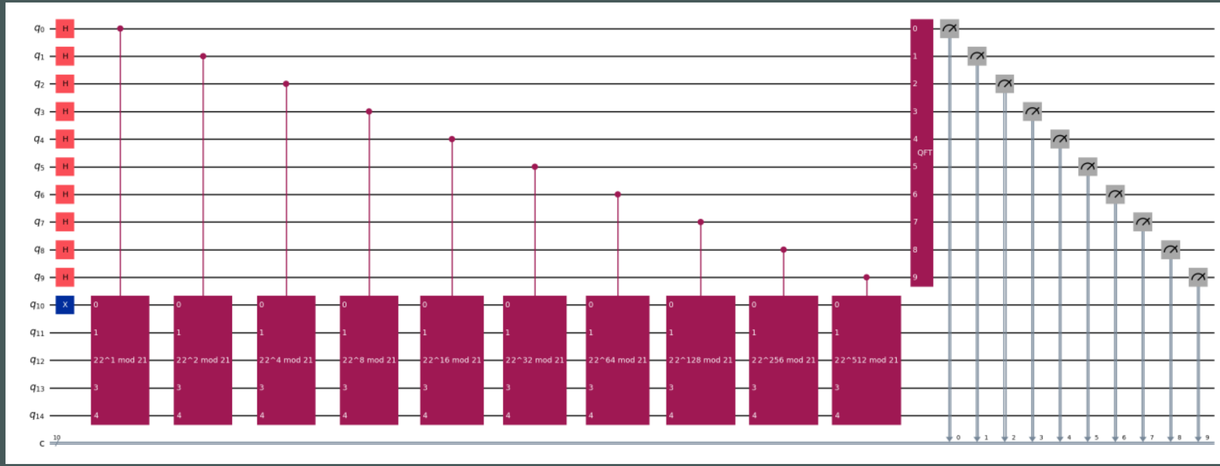
$$| a^r \ mod \ N \rangle = 1$$

To find it, we have to construct
- A state with non-zero overlap with the eigenstates of U ($|v_s\rangle$)
- A unitary operator U defined by modular multiplication
- A way to approximate the phase ϕ = r/s (using continue fraction)

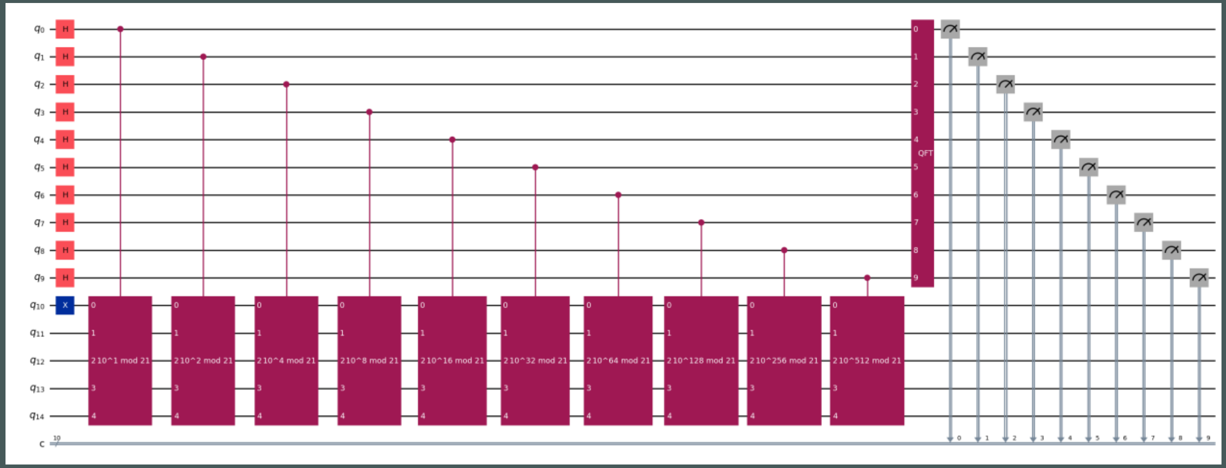
a = 2



a = 10



a = 19



$|v_s\rangle$

We can initialize the input with $|1\rangle$ (e.g., $|000\ldots1\rangle$), which has nonzero overlap with the eigenstates of Quantum interference and phase kickback encode the phase of the eigenvalue into the control register, allowing us to extract r.

U

To build the operator U, I generate a matrix that applies the modular multiplication
$|a^{power} y \; mod \; N\rangle$
acting unitarily only on the valid states y < N.
After measuring the control register,
I obtain a binary string that corresponds to an estimate of the phase ϕ = r/s.

r period approssimation

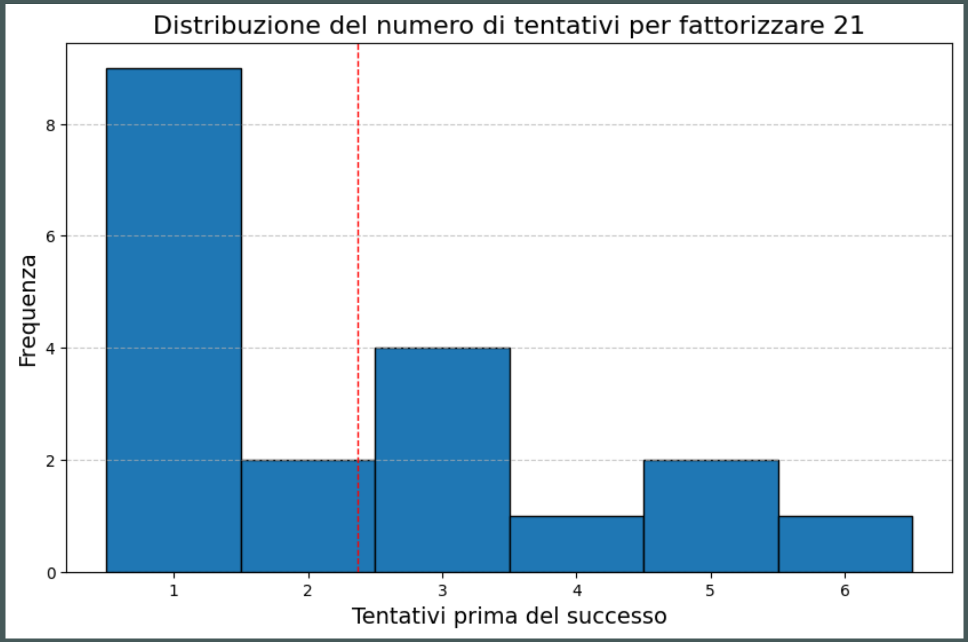
Using the continue fraction I can estimate s/r from the phase ϕ. Firstly I have to check if $\left|\frac{s}{r} - \phi\right| < \frac{1}{2r^2}$ and then I can find the convergent of the continuous fraction that fits with s/r (with r<N)

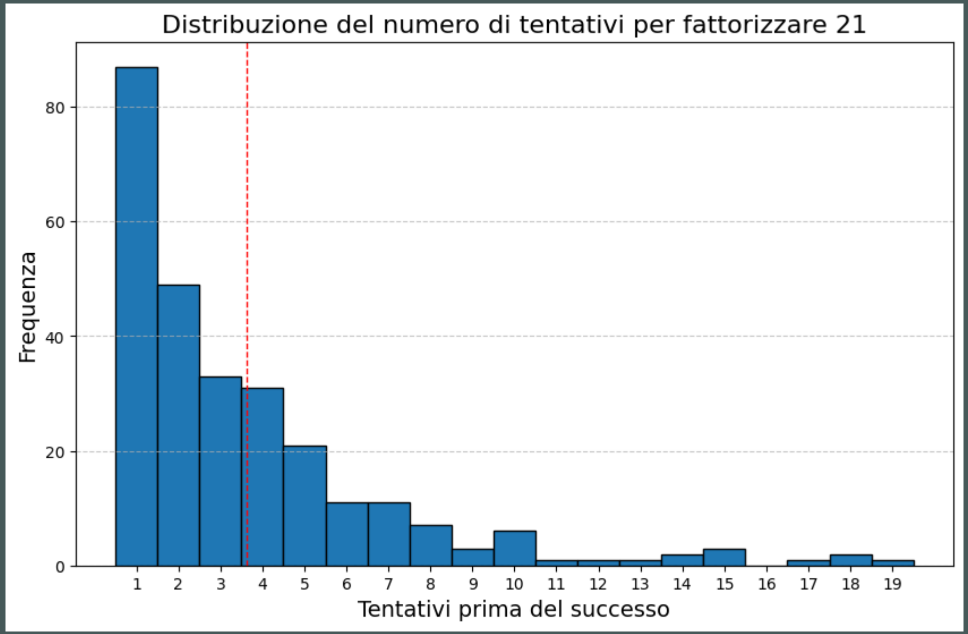
EVALUATION

Both for aerSimulation and IBM run we obtained the period r=6, as we can see:

a=2	a=10	a=19
$\lvert a^k \; mod \; N\rangle$ with k = 1 … r	$\lvert a^k \; mod \; N\rangle$ with k = 1 … r	$\lvert a^k \; mod \; N\rangle$ with k = 1 … r
2	10	19
4	16	4
8	13	13
16	4	16
11	19	10
1	1	1

Which is the smallest number to get $\lvert \; a^r \; mod \; N \; \rangle = 1$.
Analyzing the performance difference,
we observe that in simulation the correct factorization is obtained after an average of 1.8 attempts,
while on IBM Sherbrooke it requires about 3.2 attempts on average, with a worst case of 19

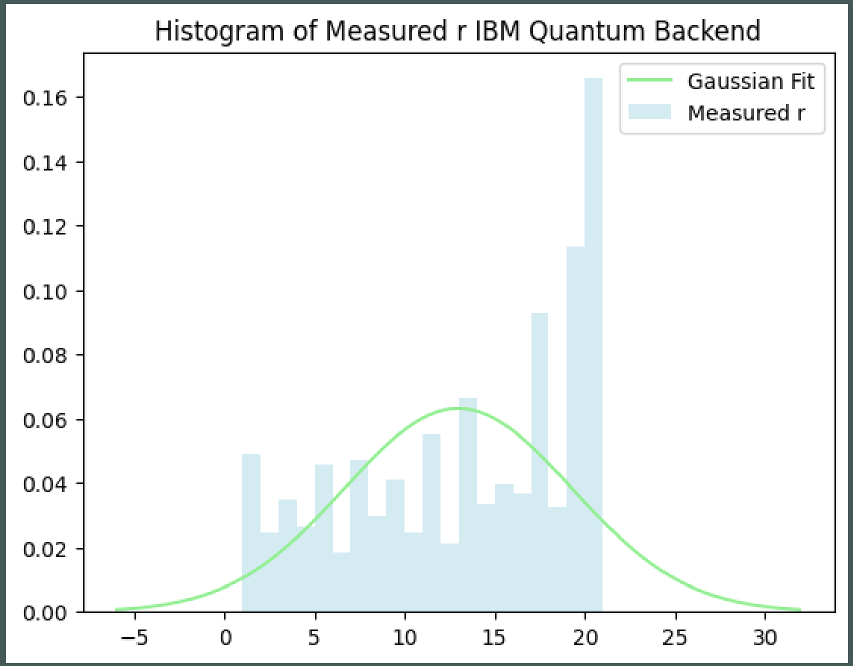


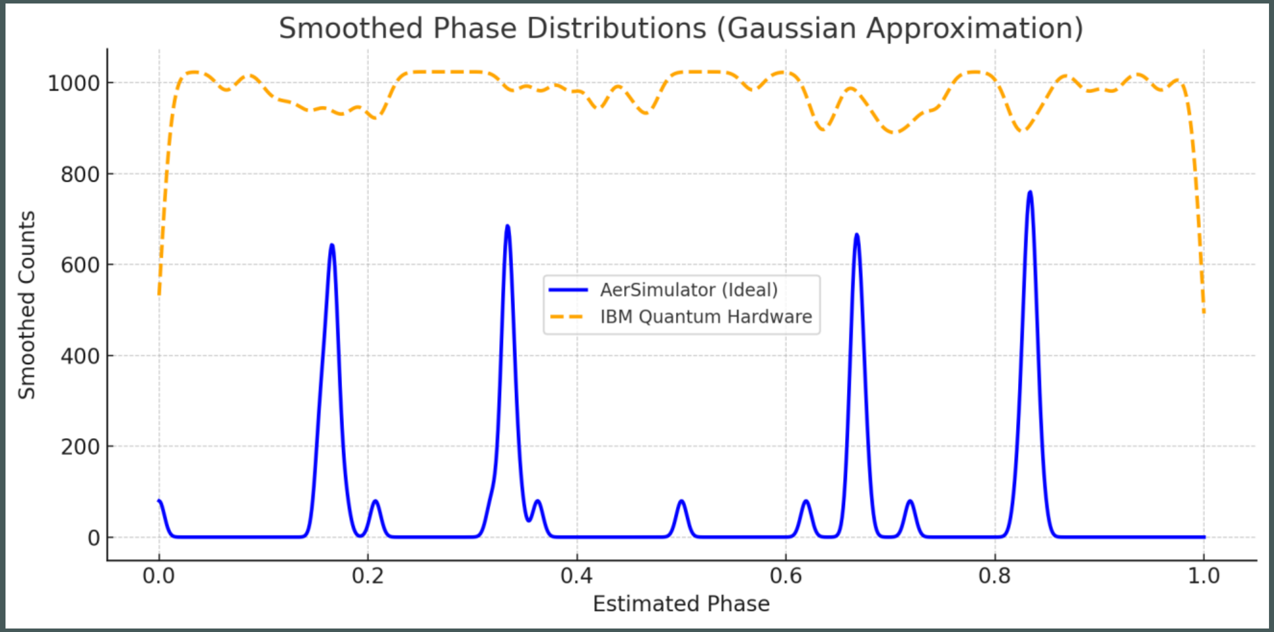


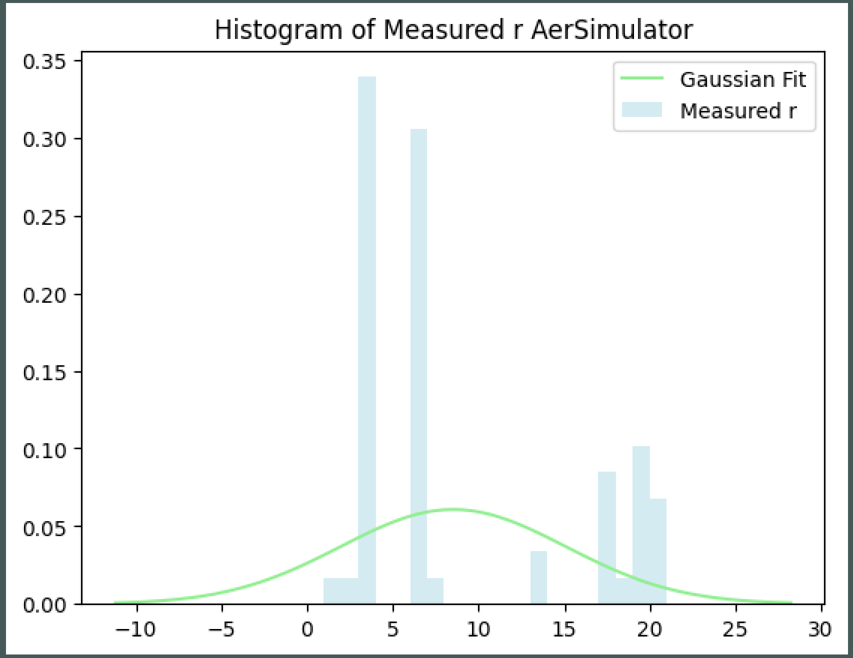
EVALUATION

In fact, as shown in these graphs,
the variance of the results is significantly different.

In real quantum hardware, performance is affected by several sources of noise:
Decoherence
imperfect gate fidelities
Limited qubit connectivity also leads to additional SWAP gates, increasing circuit depth and error accumulation.
shot noise introduces statistical fluctuations due to finite measurement repetitions. (1024 shots)







Thanks for attention