Hybrid Quantum Classical Algorithms

George Siopsis

siopsis@tennessee.edu

Department of Physics and Astronomy

The University of Tennessee

Knoxville, TN 37996-1200, USA

Introduction

- Tools for quantum information processing / computation are low level.
- Standard formulation of quantum mechanics not sufficient for interplay of classical and quantum information processing.

► Need higher-level approach.

A plethora of models of quantum computation:

- Quantum circuit (discrete variables)
- Continuous variables (classical and quantum manipulations)
- Topological quantum computing
- One-way quantum computing
- Measurement-based quantum computing
- Adiabatic quantum computing
- Quantum classical hybrid methods (near-term applicability)

► Need higher-level language.

Quantum Field Theory

[1] K. Marshall, R. Pooser, G. Siopsis, and C. Weedbrook, Phys. Rev. A **92**, 063825 (2015).

[2] K. Yeter-Aydeniz and G. Siopsis, Phys. Rev. D **97**, 036004 (2018).

Algorithms for calculations in field theories very difficult on classical computers

- e.g., lattice field theory, which discretizes space. Classical computations on the lattice increase exponentially with number of sites.

We present a method of calculating scattering amplitudes in a scalar bosonic QFT with a quartic self-interaction using CV.

- Feasible with today's technology.
- Discrete version based on qubits by Jordan, Lee, and Preskill

  [Science **336**, 1130 (2012); Quant. Inf. Comput. **14**, 1014 (2014)]

Quantum Field Theory

One dimension for simplicity – can be generalized.

Scalar field ϕ, conjugate π; they obey $[\phi(x), \pi(x')] = i\delta(x - x')$.
Discretization: Choose units in which lattice spacing $a = 1$;
$x = 0, 1, \ldots, L - 1\ ,\ \ L \gg a$.
Commutation relations: $[\phi_x, \pi_{x'}] = i\delta_{xx'}$.
Periodic boundary conditions: $\phi_L = \phi_0$.
Free Hamiltonian

$$H_0 = \frac{1}{2}\int_0^L dx\left[\pi^2 + (\partial_x\phi)^2 + m^2\phi^2\right] \to \frac{1}{2}\sum_{n=0}^{L-1}\left[\pi_x^2 + (\phi_x - \phi_{x+1})^2 + m^2\phi_x^2\right]$$

Write $H_0 = \frac{1}{2}\boldsymbol{\pi}^T\boldsymbol{\pi} + \frac{1}{2}\boldsymbol{\phi}^T\boldsymbol{V}\boldsymbol{\phi}$. Eigenvalues and eigenvectors of $\boldsymbol{V}$,

$$\omega_k = m^2 + 4\sin^2\frac{\pi k}{N}\ ,\ \ e_x^k = \frac{1}{\sqrt{L}}e^{2\pi ikx/L}\ ,\ \ k = 0, \ldots, L - 1$$

Massless case: $\boldsymbol{V}$ has zero mode. Shift m by $\sim 1/L$ to avoid problems.

Initial state

Define $A_x = \frac{1}{\sqrt{2}}(\phi_x + i\pi_x)$. Commutation relations: $[A_x, A^\dagger_{x'}] = \delta_{xx'}$.
Define vacuum by $A_x|0\rangle = 0$ (product of vacuum fields).
Need ground state of H_0.

- Diagonalize H_0: Define $a_k = \sqrt{\frac{\omega_k}{2}}(\boldsymbol{e}^\dagger\boldsymbol{\phi})_k + \frac{i}{\sqrt{2\omega_k}}(\boldsymbol{e}^\dagger\boldsymbol{\phi})_k$.
  They obey $[a_k, a_l^\dagger] = \delta_{kl}$.

$$H_0 = \sum_{k=0}^{N-1} \omega_k \left(a_k^\dagger a_k + \frac{1}{2} \right)$$

  Ground state: $a_k|\Omega\rangle = 0$.

- Let $a_x = U^\dagger A_x U$, where U is Gaussian unitary ($\sim \mathcal{O}(L^2)$ gates).
  Ground state: $|\Omega\rangle = U^\dagger|0\rangle$.
  Similarly for excited states: $a_k^\dagger|\Omega\rangle = U^\dagger A_k^\dagger|0\rangle$.

Quantum Field Theory

Initial state: Single particle wavepacket: $\sum_k f_k a_k^\dagger |\Omega\rangle$
(f_k strongly peaked at $k = k_0$)
n-particle wavepackets ($n \geq 2$) similar.

Quantum computation

Calculate scattering amplitude

$$\mathcal{A} = \langle \mathrm{out} | T \exp \left\{ i \int_{-T}^{T} dt [H_{\mathrm{int}}(t) + H_{\mathrm{c.t.}}(t)] \right\} | \mathrm{in} \rangle$$

in the limit $T \to \infty$, with quartic interaction and counterterm, respectively,

$$H_{\mathrm{int}} = \frac{\lambda}{4!} \int_0^L dx \phi^4 \to \frac{\lambda}{4} \sum_x \phi_x^4 \ , \quad H_{\mathrm{c.t.}} = \frac{\delta_m}{2} \int_0^L dx \phi^2 \to \frac{\delta_m}{2} \sum_x \phi_x^2$$

Time evolution w.r.t. H_0, implemented via successive unitaries

$$U(t) = e^{i\delta t H_{\mathrm{int}}} e^{i\delta t H_{\mathrm{c.t.}}} e^{i\delta t H_0}$$

Quantum Field Theory

Coupling constants are turned on and off adiabatically.
Unitaries $e^{i\delta t H_0}$ and $e^{i\delta t H_{\mathrm{c.t.}}}$ are Gaussian.
Remaining unitary is implemented through quartic phase gates,

$$e^{i\delta t H_{\mathrm{int}}} = \prod_x e^{i\delta t \frac{\lambda}{4!}\phi_x^4}$$

Final measurement

Final state: $|\mathrm{out}\rangle = a_{k_1}^\dagger a_{k_2}^\dagger \cdots |\Omega\rangle = U^\dagger A_{k_1}^\dagger A_{k_2}^\dagger \cdots |0\rangle$
Uncompute by applying the Gaussian unitary U, and then measure number of photons in each mode.
► need photon-number-resolving detectors with high efficiency.

- Polynomial growth of complexity (also with qubits), to be compared with exponential growth in classical lattice computations.
- Feasible with current linear optical technology.

Non-Gaussian Gates

K. Marshall, R. Pooser, G. Siopsis, and C. Weedbrook, Phys. Rev. A **91**, 032321 (2015).

To achieve universal quantum computation using continuous variables (CV) $\hat{x}$ and $\hat{p}$ (quadrature operators), one needs a non-Gaussian element, such as a cubic or higher order phase gate,

$$\hat{U} = e^{iP_n(\hat{x})}$$

where P_n is a *real* polynomial of degree n ($n \geq 3$).

- Readily available set of Gaussian operations, corresponding to Hamiltonians of first and second powers of $\hat{x}$ and $\hat{p}$.
- Need Hamiltonian that is a polynomial of $\hat{x}$ and $\hat{p}$.
  - ► hard to implement.

Non-Gaussian Gates

To implement $\hat{U}$, we first approximate it

$$\hat{U} = \left(1 + \frac{i}{N} P_n(\hat{x})\right)^N + \mathcal{O}(1/N)$$

Then we decompose this operation into linear factors

$$1 + \frac{i}{N} P_n(\hat{x}) = \mathcal{U}_0 \mathcal{U}_1 \cdots \mathcal{U}_{n-1}$$

where $\mathcal{U}_l = 1 + \gamma_l \hat{x}$ ($l = 0, 1, \ldots n-1$).

- Note that $|\mathcal{U}_0 \mathcal{U}_1 \cdots \mathcal{U}_{n-1}|^2 = 1 + \mathcal{O}(1/N^2)$
  - norm of state is approximately preserved.

Next: implement the linear operators $\mathcal{U}_l$.

Non-Gaussian Gates

To implement $\mathcal{U}_l = 1 + \gamma_l \hat{x}$ on an arbitrary state $|\psi\rangle = \int dx\, \psi(x)|x\rangle$,

- first prepare a coherent state (resource mode)

$$|\alpha_1\rangle_R = D(\alpha_1)|0\rangle_R \ , \quad D(\alpha_1) = \exp(\alpha_1 \hat{a}_R^\dagger - \alpha_1^* \hat{a}_R) \ , \quad \alpha_1 \in \mathbb{R}$$

- then interact our state of interest with the coherent state under the two-mode operator $U_2(\beta_1) = \exp[(\beta_1 \hat{a}_R^\dagger - \beta_1^* \hat{a}_R)\hat{x}]$, $\beta_1 = \gamma_l \alpha_1$
  - ► quantum non-demolition (QND) gate
  - ► requires two offline squeezed ancilla states

    [Yoshikawa, Miwa, Huck, Andersen, van Loock, Furusawa, PRL **101**, 250501 (2008)]

- arrive at the state ($\zeta_l = \alpha_1(1 + \gamma_l x)$)

$$|\Psi\rangle = \int dx\, \psi(x) U_2(\beta_1) D_R(\alpha_1)|x\rangle|0\rangle_R = \int dx\, \psi(x)|x\rangle|\zeta_l\rangle_R$$

- Next step: two different methods.

Non-Gaussian Gates

Method 1.

- theoretically simple but experimentally challenging

Apply a non-demolition measurement on the resource mode projecting it onto the space orthogonal to $|0\rangle$, i.e. ($P_{\bar{0}} = \hat{\mathbb{1}} - |0\rangle\langle 0|$),

$$P_{\bar{0}}|\zeta_l\rangle_R = \sum_{k=1}^{\infty} \frac{1}{\sqrt{k!}} \zeta_l^k |k\rangle_R \approx \zeta_l |1\rangle_R$$

Error in approximation is negligible for small x, significant for large x.

$$|\Psi\rangle \to \int dx\, \psi(x)(1 + \gamma_l \hat{x})|x\rangle|1\rangle_R = \int dx\, \psi(x)\mathcal{U}_l|x\rangle|1\rangle_R,$$

Probabilistic approach: measurement may fail, however if it does, simply discard the mode and attempt the procedure again.

Non-Gaussian Gates

Method 2.

- can feasibly be demonstrated with currently available technology

Pass the resource mode through a beam splitter of high transmittance T mixing it with a vacuum input $|0\rangle_b$

$$|\Psi\rangle|0\rangle_b \to \int dx\, \psi(x)|x\rangle|\sqrt{T}\zeta_l\rangle_R| - \sqrt{1-T}\zeta_l\rangle_b$$

Weak ancillary mode $\Rightarrow$ b-mode $\approx |0\rangle_b - \sqrt{1-T}\zeta_l|1\rangle_b$.

Send b-mode to a photodetector $\Rightarrow$ success if it clicks.

No click $\Rightarrow$ state $\int dx\, \psi(x)|x\rangle|\sqrt{T}\zeta_l\rangle_R|0\rangle_b$, and b-mode decouples.

$\hookrightarrow$ Repeat-until-success without change in state except for attenuation.

$\hookrightarrow$ Need $M \sim \mathcal{O}(1/p)$ steps, where p is the probability of subtracting a single photon.

Non-Gaussian Gates

New state: $|\Psi\rangle|0\rangle_b \to \int dx\, \psi(x)(1+\gamma_l \hat{x})|x\rangle|T^{M/2}\alpha_1(1+\gamma_l x)\rangle_R|1\rangle_b$

Decouple the resource mode by applying the QND gate $U_2(-T^{M/2}\alpha_1\gamma_l)$,

$$|\Psi\rangle|0\rangle_b \to \int dx\, \psi(x)\mathcal{U}_l|x\rangle|T^{M/2}\alpha_1\rangle_R|1\rangle_b$$

$\Rightarrow$ desired gate.

Detector imperfections:

- Efficiency $\eta < 1$

  (have successfully subtracted a photon but are unaware of this fact; attempt further photon subtractions increasing the power on the factor $(1+\gamma\hat{x})^{k>1}$ in an undesired manner)

- dark count $\nu > 0$

  (we believe we have subtracted a photon when we have not; one of the $\mathcal{U}_l$ operators is replaced by the identity operation).

Non-Gaussian Gates

Alternative cubic gates

- *Gottesman-Kitaev-Preskill (GKP) scheme* [PRA **64**, 012310 (2001)]
  - ► Create EPR Gaussian pair, and mix one of the oscillators with a coherent beam for large shift in momentum. Then measure number of photons. Then squeeze.

  Problem: Large squeezing needed – impossible with current technology.

- *Marek-Filip-Furusawa (MFF) scheme* [PRA **84**, 053802 (2011)]
  - ► Apply a QND gate on the system and appropriate resource state. Then perform homodyne measurement on resource state followed by a feed-forward Gaussian unitary.

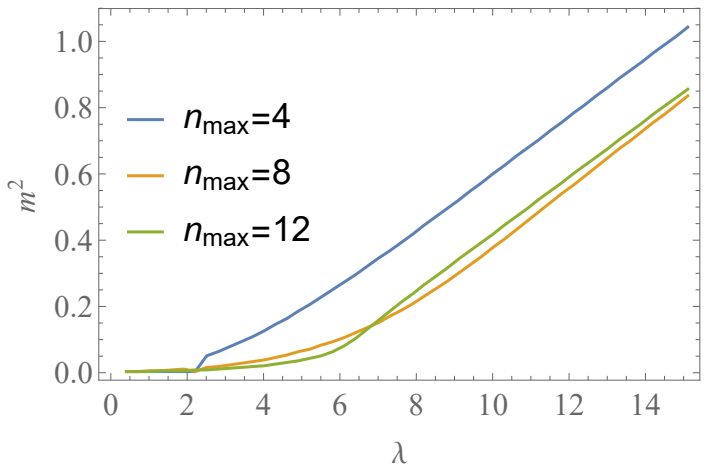
  Problem: Resource state is a superposition with up to 3 photons. To create it, simultaneous 3-photon subtraction is needed.

Variational Method

K. Yeter-Aydeniz, E. F. Dumitrescu, A. J. McCaskey, R. S. Bennink, R. C. Pooser, and G. Siopsis, arXiv:1811.12332 [quant-ph].

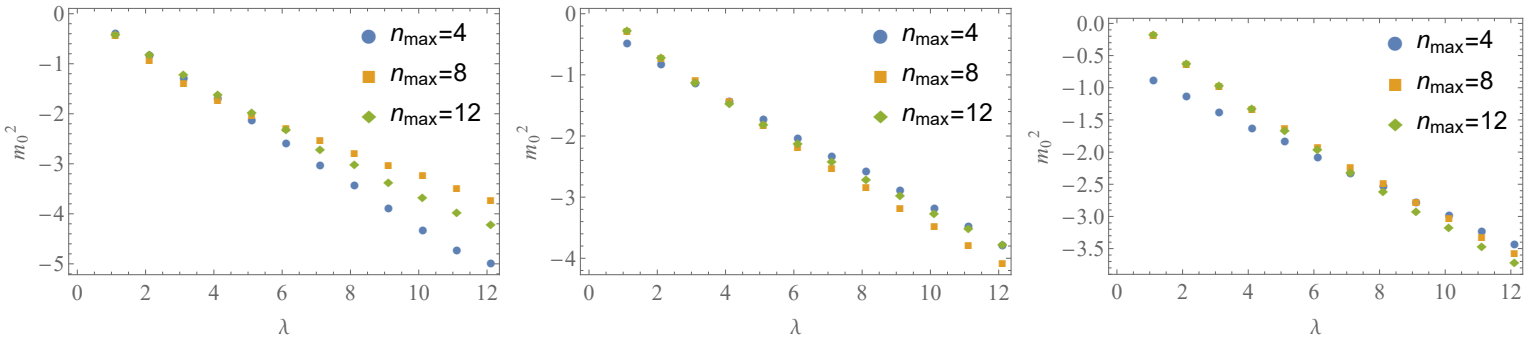
Calculate eigenvalues using variational method. Hybrid algorithm:

- Quantum calculation of trial state.
- Classical variational computation.

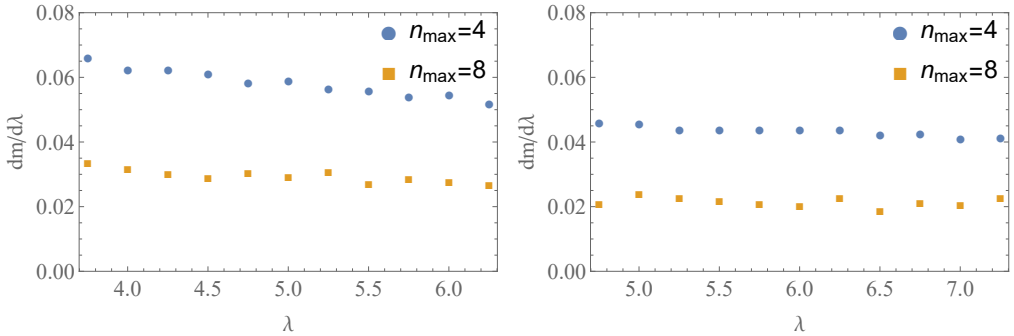


The mass gap *vs.* the interaction coefficient λ for $m_0^2 = -1.5$, $L = 2$, and Hilbert space cutoff $n_{\text{max}} = 4, 8, 12$.

Quantum Field Theory



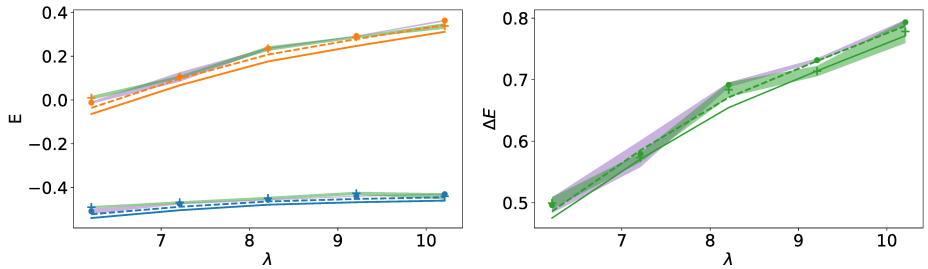
m_0^2 *vs.* interaction coefficient λ for $L = 2$, mass gap $m^2 = 0.1, 0.25, 0.5$, and cutoff $n_{\text{max}} = 4, 8, 12$.



The dependence of the gap m on the interaction coefficient λ, for $L = 2$, Hilbert space cutoff $n_{\text{max}} = 4, 8$, and bare mass parameters $m_0^2 = -1.5, -2.5$ (upper and lower panel, respectively) as $m \to 0$ showing that $\frac{dm}{d\lambda}$ approaches a constant at criticality ($m \sim |\lambda - \lambda_c|^{\nu}$, $\nu = 1$ in 1d).

Quantum Field Theory

Experimental results on IBM Tokyo quantum processor consisting of 20 fixed-frequency transmon qubits.



Experimentally optimized ground and lowest lying excited energies as a function of the interaction parameter λ are given in the left panel. Experimentally determined mass gaps $\Delta E = E_1 - E_0$ are given in the right panel. The dashed (solid) lines correspond to the theoretically optimal product (entangled) ansatz energies, which are obtained by noiseless numerical simulation. Experimental results for the product (entangled) ansatz are given by the $\bullet$ $(+)$ markers, where purple (green) error bars indicating one standard deviation are determined by repeated sampling of the energy functional at the optimal parameters. For all data points, we have taken $m_0^2 = -1.5$.

Quantum Machine Learning

[1] H.-K. Lau, R. Pooser, G. Siopsis, and C. Weedbrook, Phys. Rev. Lett. **118**, 080501 (2017).

[2] S. Das, G. Siopsis, and C. Weedbrook, Phys. Rev. A **97**, 022315 (2018).

[3] G. Siopsis, arXiv:1804.01558 [quant-ph].

Machine learning involves using specially tailored *learning algorithms* to make important predictions in fields as varied as finance, business, fraud detection, and counter terrorism.

Quantum machine learning using discrete variables (DV) has provided schemes that have shown exponential speedup in *learning algorithms*, such as supervised and unsupervised learning, support vector machine, cluster assignment, etc.

- We developed CV tools and subroutines that form the basis of exponential speedup in *learning algorithms*:
  - matrix inversion
  - principal component analysis

Quantum Machine Learning

Encoding

Classical data set $\mathbf{a} = \{a_x; x = 1, \ldots, N\}$, $N = 2^n$.

Need n qubits to encode. Basis states: $|x\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle$ ($x_i = 0, 1$).
State: $|f\rangle = \int f(\mathbf{q})|\mathbf{q}\rangle d^n q$, $f(\mathbf{q}) = \sum_x a_x \langle \mathbf{q}|x\rangle$. To create it,

- start with $|\Psi_0\rangle = 2^{-n/2} \sum_x |x\rangle$.
- Repeatedly apply the Grover operators $e^{i\pi|\Psi_0\rangle\langle\Psi_0|}$, and $e^{i\phi|x\rangle\langle x|}$.
- Complexity (number of oracle calls) is polynomial in n, if $|a_x| \lesssim 2^{-n/2}$, $\forall x$ (e.g., for states close to $|\Psi_0\rangle$), and can be as high as $\mathcal{O}(2^{n/2})$.

  [Soklakov and Schack, PRA **73**, 012307 (2006)]

Quantum Machine Learning

To implement the generalized Grover operator $e^{it\rho'}$, for a given state ρ', repeatedly apply the exponential swap operator tracing out the auxiliary mode,

$$\mathrm{tr}_{\rho'}\left(e^{i\delta t\mathcal{S}}\rho\otimes\rho' e^{-i\delta t\mathcal{S}}\right)=e^{\delta t\rho'}\rho e^{-i\delta t\rho'}+\mathcal{O}(\delta^2)$$

where $\mathcal{S}|\psi_1\rangle|\psi_2\rangle=|\psi_2\rangle|\psi_1\rangle$. [Lloyd, Mohseni, and Schack, PRA **73**, 012307 (2006)]

Exponential swap gate:

$e^{i\delta t\mathcal{S}}|\psi_1\rangle_a|\psi_2\rangle_b=\cos\delta t|\psi_1\rangle_a|\psi_2\rangle_b+i\sin\delta t|\psi_2\rangle_a|\psi_1\rangle_b$

To implement it, introduce auxiliary modes 1 and 2 in the state $|+\rangle\equiv\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)$, rotation (Gaussian) $R(\delta t)=e^{i\theta(\hat{c}_1\hat{c}_2^\dagger+\hat{c}_2\hat{c}_1^\dagger)}$ and

$$U_{\mathrm{CSWAP}}=e^{-\frac{\pi}{4}(\hat{a}\hat{b}^\dagger-\hat{b}\hat{a}^\dagger)}e^{i\pi\hat{c}_1^\dagger\hat{c}_1\hat{a}^\dagger\hat{a}}e^{\frac{\pi}{4}(\hat{a}\hat{b}^\dagger-\hat{b}\hat{a}^\dagger)}$$

swapping modes a and b depending on photon number of auxiliary mode 1.

Quantum Machine Learning

U_{CSWAP} includes non-Gaussian gate

$$e^{i\pi H_1 H_a} \ , \quad H_1 = \hat{p}_1^2 + \hat{x}_1^2 \ , \quad H_a = \hat{p}_a^2 + \hat{x}_a^2$$

implemented as, e.g.,

$$e^{i\pi H_1 H_a} = \left(e^{\frac{i\pi}{K}\hat{p}_1^2 \hat{p}_a^2} e^{\frac{i\pi}{K}\hat{p}_1^2 \hat{x}_a^2} e^{\frac{i\pi}{K}\hat{x}_1^2 \hat{p}_a^2} e^{\frac{i\pi}{K}\hat{x}_1^2 \hat{x}_a^2} \right)^K + \mathcal{O}(1/K)$$

First three factors in terms of the last factor, respectively,

$$e^{\frac{i\pi}{K}\hat{p}_1^2 \hat{p}_a^2} = e^{\frac{i\pi}{2}H_1} e^{\frac{i\pi}{2}H_a} e^{\frac{i\pi}{K}\hat{x}_1^2 \hat{x}_a^2} e^{-\frac{i\pi}{2}H_a} e^{-\frac{i\pi}{2}H_1} \ , \ \text{etc.}$$

Last factor in terms of quartic gates

$$e^{\frac{i\pi}{K}\hat{x}_1^2 \hat{x}_a^2} = e^{2ip_1 x_a} e^{\frac{i\pi}{12K}\hat{x}_1^4} e^{-4ip_1 x_a} e^{\frac{i\pi}{12K}\hat{x}_1^4} e^{2ip_1 x_a} e^{-\frac{i\pi}{6K}\hat{x}_1^4} e^{-\frac{i\pi}{6K}\hat{x}_a^4}$$

Exponential swap gate: $e^{i\delta t \mathcal{S}} = U_{\mathrm{CSWAP}} R(\delta t) U_{\mathrm{CSWAP}}$

Quantum Machine Learning

Matrix inversion

ML applications involve high-dimensional linear equations, $\mathbf{A}\mathbf{y} = \mathbf{b}$.

- ▶ $\mathbf{A}$ hermitian, $\mathbf{A}\mathbf{e}_i = \lambda_i \mathbf{e}_i$, $\mathbf{b} = \sum_i b_i \mathbf{e}_i$.
- ▶ Solution $\mathbf{y} = \mathbf{A}^{-1}\mathbf{b} = \sum_i \frac{1}{\lambda_i} b_i \mathbf{e}_i$ more efficient in DV QC.

[Harrow, Hassidin, and Lloyd, PRL **103**, 150502 (2009)]

For CV QC,

- Prepare $|\mathbf{b}\rangle$ and 2 auxiliary modes in $|q_1 = 0\rangle|q_2 = 0\rangle$.
- Apply the Grover operator $e^{i\gamma A p_1 p_2}$ (γ is adjustable).
- Measure q_1, projecting onto $\sum_i \beta_i \int dp_2 \delta(\gamma\lambda_i p_2 - q_1)|\mathbf{e}_i\rangle|q_1\rangle|p_2\rangle$.
- Measure q_2. Final state: $\sum_i \frac{1}{\lambda_i}\beta_i e^{-i\frac{q_1 q_2}{\gamma\lambda_i}}|\mathbf{e}_i\rangle|q_1\rangle|q_2\rangle$.
  - ▶ Desired solution as $\gamma \to \infty$.

Challenge: Realistically, eigenstates of quadrature $\to$ *squeezed* states.

Principal component analysis

Is vector $\mathbf{b}$ an eigenvector of $\mathbf{A}$, and what is the corresponding eigenvalue?

- ubiquitous in science and engineering
- also in quantum tomography, supervised learning and cluster assignment.

Solution with CV QC:

- Prepare $|\mathbf{b}\rangle$ and an auxiliary mode in $|q_1 = 0\rangle$.
- Apply the Grover operator $e^{i\gamma A p_1 p_2}$ (γ is adjustable).
- Measure q_1, projecting onto $\sum_i \beta_i \delta(\gamma\lambda_i - q_1)|\mathbf{e}_i\rangle|q_1\rangle$.
  - measurement outcome is proportional to one of the eigenvalues ($q_1 = \lambda_i/\gamma$) for which $\beta_i \neq 0$.
  - most probable outcome corresponds to the maximum $|\beta_i|^2$.
  - We obtain that outcome with certainty, if $|\mathbf{b}\rangle$ is an eigenstate of $\mathbf{A}$.

Vector distance

In supervised ML, new data categorized into groups by similarity to previous data. E.g., the belonging category of a vector $\mathbf{u}$ is determined by its distance to the average value of previous data, $D = |\mathbf{u} - \frac{1}{M}\sum_{i=1}^{M}\mathbf{v}_i|$.

▶ DV QC solution by Rebentrost, Mohseni, and Lloyd [PRL **113**, 130503 (2014)].

Solution with CV QC (assume $|\mathbf{u}| = |\mathbf{v}_i| = 1$, for simplicity):

- Data encoded in reference mode with the aid of an index mode,

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_I|\mathbf{u}\rangle_R + \frac{1}{\sqrt{M}}\sum_{i=1}^{M}|i\rangle_I|\mathbf{v}_i\rangle_R\right)$$

- Apply $e^{i\frac{\pi}{4}\mathcal{S}_{12}\mathcal{S}_{IR}}$ on data and auxiliary modes in coherent state $|\beta\rangle_1|0\rangle_2$.
- Trace out index and reference modes to get state of auxiliary modes

$$\rho_{12} = \frac{1}{2}|\beta 0\rangle\langle\beta 0| - iD^2|\beta 0\rangle\langle 0\beta| + iD^2|0\beta\rangle\langle\beta 0| + \frac{1}{2}|0\beta\rangle\langle 0\beta|$$

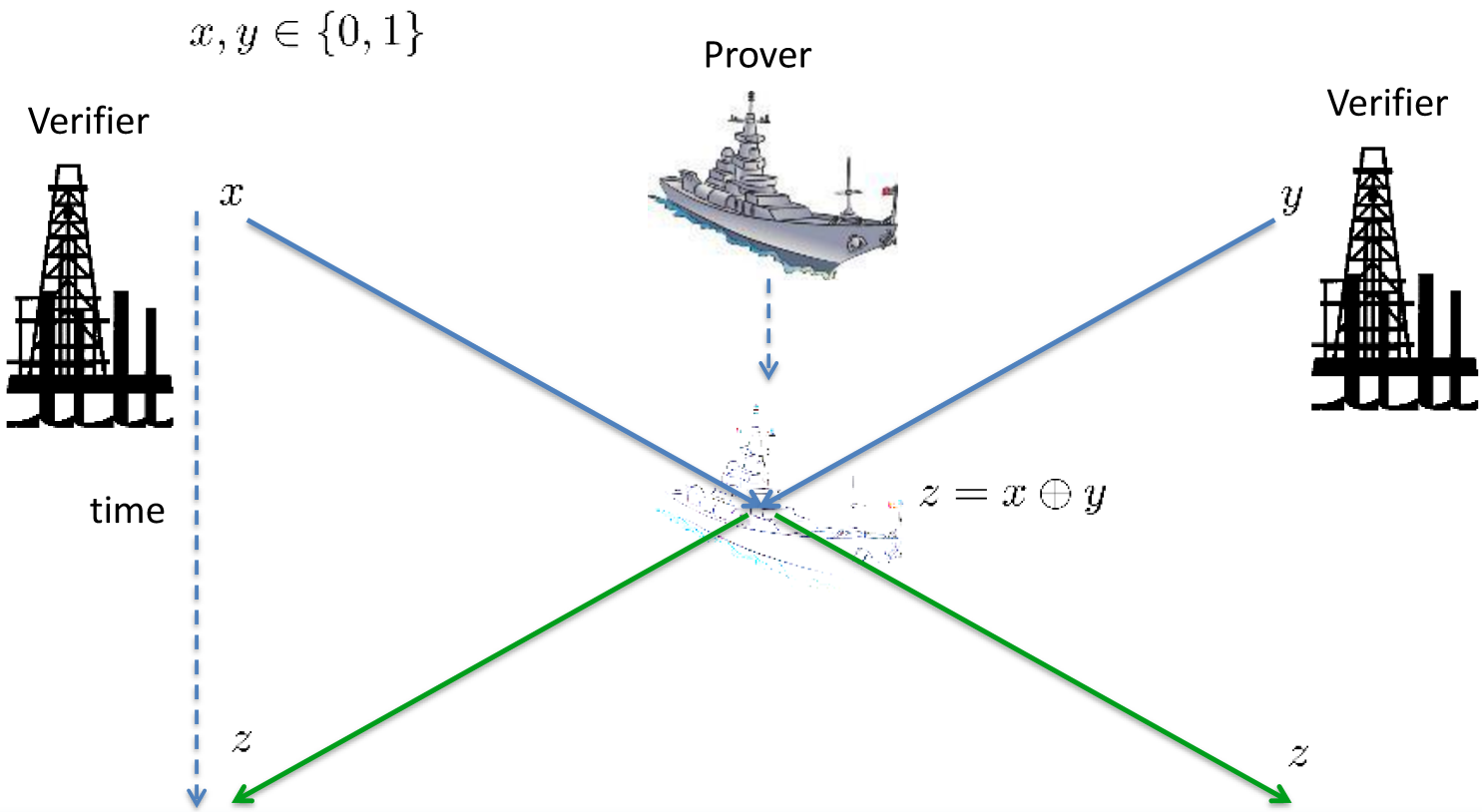
Quantum Machine Learning

- Measure P quadrature of first mode (homodyne detection).
  Probability of obtaining value p

$$\mathcal{P}(p) \propto e^{-p^2} \left(1 + 2D^2 \sin \sqrt{2}\beta p\right)$$

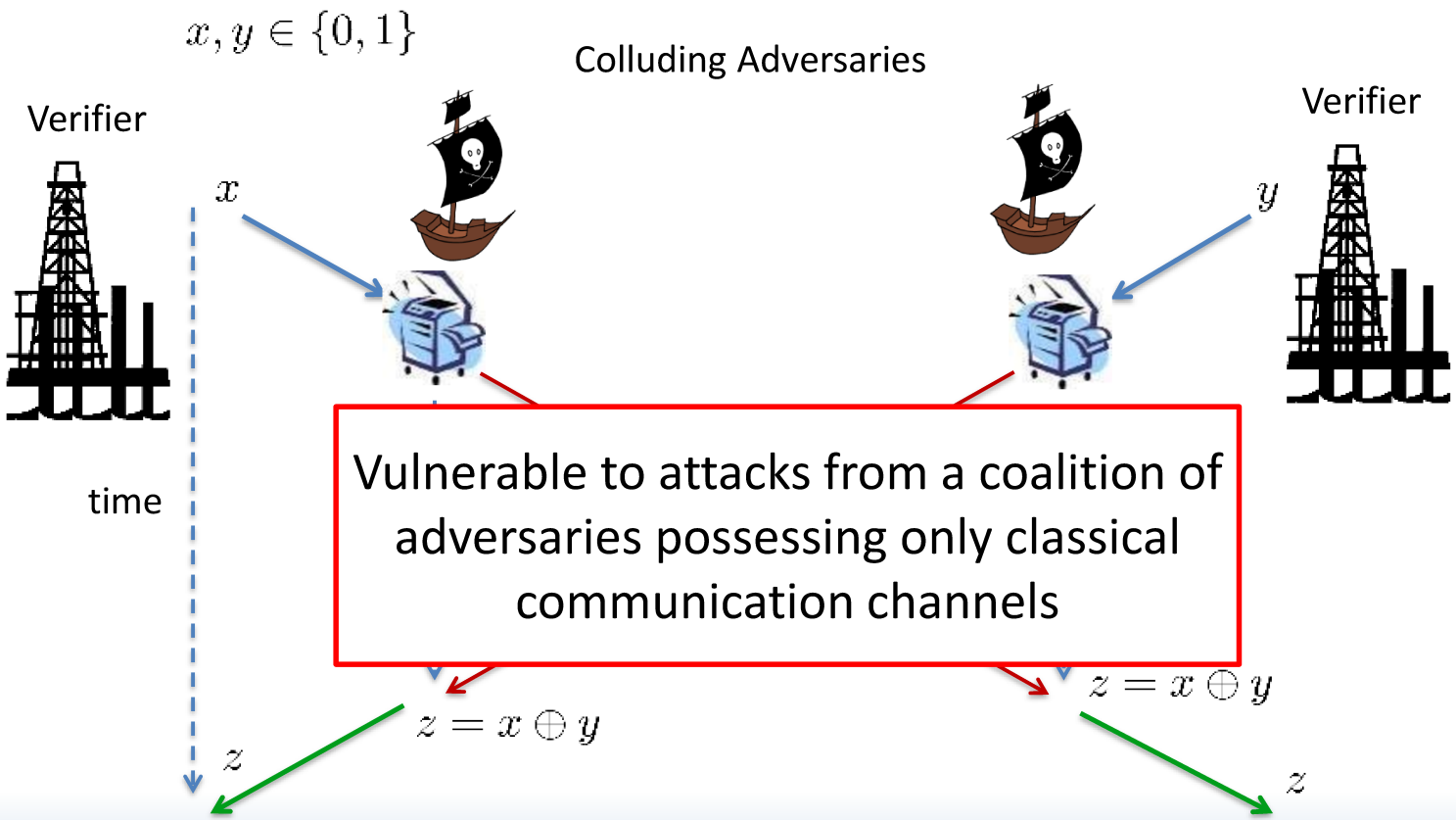
- D can be deduced from, e.g., $\mathcal{P}(p > 0) - \mathcal{P}(p < 0) \approx 0.2D^2$, for $\beta \gtrsim 4$.

Position based cryptography (PBC)



Chandran, *et al.*, *Lect. Notes Comput. Sci.* **5677**, 391 (2009).

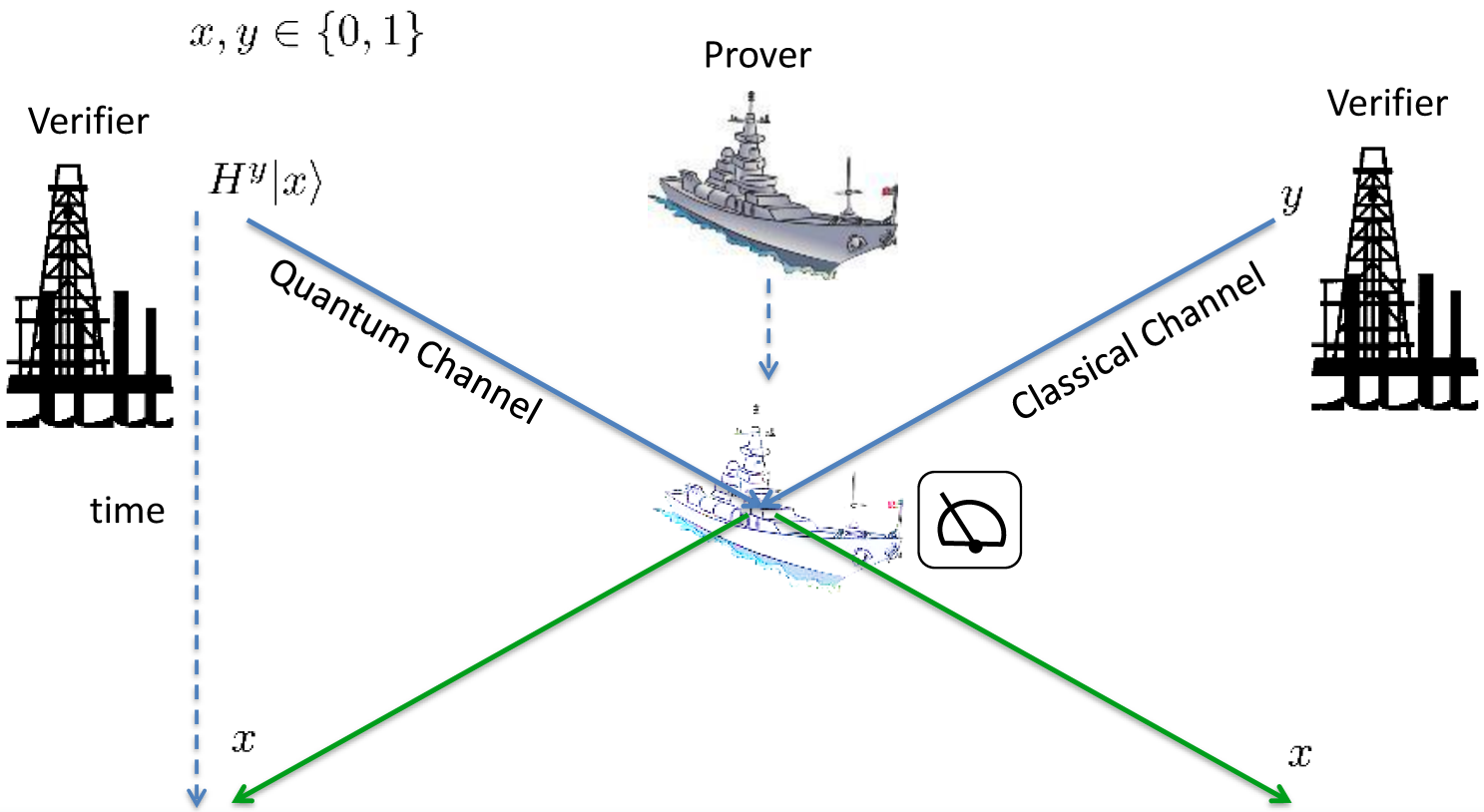
Position based cryptography (PBC)



Vulnerable to attacks from a coalition of adversaries possessing only classical communication channels

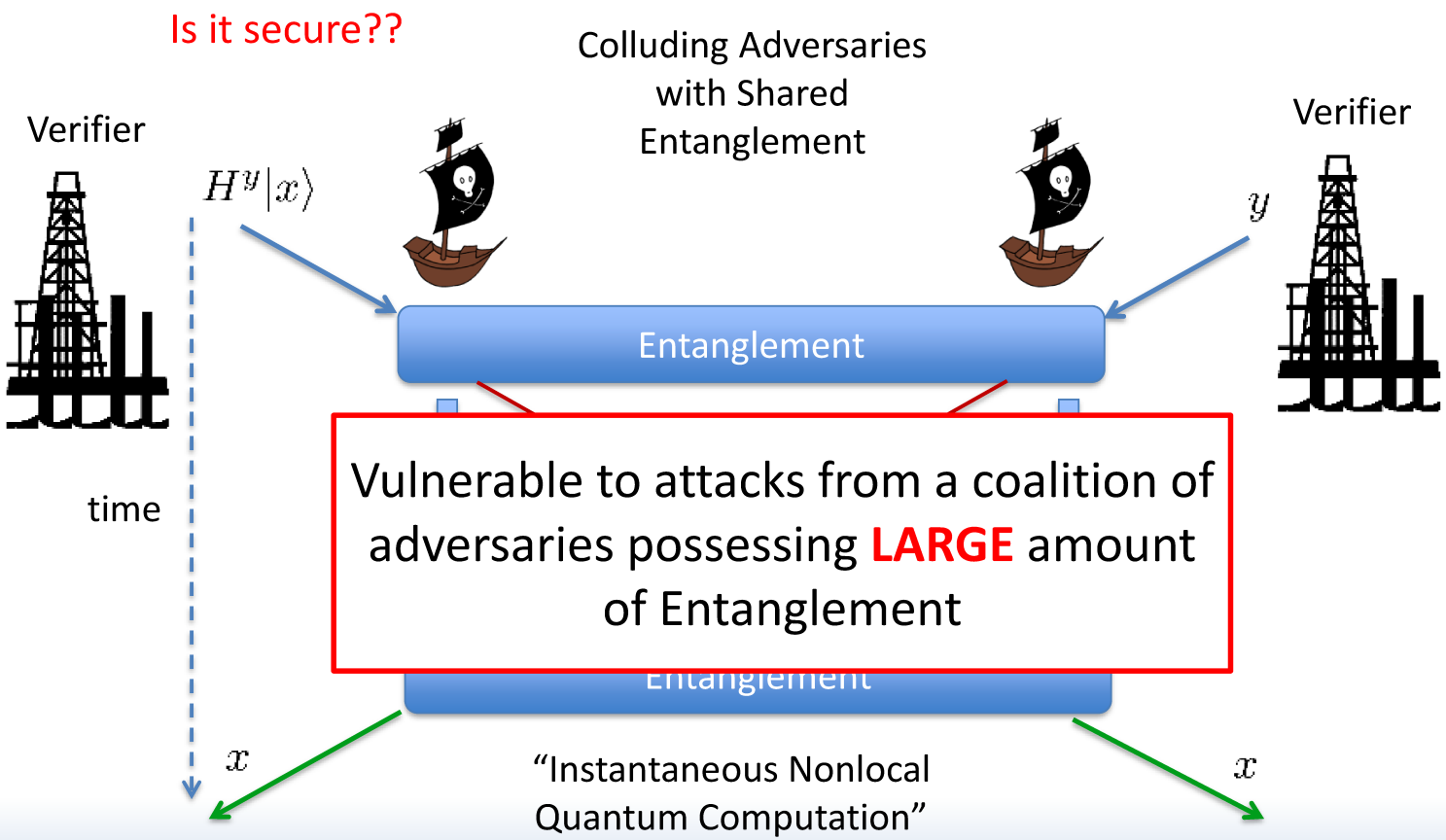
Chandran, *et al.*, *Lect. Notes Comput. Sci.* **5677**, 391 (2009).

Position based quantum cryptography (PBQC)



Chandran, *et al.*, *Lect. Notes Comput. Sci.* **391**, 5677 (2009).
Kent, *et al.*, *PRA* **84**, 012326 (2011).

Position based quantum cryptography (PBQC)

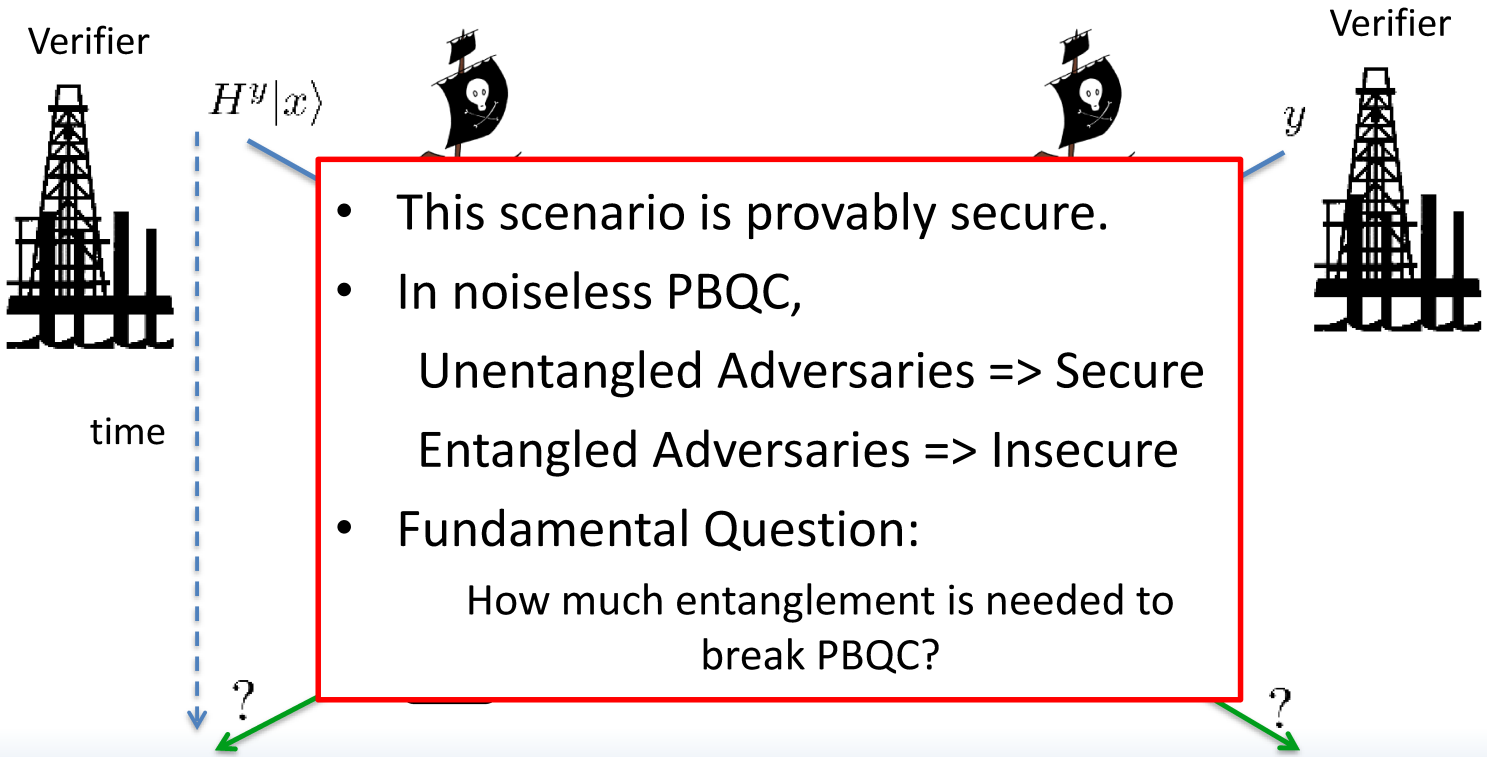


Buhrman, *et al.*, *SIAM J. Comput.* **43**, 150 (2014).

Position based quantum cryptography (PBQC)

What if the adversaries don't share entanglement??

Noiseless Quantum Channel:



- This scenario is provably secure.
- In noiseless PBQC,

  Unentangled Adversaries => Secure

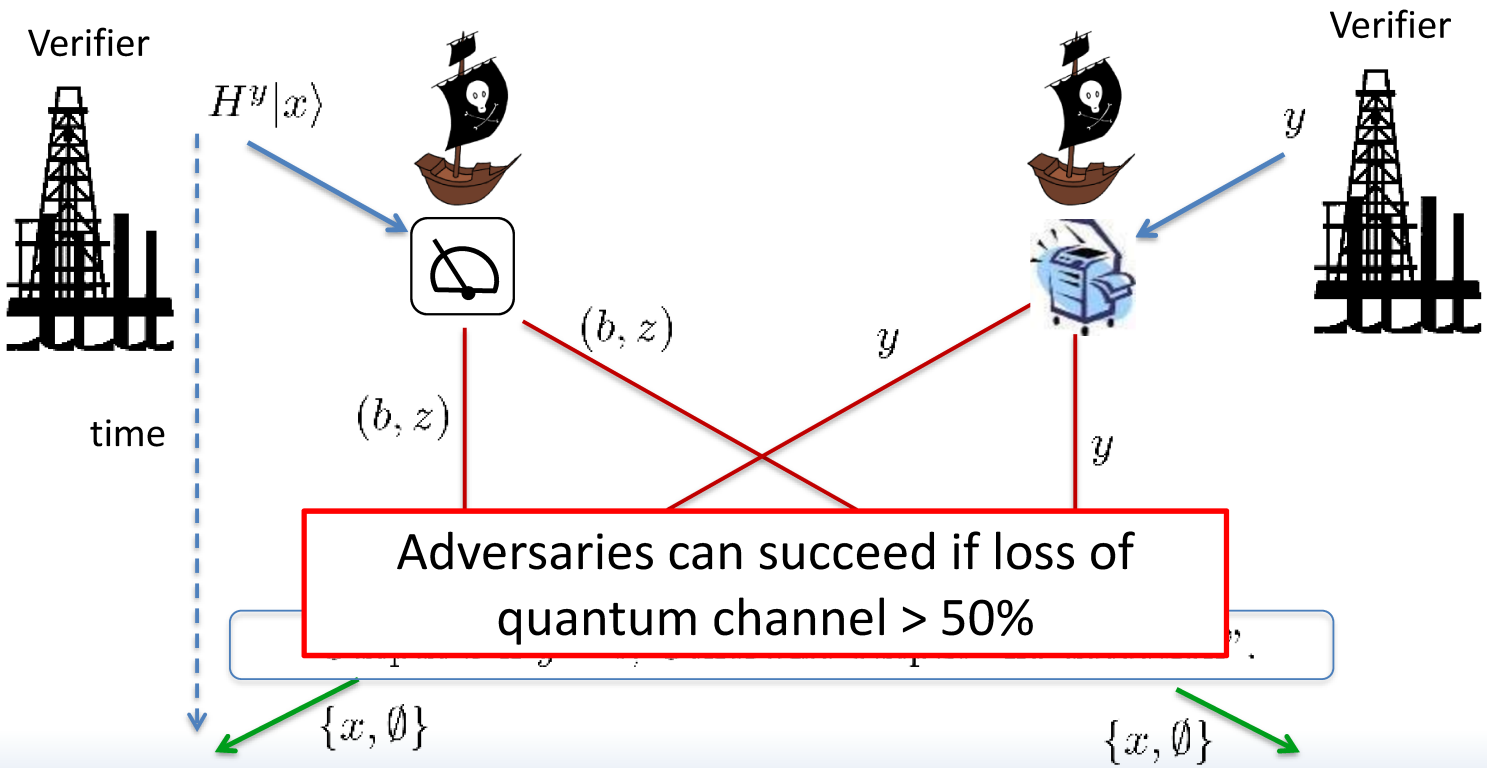
  Entangled Adversaries => Insecure
- Fundamental Question:

  How much entanglement is needed to break PBQC?

Position based quantum cryptography (PBQC)

What if the adversaries don't share entanglement??

Noisy Quantum Channel:



Adversaries can succeed if loss of quantum channel > 50%

Qi and Siopsis, *PRA* **91**, 042337 (2015).

Measurement-Device-Independent (MDI) PBQC

PHYSICAL REVIEW A **94**, 032315 (2016)

Loss-tolerant quantum secure positioning with weak laser sources

Charles Ci Wen Lim,[1,*] Feihu Xu,[2] George Siopsis,[3] Eric Chitambar,[4] Philip G. Evans,[1] and Bing Qi[1,3]

- PBQC based on the concept of measurement-device-independent QKD
- Provides a new fundamental lower bound on the entanglement needed to break PBQC:

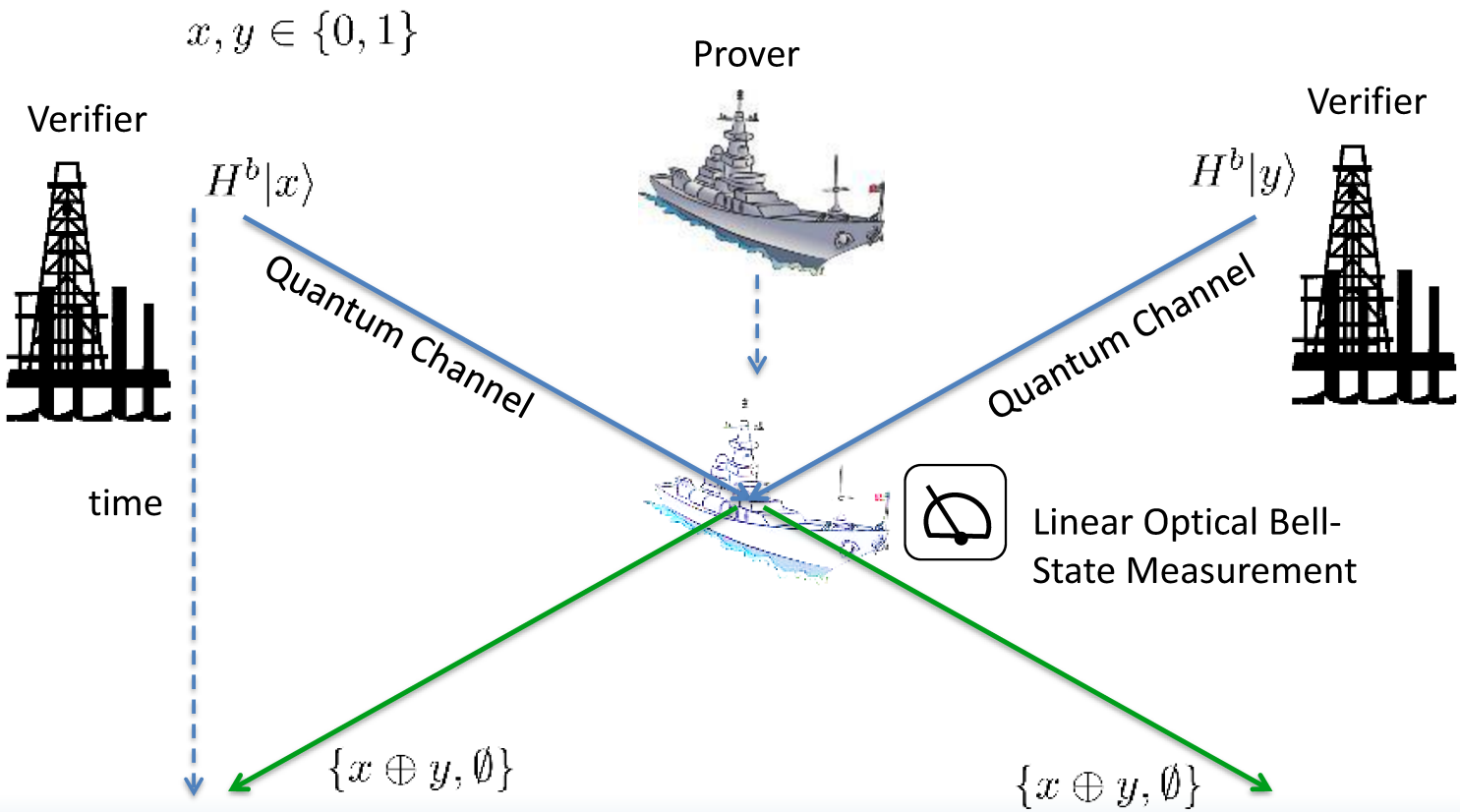
  For ideal sources and arbitrary channel loss,

  protocol is secure against *PPT adversaries*.

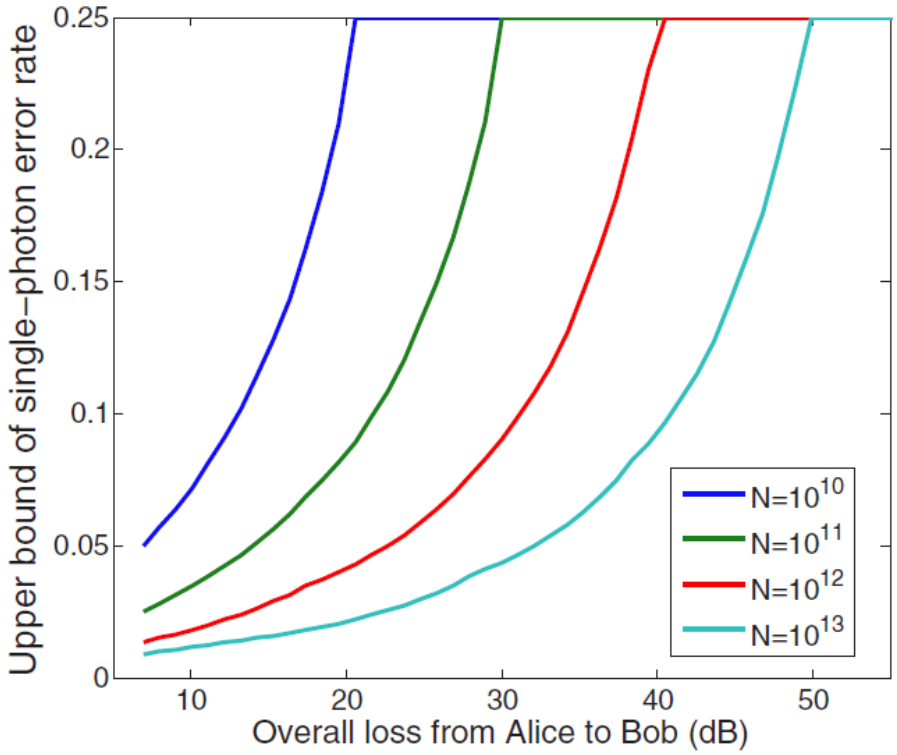
  Adversaries can share arbitrary PPT entanglement.
- For realistic sources, the protocol incorporates weak laser sources and the decoy-state method to become loss-tolerant.

Lo, Curty, and Qi, *Phys. Rev. Lett.* **108**, 130503 (2012).

Measurement-Device-Independent (MDI) PBQC



Measurement-Device-Independent (MDI) PBQC



Protocol becomes insecure when error rate > .25

- Simulation with baseline QBER of .1%, detector efficiency of 64%, and a dark count rate of 2.5 x 10^{-6}.
- MDI PBQC can tolerate a 47 dB channel loss.

Hybrid quantum classical protocol

S. Das and G. Siopsis, *Practically secure quantum position verification,* arXiv:1711.03392

We allow each party to have access to the classical random oracle $f : \{0,1\}^{2n} \to \{0,1\}$.

The steps of this protocol are as follows:

1. The verifiers agree on random $x_0, x_1, \theta \in \{0,1\}$, and n-digit random numbers $\boldsymbol{y}_0, \boldsymbol{y}_1 \in \{0,1\}^n$. V_i, for all $i \in \{0,1\}$, prepares a qubit in the state $H^\theta|x_i\rangle$, where H is the Hadamard matrix, and sends it to P, along with $\boldsymbol{y}_i$ ($i \in \{0,1\}$). Both states as well as the classical information arrive at P at the same time.

2. P computes (classically) $w = f(\boldsymbol{y}_0, \boldsymbol{y}_1)$, and applies H^w to each of the states he received. Then he performs a Bell measurement projecting onto the state $|\Psi^+\rangle$. If the measurement is successful, then he sends $z = 1$, otherwise he sends $z = 0$.

3. The verifiers accept if the result z of P's measurement is consistent with the states sent by them to P.

It appears that the adversaries need an exponentially large number of entangled pairs.