AFRL-AFOSR-UK-TR-2016-0006

HiFi-MBQC High Fidelitiy Measurement-Based Quantum Computing using Superconducting Detectors

Philip Walther
UNIVERSITT WIEN

04/04/2016
Final Report

Air Force Research Laboratory
AF Office Of Scientific Research (AFOSR)/ IOE
Arlington, Virginia 22203
Air Force Materiel Command

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04/01/2016	Final	01-Jan-2012 to 31-Dec-2015

4. TITLE AND SUBTITLE
HiFi-MBQC High Fidelitiy Measurement-Based Quantum Computing using Superconducting Detectors

5a. CONTRACT NUMBER
FA8655-11-1-3004

5b. GRANT NUMBER
Grant 113004

5c. PROGRAM ELEMENT NUMBER
61102F

6. AUTHOR(S)
Walther, Philip

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
UNIVERSITT WIEN, DR.-KARL-LUEGER-RING 1, WIEN, , 1010, AT

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
EOARD
Unit 4515
APO AE 09421-4515

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/AFOSR/IOE (EOARD)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-AFOSR-UK-TR-2015-XXXX

12. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution A: Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The major achievement of this grant was the construction and setup of an array of superconducting nanowire single photon detectors (SNSPDs) which allowed support of quantum photonics experiments leading to 14 peer-reviewed publications. We installed and tested several SNSPDs in various configurations, moving toward four-element (four detectors per spot) assemblies achievable in the next year or so. Detector efficiencies varied from 70% to 90%, close to the current world record of 93% at the target wavelength of 1.5 um. Experiments supported include first demonstration of blind quantum computing, experimental verification of quantum computers, experimental boson sampling, and several other areas.

15. SUBJECT TERMS
EOARD, photonics, cryostat, superconducting nanowire, SNSPD

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			PUTZ, VICTOR
					19b. TELEPHONE NUMBER *(Include area code)*
Unclas	Unclas	Unclas	SAR		235-6013

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g. 30-06-1998; xx-06-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATE COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33315-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report. e.g. AFOSR-82-1234.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. 61101A.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, J, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/ restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

Final Report for for 11-3004 HiFi-MBQC
High Fidelitiy Measurement-Based Quantum Computing using Superconducting Detectors
March 2016

This project by the EOARD played a key role in pushing quantum technology beyond state of the art and in supporting experiments that demonstrated quantum computing and quantum simulations.

The main budget contribution was dedicated to develop superconducting nanowire detectors with efficiencies above 93% at telecom-wavelength. This is a major achievement and opens up optical quantum information processing with low loss in fiber networks. However, the technical challenges in developing the required and new superconducting material as well as the fabrication techniques led to significant delays. Currently the final goal of operating four-element detectors (i.e. four detectors per photon detection spot), which allow pseudo photon-resolving resolution, will take at least another year from now as the new materials' properties are still under investigation. Nevertheless, this project can be seen as extremely successfully by supporting these developments, which were done in collaboration with the US-company PhotonSpot Inc.

It is worth the mention that this project supported also quantum photonics experiments that were related to the detection of single photons for quantum information processing. Therefore, this project was also acknowledged in 14 peer-reviewed publications, among them one in Science, three in Nature Physics, and one in Nature Photonics and Nature Communications.

Development of novel superconducting nanowire single-photon detectors

With the support of this research program we are in close collaboration with the US company *Photonspot* to develop novel superconducting nanowire technology. For exploiting the full quantum efficiency of the detectors an extra-ordinary cryostats is needed that is capable to reach 0.9K and to handle a significant heat load due to the 48 coaxial cables of the targeted twelve four-element detectors.

The company *Entropy* was building our customized detector, where my PhD student Lorenzo Procopio, whose salary is funded by this project, was supporting them with the design. In January 2014 the company could finally reach the specifications, which took almost one year longer than expected. In the Figure 1a the cryostat system is shown where the different cooling stages can be seen.

During the course of this project we have installed and tested several superconducting nano-wire detectors operating at a wavelength of 1.5 um, which is the ideal wavelength for fiber-based quantum computer networks. We went through three stages of design before arriving at our current detector efficiencies. Our first prototype was a low-efficiency detector (~5% efficiency at 1.5 um) based on a Niobium-Nitride superconductor. The second prototype was based on a novel amorphous superconductor, made of a tungsten-silicide. These detectors had ~30% efficiency at 1.5 um.

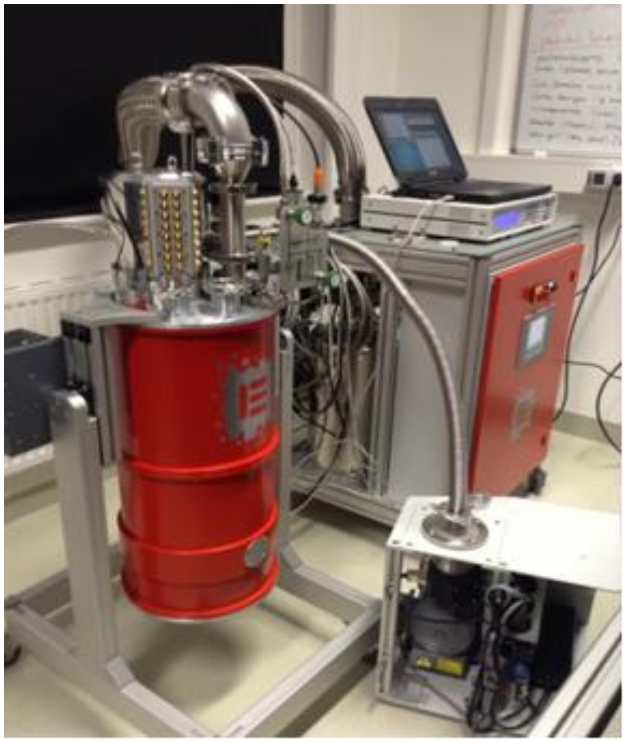

Figure 1a. Our closed cycle refrigerator. Our cooling refrigerator consists of a pulse-tube cooler mounted in a trolley with a helium compressor, buffer tank, vacuum pump station and a rack with gas handling which has the electronic control cabinet.

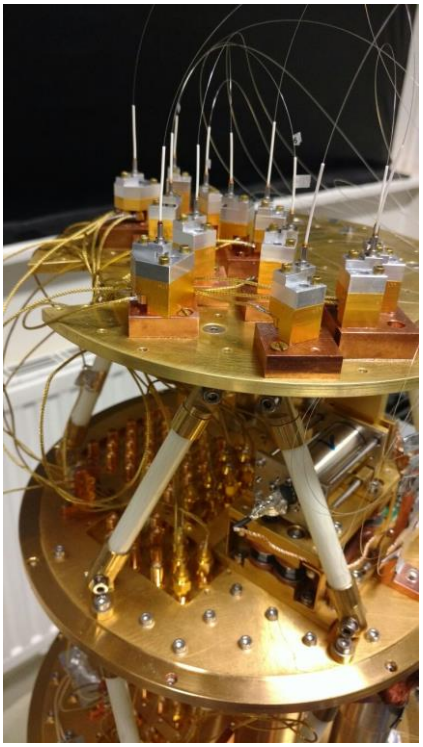

Figure1b. Our current superconducting nanowire detectors mounted inside the refrigerator. The input optical fibers and the read-out electronic wires are visible.

Our final design was also made with a tungsten-silicide, but with an optical cavity surrounding the superconductor. These detectors have extremely good performances as we measured timing jitters of ~250 ps and detection efficiencies between 70% and 90%, which is close to the world-record detection efficiency of 93% at 1.5 um. A picture of our single-photon detectors is shown in Figure 1b. The detectors are fiber-coupled to allow them to be installed in our cooling system as well as being accessible from our experimental quantum computer configuration.

The research program HiFi-MBQC supported various scientific achievements due to our improved knowledge for the detection of photons and processing of electronic signals. The list of related publications can be summarized as the following:

Related scientific achievements that were supported by Hifi-MBQC

1) First Demonstration of Blind Quantum Computing

Quantum computers, besides offering substantial computational speedups, are also expected to preserve the privacy of a computation. This project supported the experimental demonstration of the first blind quantum computing in which the input, computation, and output all remain unknown to the computer. We exploit the conceptual framework of measurement-based quantum computation that enables a client to delegate a computation to a quantum server. Various blind delegated computations, including one- and two-qubit gates and the Deutsch and Grover quantum algorithms, are demonstrated. The client only needs to be able to prepare and transmit individual photonic qubits. Our demonstration is crucial for unconditionally secure quantum cloud computing and might become a key ingredient for real-life applications, especially when considering the challenges of making powerful quantum computers widely available.

Reference: S. Barz, E. Kashefi, A. Broadbent, J. Fitzsimons, A. Zeilinger, P. Walther,
Demonstration of blind quantum computing,
Science 335, 303 (2012).

2) Experimental verification of quantum computers

Another experiment was building on the previous achievements of the so-called blind quantum computing, which allowed to address the fundamental question of verifying a quantum computer by classical means. In an experiment we could demonstrated that an almost classical proofer can interact with a quantum computer to verify the computation itself and the corresponding result. Obviously such capabilities are of importance when quantum computers or quantum simulators will soon reach the computational power that no conventional computer can calculate the result.

Reference: S. Barz, J. F. Fitzsimons, E. Kashefi, P. Walther,
Experimental verification of quantum computation,
Nature Physics 9, 727-731 (2013)

3)No-go theorem for passive single-rail linear optical quantum computing

Photonic quantum systems are among the most promising architectures for quantum computers. It is well known that for dual-rail photons effective non-linearities and near-deterministic non-trivial two-qubit gates can be achieved via the measurement process and by introducing ancillary photons. While in principle this opens a legitimate path to scalable linear optical quantum computing, the technical requirements are still very challenging and thus other optical encodings are being actively investigated. One of the alternatives is to use single-rail encoded photons, where entangled states can be deterministically generated. With the support of this project we prove that even for such

systems universal optical quantum computing using only passive optical elements such as beam splitters and phase shifters is not possible. Our result provides useful guidance for the design of optical quantum computers.

Reference: L. Wu, P. Walther, D. Lidar
No-go theorem for passive single-rail linear optical quantum computing,
Scientific Reports 3, 1394 (2013).

4) Quantum discord as resource for remote state preparation

The existence of better-than-classical quantum information processing models which consume very little or no entanglement suggests that separable or weakly entangled states could be extremely useful tools for information processing as they are much easier to prepare and control even in dissipative environments. It has been proposed that a resource of advantage is the generation of quantum discord, a measure of non-classical correlations that includes entanglement as a subset. With the support of HiFi-MBQC we show that quantum discord is the necessary resource for quantum remote state preparation. We explicitly show that the geometric measure of quantum discord is related to the fidelity of this task, which provides its operational meaning. Our results are experimentally demonstrated using photonic quantum systems. Moreover, we demonstrate that separable states with non-zero quantum discord can outperform entangled states. Therefore, the role of quantum discord might provide fundamental insights for resource-efficient quantum information processing.

Reference: B. Dakic, Y.-O. Lipp, X.S. Ma, M. Ringbauer, S. Kropatschek, S. Barz, T. Paterek, V. Vedral, A. Zeilinger, C. Brukner, P. Walther,
Quantum discord as optimal resource for remote state preparation,
Nature Physics 8, 666 (2012).

5) Experimental Boson sampling as resource-efficient intermediate quantum computation

This project allowed us to use intergrated waveguide technology for multi-photon random-walk experiments. In cooperation with the group of Prof. Alexander Szameit at the University of Jena waveguide structures were designed and fabricated using a femto-second direct-write technology. The first experiment was dedicated to demonstrate Boson-sampling computation. This intermediate model of quantum computation is of particular interest as the bosonic interference of photons in random networks is already hard to simulate on conventional computers. In contrast to universal models of photonic quantum computers that rely on ancilla photons, measurement-induced interactions, and adaptive feed-forward techniques, the boson-sampling computation requires only passive optical elements. This relaxes the physical requirements significantly such that a continuous improvement of current multi-photon sources and detection effciencies as well as reducing the losses in integrated circuits, might lead to quantum computations in regimes where classical verification is no longer possible in the near future.

Reference: M. Tillmann, B. Dakic, R. Heilmann, S. Nolte, A. Szameit, P. Walther,
Experimental Boson sampling,
Nature Photonics 7, 540-544 (2013)

6) Experimental studies for the photonic quantum simulation of frustrated Heisenberg spin systems

Recent experiments have shown that photonic quantum systems have the advantage to exploit quantum interference for the quantum simulation of the ground state of Heisenberg spin systems. With the support of the EOARD project we were able to characterize this quantum interference at a

tuneable beam splitter and further investigate the measurement-induced interactions of a simulated four-spin system by comparing the entanglement dynamics using pairwise concurrence. We also studied theoretically a four-site square lattice with next-nearest neighbor interactions and a six-site checkerboard lattice, which will be in reach of future quantum technology that is currently developed via this EOARD project.

Reference: X.S. Ma, B. Dakic, S. Kropatschek, W. Naylor, Y.-H. Chan, Z.-X. Gong, L.-M. Duan, A. Zeilinger, P. Walther,
Towards photonic quantum simulation of ground state configurations of Heisenberg square and checkerboard lattice spin systems
Scientific Reports 4, 3583(2014).

7) Review on the progress for photonic quantum simulators

This research program also supported a review article on photonic quantum simulators. The photonic quantum technology available today is reaching the stage where significant advantages arise for the simulation of interesting problems in quantum chemistry, quantum biology and solid-state physics. In addition, photonic quantum systems also offer the unique benefit of being mobile over free space and in waveguide structures, which opens new perspectives to the field by enabling the natural investigation of quantum transport phenomena.

Reference: X.S. Ma, B. Dakic, P. Walther,
Photonic toolbox for quantum simulation,
Adv. Chem. Phys. 154, 229 (2014).

8) A two-qubit photonic quantum processor and its application to solving systems of linear equations

Large-scale quantum computers will require the ability to apply long sequences of entangling gates to many qubits. In a photonic architecture, where single-qubit gates can be performed easily and precisely, the application of consecutive two-qubit entangling gates has been a significant obstacle. With the support of the EOARD project we could demonstrate a two-qubit photonic quantum processor that implements two consecutive Control-NOT gates on the same pair of polarisation-encoded qubits. To demonstrate the flexibility of our system, we implemented various instances of the quantum algorithm for solving of systems of linear equations.

Reference: S. Barz, I. Kassal, M. Ringbauer, Y.O. Lipp, B. Dakic, A. Aspuru-Guzik, P. Walther,
A two-qubit photonic quantum processor and its application to solving systems of linear equations,
Scientific Reports 4, 6115 (2014).

9) Investigation of crucial elements of measurement-based quantum error correction

In measurement-based quantum computing an algorithm is performed by measurements on highly entangled resource states. Within the EOARD project we could consider measurement-based information processing in the presence of noise and demonstrate quantum error detection. We implemented the protocol using a four-qubit photonic cluster state where we first encode a general qubit nonlocally such that phase errors can be detected. We then read out the error syndrome and analyze the output states after decoding. Our demonstration showed a building block for measurement-based quantum computing which is crucial for realistic scenarios.

Reference: S. Barz, R. Vasconcelos, C. Greganti, M. Zwerger, W. Dür, H. J. Briegel, P. Walther,
Demonstrating elements of measurement-based quantum error correction
Physical Review A 90, 042302 (2014).

10) Experimental superposition of orders of quantum gates for achieving computational speed-up with respect to regular quantum computers

Quantum computers achieve a speed-up by placing quantum bits in superpositions of different states. However, it has recently been appreciated that quantum mechanics also allows one to superimpose different operations. Furthermore, it has been shown that using a qubit to coherently control the gate order allows one to accomplish a task determining if two gates commute or anti-commute with fewer gate uses than any known quantum algorithm. With the support of the EOARD project we experimentally demonstrated this advantage, in a photonic context. We created the required superposition of gate orders by using additional degrees of freedom of the photons encoding our qubits. The new resource we exploited allows quantum algorithms to be implemented with an efficiency unlikely to be achieved on a fixed gate-order quantum computer.

Reference: L. M. Procopio, A. Moqanaki, M. Araújo, F.Costa, I. A. Calafell, E. G. Dowd,D. R. Hamel, L. A. Rozema, Č. Brukner, P. Walther,
Experimental superposition of orders of quantum gates
Nature Communications 6, 7913 (2015).

11) Practical and efficient experimental characterization of multiqubit stabilizer states

Vast developments in quantum technology have enabled the preparation of quantum states with more than a dozen entangled qubits. The full characterization of such systems demands distinct constructions depending on their specific type and the purpose of their use. Here we present a method that scales linearly with the number of qubits, for characterizing stabilizer states. Our approach allows simultaneous extraction of information about the fidelity, the entanglement and the nonlocality of the state and thus is of high practical relevance. We demonstrate the efficient applicability of our method by performing an experimental characterization of a photonic four-qubit cluster state and three- and four-qubit Greenberger-Horne-Zeilinger states. Our scheme can be directly extended to larger-scale quantum information tasks.

Reference: Ch. Greganti, M.-C. Roehsner, S. Barz, M. Waegell, P. Walther
Practical and efficient experimental characterization of multiqubit stabilizer states
Physical Review A 91, 022325 (2015).

12) Linear-Optical Generation of Eigenstates of the Two-Site XY Model

Much of the anticipation accompanying the development of a quantum computer relates to its application to simulating dynamics of another quantum system of interest. Within this project we study the building blocks for simulating quantum spin systems with linear optics. We experimentally generate the eigenstates of the XY Hamiltonian under an external magnetic field. The implemented quantum circuit consists of two control-NOT gates, which are realized experimentally by harnessing entanglement from a photon source and by applying a control-Phase gate. We tune the ratio of coupling constants and magnetic field by changing local parameters. This implementation of the XY model using linear quantum optics might open the door to the future studies of quenching dynamics using linear optics.

Reference: S. Barz, B. Dakic, Y.-O. Lipp, F. Verstraete, J.D. Whitfield, P. Walther
Linear-Optical Generation of Eigenstates of the Two-Site XY Model
Physical Review X , 021010 (2015).

13) Generalized Multiphoton Quantum Interference

With the support of Hifi-MBQC we exploit tunable distinguishability to reveal the full spectrum of multiphoton nonclassical interference. We investigate this in theory and experiment by controlling the delay times of three photons injected into an integrated interferometric network. We derive the entire coincidence landscape and identify transition matrix immanants as ideally suited functions to describe the generalized case of input photons with arbitrary distinguishability. We introduce a compact description by utilizing a natural basis that decouples the input state from the interferometric network, thereby providing a useful tool for even larger photon numbers.

Reference: M. Tillmann, S.-H. Tan, S. E. Stoeckl, B.C. Sanders, H. de Guise, R. Heilmann, S. Nolte, A. Szameit, P. Walther
Generalized Multiphoton Quantum Interference
Physical Review X 5, 041015 (2015).

14) Demonstration of measurement-only blind quantum computing

Blind quantum computing allows for secure cloud networks of quasi-classical clients and a fully-fledged quantum server. Recently, a new protocol has been proposed, which requires a client to perform only measurements. With the support of this EOARD project we demonstrate a proof-of-principle implementation of this measurement-only blind quantum computing, exploiting a photonic set-up to generate four-qubit cluster states for computation. Feasible technological requirements for the client and the device-independent blindness make this scheme very applicable for future secure quantum networks.

Reference: Ch. Greganti, M.-C. Roehsner, S. Barz, T. Morimae, P. Walther
Demonstration of measurement-only blind quantum computing
New Journal of Physics 18, 01320 (2016.)