Practical Quantum Cryptanalysis by Variational Quantum Cloning

Brian Coyle, **Mina Doosti**, Elham Kashefi & Niraj Kumar

ArXiv: 2012.11424

Abstract

Cryptanalysis on standard quantum cryptographic systems involves finding optimal adversarial attack strategies on the underlying protocols. In many cases, these attacks rely on an adversary's ability to clone unknown quantum states which and extract secret information. Explicit optimal attack strategies typically require high computational resources or in many cases, are unknown. Here, we propose variational quantum cloning (VQC), a quantum machine learning based cryptanalysis algorithm which allows an adversary to obtain optimal (approximate) cloning strategies with short depth quantum circuits, trained using hybrid classical-quantum techniques. The algorithm contains:

- Operationally meaningful cost functions with theoretical guarantees,
- Quantum circuit structure learning and gradient descent based optimisation.

This enables the the end-to-end discovery of hardware efficient quantum circuits to clone specific families of quantum states, and leads to an improvement in cloning fidelites when implemented on quantum hardware: the Rigetti Aspen chip.
Finally, we derive cloning attacks on two quantum coin flipping protocols as examples, which we construct explicitly using VQC.

Quantum cloning

The task is to take a quantum state and produce two (perfect) 'clones' of it (deterministically). The no-cloning theorem is a pillar of quantum mechanics and forbids this. However, if the 'perfectness' requirement of the cloned states is relaxed, we get *approximate* quantum cloning [1]. The '*quality*' of clones is measured relative to local fidelity:

$$F_{\text{L}}(\rho_{\text{ideal}}, \sigma_{\text{clone}}) = \left(\text{Tr}\sqrt{\sqrt{\rho_{\text{ideal}}}\,\sigma_{\text{clone}}\sqrt{\rho_{\text{ideal}}}}\right)^2$$

Approximate cloning machines (unitaries: U_{clone}) come in two forms:

Universal:
E.g. clone all single qubit states.
Optimal achievable fidelity for clones [2]:

$$F^{\text{U}}_{\text{L,opt}} = 5/6 \approx 0.833$$

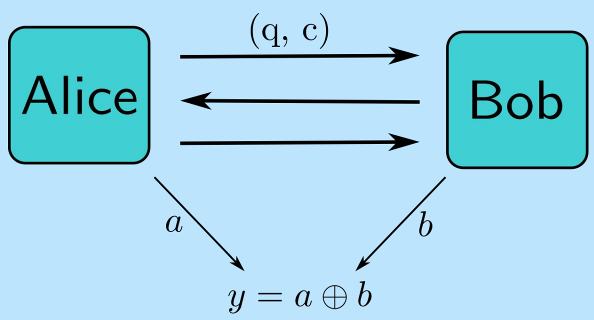
State-dependent:
Restricted to specific families of states, $\mathcal{S}$
for example phase-covariant states:

$$|\psi(\eta)\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + e^{i\eta}|1\rangle)$$

Optimal fidelity: $F^{\text{PC}}_{\text{L,opt}} \approx 0.85 > 5/6$

Quantum coin flipping protocols

Coin flipping is a cryptographic primitive that allows two parties (without mutual trust) to remotely agree on a random bit (y) without either party being able to bias the coin in its favour. A "biased coin" has one outcome (Heads/Tails) being more likely



Alice and Bob may exchange quantum (q) and/or classical (c) information to perform the (strong) coin flipping protocol. Alice and Bob both contribute a bit, ***a*** or ***b*** respectively to the final coin.

Quantum coin flipping states:

Many coin flipping protocols use the following set of quantum states (fixed overlap states) to perform the protocol

$$|\phi_{x,a}\rangle = \begin{cases} |\phi_{x,0}\rangle = \cos\phi|0\rangle + (-1)^x \sin\phi|1\rangle \\ |\phi_{x,1}\rangle = \sin\phi|0\rangle + (-1)^{x\oplus 1}\cos\phi|1\rangle \end{cases}$$

The protocol of Aharonov et. al. [5], $\mathcal{P}$

In this protocol, Alice utilises all 4 of the above states with the angle $\phi := \frac{\pi}{8}$. She encodes her contribution to the coin (her bit, a) in the 'basis' information of the above states.
A dishonest party (Bob) can bias if learns the basis (i.e. he learns Alice's bit, ***a***).

Variational quantum cloning

Variational Quantum Cloning (VarQlone) is a variational quantum algorithm [2], suitable for NISQ computers and can be used to find short depth circuits for approximate cloning machines. We also extend to $M \to N$ cloning, taking M copies of the input state and producing N output clones.
Note a similar idea appeared in [3].

A simple reinforcement learning based approach is used to search over circuit structure using quantum gates from a 'gate pool', $\mathcal{G}$, typically to fit a given quantum hardware requirements (i.e. using native gates).

We use analytic gradients of the cost functions from the parameter shift rule [4].

Cost functions:

We use local and global cost functions which serve different purposes, e.g. a local cost:

$$\text{C}_{\text{L}}(\theta) := 1 - \frac{1}{N}\sum_{j=1}^{N}\mathbb{E}\left[F_{\text{L}}\left(|\psi\rangle\langle\psi|, \rho^j_\theta\right)\right]$$

Faithfulness

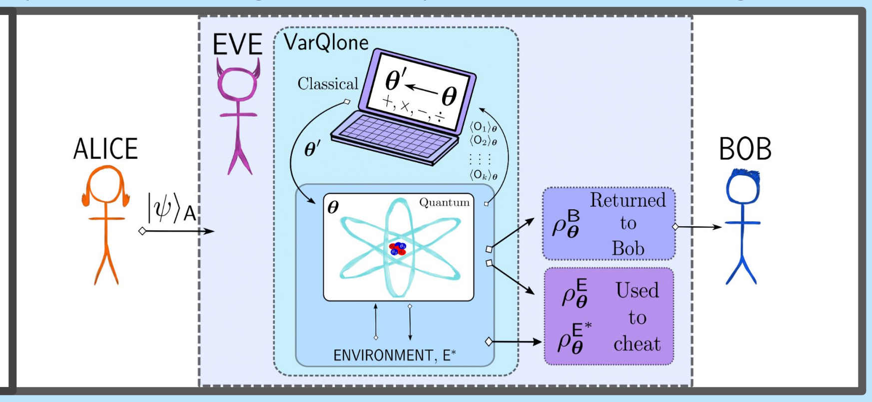
The cost functions are faithful - closeness to minimum implies closeness of each clone (j) to ideal (in some metric):

$$|\text{C}_{\text{L}}(\theta) - \text{C}^{\text{opt}}_{\text{L}}| \le \epsilon \to D(\rho^{\psi,j}_\theta, \rho^{\psi,j}_{\text{opt}}) \le f(\epsilon) \quad \forall|\psi\rangle \in \mathcal{S}, \forall j$$

Variational quantum cryptanalysis

Using VarQlone, we can build constructive attacks on quantum protocols whose security may reduce to quantum cloning (for example BB84 QKD, see Figure).

Eve can build an approximate cloning machine to attack Alice & Bobs communication. Eve's goal is to create 2 clones of Alice's state to gain information, using ancillary states, E*. She can achieve better performance using a state -dependent cloner if she has side information.

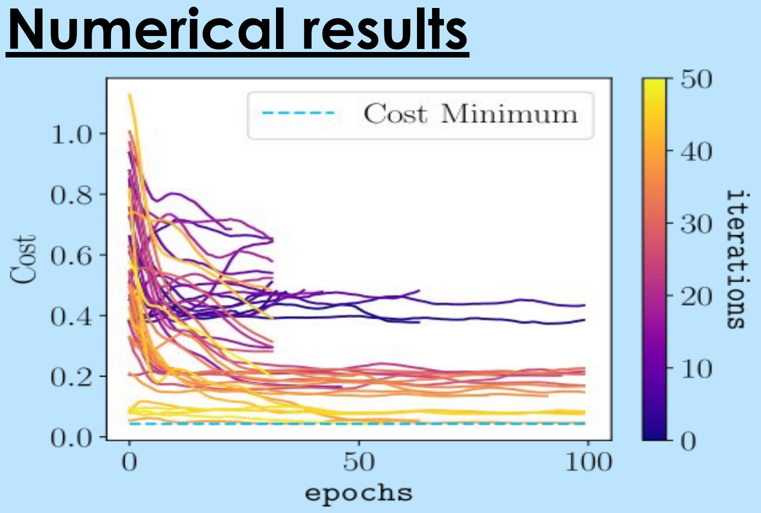


Explicitly, we derive a cloning based attack that Bob can implement coin flipping protocols to bias the coin. As an explicit example, we can prove:

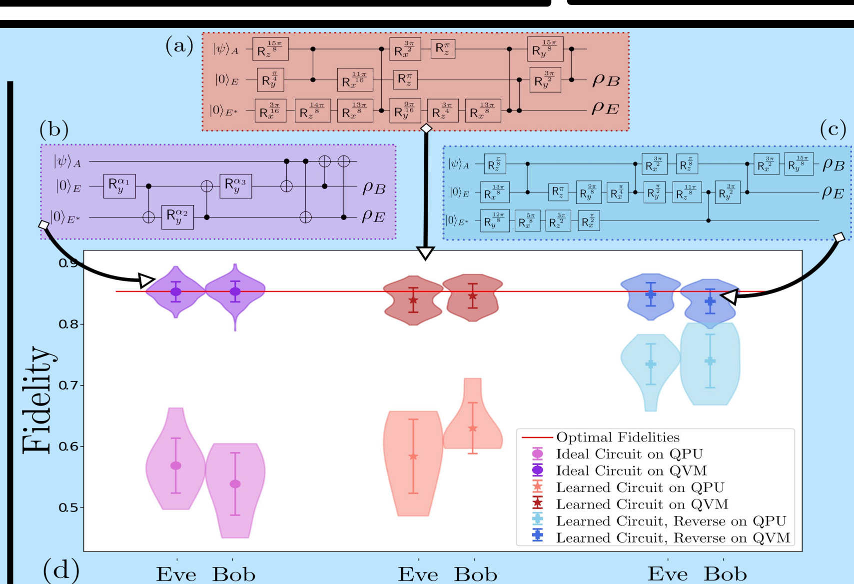
Theorem:
Using a *local* VarQlone cloning attack on the protocol, $\mathcal{P}$, Bob can achieve a bias:

$$\epsilon_{\mathcal{P},\text{VarQlone}} \approx 0.24$$

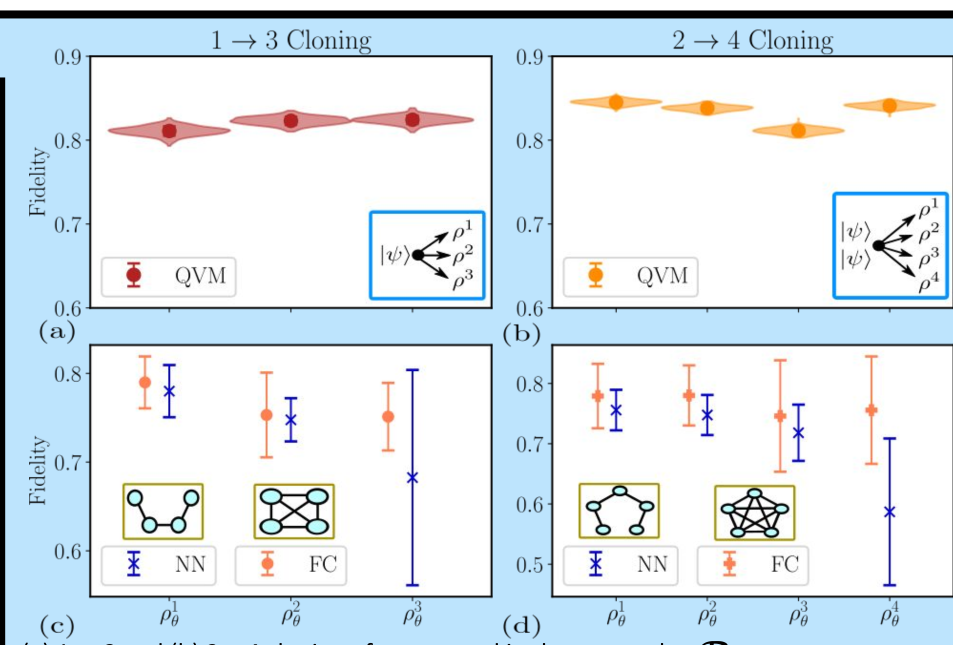
Numerical results



VQC learning to find a 'good' circuit structure using the gate pool. Each iteration corresponds to a different circuit, whose parameters are then optimised by gradient descent using Adam'. Example shown for phase covariant cloning. After 50 iterations, a circuit has been found which achieves the cost function minimum.



Cloning phase-covariant states in a BB84 like protocol. One clone goes to Bob and the other to Eve. (b) 'Ideal' circuit, (a, c) VQC learned circuits. VQC learns circuits which saturate theoretical optimal fidelity in simulator (QVM) and display higher fidelities on Rigetti Hardware (QPU)



(a) 1 -> 3 and (b) 2-> 4 cloning of states used in the protocol, $\mathcal{P}$
(c, d) The effect of fully connected (FC) versus nearest neighbour (NN) gate pools, $\mathcal{G}$

[1] Quantum Cloning - Scarani et. al. Rev. Mod. Phys. 77, 1225-1256 (2005)
[2] Variational Quantum Algorithms - Cerezo et. al. arXiv - 2012.09265
[3] Jašek et. al. Optics Express, 27, 22 pp. 32454-32464
[4] Evaluating Analytic Gradients on Quantum Hardware - Schuld et. al. Phys. Rev. A 99, 032331
[5] Quantum Bit Escrow - Aharonov et. al STOC '00 705-714.