Quantum algorithms implementation on noisy quantum computers

Walter Pogosov
Dukhov Research Institute of Automatics (Rosatom Corporation), Moscow, Russia;
Institute for Theoretical and Applied Electrodynamics RAS;
Moscow Institute of Physics and Technology.

In collaboration with **A. Zhukov**, **E. Kiktenko**, **D. Babukhin**, **A. Elistratov**, **S. Remizov**, and **Yu. Lozovik**

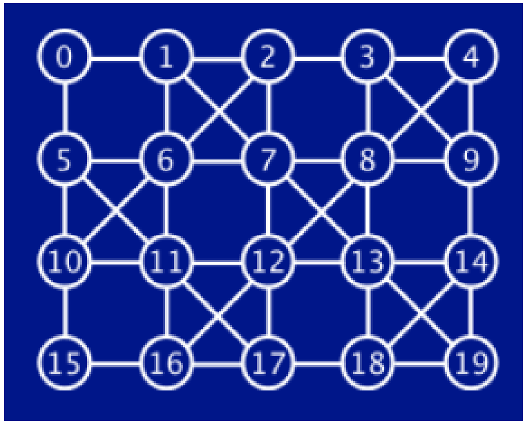
ROSATOM RQC Russian Quantum Center Russian Academy of Sciences MIPT MOSCOW INSTITUTE OF PHYSICS AND TECHNOLOGY Lomonosov Moscow State University

Outline

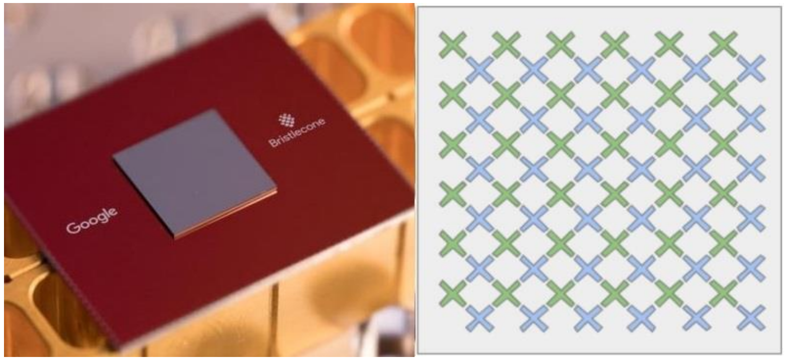
- Introduction / Motivation
- Algorithmic simulation of far-from-equilibrium dynamics
- Quantum communication protocols as a benchmark for programmable quantum computers
- “Quantum machine learning” with noisy quantum devices
- Summary

State-of-the art superconducting quantum computers

20-qubit IBM device



72-qubit Google device



Nontrivial physics begins with tens of qubits
(2^{60} quantum states is too many to simulate from first principles for most powerful modern supercomputers)

Are we close to some practical applications?

Not evident…

Problems: decoherence and gate errors (**mainly two-qubit gates**).
Possible solutions: error correction codes (overhead of resources); hybrid quantum-classical calculations with relatively shallow quantum circuits; error mitigation or partial correction…
Hope: Heuristic combination of these strategies – "quantum supremacy" in the near-term future (without full error correction).

New ideas are highly desirable !

Recent examples:
- Variational solvers for simulations of physical quantum systems -- an alternative to the canonical phase estimation algorithms.
- Quantum machine learning, classification, clustering, and detecting hidden patterns in huge amounts of data.

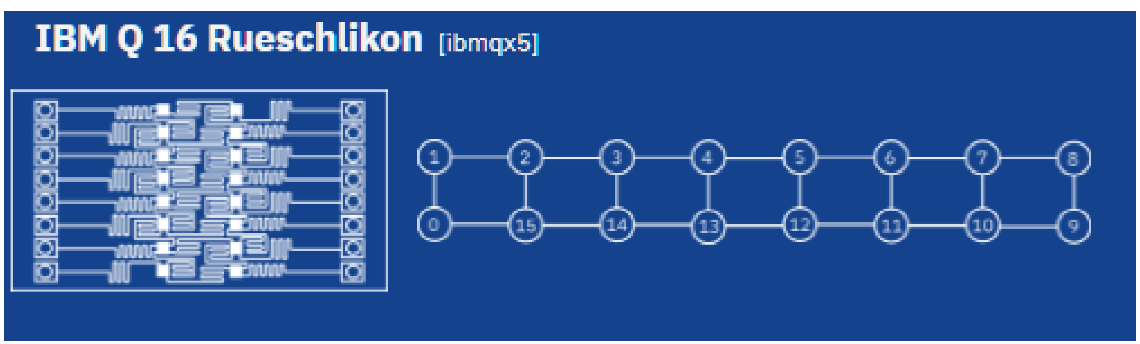
Aims of our work:

-Ideas on what can be simulated with noisy quantum hardware

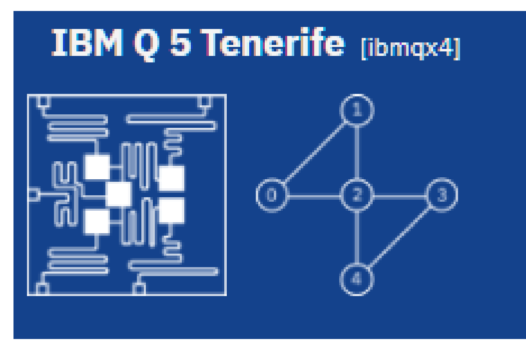
-Ideas on benchmarking of capabilities of state-of-the-art machines

-Development of error mitigation schemes (series of case studies)

16-qubit chip (QISKIT)



5-qubit chip (composer)



II. Algorithmic simulation of far-from-equilibrium dynamics

A. A. Zhukov, S. V. Remizov, W. V. P., Yu. E. Lozovik, Quant. Inf. Proc. **17**, 223 (2018); arXiv:1807.10149.

Far-from-equilibrium dynamics

Nonequilibrium quantum relaxation in <u>closed</u> many-body systems. Current experimental platform and setup: quenches in trapped cold-atom gases.

Central issues:

1. Whether the system relaxes to a stationary state ("thermalization")? What are its characteristics?
2. Dynamical *evolution* of order, correlations, entanglement.

- Depends on the integrability of the model
- Depends on the initial state

Far-from-equilibrium dynamics

Our messages:

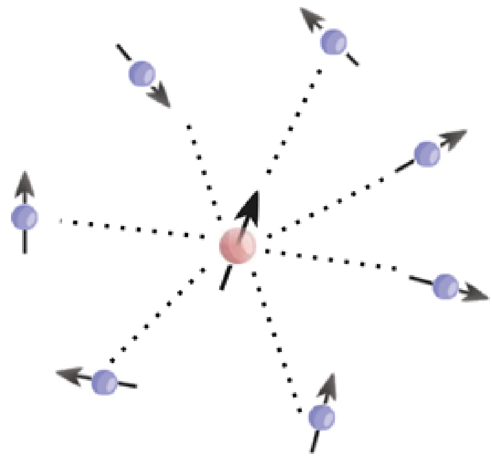
Algorithmic quantum simulation of *spin* dynamics is prospective. Back to the unitary evolution, but no phase estimation algorithms, no “chemical accuracy”, no nonlocality (fermionic statistics enforced through Hamiltonian).

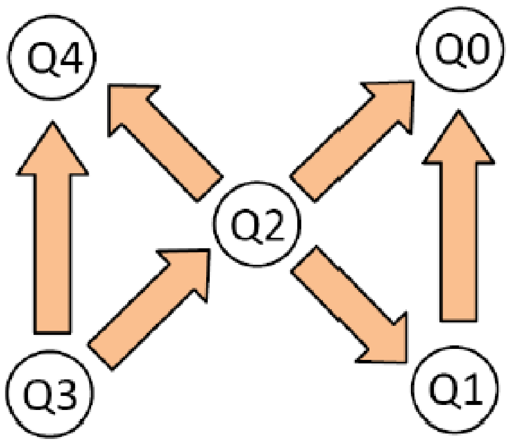
High flexibility: the same chip can be used for dynamics of different spin models starting from different initial conditions.

Experiments with real quantum hardware, which unveil its capabilities. Playground for error mitigation.

Simplest example: central spin model and 5-qubit device

- Topology matters -- direct mapping between degrees of freedom of a modeled system and degrees of freedom of the physical qubits of the chip





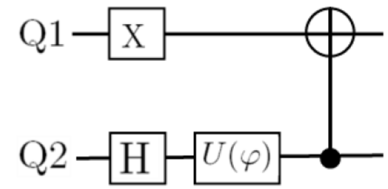
$$H_{cs} = \sum_{j=1}^{L} \epsilon_j(\sigma_{j,z} + 1/2) + \epsilon_c(\sigma_{c,z} + 1/2) + g\sum_{j=1}^{L}(\sigma_c^+\sigma_j^- + \sigma_c^-\sigma_j^+)$$

- Full resonance (in the rotating frame)

$$H = g\sum_{j=1}^{L}(\sigma_c^+\sigma_j^- + \sigma_c^-\sigma_j^+) \quad \Rightarrow \quad H = \frac{g}{2}\sum_{j=1}^{L}(\sigma_c^x\sigma_j^x + \sigma_c^y\sigma_j^y)$$

- **Three-particle system**: initial state – entangled "bath"

$$\Psi(0) = |\downarrow\rangle \otimes \frac{1}{\sqrt{2}}\left(|\downarrow\uparrow\rangle + e^{i\varphi}|\uparrow\downarrow\rangle\right)$$

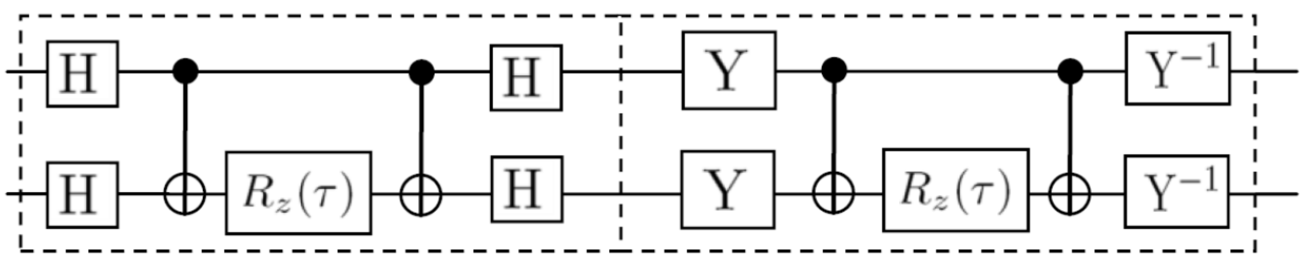


tunable phase parameter. Dynamics of the central spin can be suppressed due to the negative quantum interference of contributions from two qubits

$\varphi = \pi$

- Cancellation of two contribution coming from two different spins.
- No central spin dynamics. "Dark" state from quantum optics.
- Excitation blockade in the bath due to the quantum interference.

Building block of Trotterized evolution operator

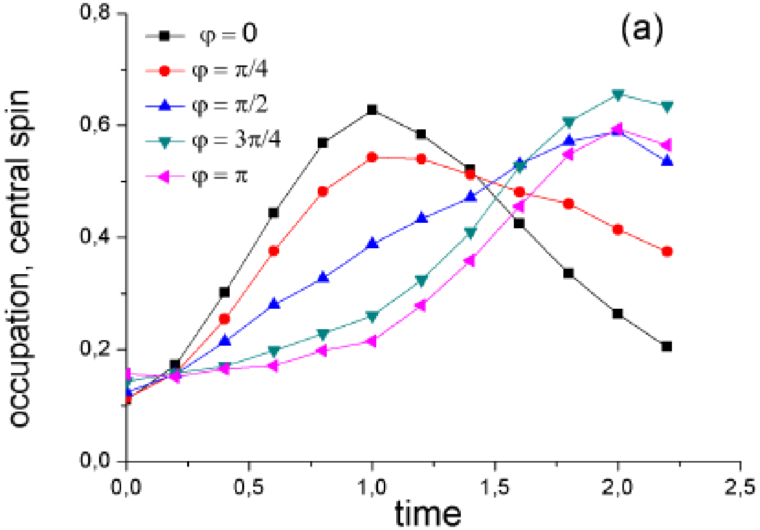


$\exp\left(-i\frac{\tau}{2}\sigma_c^x \otimes \sigma_j^x\right)$ $\exp\left(-i\frac{\tau}{2}\sigma_c^y \otimes \sigma_j^y\right)$

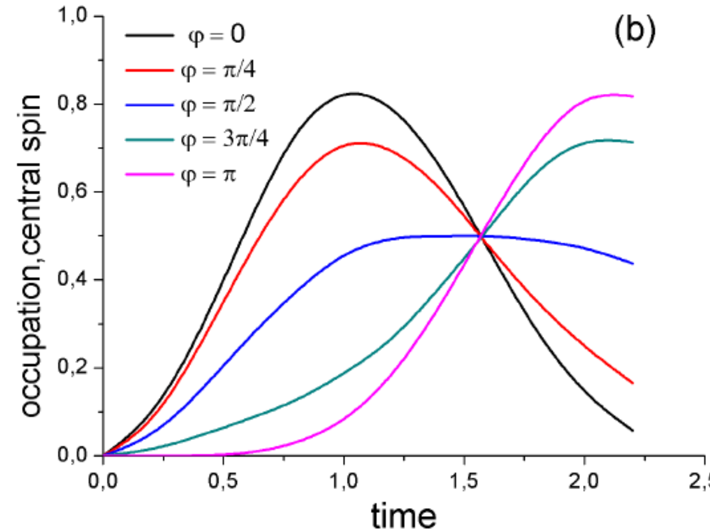
Quantum circuit for $\exp\left(-i\frac{\tau}{2}\sigma_c^x \otimes \sigma_j^x\right)\exp\left(-i\frac{\tau}{2}\sigma_c^y \otimes \sigma_j^y\right)$

Two-particle entangled state: Population of the central particle

experiment (8192 runs per point)



theory



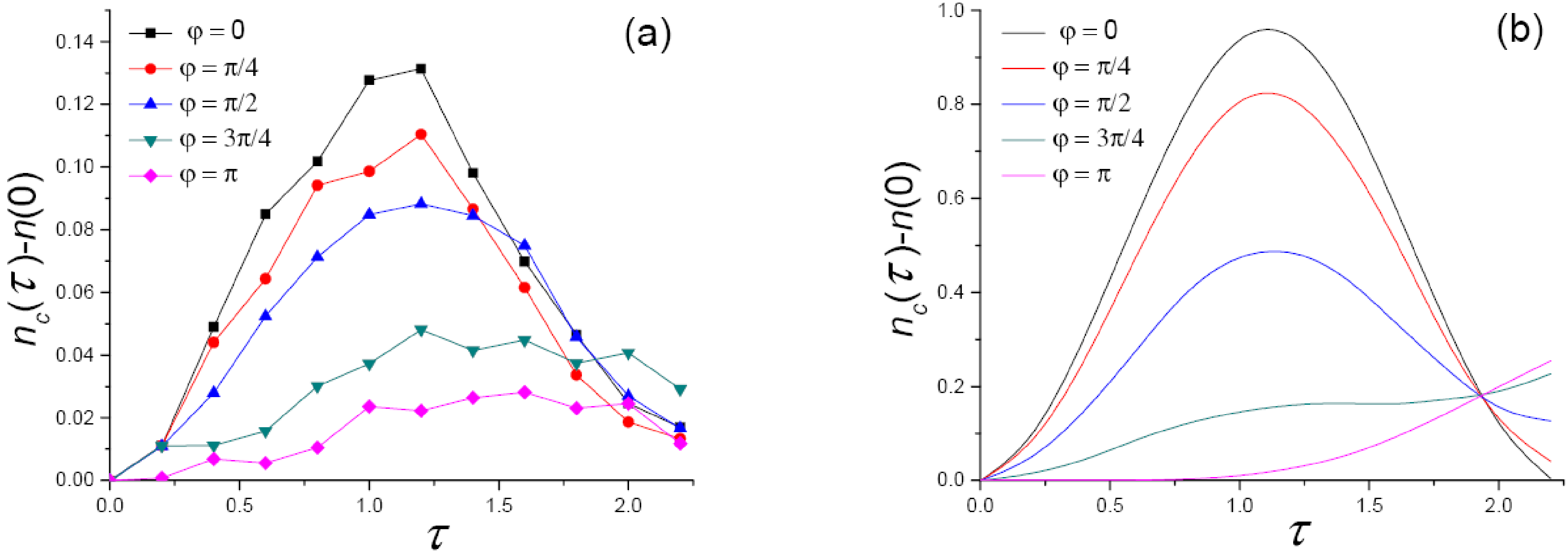
*Theory is not exact. Approximation of the same level – **single-step Trotter decomposition***

- Dark and bright states known from quantum optics
- Entanglement in the bath and quantum interference effects block excitation transfer to the center

- Noisy “background” is independent on time.
- Many gates – randomization of wrong outputs (averaging of many wrong and uncorrelated distributions). Compatible with the quasiprobability distribution picture.
- Can errors help? Probably, yes, for “intermediate-depth” circuits.

Error mitigation in the regime of large errors: 3 Trotter steps

$$\Delta n_c(\tau) = n_c(\tau) - n_c(\tau = 0)$$ - analyzing differences

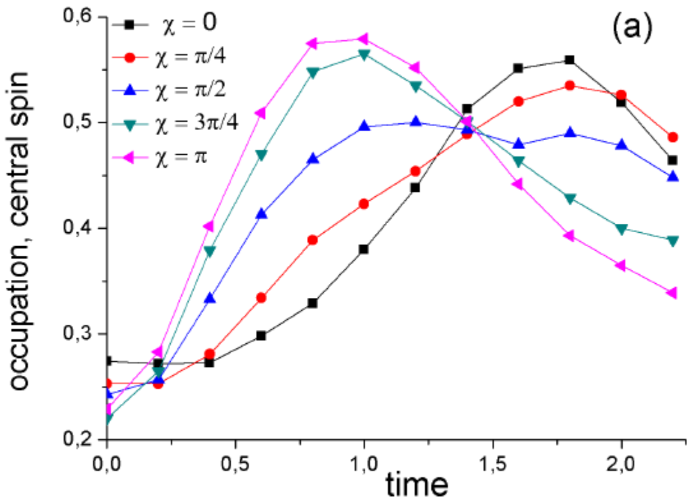


The results of our experiment (a) and theory (b) for $\Delta n_c(\tau)$ as a function of the dimensionless time τ for the Trotter number $N = 3$. Different curves correspond to different values of phase parameter φ entering the initial state.

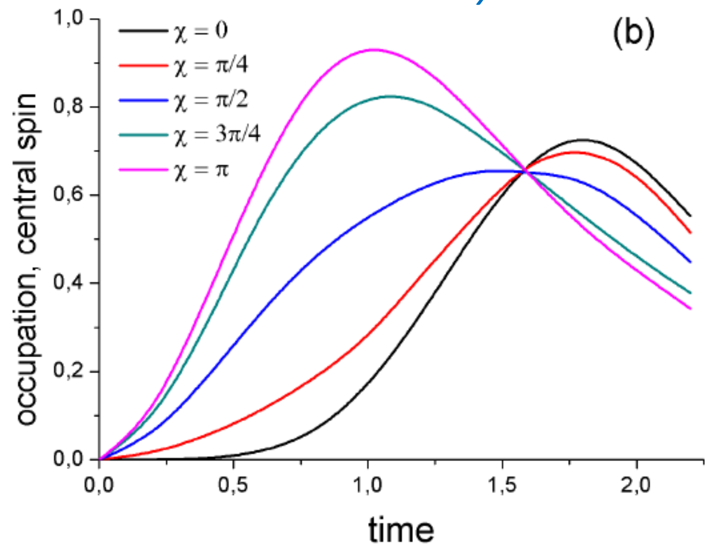
Three-particle entangled state: Population of central particle

$$\Psi(0) = |\downarrow\rangle \otimes \frac{1}{\sqrt{6}} \left(|\downarrow\downarrow\uparrow\rangle - 2e^{i\chi}|\downarrow\uparrow\downarrow\rangle + |\uparrow\downarrow\downarrow\rangle \right)$$

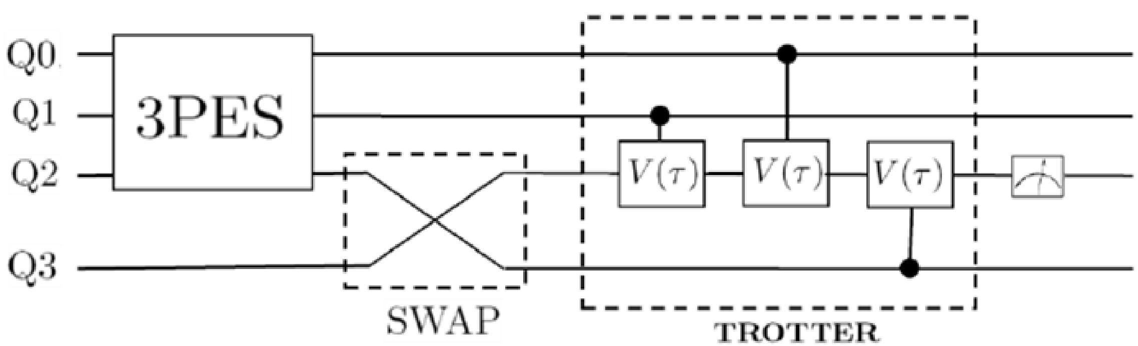
experiment (8192 runs per point)

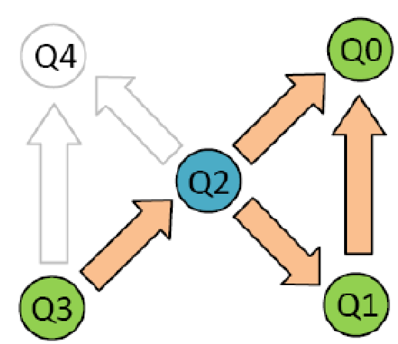


theory



- Dark and bright states: quantum superpositions of two-particle entangled states
- Method to benchmark multiqubit entanglement in noisy hardware

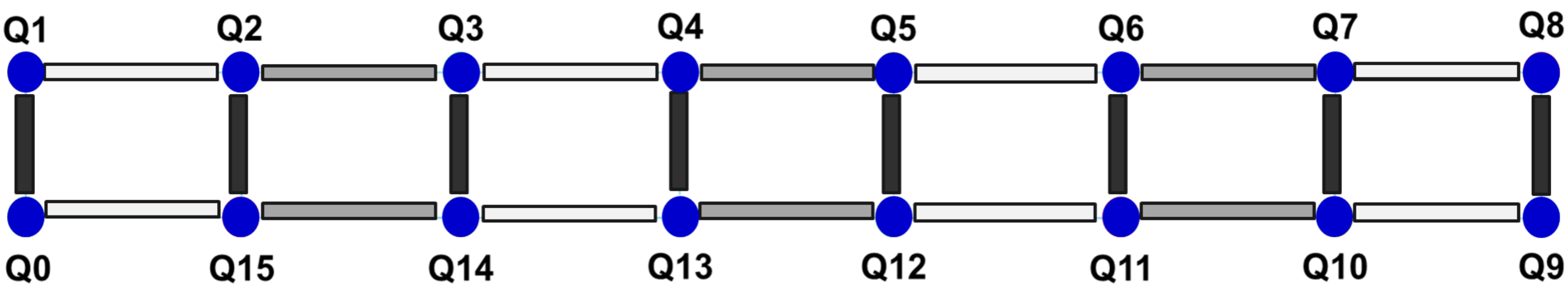




Transverse-field Ising model and 16-qubit IBM device

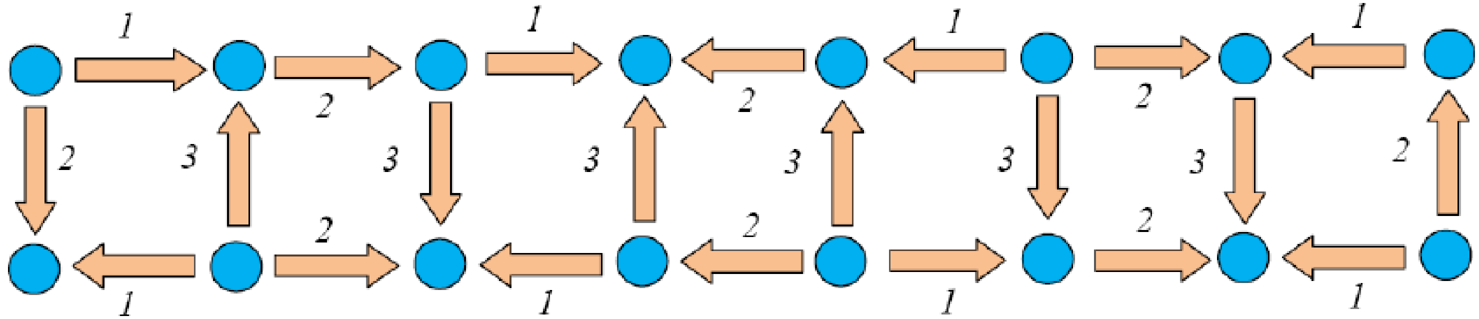
- Ising model in a transverse field – simplest and most popular playground to study far-from-equilibrium dynamics.
- Non-stochastic and nonintegrable model.

$$H = -J \sum_{\langle i,j \rangle} \sigma_z^i \sigma_z^j - \alpha \sum_i \sigma_x^i$$



$|\downarrow \ldots \downarrow\rangle$ initial state

16-spin Ising ladder after 1 Trotter step: experiment vs theory



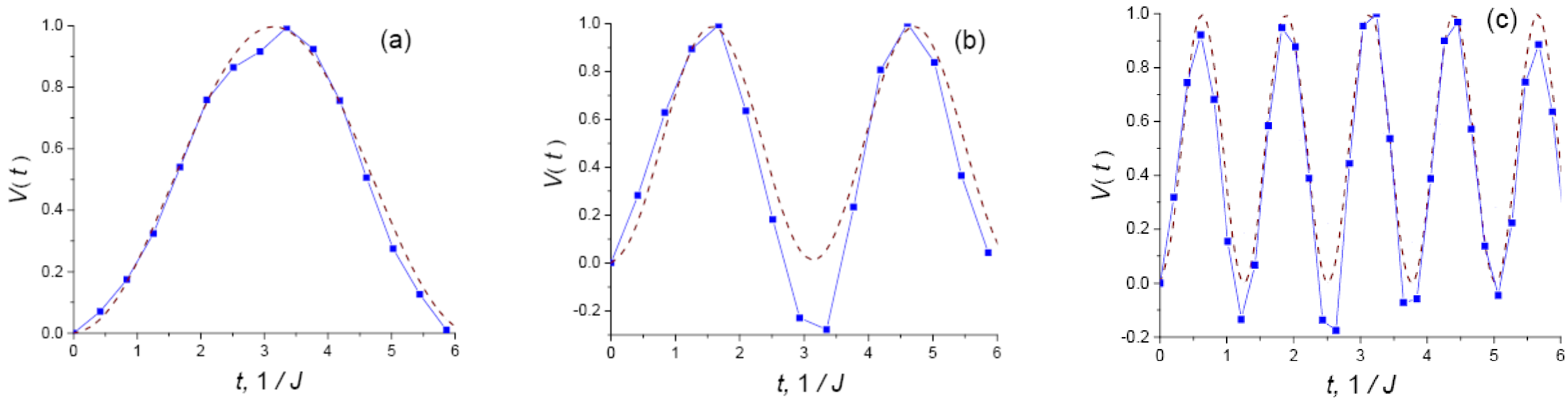


Fig. 18 (Color online) The results of our experiment (solid blue lines) and theory (dashed brown lines) for V defined in Eq. (10) in the case of the 16-spin transverse Ising ladder at $\alpha = J$ (a), $\alpha = 2J$ (b), $\alpha = 5J$ (c) as a function of the dimensionless time τ for the Trotter number $N = 1$.

$$V(\tau) = \frac{n(\tau) - n(0)}{\max n(\tau) - n(0)}.$$

Error mitigation in the large error regime

Summary-I

- The dependence of the dynamics on the initial state can be reproduced with the state-of-the-art hardware (correct initial dynamics). However, very few Trotter steps can be implemented mainly due to the gate errors (further dynamics is problematic).

-Interesting problems ~ ten Trotter steps ~ order of magnitude decrease of two-qubit gate errors.

-Results of the modeling can be improved to some extent using error mitigation *even in the regime of large errors. Errors sometimes can help (for intermediate-depth circuits)…*

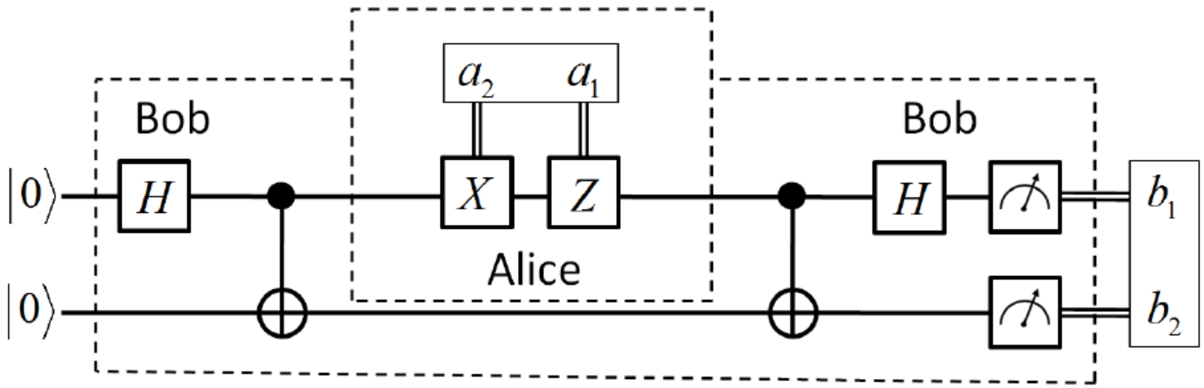
III. Quantum communication protocols as a benchmark for programmable quantum computers

-Deep benchmarking of capabilities of quantum processors
-"Quantum advantage" with real noisy quantum hardware
- Rigorous quantification: entropy-based quantities
-Playground for error mitigation strategies

A. A. Zhukov, E. O. Kiktenko, A. A. Elistratov, W. V. P., Yu. E. Lozovik, submitted to QIP.

Extended superdense coding

Central idea – two bits of information can be transferred with a single qubit used in quantum communication (thanks to entanglement). "Quantum advantage".



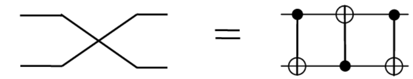
- Bob prepares two qubits in entangled states and sends one of them to Alice.
- Alice applies a couple of single-qubit gates and sends the qubit back to Bob.

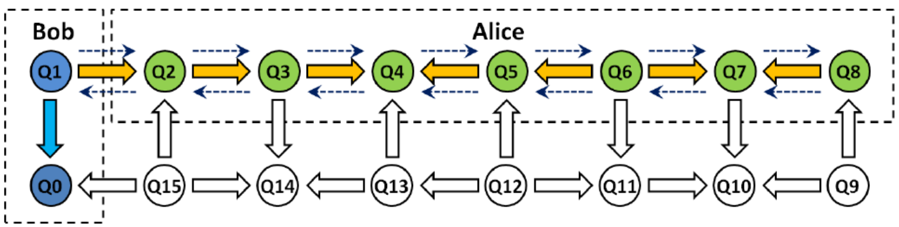
00, 10, 01, and 11 are encoded into II, ZI, IX, and ZX, respectively.

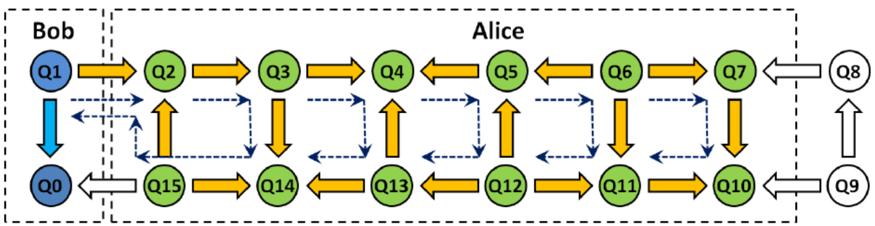
- Bob performs measurements and extracts two bits of information

An efficiency of information transfer

- Alice and Bob are placed in distant qubits of the machine.
- Single-qubit states are SWAPed from Bob to Alice and backwards.







Entropy-based characteristics

Mutual information

$$\mathcal{I}(A,B) = H(B) - H(B|A),$$

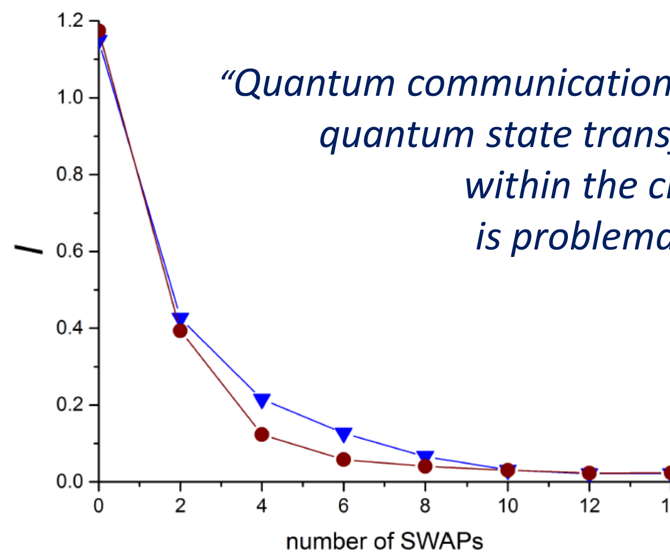
between the Alice's input $A = (a_1, a_2)$ and Bob's output $B = (b_1, b_2)$.

For the ideal system: $\mathcal{I}(A,B) = 2$

$\boxed{\mathcal{I}(A,B) > 1 \text{ – ''quantum advantage''}}$

Examples of output distributions

SWAPs	$a_1,\ a_2$	$b_1,\ b_2$			
		0,0	1,0	0,1	1,1
0	0,0	0.940	0.022	0.031	0.008
	1,0	0.117	0.815	0.029	0.039
	0,1	0.121	0.015	0.840	0.024
	1,1	0.031	0.114	0.115	0.739
2	0,0	0.684	0.078	0.172	0.067
	1,0	0.154	0.551	0.094	0.201
	0,1	0.250	0.063	0.617	0.069
	1,1	0.113	0.265	0.136	0.486



"Quantum communication" / quantum state transfer within the chip is problematic

Entropy-based characteristics

Mutual information

$$\mathcal{I}(A,B) = H(B) - H(B|A),$$

between the Alice's input $A = (a_1, a_2)$ and Bob's output $B = (b_1, b_2)$.

$$H(X) = -\sum_x \Pr(X = x) \log_2 \Pr(X = x)$$

is a Shannon entropy of a random variable X with possible values $\{x\}$ and

$$H(X|Y) = -\sum_y \Pr(Y = y) \sum_x \Pr(X = x|Y = y) \log_2 \Pr(X = x|Y = y)$$

is conditional entropy of X given random variable Y with possible values $\{y\}$.

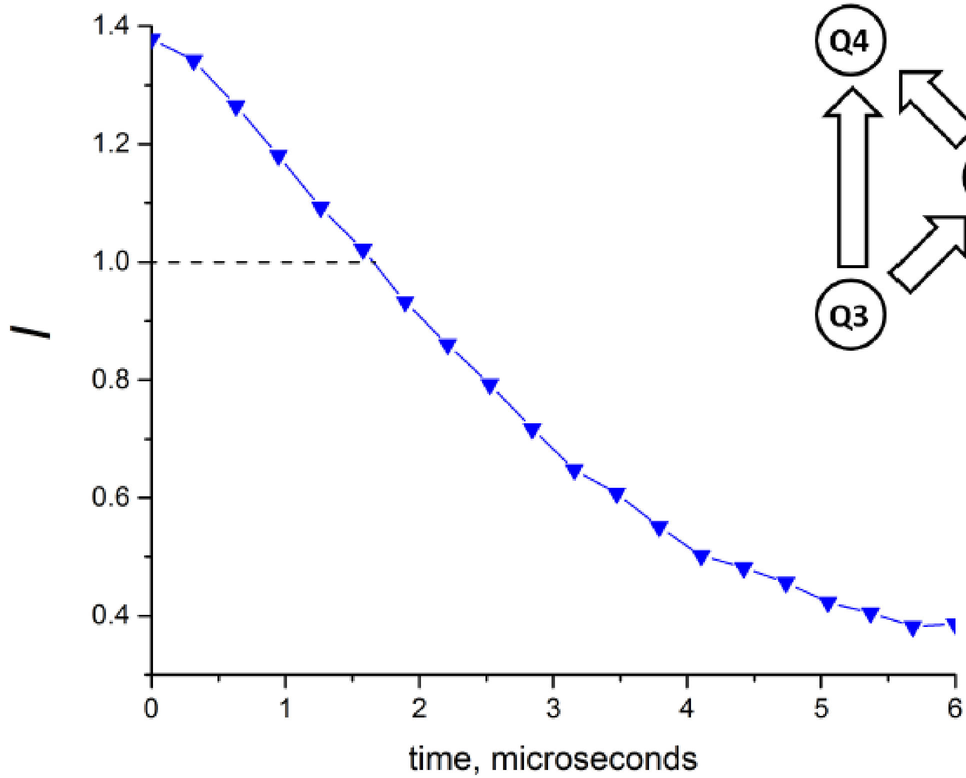
For the ideal system: $\mathcal{I}(A,B) = 2$

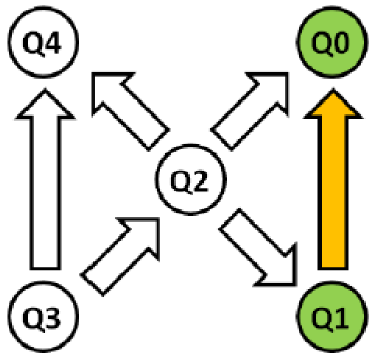
$$\boxed{\mathcal{I}(A,B) > 1 - \text{"quantum advantage"}}$$

Evaluation of mutual information is the most rigorous way to quantify an efficiency of the protocol implementation

Simulations of quantum memory imperfections

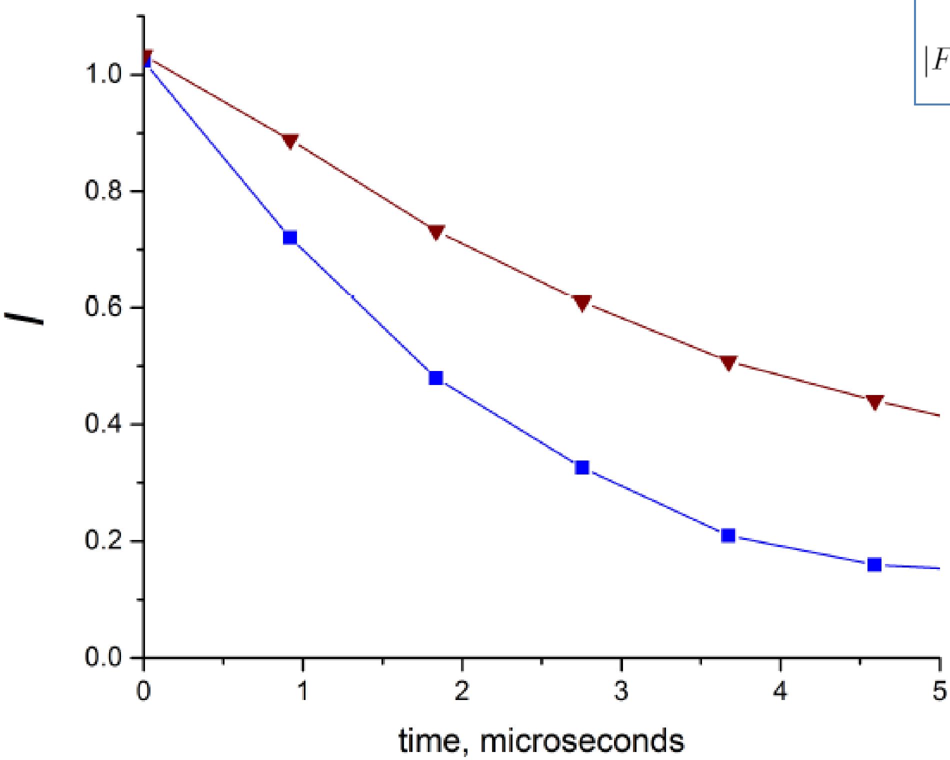
- Time delay is implemented using a train of identity gates before Alice makes encoding.
- Alice and Bob are not separated (Alice now is also at Q0 and Q1).





"Decay time" of quantum regime is much shorter than T_1 and T_2.

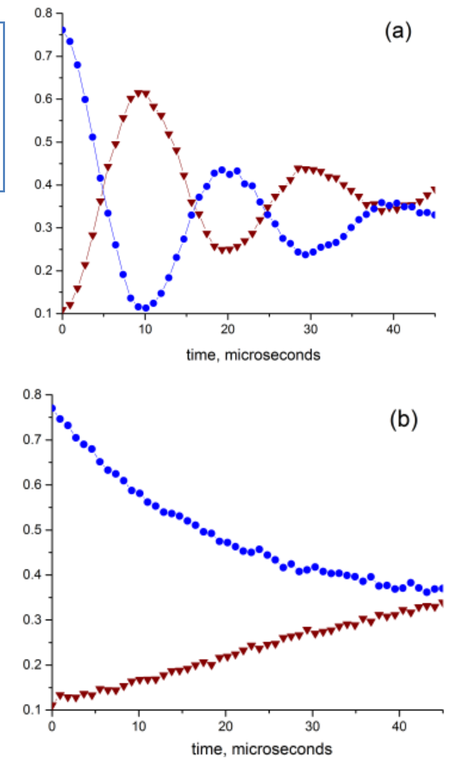
Correction of *coherent* errors in 16-qubit device



Oscillations of Bell states

$$|F_+\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$$

$$|F_-\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$$

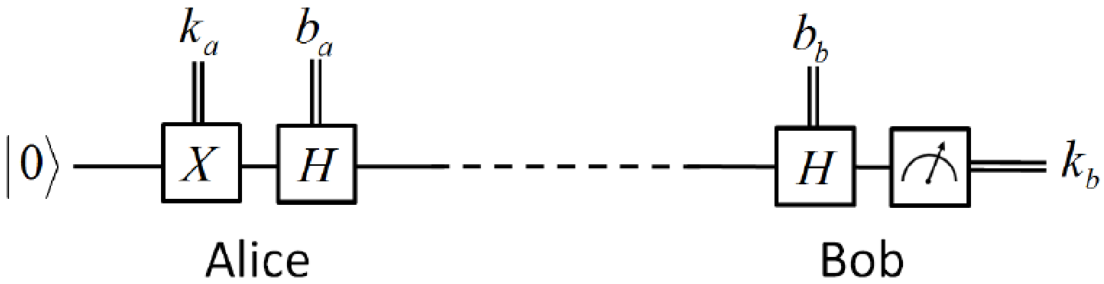


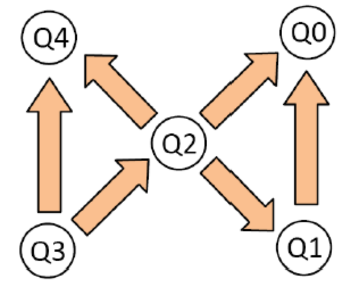
$t_{\rm osc} \simeq 10$ microseconds

Correction of coherent errors (phase drift in Bell states) after the train of identity gates.

$$U(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix} \qquad \varphi = -\pi t / t_{\rm osc}$$

Quantum key distribution BB84





Alice encodes 0 or 1 of a key in the qubit Q1 using single-qubit gates I or X, respectively. After that, we choose the basis "+" or "×" by applying single-qubit gates I or H respectively. Then, we apply a train of identity gates. Finally, Bob measures this qubit in the same basis "+" or "×" (we analyze a sifted key). A set of single measurements.

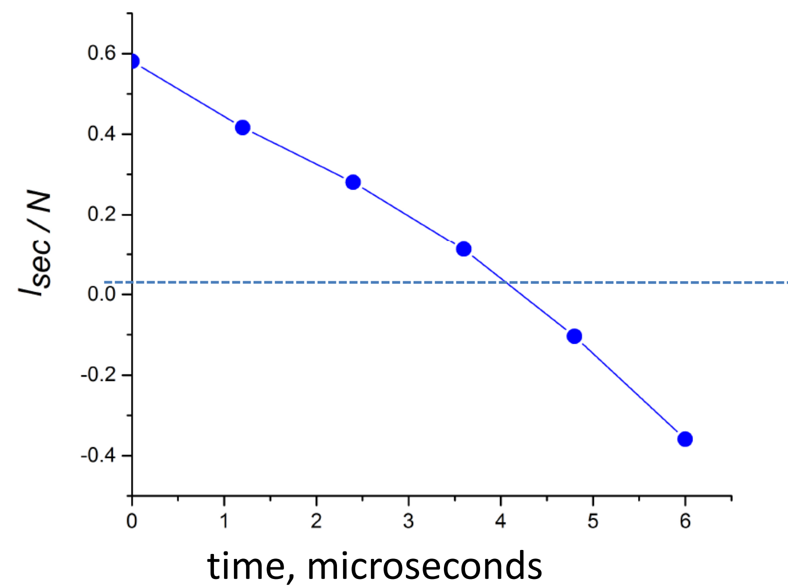
The length of secure key as a function of the delay time

$$l_{\rm sec} = N(1 - h(q)) - N f_{\rm ec} h(q), \tag{9}$$

where N is length of sifted keys,

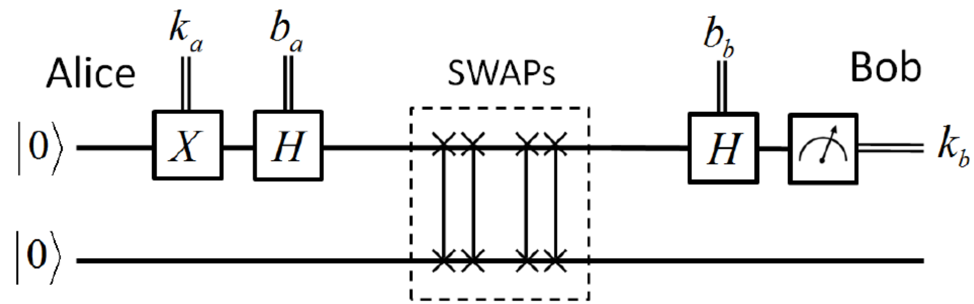
$$h(q) = -q\log_2 q - (1-q)\log_2(1-q) \tag{10}$$

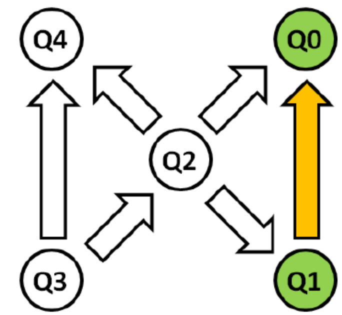
is binary entropy function and $f_{\rm ec}$ is "efficiency" of information reconciliation algorithm (in all the further considerations we take $f_{\rm ec} = 1.15$, that correspond to real practise [44]). The expression (9) gives a length to which the reconciled sifted keys should be shortened by employing publicly announced random hash function from universal$_2$ set at the stage of privacy amplification [45]. Note, that negatives values of $l_{\rm sec}$ correspond to the fact of impossibility to distill the provably secure keys.



Vanishes much faster than both T_1 and T_2

Robustness with respect to the quantum information transfer





Alice and Bob are both at Q0. Multiple SWAPs between Q0 and Q1.

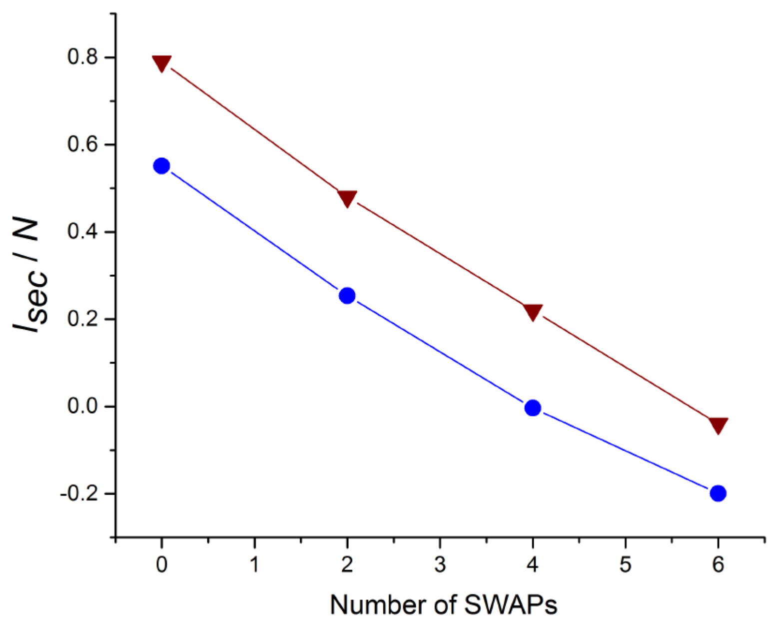
Error mitigation. Define new logical qubit:

$$|0\rangle_{\text{logic}} = |10\rangle \text{ and } |1\rangle_{\text{logic}} = |01\rangle$$

Post-selection: discard results of the form

$$|00\rangle \text{ and } |11\rangle$$

Alice and Bob are both at Q0 and Q1 *at once*.
Even number of SWAPs between Q0 and Q1.



Results for both approaches

Table 5 The error distribution for BB84 protocol for different values of time delay. For each input, 8192 runs of the algorithm on 5-qubit IBMqx4 device have been performed.

Basis, bits	Time, μs					
	0.0	1.2	2.4	3.6	4.8	6.0
$+$,0	0.008	0.011	0.009	0.010	0.008	0.005
$\times$,0	0.011	0.027	0.052	0.081	0.098	0.120
$+$,1	0.051	0.076	0.095	0.119	0.177	0.251
$\times$,1	0.050	0.071	0.091	0.122	0.176	0.260

Table 7 The error distribution for BB84 protocol for different number of SWAPs. Each logical qubit has been composed from two physical qubits. Post-selection procedure has been applied. For each input, 8192 runs of the algorithm on 5-qubit IBMqx4 device have been performed. Numbers in brackets indicate fractions of data accepted after the post-selection.

Basis, bits	SWAPs			
	0	2	4	6
$+$,0	0.003 (90%)	0.028 (85%)	0.048 (79%)	0.076 (75%)
$\times$,0	0.024 (86%)	0.053 (84%)	0.081 (81%)	0.111 (78%)
$+$,1	0.002 (89%)	0.029 (82%)	0.059 (77%)	0.094(71%)
$\times$,1	0.021 (83%)	0.05 (76%)	0.089 (70%)	0.139 (63%)

Summary-II

- Quantum communication protocols as deep benchmarks for programmable quantum computers.

-Transfer of information between distant parts of superconducting quantum chips is currently problematic. Scaling?

-Time scales for the decay of “quantum regime” can be much shorter than T_1 and T_2.

-Algorithm- and processor-dependent error mitigation schemes.

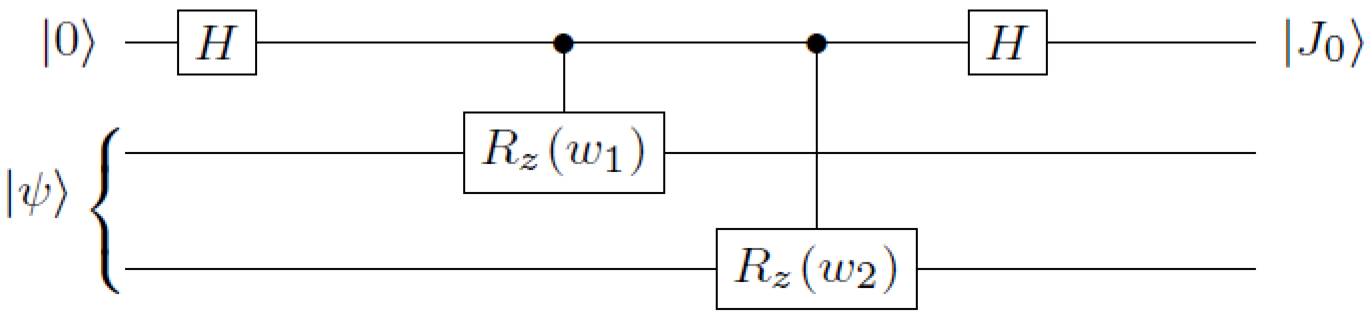
IV. “Quantum machine learning” with noisy quantum devices

- Classification of “patterns”, which are purely quantum (characteristics of entanglement), and difficult to recognize classically. Quantum sensing.
- Phase estimation as a block in quantum machine learning schemes.

Hybrid quantum-classical scheme

- Quantum block – phase estimation algorithm with free parameters
- Classical block – training of the circuit by finding optimal values of these parameters (training states, tuning free parameters)
- Deterministic and nondestructive classification of input states

Toy model



- An ideal quantum machine, after the proper training, must answer in just a single query what class of states it is.
- Otherwise – probabilistic classification:

$$|\Phi_\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$

$$|\Psi_\pm\rangle = \frac{1}{\sqrt{2}}(|10\rangle \pm |01\rangle)$$

$$P = \frac{1}{2} + \frac{1}{2}\left(|\langle\Phi_+|\psi\rangle|^2 + |\langle\Phi_-|\psi\rangle|^2 - |\langle\Psi_+|\psi\rangle|^2 - |\langle\Psi_-|\psi\rangle|^2\right)$$

Theory

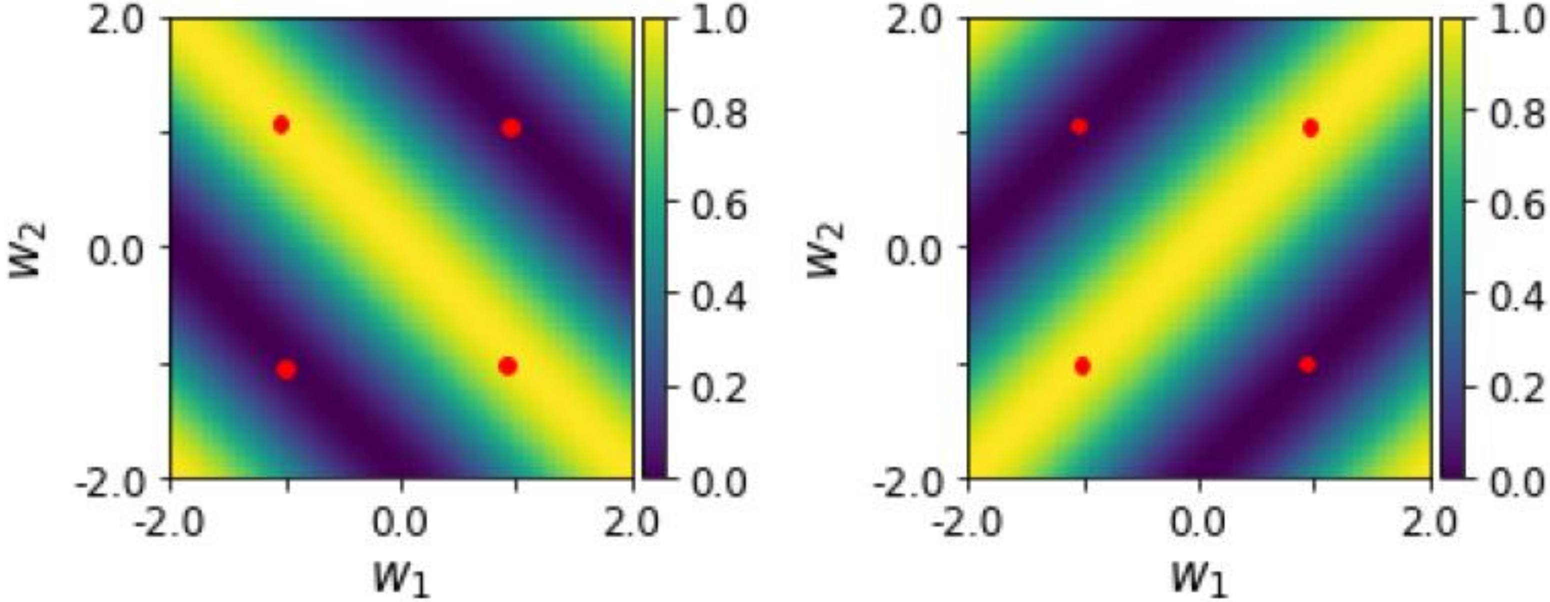
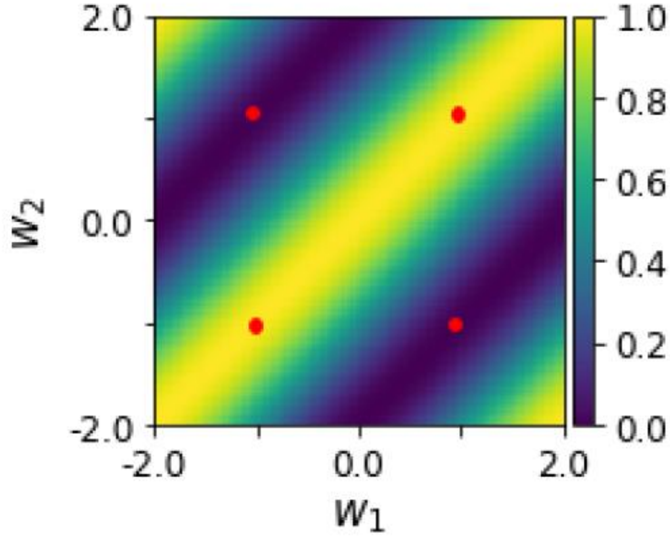
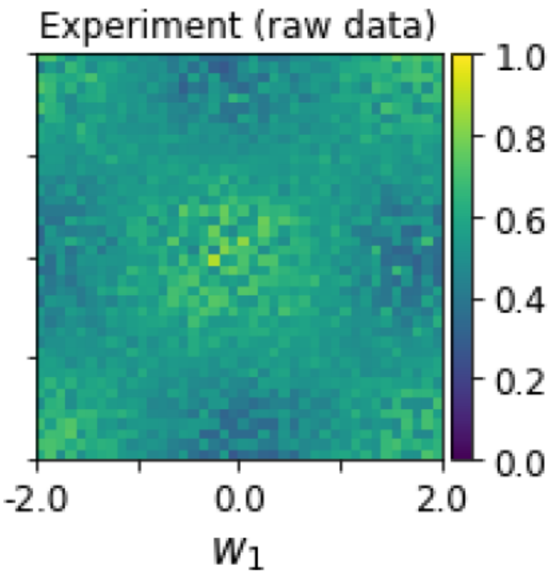


Fig. 2: Probability patterns of measuring qubit J_0 in a state $|0\rangle$ for the first (a) and for the second (b) Bell pair. Parameter points where a discrimination between two pairs of Bell states is done in one measurement are marked red

Theory versus experiment

- Probability patterns for measuring ancilla qubit in the state 0

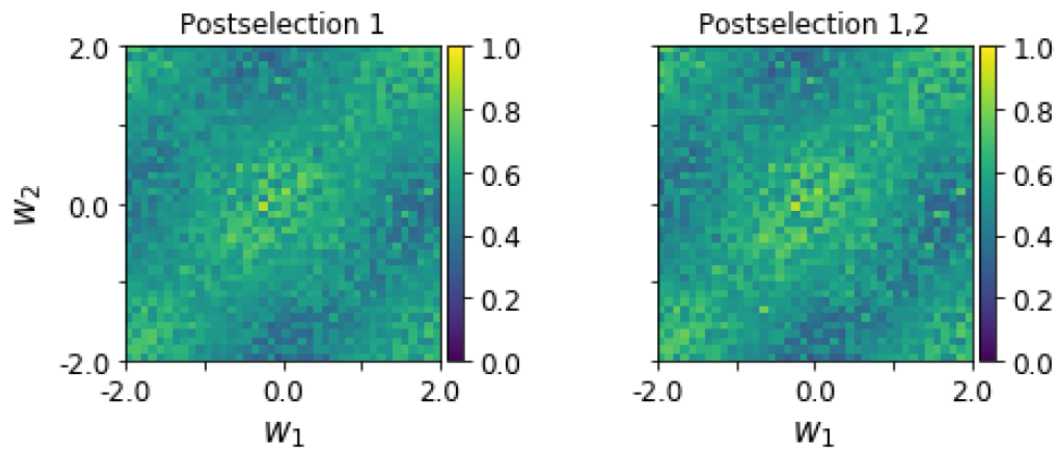




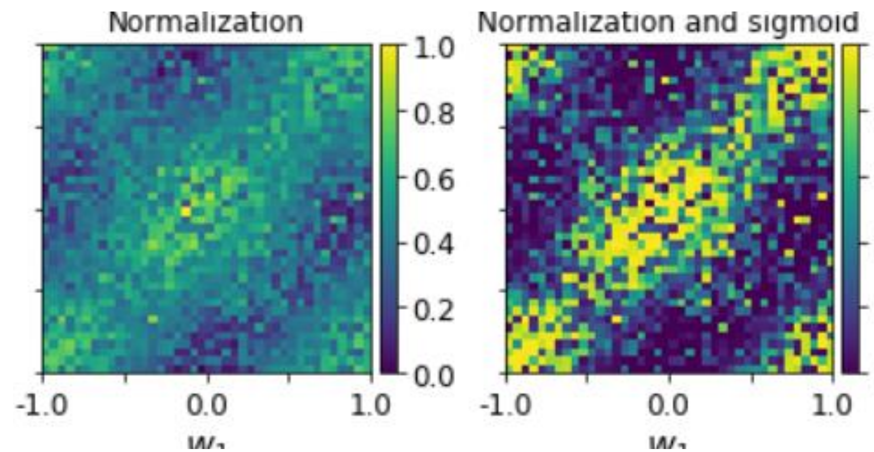
- Red points – deterministic and nondestructive classification from a single measurement

Playground for error mitigation in hybrid quantum-classical schemes

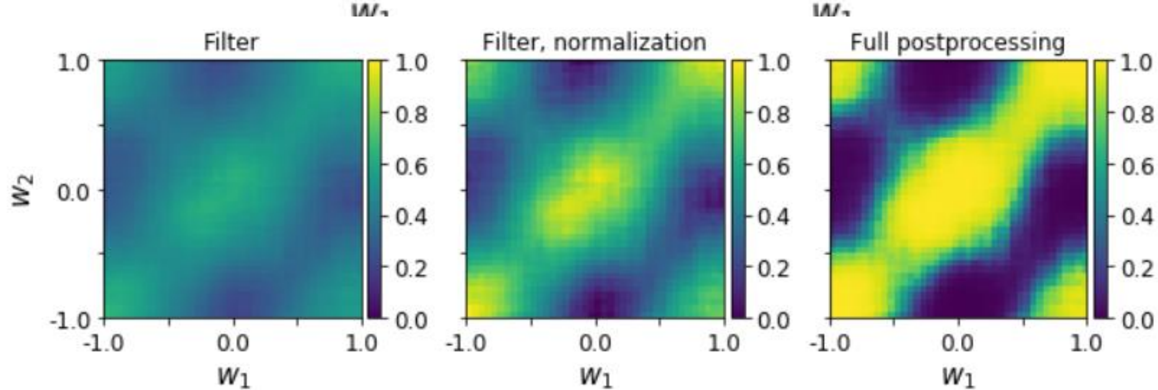
Step 1: postselection



Step 2: normalization
(no fitting - only information on max and min)



Step 3: filtering
(no fitting - only information on typical gradients)



Summary-III

- It seems possible to work with data from quantum hardware, heavily damaged by noise

- We acknowledge use of the IBM Quantum Experience for this work.
- The viewpoints expressed are those of the authors and do not reflect the official policy or position of IBM or the IBM Quantum Experience team.

Gate errors

- Single-qubit gates can be implemented with the high fidelity
- Two-qubit gates are problematic

Typical error in superconducting realization is of the order of 1%.

Estimation of total error for spin (!) models

In our simulations, the total error per physical qubit can be estimated as $2p_{CNOT}N_{neig}N\nu$, where p_{CNOT} is the CNOT error, N_{neig} is the number of spins participating in the interaction with the given spin, and ν is a number, which characterizes the complexity of the spin-spin interaction (ν ranges from 1 for Ising models, which include only zz interaction, to 3 for Heisenberg model, which includes interactions of three types, xx, yy, and zz).

To have a error of the order of 1 %
after 10 Trotter steps, CNOT error must be 10^(-4)

Increase of Trotter number – decrease of (mathematical) Trotterization error, but increase of (physical) errors of the device

Discretizing dynamics

- Free evolution (through evolution operator)

$$\Psi(t) = e^{-iHt}\Psi(0)$$

This representation is needed for quantum computer and not for us!

Trotter-Suzuki decomposition

$$e^{-it(H_A+H_B)} = e^{-itH_A}e^{-itH_B} + \frac{(it)^2}{2!}[H_A, H_B] + \ldots$$

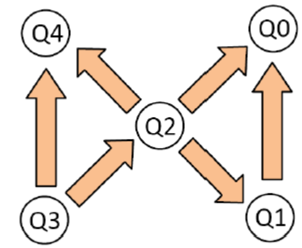
$$e^{-it(H_A+H_B)} \simeq \left(e^{-iH_At/n}e^{-iH_Bt/n}\right)^n$$

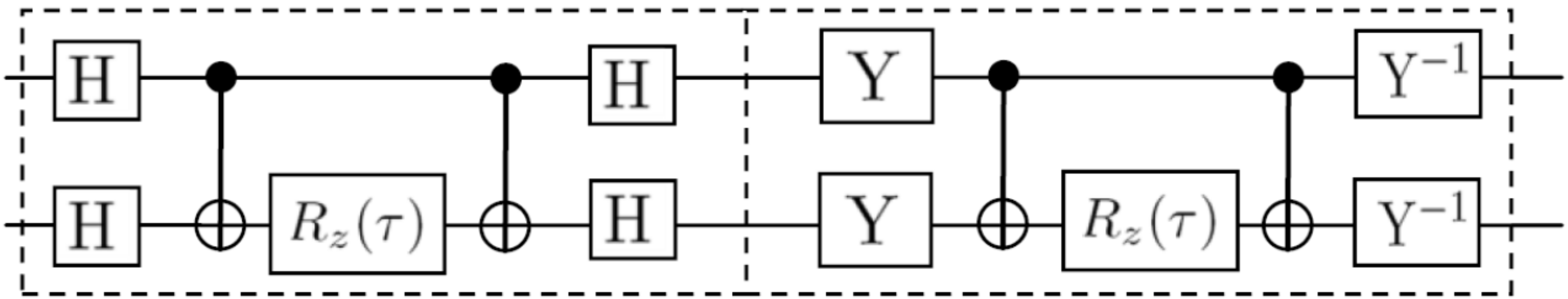
exact in the limit $n \to \infty$

The larger number of Trotter steps,
the smaller (mathematical) Trotterization error

- Main building block for modeling the interaction

$$H = \frac{g}{2}\sum_{j=1}^{L}(\sigma_c^x \sigma_j^x + \sigma_c^y \sigma_j^y)$$

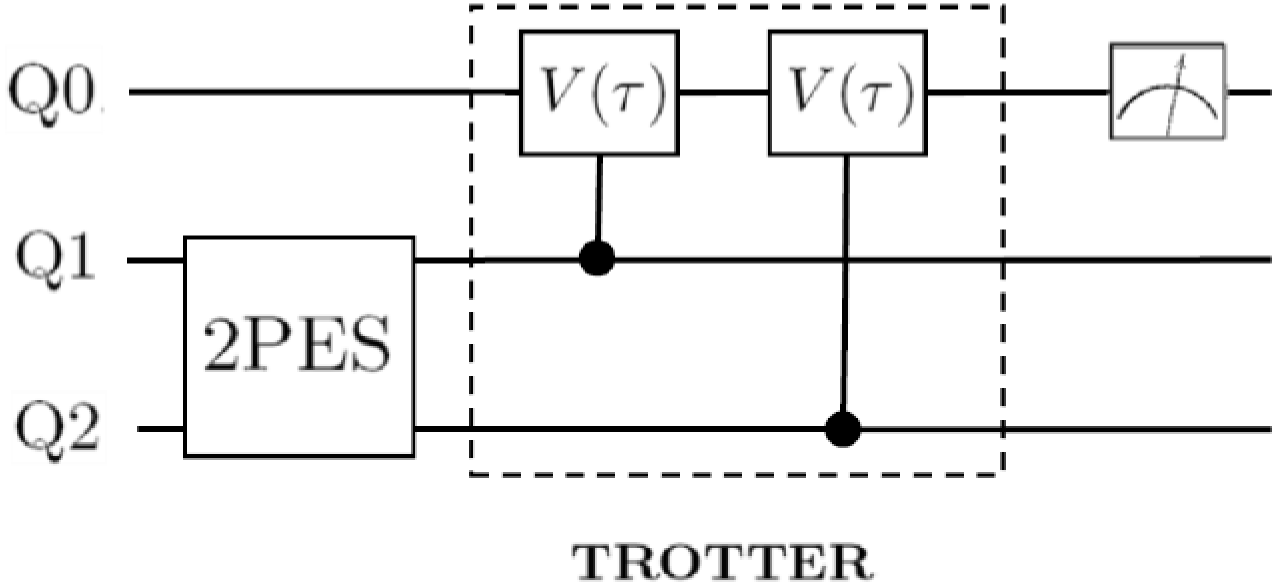


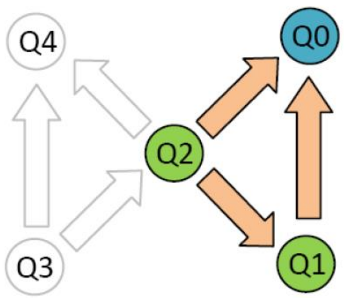


$\exp\left(-i\frac{\tau}{2}\sigma_c^x \otimes \sigma_j^x\right)$ $\exp\left(-i\frac{\tau}{2}\sigma_c^y \otimes \sigma_j^y\right)$

Quantum circuit for $\exp\left(-i\frac{\tau}{2}\sigma_c^x \otimes \sigma_j^x\right)\exp\left(-i\frac{\tau}{2}\sigma_c^y \otimes \sigma_j^y\right)$

Full quantum circuit

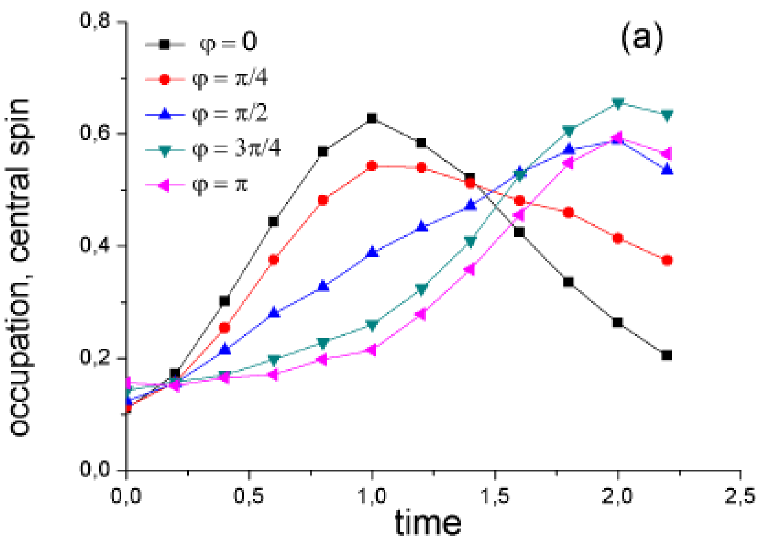




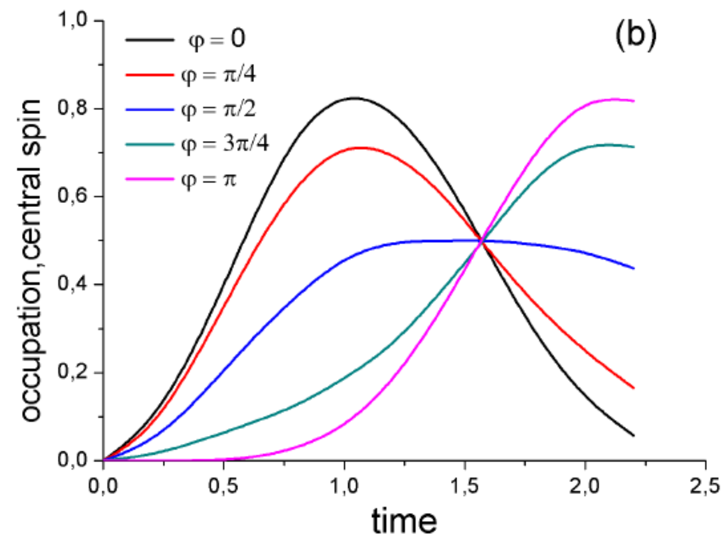
Quantum circuit for the evolution of the system starting from the initial state of two-particle entangled state of the bath and unexcited central spin at the Trotter number $N = 1$.

Two-particle entangled state: Population of the central particle

experiment (8000 runs per point)



theory

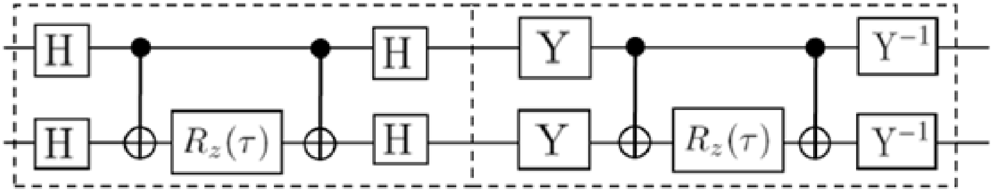


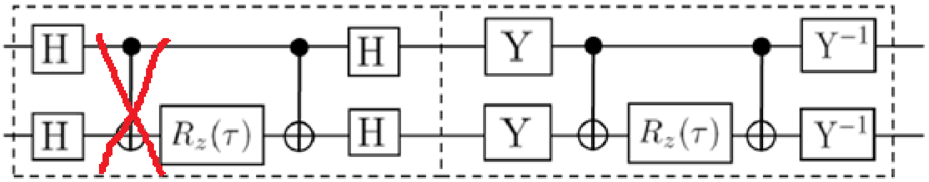
*Attention! Theory is not exact. Approximation of the same level – **one-step Trotter decomposition***

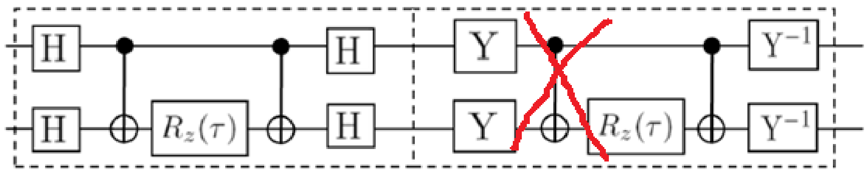
- Dark and bright states known from quantum optics
- Entanglement in the bath and quantum interference effects block excitation transfer to the center

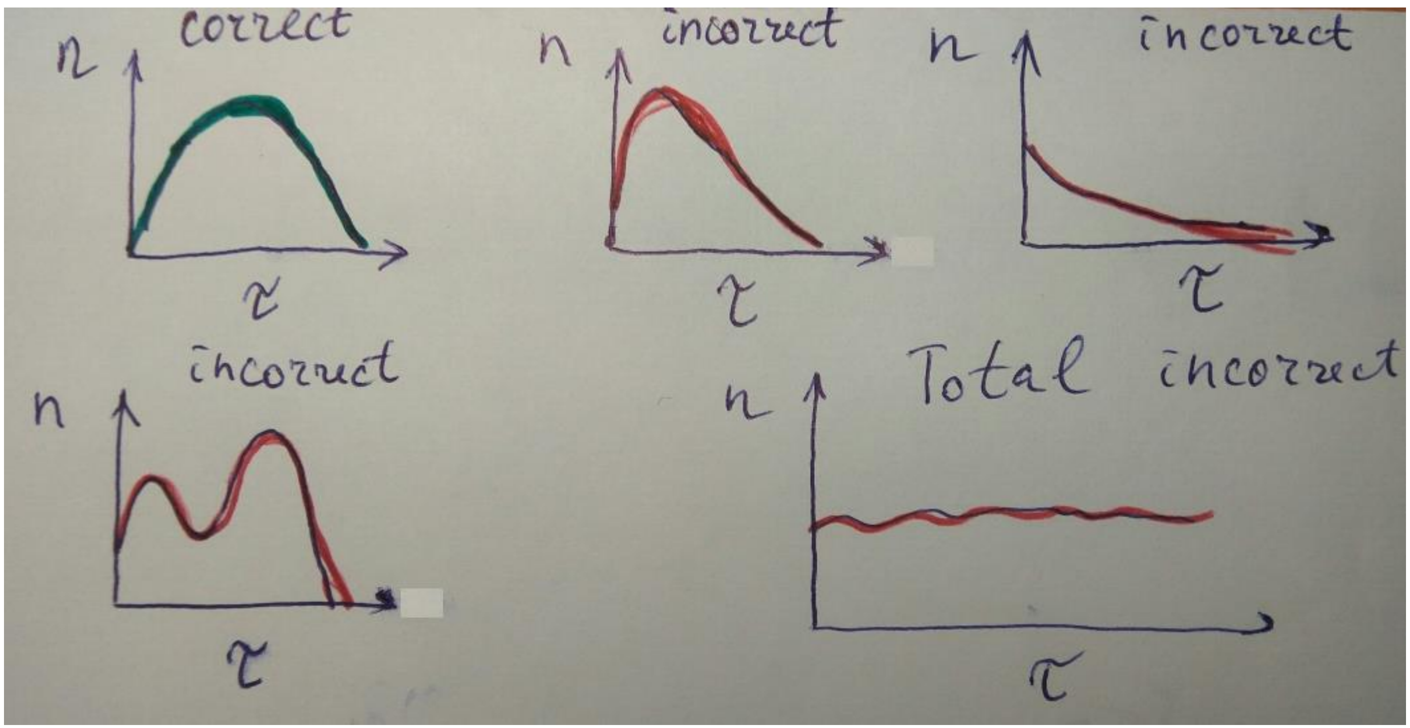
- Noisy “background” is independent on time!
- Many gates – randomization of wrong outputs.
- Can errors help?? Probably, yes, in some “intermediate” regimes.

Nature of “randomization”







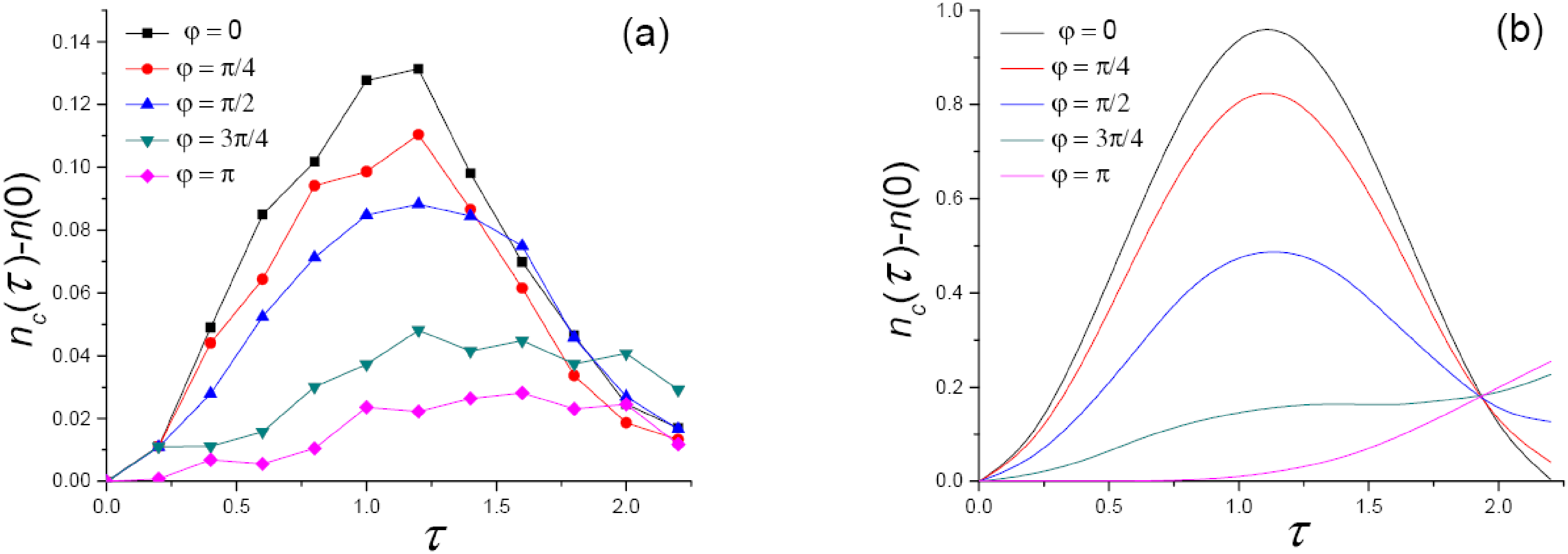


Errors can play a positive role

- For shallow circuits errors are always bad
- For deep circuits they are also bad (exponential decay of information vs number of gates)
- For intermediate-depth circuits, they can be positive (in some sense)

Error mitigation in the regime of large errors: 3 Trotter steps

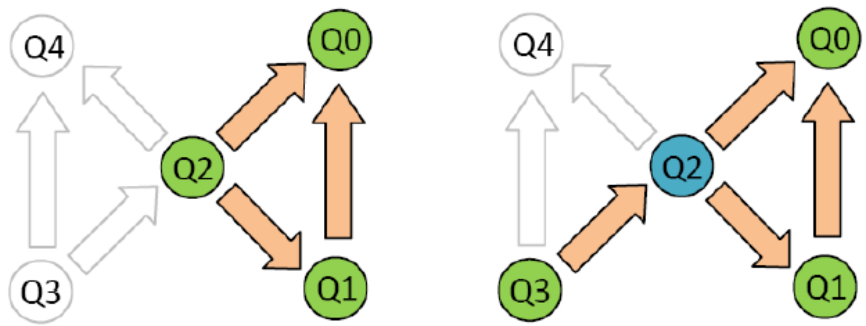
$$\Delta n_c(\tau) = n_c(\tau) - n_c(\tau = 0)$$ - analyzing differences



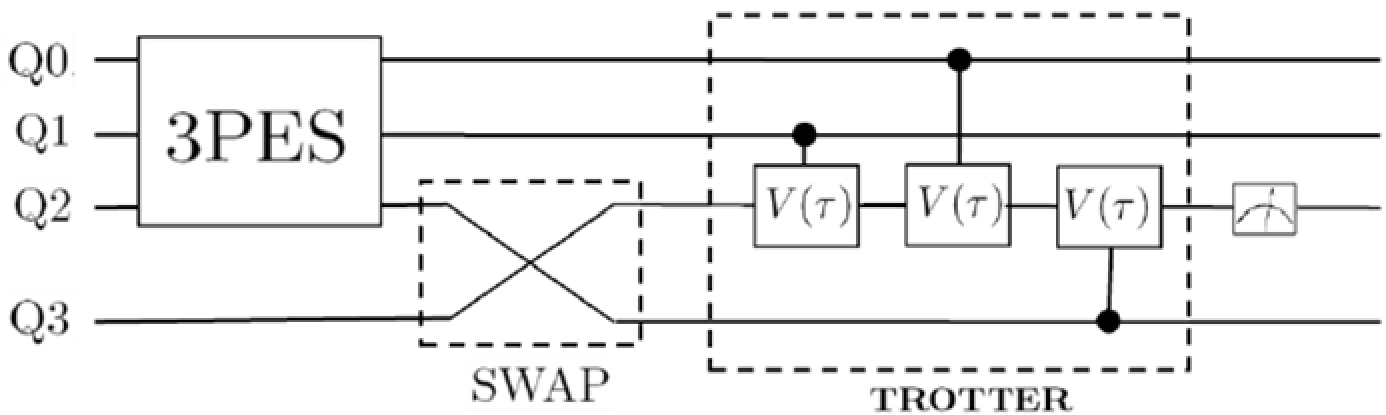
The results of our experiment (a) and theory (b) for $\Delta n_c(\tau)$ as a function of the dimensionless time τ for the Trotter number $N = 3$. Different curves correspond to different values of phase parameter φ entering the initial state.

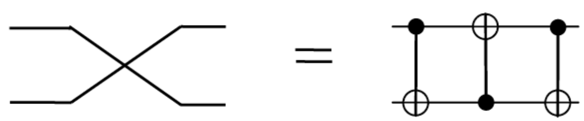
- Initial state of the system – entangled "bath"

$$\Psi(0) = |\downarrow\rangle \otimes \frac{1}{\sqrt{6}} \left(|\downarrow\downarrow\uparrow\rangle - 2e^{i\chi} |\downarrow\uparrow\downarrow\rangle + |\uparrow\downarrow\downarrow\rangle \right)$$



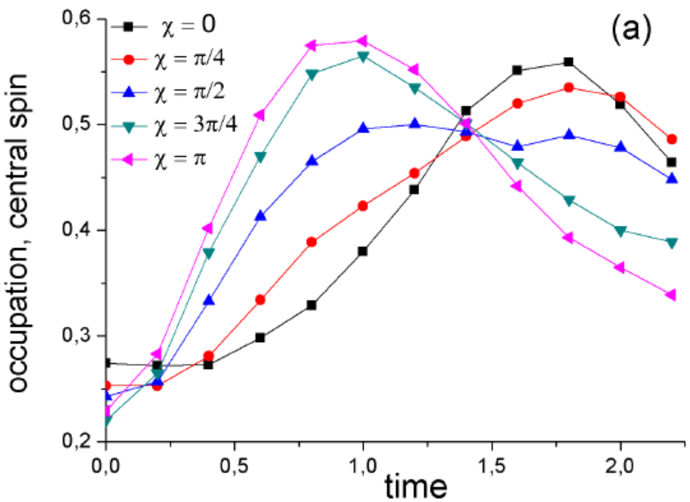
(a) (b)



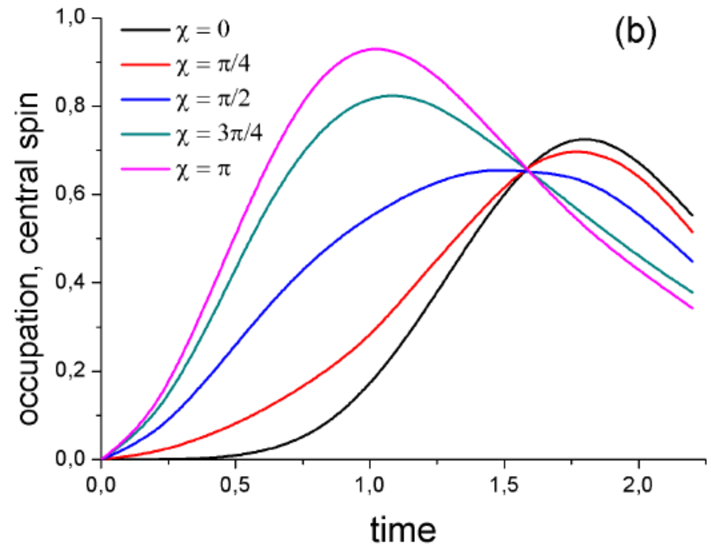


Three-particle entangled state: Population of central particle

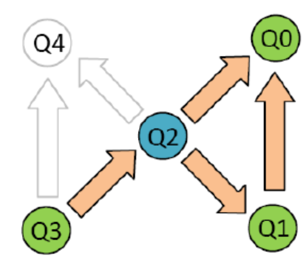
experiment



theory



$$\Psi(0) = |\downarrow\rangle \otimes \frac{1}{\sqrt{6}} \left(|\downarrow\downarrow\uparrow\rangle - 2e^{i\chi} |\downarrow\uparrow\downarrow\rangle + |\uparrow\downarrow\downarrow\rangle \right)$$

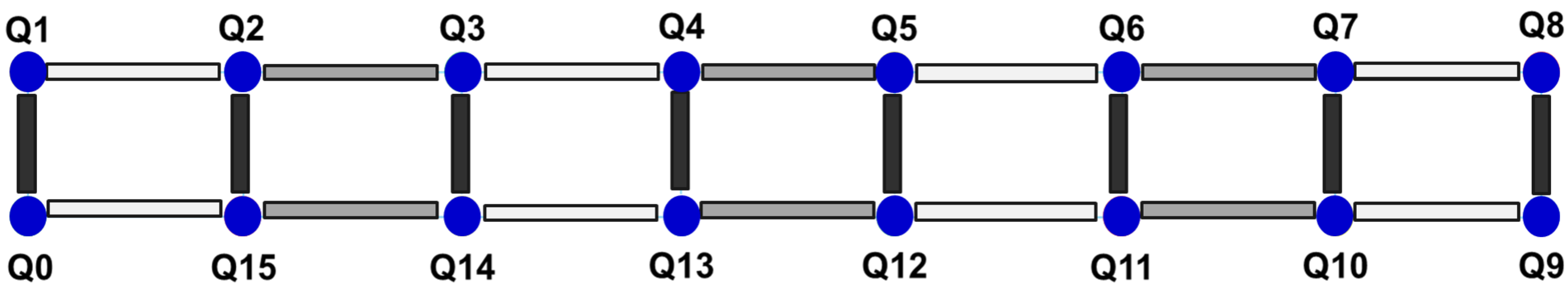


- Dark and bright states: quantum superpositions of two-particle entangled states
- Entanglement in the bath and quantum interference effects block excitation transfer to the center

Transverse-field Ising model and 16-qubit IBM device

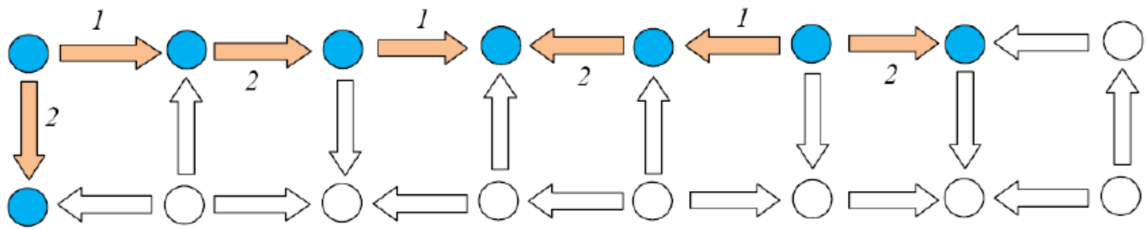
- Ising model in a transverse field – simplest and most popular
Playground to study far-from-equilibrium dynamics and thermalization.
- Non-stochastic and nonintegrable model.

$$H = -J \sum_{\langle i,j \rangle} \sigma_z^i \sigma_z^j - \alpha \sum_i \sigma_x^i$$



$|\downarrow \ldots \downarrow\rangle$ initial state

8-spin Ising chain after 1 Trotter step: experiment vs theory



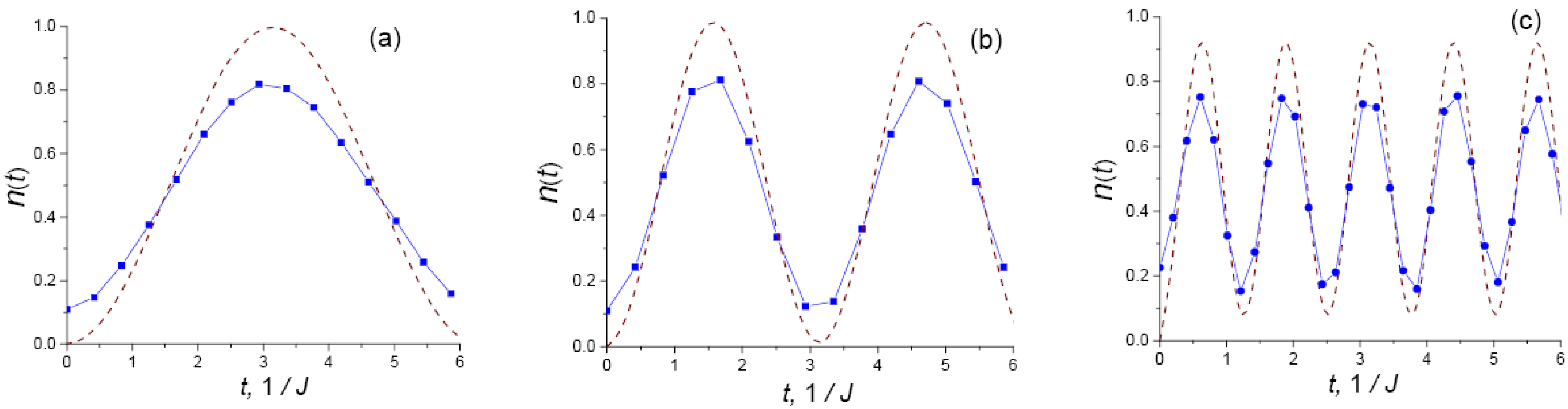
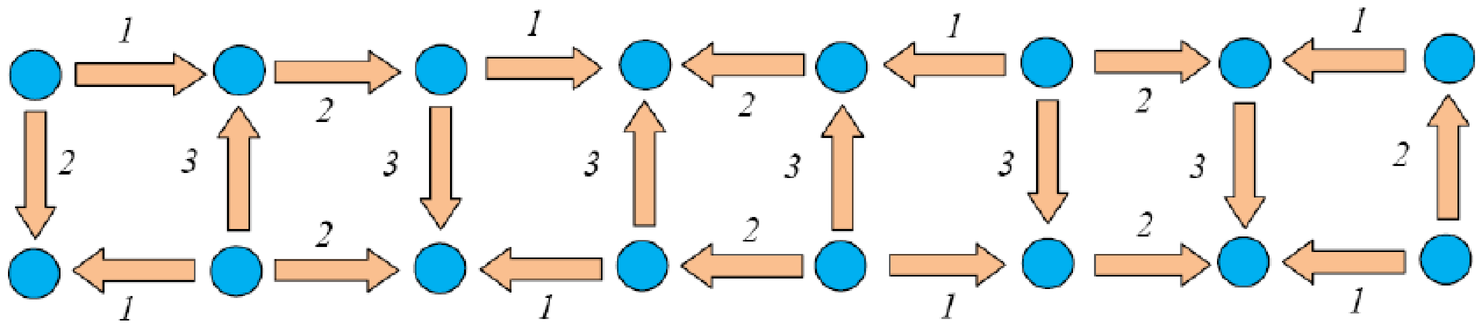


Fig. 15 (Color online) The results of our experiment (solid blue lines) and theory (dashed brown lines) for the mean occupation n of the upper levels of the 8-spin transverse Ising chain at $\alpha = J$ (a), $\alpha = 2J$ (b), $\alpha = 5J$ (c) as a function of the time t for the Trotter number $N = 1$.

$$V(\tau) = \frac{n(\tau) - n(0)}{\max n(\tau) - n(0)}.$$

Error mitigation in the large error regime

16-spin Ising ladder after 1 Trotter step: experiment vs theory



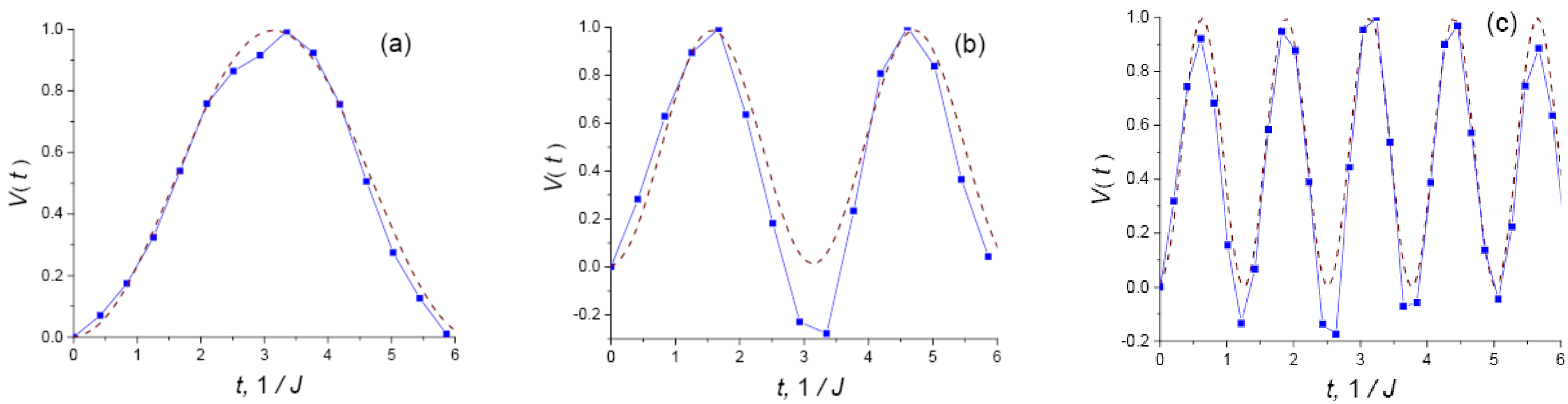


Fig. 18 (Color online) The results of our experiment (solid blue lines) and theory (dashed brown lines) for V defined in Eq. (10) in the case of the 16-spin transverse Ising ladder at $\alpha = J$ (a), $\alpha = 2J$ (b), $\alpha = 5J$ (c) as a function of the dimensionless time τ for the Trotter number $N = 1$.

$$V(\tau) = \frac{n(\tau) - n(0)}{\max n(\tau) - n(0)}.$$

Error mitigation in the large error regime

Error mitigation: **2** Trotter steps for 8-spin chain

$$V(\tau) = \frac{n(\tau) - n(0)}{\max n(\tau) - n(0)}.$$

Analysis of variations (properly normalized)

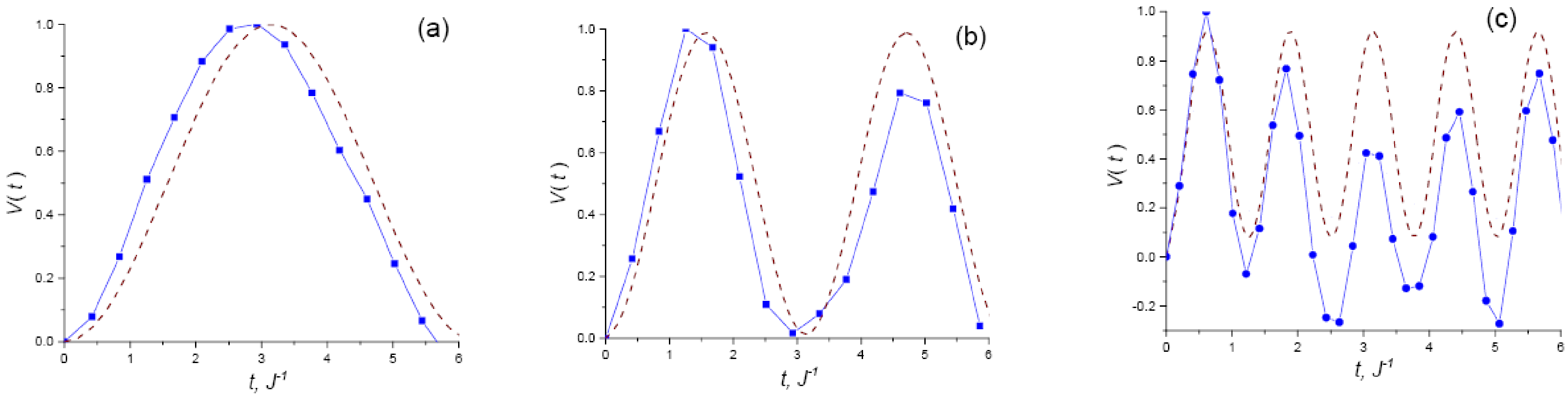


Fig. 16 (Color online) The results of our experiment (solid blue lines) and theory (dashed brown lines) for V defined in Eq. (10) in the case of the 8-spin transverse Ising chain at $\alpha = J$ (a), $\alpha = 2J$ (b), $\alpha = 5J$ (c) as a function of the dimensionless time τ for the Trotter number $N = 2$.

Entropy-based characteristics

Mutual information

$$\mathcal{I}(A,B) = H(B) - H(B|A),$$

between the Alice's input $A = (a_1, a_2)$ and Bob's output $B = (b_1, b_2)$.

$$H(X) = -\sum_x \Pr(X = x) \log_2 \Pr(X = x)$$

is a Shannon entropy of a random variable X with possible values $\{x\}$ and

$$H(X|Y) = -\sum_y \Pr(Y = y) \sum_x \Pr(X = x|Y = y) \log_2 \Pr(X = x|Y = y)$$

is conditional entropy of X given random variable Y with possible values $\{y\}$.

For the ideal system: $\mathcal{I}(A,B) = 2$

$$\boxed{\mathcal{I}(A,B) > 1 - \text{"quantum advantage"}}$$

Evaluation of mutual information is the most rigorous way to quantify an efficiency of the protocol implementation

Quantum key distribution BB84

The length of final (identical and secure) keys K_A^{sift} and K_B^{sift} is given by

$$l_{\text{sec}} = N(1 - h(q)) - N f_{\text{ec}} h(q),$$

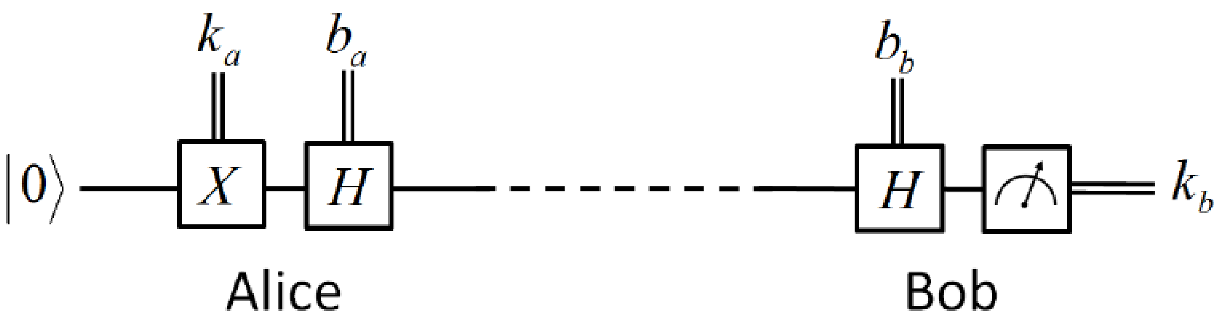
where N is length of sifted keys, q is an error between K_A^{sift} and K_B^{sift}

$$h(q) = -q \log_2 q - (1 - q) \log_2 (1 - q)$$

is binary entropy function and f_{ec} is "efficiency" of information reconciliation algorithm (in all the further considerations we take $f_{\text{ec}} = 1.15$, that correspond to real practise [44]). The expression (9) gives a length to which the reconciled sifted keys should be shortened by employing publicly announced random hash function from universal$_2$ set at the stage of privacy amplification [45]. Note, that negatives values of l_{sec} correspond to the fact of impossibility to distill the provably secure keys.

Alice encodes 0 or 1 of a key in the qubit Q1 using single-qubit gates I or X, respectively. After that, we choose the basis "+" or "×" by applying single-qubit gates I or H respectively. Then, we apply a train of identity gates. Finally, Bob measures this qubit in the same basis "+" or "×" (we analyze a sifted key). A set of single measurements.

Alice and Bob are now at the same site (qubit Q1)



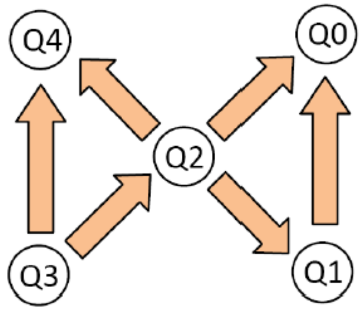


Table 5 The error distribution for BB84 protocol for different values of time delay. For each input, 8192 runs of the algorithm on 5-qubit IBMqx4 device have been performed.

Basis, bits	Time, μs					
	0.0	1.2	2.4	3.6	4.8	6.0
+,0	0.008	0.011	0.009	0.010	0.008	0.005
×,0	0.011	0.027	0.052	0.081	0.098	0.120
+,1	0.051	0.076	0.095	0.119	0.177	0.251
×,1	0.050	0.071	0.091	0.122	0.176	0.260

Table 7 The error distribution for BB84 protocol for different number of SWAPs. Each logical qubit has been composed from two physical qubits. Post-selection procedure has been applied. For each input, 8192 runs of the algorithm on 5-qubit IBMqx4 device have been performed. Numbers in brackets indicate fractions of data accepted after the post-selection.

Basis, bits	SWAPs			
	0	2	4	6
+,0	0.003 (90%)	0.028 (85%)	0.048 (79%)	0.076 (75%)
×,0	0.024 (86%)	0.053 (84%)	0.081 (81%)	0.111 (78%)
+,1	0.002 (89%)	0.029 (82%)	0.059 (77%)	0.094(71%)
×,1	0.021 (83%)	0.05 (76%)	0.089 (70%)	0.139 (63%)