

# Applications for Quantum Computers

**SVA**

A Brief Overview of Quantum Algorithms

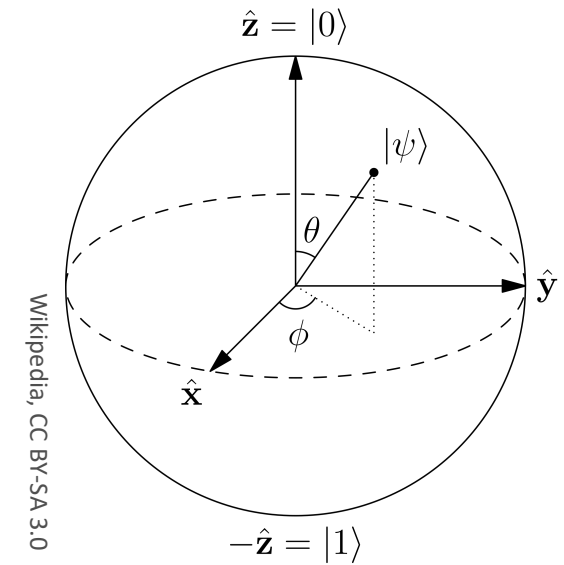
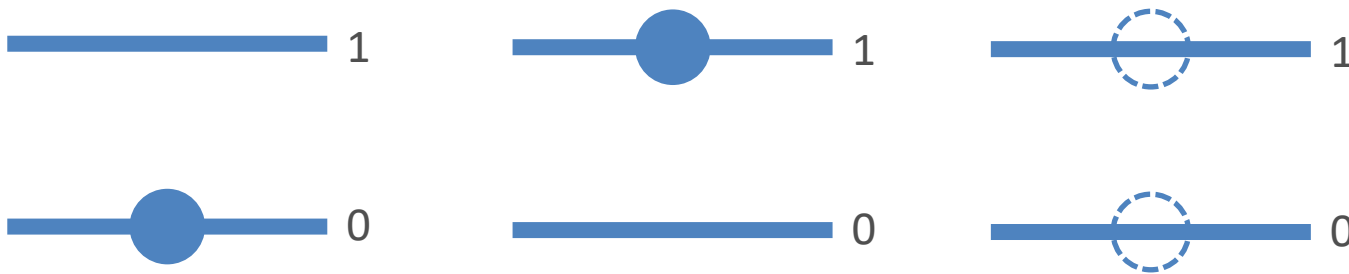
# Quantum Computing

# Quantum Computing / Qubits

/ Store Information

/ Exponential Space

| No | States                                    |
|----|---|
| 1  | 0, 1                                      |
| 2  | 00, 01, 10, 11                            |
| 3  | 000, 001, 010, 011,<br>100, 101, 110, 111 |
| 4  | 0000, 0001, 0010, ...                     |



# Quantum Computing

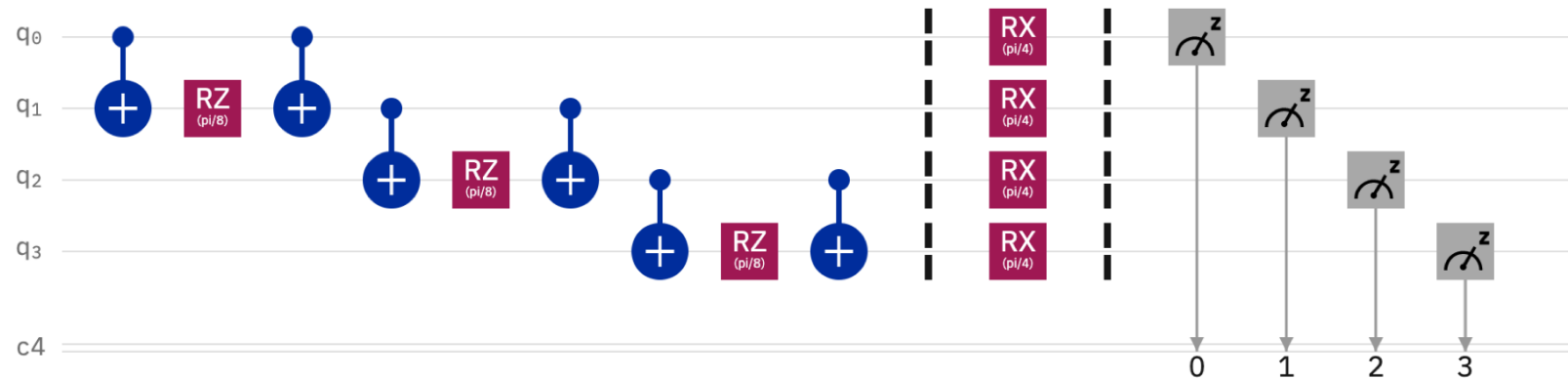
## / Gates & Circuits

Manipulate Information

Extract Information by Measurement

Act on Collection of Qubits

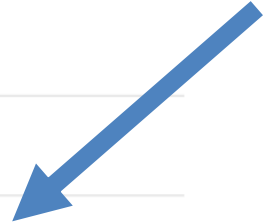
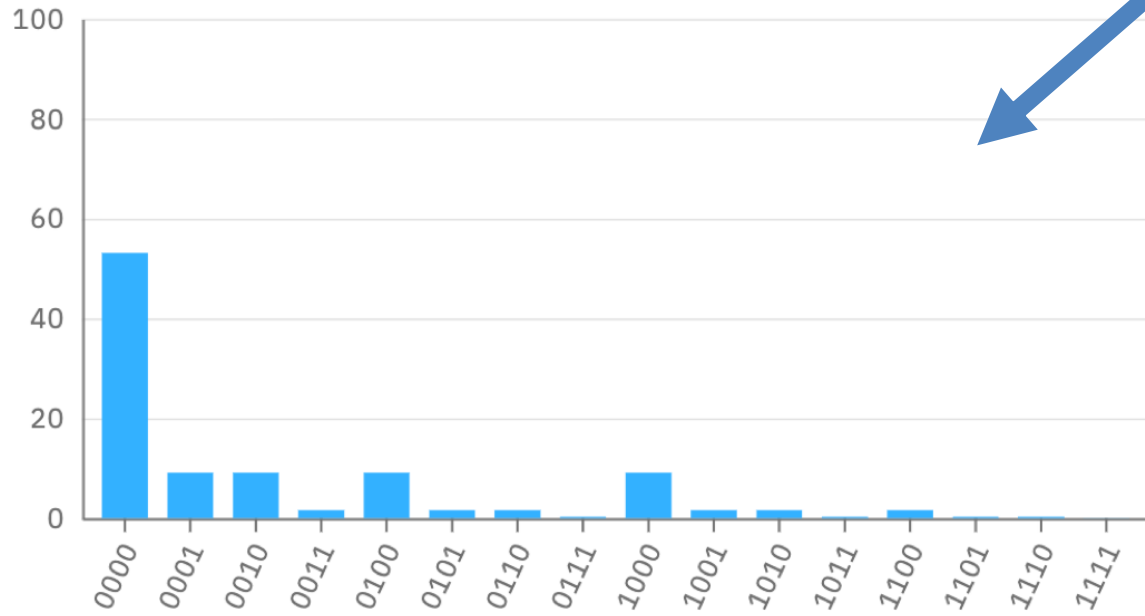
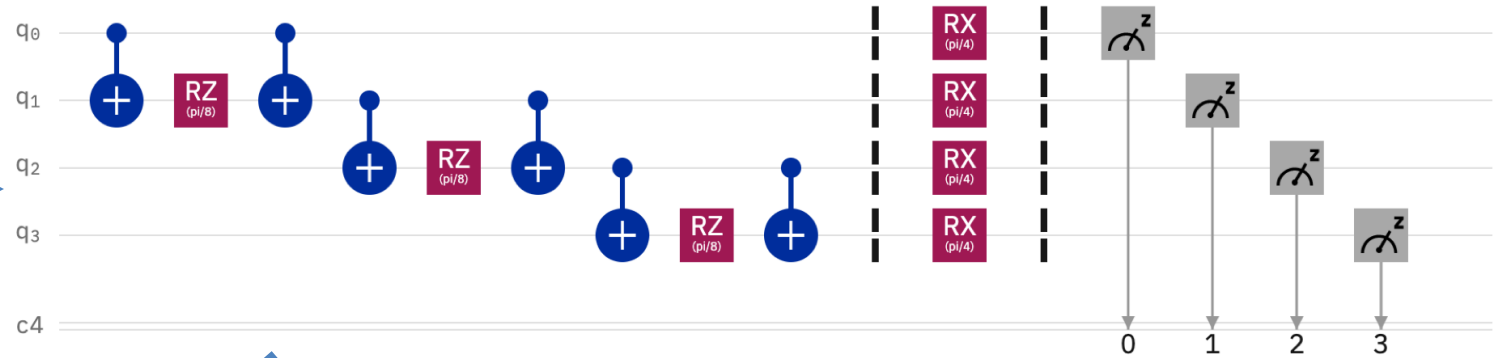
Qubits as Lines, Gates as Blocks





# / Computation Model

Problem,  
Classical Preprocessing



Result,  
Classical Postprocessing

# Classical Algorithms

/ Examples: Shor, HHL, Grover, ...

/ Read the Fineprint

/ Proven Speedup

/ Quantum Error Correction

# / Shor's Algorithm

**Problem: What are the factors of 4245221?**

/ Classical Solution:

1.  $4245221 = 3 * 1415073 + 2$
2.  $4245221 = 5 * 849044 + 1$
3.  $4245221 = 7 * 606460 + 1$
4.  $4245221 = 11 * 385929 + 2$
5. ...
- n.  $4245221 = 2011 * 2111 + 0$

/ No Efficient Classical Algorithm

/ General Number Field Sieve

/ Basis for RSA, ECC, ...



# / Shor's Algorithm

How to factorize  $n$ :

1. Choose number  $x$  with  $1 < x < n$
2. Calculate  $\gcd(x, n)$ 
  1. If  $\gcd(x, n) \neq 1$ , finish ✓
  2. If  $\gcd(x, n) = 1$ , continue X
3. Calculate smallest  $r$  with  $x^r \equiv 1 \pmod n$ 
  1. If  $r$  is odd, restart X
  2. If  $x^{r/2} \equiv -1 \pmod n$ , restart X
4. Extract Results
  1. Calculate  $\gcd(x^{r/2} - 1, n)$ , finish ✓
  2. Calculate  $\gcd(x^{r/2} + 1, n)$ , finish ✓

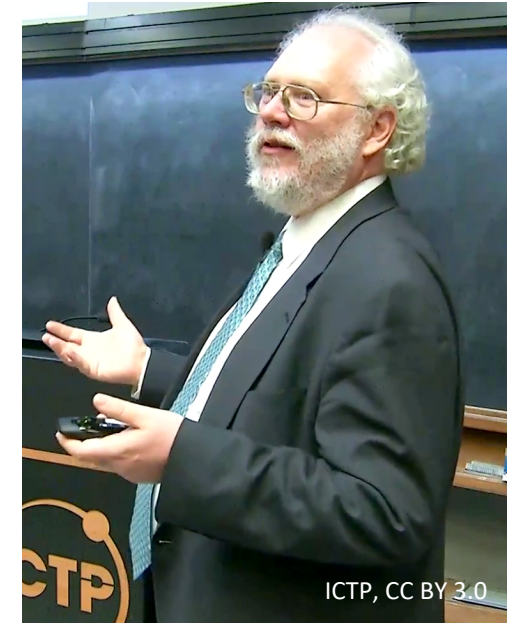
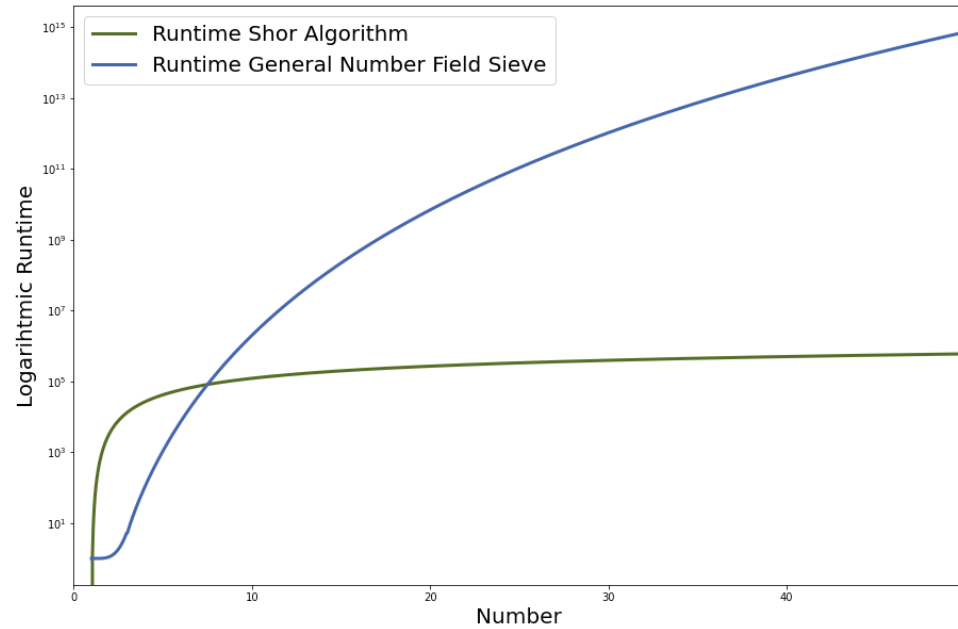
How to factorize 4245221:

1. Choose  $x = 1000$
2. Check  $\gcd(1000, 4245221) = 1$  ✓
3. Calculate  $r = 141370$
4. Extract Results
  1.  $\gcd(x^{r/2} - 1, n) = 2011$
  2.  $\gcd(x^{r/2} + 1, n) = 2111$

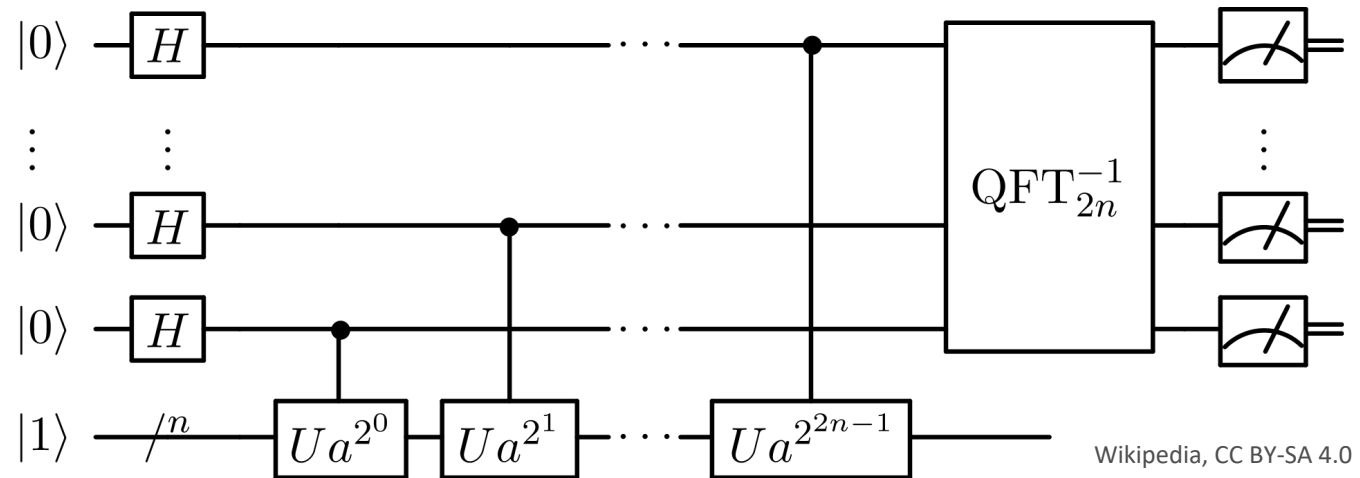
# Classical Algorithms / Shor's Algorithm

Order Finding Problem

Polynomial Runtime



ICTP, CC BY 3.0

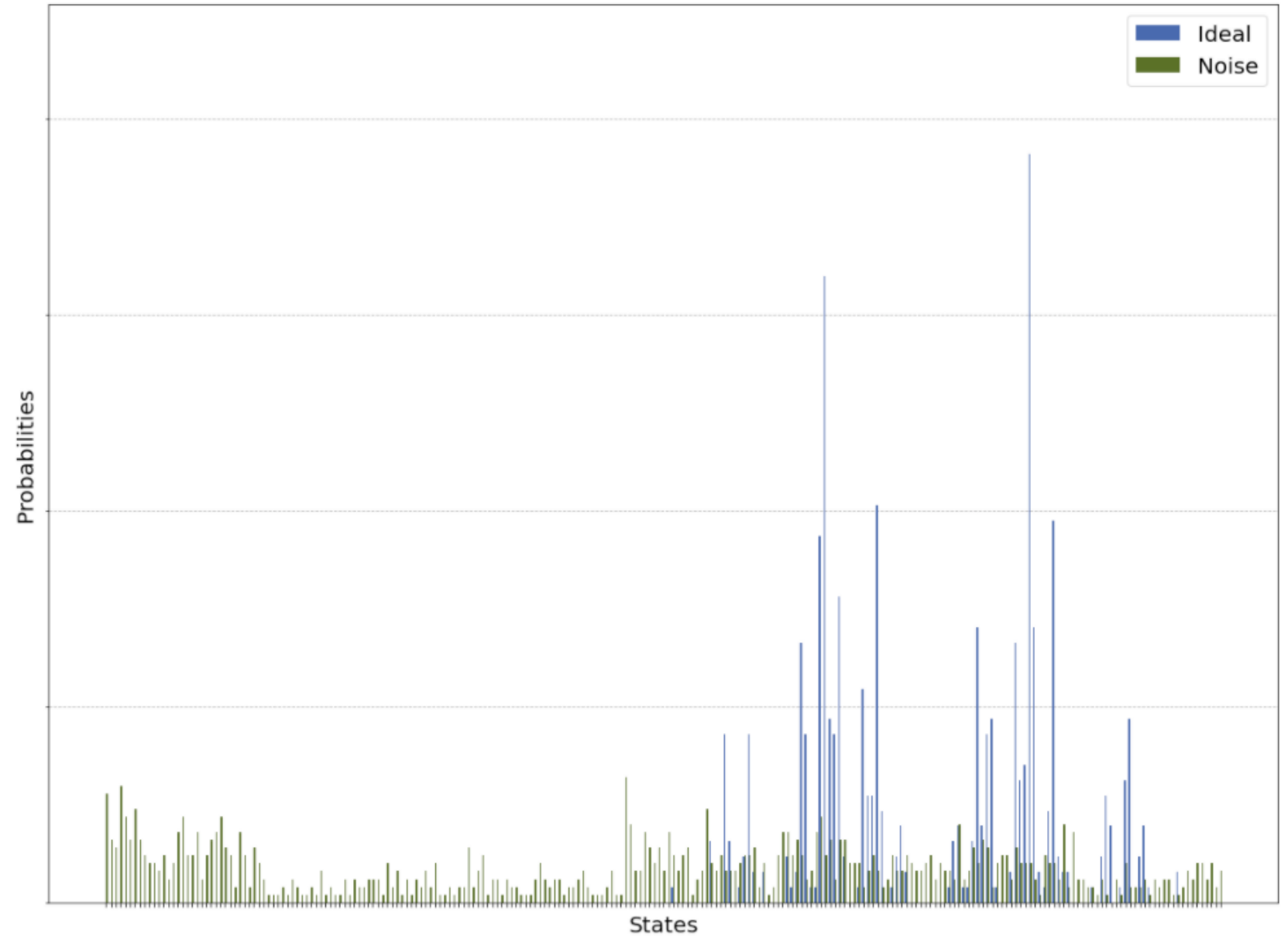


# Classical Algorithms / Shor's Algorithm

Error Sensitivity

Single Qubit Errors

Multi Qubit Errors



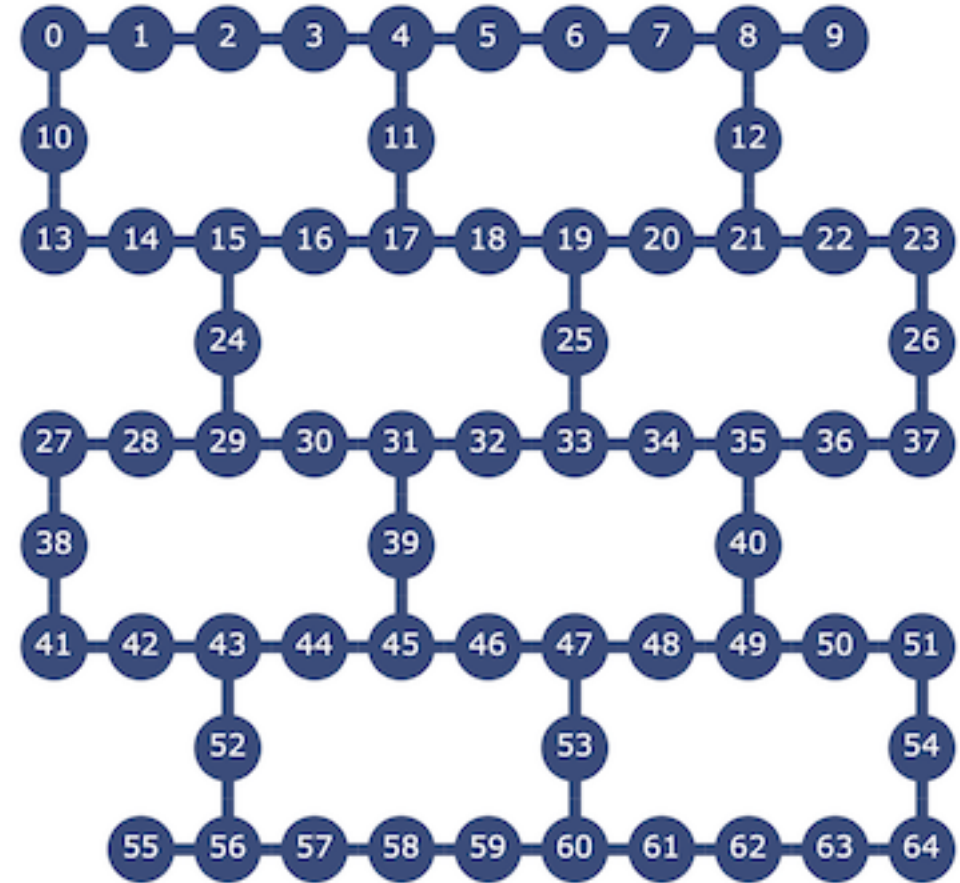
# Hybrid Algorithms



/ Limited Qubit Number

/ Limited Qubit Connectivity

/ Limited Qubit/Gate Fidelity



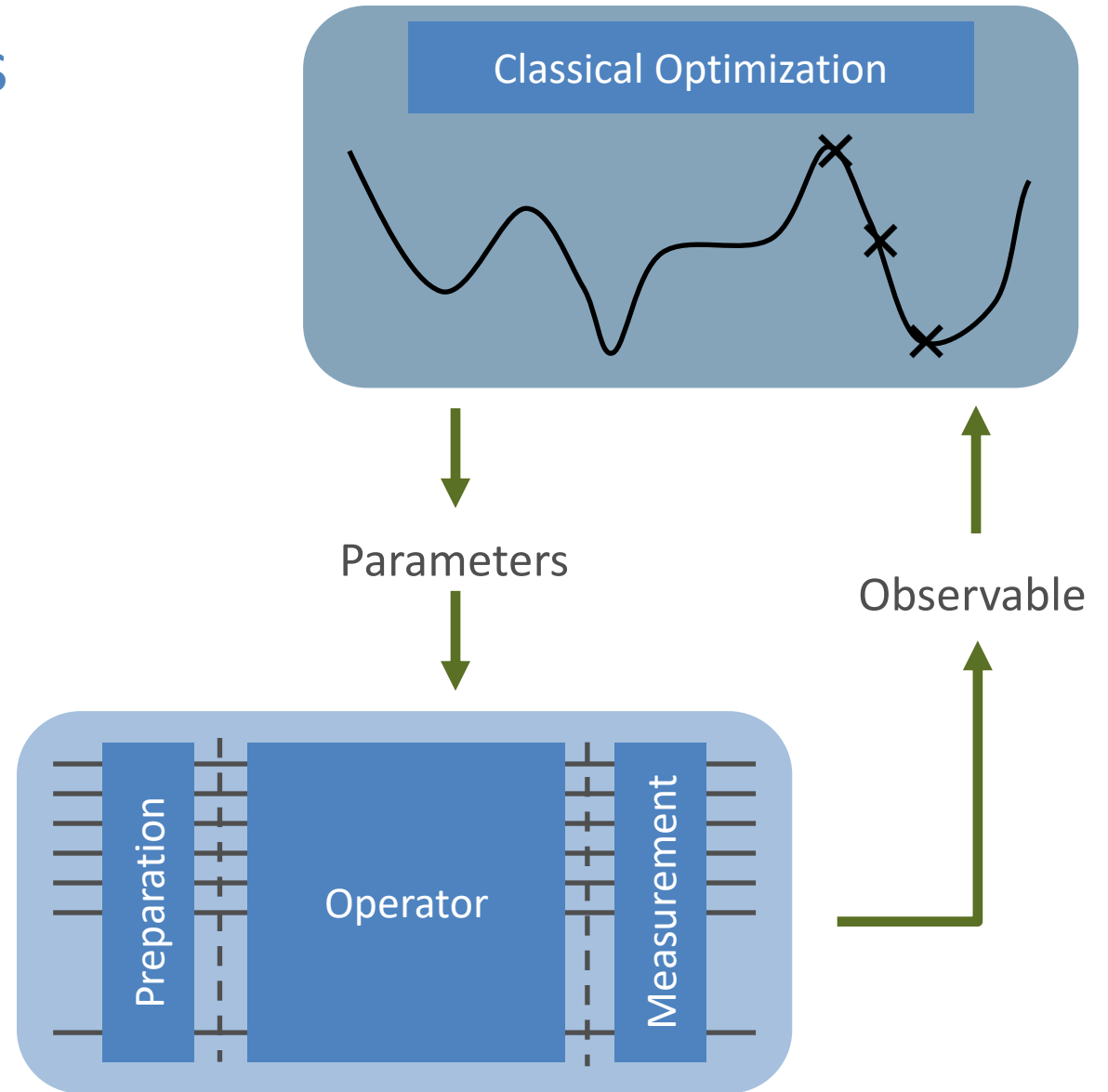
IBMQ Manhattan, IBM Quantum Team (2020)

# / Variational Quantum Algorithms

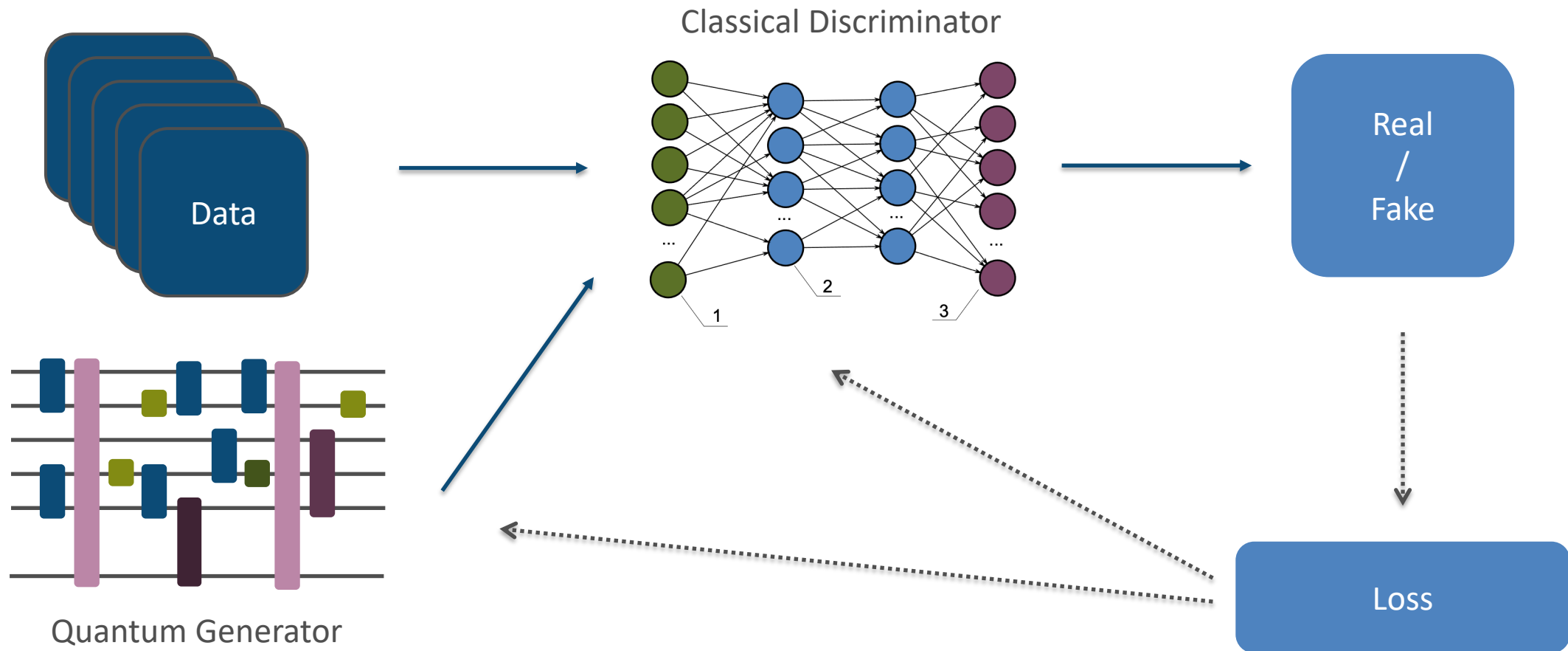
/ Interplay of Classical & Quantum Computer

/ No proven Speedup

/ Applications in Chemistry, Optimization and Quantum Machine Learning



# / Quantum Generative Adversarial Network



# Epilogue



# / Summary

/ Different Applications

/ Proven Speedup -> QEC

/ Classical & Hybrid Algorithms

/ Interesting Developments

/ Quantum Error Correction

/ Many Applications unknown!

# Time for Questions!



**CHRISTOPHER ZACHOW**

System Engineer Quantum Computing  
SVA System Vertrieb Alexander GmbH

Tel.: +49 160 9700 4538

[christopher.zachow@sva.de](mailto:christopher.zachow@sva.de)

Breslauer Platz 4

50668 Köln

