Hacking Cryptographic Protocols with Advanced Variational Quantum Attacks

Notes and Preliminaries

MohamadAli Khajeian

School of Engineering Science
University of Tehran

May 16, 2025

Introduction to Cryptography

- **Definition**: Cryptography is the science of securing communication through mathematical techniques, ensuring confidentiality, integrity, and authenticity.

Symmetric Cryptography

- Uses a single key for encryption and decryption.
- **Famous Block Ciphers**: AES, DES, 3DES, Blowfish

Asymmetric Cryptography

- Uses a public-private key pair for secure communication.
- **Famous Protocols & Algorithms**: RSA, ECC, Diffie-Hellman Key Exchange

Quantum Threats to Cryptography

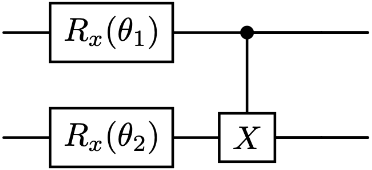
- Quantum computers threaten classical cryptography by efficiently solving problems like integer factorization (breaking RSA) and discrete logarithms (breaking ECC).
  - Shors Algorithm
    - Exponential speedup for factoring large numbers.
    - Breaks RSA, ECC, and Diffie-Hellman.
  - Grovers Algorithm
    - Quadratic speedup for brute-force search.
    - Weakens symmetric encryption.

Variational Quantum Algorithms (VQAs)

- incredibly popular approach for quantum algorithms on near-term quantum devices
- we know the task we want to accomplish, but we don't know the circuit
- can classically "learn" the circuit that best solves our task.

Variational Quantum Algorithms (VQAs)

- rely on Paramterized Quantum circuits



Variational Quantum Algorithms (VQAs)

- The goal is to find the parameters that perform the desired task.
- VQAs are quantum-classical hybrid algorithms the parametrized quantum circuit is the quantum part, while the tuning of parameters is the classical component.

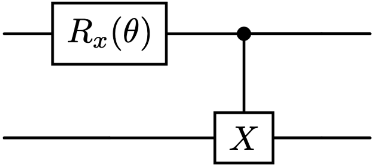
Variational Quantum Algorithms (VQAs)

In most of the cases, VQAs can be broken down into three main steps:

1. A quantum circuit $U(\vec{\theta})$, often called Ansatz, parametrized by a set of free parameters $\vec{\theta}$
2. A measurement of an observable $\mathscr{M}$ and a computation of a cost function in base of this measurement.
3. An optimization of the free parameters $\vec{\theta}$ performed in a classical computer that queries to the quantum device.

Ansatzes

- In physics and mathematics, the german word Ansatz, or in plural Ansätze (Ansatzes in english), refers to guessing a solution.
- When trying to solve a task using a Variational Quantum Algorithms, what we guess is the quantum circuit $U(\vec{\theta})$ that solves our task, so we refer to such circuit simply as ansatz.



Ansatzes

We start with the initial state $|0\rangle \otimes |0\rangle$:

$$\left|\psi_0\right\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

First, we apply the $R_x(\theta)$ gate to the first qubit. The matrix for $R_x(\theta)$ is:

$$R_x(\theta) = \begin{pmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

Applying $R_x(\theta)$ to the initial state $\left|\psi_0\right\rangle$:

$$\begin{aligned} \left|\psi_1\right\rangle &= (R_x(\theta) \otimes I) |0\rangle \otimes |0\rangle = (R_x(\theta) |0\rangle) \otimes (I |0\rangle) \\ &= (\cos(\theta/2) |0\rangle - i\sin(\theta/2) |1\rangle) \otimes |0\rangle \\ &= \cos(\theta/2) |00\rangle - i\sin(\theta/2) |10\rangle. \end{aligned}$$

Ansatzes

Next, we apply the CNOT gate, where the first qubit is the control and the second qubit is the target:

$$\left|\psi_2\right\rangle = \text{CNOT}\left|\psi_1\right\rangle = \cos(\theta/2)\,|00\rangle - i\sin(\theta/2)\,|11\rangle\,.$$

So, this represents final quantum state one can build with this ansatz.

Cost Function

In variational quantum algorithms, we usually define the cost function as the expectation value of a given observable $\hat{\mathcal{M}}$:

$$C(\vec{\theta}) = \langle 0| U^{\dagger}(\vec{\theta}) \hat{\mathcal{M}} U(\vec{\theta}) |0\rangle .$$

Cost Function

There are several criteria, that the cost function must meet to guide our choice:

1. **Faithfulness**: The minimum of $C(\vec{\theta})$ should correspond to the problem's solution.
2. **Efficient Estimation**: It must be possible to *efficiently estimate* $C(\vec{\theta})$ by taking measurements on a quantum computer, possibly with classical post-processing. Additionally, to maintain a potential quantum advantage with a VQA, $C(\vec{\theta})$ should not be efficiently computable classically.
3. **Operational Meaningfulness**: Smaller values of the cost function should represent better solutions.
4. **Trainability**: It should be feasible to efficiently optimize the parameters $\vec{\theta}$.

Optimizers

Once we have defined the ansatz and the cost function, the next step is to optimize the trainable parameters:

$$\vec{\theta}_{\text{opt}} = \arg\min_{\vec{\theta}} C(\vec{\theta})$$

where $\vec{\theta}_{\text{opt}}$ minimizes the cost function C.

Optimizers

- There exist many ways to perform this optimization, but it is known that gradient-based methods can help in speeding up the optimization tasks and guaranteeing the convergence.
- You may wonder: how can we calculate the derivative of the quantum circuit? thanks to the magic of the Parameter-Shift Rule (PSR)!

Parameter-Shift Rule

- PSR is a mathematical technique that allows us to compute the gradient of a specific quantum circuit by evaluating the original expectation value twice, but with one circuit parameter shifted by a fixed value.

Parameter-Shift Rule

The quantum circuit whose gradient we want to compute generally consists of multiple gates. Let us consider a unitary gate in the form:

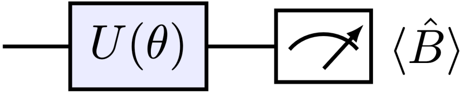
$$U(\theta) = e^{-\frac{i}{2}\theta \hat{P}_j},$$

where $\hat{P}_j$ is the Hermitian generator of $U(\theta)$ and corresponds to a Pauli operator. The gradient of $U(\theta)$ is given by:

$$\nabla U(\theta) = -\frac{i}{2}\hat{P}_j U(\theta) = -\frac{i}{2} U(\theta) \hat{P}_j.$$

Parameter-Shift Rule

Then, what we try to do is computing the gradient of the following circuit:



which mathematically corresponds to this function:

$$f(\theta) = \langle \hat{B} \rangle = \langle 0| U^{\dagger}(\theta) \hat{B} U(\theta) |0\rangle .$$

Parameter-Shift Rule

The gradient of $f(\theta)$ is:

$$\begin{aligned}\nabla f(\theta) &= \nabla \left\langle \hat{B} \right\rangle \\ &= \langle 0| \left(\nabla U^\dagger(\theta) \hat{B} U(\theta) + U^\dagger(\theta) \hat{B} \nabla U(\theta) \right) |0\rangle \\ &= \frac{i}{2} \langle 0| U^\dagger(\theta) (\hat{P}_j \hat{B} - \hat{B} \hat{P}_j) U(\theta) |0\rangle \\ &= \frac{i}{2} \langle 0| U^\dagger(\theta) [\hat{P}_j, \hat{B}] U(\theta) |0\rangle\end{aligned}$$

Using the commutator identity for Pauli operators:

$$[\hat{P}_j, \hat{B}] = -i \left(U^\dagger\left(\tfrac{\pi}{2}\right) \hat{B} U\left(\tfrac{\pi}{2}\right) - U^\dagger\left(-\tfrac{\pi}{2}\right) \hat{B} U\left(-\tfrac{\pi}{2}\right) \right),$$

Parameter-Shift Rule

we substitute into the gradient expression to obtain:

$$\nabla f(\theta) = \frac{1}{2} \langle 0| U^{\dagger}(\theta) \left(U^{\dagger}\left(\tfrac{\pi}{2}\right) \hat{B} U\left(\tfrac{\pi}{2}\right) - U^{\dagger}\left(-\tfrac{\pi}{2}\right) \hat{B} U\left(-\tfrac{\pi}{2}\right) \right) U(\theta) |0\rangle .$$

Finally, rewriting it in terms of quantum functions, the gradient of the quantum circuits reads:

$$\nabla f(\theta) = \frac{1}{2} \left[f(\theta + \tfrac{\pi}{2}) - f(\theta - \tfrac{\pi}{2}) \right]$$

Gradient Descent

1. **Initialization**:
   - Start with an initial guess for the parameters θ, denoted as $\theta^{(0)}$. This initial guess can be random or based on some heuristic.
2. **Compute Gradient**:
   - Calculate the gradient $\nabla f(\theta)$, which represents the vector of partial derivatives of f with respect to each parameter θ_i. The gradient provides the direction of the steepest ascent. For each parameter θ_i:

$$(\nabla f(\theta))_i = \frac{\partial f(\theta)}{\partial \theta_i}.$$

In practice, libraries like PennyLane use efficient methods such as the Parameter Shift Rule to compute these gradients for quantum circuits.

Gradient Descent

3. **Update Parameters**:
   - Adjust parameters in the opposite direction of the gradient:

$$\theta^{(k+1)} = \theta^{(k)} - \eta \nabla f(\theta^{(k)})$$

4. **Iterate Until Convergence**:
   - Repeat steps 2-3 until:
     - $\Delta f(\theta) < \epsilon$ (function change threshold)
     - $\|\nabla f(\theta)\| < \epsilon$ (gradient magnitude)

Variational Quantum Attacks Algorithms (VQAAs)

- **Definition**: A hybrid quantum-classical approach that uses variational quantum circuits to optimize attacks on cryptographic protocols.

1. Introduction
2. Variational Quantum Algorithms (VQAs)
3. References

[1] B. Aizpurua, P. Bermejo, J. E. Martínez, and R. Orús, “Hacking cryptographic protocols with advanced variational quantum attacks,” *ACM Transactions on Quantum Computing*, Feb. 2025.

[2] X. Q. Technologies, “Introduction to variational quantum algorithms,” *PennyLane Documentation*, 2023.