AFRL-AFOSR-JP-TR-2021-0009

Feasible Quantum Technology for Secure Classical Computing

Walther, Philip
UNIVERSITT WIEN
DR.-KARL-LUEGER-RING 1
WIEN, , 1010
AT

08/03/2021
Final Technical Report

Air Force Research Laboratory
Air Force Office of Scientific Research
Asian Office of Aerospace Research and Development
Unit 45002, APO AP 96338-5002

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
03-08-2021	Final	17 May 2017 - 30 Sep 2020

4. TITLE AND SUBTITLE
Feasible Quantum Technology for Secure Classical Computing

5a. CONTRACT NUMBER
FA2386-17-1-4011

5b. GRANT NUMBER

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)
AOARD
UNIT 45002
APO AP 96338-5002

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

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-AFOSR-JP-TR-2021-0009

12. DISTRIBUTION/AVAILABILITY STATEMENT
A Distribution Unlimited: PB Public Release

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			CHRISTOPHER VERGIEN
U	U	U	SAR	10	**19b. TELEPHONE NUMBER** *(Include area code)* 315-227-7002

Final Report for AOARD Grant FA2386-17-1-4011

"**Feasible Quantum Technology for Secure Classical Computing**"

February 15th, 2020

Name of Principal Investigator: **Philip Walther**

- e-mail address: philip.walther@univie.ac.at
- Institution: University of Vienna, Faculty of Physics
- Mailing Address: Boltzmanngasse 5, 1090 Vienna, Austria, Europe
- Phone: 0043-1-4277-72561

Period of Performance: May/17/2017 – September/30/2020

Abstract:
During the last few years it was shown that quantum-enhances data protection is not only possible for communication tasks, but also for quantum computations and even classical software when quantum technology is used. This project by the AOARD played a key role in the development of feasible photonic quantum technology for quantum-enhanced security for classical and with some extend also quantum computers.
The main focus of this project was put on real-life demonstrations of so-called classical one-time programs and signatures by building an urban test network that allowed for the investigation under realistic conditions. Our demonstration of simplified schemed that exploit quantum entanglement showed that a significant increase in transmission rates is possible, while reducing the technical complexity at the same time.
In parallel, this project supported also the demonstration of homomorphically-encrypted quantum walks, which belongs to the active research field of secure quantum computing. By using customized integrated optical networks, we could show that photons are ideally suited for such tasks.
Due to the exchange and interaction with other projects in our group it is worth the mention that this project supported also quantum photonics experiments that were related to photonic quantum information processing, including new photon-photon gates exploiting the remarkable properties of graphene. Therefore, this project contributed to a few research results, which led to nine acknowledgments in peer-reviewed publications, among them one in Nature Physics, one in Nature Nanotechnology, one in Nature Communications and four in npj Quantum Information. In addition, there are two publications acknowledged that are currently under review in high-impact journals.

Introduction:
Quantum technology opens up a new era of information processing by enabling unprecedented computational speed-up for quantum computes, but also by allowing an unconditional level of cybersecurity. Whereas secure communication such as quantum cryptography has been developed and optimized since the beginning of the field of quantum information, it was just during the last decade that it has been shown that also secure computing and cloud networks are possible when exploiting quantum technological resources. Facing our globalized world, where our society heavily relies on computer networks, delegated data processing and cloud computing, such quantum-enhanced protection of user data, software information or other applications is of broad and immediate interest and thus an active field of research.
Our group has put a research focus on cybersecurity since our pioneering demonstration of blind quantum computation in 2012. Recently we have developed a scheme for unconditional security for classical computers by exploiting small and feasible quantum technology based on single photons to augment classical computer software.
With the support of this project we could improve the feasibility of hybrid quantum-classical systems for demonstrating probabilistic one-time programs between two buildings in Vienna. One-time programs are a cryptographic primitive in which a server provides a client with a software in such a way that the client can obtain only one input-output pair before the program is destroyed. Remarkably, both the input of the client and the software of the server remain private.

We could further contribute to the active field of secure quantum computing by not only demonstrating homomorphically-encrypted quantum walks, but also by showing new quantum cryptography schemes using a single photon using an interferometric network. Furthermore, we also contributed to new methods for the efficient verification of large-scale entangle quantum systems and to important photonic quantum computer technology developments, reaching from intergrated photonic quantum gates to Graphene-based nonlinearties.

Results and Discussion:
The achievements of this research project let to various scientific achievements that were evaluated via peer-review and published in established journals. In the following are the results summarized:

1) Quantum advantage for probabilistic one-time programs [Ref. 4]
At the beginning of this project we were able to finish the first proof-of-principle demonstration of probabilistic one-time programs (Fig.1). One-time programs are classical computer programs that allow a client to execute software for one and only one input without leaking this input to the software provider or the full logic of the software to the client. One-time programs have been thought to be impossible for a long time in the classical as well as the quantum case. We have, however, demonstrated in theory and experiment that allowing for a bounded probability of error enables the implementation of one-time programs encoding classical software protected by small quantum systems.
The focus of this proof-of-principle realization was to demonstrate the feasibility of such programs, which has been achieved by running several classical programs. Furthermore, the continued work on one-time programs allowed us to develop a new application which is impossible to implement classically. This application, the one-time delegation of a digital signature (Fig.2) allows a client, Bob, to sign one and only one message of his choice in Alice's name, e.g. she grants him a one-time power of attorney.

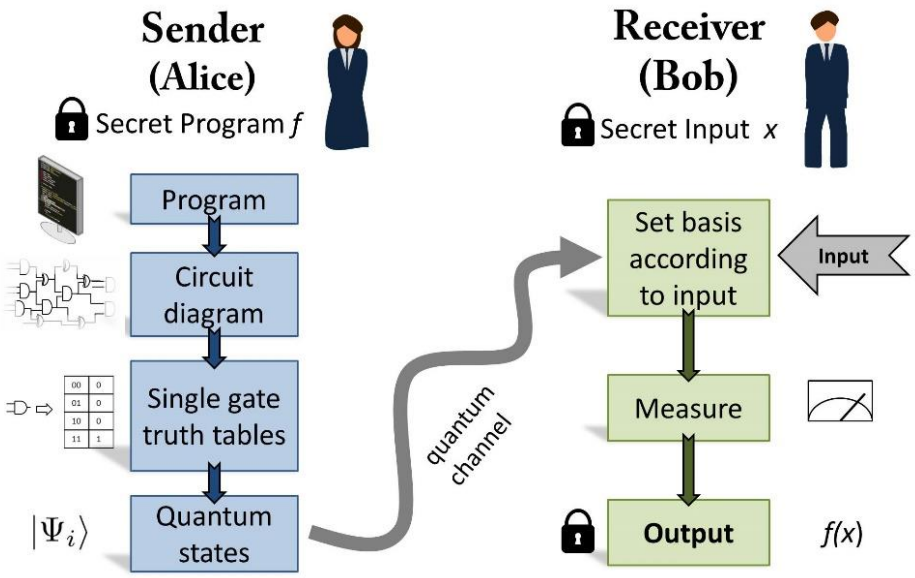
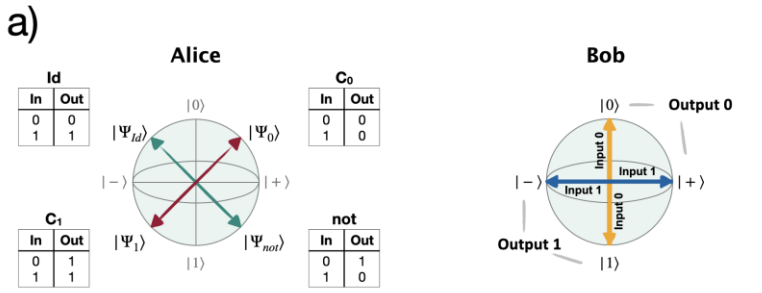
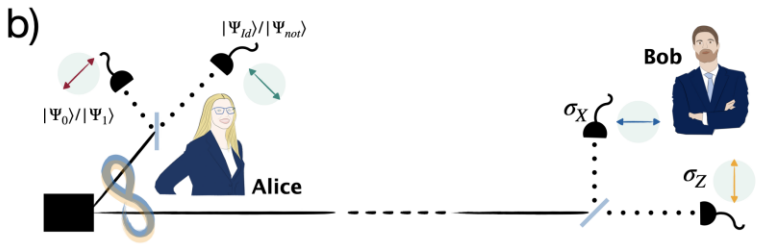


Figure 1 Overview of a probabilistic one-time program scheme. Alice possesses a secret program, f, and Bob a secret input, x. Alice converts f into a logic circuit. Next, Alice encodes the logic gates comprising the circuit as non-orthogonal quantum states. For the particular encoding scheme we realise experimentally, these are always separable states. These states are sent to Bob via a quantum channel. Bob executes the program by sequentially measuring the quantum states corresponding to individual logic gates. The basis for each measurement is determined by Bob's input to that gate and the measurement result represents the output of the gate, up to some bounded probability of error. The encoding can be chosen such that it suffices for Bob to make only single qubit measurements. Intuitively, the security of the scheme stems from the fact that the measurements corresponding to different inputs for a given gate do not commute, which prevents Bob from evaluating more than one input.

2) Probabilistic one-time programs using quantum entanglement (Ref. 13, under review)

Whereas first proof-of-principle experiments of one-time programs demonstrated the feasibility of such quantum software, the practical applications were limited due to the requirement of using the software on-the-fly combined with technological challenges due to the need for active optical switching and a large amount of classical communication. With the help of this project we were able to develop an improved protocol for one-time programs that resolves major drawbacks of previous schemes, by employing entangled qubit pairs (Fig.2). This results in four orders of magnitude higher count rates as well the ability to execute a program long after the quantum information exchange has taken place. We demonstrate our protocol over an underground fiber link between university buildings in downtown Vienna (Fig.3). Finally, together with our implementation of a one-time delegation of signature authority this emphasizes the compatibility of our scheme with prepare-and-measure quantum internet networks.





Run #	1	2	3	4	5	6	7	8	9	10	11	12
Gate Alice projects on	C_0	Id	not	C_1	Id	C_1	C_0	not	Id	C_1	not	C_0
Gate sent to Bob	C_1	not	Id	C_0	not	C_0	C_1	Id	not	C_0	Id	C_1
Measurement Basis Bob	σ_X	σ_Z	σ_Z	σ_X	σ_Z	σ_X	σ_X	σ_X	σ_Z	σ_Z	σ_X	σ_Z
Input	1	0	0	1	0	1	1	1	0	0	1	0
Output	1	1	0	0	1	0	1	1	1	0	1	1

Figure 2: Scheme for probabilistic one-time programs: a) shows the truth tables defining all possible 1-bit logic gates together with the quantum states representing the different G1 gates on the Blochsphere. In b) we give the mapping of Bob's binary inputs to a measurement basis. An input of 0 maps to a measurement in the σZ (Z) basis while an input of 1 maps to a measurement in the σX (X) basis. Outputs are defined to be 0 if Bob projects onto the positive eigenstate and 1 for the negative eigenstate. The success probability of the gates is given by PS ≈ 0.85. b) Establishing the shared table- Alice randomly prepares one of the four possible 1-bit gate-OTPs by randomly measuring her |Bell-state in one of the two bases. This collapses Bob's qubit into the orthogonal state which is sent over a quantum channel to Bob. He will randomly measure in σZ or σX, corresponding to a random input of 0 or 1 to the gate. Alice notes the gates sent (blue shaded row) and Bob the inputs and outputs of the gate (red shaded row). These (classical) records form the shared table which will later be used to execute a program. Alice and Bob repeat this procedure until a sufficient amount of gate-OTPs has been exchanged. To increase clarity of the illustrations the gates are shown here with a 100% success probability. In a real implementation Bob will receive the correct output with a probability of PS ≈ 0.85.

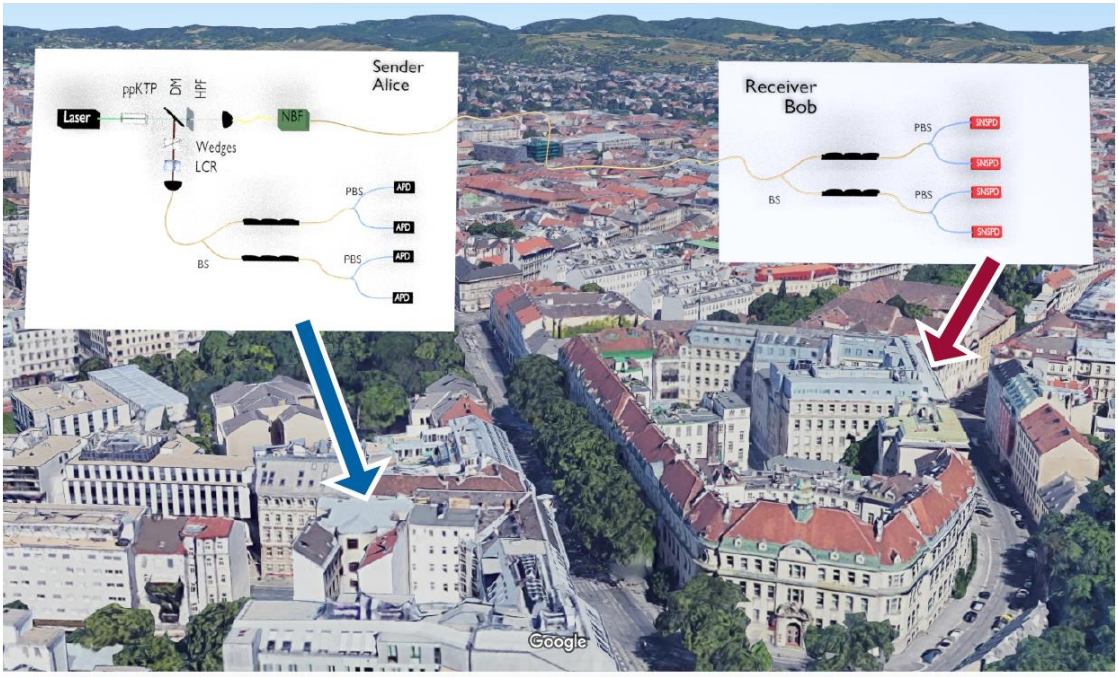


Figure 3: Experimental setup and approximate fiber path connecting Alice and Bob: The labo ratories of Alice and Bob are located at different buildings of the University in Vienna, but c onnected by a quantum channel consisting of a single-mode fiber with a length of 641m. Pol arization entangled photons are created via SPDC using a 515nm cw-pump-laser directed on to a ppKTP crystal, emitting polarisation-entangled photon pairs that are used for implementi ng one-time programs and delegated digital signatures.

3) Experimental Two-Way Communication with One Photon [Ref 7]

Supported by this AOARD project we were able to perform the experimental demonstration of two-way communication between two distant parties that can exchange only a single particle once, an impossible task in classical physics. This was achieved through preparation of a single photon in a coherent superposition of the two parties' locations. Furthermore, it was shown that this concept allows the parties to perform secure and anonymous quantum communication employing one particle per transmitted bit. These important features can lead to the realization of new quantum communication schemes, which are simultaneously anonymous, secure, and resource-efficient

4) Trace-free counterfactual communication with a nanophotonic processor [Ref. 6]

Another project was dedicated to the demonstration of counterfactual communication. Here, particles and information can travel in opposite directions. In essence, the quantum Zeno effect allows Bob to transmit a message to Alice by encoding information in particles he never interacts with. A first remarkable protocol for counterfactual communication relied on thousands of ideal optical operations for high success rate performance. Experimental realizations of that protocol have thus employed post-selection to demonstrate counterfactuality. This post-selection, together with arguments concerning a so-called “weak trace” of the particles traveling from Bob to Alice, have led to a discussion regarding the counterfactual nature of the protocol. Here we circumvent these controversies, implementing a new, and fundamentally different, protocol in a programmable nanophotonic processor, based on reconfigurable silicon-on-insulator waveguides that operate at telecom wavelengths (Fig.4).

This, together with our telecom single-photon source and highly efficient superconducting nanowire single-photon detectors, provides a versatile and stable platform for a high-fidelity implementation of counterfactual communication with single photons, allowing us to actively tune the number of steps in the Zeno measurement, and achieve a bit error probability below 1%, without post-selection and with a vanishing weak trace. Our demonstration shows how our programmable nanophotonic processor could be applied to more complex counterfactual tasks and quantum information protocols.

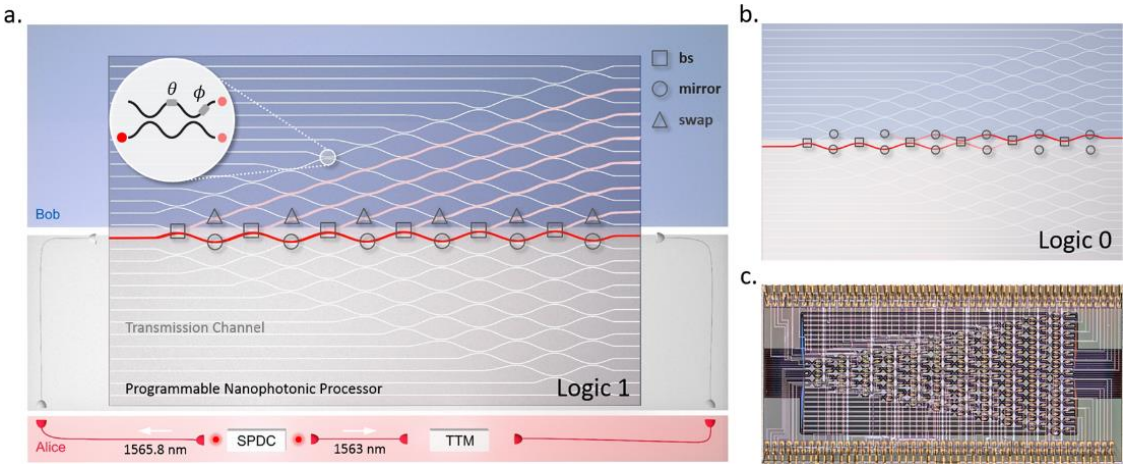


Figure 3 Experimental scheme using a tuneable nanophotonic processor for demonstrating the counterfactual communication protocol. a) b) Our experiment is implemented in a programmable nanophotonic processor (PNP), which is composed of 26 interconnected waveguides. The waveguides are coupled by 88 Mach-Zehnder interferometers (MZIs), as indicated by the top-left inset. Each MZI is equipped with a pair of thermo-optic phase shifters, which allows us to treat them as beamsplitters with fully tunable reflectivities. c)Micrograph of the PNP with dimensions 4.9 × 2.4 mm.

5) Experimental Quantum Homomorphic Encryption [Ref 9]

Building on the scientific achievements that were support by the previous EOARD project "Quantum-enhanced cyber security: Experimental quantum computation with quantum-encrypted data (FA9550-1-6-1-0004)", this program supported also the demonstration of a quantum homomorphic encryption (Fig.4). Homomorphic encryption is one of the most promising schemes for secure delegated computation. Here, the client's data is encrypted in such a way that the server can process it even though he cannot decrypt it. Moreover, in contrast to other protocols, the client and server do not need to communicate during the computation; because of this feature, the coherence times required for homomorphic-encrypted quantum computation are much shorter than those for, e.g., blind quantum computation, dramatically boosting the protocol's performance and practicality.

We used the particular advantages of photons for delegated computing to demonstrate a homomorphic-encrypted quantum random walk (Fig.5). To do this, it was necessary for us to implement polarization-independent path unitaries, a major experimental challenge. Using a new annealing technique, we fabricated waveguides with very low birefringence, thus decoupling the result of a quantum random walk from the photon's polarization. Quantum random walks are interesting examples of quantum computation to demonstrate because they are classically computationally hard, while being experimentally undemanding, since feed-forward operations are not required. The security of the encrypted data in our protocol is asymptotic, scaling well with the dimension of the random walk. Furthermore, recent theoretical work indicates that future experiments taking advantage of other photonic degrees of freedom would scale even better.

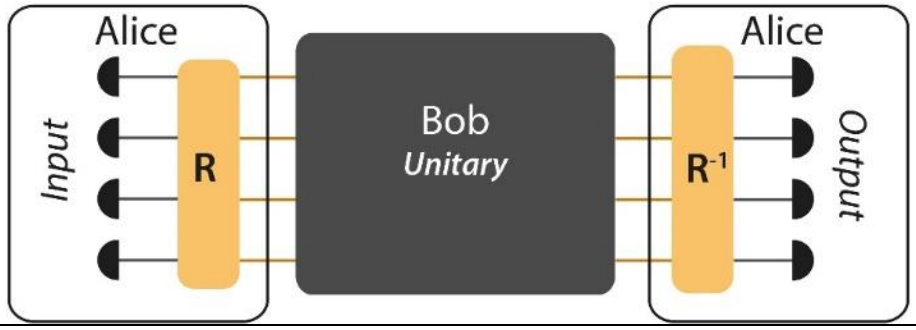


Figure 4. Homomorphic encryption protocol. Alice encrypts her plain-text input-state using a polarization rotation. Bob executes the computation on the encrypted data before returning the result to Alice which can access the decrypted result by inverting the encryption operation.

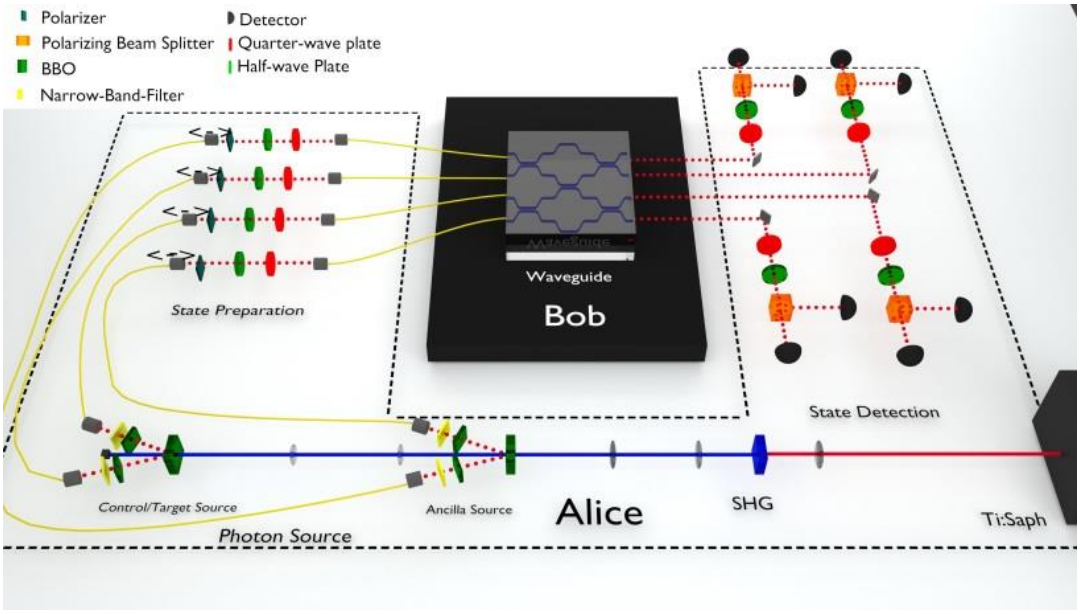


Figure 5. Experimental Setup. The photons were produced using spontaneous parametric down conversion (SPDC). The computation was carried out on the chip owned by Bob, which features special polarization independent unitaries.

6) Experimental few-copy multipartite entanglement detection (Ref 5)

Within this project we have developed a generic framework for efficient entanglement detection that translates any entanglement witness into a resource-efficient probabilistic scheme, whose confidence grows exponentially with the number of individual detection events, namely copies of the quantum state. To benchmark our findings, we experimentally verify the presence of entanglement in a photonic six-qubit cluster state generated using three single-photon sources operating at telecommunication wavelengths (Fig.6). Remarkably, we find that the presence of entanglement can be certified with at least 99.74% confidence by detecting only 20 copies of the quantum state. Additionally, we show that genuine six-qubit entanglement is verified with at least 99% confidence by using 112 copies of the state.

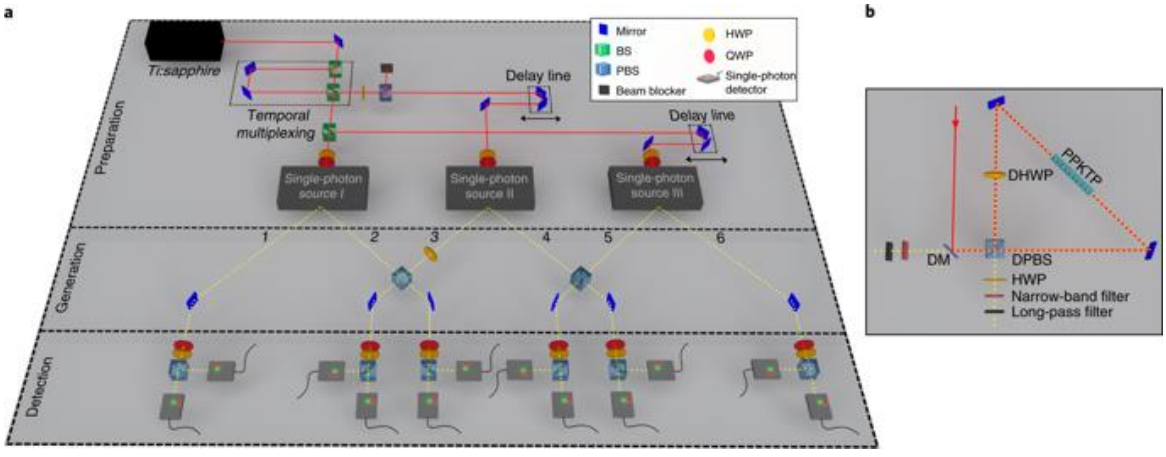


Figure 6: Experimental setup for the generation of a photonic 6-qubit cluster state that was used for implementing the developed entanglement detection method using only a few measurement detections.

7) Tuning single-photon sources for telecom multi-photon experiments (Ref 1)

Multi-photon state generation is of great interest for near-future quantum simulation and quantum computation experiments. To-date spontaneous parametric down-conversion is still the most promising process, even though two major impediments still exist: accidental photon noise caused by the probabilistic non-linear process and imperfect single-photon purity arising from spectral entanglement between the photon pairs. In this work, we overcome both of these difficulties by exploiting a passive temporal multiplexing scheme and carefully optimizing the spectral properties of the down-converted photons using periodically-poled KTP crystals. We construct two down-conversion sources in the telecom wavelength regime, finding spectral purities of > 91%, while maintaining high four-photon count rates. We use single-photon grating spectrometers together with superconducting nanowire single-photon detectors to perform a detailed characterization of our multi-photon source. Our methods provide practical solutions to produce high-quality multi-photon states, which are in demand for many quantum photonics applications.

8) Integrated-optics heralded controlled-NOT gate for polarization-encoded qubits (Ref 2)

Recent progress in integrated-optics technology has made photonics a promising platform for quantum networks and quantum computation protocols. Integrated optical circuits are characterized by small device footprints and unrivalled intrinsic interferometric stability. Here, we take advantage of femtosecond-laser-written waveguides' ability to process polarization-encoded qubits and present an implementation of a heralded controlled-NOT gate on chip. We evaluate the gate performance in the computational basis and a superposition basis, showing that the gate can create polarization entanglement between two photons. Transmission through the integrated device is optimized using thermally expanded core fibers and adiabatically reduced mode-field diameters at the waveguide facets. This demonstration underlines the feasibility of integrated quantum gates for all-optical quantum networks and quantum repeaters.

9) Quantum computing with graphene plasmons (Ref 4)

Among the various approaches to quantum computing, all-optical architectures are especially promising due to the robustness and mobility of single photons. However, the creation of the two-photon quantum logic gates required for universal quantum computing remains a challenge. Here we propose a universal two-qubit quantum logic gate, where qubits are encoded in surface plasmons in graphene nanostructures, that exploits graphene's strong third-order nonlinearity and long plasmon lifetimes to enable single-photon-level interactions. In particular, we utilize strong two-plasmon absorption in graphene nanoribbons, which can greatly exceed single-plasmon absorption to create a "square-root-of-swap" that is protected by the quantum Zeno effect against evolution into undesired failure modes. Our gate does not require any cryogenic or vacuum technology, has a footprint of a few hundred nanometers, and reaches fidelities and success rates well above the fault-tolerance threshold, suggesting that graphene plasmonics offers a route towards scalable quantum technologies.

10) Giant enhancement of 3rd-harmonic generation in graphene–metal heterostructures (Ref 8)

Nonlinear nanophotonics leverages engineered nanostructures to funnel light into small volumes and intensify nonlinear optical processes with spectral and spatial control. Owing to its intrinsically large and electrically tunable nonlinear optical response, graphene is an especially promising nanomaterial for nonlinear optoelectronic applications. Here we report on exceptionally strong optical nonlinearities in graphene–insulator–metal heterostructures, which demonstrate an enhancement by three orders of magnitude in the third-harmonic signal compared with that of bare graphene. Furthermore, by increasing the graphene Fermi energy through an external gate voltage, we find that graphene plasmons mediate the optical nonlinearity and modify the third-harmonic signal. Our findings show that graphene–insulator–metal is a promising heterostructure for optically controlled and electrically tunable nano-optoelectronic components.

List of Publications and Significant Collaborations that resulted from your AOARD supported project:

a) papers published in peer-reviewed journals,

1. "Tuning single-photon sources for telecom multi-photon experiments", C. Greganti, P. Schiansky, I. Alonso Calafell, L.M. Procopio, L.A. Rozema, P. Walther, **Optics Express** 26, 3286-3302 (2018).
2. "Integrated-optics heralded controlled-NOT gate for polarization-encoded qubits", J. Zeuner, A.N. Sharma, M. Tillmann, R. Heilmann, M. Gräfe, A. Moqanaki, A. Szameit, P. Walther, **npj Quantum Information** 4, 13 (2018).
3. "Quantum advantage for probabilistic one-time programs", M.-C. Roehsner, J. A. Kettlewell, T. B. Batalhão, J. F. Fitzsimons, P. Walther, **Nature Communications** 9, 5225 (2018).
4. "Quantum computing with graphene plasmons", I. Alonso Calafell, J. D. Cox, M. Radonjić, J. R. M. Saavedra, F. J. García de Abajo, L. A. Rozema, P. Walther, **npj Quantum Information** 5, 37 (2019).
5. "Experimental few-copy multipartite entanglement detection", V. Saggio, A. Dimić, C. Greganti, L. A. Rozema, P. Walther, B. Dakić, **Nature Physics** 15, 935–940 (2019).
6. "Trace-free counterfactual communication with a nanophotonic processor", I. Alonso Calafell, T. Strömberg, D. R. M. Arvidsson-Shukur, L. A. Rozema, V. Saggio, C. Greganti, N. C. Harris, M. Prabhu, J. Carolan, M. Hochberg, T. Baehr-Jones, D. Englund, C. H. W. Barnes, P. Walther, **npj Quantum Information** 5, 61 (2019).
7. "Experimental Two-Way Communication with One Photon", F. Massa, A. Moqanaki, Ä. Baumeler, F. Del Santo, J. A. Kettlewell, B. Dakić, P. Walther, **Advanced Quantum Technologies** (2019).
8. "Giant enhancement of third-harmonic generation in graphene–metal heterostructures", I. Alonso Calafell, L.A. Rozema, D. Alcaraz Iranzo, A. Trenti, P.K. Jenke, J.D. Cox, A. Kumar, H. Bieliaiev, S. Nanot, C. Peng, D.K. Efetov, J.Y. Hong, J. Kong, D.R. Englund, F. J. García de Abajo, F. H. L. Koppens, P. Walther, **Nature Nanotechnology** https://doi.org/10.1038/s41565-020-00808-w (2020).
9. "Experimental Quantum Homomorphic Encryption", J. Zeuner, I. Pitsios, S.-H. Tan, A.N. Sharma, J.F. Fitzsimons, R. Osellame, P. Walther, **npj Quantum Information** 7, 25 (2021)

b) papers published in peer-reviewed conference proceedings,

none

c) papers published in non-peer-reviewed journals and conference proceedings,

10. "New methods for exploiting quantum information in photons", L. Rozema, P. Walther, **SciTech Europa Quarterly** 27 (2018).
11. "Photonic quantum technology for quantum computing, data protection and fundamental quantum science", M.-C. Roehsner, P. Walther, **Open Access Government** Edition 19, 184-185 (2018).

d) conference presentations without papers,

i. "Quantum photonics for novel quantum computing and testing quantum physics foundations", Invited talk at the Photonics North 2017 Symposium on Light-Matter Interactions at the Quantum Level, University of Ottawa, Ottawa, Canada, Jun. 06, 2017.

ii. "Quantum photonics for novel quantum computing and testing quantum physics foundations", Invited talk at the META'17 - 8th International Conference on Metamaterials, Photonic Crystals and Plasmonics, University of Strathclyde, Incheon-Seoul, South Korea, Jul. 27, 2017.

iii. "Advantages of photonic quantum technology for novel quantum computing schemes", Invited talk at the Conference on Quantum Information and Quantum Control VII, The Fields Institute for Research in Mathematical Sciences, Toronto, Canada, Aug. 29, 2017.

iv. "Quantum photonics for novel quantum computing and testing quantum physics foundations", Invited talk at the Advanced School and Workshop on Quantum Science and Quantum Technologies, International Centre for Theoretical Physics, Triest, Italy, Sept. 13, 2017.

v. "Quantum computing and quantum physics foundations exploiting photonic quantum technology",

Invited talk at the International Workshop on Quantum Information, Quantum Control and Quantum Devices, Universidad del País Vasco, Bilbao, Spain, Sept. 29, 2017.

vi. "Quantentechnologie für Datensicherheit", Invited talk at the Wissenschaftsfilmtag "Bereits zugestimmt!", Vienna, Austria, Jun. 12, 2018.

vii. „Quantum Photonics for Quantum Causality and other novel Quantum Information Tasks", Invited talk at the Modern Topics in Quantum Information Workshop, Universade Federal do Rio Grande do Norte, Natal, Brazil, Aug. 01, 2018.

viii. "Integrated photonics for secure quantum computing and novel quantum communication tasks", Invited talk at the Nature Conference on Nanophotonics and Integrated Photonics, Nanjing University, Nanjing, China, Nov. 11, 2018.

ix. "Quantum photonics for secure quantum computing and counter-intuitive quantum communications", Invited seminar talk at the Paderborn University, Paderborn, Germany, Jan. 15, 2019.

x. "Quantum Photonics for Computer Security and other Applications", Invited talk at the Photonics for Quantum Workshop, Rochester Institute of Technology, Rochester, New York, USA, Jan. 24, 2019.

xi. "Quantum photonics for secure data processing and other applications", Invited colloquium talk at the University of Trento, Trento, Italy, Mar. 15, 2019.

xii. "Quantum Photonics for Computer Security and other Applications", Invited talk at the Oasis 7 - International Conference and Exhibition on Optics and Electro-Optics, The Israel Lasers and Electro Optics Society, Tel Aviv, Israel, Apr. 02, 2019.

xiii. "Quantum photonics for a new level of computer security and enhanced quantum computer architectures", Invited colloquium talk at the Weizmann Institute of Science, Rehovot, Israel, Apr. 04, 2019.

xiv. "Quantum photonics enabling novel quantum computer applications", Invited seminar talk at the University of Lubljana, Lubljana, Slovenia, May 27, 2019.

xv. "Quantum photonics for secure quantum computing and novel communication tasks", Invited talk at the 26th Central European Workshop on Quantum Optics, Paderborn University, Paderborn, Germany, Jun. 07, 2019.

xvi. "Integrated Quantum Photonics for secure quantum computing and novel communication tasks", Invited talk at the 2019 IEEE Photonics Society Summer Topics Meeting, Institute of Electrical and Electronics Engineers, Fort Lauderdale, Florida, USA, Jul. 08, 2019.

xvii. "Quantum photonics for secure quantum and classical computing", Invited talk at the SPIE Conference on Quantum Technologies and Quantum Information Science V, The International Society for Optics and Photonics, Strasbourg, France, Sept. 10, 2019.

xviii. "Multiphoton processing using integrated optics", Invited talk at the QLIGHT2019, University of Stuttgart, Sapienza University and University of Pavia, Erice, Italy, Oct. 02, 2019.

xix. "Quantum photonics enabling novel quantum computer applications", Invited seminar talk at the Joint Quantum Institute, University of Maryland, Washington, Maryland, USA, Oct. 21, 2019.

xx. Tutorial "Quantum Technologies", Invited talk at the Vienna Graduate Conference on Complex Quantum Systems, University of Vienna, Vienna, Austria, Oct. 30, 2019.

xxi. "Quantum photonics enabling novel quantum computer applications", Invited talk at the Escola de Verão de Física de Curitiba & Workshop on Quantum Computation and Quantum Information, Universidade Federal do Paraná, Curitiba, Brazil, Feb. 11, 2020.

e) manuscripts submitted but not yet published,

12. "Experimental quantum cryptography with classical users", F. Massa, P. Yadav, A. Moqanaki, W.O. Krawec, P. Mateus, N. Paunkovic, A. Souto, P. Walther, (under review); Preprint: arXiv: 1908.01780 [quant-ph]

13. "Probabilistic one-time programs using quantum entanglement", M.-C. Roehsner, J.A. Kettlewell, J.F. Fitzsimons, P. Walther, (under review), Preprint: arXiv:2008.02294 [quant-ph]

f) provide a list any interactions with industry or with Air Force Research Laboratory scientists or significant collaborations that resulted from this work.

i. International Student Exchange Program (ISEP) for Marie-Christine Röhsner to visit Prof. Joe Fitzsimons at the National University of Singapore and the Singapore University of Technology and Design for extended discussions on the quantum advantage for probabilistic one-time programs.
Date: Aug. 16, 2017 – Aug. 31, 2017

ii. Visit of Jonas Zeuner to Max Tillmann at the Massachusetts Institute of Technology.
Date: Feb. 23, 2018 – Mar. 24, 2018

iii. Secondment of Jonas Zeuner at the group of Prof. Dirk Englund at the Massachusetts Institute of Technology. Talk "Quantum Photonics for Computer Security and other Applications" and discussions with physicists from the USAF/AFRL.
Date: Jan. 23, 2019 – Jan. 25, 2019

iv. SPIE Conference Strassbourg. Talk "Quantum photonics for secure quantum and classical computing"
Date: Sept. 09 – Sept 12, 2019