Quantum Veto Protocol


ars technica
MAIN MENU MY STORIES: 25 FORUMS SUBSCRIBE JOBS
Ars Technica has arrived in Europe. Check it out!
RISK ASSESSMENT / SECURITY & HACKTIVISM

Geneva brings quantum cryptography to Internet voting

Geneva has adopted innovative new quantum cryptography technology to ensure ...

by Ryan Paul - Oct 12, 2007 9:17pm IST

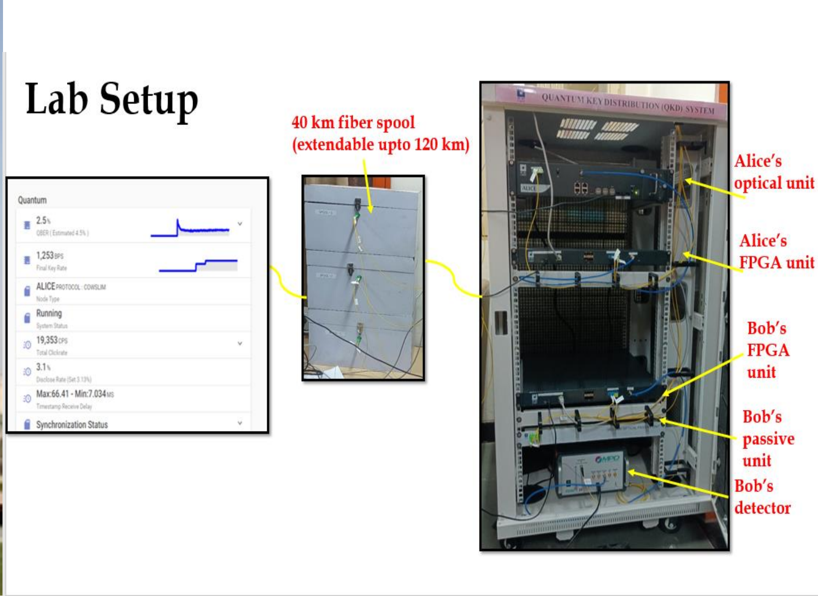
Share Tweet Email

Geneva, Switzerland, has long been at the forefront of electronic voting innovation. In 2004, Geneva rolled out one of the first Internet voting systems in the world. Now Geneva is touting its new unique electronic voting security system that uses quantum cryptography to guarantee against

Anirban Pathak
Jaypee Institute of Information Technolog
A10, Sector 62, Noida
Contact details for post-talk queries:
anirbanpathak@yahoo.co.in, 971706649

Quantum Algorithm Webinar Series entitled Quantum Algorithm Using Qniverse: Dive into the future of computing, CDAC Bangalore, July 23, 2025.

Starting point of our trip: We are located here

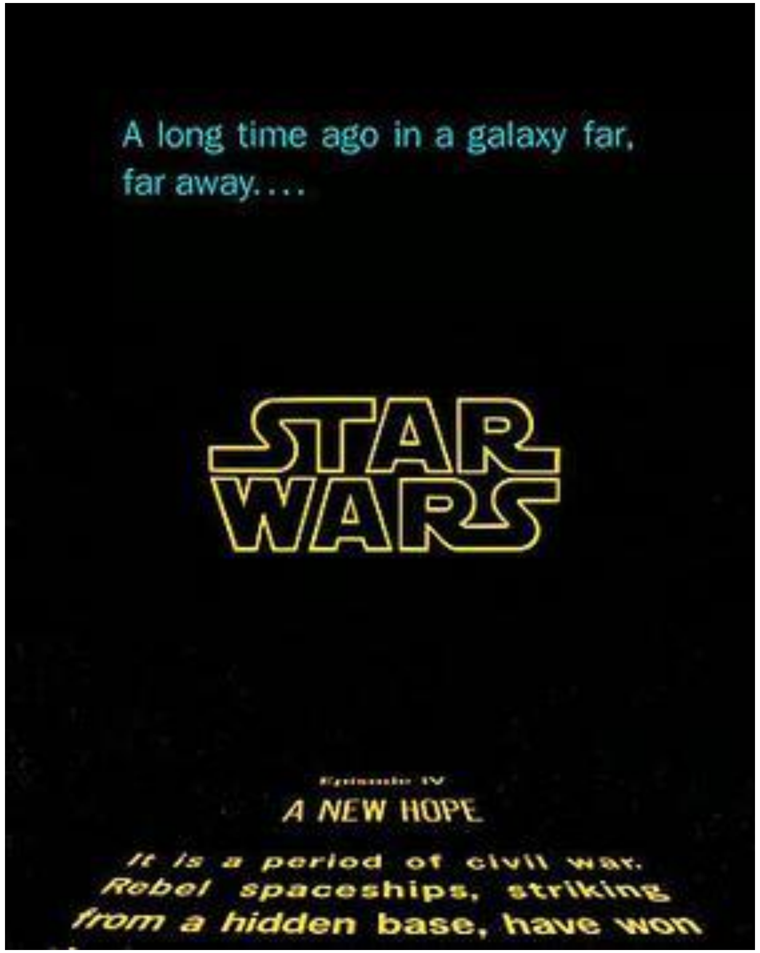


Motivation behind this talk

In a galaxy far far away ...

- *During an open meeting, the Galactic Security Council must decide whether to invade an enemy planet. One delegate wishes to veto the measure, but worries that such a move might jeopardize the relations with some other member states. How can he veto the proposal without revealing his identity?*

Above are the starting lines of Feng Hao and Piotr Zielinski's book chapter entitled, "**The Power of Anonymous Veto in Public Discussion**", published in M.L. Gavrilova et al. (Eds.): Trans. on Comput. Sci. IV, LNCS 5430, pp. 41–52, 2009.



Anonymous veto: Why and where?

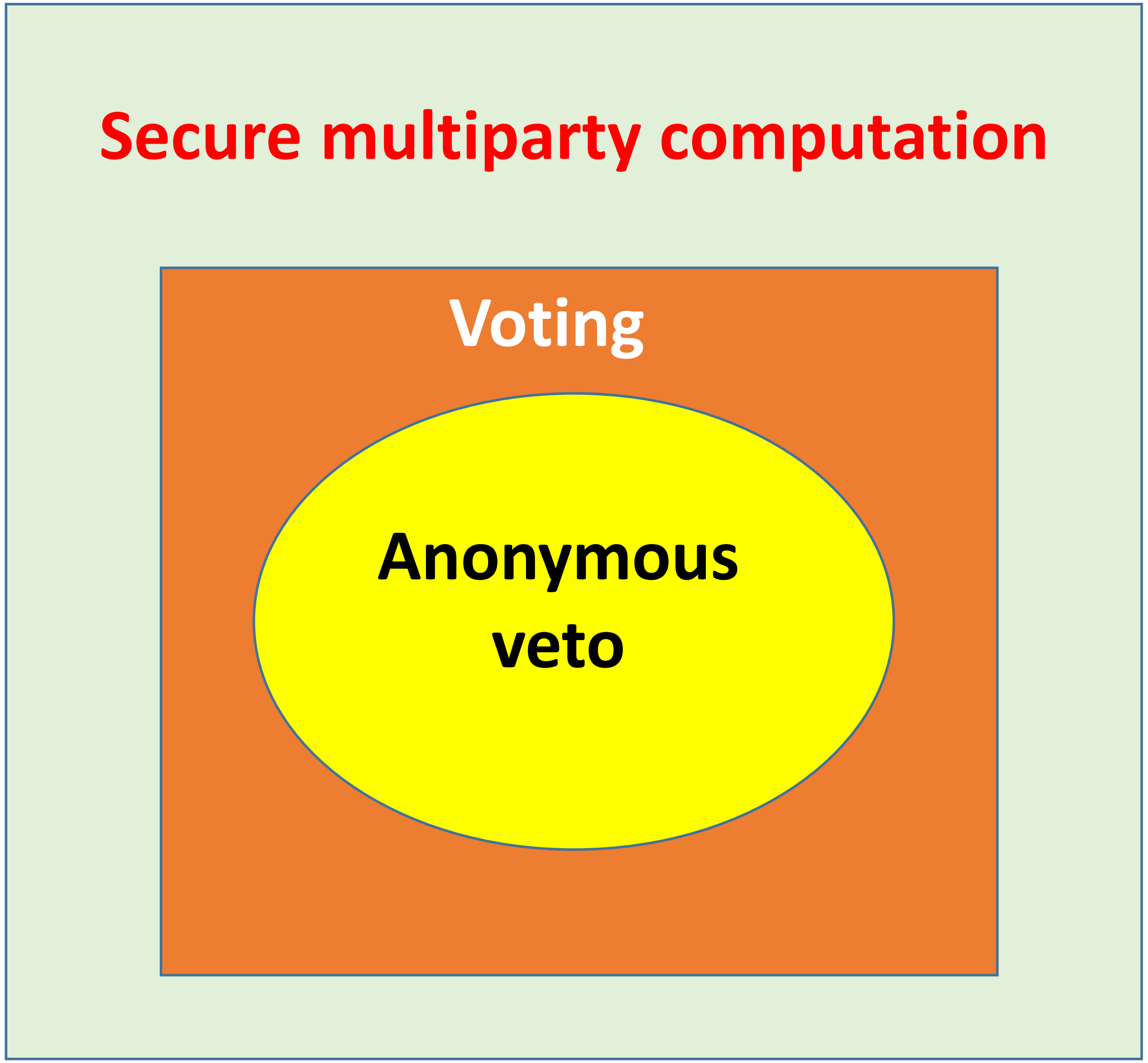
Why

- **Anonymity Protects Individual Rights:** It protects individuals from potential negative consequences for expressing their views.
- **Creates a window for honest feedback:** Individuals can express dissenting opinions without the fear of being marginalised.
- **Protects interests of a minority:** A minority can protect its interests from being overridden by a larger group.

Where

- In important cases, juries may decide to vote anonymously.
- The UN Security Council's permanent members hold veto power, but in some cases, the specific country casting the veto might be sensitive. An anonymous veto could allow for more flexibility and less political tension

Let us understand the relation of quantum veto with other schemes of multiparty computation



- Basic definition: **Anonymous Veto is a** mechanism where a decision can be made by a group without revealing which specific members (if any) voted against it. When quantum resources are used for designing a protocol for anonymous veto, we refer to it as quantum anonymous veto (QAV).
- Voting and dining cryptographer's problem are closely related to QAV.

Anonymous Veto as a computational problem

Definition 1 An AV protocol of n voters returns $\mathcal{V}_n = 0$ if all the voters support the proposal and $\mathcal{V}_n = 1$ otherwise. In other words, an n input function $\mathcal{V}_n \in \{0, 1\}$ is computed as

$$\mathcal{V}_n = \vee_i \mathcal{W}_i = \begin{cases} 0 & \text{iff } \mathcal{W}_i = 0 \ \forall i, \\ 1 & \text{otherwise}, \end{cases} \tag{1}$$

where the ith input $\mathcal{W}_i \in \{0, 1\}$ is supplied by the ith voter, and the logical OR operation $\vee_i$ performed over all the i inputs returns 0 only when all the inputs are 0. Thus, $\mathcal{V}_n = 0$ or 1 provides whether $k = 0$ or $k \neq 0$ number of voters veto the proposal among all the n voters, respectively.

Requirements for AV protocol

Eligibility: No one except the authorized voters shall be allowed to vote.

Privacy: It means that nobody except the voter should be able to know how a particular voter has voted.

Binding: No one (including the voter himself) can change the vote $\mathcal{W}_i$ after its submission.

Correctness: If the adversary is passive, then the result bit $\mathcal{V}_n = 0 \Longleftrightarrow \mathcal{W}_i = 0\ \forall i$ is generated. In other words, it means that after faithfully following the protocol, one is able to successfully detect a veto or unanimous agreement with probability 1.

Verifiability: All the participants can verify the result $\mathcal{V}_n$.

Robustness: If the adversary is passive, then the result bit $\mathcal{V}_n = i\ \forall i \in \{0, 1\}$ is generated. It means that the system obtains the result if adversary is passive, i.e. under the effect of the noise in the systems.

Note: Qniverse implementation is proof of principle implementation as identity authentication, eavesdropping checking, etc. are not done.

What is one-sided two-party computation?

- Alice and Bob have secret inputs
  $i \in \{1,2,\cdots,n\}$ and $j \in \{1,2,\cdots,n\}$, respectively.
- An *ideal* one-sided two-party secure computation: Alice helps Bob to compute a prescribed function

$$f(i,j) \in (1,2,\cdots,p)$$

in such a way that, at the end of the protocol, (a) Bob learns *f* (*i*, *j*) unambiguously, (b) Alice learns nothing about *j* or *f* (*i*, *j*), and (c) Bob knows nothing about *i* more than what logically follows from the values of *j* and *f* (*i*, *j*).

We will call these conditions as condition (a), (b) and (c).

Lo’s results and arguments 1

- Three conditions for security- (a), (b), and (c) are incompatible in the sense that if (a) and (b) are satisfied, then a cheating strategy can be designed that would allow Bob to learn the values of $f\ (i, j)$ for *all* j’s, thus violating security requirement (c).

Lo’s work and subsequent works implied impossibility of 2 party secure computation, but did not tell much about secure multi-party computation (SMC)

Special cases of one-sided two-party computation?

- Socialist millionaire problem:

  Compute (i) $f(i.j)=1$ if $i=j$ and else $f(I,j)=0$

  or, (ii) $f(i.j)=1$ if $i>j$ and else $f(I,j)=0$

  or, (iii) $f(i.j)=1$ if $i>j$ and else $f(I,j)=0$

Note: Socialist millionaire problem is also implemented in Qniverse

Other SMC tasks of interest
Quantum e-commerce,
Quantum Veto,
Quantum Voting,
Quantum Lottery,
Quantum e-auction

- Quantum private comparison (QPC) is a special case of socialist millionaire problem

  The task is to check equality of private

  information: (i) $f(i.j)=1$ if $i=j$ and else $f(I,j)=0$

A more general case of two-party secure computation is SMC.

First protocol of quantum voting: Hillery's protocol or HZBB06 protocol

Part of our views: Protocols for quantum binary voting, K. Thapliyal, R. D. Sharma, **A. Pathak**, Int. J. Quant. Infor. **15** (2017) 1750007

Step 1: An honest (non-cheating) authority Charlie prepares an entangled state

$$|\psi_0\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}|k\rangle|k\rangle,$$

where N is the number of voters. Ex. for $N=3, |\psi_0\rangle = \frac{1}{\sqrt{3}}\left(|00\rangle+|11\rangle+|22\rangle\right)$

Step 2: Charlie keeps one of the qunits (say the second one) and sends the first one to the first voter (say Alice$_1$), who registers her "no" vote by applying Identity operator (thus doing nothing) and "yes" vote by applying

$$U_{yes} : U_{yes}|k\rangle = |k+1\rangle,$$

where + denotes a modulo N addition.

M. Hillery, et al. *Physics Letters A* 349.1-4 (2006): 75-81.

Background works that led to the protocol implemented in Qniverse

International Journal of Quantum Information | Vol. 15, No. 01, 1750007 (2017)

Protocols for quantum binary voting

Kishore Thapliyal, Rishi Dutt Sharma, and Anirban Pathak

arXiv > quant-ph > arXiv:2206.03182

Quantum Physics

[Submitted on 7 Jun 2022]

Anonymous voting scheme using quantum assisted blockchain

Sandeep Mishra, Kishore Thapliyal, S Krish Rewanth, Abhishek Parakh, Anirban Pathak

Our early interest was binary voting with travelling ballot, but lately we moved to veto as number of voters are usually less and modern technology can implement QAV.

Mishra et al. *EPJ Quantum Technology* (2022) 9:14
https://doi.org/10.1140/epjqt/s40507-022-00133-2

EPJ.org

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Check for updates

Quantum anonymous veto: a set of new protocols

Sandeep Mishra[1], Kishore Thapliyal[2], Abhishek Parakh[3] and Anirban Pathak[1*]

Reports 7 protocols for QAV

Quantum Information Processing (2022) 21:311
https://doi.org/10.1007/s11128-022-03650-2

Check for updates

Experimental realization of quantum anonymous veto protocols using IBM quantum computer

Satish Kumar[1] · Anirban Pathak[1]

Out of the 7 protocols of above paper, 2 were implemented here, in Qniverse 1 of those 2 is implemented using Bell states.

Basic ideas 1: Bra-ket notaiton

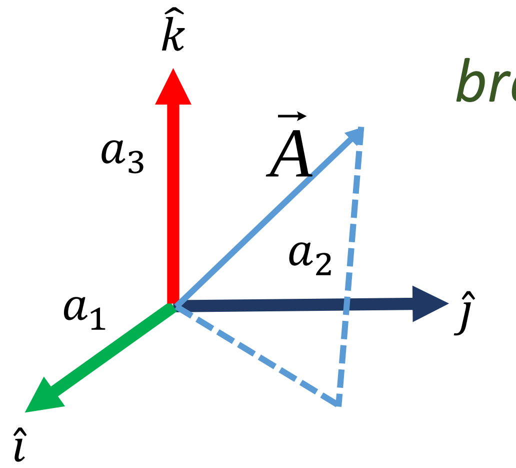
Consider a vector A in 3D Euclidean space, $A \in \mathbb{R}^3$. It is easy to see equivalences between ordinary notation and bra-ket notation in vector A. Vector A is the linear combination of the basis vectors represent the coordinates.

$$\langle \quad | \quad \rangle \longrightarrow \langle bra|ket \rangle$$

$$\vec{A}\; a_1\hat{\imath} + a_2\hat{\jmath} + a_3\hat{k}$$

$$= a_1\begin{pmatrix}1\\0\\0\end{pmatrix} + a_2\begin{pmatrix}0\\1\\0\end{pmatrix} + a_3\begin{pmatrix}0\\0\\1\end{pmatrix}$$

$$= \begin{pmatrix}a_1\\0\\0\end{pmatrix} + \begin{pmatrix}0\\a_2\\0\end{pmatrix} + \begin{pmatrix}0\\0\\a_3\end{pmatrix} = \begin{pmatrix}a_1\\a_2\\a_3\end{pmatrix}$$



bra-ket

Inner product

$\langle A|B\rangle =$ inner product of *ket* $|A\rangle$ with *ket* $|B\rangle$

$$= \sum_{n=1}^{N} a_n^* e_n^* b_n e_n = \begin{pmatrix} a_1^* & a_2^* & \dots & a_N^* \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_N \end{pmatrix}$$

where a_i^* denotes the complex conjugate of a_i and $\langle A|$ is the conjugate of *ket A* ($|A\rangle$) called *bra* A . The *bra-ket* notation splits inner product in pieces *bra* and *ket*.

$\langle \quad | \quad \rangle \longrightarrow \langle bra|ket\rangle$

bra-ket

Example:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \Rightarrow \langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix}$$

$$\therefore \langle 0|0\rangle = \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1.$$

Similarly,

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \Rightarrow \langle 1| = \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$\therefore \langle 1|0\rangle = \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 0.$$

Outer product

Outer products are defined as

$$|A\rangle\langle B|$$

They are extremely useful in describing density operators, quantum gates, etc.

Example:

A not gate can be written as $NOT = |0\rangle\langle 1| + |1\rangle\langle 0|$

Examples:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \Rightarrow \langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \Rightarrow \langle 1| = \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$\therefore |0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Similarly,

$$|1\rangle\langle 0| = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Thus,

$$|0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Outer product and quantum gates

Check

$NOT|0\rangle = |1\rangle$ and $NOT|1\rangle = |0\rangle$

as $\langle 0|0\rangle = \langle 1|1\rangle = 1$ and $\langle 1|0\rangle = \langle 0|1\rangle = 1$

do check

$$NOT|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$NOT|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

A gate can be expressed as a matrix or as a sum of outer products

- Hadamard gate:

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

$$H|0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),$$

$$H|1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

Pauli matrices are quantum gates

Every gate computes a function. For example, *NOT* gate computes $f(x) = \bar{x}$.

$$X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \Rightarrow X|0\rangle = |1\rangle;\, X|1\rangle = |0\rangle,$$

$$iY = i\sigma_y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \Rightarrow i\sigma_y|0\rangle = -|1\rangle;\, i\sigma_y|1\rangle = |0\rangle,$$

$$Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \Rightarrow Z|0\rangle = |0\rangle;\, Z|1\rangle = -|1\rangle,$$

$$I = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow I|0\rangle = |0\rangle;\, I|1\rangle = |1\rangle,$$

We will use Z gate in veto

Gates are sequentially added to form circuits and a group of circuits build quantum computer. To build a real quantum computer you need all single qubit gates and at least one real two qubit gate (say *CNOT*) which can not be decomposed into one qubit gates.

Tensor product

$$\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a\begin{bmatrix} c \\ d \end{bmatrix} \\ b\begin{bmatrix} c \\ d \end{bmatrix} \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

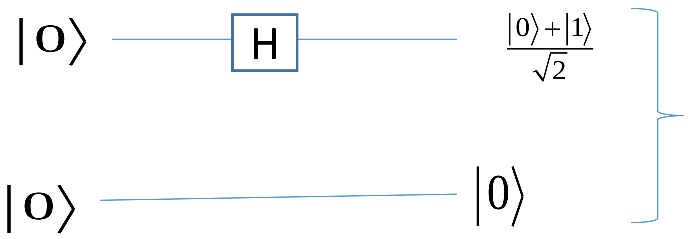
Similarly,

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

Mathematica command for performing tensor product of matrices A and B is KroneckerProduct[A,B], In Matlab it is kron(A,B)

Tensor product and quantum circuit

$$H|0\rangle \otimes I_2|0\rangle = (H \otimes I_2)(|0\rangle \otimes |0\rangle) = (H \otimes I_2)|00\rangle$$



$$\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |0\rangle = \frac{|00\rangle+|10\rangle}{\sqrt{2}}$$

$$\Rightarrow \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$H \otimes I_2 = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

$$H \otimes I_2|00\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}$$

Tensor product leads to the definition of entangled states

If you cannot express a bipartite (or two mode) state vector as the tensor product of the state vectors of the individual particle (mode), the composite state is called entangled, i.e., inseparable

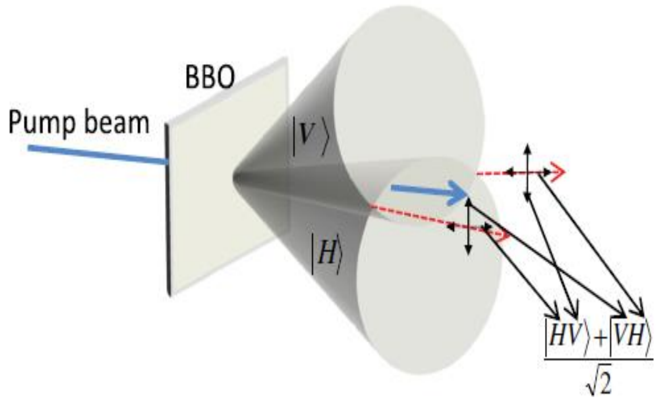
Thus,

$|\psi\rangle_{AB} \neq |\psi\rangle_A \otimes |\psi\rangle_B$ ⇒Entangled; Example:

$$|\psi\rangle_{AB} = \frac{(|00\rangle + |11\rangle)_{AB}}{\sqrt{2}}$$

Similarly, state is separable if $|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B$

Example: $|00\rangle, |10\rangle, |01\rangle, |11\rangle, \frac{|00\rangle \pm |01\rangle}{\sqrt{2}}$



Entanglement is superposition in the tensor product space

Recall: Outer product, tensor product and quantum gates again

- A gate *A* in general:

$$A = \sum_i |output_i\rangle\langle input_i|$$

- *SWAP* Gate

$$|xy\rangle \to |yx\rangle$$

$$\therefore |00\rangle \to |00\rangle, |01\rangle \to |10\rangle,$$
$$|10\rangle \to |01\rangle, |11\rangle \to |11\rangle$$

$$SWAP = |00\rangle\langle 00| + |10\rangle\langle 01| + |01\rangle\langle 10| + |11\rangle\langle 11|$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Similarly,

$CNOT$ maps

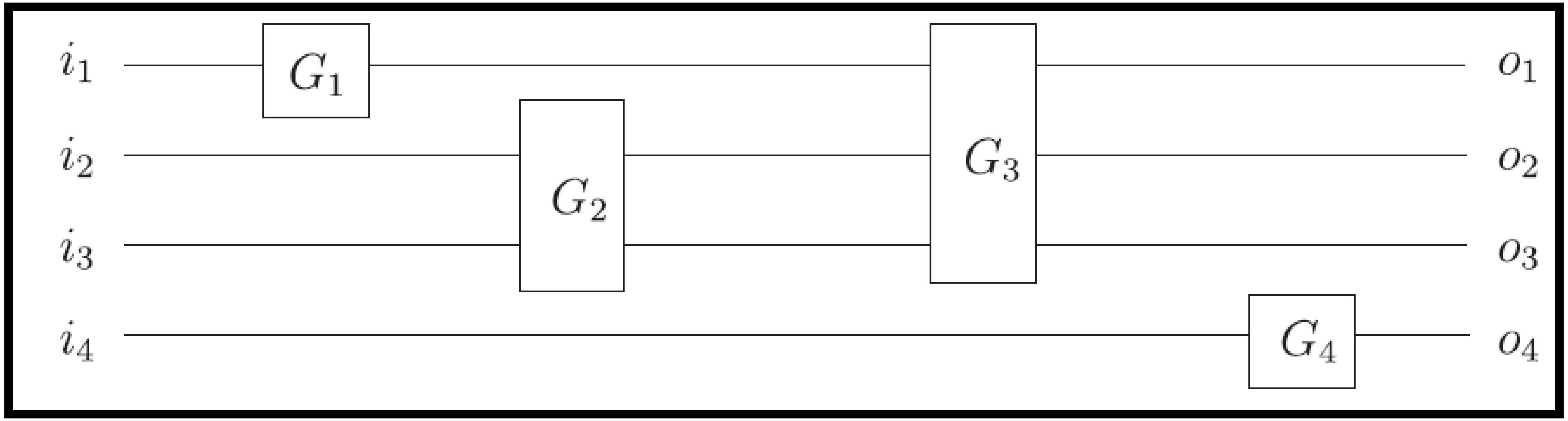
$$|00\rangle \to |00\rangle, |01\rangle \to |01\rangle,$$
$$|10\rangle \to |11\rangle, |11\rangle \to |10\rangle$$

$$CNOT = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

You can write your own code to simulate quantum circuits

Circuit model of computation



Linear Algebra Formulation of the Circuit Model

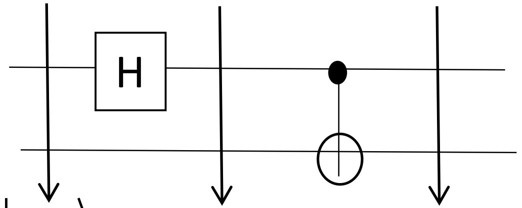
$$X|0\rangle \longrightarrow |1\rangle$$

$$X|1\rangle \longrightarrow |0\rangle$$

$$|\psi\rangle = (\alpha|0\rangle + \beta|1\rangle) = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$$

$$X|\psi\rangle = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \times \begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\beta\\ \alpha\end{pmatrix} = (\beta|0\rangle + \alpha|1\rangle)$$

Quantum circuit model



$$|00\rangle \qquad \frac{|00\rangle + |10\rangle}{\sqrt{2}} \qquad \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Check what a CNOT followed by Hadamard do

The work implemented in Qniverse

Quantum Information Processing (2022) 21:311
https://doi.org/10.1007/s11128-022-03650-2

Experimental realization of quantum anonymous veto protocols using IBM quantum computer

Satish Kumar[1] · Anirban Pathak[1]

Received: 18 November 2021 / Accepted: 3 August 2022

Let's understand the protocol

- There is a semi-honest voting authority (VA) named as Alice who conducts the voting. In the specific case implemented in Qniverse, Alice initially creates a Bell state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
- **Protocol A**:

Step A1: VA prepares a maximally entangled Bell state ($|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$), and keeps the first qubit (home qubit) with herself while sends the second qubit (travel qubit) to the first voter (V_1).

Step A2: V_1 applies $\sigma_z(t) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2^t}} \end{bmatrix}$ with $t = 0$ if he wishes to perform a veto; otherwise, he applies Identity operation $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. After the application of unitary on the travel qubit, V_1 sends the travel qubit to V_2, who encodes his vote in the similar manner and subsequently sends the travel qubit to V_3, and the process continues till V_n finally sends the travel qubit to VA after executing his voting right.

Note: $t + 1$ is the number of iterations of the protocol. Thus, $t = 0$ refers to the first iteration, and in the first iteration, to perform a veto, a voter would apply $\begin{pmatrix} 1 & 0 \\ 0 & e^{\iota\pi} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_z$. If odd number of vetos applied $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ will become $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ and a Bell measurement will reveal that but no veto and and even number of veto will yield $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and result will be nonconclusive.

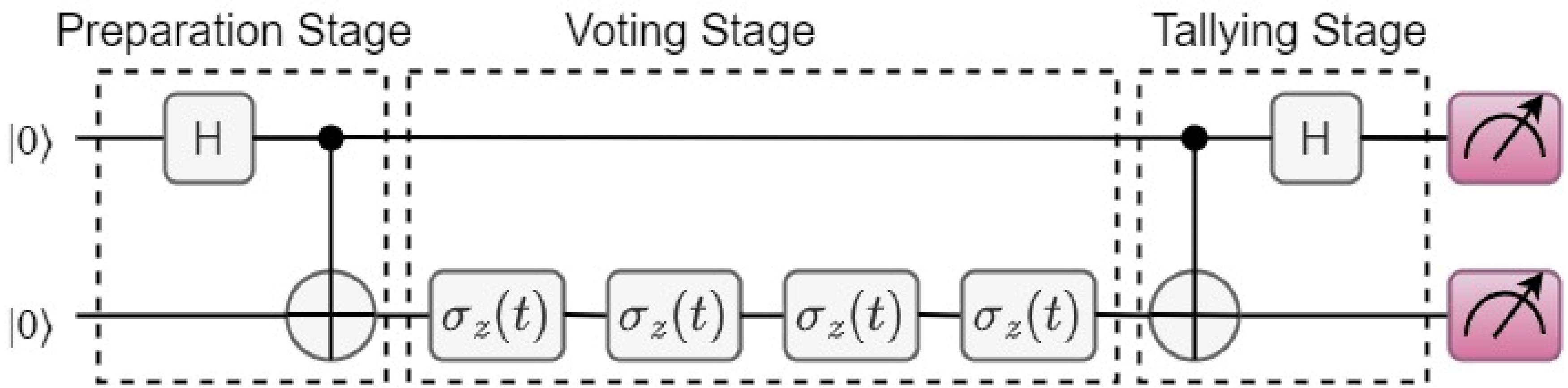
Protocol A: Continued

Step A3: VA performs a Bell measurement using the home qubit available with him and the travel qubit received from V_n.
Step A4: Steps A1–A3 are repeated for $t = 1$ and so on till one gets a conclusive result with each iteration increasing the value of t by one.

Example 1: There are 2 voters only. If the state after the first iteration is found to be $\frac{1}{\sqrt{2}}(|00\rangle - 11\rangle)$ then one of the voters has applied veto. However, if VA obtains $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ the result is nonconclusive as the outcome may arise for both applying veto or no one applying veto. In the next iteration to implement veto a voter has to apply $\begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\iota\pi}{2}} \end{pmatrix}$ and consequently combined effect of 2 voter applying veto will be $\begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\iota\pi}{2}} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\iota\pi}{2}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\iota\pi} \end{pmatrix} = \sigma_z$. So output state will be $\frac{1}{\sqrt{2}}(|00\rangle - 11\rangle)$ if both perform veto and $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ if no one perform veto.

Example 2: Four voters. If 1 or 3 perform veto after first iteration, we obtain $\frac{1}{\sqrt{2}}(|00\rangle - 11\rangle)$=> Conclusive result.
If two voters perform veto after second iteration, we obtain $\frac{1}{\sqrt{2}}(|00\rangle - 11\rangle)$=> Conclusive result.
If four voters perfrom veto after third iteration, we obtain $\frac{1}{\sqrt{2}}(|00\rangle - 11\rangle)$=> Conclusive result.

Example 2 elaborated



A quantum circuit for experimental realization of Protocol A in case of 4 voters.

- Voter applies $\sigma_z(t) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2^t}} \end{bmatrix}$ in t^{th} iteration if he wishes to perform a veto, otherwise he applies identity operation $\mathrm{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Example 2 elaborated

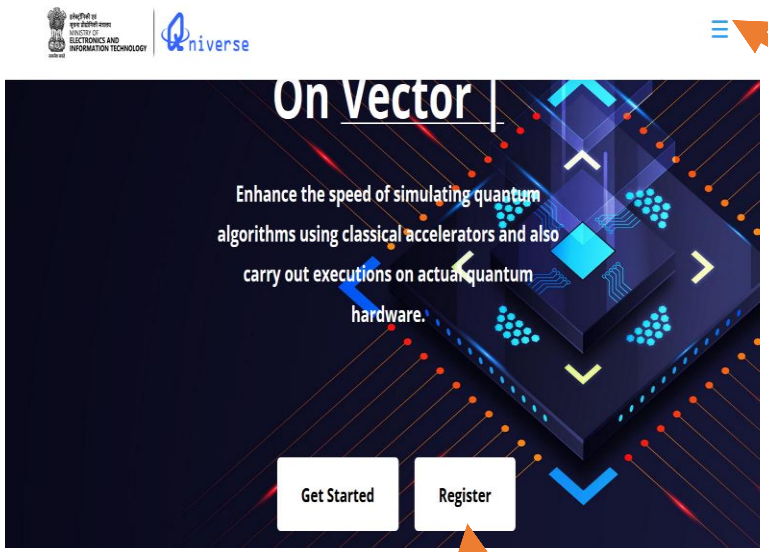
Case	Initial state	Number of veto	Which voter(s) has (have) vetoed	Iteration no.	Final state	Result	Simulator result (or expected measurement outcome)
1	$\|\phi^+\rangle$	0	No one	Iteration 1	$\|\phi^+\rangle$	Inconclusive	00
2	$\|\phi^+\rangle$	1	Any one voter among the 4 voters	Iteration 1	$\|\phi^-\rangle$	Conclusive	10
3	$\|\phi^+\rangle$	2	Any two of the 4 voters (e.g., 1st & 3rd or 3rd & 4th)	Iteration 1	$\|\phi^+\rangle$	Inconclusive	00
				Iteration 2	$\|\phi^-\rangle$	Conclusive	10
4	$\|\phi^+\rangle$	3	Any three of the 4 voters (e.g., 1st, 2nd & 4th or 1st, 3rd & 4th)	Iteration 1	$\|\phi^-\rangle$	Conclusive	10
5	$\|\phi^+\rangle$	4	All the four voters	Iteration 1	$\|\phi^+\rangle$	Inconclusive	00
				Iteration 2	$\|\phi^+\rangle$	Inconclusive	00
				Iteration 3	$\|\phi^-\rangle$	Conclusive	10

Quantum anonymous veto using Qniverse: Step-by-step guide

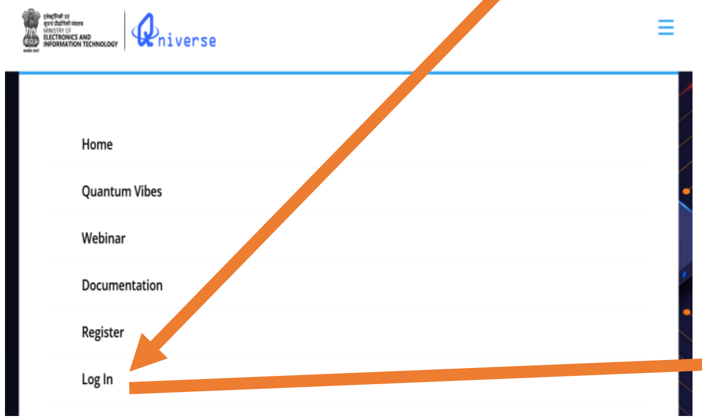
1. Go to https://qniverse.in/ (you can also start directly from https://qniverse.in/login/ and reach to the window shown in bottom right)
2. Register by clicking on Register as shown below

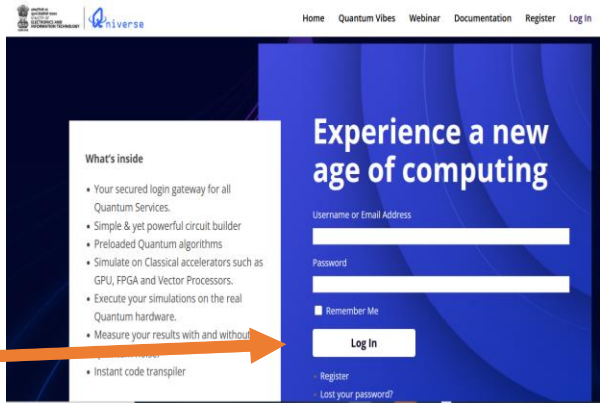
3. Login after registration (initially you will get 150 credits)

Click here to login



Click here to register

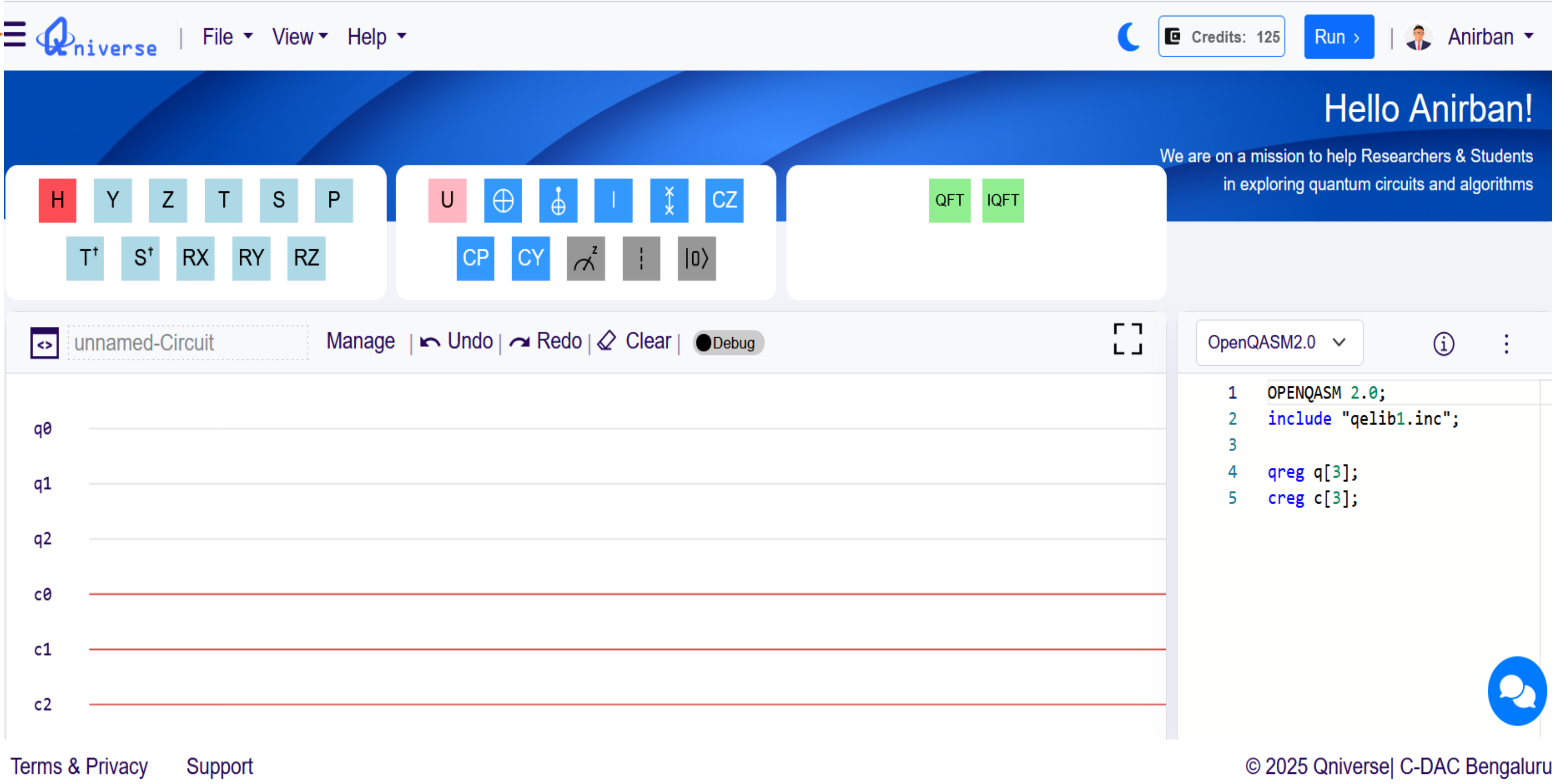


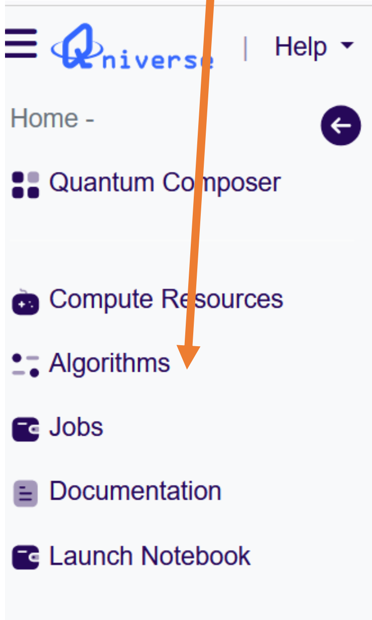


Quantum anonymous veto using Qniverse

Once you login, your screen will appear as below

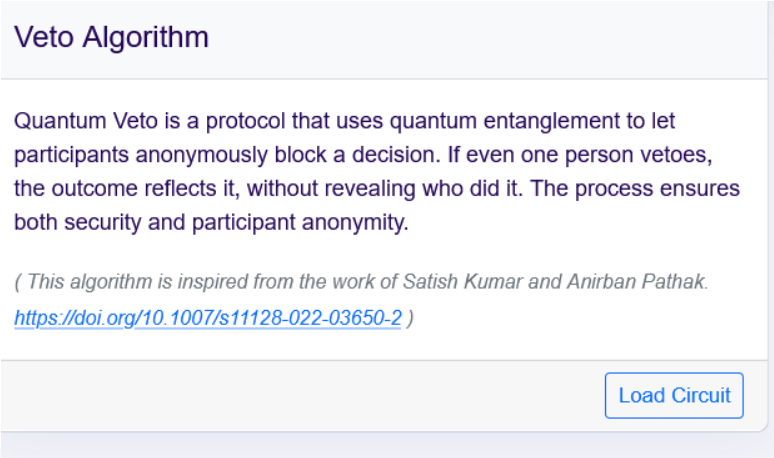
4. Click here first and then
5. Select the Algorithms icon (see below)

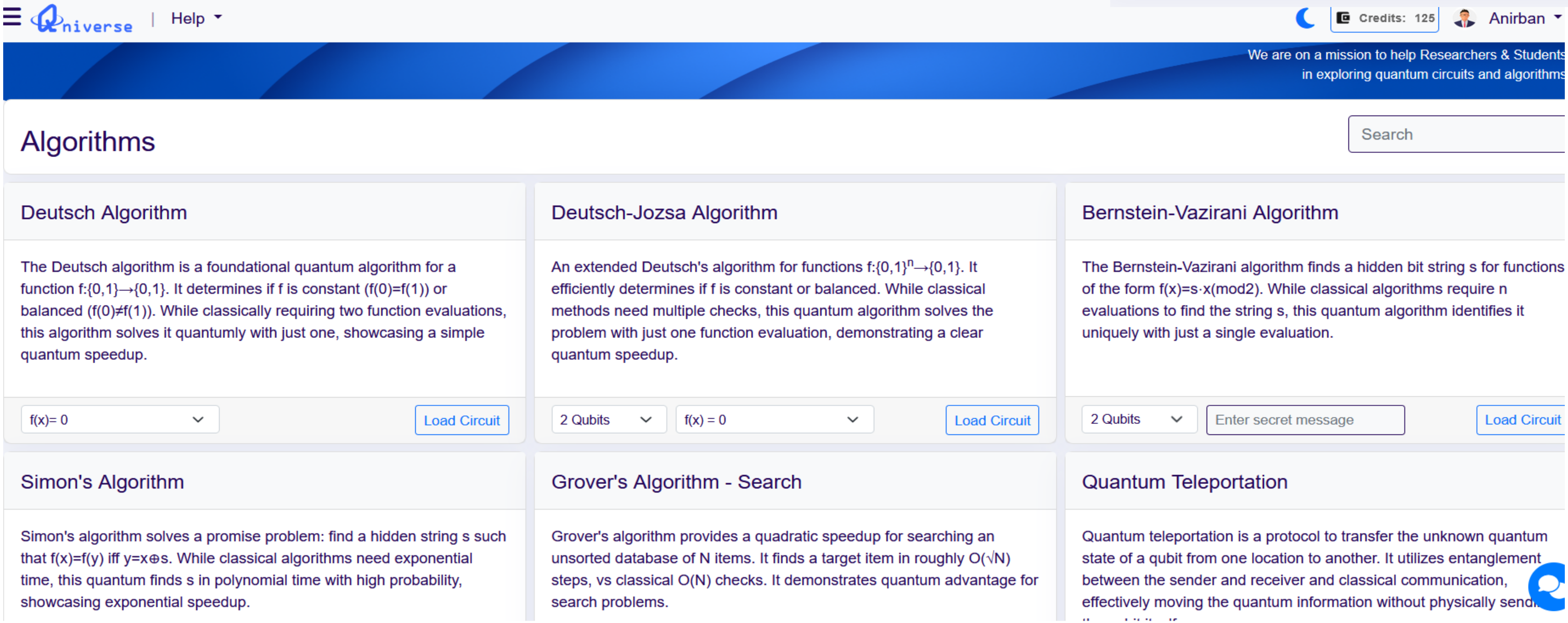




Quantum anonymous veto using Qniverse

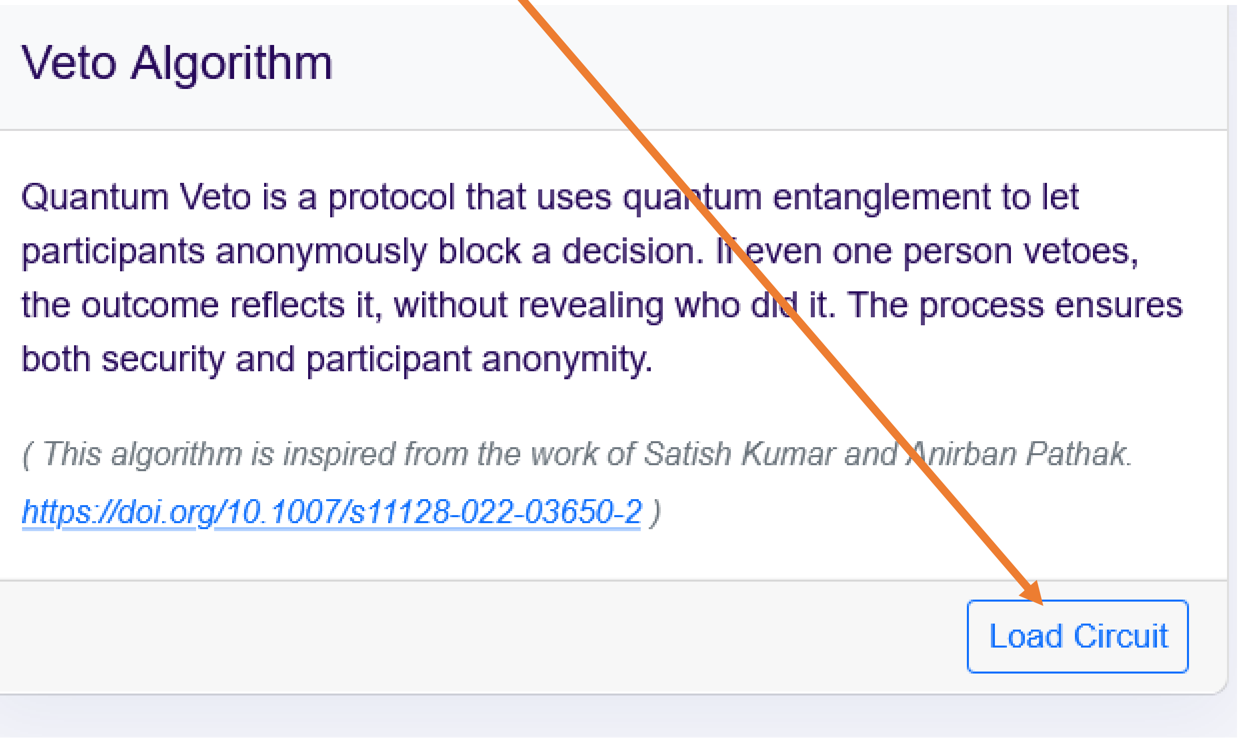
- 6. On clicking Algorithms icon you will see a window like this. Go down to find Veto Algorithm or just type veto in the search icon. Veto algorithm icon will appear like the one shown in right.



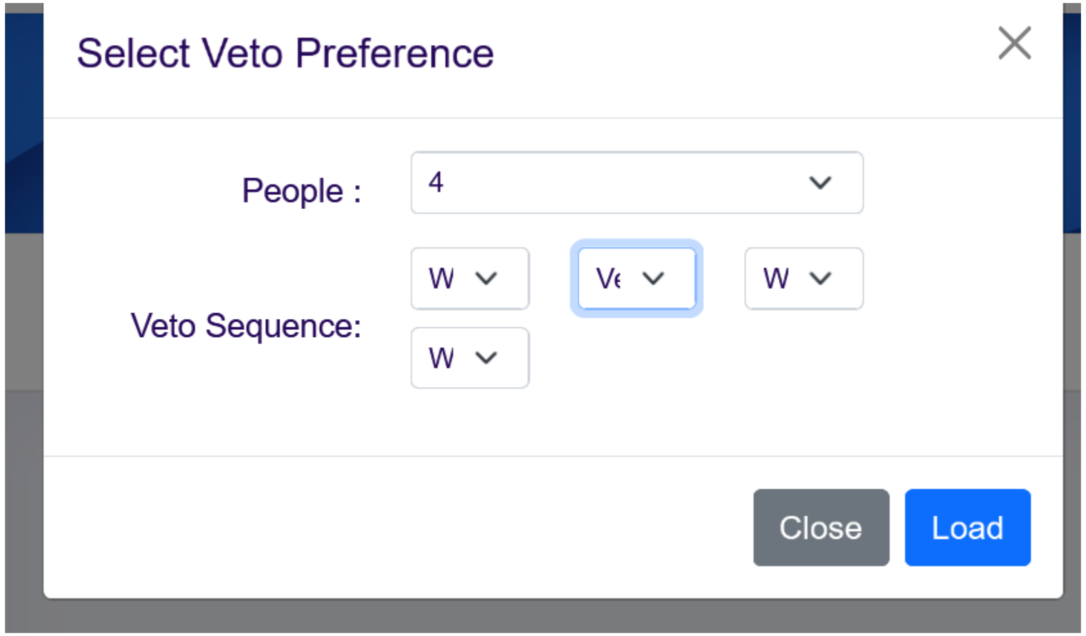


Quantum anonymous veto using Qniverse

7. Click on load circuit.

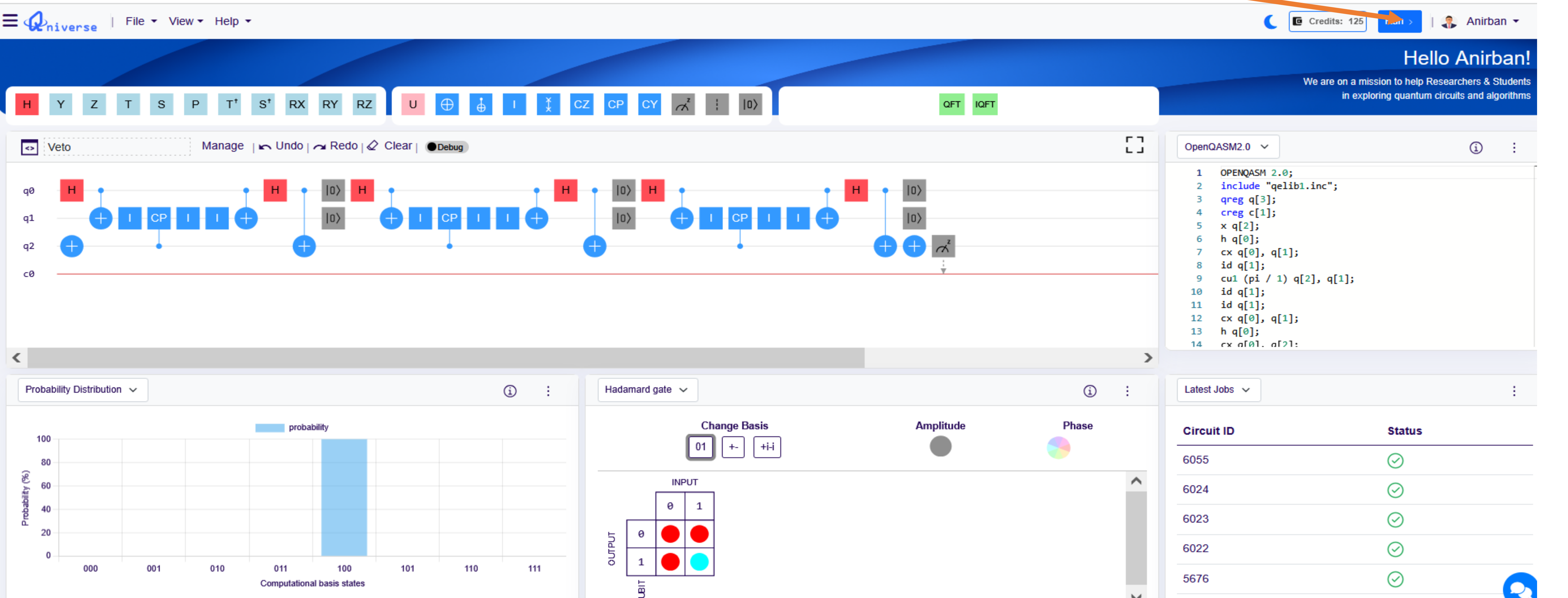


8. On clicking Load circuit following window will appear. Select the number of voters and who is using his right to veto here (let’s select four voters and 2nd is applying veto). Once selected press load.



Quantum anonymous veto using Qniverse

9. On clicking load an in-built iterative circuit will appear as shown below. To run it you have to click at Run icon in the top right.



Let’s play with Qniverse

1. Check number of iterations: If n number of voters participate in the process, then the maximum number of iterations required to arrive on conclusive result would be $1 + \log_2 n$ with every iteration eliminating half of the voting possibilities.

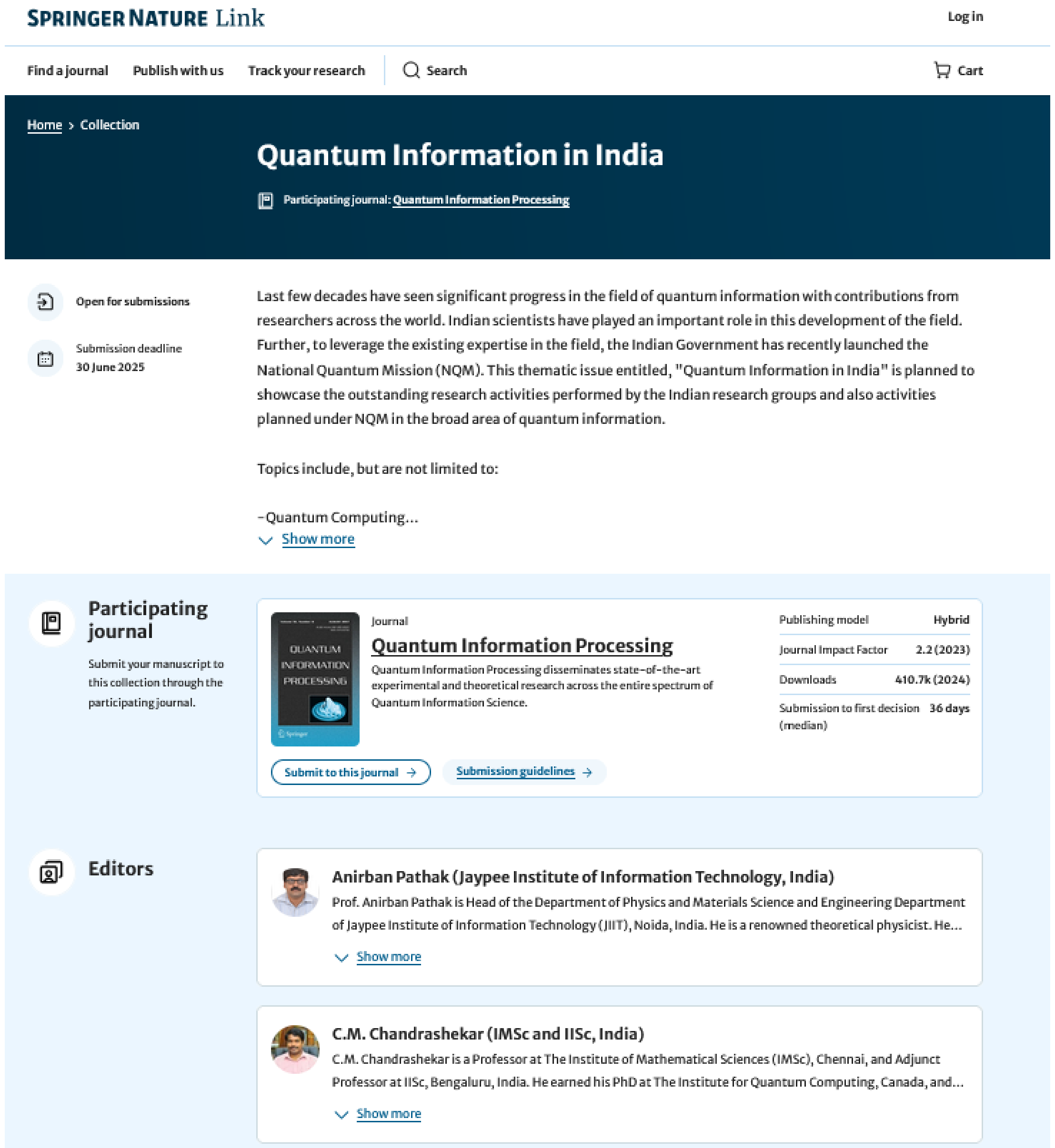
No of voter	Number of iteration
2	2
3-4	3
5-8	4
9-16	5

2. Let’s understand the circuit in view of the theoretical protocol. Check how the applied unitary to perform veto is changing with the number of iteration

Problems to play and learn: Implement other 6 protocols designed by us and protocols designed by others using Qniverse

Before we close: Some advertisements

- We have open position for JRF and RA in NQM project related to photonic quantum computing (apply by email as soon as possible)
- Our Department offers MSc (physics) with possible specialisation in Quantum Technologies, and PhD in Physics and we are always looking for bright students. MSc admission is still open.
- We also welcome interns



Thank you