AFRL-AFOSR-UK-TR-2017-0020

Quantum-Enhanced Cyber Security: Experimental Computation on Quantum-Encrypted Data

Philip Walther
UNIVERSITT WIEN

03/02/2017
Final Report

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

FORM SF 298

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
13-03-2017	Final	15 Oct 2015 to 31 Dec 2016

4. TITLE AND SUBTITLE
Quantum-Enhanced Cyber Security: Experimental Computation on Quantum-Encrypted Data

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA9550-16-1-0004

5c. PROGRAM ELEMENT NUMBER
61102F

6. AUTHOR(S)
Philip Walther

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

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-AFOSR-UK-TR-2017-0020

12. DISTRIBUTION/AVAILABILITY STATEMENT
A DISTRIBUTION UNLIMITED: PB Public Release

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The main budget contribution was dedicated to develop and investigate the high-quality processing of polarization-encoded photos using laser-written waveguides. The PI developed novel techniques for reducing the photon loss when coupling to waveguide structures as well as new methods for the characterization of complex waveguide structures. All the within this project developed methods and technologies are necessary prerequisites for performing experimental quantum computations with quantum-encrypted data. Even though the project finished before such a computation could be demonstrated, it must be it must be emphasized that this project is a success by enabling the challenging and necessary developments for this ambitious goal. It is worth the mention that the scientific developments of this project contributed directly also to two additional peer-reviewed publications: one theory paper in the Journal of Optics and one experimental paper in Science Advances.

15. SUBJECT TERMS
quantum, EOARD

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			SERNA, MARIO
Unclassified	Unclassified	Unclassified	SAR	5	**19b. TELEPHONE NUMBER** *(Include area code)* 315-227-7002

Final Report for FA9550-1-6-1-0004
Quantum-enhanced cyber security:
Experimental quantum computation with quantum-encrypted data
February 2017

This project by the AFOSR played a key role in developing integrated quantum photonic technology for processing two degrees of freedom for photons: polarization and path. The main budget contribution was dedicated to develop and investigate the high-quality processing of polarization-encoded photos using laser-written waveguides. We developed novel techniques for reducing the photon loss when coupling to waveguide structures as well as new methods for the characterization of complex waveguide structures. All the within this project developed methods and technologies are necessary prerequisites for performing experimental quantum computations with quantum-encrypted data. Even though the project finished before such a computation could be demonstrated, it must be it must be emphasized that this project is a success by enabling the challenging and necessary developments for this ambitious goal.

It is worth the mention that the scientific developments of this project contributed directly also to two additional peer-reviewed publications: one theory paper in the Journal of Optics and one experimental paper in Science Advances.

Processing of hyper-encoded qubits via integrated circuits

The main effort of this project is to develop photonic integrated circuits that allow to process single-photons with arbitrary polarization and to improve reconstruction methods for complex waveguide arrays. This capability of processing polarization- and path-encoded qubits is crucial for implementing quantum-encrypted data as the polarization-degree of freedom is used for the encryption whereas the path-degree-of-freedom for implementing the quantum computer gates.

Most of integrated waveguides suffer from high dephasing and decoherence of polarization qubits. Waveguides produced via femtosecond laser writing are presently the only ones that enable to work with the polarization degree of freedom. The advantage of such waveguides is very low birefringence (relative index of refraction difference is 10^{-5}) which leads to almost no decoherence and only moderate dephasing over the typical waveguide length of 5-10cm. One of the challenges of using polarization qubits on a chip is coupling the photons from free space spontaneous parametric down-conversion sources to the chip. Efficient coupling can only be done with v-groove fiber arrays. The polarization compensation necessary for the use of single mode fibers is difficult since one side of the fiber is attached to the chip. Our group has - with the support from this project - resolved this problem by mounting the waveguide in a way that it can be moved around the coupling position in a controlled way. The polarization shift in the input/output fiber-array can be measured separately and compensated, thus making it possible to use standard single mode fibers.

An additional problem that had to be overcome was poor mode matching between the fiber arrays and the waveguide. The solution of this requires two stages. The first one is to use a special femtosecond writing technique to adiabatically lower the mode field diameter in the chip. The second one is to increase the mode-field diameter of the fiber with a process called adiabatic thermal expansion (see Fig. 1). The improvement of coupling efficiency due to better mode matching is 50%.

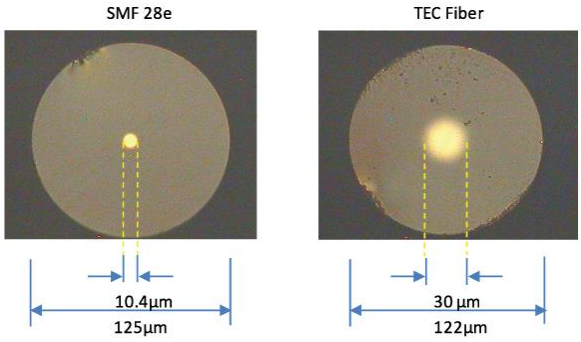

Figure 1 Example of an adiabatically increased core fiber Source:gofoton.com

Polarization waveplates on a chip have already been demonstrated. The next step was the characterization of a polarizing beam splitter (PBS) which was successfully accomplished by our group. The visibility of the PBS is around 99% (tested with coherent light). To check the capabilities of polarization qubits on chip further, two separable photons were projected into a Bell state using the integrated chip with final fidelity of 94%.

Polarization-encrypted random walks or homomorphic quantum computing on chip has not been performed yet. However, all the steps done so far are necessary prerequisites for doing so. Since the characterization of the waveguide in terms of polarization elements (waveplates, polarizing beam splitters) is almost finished and the consequences of the inherent birefringence of the chip have been addressed, such complex encrypted computations should be the next possible step.

Scientific achievements that were supported by this project

1) Optimization and discussion of various reconstruction methods for linear optical networks

Linear optical elements are pivotal instruments in the manipulation of classical and quantum states of light. Recent progress in integrated quantum photonic technology enabled the implementation of large numbers of such elements on chip, in particular passively stable interferometers. However, it is a challenge to characterize the optical transformation of such a device as the individual optical elements are not directly accessible. Thus only an effective overall transformation can be recovered. With the support of this project we present a reconstruction approach based on a global optimization of element parameters and compare it to two prominently used approaches. We numerically evaluate their performance for networks up to 14 modes and various levels of error on the primary data.

Reference: M. Tillmann, Ch. Schmidt, P. Walther,
On unitary reconstruction of linear optical networks,
Journal of Optics 18, 114002 (2016).

2) Experimental verification of an indefinite causal order

Investigating the role of causal order in quantum mechanics has recently revealed that the causal distribution of events may not be a-priori well-defined in quantum theory. While this has triggered a growing interest on the theoretical side, in particular as the superposition of quantum gate orders enables additional speed-ups with respect to regular quantum computer architectures, creating processes without a causal order is an experimental task. Supported by this project we report the first decisive demonstration of a process with an indefinite causal order. To do this, we quantify how incompatible our set-up is with a definite causal order by measuring a causal witness. This mathematical object incorporates a series of measurements which are designed to yield a certain outcome only if the process under examination is not consistent with any well-defined causal order. In our experiment we perform a measurement in a superposition of causal orders - without destroying the coherence - to acquire information both inside and outside of a causally non-ordered process. Using this information, we experimentally determine a causal witness, demonstrating by almost seven standard deviations that the experimentally implemented process does not have a definite causal order.

Reference: G. Rubino, L. Rozema, A. Feix, M. Araújo, J. Zeuner,
L. Procopio, Č. Brukner, P. Walther,
Experimental verification of an indefinite causal order,
Science Advances (in print)